



Intercambio de inteligencia sobre ciberamenazas en AWS

# AWS Orientación prescriptiva



# AWS Orientación prescriptiva: Intercambio de inteligencia sobre ciberamenazas en AWS

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

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

---

# Table of Contents

Introducción .....	1
Modelo de intercambio de CTI .....	3
Seguridad de la nube .....	3
Seguridad en la nube .....	4
Arquitectura CTI .....	5
Implementación de una plataforma de inteligencia de amenazas .....	7
Ingerir CTI .....	8
Automatizar los controles de seguridad .....	8
Amazon GuardDuty .....	11
Amazon Route 53 Resolver Firewall de DNS .....	13
AWS Network Firewall .....	14
Ganar visibilidad .....	16
Registrar el tráfico de la red .....	16
Centralizar los hallazgos de seguridad en AWS .....	17
Integración AWS datos de seguridad con otros datos empresariales .....	19
Compartiendo el CTI .....	19
Pasos a seguir a continuación .....	22
AWS recursos .....	22
Servicio de AWS documentación .....	22
recursos STIX .....	23
Plataformas de inteligencia de amenazas .....	23
Colaboradores .....	24
Creación .....	24
Revisando .....	24
Redacción técnica .....	24
Historial de documentos .....	25
Glosario .....	26
# .....	26
A .....	27
B .....	30
C .....	32
D .....	36
E .....	40
F .....	42

---

G .....	44
H .....	45
I .....	47
L .....	49
M .....	51
O .....	55
P .....	58
Q .....	61
R .....	61
S .....	64
T .....	68
U .....	70
V .....	71
W .....	71
Z .....	72
.....	lxxiv

# Intercambio de inteligencia sobre ciberamenazas en AWS

Amazon Web Services ([colaboradores](#))

Diciembre de 2024 ([historial del documento](#))

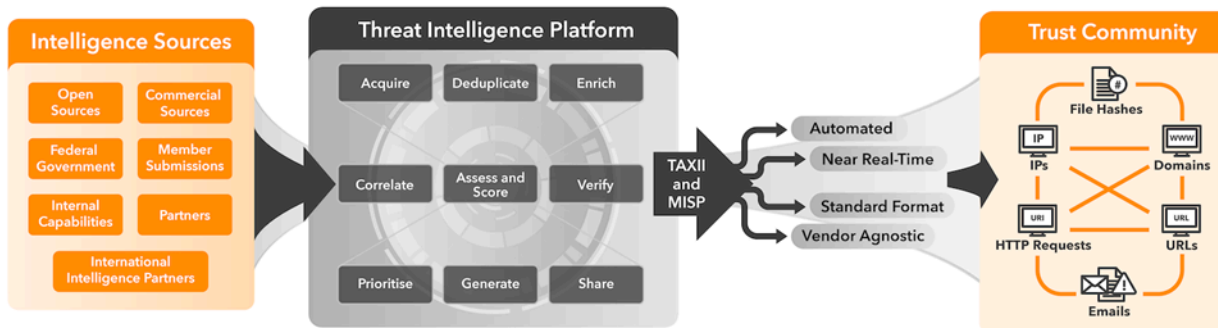
A medida que surgen nuevos riesgos, las mejores prácticas para proteger las cargas de trabajo críticas en la nube evolucionan continuamente. A medida que aumenta el número de activos conectados a Internet que requieren protección, también aumenta el riesgo de que se produzca un incidente de seguridad asociado a los actores de amenazas. La inteligencia sobre ciberamenazas (CTI) consiste en la recopilación y el análisis de datos que indican la intención, la oportunidad y la capacidad del actor de una amenaza. Se basa en pruebas y es procesable, y sirve de base para las actividades de ciberdefensa. A menudo incluye información sobre la atribución de los actores, las tácticas, las técnicas y los procedimientos, los motivos o los objetivos.

La CTI se puede compartir dentro de una organización, entre organizaciones de una comunidad de confianza, con los centros de intercambio y análisis de información (ISACs) o con otras entidades, como las autoridades gubernamentales. Algunos ejemplos de autoridades gubernamentales son el [Centro Australiano de Ciberseguridad \(ACSC\)](#) y la [Agencia Estadounidense de Ciberseguridad e Infraestructura \(CISA\)](#).

Como todas las formas de inteligencia, el contexto de las amenazas es fundamental. El uso compartido de la CTI contribuye a la gestión dinámica de los riesgos de ciberseguridad. Es esencial para una defensa, respuesta y recuperación oportunas en materia de ciberseguridad. Esto aumenta la eficiencia y la eficacia de las capacidades de ciberseguridad. El contexto de las amenazas también es esencial para distinguir entre los requisitos de capacidad de la CTI relacionados con los diferentes objetivos. Por ejemplo, los actores sofisticados pueden atacar a empresas o gobiernos específicos, mientras que los actores de productos básicos utilizan herramientas y técnicas fácilmente disponibles para atacar ampliamente a personas y organizaciones.

La planificación de la seguridad, la observabilidad, el análisis de la inteligencia sobre amenazas, la automatización del control de seguridad y el intercambio de información dentro de una comunidad de confianza son partes clave del ciclo de vida de la inteligencia sobre amenazas. AWS le ayuda a automatizar las tareas de seguridad manuales para detectar las amenazas con mayor precisión, responder más rápido y generar inteligencia sobre amenazas de alta calidad que puede compartir. Puede descubrir un nuevo ciberataque, analizarlo, generar un CTI, compartirlo y aplicarlo, todo a velocidades diseñadas para evitar que se produzca un segundo ataque.

Esta guía describe cómo implementar una plataforma de inteligencia de amenazas en AWS. Las comunidades de confianza proporcionan la CTI, y la plataforma la incorpora para identificar información útil y automatizar los controles de protección y detección del entorno. AWS La siguiente imagen muestra el ciclo de vida de la inteligencia sobre amenazas. El CTI llega desde su origen y, a continuación, la plataforma de inteligencia de amenazas lo procesa. Al utilizar el protocolo [de intercambio automatizado confiable de información de inteligencia \(TAXII\)](#) o la [plataforma de intercambio de información sobre malware \(MISP\)](#), el CTI se comparte con la comunidad de confianza para que tome medidas.



La plataforma de inteligencia de amenazas utiliza la CTI para implementar automáticamente los controles de seguridad en su AWS entorno o para notificar a su equipo de seguridad si es necesaria una acción manual. Un control preventivo es un control de seguridad diseñado para evitar que se produzca un evento. Algunos ejemplos incluyen la automatización de listas de bloqueo de direcciones IP o nombres de dominio incorrectos conocidos mediante firewalls de red, solucionadores de DNS y otros sistemas de prevención de intrusiones (IPS). Un control de detección es un control de seguridad diseñado para detectar, registrar y alertar después de que se produzca un evento. Algunos ejemplos incluyen la supervisión continua de actividades maliciosas y la búsqueda en los registros de pruebas de problemas o eventos.

Puede agrupar cualquier hallazgo en una herramienta de observación de la seguridad centralizada, como [AWS Security Hub CSPM](#) por ejemplo. Luego, puede compartir los hallazgos con una comunidad de confianza para crear de forma colaborativa un panorama integral de las amenazas.

# Modelo de responsabilidad compartida para compartir CTI

El [modelo de responsabilidad AWS compartida](#) define cómo se comparte la responsabilidad en materia de seguridad y cumplimiento en la nube. AWS protege la infraestructura en la que se ejecutan todos los servicios que se ofrecen en la nube Nube de AWS, lo que se conoce como seguridad de la nube. Usted es responsable de proteger el uso que hace de esos servicios, como sus datos y aplicaciones. Esto se conoce como seguridad en la nube.

## Seguridad de la nube

La seguridad es la máxima prioridad en AWS. Trabajamos arduamente para ayudar a evitar que los problemas de seguridad causen interrupciones en su organización. A medida que nos esforzamos por defender nuestra infraestructura y sus datos, utilizamos nuestros conocimientos a escala mundial para recopilar un gran volumen de inteligencia de seguridad, a escala y en tiempo real, con el fin de protegerlo automáticamente. Siempre que es posible, sus sistemas de seguridad interrumpen AWS las amenazas allí donde esa acción tiene más impacto. A menudo, este trabajo se lleva a cabo entre bastidores.

Todos los días, en toda la Nube de AWS infraestructura, detectamos y frustramos con éxito cientos de ciberataques que, de otro modo, podrían resultar perjudiciales y costosos. Estas victorias importantes, pero en su mayoría invisibles, se logran con una red global de sensores y un conjunto asociado de herramientas de interrupción. Al utilizar estas capacidades, dificultamos y encarecemos los ciberataques contra nuestra red e infraestructura.

AWS tiene la mayor presencia de red pública de todos los proveedores de servicios en la nube. Esto proporciona a AWS una visión incomparable y en tiempo real de determinadas actividades en Internet. [MadPotes](#) es una red de sensores de amenazas distribuida a nivel mundial (conocidos como honeypots). MadPot ayuda a los equipos AWS de seguridad a entender las tácticas y técnicas de los atacantes. Cada vez que un atacante intenta atacar uno de los sensores de amenazas, AWS recopila y analiza los datos.

Sonaris es otra herramienta interna que se utiliza en AWS para analizar el tráfico de la red. Identifica y detiene los intentos no autorizados de acceder a una gran cantidad de cuentas y recursos. Entre mayo de 2023 y abril de 2024, Sonaris rechazó más de 24 000 millones de intentos de escanear los datos de los clientes almacenados en Amazon Simple Storage Service (Amazon S3). También evitó casi 2,6 billones de intentos de descubrir cargas de trabajo vulnerables que se ejecutaban en Amazon Elastic Compute Cloud (Amazon EC2).

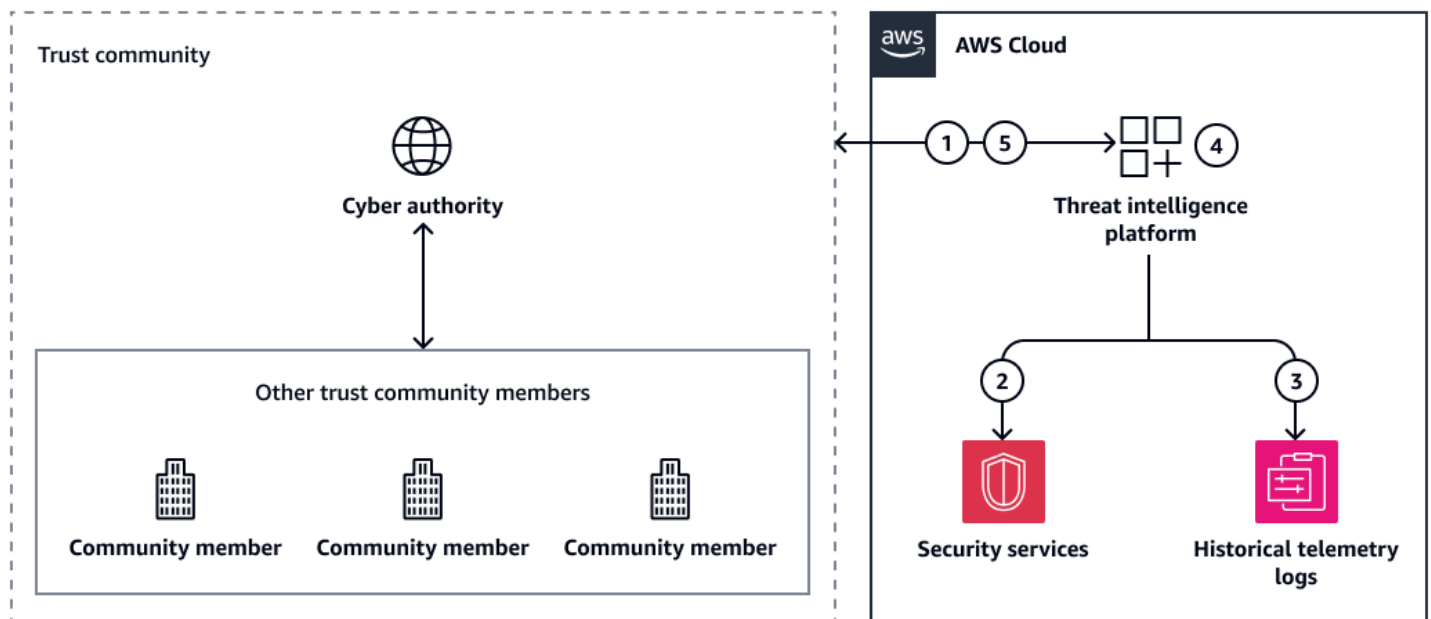
# Seguridad en la nube

Esta guía se centra en las mejores prácticas de inteligencia sobre ciberamenazas (CTI) en el. Nube de AWS. Usted es responsable de generar una CTI localizada y contextualizada. Usted controla dónde se almacenan sus datos, cómo se protegen y quién tiene acceso a ellos. AWS no tiene visibilidad de sus datos de registro, supervisión y auditoría, lo cual es esencial para la seguridad basada en la tecnología informática en la nube.

[Structured Threat Information Expression \(STIX\)](#) es un lenguaje de código abierto y un formato de serialización que se utiliza para intercambiar CTI. Los indicadores como los hashes de los archivos, los dominios URLs, las solicitudes HTTP y las direcciones IP son resultados importantes que se deben compartir para bloquear las amenazas. Sin embargo, una acción eficaz depende de información adicional, como los índices de certeza y las correlaciones entre conjuntos de intrusiones. STIX 2.1 define 18 [objetos de dominio STIX](#), incluidos el patrón de ataque, el curso de acción, el actor de la amenaza, la ubicación geográfica y la información sobre el malware. También presenta conceptos, como los índices de confianza y las relaciones, que ayudan a las entidades a diferenciar la señal del ruido en el gran volumen de datos que recopila la plataforma de inteligencia de amenazas. Puede detectar, analizar y compartir este nivel de detalle sobre las amenazas en sus AWS entornos. Para obtener más información, consulte la sección [Automatizar los controles de seguridad preventivos y de detección](#) de esta guía.

# Arquitectura de inteligencia sobre ciberamenazas en AWS

La siguiente figura muestra una arquitectura generalizada para utilizar una fuente de amenazas a fin de integrar la inteligencia sobre ciberamenazas (CTI) en su entorno. AWS La CTI se comparte entre la plataforma de inteligencia de amenazas de la entidad Nube de AWS, la autoridad cibernética seleccionada y otros miembros de la comunidad de confianza.



Muestra el siguiente flujo de trabajo:

1. La plataforma de inteligencia de amenazas recibe una CTI procesable de la autoridad cibernética o de otros miembros de la comunidad de confianza.
2. La plataforma de inteligencia de amenazas asigna a los servicios AWS de seguridad la tarea de detectar y prevenir eventos.
3. La plataforma de inteligencia sobre amenazas recibe información sobre amenazas de Servicios de AWS.
4. Si se produce un evento, la plataforma de inteligencia de amenazas selecciona una nueva CTI.
5. La plataforma de inteligencia de amenazas comparte el nuevo CTI con la autoridad cibernética. También puede compartir el CTI con otros miembros de la comunidad de confianza.

Hay muchas autoridades cibernéticas que ofrecen feeds de CTI. Algunos ejemplos incluyen el [Centro Australiano de Ciberseguridad \(ACSC\)](#), el programa [Connect Inform Share Protect \(CISP\)](#) ofrecido

por el Centro Nacional de Ciberseguridad del Reino Unido y el programa [Malware Free Networks \(MFN\)](#) ofrecido por la Oficina de Seguridad de las Comunicaciones del Gobierno de Nueva Zelanda. Muchos AWS socios también ofrecen canales para compartir información sobre CTI.

Para empezar a compartir CTI, le recomendamos que haga lo siguiente:

1. [Implementación de una plataforma de inteligencia de amenazas](#): implemente una plataforma que ingiera, agregue y organice los datos de inteligencia de amenazas de múltiples fuentes y en diferentes formatos.
2. [Recopilación de información sobre ciberamenazas](#): integre su plataforma de inteligencia sobre amenazas con uno o más proveedores de fuentes de información sobre amenazas. Cuando reciba un feed de amenazas, utilice su plataforma de inteligencia de amenazas para procesar la nueva CTI e identificar la información útil que sea relevante para las operaciones de seguridad de su entorno. Automatice en la medida de lo posible, pero hay algunas situaciones en las que es necesario tomar decisiones informadas por una persona.
3. [Automatización de los controles de seguridad preventivos y de detección](#): Implemente la CTI en los servicios de seguridad de su arquitectura que proporcionan controles preventivos y de detección. Estos servicios se conocen comúnmente como sistemas de prevención de intrusiones (IPS). Si AWS, usa las API de servicio para configurar listas de bloqueo que deniegan el acceso desde las direcciones IP y los nombres de dominio proporcionados en las fuentes de amenazas.
4. [Ganar visibilidad con mecanismos de observación](#): mientras las operaciones de seguridad se llevan a cabo en su entorno, usted recopila nuevas CTI. Por ejemplo, puede observar una amenaza incluida en el feed de amenazas o puede observar indicios de peligro asociados a una intrusión (como una vulnerabilidad de [día cero](#)). La centralización de la inteligencia de amenazas proporciona un mayor conocimiento de la situación en todo el entorno, de modo que puede revisar la CTI existente y la CTI recién descubierta en un solo sistema.
5. [Comparta la CTI con su comunidad de confianza](#): para completar el ciclo de vida de la CTI compartida, genere su propia CTI y compártala de nuevo con su comunidad de confianza.

En el siguiente vídeo, titulado [Cómo ampliar el intercambio de información sobre ciberamenazas con el Centro de Ciberseguridad de Australia](#), se analizan estos pasos con más detalle. Si bien en este vídeo se analizan las capacidades de intercambio de información y comunicación del Centro de Ciberseguridad de Australia, los pasos son los mismos, independientemente de la fuente de amenazas que elija o de su ubicación.

# Implementación de una plataforma de inteligencia de amenazas

Una plataforma de inteligencia de amenazas ingiere, agrega y organiza los datos de inteligencia de amenazas de múltiples fuentes y en diferentes formatos. Permite a los analistas ver, priorizar y actuar en función de la información sobre ciberamenazas (CTI) recibida de su comunidad de confianza.

[OpenCTI](#) y [MISP](#) son plataformas comunes de inteligencia de amenazas de código abierto. Los AWS socios también ofrecen soluciones en [AWS Marketplace](#). Debe tener en cuenta el nivel de habilidad de su equipo de seguridad al elegir una plataforma de inteligencia de amenazas. El MISP puede ser potente pero complejo, y OpenCTI tiene una interfaz de usuario más intuitiva.

Al elegir una plataforma de inteligencia de amenazas, tenga en cuenta lo siguiente:

- Características: ¿La plataforma ofrece funciones como la supervisión en tiempo real, la detección y el análisis de amenazas?
- Fuentes de datos: ¿Utiliza la plataforma una variedad de fuentes, incluidas fuentes de amenazas, inteligencia de la dark web, redes sociales e inteligencia de código abierto?
- Calidad de los datos: ¿cuenta la plataforma con procesos para garantizar que la información sea precisa y fiable?
- Escalabilidad: ¿puede la plataforma adaptarse a las necesidades cambiantes de su organización, como el crecimiento y la evolución de las amenazas?
- Integración: ¿se puede integrar la plataforma con las herramientas y la infraestructura de seguridad existentes?
- Experiencia de usuario: ¿la plataforma es fácil de navegar y usar?
- Personalización: ¿se puede personalizar la plataforma para satisfacer las necesidades específicas de su organización?
- Costo: ¿la plataforma es rentable, incluidos los costos de licencia y los requisitos de mantenimiento?

Puede implementar su plataforma de inteligencia de amenazas en su nube privada virtual (VPC). Puede implementarlo directamente en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o mediante tecnología de contenedores, como Amazon Elastic Container Service (Amazon ECS) o AWS Fargate. Para obtener más información sobre cómo elegir el servicio de AWS contenedores adecuado para el desarrollo de aplicaciones modernas, consulte [Elegir un servicio de AWS contenedores](#).

## Ingerir inteligencia sobre ciberamenazas

El primer paso del proceso de ingesta consiste en convertir los datos de inteligencia sobre ciberamenazas (CTI) de las fuentes de amenazas a un formato que su plataforma de inteligencia de amenazas pueda asimilar. Esto se denomina conversión de CTI. Los datos del feed de amenazas pueden venir en varios formatos, como [Structured Threat Information Expression \(STIX\)](#). Debe reestructurar los datos entrantes en un formato predecible y fácil de consumir que sea adecuado para los productos de seguridad que utilice en su entorno. AWS

Para lograr la máxima compatibilidad, le recomendamos que convierta los datos a un formato JSON. Por ejemplo, [AWS Step Functions](#) puede consumir datos en formato JSON y los flujos de trabajo de automatización pueden consumir este formato de manera más fácil y coherente. Encontrará más información sobre la creación de flujos de trabajo automatizados en la siguiente sección, [Automatización de los controles de seguridad preventivos y de detección](#).

Para acelerar la ingesta de datos de CTI, puede automatizar las transformaciones de datos. Los datos se convierten a medida que se ingieren y, a continuación, se transfieren directamente a la plataforma de inteligencia de amenazas. Puedes usar una AWS Lambda función para completar la transformación y puedes organizar el proceso a través Servicios de AWS de AWS Step Functions [Amazon EventBridge](#).

Cuando ingieres CTI, puedes elegir qué atributos extraer y conservar. La cantidad exacta de detalles requerida puede variar en función de las necesidades de su empresa. Sin embargo, para actualizar los firewalls y otros servicios de seguridad, recomendamos los siguientes atributos mínimos:

- Dirección IP y dominio
- Amenaza
- Añada o elimine de sus listas de amenazas internas

Extraiga los atributos que desee usar y, a continuación, formatee los en una plantilla JSON estructurada.

## Automatizar los controles de seguridad preventivos y de detección

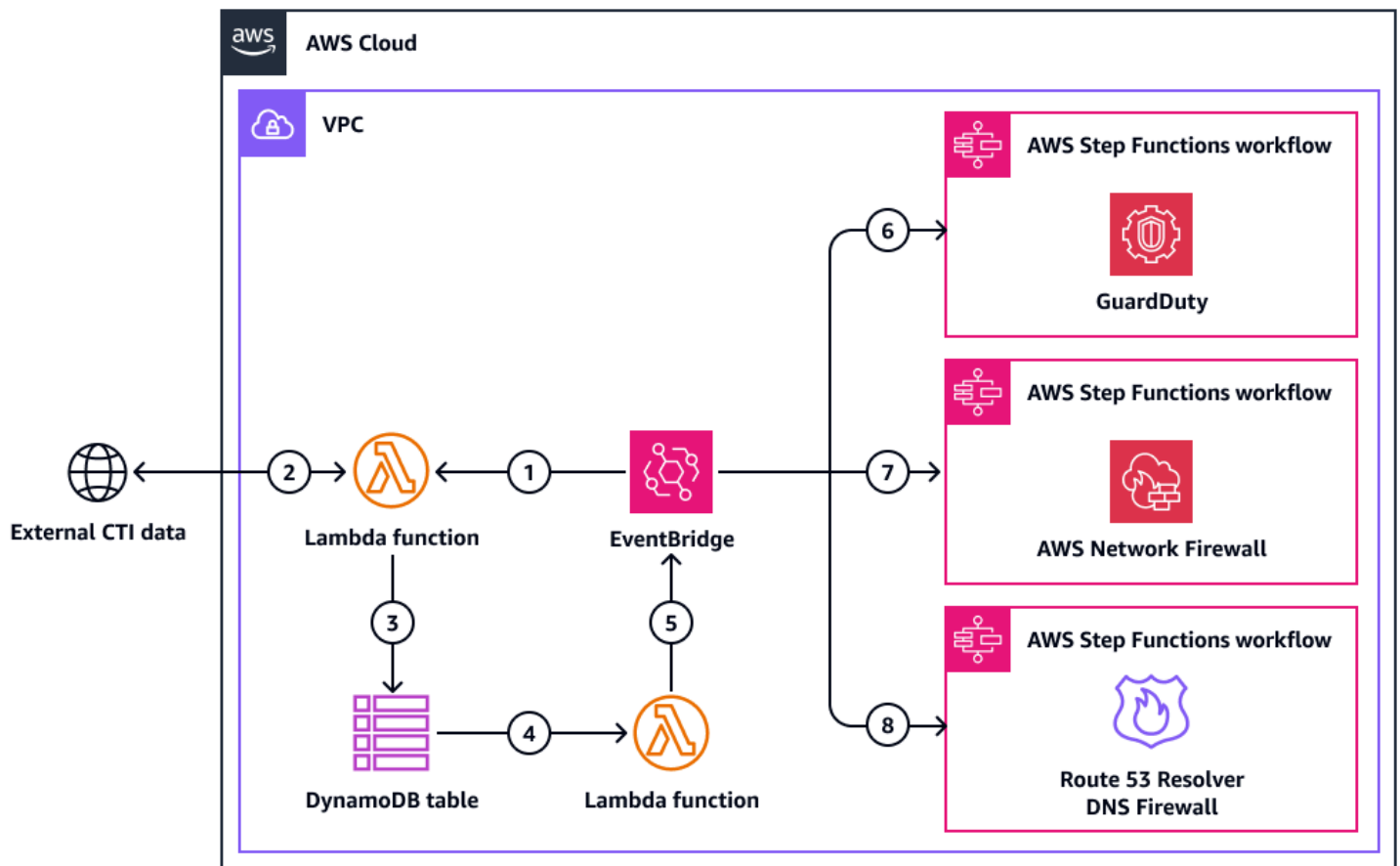
Una vez incorporada la inteligencia sobre ciberamenazas (CTI) a la plataforma de inteligencia sobre amenazas, puede automatizar el proceso de realizar cambios de configuración en respuesta a los datos. Las plataformas de inteligencia sobre amenazas le ayudan a gestionar la información sobre

ciberamenazas y a observar su entorno. Ofrecen la capacidad de estructurar, almacenar, organizar y visualizar información técnica y no técnica sobre las ciberamenazas. Pueden ayudarlo a crear una imagen de las amenazas y combinar una variedad de fuentes de inteligencia para perfilar y rastrear las amenazas, como las [amenazas persistentes avanzadas \(APT\)](#).

La automatización puede reducir el tiempo que transcurre entre la recepción de información sobre amenazas y la implementación de los cambios de configuración en el entorno. No todas las respuestas de la CTI se pueden automatizar. Sin embargo, automatizar tantas respuestas como sea posible ayuda a su equipo de seguridad a priorizar y evaluar el CTI restante de manera más oportuna. Cada organización debe determinar qué tipos de respuestas de CTI se pueden automatizar y cuáles requieren un análisis manual. Tome esta decisión en función del contexto de la organización, como los riesgos, los activos y los recursos. Por ejemplo, algunas organizaciones pueden optar por automatizar los bloqueos de dominios o direcciones IP que se sepa que son incorrectos, pero es posible que deban investigar a un analista antes de bloquear las direcciones IP internas.

En esta sección se proporcionan ejemplos de cómo configurar respuestas de CTI automatizadas en [Amazon GuardDuty](#) y [Amazon Route 53 Resolver DNS Firewall](#). [AWS Network Firewall](#) Puede implementar estos ejemplos de forma independiente. Deje que los requisitos y necesidades de seguridad de su organización guíen sus decisiones. Puede automatizar los cambios de configuración Servicios de AWS mediante un [AWS Step Functions](#) flujo de trabajo (también denominado máquina de estados). Cuando una [AWS Lambda](#) función termina de convertir el CTI al formato JSON, desencadena un EventBridge evento de [Amazon](#) que inicia el flujo de trabajo de Step Functions.

En el siguiente diagrama se muestra un ejemplo de arquitectura. Los flujos de trabajo de Step Functions actualizan automáticamente la lista de amenazas GuardDuty, la lista de dominios en Route 53 Resolver DNS Firewall y el grupo de reglas en Network Firewall.



En la figura se muestra el siguiente flujo de trabajo:

1. Un EventBridge evento se inicia de forma regular. Este evento inicia una AWS Lambda función.
2. La función Lambda recupera los datos de CTI de la fuente de amenazas externa.
3. La función Lambda escribe los datos de CTI recuperados en una tabla de Amazon DynamoDB.
4. Al escribir datos en la tabla de DynamoDB, se inicia un evento de flujo de captura de datos de cambios que inicia una función Lambda.
5. Si se han producido cambios, una función Lambda inicia un nuevo evento en EventBridge. Si no se ha producido ningún cambio, se completa el flujo de trabajo.
6. Si el CTI está relacionado con registros de direcciones IP, EventBridge inicia un flujo de trabajo de Step Functions que actualiza automáticamente la lista de amenazas en Amazon GuardDuty. Para obtener más información, consulta [Amazon GuardDuty](#) en esta sección.
7. Si el CTI se refiere a registros de direcciones IP o dominios, EventBridge inicia un flujo de trabajo de Step Functions que actualiza automáticamente el grupo de reglas de AWS Network Firewall. Para obtener más información, consulte [AWS Network Firewall](#) en esta sección.

- Si el CTI se refiere a registros de dominio, EventBridge inicia un flujo de trabajo de Step Functions que actualiza automáticamente la lista de dominios en Amazon Route 53 Resolver DNS Firewall. Para obtener más información, consulte el [Firewall de Amazon Route 53 Resolver DNS](#) en esta sección.

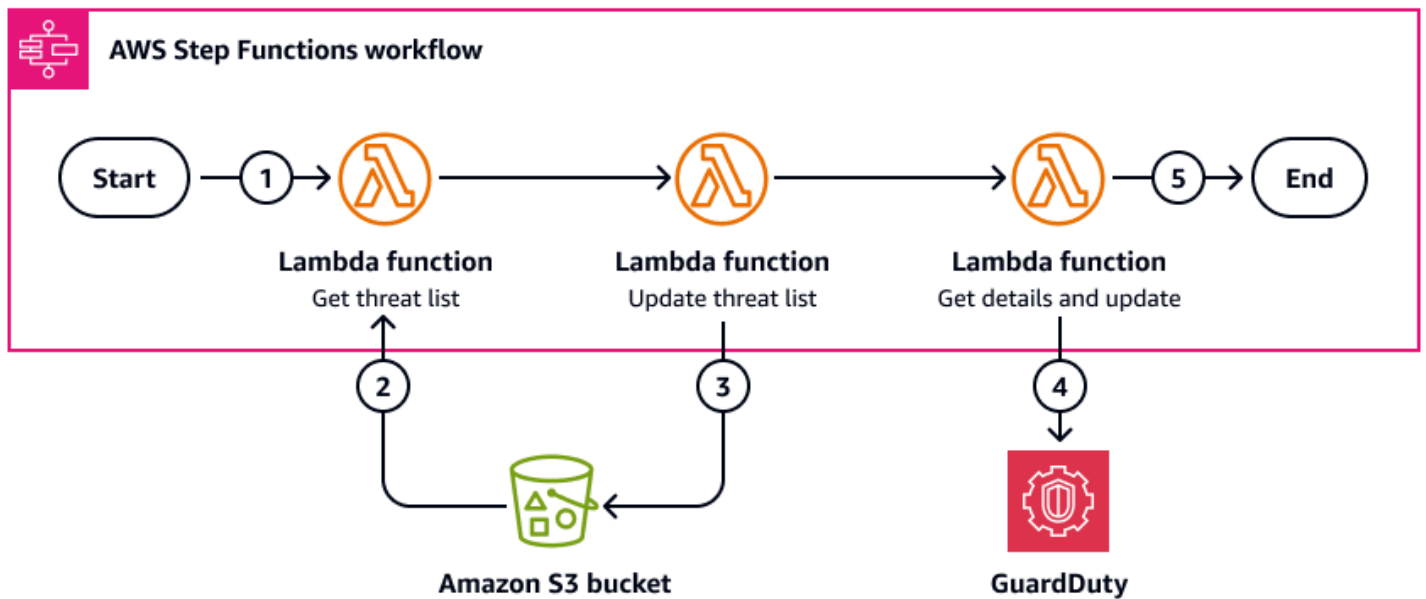
## Amazon GuardDuty

[Amazon GuardDuty](#) es un servicio de detección de amenazas que monitorea continuamente sus cargas de trabajo Cuentas de AWS y las de sus cargas de trabajo para detectar actividades no autorizadas y ofrece resultados de seguridad detallados para garantizar la visibilidad y la corrección. Al actualizar automáticamente la lista de GuardDuty amenazas de los feeds de CTI, puede obtener información sobre las amenazas que podrían estar accediendo a sus cargas de trabajo. GuardDuty mejora sus capacidades de control de detectives.

### Tip

GuardDuty se integra de forma nativa con [AWS Security Hub CSPM](#). Security Hub CSPM proporciona una visión completa del estado de su seguridad AWS y le ayuda a comprobar su entorno según los estándares y las mejores prácticas del sector de la seguridad. Cuando se integra GuardDuty con el Security Hub CSPM, GuardDuty los resultados se envían automáticamente al Security Hub CSPM. Luego, Security Hub CSPM puede incluir esos hallazgos en su análisis de su postura de seguridad. Para obtener más información, consulte [Integración con AWS Security Hub CSPM](#) en la GuardDuty documentación. En Security Hub CSPM, puede utilizar [las automatizaciones](#) para mejorar sus capacidades de detección y control de seguridad responsivo.

La siguiente imagen muestra cómo un flujo de trabajo de Step Functions puede utilizar la CTI de una fuente de amenazas para actualizar la lista de amenazas. GuardDuty Cuando una función Lambda termina de convertir el CTI al formato JSON, desencadena un EventBridge evento que inicia el flujo de trabajo.



En el diagrama se muestran los siguientes pasos:

1. Si el CTI se refiere a registros de direcciones IP, se EventBridge inicia el flujo de trabajo de Step Functions.
2. Una función Lambda recupera la lista de amenazas, que se almacena como un objeto en un bucket de Amazon Simple Storage Service (Amazon S3).
3. Una función Lambda actualiza la lista de amenazas con los cambios de dirección IP en el CTI. Guarda la lista de amenazas como una nueva versión del objeto en el bucket original de Amazon S3. El nombre del objeto no ha cambiado.
4. Una función Lambda utiliza llamadas a la API para recuperar el ID del GuardDuty detector y el ID del conjunto de información sobre amenazas. Utiliza estos ID para actualizarlos y hacer referencia GuardDuty a la nueva versión de la lista de amenazas.

#### **Note**

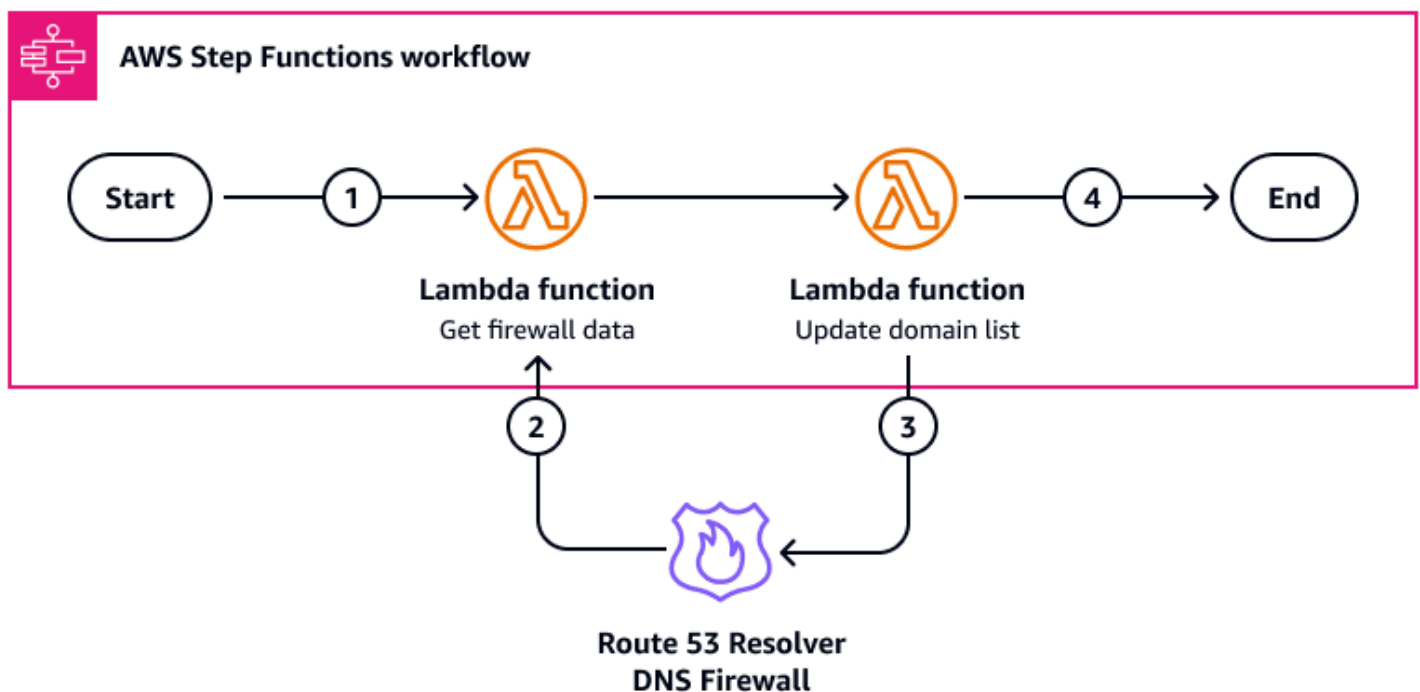
No puede recuperar un GuardDuty detector y una lista de direcciones IP específicos porque se recuperan como una matriz. Por lo tanto, le recomendamos que solo tenga uno de cada uno en el objetivo Cuenta de AWS. Si utiliza más de uno, debe asegurarse de que se extraigan los datos correctos en la función Lambda final de este flujo de trabajo.

5. Finaliza el flujo de trabajo de Step Functions.

## Amazon Route 53 Resolver Firewall de DNS

Amazon Route 53 Resolver El [firewall de DNS](#) le ayuda a filtrar y regular el tráfico DNS saliente para su nube privada virtual (VPC). En el firewall de DNS, se crea un grupo de reglas que bloquea las direcciones de dominio que identifica la fuente de CTI. Configura un flujo de trabajo de Step Functions para añadir y eliminar dominios automáticamente de este grupo de reglas.

La siguiente imagen muestra cómo un flujo de trabajo de Step Functions puede utilizar la CTI de una fuente de amenazas para actualizar la lista de dominios en Amazon Route 53 Resolver DNS Firewall. Cuando una función Lambda termina de convertir el CTI al formato JSON, desencadena un EventBridge evento que inicia el flujo de trabajo.



En el diagrama se muestran los siguientes pasos:

1. Si el CTI se refiere a registros de dominio, EventBridge inicia el flujo de trabajo de Step Functions.
2. Una función Lambda recupera los datos de la lista de dominios del firewall. Para obtener más información sobre la creación de esta función Lambda, consulte [get\\_firewall\\_domain\\_list](#) en la documentación. AWS SDK para Python (Boto3)
3. Una función Lambda utiliza el CTI y los datos recuperados para actualizar la lista de dominios. Para obtener más información sobre la creación de esta función Lambda, consulte [update\\_firewall\\_domains](#) en la documentación de Boto3. La función Lambda puede añadir, eliminar o reemplazar dominios.

#### 4. Finaliza el flujo de trabajo de Step Functions.

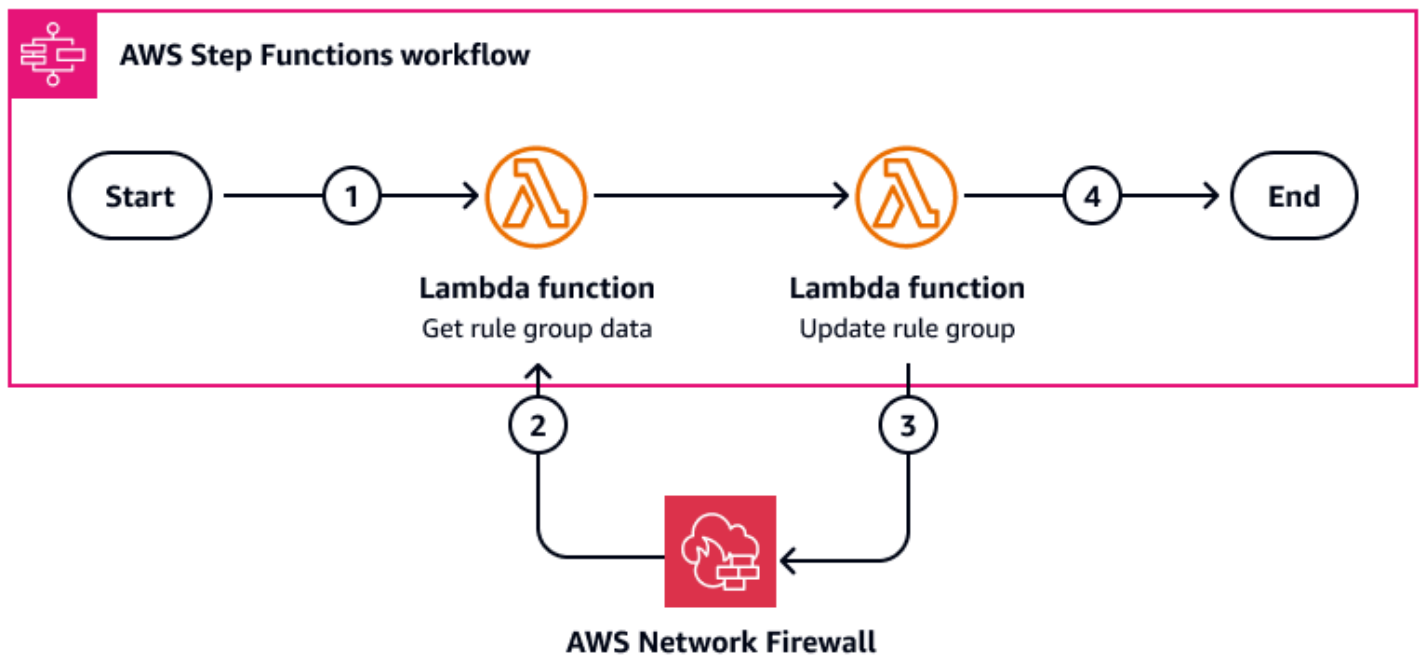
Recomendamos que siga las siguientes prácticas recomendadas:

- Le recomendamos que utilice el firewall DNS Route 53 Resolver y AWS Network Firewall. El Firewall de DNS filtra el tráfico de DNS y el Firewall de red filtra el resto del tráfico.
- Le recomendamos que habilite el registro para el Firewall de DNS. Puede crear controles de detección que supervisen los datos de registro y le avisen si un dominio restringido intenta enviar tráfico a través del firewall. Para obtener más información, consulte [Supervisión de los grupos de reglas del firewall DNS de Route 53 Resolver con Amazon CloudWatch](#).

## AWS Network Firewall

[AWS Network Firewall](#) es un servicio de detección y prevención de intrusiones y firewall de red gestionado y con estado para las VPC de la Nube de AWS. Filtra el tráfico en el perímetro de su VPC, lo que le ayuda a bloquear las amenazas. El uso de fuentes de inteligencia sobre amenazas para actualizar automáticamente los grupos de reglas de Network Firewall puede ayudar a proteger las cargas de trabajo y los datos en la nube de su organización frente a actores malintencionados.

La siguiente imagen muestra cómo un flujo de trabajo de Step Functions puede utilizar la CTI de una fuente de amenazas para actualizar uno o más grupos de reglas en Network Firewall. Cuando una función Lambda termina de convertir el CTI al formato JSON, desencadena un EventBridge evento que inicia el flujo de trabajo.



En el diagrama se muestran los siguientes pasos:

1. Si el CTI se refiere a registros de direcciones IP o dominios, EventBridge inicia un flujo de trabajo de Step Functions que actualiza automáticamente el grupo de reglas en Network Firewall.
2. Una función Lambda recupera los datos del grupo de reglas de Network Firewall.
3. Una función Lambda usa el CTI para actualizar el grupo de reglas. Agrega o elimina direcciones IP o dominios.
4. Finaliza el flujo de trabajo de Step Functions.

Recomendamos que siga las siguientes prácticas recomendadas:

- Network Firewall puede tener varios grupos de reglas. Cree grupos de reglas independientes para los dominios y las direcciones IP.
- Le recomendamos que habilite el registro para Network Firewall. Puede crear controles de detección que supervisen los datos de registro y le avisen si un dominio o una dirección IP restringidos intenta enviar tráfico a través del firewall. Para obtener más información, consulte [Registrar el tráfico de red desde AWS Network Firewall](#).
- Le recomendamos que utilice el firewall DNS Route 53 Resolver y AWS Network Firewall. El Firewall de DNS filtra el tráfico de DNS y el Firewall de red filtra el resto del tráfico.

## Ganar visibilidad con mecanismos de observabilidad

La capacidad de ver los eventos de seguridad que se han producido es tan importante como establecer los controles de seguridad adecuados. En el pilar de seguridad del AWS Well-Architected Framework, las mejores prácticas de detección incluyen [configurar el registro de servicios y aplicaciones](#) y [capturar los registros, los hallazgos y las métricas en ubicaciones estandarizadas](#). Para implementar estas prácticas recomendadas, debe registrar la información que le ayude a identificar los eventos y, a continuación, procesarla en un formato que pueda ser consumido por las personas, idealmente en una ubicación centralizada.

En esta guía se recomienda utilizar [Amazon Simple Storage Service \(Amazon S3\)](#) para centralizar los datos de registro. Amazon S3 admite el almacenamiento de registros tanto AWS Network Firewall para Amazon Route 53 Resolver DNS Firewall como para DNS. Luego, usa [AWS Security Hub CSPM](#) [Amazon Security Lake](#) para centralizar los hallazgos de Amazon y otros GuardDuty hallazgos de seguridad en una sola ubicación.

### Registrar el tráfico de la red

En la sección [Automatización de los controles de seguridad preventivos y](#) de detección de esta guía se describe el uso AWS Network Firewall de un firewall de Amazon Route 53 Resolver DNS para automatizar las respuestas a la inteligencia sobre ciberamenazas (CTI). Se recomienda configurar el registro para ambos servicios. Puede crear controles de detección que supervisen los datos de registro y le avisen si un dominio o una dirección IP restringidos intenta enviar tráfico a través del firewall.

Al configurar estos recursos, tenga en cuenta sus requisitos de registro individuales. Por ejemplo, el registro de Network Firewall solo está disponible para el tráfico que se reenvía al motor de reglas con estado. Se recomienda seguir un modelo de confianza cero y reenviar todo el tráfico al motor de reglas con estado. Sin embargo, si desea reducir los costes, puede excluir el tráfico en el que su organización confíe.

Tanto Network Firewall como DNS Firewall admiten el registro en Amazon S3. Para obtener más información sobre la configuración del registro para estos servicios, consulte [Registrar el tráfico de red procedente del](#) firewall de [DNS AWS Network Firewall y configurar el registro para dicho firewall](#). Para ambos servicios, puede configurar el registro en un bucket de Amazon S3 a través del Consola de administración de AWS.

## Centralizar los hallazgos de seguridad en AWS

[AWS Security Hub CSPM](#) proporciona una visión integral del estado de su seguridad AWS y le ayuda a evaluar su AWS entorno en función de los estándares y las mejores prácticas del sector de la seguridad. Security Hub CSPM puede generar hallazgos asociados a sus controles de seguridad. También puede recibir hallazgos de otros Servicios de AWS, como Amazon GuardDuty. Puede usar Security Hub CSPM para centralizar las conclusiones y los datos de sus productos y de Cuentas de AWS otros Servicios de AWS productos compatibles. Para obtener más información sobre las integraciones, consulte [Descripción de las integraciones en Security Hub CSPM en la documentación de Security Hub CSPM](#).

Security Hub CSPM también incluye funciones de automatización que le ayudan a clasificar y solucionar los problemas de seguridad. Por ejemplo, puede usar reglas de automatización para actualizar automáticamente resultados críticos cuando un control de seguridad falla. También puedes usar la integración con Amazon EventBridge para iniciar respuestas automáticas a hallazgos específicos. Para obtener más información, consulte [Modificación automática de los hallazgos del CSPM del Security Hub y actuar en función de ellos en la documentación del Security Hub sobre el CSPM](#).

Si utilizas Amazon GuardDuty, te recomendamos que lo configures GuardDuty para enviar sus resultados a Security Hub (CSPM). Luego, Security Hub CSPM puede incluir esos hallazgos en su análisis de su postura de seguridad. Para obtener más información, consulte [Integración con AWS Security Hub CSPM](#) en la GuardDuty documentación.

Tanto para Network Firewall como para Route 53 Resolver DNS Firewall, puede crear hallazgos personalizados a partir del tráfico de red que está registrando. [Amazon Athena](#) es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar. Puede crear consultas en Athena que escaneen los registros de Amazon S3 y extraigan los datos relevantes. Para obtener instrucciones, consulte [Primeros pasos](#) en la documentación de Athena. A continuación, puede usar una AWS Lambda función para convertir los datos de registro relevantes al [formato de búsqueda de AWS seguridad \(ASFF\)](#) y enviar el hallazgo a Security Hub CSPM. A continuación se muestra un ejemplo de función Lambda que convierte los datos de registro de Network Firewall en un hallazgo de CSPM de Security Hub:

```
Import { SecurityHubClient, BatchImportFindingsCommand, GetFindingsCommand } from
"@aws-sdk/client-securityhub";

Export const handler = async(event) => {
  const date = new Date().toISOString();
```

```
const config = {
  Region: REGION
};

const input = {
  Findings: [
    {
      SchemaVersion: '2018-10-08',
      Id: ALERTLOGS3BUCKETID,
      ProductArn: FIREWALLMANAGERARN,
      GeneratorId: 'alertlogs-to-findings',
      AwsAccountId: ACCOUNTID,
      Types: 'Unusual Behaviours/Network Flow/Alert',
      CreatedAt: date,
      UpdatedAt: date,
      Severity: {
        Normalized: 80,
        Product: 8
      },
      Confidence: 100,
      Title: 'Alert Log to Findings',
      Description: 'Network Firewall Alert Log into Finding - add
        top level dynamic detail',
      Resources: [
        {
          /*these are custom resources. Contain deeper details of your event
here*/
          firewallName: 'Example Name',
          event: 'Example details here'
        }
      ]
    }
  ]
};

const client = new SecurityHubClient(config);
const command = new BatchImportFindingsCommand(input);
const response = await client.send(command);
return { statusCode: 200, response };
};
```

El patrón que siga para extraer y enviar información a Security Hub CSPM depende de sus necesidades empresariales individuales. Si necesita que los datos se envíen de forma regular, puede utilizarlos EventBridge para iniciar el proceso. Si desea recibir una alerta cuando se añada la información, puede utilizar [Amazon Simple Notification Service \(Amazon SNS\)](#). Hay muchas maneras de abordar esta arquitectura, por lo que es importante planificar adecuadamente para satisfacer las necesidades de su empresa.

## Integración AWS datos de seguridad con otros datos empresariales

[Amazon Security Lake](#) puede automatizar la recopilación de datos de registros y eventos relacionados con la seguridad de servicios integrados Servicios de AWS y de terceros. También le ayuda a gestionar el ciclo de vida de los datos con configuraciones de retención y replicación personalizables. Security Lake convierte los datos ingeridos al formato Apache Parquet y a un esquema estándar de código abierto denominado Open Cybersecurity Schema Framework (OCSF). Gracias a la compatibilidad con OCSF, Security Lake normaliza y combina los datos de seguridad procedentes de AWS una amplia gama de fuentes de datos de seguridad empresariales. Otros Servicios de AWS y servicios de terceros pueden suscribirse a los datos almacenados en Security Lake para responder a los incidentes y analizar los datos de seguridad.

Puede configurar Security Lake para recibir las conclusiones del Security Hub CSPM. Para activar esta integración, debe habilitar ambos servicios y añadir Security Hub CSPM como fuente en Security Lake. Una vez que complete estos pasos, el CSPM de Security Hub empieza a enviar todos los resultados a Security Lake. Security Lake normaliza automáticamente las conclusiones del CSPM de Security Hub y las convierte en OCSF. En Security Lake, puede agregar uno o más suscriptores para consumir los resultados del CSPM de Security Hub. Para obtener más información, consulte [Integración con AWS Security Hub CSPM](#) en la documentación de Security Lake.

En el siguiente vídeo, [AWS Re:inForce 2024: Cyber Threat Intelligence Sharing on AWS](#), se explica cómo utilizar las integraciones de Security Hub CSPM y Security Lake para compartir CTI.

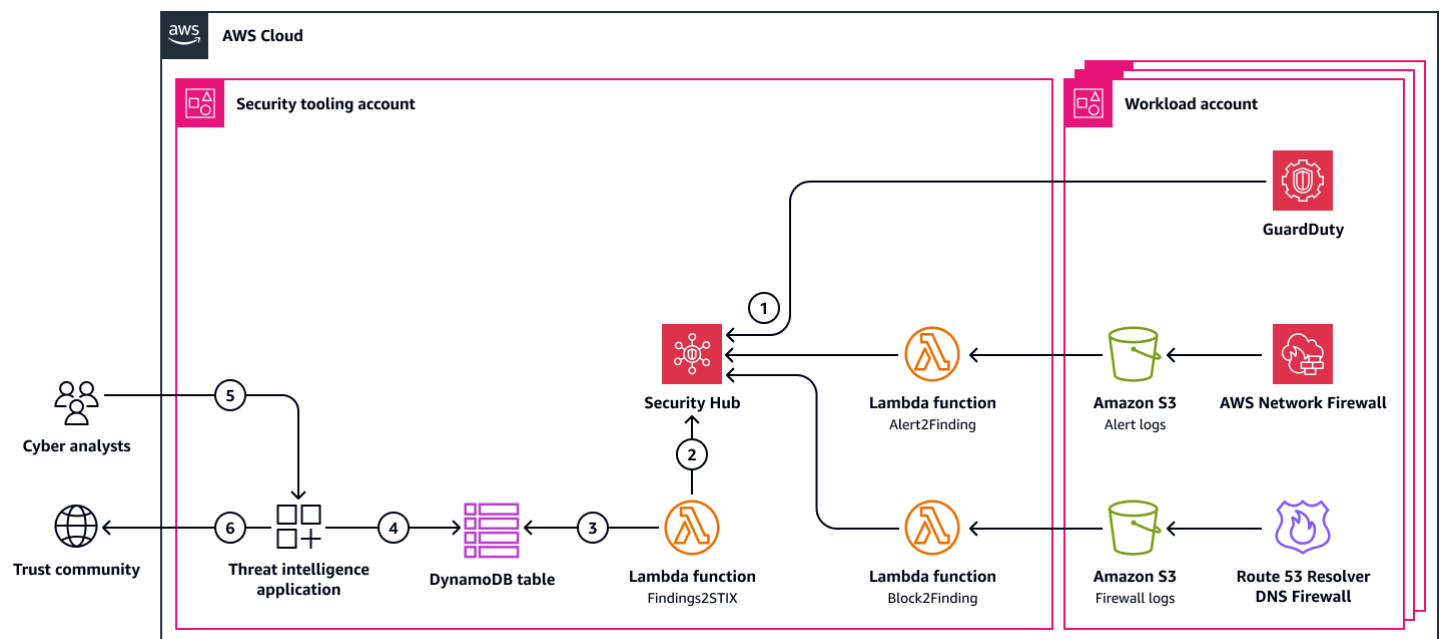
## Comparta CTI con su comunidad de confianza

La comunidad a la que envías la información sobre ciberamenazas (CTI) suele ser la misma a la que recibes la CTI. Sin embargo, puede optar por compartirla con más personas. Por ejemplo, puede optar por compartirla con organizaciones gubernamentales o reguladoras en las que confíe, como el centro nacional de ciberseguridad o los centros de análisis e intercambio de información (ISAC). El objetivo es propagar e implementar rápidamente la CTI agrupando los hallazgos de varias

organizaciones. Su plataforma de inteligencia de amenazas gestiona las integraciones de las API para compartirlas con varios canales.

El envío de la CTI a la comunidad de confianza se produce al mismo tiempo que se implementan controles preventivos y de detección. Los registros se utilizan para ayudar a identificar los eventos de seguridad. Luego, centraliza los eventos y los hallazgos para poder obtener rápidamente una visión general de su Cuentas de AWS postura de seguridad. Luego, sus equipos de seguridad, como sus analistas cibernéticos, pueden identificar cualquier información que pueda ser valiosa. Como ya tiene los resultados AWS Security Hub CSPM, puede convertirlos al formato utilizado en la fuente de amenazas, como JSON o STIX. A continuación, envía el CTI al proveedor del feed. Sus plataformas de inteligencia de amenazas ingieren, anonimizan y validan el CTI que usted proporciona. Luego, su CTI se comparte con una comunidad aún más amplia.

La siguiente imagen muestra cómo generar un CTI y luego compartirlo con tu comunidad de confianza, incluidas las autoridades cibernéticas y otros miembros de la comunidad. Servicios de AWS



Este diagrama muestra el siguiente flujo de trabajo:

1. Los hallazgos se crean en AWS Security Hub CSPM.
2. Una AWS Lambda función recupera los resultados del Security Hub CSPM y los convierte a un formato que se pueda compartir, como JSON o STIX.
3. La función Lambda almacena los resultados en una tabla de Amazon DynamoDB.

4. La plataforma de inteligencia de amenazas de terceros, que se ejecuta en Amazon Elastic Compute Cloud (Amazon EC2) o Amazon Elastic Container Service (Amazon ECS), recupera los resultados de la tabla de DynamoDB.
5. Un analista cibernético analiza el CTI de la plataforma de inteligencia de amenazas.
6. La plataforma de inteligencia de amenazas publica el CTI entre la comunidad de confianza, que está formada por otros productores y consumidores de CTI.

## Próximos pasos y recursos

Tenga en cuenta los activos, el sector y el entorno de amenazas de su organización. Estos factores deberían servir de base a las comunidades de confianza a las que decidas unirte para compartir información sobre ciberamenazas. Muchas autoridades cibernéticas de todo el mundo ofrecen fuentes de inteligencia sobre amenazas. Tenga en cuenta lo que se ofrece y elija lo que mejor se adapte al caso de uso de su organización. Utilice esta guía como un enfoque modular y adáptela en consecuencia para su organización.

Le recomendamos que consulte los siguientes recursos adicionales. Estos recursos pueden ayudarle a crear o implementar una plataforma de inteligencia sobre amenazas en su AWS entorno y ayudarle a configurar el intercambio de inteligencia sobre ciberamenazas.

## AWS recursos

- [AWS Centro de arquitectura](#)
- [AWS Re:inForce 2024: se comparte información sobre AWS ciberamenazas](#) (vídeo)
- [AWS Summit ANZ 2023: Ampliar el intercambio de inteligencia sobre ciberamenazas con el Centro de Ciberseguridad de los Estados Unidos](#) (vídeo)

## Servicio de AWS documentación

- [Documentación de Amazon DynamoDB](#)
- [EventBridge Documentación de Amazon](#)
- [GuardDuty Documentación de Amazon](#)
- [Documentación de AWS Lambda](#)
- [AWS Network Firewall documentación](#)
- [Amazon Route 53 Resolver documentación sobre DNS Firewall](#)
- [Documentación de AWS Security Hub CSPM](#)
- [Documentación de Amazon Security Lake](#)
- [Documentación del Amazon Simple Storage Service \(Amazon S3\)](#)
- [AWS Step Functions documentación](#)

## recursos STIX

- [Ejemplos de STIX 2.1](#)
- [Indicador de URL maliciosa](#)

## Plataformas de inteligencia de amenazas

- [OpenCTI](#)
- [MISP](#)

# Colaboradores

Las siguientes personas colaboraron en la elaboración de esta guía.

## Creación

- Jess Modini, tecnóloga sénior, AWS
- Alexa Donovan, arquitecta asociada de soluciones, AWS
- Steven Ryan, arquitecto de soluciones asociado, AWS
- Byron Pogson, arquitecto de soluciones de seguridad, AWS

## Revisando

- Brian Farnhill, ingeniero sénior de desarrollo de software, AWS
- Marc Luescher, arquitecto sénior de soluciones, AWS
- Stefan Mijic, especialista en garantía de seguridad, AWS
- Timothy Woodill, arquitecto de soluciones para el sector público, AWS

## Redacción técnica

- Lilly AbouHarb, redactora técnica sénior, AWS

# Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las [notificaciones RSS](#).

Cambio	Descripción	Fecha
<a href="#">Publicación inicial</a>	—	12 de diciembre de 2024

# AWS Glosario de orientación prescriptiva

Los siguientes son términos de uso común en las estrategias, guías y patrones proporcionados por la Guía AWS prescriptiva. Para sugerir entradas, utilice el enlace [Enviar comentarios](#) al final del glosario.

## Números

### Las 7 R

Siete estrategias de migración comunes para trasladar aplicaciones a la nube. Estas estrategias se basan en las 5 R que Gartner identificó en 2011 y consisten en lo siguiente:

- **Refactor/re-architect** — Mueva una aplicación y modifique su arquitectura aprovechando al máximo las funciones nativas de la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: migre su base de datos Oracle local a la PostgreSQL-Compatible edición Amazon Aurora.
- **Redefinir la plataforma (transportar y redefinir)**: traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: Migrar la base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la nube de Nube de AWS.
- **Recomprar (readquirir)**: cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: migre su sistema de gestión de relaciones con los clientes (CRM) a Salesforce.com.
- **Volver a alojar (migrar mediante lift-and-shift)**: traslade una aplicación a la nube sin hacer cambios para aprovechar las funcionalidades de la nube. Ejemplo: Migrar la base de datos de Oracle en las instalaciones a Oracle en una instancia de EC2 en la Nube de AWS.
- **Reubicar**: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma en las instalaciones a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- **Retener (revisitar)**: conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

- Retirar: retire o elimine las aplicaciones que ya no sean necesarias en un entorno de origen.

## A

### A2A () Agent-to-Agent

Un protocolo completo para la colaboración entre agentes que facilita la delegación de tareas y la transferencia de estados.

### ABAC

Consulte [control de acceso basado en atributos](#).

### servicios abstractos

Consulte [servicios administrados](#).

### ACID

Consulte [atomicidad, consistencia, aislamiento, durabilidad](#).

### migración activa-activa

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas (mediante una herramienta de replicación bidireccional o mediante operaciones de escritura doble) y ambas bases de datos gestionan las transacciones de las aplicaciones conectadas durante la migración. Este método permite la migración en lotes pequeños y controlados, en lugar de requerir una transición única. Es más flexible, pero requiere más trabajo que una [migración activa-pasiva](#).

### migración activa-pasiva

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas, pero solo la de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

### Agente

Un sistema de IA que puede razonar, planificar y tomar medidas de forma autónoma utilizando herramientas para alcanzar los objetivos.

## Agent Ops

Prácticas operativas para crear, probar, implementar y ejecutar agentes de IA en producción a escala.

## función de agregación

Función SQL que actúa en un grupo de filas y calcula un único valor de devolución para el grupo. Entre los ejemplos de funciones de agregación se incluyen SUM y MAX.

## IA

Consulte [inteligencia artificial](#).

## AIOps

Consulte [operaciones de inteligencia artificial](#)

## anonimización

El proceso de eliminar permanentemente la información personal de un conjunto de datos. La anonimización puede ayudar a proteger la privacidad personal. Los datos anonimizados ya no se consideran datos personales.

## antipatronos

Una solución que se utiliza con frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa.

## control de aplicaciones

Enfoque de seguridad que permite usar de manera exclusiva aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

## cartera de aplicaciones

Recopilación de información detallada sobre cada aplicación que utiliza una organización, incluido el costo de creación y mantenimiento de la aplicación y su valor empresarial. Esta información es clave para [el proceso de detección y análisis de la cartera](#) y ayuda a identificar y priorizar las aplicaciones que se van a migrar, modernizar y optimizar.

## inteligencia artificial (IA)

El campo de la informática que se dedica al uso de tecnologías informáticas para realizar funciones cognitivas que suelen estar asociadas a los seres humanos, como el aprendizaje, la resolución de problemas y el reconocimiento de patrones. Para más información, consulte [¿Qué es la inteligencia artificial?](#)

## operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo se utiliza AIOps en la estrategia de migración de AWS, consulte la [Guía de integración de operaciones](#).

## cifrado asimétrico

Algoritmo de cifrado que utiliza un par de claves, una clave pública para el cifrado y una clave privada para el descifrado. Puede compartir la clave pública porque no se utiliza para el descifrado, pero el acceso a la clave privada debe estar sumamente restringido.

## atomicidad, consistencia, aislamiento, durabilidad (ACID)

Conjunto de propiedades de software que garantizan la validez de los datos y la fiabilidad operativa de una base de datos, incluso en caso de errores, cortes de energía u otros problemas.

## control de acceso basado en atributos (ABAC)

La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte [ABAC AWS en la](#) documentación AWS Identity and Access Management (IAM).

## origen de datos fidedigno

Ubicación en la que se almacena la versión principal de los datos, que se considera la fuente de información más fiable. Puede copiar los datos del origen de datos autorizado a otras ubicaciones con el fin de procesarlos o modificarlos, por ejemplo, anonimizarlos, redactarlos o seudonimizarlos.

## Zona de disponibilidad

Una ubicación distinta dentro de una Región de AWS que está aislada de los fallos en otras zonas de disponibilidad y que proporciona una conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

## AWS Marco de adopción de la nube (AWS CAF)

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y

operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la [Página web de AWS CAF](#) y el [Documento técnico de AWS CAF](#).

## AWS Marco de calificación de la carga de trabajo (AWS WQF)

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQF se incluye con AWS Schema Conversion Tool (). AWS SCT Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

## B

### bot malicioso

[Bot](#) destinado a causar interrupciones o daños a personas u organizaciones.

### BCP

Consulte [planificación de la continuidad del negocio](#).

### gráfico de comportamiento

Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las llamadas sospechosas a la API y acciones similares. Para obtener más información, consulte [Datos en un gráfico de comportamiento](#) en la documentación de Detective.

### sistema big-endian

Un sistema que almacena primero el byte más significativo. Consulte también [endianidad](#).

### clasificación binaria

Un proceso que predice un resultado binario (una de las dos clases posibles). Por ejemplo, es posible que su modelo de ML necesite predecir problemas como “¿Este correo electrónico es spam o no es spam?” o “¿Este producto es un libro o un automóvil?”.

## filtro de floración

Estructura de datos probabilística y eficiente en términos de memoria que se utiliza para comprobar si un elemento es miembro de un conjunto.

## blue/green despliegue

Estrategia de implementación en la que se crean dos entornos separados, pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación se ejecuta en el otro entorno (verde). Esta estrategia lo ayuda a hacer reversiones rápidas con un impacto mínimo.

## bot

Aplicación de software que ejecuta tareas automatizadas a través de Internet y simula la actividad o interacción humana. Algunos bots son útiles o beneficiosos, como los rastreadores web que indexan la información de Internet. Otros bots, conocidos como bots maliciosos, tienen como objetivo causar interrupciones o daños a personas u organizaciones.

## botnet

Redes de [bots](#) infectadas por [malware](#) y que están bajo el control de una sola parte, conocida como pastor de bots u operador de bots. Las botnets son el mecanismo más conocido para escalar los bots y su impacto.

## branch

Área contenida de un repositorio de código. La primera rama que se crea en un repositorio es la rama principal. Puede crear una rama nueva a partir de una rama existente y, a continuación, desarrollar características o corregir errores en la rama nueva. Una rama que se genera para crear una característica se denomina comúnmente rama de característica. Cuando la característica se encuentra lista para su lanzamiento, se vuelve a combinar la rama de característica con la rama principal. Para obtener más información, consulte [Acerca de las sucursales](#) (GitHub documentación).

## acceso de emergencia

En circunstancias excepcionales y mediante un proceso aprobado, es una forma rápida de que un usuario pueda acceder a un Cuenta de AWS sitio al que normalmente no tiene permisos de acceso. Para obtener más información, consulte el indicador de [implementación de procedimientos rompe-cristales](#) en la AWS Well-Architected guía.

## estrategia de implementación sobre infraestructura existente

La infraestructura existente en su entorno. Al adoptar una estrategia de implementación sobre infraestructura existente para una arquitectura de sistemas, se diseña la arquitectura en función de las limitaciones de los sistemas y la infraestructura actuales. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de [implementación desde cero](#).

## caché de búfer

El área de memoria donde se almacenan los datos a los que se accede con más frecuencia.

## capacidad empresarial

Lo que hace una empresa para generar valor (por ejemplo, ventas, servicio al cliente o marketing). Las arquitecturas de microservicios y las decisiones de desarrollo pueden estar impulsadas por las capacidades empresariales. Para obtener más información, consulte la sección [Organizado en torno a las capacidades empresariales](#) del documento técnico [Ejecutar microservicios en contenedores en AWS](#).

## planificación de la continuidad del negocio (BCP)

Plan que aborda el posible impacto de un evento disruptivo, como una migración a gran escala en las operaciones y permite a la empresa reanudar las operaciones rápidamente.

# C

## CAF

Consulte [AWS Cloud Adoption Framework](#).

## implementación canario

Lanzamiento lento e incremental de una versión para los usuarios finales. Cuando tenga mayor confianza en la nueva versión, la implementa y reemplaza la versión actual en su totalidad.

## CCoE

Consulte [Centro de excelencia en la nube](#).

## CDC

Consulte [captura de datos de cambios](#).

## captura de datos de cambio (CDC)

Proceso de seguimiento de los cambios en un origen de datos, como una tabla de base de datos, y registro de los metadatos relacionados con el cambio. Puede utilizar los CDC para diversos fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

## ingeniería del caos

Introducción intencionada de fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puedes usar [AWS Fault Injection Service \(AWS FIS\)](#) para realizar experimentos que estresen tus AWS cargas de trabajo y evalúen su respuesta.

## CI/CD

Consulte [integración continua y entrega continua](#).

## clasificación

Un proceso de categorización que permite generar predicciones. Los modelos de ML para problemas de clasificación predicen un valor discreto. Los valores discretos siempre son distintos entre sí. Por ejemplo, es posible que un modelo necesite evaluar si hay o no un automóvil en una imagen.

## Desarrollador ciudadano

Un usuario empresarial que crea aplicaciones de IA utilizando plataformas sin code/low código sin conocimientos técnicos especializados.

## cifrado del cliente

Cifrado de datos localmente, antes de que el objetivo los Servicio de AWS reciba.

## Centro de excelencia en la nube (CCoE)

Equipo multidisciplinario que impulsa los esfuerzos de adopción de la nube en toda la organización, incluido el desarrollo de las prácticas recomendadas en la nube, la movilización de recursos, el establecimiento de plazos de migración y la dirección de la organización durante las transformaciones a gran escala. Para obtener más información, consulte las [publicaciones de CCoE](#) en el blog de estrategia Nube de AWS empresarial.

## computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar relacionada con la tecnología de [computación de periferia](#).

## modelo operativo en la nube

En una organización de TI, el modelo operativo que se utiliza para crear, madurar y optimizar uno o más entornos de nube. Para obtener más información, consulte [Creación de su modelo operativo de nube](#).

## etapas de adopción de la nube

Las siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a la Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realización de inversiones fundamentales para escalar la adopción de la nube (p. ej., crear una zona de aterrizaje, definir un CCoE, establecer un modelo de operaciones)
- Migración: migración de aplicaciones individuales
- Re-invention — Optimizar los productos y servicios e innovar en la nube

Stephen Orban definió estas etapas en la entrada del blog [The Journey Toward Cloud-First & the Stages of Adoption del](#) blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la [guía de preparación para la migración](#).

## CMDB

Consulte [base de datos de administración de configuración](#).

## repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Algunos repositorios en la nube comunes son GitHub o Bitbucket Cloud. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola CI/CD canalización puede utilizar varios repositorios.

## caché en frío

Una caché de búfer que está vacía no está bien poblada o contiene datos obsoletos o irrelevantes. Esto afecta al rendimiento, ya que la instancia de la base de datos debe leer desde la memoria principal o el disco, lo que es más lento que leer desde la memoria caché del búfer.

## datos fríos

Datos a los que se accede con poca frecuencia y que suelen ser históricos. Al consultar este tipo de datos, normalmente se aceptan consultas lentas. Trasladar estos datos a niveles o clases de almacenamiento de menor rendimiento y menos costosos puede reducir los costos.

## visión artificial (CV)

Campo de la [IA](#) que utiliza el machine learning para analizar y extraer información de formatos visuales, como imágenes y videos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

## deriva de configuración

En el caso de una carga de trabajo, un cambio en la configuración con respecto al estado esperado. Podría provocar que la carga de trabajo deje de cumplir las normas y, por lo general, es gradual e involuntaria.

## base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, los datos de una CMDB se utilizan en la etapa de detección y análisis de la cartera de productos durante la migración.

## paquete de conformidad

Un conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus controles de conformidad y seguridad. Puede implementar un paquete de conformidad como una entidad única en una región Cuenta de AWS y, o en una organización, mediante una plantilla YAML. Para obtener más información, consulta los [paquetes de conformidad](#) en la documentación. AWS Config

## integración y entrega continuas (I) CI/CD

El proceso de automatización de las etapas de origen, creación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD se describe comúnmente como una canalización. CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar más rápido. Para obtener más información, consulte [Beneficios de la entrega continua](#). CD también puede significar implementación continua. Para obtener más información, consulte [Entrega continua frente a implementación continua](#).

## CV

Consulte [visión artificial](#).

## D

### datos en reposo

Datos que están estacionarios en la red, como los datos que se encuentran almacenados.

### clasificación de datos

Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de los datos es un componente del pilar de seguridad del AWS Well-Architected Framework. Para obtener más información, consulte [Clasificación de datos](#).

### deriva de datos

Una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de machine learning, o un cambio significativo en los datos de entrada a lo largo del tiempo. La deriva de datos puede reducir la calidad, la precisión y la imparcialidad generales de las predicciones de los modelos de machine learning.

### datos en tránsito

Datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red.

### mallado de datos

Marco de arquitectura que proporciona una propiedad de datos distribuida y descentralizada con una administración y una gobernanza centralizadas.

### minimización de datos

El principio de recopilar y procesar solo los datos estrictamente necesarios. Practicar la minimización de los datos Nube de AWS puede reducir los riesgos de privacidad, los costos y la huella de carbono de la analítica.

### perímetro de datos

Un conjunto de barreras preventivas en su AWS entorno que ayudan a garantizar que solo las identidades confiables accedan a los recursos confiables desde las redes esperadas. Para obtener más información, consulte [Crear un perímetro de datos sobre](#) AWS

## preprocesamiento de datos

Transformar los datos sin procesar en un formato que su modelo de ML pueda analizar fácilmente. El preprocesamiento de datos puede implicar eliminar determinadas columnas o filas y corregir los valores faltantes, incoherentes o duplicados.

## procedencia de los datos

El proceso de rastrear el origen y el historial de los datos a lo largo de su ciclo de vida, por ejemplo, la forma en que se generaron, transmitieron y almacenaron los datos.

## titular de los datos

Persona cuyos datos se recopilan y procesan.

## almacenamiento de datos

Sistema de administración de datos que respalda la inteligencia empresarial, como los análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para las consultas y los análisis.

## lenguaje de definición de datos (DDL)

Instrucciones o comandos para crear o modificar la estructura de tablas y objetos de una base de datos.

## lenguaje de manipulación de datos (DML)

Instrucciones o comandos para modificar (insertar, actualizar y eliminar) la información de una base de datos.

## DDL

Consulte [lenguaje de definición de bases de datos](#).

## conjunto profundo

Combinar varios modelos de aprendizaje profundo para la predicción. Puede utilizar conjuntos profundos para obtener una predicción más precisa o para estimar la incertidumbre de las predicciones.

## aprendizaje profundo

Un subcampo del ML que utiliza múltiples capas de redes neuronales artificiales para identificar el mapeo entre los datos de entrada y las variables objetivo de interés.

## defensa en profundidad

Un enfoque de seguridad de la información en el que se distribuyen cuidadosamente una serie de mecanismos y controles de seguridad en una red informática para proteger la confidencialidad, la integridad y la disponibilidad de la red y de los datos que contiene. Al adoptar esta estrategia AWS, se añaden varios controles en diferentes capas de la AWS Organizations estructura para ayudar a proteger los recursos. Por ejemplo, un enfoque de defensa en profundidad podría combinar la autenticación multifactor, la segmentación de la red y el cifrado.

## administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de ese servicio. Esta cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte [Servicios que funcionan con AWS Organizations](#) en la documentación de AWS Organizations .

## Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

## entorno de desarrollo

Consulte [entorno](#).

## control de detección

Un control de seguridad que se ha diseñado para detectar, registrar y alertar después de que se produzca un evento. Estos controles son una segunda línea de defensa, ya que lo advierten sobre los eventos de seguridad que han eludido los controles preventivos establecidos. Para obtener más información, consulte [Controles de detección](#) en Implementación de controles de seguridad en AWS.

## asignación de flujos de valor para el desarrollo (DVSM)

Proceso que se utiliza para identificar y priorizar las restricciones que afectan negativamente a la velocidad y la calidad en el ciclo de vida del desarrollo de software. DVSM amplía el proceso de asignación del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

## gemelo digital

Representación virtual de un sistema del mundo real, como un edificio, una fábrica, un equipo industrial o una línea de producción. Los gemelos digitales son compatibles con el mantenimiento predictivo, la supervisión remota y la optimización de la producción.

## tabla de dimensiones

En un [esquema en estrella](#), tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos en una tabla de hechos. Los atributos de la tabla de dimensiones suelen ser campos de texto o números discretos que se comportan como texto. Estos atributos se suelen utilizar para restringir consultas, filtrarlas y etiquetar los conjuntos de resultados.

## desastre

Un evento que impide que una carga de trabajo o un sistema cumplan sus objetivos empresariales en su ubicación principal de implementación. Estos eventos pueden ser desastres naturales, fallos técnicos o el resultado de acciones humanas, como una configuración incorrecta involuntaria o un ataque de malware.

## recuperación de desastres (DR)

Estrategia y proceso que utiliza para minimizar el tiempo de inactividad y la pérdida de datos a causa de un [desastre](#). Para obtener más información, consulte [Recuperación de cargas de trabajo ante desastres en AWS: Recuperación en la nube](#) en el AWS Well-Architected marco.

## DML

Consulte [lenguaje de manipulación de bases de datos](#).

## diseño basado en el dominio

Un enfoque para desarrollar un sistema de software complejo mediante la conexión de sus componentes a dominios en evolución, o a los objetivos empresariales principales, a los que sirve cada componente. Eric Evans introdujo este concepto en su libro *Domain-Driven Design: Tackling Complexity in the Heart of Software* (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte [Modernización gradual de los servicios web antiguos de ASP.NET Microsoft \(ASMX\) mediante contenedores y Amazon API Gateway](#).

## DR

Consulte [recuperación ante desastres](#).

## Detección de desviaciones

Seguimiento de las desviaciones con respecto a una configuración con línea de base. Por ejemplo, puedes usarlo AWS CloudFormation para [detectar desviaciones en los recursos del sistema](#) o puedes usarlo AWS Control Tower para [detectar cambios en tu landing zone](#) que puedan afectar al cumplimiento de los requisitos de gobierno.

## DVSM

Consulte [asignación de flujos de valor para el desarrollo](#).

## E

### EDA

Consulte [análisis de datos de tipo exploratorio](#).

### EDI

Consulte [intercambio electrónico de datos](#).

### computación en la periferia

La tecnología que aumenta la potencia de cálculo de los dispositivos inteligentes en la periferia de una red de IoT. En comparación con la [computación en la nube](#), la computación de periferia puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

### intercambio electrónico de datos (EDI)

Intercambio automatizado de documentos comerciales entre organizaciones. Para más información, consulte [¿Qué es el intercambio electrónico de datos?](#)

### cifrado

Proceso de computación que transforma datos de texto plano, que son legibles por humanos, en texto cifrado.

### clave de cifrado

Cadena criptográfica de bits aleatorios que se genera mediante un algoritmo de cifrado. Las claves pueden variar en longitud y cada una se ha diseñado para ser impredecible y única.

## endianidad

El orden en el que se almacenan los bytes en la memoria del ordenador. Big-endian los sistemas almacenan primero el byte más significativo. Little-endian los sistemas almacenan primero el byte menos significativo.

## punto de conexión

Consulte [punto de conexión de servicio](#).

## servicio de punto de conexión

Servicio que puede alojar en una nube privada virtual (VPC) para compartir con otros usuarios. Puede crear un servicio de punto final con AWS PrivateLink entidades principales Cuentas de AWS o AWS Identity and Access Management (de IAM) y conceder permisos a ellas. Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte [Creación de un servicio de punto de conexión](#) en la documentación de Amazon Virtual Private Cloud (Amazon VPC).

## planificación de recursos empresariales (ERP)

Sistema que automatiza y administra los procesos empresariales clave (como la contabilidad, [MES](#) y la administración de proyectos) de una empresa.

## cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte el [cifrado de sobres](#) en la documentación de AWS Key Management Service (AWS KMS).

## entorno

Una instancia de una aplicación en ejecución. Los siguientes son los tipos de entornos más comunes en la computación en la nube:

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.

- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En un CI/CD proceso, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

## epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las epopeyas AWS de seguridad de CAF incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la [Guía de implementación del programa](#).

## ERP

Consulte [planificación de recursos empresariales](#).

## análisis de datos de tipo exploratorio (EDA)

El proceso de analizar un conjunto de datos para comprender sus características principales. Se recopilan o agregan datos y, a continuación, se realizan las investigaciones iniciales para encontrar patrones, detectar anomalías y comprobar las suposiciones. El EDA se realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

## F

### tabla de hechos

Tabla central de un [esquema en estrella](#). Almacena datos cuantitativos sobre operaciones empresariales. Por lo general, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

### Fail Fast

Filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de los enfoques ágiles.

## límite de aislamiento de errores

En el Nube de AWS, un límite, como una zona de disponibilidad Región de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para más información, consulte [AWS Fault Isolation Boundaries](#).

## rama de característica

Consulte [rama](#).

## características

Los datos de entrada que se utilizan para hacer una predicción. Por ejemplo, en un contexto de fabricación, las características pueden ser imágenes que se capturan periódicamente desde la línea de fabricación.

## importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, esto se expresa como una puntuación numérica que se puede calcular mediante diversas técnicas, como las explicaciones aditivas de Shapley (SHAP) y los gradientes integrados. Para obtener más información, consulte [Interpretabilidad del modelo de aprendizaje automático](#) con AWS

## transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

## peticiones con pocos pasos

Proporcionar a un [LLM](#) una pequeña cantidad de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que lleve a cabo una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, en el que los modelos aprenden a partir de ejemplos (tomas) integrados en las instrucciones. Few-shot Las indicaciones pueden ser eficaces para tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también [peticiones desde cero](#).

## FGAC

Consulte [control de acceso detallado](#).

## control de acceso preciso (FGAC)

El uso de varias condiciones que tienen por objetivo permitir o denegar una solicitud de acceso.  
migración relámpago

Método de migración de bases de datos que utiliza la replicación continua de datos mediante la [captura de datos de cambio](#) para migrar los datos en el menor tiempo posible, en lugar de utilizar un enfoque gradual. El objetivo es reducir al mínimo el tiempo de inactividad.

## FM

Consulte [modelo fundacional](#).

## Modelo fundacional (FM)

Gran red neuronal de aprendizaje profundo que se entrenó con conjuntos de datos masivos de datos generalizados y no etiquetados. Los FM pueden hacer una amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para más información, consulte [¿Qué son los modelos fundacionales?](#)

## Puerta de enlace FM

Un intermediario centralizado que controla y normaliza el acceso a los modelos básicos. También se conoce como puerta de enlace LLM.

# G

## IA generativa

Subconjunto de modelos de [IA](#) que se entrenaron con grandes cantidades de datos y que pueden utilizar una simple petición de texto para crear contenido y artefactos nuevos, como imágenes, videos, texto y audio. Para más información, consulte [¿Qué es la IA generativa?](#)

## bloqueo geográfico

Consulte [restricciones geográficas](#).

## restricciones geográficas (bloqueo geográfico)

En Amazon CloudFront, una opción para impedir que los usuarios de países específicos accedan a las distribuciones de contenido. Puede utilizar una lista de permitidos o bloqueados para especificar los países aprobados y prohibidos. Para obtener más información, consulta [Restringir la distribución geográfica del contenido](#) en la CloudFront documentación.

## Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, mientras que el [flujo de trabajo basado en enlaces troncales](#) es el enfoque moderno preferido.

## imagen dorada

Instantánea de un sistema o software que se usa como plantilla para implementar nuevas instancias de ese sistema o software. Por ejemplo, en la fabricación, una imagen dorada se puede utilizar para aprovisionar software en varios dispositivos y ayuda a mejorar la velocidad, la escalabilidad y la productividad de las operaciones de fabricación de dispositivos.

## estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como [implementación sobre infraestructura existente](#). Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

## barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y la conformidad en todas las unidades organizativas (OU). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de permisos de IAM. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

## barandas (AI)

Mecanismos de seguridad que filtran, validan y restringen las entradas y salidas de los [agentes](#) para ayudar a garantizar un comportamiento responsable y seguro de la IA.

# H

## HA

Consulte [alta disponibilidad](#).

## migración heterogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que utilice un motor de base de datos diferente (por ejemplo, de Oracle a Amazon Aurora). La migración heterogénea suele ser parte de un esfuerzo de rediseño de la arquitectura y convertir el esquema puede ser una tarea compleja. [AWS ofrece AWS SCT](#), lo cual ayuda con las conversiones de esquemas.

## alta disponibilidad (HA)

La capacidad de una carga de trabajo para funcionar de forma continua, sin intervención, en caso de desafíos o desastres. Los sistemas de alta disponibilidad están diseñados para realizar una conmutación por error automática, ofrecer un rendimiento de alta calidad de forma constante y gestionar diferentes cargas y fallos con un impacto mínimo en el rendimiento.

## modernización histórica

Un enfoque utilizado para modernizar y actualizar los sistemas de tecnología operativa (TO) a fin de satisfacer mejor las necesidades de la industria manufacturera. Un histórico es un tipo de base de datos que se utiliza para recopilar y almacenar datos de diversas fuentes en una fábrica.

## datos de reserva

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de [machine learning](#). Puede utilizar los datos de reserva para evaluar el rendimiento del modelo mediante la comparación de las predicciones del modelo con los datos de reserva.

## human-in-the-loop (HiTL)

Un patrón de flujo de trabajo en el que la ejecución de los [agentes](#) se detiene para su revisión y aprobación por parte de una persona en los puntos de decisión críticos.

## migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS para SQL Server). La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

## datos recientes

Datos a los que se accede con frecuencia, como datos en tiempo real o datos traslacionales recientes. Por lo general, estos datos requieren un nivel o una clase de almacenamiento de alto rendimiento para proporcionar respuestas rápidas a las consultas.

## hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, una revisión suele realizarse fuera del flujo de trabajo habitual de las DevOps versiones.

## periodo de hiperatención

Periodo, inmediatamente después de la transición, durante el cual un equipo de migración administra y monitorea las aplicaciones migradas en la nube para solucionar cualquier problema. Por lo general, este periodo dura de 1 a 4 días. Al final del periodo de hiperatención, el equipo de migración suele transferir la responsabilidad de las aplicaciones al equipo de operaciones en la nube.

## I

## laC

Consulte [infraestructura como código](#).

## políticas basadas en identidades

Política asociada a uno o más directores de IAM que define sus permisos en el entorno. Nube de AWS

## aplicación inactiva

Aplicación que utiliza un promedio de CPU y memoria de entre 5 y 20 por ciento durante un periodo de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

## IIoT

Consulte [Internet de las cosas industrial](#).

## infraestructura inmutable

Modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar o modificar la infraestructura existente o aplicarle revisiones. Las infraestructuras inmutables son de manera intrínseca más coherentes, fiables y predecibles que las [infraestructuras mutables](#). Para obtener más información, consulte las mejores prácticas del [Framework para implementar con una infraestructura inmutable](#). AWS Well-Architected

## VPC entrante (de entrada)

En una arquitectura de AWS cuentas múltiples, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La [Arquitectura de referencia de seguridad de AWS](#) recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

## migración gradual

Estrategia de transición en la que se migra la aplicación en partes pequeñas en lugar de realizar una transición única y completa. Por ejemplo, puede trasladar inicialmente solo unos pocos microservicios o usuarios al nuevo sistema. Tras comprobar que todo funciona correctamente, puede trasladar microservicios o usuarios adicionales de forma gradual hasta que pueda retirar su sistema heredado. Esta estrategia reduce los riesgos asociados a las grandes migraciones.

## Industria 4.0

Un término que [Klaus Schwab](#) introdujo en 2016 para referirse a la modernización de los procesos de fabricación mediante avances en la conectividad, los datos en tiempo real, la automatización, el análisis y. AI/ML

## infraestructura

Todos los recursos y activos que se encuentran en el entorno de una aplicación.

## infraestructura como código (IaC)

Proceso de aprovisionamiento y administración de la infraestructura de una aplicación mediante un conjunto de archivos de configuración. La IaC se ha diseñado para ayudarlo a centralizar la administración de la infraestructura, estandarizar los recursos y escalar con rapidez a fin de que los entornos nuevos sean repetibles, fiables y consistentes.

## Internet de las cosas industrial (IIoT)

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte [Creación de una estrategia de transformación digital del Internet de las cosas industrial \(IIoT\)](#).

## VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red entre las VPC (iguales o Regiones de AWS diferentes), Internet y las redes locales. La [Arquitectura de referencia de seguridad de AWS](#) recomienda configurar su

cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

## Internet de las cosas (IoT)

Red de objetos físicos conectados con sensores o procesadores integrados que se comunican con otros dispositivos y sistemas a través de Internet o de una red de comunicación local. Para obtener más información, consulte [¿Qué es IoT?](#).

## interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para obtener más información, consulte Interpretabilidad del modelo [de aprendizaje automático](#) con AWS

## IoT

Consulte [Internet de las cosas](#).

## biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. La ITIL proporciona la base para la ITSM.

## administración de servicios de TI (ITSM)

Actividades asociadas con el diseño, la implementación, la administración y el soporte de los servicios de TI para una organización. Para obtener información sobre la integración de las operaciones en la nube con las herramientas de ITSM, consulte la [Guía de integración de operaciones](#).

## ITIL

Consulte [biblioteca de información de TI](#).

## ITSM

Consulte [administración de servicios de TI](#).

## L

## control de acceso basado en etiquetas (LBAC)

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección

entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

#### zona de aterrizaje

Una landing zone es un AWS entorno multicuenta bien diseñado, escalable y seguro. Este es un punto de partida desde el cual las empresas pueden lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura. Para obtener más información sobre las zonas de aterrizaje, consulte [Configuración de un entorno de AWS seguro y escalable con varias cuentas](#).

#### modelo de lenguaje de gran tamaño (LLM)

Modelo de [IA](#) de aprendizaje profundo que se entrenó previamente con una gran cantidad de datos. Un LLM puede llevar a cabo varias tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para más información, consulte [¿Qué es un LLM \(modelo de lenguaje de gran tamaño\)?](#)

#### migración grande

Migración de 300 servidores o más.

#### LBAC

Consulte [control de acceso basado en etiquetas](#).

#### privilegio mínimo

La práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte [Aplicar permisos de privilegio mínimo](#) en la documentación de IAM.

#### migrar mediante lift-and-shift

Consulte [Las 7 R](#).

#### sistema little-endian

Un sistema que almacena primero el byte menos significativo. Consulte también [endianidad](#).

#### LLM

Consulte [modelo de lenguaje de gran tamaño](#).

#### entornos inferiores

Consulte [entorno](#).

# M

## machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte [Machine learning](#).

## rama principal

Consulte [rama](#).

## malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware podría interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los registradores de pulsaciones de teclas.

## Servicios administrados

Servicios de AWS en el que AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y se accede a los puntos finales para almacenar y recuperar datos. Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB son ejemplos de servicios administrados. También se conocen como servicios abstractos.

## sistema de ejecución de fabricación (MES)

Sistema de software para seguir, supervisar, documentar y controlar los procesos de producción que convierten las materias primas en productos acabados en la zona de producción.

## MAP

Consulte [Programa de aceleración de la migración](#).

## MCP

Consulte [Model Context Protocol](#).

## Protocolo de contexto para modelos (MCP)

Un protocolo sin estado para la comunicación entre el [agente](#) y la [herramienta](#).

## Servidor MCP

Un servicio que expone una o más [herramientas](#) a través del protocolo [Model Context](#).

## mecanismo

Proceso completo mediante el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para hacer ajustes. Un mecanismo es un ciclo que se refuerza y mejora por sí mismo a medida que funciona. Para obtener más información, consulte [Creación de mecanismos](#) en el AWS Well-Architected marco.

## cuenta de miembro

Todas las Cuentas de AWS demás cuentas, excepto la de administración, que forman parte de una organización AWS Organizations. Una cuenta no puede pertenecer a más de una organización a la vez.

## MES

Consulte [sistema de ejecución de fabricación](#).

## Message Queuing Telemetry Transport (MQTT)

[Un protocolo de comunicación ligero de máquina a máquina \(M2M\), basado en el publish/subscribe patrón, para dispositivos de IoT con recursos limitados.](#)

## microservicio

Un servicio pequeño e independiente que se comunica a través de API bien definidas y que, por lo general, es propiedad de equipos pequeños e independientes. Por ejemplo, un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte [Integrar](#) microservicios mediante servicios sin servidor. AWS

## arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de una interfaz bien definida mediante API ligeras. Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte [Implementación de microservicios](#) en. AWS

## Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a

compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

### migración a escala

Proceso de transferencia de la mayoría de la cartera de aplicaciones a la nube en oleadas, con más aplicaciones desplazadas a un ritmo más rápido en cada oleada. En esta fase, se utilizan las prácticas recomendadas y las lecciones aprendidas en las fases anteriores para implementar una fábrica de migración de equipos, herramientas y procesos con el fin de agilizar la migración de las cargas de trabajo mediante la automatización y la entrega ágil. Esta es la tercera fase de la [estrategia de migración de AWS](#).

### fábrica de migración

Cross-functional equipos que agilizan la migración de las cargas de trabajo mediante enfoques ágiles y automatizados. Los equipos de las fábricas de migración suelen estar compuestos por analistas y propietarios de operaciones, ingenieros de migración, desarrolladores y DevOps profesionales que trabajan a pasos agigantados. Entre el 20 y el 50 por ciento de la cartera de aplicaciones empresariales se compone de patrones repetidos que pueden optimizarse mediante un enfoque de fábrica. Para obtener más información, consulte la [discusión sobre las fábricas de migración](#) y la [Guía de fábricas de migración a la nube](#) en este contenido.

### metadatos de migración

Información sobre la aplicación y el servidor que se necesita para completar la migración. Cada patrón de migración requiere un conjunto diferente de metadatos de migración. Algunos ejemplos de metadatos de migración son la subred de destino, el grupo de seguridad y AWS la cuenta.

### patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: rehospede la migración a Amazon EC2 AWS con Application Migration Service.

### Migration Portfolio Assessment (MPA)

Herramienta en línea que proporciona información a fin de validar los argumentos comerciales necesarios para migrar a la Nube de AWS. La MPA ofrece una evaluación detallada de la cartera (adecuación del tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y

planificación de oleadas). La [herramienta MPA](#) (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores de los socios de APN.

### Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar sus puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas mediante el AWS CAF. Para obtener más información, consulte la [Guía de preparación para la migración](#). La MRA es la primera fase de la [estrategia de migración de AWS](#).

### estrategia de migración

Enfoque utilizado para migrar una carga de trabajo a la Nube de AWS. Para más información, consulte la entrada [Las 7 R](#) de este glosario y también [Mobilize your organization to accelerate large-scale migrations](#).

### ML

Consulte [machine learning](#).

### modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia y aprovechar las innovaciones. Para más información, consulte [Strategy for modernizing applications in the Nube de AWS](#).

### evaluación de la preparación para la modernización

Evaluación que ayuda a determinar la preparación para la modernización de las aplicaciones de una organización; identifica los beneficios, los riesgos y las dependencias; y determina qué tan bien la organización puede soportar el estado futuro de esas aplicaciones. El resultado de la evaluación es un esquema de la arquitectura objetivo, una hoja de ruta que detalla las fases de desarrollo y los hitos del proceso de modernización y un plan de acción para abordar las brechas identificadas. Para más información, consulte [Evaluating modernization readiness for applications in the Nube de AWS](#).

### aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar

una arquitectura de microservicios. Para obtener más información, consulte [Descomposición de monolitos en microservicios](#).

## MPA

Consulte [Migration Portfolio Assessment](#).

## MQTT

Consulte [Message Queuing Telemetry Transport](#).

## clasificación multiclase

Un proceso que ayuda a generar predicciones para varias clases (predice uno de más de dos resultados). Por ejemplo, un modelo de ML podría preguntar “¿Este producto es un libro, un automóvil o un teléfono?” o “¿Qué categoría de productos es más interesante para este cliente?”.

## infraestructura mutable

Modelo que actualiza y modifica la infraestructura actual para las cargas de trabajo de producción. Para mejorar la coherencia, la confiabilidad y la previsibilidad, el AWS Well-Architected Marco recomienda el uso de una [infraestructura inmutable](#) como práctica recomendada.

## O

### OAC

Consulte [control de acceso de origen](#).

### OAI

Consulte [identidad de acceso de origen](#).

### OCM

Consulte [administración del cambio organizacional](#).

## migración fuera de línea

Método de migración en el que la carga de trabajo de origen se elimina durante el proceso de migración. Este método implica un tiempo de inactividad prolongado y, por lo general, se utiliza para cargas de trabajo pequeñas y no críticas.

## OI

Consulte [integración de operaciones](#).

## OLA

Consulte [acuerdo de nivel operativo](#).

### migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

## OPC-UA

Consulte [Open Process Communications: arquitectura unificada](#).

### Comunicaciones de proceso abierto: arquitectura unificada () OPC-UA

Un protocolo de comunicación de máquina a máquina (M2M) para la automatización industrial. OPC-UA proporciona un estándar de interoperabilidad con esquemas de cifrado, autenticación y autorización de datos.

### acuerdo de nivel operativo (OLA)

Acuerdo que aclara lo que los grupos de TI operativos se comprometen a ofrecerse entre sí, para respaldar un acuerdo de nivel de servicio (SLA).

### revisión de la preparación operativa (ORR)

Lista de comprobación de preguntas y prácticas recomendadas asociadas que son útiles para comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles errores. Para obtener más información, consulte [las revisiones de preparación operativa \(ORR\)](#) en el AWS Well-Architected marco.

### tecnología operativa (TO)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En el sector de la fabricación, la integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la [industria 4.0](#).

### integración de operaciones (OI)

Proceso de modernización de las operaciones en la nube, que implica la planificación de la preparación, la automatización y la integración. Para obtener más información, consulte la [Guía de integración de las operaciones](#).

## registro de seguimiento organizativo

Un registro creado por y AWS CloudTrail que registra todos los eventos Cuentas de AWS de una organización AWS Organizations. Este registro de seguimiento se crea en cada Cuenta de AWS que forma parte de la organización y realiza un seguimiento de la actividad en cada cuenta. Para obtener más información, consulte [Crear un registro para una organización](#) en la CloudTrail documentación.

## administración del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. La OCM ayuda a las empresas a prepararse para nuevos sistemas y estrategias y a realizar la transición a ellos, al acelerar la adopción de cambios, abordar los problemas de transición e impulsar cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de personal, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la [Guía de OCM](#).

## control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). El OAC admite todos los buckets de S3 Regiones de AWS, el cifrado del lado del servidor con AWS KMS (SSE-KMS) y DELETE las solicitudes PUT y dinámicas al bucket de S3.

## identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando utiliza OAI, CloudFront crea un principal con el que Amazon S3 puede autenticarse. Los directores autenticados solo pueden acceder al contenido de un bucket de S3 a través de una distribución específica. CloudFront Consulte también el [OAC](#), que proporciona un control de acceso más detallado y mejorado.

## ORR

Consulte [revisión de la preparación operativa](#).

## OT

Consulte [tecnología operativa](#).

## VPC saliente (de salida)

En una arquitectura de AWS cuentas múltiples, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La [Arquitectura de referencia de seguridad de AWS](#) recomienda

configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

## P

### límite de permisos

Una política de administración de IAM que se adjunta a las entidades principales de IAM para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte [Límites de permisos](#) en la documentación de IAM.

### información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos de información de identificación personal son los nombres, las direcciones y la información de contacto.

### PII

Consulte [información de identificación personal](#).

### manual de estrategias

Conjunto de pasos predefinidos que capturan el trabajo asociado a las migraciones, como la entrega de las funciones de operaciones principales en la nube. Un manual puede adoptar la forma de scripts, manuales de procedimientos automatizados o resúmenes de los procesos o pasos necesarios para operar un entorno modernizado.

### PLC

Consulte [controlador lógico programable](#).

### PLM

Consulte [administración del ciclo de vida del producto](#).

### policy

Objeto que puede definir permisos (consulte [política basada en identidad](#)), especificar las condiciones de acceso (consulte [política basada en recursos](#)) o definir los permisos máximos para todas las cuentas de una organización de AWS Organizations (consulte [política de control de servicio](#)).

## persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades.

## evaluación de cartera

Proceso de detección, análisis y priorización de la cartera de aplicaciones para planificar la migración. Para obtener más información, consulte la [Evaluación de la preparación para la migración](#).

## predicate

Condición de consulta que devuelve `true` o `false`. En general, se encuentra en una cláusula `WHERE`.

## inserción de predicados

Técnica de optimización de consultas en bases de datos que filtra los datos de la consulta antes de transferirlos. Esta técnica reduce la cantidad de datos de la base de datos relacional que se tienen que recuperar y procesar. Además, mejora el rendimiento de las consultas.

## control preventivo

Un control de seguridad diseñado para evitar que ocurra un evento. Estos controles son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Para obtener más información, consulte [Controles preventivos](#) en Implementación de controles de seguridad en AWS.

## entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz para un Cuenta de AWS rol de IAM o un usuario. Para obtener más información, consulte Entidad principal en [Términos y conceptos de roles](#) en la documentación de IAM.

## Privacidad desde el diseño

Enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de desarrollo.

## zonas alojadas privadas

Contenedor que aloja información acerca de cómo desea que responda Amazon Route 53 a las consultas de DNS de un dominio y sus subdominios en una o varias VPC. Para obtener más información, consulte [Uso de zonas alojadas privadas](#) en la documentación de Route 53.

## control proactivo

[Control de seguridad](#) que se diseñó para evitar la implementación de recursos que no cumplan con la normativa. Estos controles analizan los recursos antes de aprovisionarlos. Si el recurso no cumple con los requisitos del control, no se aprovisiona. Para obtener más información, consulte la [guía de referencia de controles](#) en la AWS Control Tower documentación y consulte [Controles proactivos](#) en Implementación de controles de seguridad en AWS.

## administración del ciclo de vida del producto (PLM)

Administración de los datos y los procesos de un producto a lo largo de todo su ciclo de vida, desde el diseño, el desarrollo y el lanzamiento, pasando por el crecimiento y la madurez, hasta la reducción de su uso y su retirada.

## entorno de producción

Consulte [entorno](#).

## controlador lógico programable (PLC)

En el sector de la fabricación, computadora adaptable y altamente fiable que supervisa las máquinas y automatiza los procesos de fabricación.

## encadenamiento de peticiones

Uso de la salida de una petición de [LLM](#) como entrada para la siguiente petición a fin de generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en tareas secundarias o para refinar o ampliar de forma iterativa una respuesta preliminar. Ayuda a mejorar la precisión y la relevancia de las respuestas de un modelo y permite obtener resultados más detallados y personalizados.

## seudonimización

El proceso de reemplazar los identificadores personales de un conjunto de datos por valores de marcadores de posición. La seudonimización puede ayudar a proteger la privacidad personal. Los datos seudonimizados siguen considerándose datos personales.

## publish/subscribe (pub/sub)

Patrón que permite establecer comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un [MES](#) basado en microservicios, un microservicio puede publicar mensajes de eventos en un canal al que se pueden suscribir otros microservicios. El sistema puede agregar nuevos microservicios sin cambiar el servicio de publicación.

## Q

### plan de consulta

Serie de pasos, como instrucciones, que se utilizan para acceder a los datos de un sistema de base de datos relacional SQL.

### regresión del plan de consulta

El optimizador de servicios de la base de datos elige un plan menos óptimo que antes de un cambio determinado en el entorno de la base de datos. Los cambios en estadísticas, restricciones, configuración del entorno, enlaces de parámetros de consultas y actualizaciones del motor de base de datos PostgreSQL pueden provocar una regresión del plan.

## R

### Matriz RACI

Consulte [responsable, fiable, consultada e informada \(RACI\)](#).

### RAG

Consulte [generación aumentada por recuperación](#).

### ransomware

Software malicioso que se ha diseñado para bloquear el acceso a un sistema informático o a los datos hasta que se efectúe un pago.

### Matriz RASCI

Consulte [responsable, fiable, consultada e informada \(RACI\)](#).

## RCAC

Consulte [control de acceso por filas y columnas](#).

### réplica de lectura

Una copia de una base de datos que se utiliza con fines de solo lectura. Puede enrutar las consultas a la réplica de lectura para reducir la carga en la base de datos principal.

### rediseñar

Consulte [Las 7 R](#).

### objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

### objetivo de tiempo de recuperación (RTO)

La demora máxima aceptable entre la interrupción del servicio y el restablecimiento del servicio.

### refactorizar

Consulte [Las 7 R](#).

## Region

Conjunto de AWS recursos en un área geográfica. Cada uno Región de AWS está aislado e independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para más información, consulte [Specify which Regiones de AWS your account can use](#).

### regresión

Una técnica de ML que predice un valor numérico. Por ejemplo, para resolver el problema de “¿A qué precio se venderá esta casa?”, un modelo de ML podría utilizar un modelo de regresión lineal para predecir el precio de venta de una vivienda en función de datos conocidos sobre ella (por ejemplo, los metros cuadrados).

### volver a alojar

Consulte [Las 7 R](#).

### versión

En un proceso de implementación, el acto de promover cambios en un entorno de producción.

reubicar

Consulte [Las 7 R](#).

redefinir la plataforma

Consulte [Las 7 R](#).

recomprar

Consulte [Las 7 R](#).

resiliencia

Capacidad de una aplicación para resistir interrupciones o recuperarse de ellas. Al planificar la resiliencia en la Nube de AWS, la [alta disponibilidad](#) y la [recuperación ante desastres](#) son consideraciones comunes. Para más información, consulte [Resiliencia en la Nube de AWS](#).

política basada en recursos

Una política asociada a un recurso, como un bucket de Amazon S3, un punto de conexión o una clave de cifrado. Este tipo de política especifica a qué entidades principales se les permite el acceso, las acciones compatibles y cualquier otra condición que deba cumplirse.

matriz responsable, confiable, consultada e informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina matriz RASCI y, si la excluye, se denomina matriz RACI.

control receptivo

Un control de seguridad que se ha diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Para obtener más información, consulte [Controles receptivos](#) en Implementación de controles de seguridad en AWS.

retain

Consulte [Las 7 R](#).

retirar

Consulte [Las 7 R](#).

## Generación aumentada de recuperación (RAG)

Tecnología de [IA generativa](#) mediante la que un [LLM](#) hace referencia a un origen de datos autorizado que se encuentra fuera de sus orígenes de datos de entrenamiento antes de generar una respuesta. Por ejemplo, un modelo de RAG podría hacer una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para más información, consulte [¿Qué es RAG \(generación aumentada por recuperación\)?](#)

## rotación

Proceso mediante el que periódicamente se actualiza un [secreto](#) para que resulte más difícil que un atacante pueda acceder a las credenciales.

## control de acceso por filas y columnas (RCAC)

El uso de expresiones SQL básicas y flexibles que tienen reglas de acceso definidas. El RCAC consta de permisos de fila y máscaras de columnas.

## RPO

Consulte [objetivo de punto de recuperación](#).

## RTO

Consulte [objetivo de tiempo de recuperación](#).

## manual de procedimientos

Conjunto de procedimientos manuales o automatizados necesarios para realizar una tarea específica. Por lo general, se diseñan para agilizar las operaciones o los procedimientos repetitivos con altas tasas de error.

# S

## SAML 2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta función permite el inicio de sesión único (SSO) federado, de modo que los usuarios pueden iniciar sesión en la Consola de administración de AWS o llamar a las operaciones de la AWS API sin tener que crear un usuario en IAM para todos los miembros de la organización. Para obtener más información sobre la federación basada en SAML 2.0, consulte [Acerca de la federación basada en SAML 2.0](#) en la documentación de IAM.

## SCADA

Consulte [control de supervisión y adquisición de datos](#).

## SCP

Consulte [política de control de servicio](#).

## secreta

En AWS Secrets Manager, información confidencial o restringida, como una contraseña o credenciales de usuario, que se almacena de forma cifrada. Se compone del valor del secreto y de sus metadatos. El valor del secreto puede ser binario, una sola cadena o varias cadenas. Para más información, consulte [What's in a Secrets Manager secret?](#) en la documentación de Secrets Manager.

## seguridad desde el diseño

Enfoque de ingeniería de sistemas que tiene en cuenta la seguridad durante todo el proceso de desarrollo.

## control de seguridad

Barrera de protección técnica o administrativa que impide, detecta o reduce la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Existen cuatro tipos de controles de seguridad principales: [preventivos](#), [de detección](#), [de respuesta](#) y [proactivos](#).

## refuerzo de la seguridad

Proceso de reducir la superficie expuesta a ataques para hacerla más resistente a los ataques. Esto puede incluir acciones, como la eliminación de los recursos que ya no se necesitan, la implementación de prácticas recomendadas de seguridad consistente en conceder privilegios mínimos o la desactivación de características innecesarias en los archivos de configuración.

## sistema de información sobre seguridad y administración de eventos (SIEM)

Herramientas y servicios que combinan sistemas de administración de información sobre seguridad (SIM) y de administración de eventos de seguridad (SEM). Un sistema de SIEM recopila, monitorea y analiza los datos de servidores, redes, dispositivos y otras fuentes para detectar amenazas y brechas de seguridad y generar alertas.

## automatización de la respuesta de seguridad

Acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o corregirlo. Estas automatizaciones sirven como controles de seguridad

[preventivos o adaptables](#) que le ayudan a implementar las mejores prácticas AWS de seguridad. La modificación de un grupo de seguridad de VPC, la aplicación de revisiones a una instancia de Amazon EC2 o la rotación de credenciales son algunos ejemplos de acciones de respuesta automatizadas.

#### cifrado del servidor

Cifrado de los datos en su destino, por parte de Servicio de AWS quien los recibe.

#### política de control de servicio (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. Las SCP definen barreras de protección o establecen límites a las acciones que un administrador puede delegar en los usuarios o roles. Puede utilizar las SCP como listas de permitidos o rechazados, para especificar qué servicios o acciones se encuentra permitidos o prohibidos. Para obtener más información, consulte [las políticas de control del servicio](#) en la AWS Organizations documentación.

#### punto de enlace de servicio

La URL del punto de entrada de un Servicio de AWS. Para conectarse mediante programación a un servicio de destino, puede utilizar un punto de conexión. Para obtener más información, consulte [Puntos de conexión de Servicio de AWS](#) en Referencia general de AWS.

#### acuerdo de nivel de servicio (SLA)

Acuerdo que aclara lo que un equipo de TI se compromete a ofrecer a los clientes, como el tiempo de actividad y el rendimiento del servicio.

#### indicador de nivel de servicio (SLI)

Medición de un aspecto del rendimiento de un servicio, como la tasa de errores, la disponibilidad o el rendimiento.

#### objetivo de nivel de servicio (SLO)

Métrica objetivo que representa el estado de un servicio medido mediante un [indicador de nivel de servicio](#).

#### modelo de responsabilidad compartida

Un modelo que describe la responsabilidad con AWS la que compartes la seguridad y el cumplimiento de la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el [Modelo de responsabilidad compartida](#).

## Shadow AI

Aplicaciones de [IA](#) no autorizadas creadas o utilizadas fuera de los canales regulados dentro de una organización.

## SIEM

Consulte [sistema de administración de eventos e información de seguridad](#).

## único punto de error (SPOF)

Error en un único componente crítico de una aplicación que puede interrumpir el sistema.

## SLA

Consulte [acuerdo de nivel de servicio](#).

## SLI

Consulte [indicador de nivel de servicio](#).

## SLO

Consulte [objetivo de nivel de servicio](#).

## modelo de dividir y sembrar

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para más información, consulte [Phased approach to modernizing applications in the Nube de AWS](#).

## SPOF

Consulte [único punto de error](#).

## esquema en estrella

Estructura organizativa de una base de datos que utiliza una tabla de hechos de gran tamaño para almacenar datos transaccionales o medidos y una o varias tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para utilizarse en un [almacén de datos](#) o con fines de inteligencia empresarial.

## patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado.

Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue [presentado por Martin Fowler](#) como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo de cómo aplicar este patrón, consulte [Modernización gradual de los servicios web antiguos de Microsoft ASP.NET \(ASMX\) mediante contenedores y Amazon API Gateway](#).

## subred

Un intervalo de direcciones IP en la VPC. Una subred debe residir en una sola zona de disponibilidad.

## control de supervisión y adquisición de datos (SCADA)

En el sector de la fabricación, sistema que utiliza hardware y software para supervisar los activos físicos y las operaciones de producción.

## cifrado simétrico

Un algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar los datos.

## pruebas sintéticas

Prueba de un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o supervisar el rendimiento. Puede usar [Amazon CloudWatch Synthetics](#) para crear estas pruebas.

## petición del sistema

Técnica para proporcionar contexto, instrucciones o pautas a un [LLM](#) para dirigir su comportamiento. Las peticiones del sistema ayudan a establecer el contexto y las reglas para las interacciones con los usuarios.

# T

## etiquetas

Key-value pares que actúan como metadatos para organizar sus AWS recursos. Las etiquetas pueden ayudar a administrar, identificar, organizar, buscar y filtrar recursos de . Para obtener más información, consulte [Etiquetado de los recursos de AWS](#).

## variable de destino

El valor que intenta predecir en el ML supervisado. Esto también se conoce como variable de resultado. Por ejemplo, en un entorno de fabricación, la variable objetivo podría ser un defecto del producto.

## lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

## entorno de prueba

Consulte [entorno](#).

## entrenamiento

Proporcionar datos de los que pueda aprender su modelo de ML. Los datos de entrenamiento deben contener la respuesta correcta. El algoritmo de aprendizaje encuentra patrones en los datos de entrenamiento que asignan los atributos de los datos de entrada al destino (la respuesta que desea predecir). Genera un modelo de ML que captura estos patrones. Luego, el modelo de ML se puede utilizar para obtener predicciones sobre datos nuevos para los que no se conoce el destino.

## herramienta

Una función o API que un [agente](#) puede invocar para realizar operaciones en sistemas externos.

## puerta de enlace de tránsito

Centro de tránsito de red que puede utilizar para interconectar las VPC y las redes en las instalaciones. Para obtener más información, consulte [Qué es una pasarela de tránsito](#) en la AWS Transit Gateway documentación.

## flujo de trabajo basado en enlaces troncales

Un enfoque en el que los desarrolladores crean y prueban características de forma local en una rama de característica y, a continuación, combinan esos cambios en la rama principal. Luego, la rama principal se adapta a los entornos de desarrollo, preproducción y producción, de forma secuencial.

## acceso de confianza

Otorgar permisos a un servicio que especifique para realizar tareas en su organización AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración por usted. Para obtener más información, consulte [AWS Organizations Utilización con otros AWS servicios](#) en la AWS Organizations documentación.

## ajuste

Cambiar aspectos de su proceso de formación a fin de mejorar la precisión del modelo de ML. Por ejemplo, puede entrenar el modelo de ML al generar un conjunto de etiquetas, incorporar etiquetas y, luego, repetir estos pasos varias veces con diferentes ajustes para optimizar el modelo.

## equipo de dos pizzas

Un DevOps equipo pequeño al que puedes alimentar con dos pizzas. Un equipo formado por dos integrantes garantiza la mejor oportunidad posible de colaboración en el desarrollo de software.

# U

## incertidumbre

Un concepto que hace referencia a información imprecisa, incompleta o desconocida que puede socavar la fiabilidad de los modelos predictivos de ML. Hay dos tipos de incertidumbre: la incertidumbre epistémica se debe a datos limitados e incompletos, mientras que la incertidumbre aleatoria se debe al ruido y la aleatoriedad inherentes a los datos.

## tareas indiferenciadas

También conocido como tareas arduas, es el trabajo que es necesario para crear y operar una aplicación, pero que no proporciona un valor directo al usuario final ni proporciona una ventaja competitiva. Algunos ejemplos de tareas indiferenciadas son la adquisición, el mantenimiento y la planificación de la capacidad.

## entornos superiores

Consulte [entorno](#).

## V

### succión

Una operación de mantenimiento de bases de datos que implica limpiar después de las actualizaciones incrementales para recuperar espacio de almacenamiento y mejorar el rendimiento.

### control de versión

Procesos y herramientas que realizan un seguimiento de los cambios, como los cambios en el código fuente de un repositorio.

### Emparejamiento de VPC

Conexión entre dos VPC que permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulte [¿Qué es una interconexión de VPC?](#) en la documentación de Amazon VPC.

### vulnerabilidad

Defecto de software o hardware que pone en peligro la seguridad del sistema.

## W

### caché caliente

Un búfer caché que contiene datos actuales y relevantes a los que se accede con frecuencia. La instancia de base de datos puede leer desde la caché del búfer, lo que es más rápido que leer desde la memoria principal o el disco.

### datos templados

Datos a los que el acceso es infrecuente. Al consultar este tipo de datos, normalmente se aceptan consultas moderadamente lentas.

### función de ventana

Función SQL que hace un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para las tareas de procesamiento, como calcular una media móvil o acceder al valor de las filas en función de la posición relativa de la fila actual.

## carga de trabajo

Conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.

## flujo de trabajo

Grupos funcionales de un proyecto de migración que son responsables de un conjunto específico de tareas. Cada flujo de trabajo es independiente, pero respalda a los demás flujos de trabajo del proyecto. Por ejemplo, el flujo de trabajo de la cartera es responsable de priorizar las aplicaciones, planificar las oleadas y recopilar los metadatos de migración. El flujo de trabajo de la cartera entrega estos recursos al flujo de trabajo de migración, que luego migra los servidores y las aplicaciones.

## WORM

Consulte [escritura única y lectura múltiple](#).

## WQF

Consulte [AWS Workload Qualification Framework](#).

## escritura única y lectura múltiple (WORM)

Modelo de almacenamiento que escribe los datos una sola vez y evita que se eliminen o modifiquen. Los usuarios autorizados pueden leer los datos tantas veces como sea necesario, pero no los pueden cambiar. Esta infraestructura de almacenamiento de datos se considera [inmutable](#).

## Z

### ataque de día cero

Ataque, normalmente de malware, que se aprovecha de una [vulnerabilidad de día cero](#).

### vulnerabilidad de día cero

Un defecto o una vulnerabilidad sin mitigación en un sistema de producción. Los agentes de amenazas pueden usar este tipo de vulnerabilidad para atacar el sistema. Los desarrolladores suelen darse cuenta de la vulnerabilidad a raíz del ataque.

### peticiones desde cero

Proporcionar a un [LLM](#) instrucciones para llevar a cabo una tarea, pero sin ejemplos (pasos) que puedan ayudar a guiarlo. El LLM debe usar los conocimientos del entrenamiento previo para

llevar a cabo la tarea. La eficacia de la petición desde cero depende de la complejidad de la tarea y de la calidad de la petición. Consulte también [peticiones con pocos pasos](#).

#### aplicación zombi

Aplicación que utiliza un promedio de CPU y memoria menor al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.