



Aplicación del marco AWS Well-Architected a Amazon Applications WorkSpaces

AWS Guía prescriptiva



AWS Guía prescriptiva: Aplicación del marco AWS Well-Architected a Amazon Applications WorkSpaces

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
Destinatarios previstos	1
Objetivos	2
Pilar de excelencia operativa	3
Organice los equipos en función de los resultados empresariales	3
Implemente la observabilidad para obtener información procesable	4
Automatice de forma segura cuando sea posible	5
Realice cambios frecuentes, pequeños y reversibles	7
Refina los procedimientos de operaciones con frecuencia	8
Anticipe el fracaso	9
Aprenda de todos los eventos y métricas operativos	10
Utilice servicios gestionados	11
Pilar de seguridad	12
Implemente una base de identidad sólida	12
Mantenga la trazabilidad	13
Aplica la seguridad en todos los niveles	14
Automatice las prácticas recomendadas de seguridad	15
Mantenga a las personas alejadas de los datos	16
Prepárese para los eventos de seguridad	16
Pilar de fiabilidad	18
Recuperación automática de errores	18
Prueba de los procedimientos de recuperación	19
Escale horizontalmente para aumentar la disponibilidad de la carga de trabajo agregada	19
Deja de adivinar la capacidad	20
Gestione los cambios mediante la automatización	20
Pilar de eficiencia de rendimiento	21
Democratice las tecnologías avanzadas	21
Globalícese en cuestión de minutos	22
Utilice arquitecturas sin servidor	22
Experimenta con más frecuencia	23
Considera la simpatía mecánica	23
Pilar de optimización de costos	25
Implementación de la administración financiera en la nube	25
Añada un modelo de consumo	25

Mida la eficiencia general	26
Deje de gastar dinero en levantar objetos pesados indiferenciados	26
Analice y atribuya los gastos	27
Pilar de sostenibilidad	29
Comprensión del impacto	29
Establezca objetivos de sostenibilidad	29
Maximizar el uso	30
Anticipe y adopte ofertas de hardware y software nuevas y más eficientes	30
Servicios gestionados usados	31
Reduzca el impacto descendente de sus cargas de trabajo en la nube	31
Recursos	32
AWS documentación	32
AWS publicaciones de blog	32
Historial de documentos	35
Glosario	36
#	36
A	37
B	40
C	42
D	45
E	50
F	52
G	54
H	55
I	56
L	59
M	60
O	65
P	67
Q	70
R	71
S	74
T	78
U	79
V	80
W	80

Z	82
.....	lxxxiii

Aplicación del marco AWS Well-Architected a Amazon Applications WorkSpaces

Mohamed Wali, Amazon Web Services

Julio de 2025 ([historia del documento](#))

[En esta guía se describen las prácticas recomendadas para aplicar el marco de trabajo de AWS Well-Architected al utilizar Amazon Applications WorkSpaces](#) WorkSpaces Applications es un servicio de streaming de aplicaciones totalmente gestionado que le permite transmitir aplicaciones de escritorio a los usuarios sin tener que volver a escribirlas.

El AWS Well-Architected Framework ayuda a los arquitectos de la nube a crear infraestructuras seguras, de alto rendimiento, resilientes y eficientes para una variedad de aplicaciones y cargas de trabajo. También proporciona un enfoque coherente para que los usuarios y los AWS socios evalúen las arquitecturas e implementen diseños escalables.

El AWS Well-Architected Framework se basa en seis pilares:

- Excelencia operativa
- Seguridad
- Fiabilidad
- Eficiencia del rendimiento
- Optimización de costos
- Sostenibilidad

Esta guía explica cómo se aplican estos pilares y mejores prácticas al uso WorkSpaces de las aplicaciones.

Destinatarios previstos

Esta guía es para:

- Arquitectos e ingenieros de nube que diseñan e implementan soluciones de WorkSpaces aplicaciones y necesitan asegurarse de que sus arquitecturas sigan las mejores prácticas de AWS Well-Architected Framework.

- Los equipos de operaciones de TI que gestionan y mantienen los entornos de WorkSpaces aplicaciones, gestionan la gestión, el escalado y la supervisión de la flota y necesitan optimizar los costes y el rendimiento.
- Organismos o empresas que están pensando en utilizar WorkSpaces aplicaciones o que ya las utilizan, desean transmitir aplicaciones de escritorio a sus usuarios y necesitan crear infraestructuras seguras, de alto rendimiento, resilientes y eficientes.

Objetivos

Seguir las prácticas recomendadas de esta guía le ayudará a:

- Cree una infraestructura segura, de alto rendimiento, resiliente y eficiente para transmitir aplicaciones de escritorio en streaming en. Nube de AWS
- Aplique un enfoque coherente al evaluar WorkSpaces las arquitecturas de las aplicaciones e implementar diseños escalables.

Pilar de excelencia operativa

La excelencia operativa (OE) representa la dedicación a crear soluciones de software de alta calidad que cumplan y superen constantemente las expectativas de los usuarios. El [pilar de excelencia operativa del AWS Well-Architected Framework](#) abarca estrategias comprobadas para una organización eficaz del equipo, un diseño sólido de la carga de trabajo, operaciones eficientes a gran escala y una adaptación perfecta a los requisitos cambiantes a lo largo del tiempo. Al cumplir estos principios, las organizaciones pueden garantizar que sus sistemas sigan siendo resilientes, eficientes y alineados con las cambiantes necesidades empresariales.

Áreas de enfoque clave para aplicar este pilar a su entorno de streaming de WorkSpaces aplicaciones:

- Monitoreo y observabilidad
- Automatización y DevOps
- Procedimientos operativos y documentación
- Support y gestión de incidentes

Organice los equipos en función de los resultados empresariales

Cree un modelo operativo alineado con la nube con un fuerte compromiso de liderazgo, en el que los objetivos empresariales y los indicadores clave de rendimiento (KPIs) impulsen la transformación organizacional mediante la optimización de las personas, los procesos y la tecnología.

- Estructura de equipo. Establezca equipos dedicados que se adapten a los resultados de la transmisión de aplicaciones. Por ejemplo:
 - El equipo de administración de imágenes es responsable del empaquetado de las aplicaciones y de la optimización de las imágenes.
 - El equipo de operaciones de la flota gestiona la capacidad, el rendimiento y el escalado.
 - El equipo de experiencia de usuario se encarga del apoyo y la satisfacción de los usuarios finales.
- KPIs y métricas. Defina y realice un seguimiento de las métricas alineadas con el negocio, tales como:
 - Tasas de disponibilidad de las aplicaciones

- Es hora de implementar nuevas aplicaciones
- Coste por hora de streaming de aplicaciones
- Modelo operativo. Cree procesos claros para:
 - Incorporación y actualizaciones de aplicaciones
 - Gestión de la capacidad de la flota
 - Aprovisionamiento de acceso de usuarios
 - Respuesta y resolución de incidentes

Implemente la observabilidad para obtener información procesable

Implemente un monitoreo y una observabilidad integrales para rastrear el estado de la carga de KPIs trabajo. Este principio permite tomar decisiones basadas en datos y mejorar proactivamente el rendimiento, la fiabilidad y los costes.

- Implemente la supervisión del rendimiento. Configura [Amazon CloudWatch](#) para:
 - Garantice una capacidad suficiente para satisfacer la demanda. Por ejemplo, puede utilizar las siguientes métricas:
 - `AvailableCapacity` para supervisar las instancias de streaming disponibles
 - `InUseCapacity` para realizar un seguimiento de las instancias utilizadas actualmente
 - `CapacityUtilization` para monitorear el porcentaje de uso de la flota
 - Supervise la experiencia y el rendimiento del usuario.
 - Identifique y aborde los problemas de servicio con prontitud.
- Realice un seguimiento y analice los informes de uso de WorkSpaces las aplicaciones.
- Capture y analice los registros de las aplicaciones. Para obtener más información, consulte las entradas del AWS blog [Uso de Kinesis Agent para Linux para transmitir registros de WorkSpaces aplicaciones en aplicaciones y Uso de Kinesis Agent para Microsoft Windows para almacenar registros de eventos de Windows de WorkSpaces aplicaciones](#).
- Supervise WorkSpaces las métricas y los eventos de las aplicaciones mediante notificaciones de chat. Para obtener más información, consulte la entrada del AWS blog [Supervise y automatice la computación de usuario AWS final \(EUC\) con AWS Chatbot](#).
- Habilite la gestión proactiva de las sesiones mediante señales visuales. Para obtener más información, consulta la entrada del AWS blog [Mostrar el vencimiento de la sesión y un temporizador de cuenta atrás en Amazon WorkSpaces Applications](#).

- Cree visualizaciones para patrones y tendencias de uso. Para obtener más información, consulta la entrada del AWS blog [Ingesta y visualiza los informes de uso de Amazon WorkSpaces Applications en Amazon OpenSearch Service](#).
- Utilice el kit de herramientas EUC para supervisar las sesiones activas, realizar un seguimiento del inventario de la flota y generar informes de las sesiones (exportación a CSV). Para obtener más información, consulte la entrada del AWS blog [Use the EUC Toolkit para gestionar Amazon WorkSpaces Applications y Amazon](#). WorkSpaces

Automatice de forma segura cuando sea posible

Aplique los principios de la infraestructura como código (IaC) para automatizar todos los aspectos de las operaciones de carga de trabajo. Utilice barandas para garantizar una ejecución segura y coherente y, al mismo tiempo, reducir la intervención manual.

- Automatice la creación y configuración de imágenes de WorkSpaces aplicaciones mediante la CLI de Image Assistant. Para obtener más información, [consulte Crear la imagen de Amazon WorkSpaces Applications mediante programación mediante las operaciones CLI de Image Assistant](#) en la documentación de WorkSpaces aplicaciones.
- Instalación de aplicaciones: utilice la CLI de Image Assistant para automatizar la instalación de aplicaciones durante la creación de imágenes.
- Creación de imágenes: cree imágenes de WorkSpaces aplicaciones mediante programación mediante los comandos CLI de Image Assistant.
- Gestión de la configuración: automatice la configuración de los ajustes predeterminados de la aplicación y los parámetros de inicio.
- Automatice la personalización de WorkSpaces las imágenes de las aplicaciones. Para obtener más información, consulte la AWS entrada del blog [Cómo crear automáticamente imágenes personalizadas de WorkSpaces aplicaciones para Windows](#).
- Aplique el iAC para implementar la infraestructura y los componentes de las WorkSpaces aplicaciones. Para obtener más información, consulte la entrada del AWS blog [Automatización del despliegue de infraestructuras y WorkSpaces aplicaciones para Amazon Applications with Terraform](#).
- Implemente procesos automatizados para la gestión de flotas, que incluyen:
 - Escalamiento de la flota en función de la demanda. Configure políticas de escalado automático para ajustar la capacidad de la flota automáticamente en función de las métricas de utilización.

Para obtener más información, consulta la entrada del AWS blog [Use AWS Lambda to adjust scaling steps and umbrals for Amazon WorkSpaces Applications](#).

- Actualizaciones de imágenes base. Aproveche las actualizaciones automáticas de la imagen base de la WorkSpaces aplicación que proporciona AWS.
- Optimización de la capacidad. Configure umbrales de escalado automatizados para optimizar el uso de los recursos en función de los patrones de demanda.
- Configure las barandillas para automatizar los controles de seguridad:
 - Límites de tamaño máximo de la flota. Establezca límites superiores en la capacidad de la flota para evitar el sobreaprovisionamiento.
 - Configuración de políticas de escalado. Implemente políticas de escalado escalonado o escalado de seguimiento objetivo con los umbrales adecuados.
 - Cuotas de servicio. Utilice las cuotas de AWS servicio como límites integrados para evitar una asignación excesiva de recursos.
 - Protección escalable. Configure la protección escalable para evitar que se eliminen las instancias activas durante los eventos de escalado.
- Realice pruebas y validaciones, incluidas las pruebas de creación de imágenes, flota e integración.
 - Pruebas con el generador de imágenes:
 - Pruebe las aplicaciones directamente en la interfaz del generador de imágenes.
 - Verifique el inicio y la funcionalidad de la aplicación.
 - Pruebe los ajustes y las configuraciones del usuario.
 - Valide la compatibilidad de las aplicaciones.
 - Pruebas de flota:
 - Pruebe las sesiones de streaming desde diferentes dispositivos cliente.
 - Verifica los derechos y el acceso de los usuarios.
 - Valide el rendimiento de las aplicaciones.
 - Pruebe la experiencia del usuario con elementos y operaciones como el portapapeles, la transferencia de archivos y la impresión.
 - Pruebas de integración:
 - Pruebe la autenticación basada en Active Directory o SAML 2.0.
 - Pruebe las carpetas principales y el almacenamiento persistente.
 - Pruebe los derechos de las aplicaciones.

- Pruebe la redirección del dispositivo USB (si está configurada).
- Utilice el administrador de WorkSpaces aplicaciones para automatizar el empaquetado y la implementación de las aplicaciones. Para obtener más información, consulte la entrada del AWS blog [Optimice la incorporación de aplicaciones con el administrador de aplicaciones para Amazon WorkSpaces Applications](#).
- Automatice la implementación de nuevas versiones de aplicaciones mediante el uso de canalizaciones de integración y entrega continuas (CI/CD). Para obtener más información, consulte la entrada del AWS blog [Screening Eagle: Optimice CI/CD and End User Experience in Amazon WorkSpaces Applications](#).

Realice cambios frecuentes, pequeños y reversibles

Cree cargas de trabajo escalables y poco acopladas que permitan despliegues automatizados frecuentes y a pequeña escala con un riesgo mínimo y funciones de reversión sencillas.

- Para las actualizaciones de imágenes, utilice la creación de imágenes versionadas y las actualizaciones incrementales.
 - Creación de imágenes versionadas:
 - Cree nuevas imágenes para cada conjunto de cambios mediante un generador de imágenes.
 - Mantenga varias versiones de imágenes para admitir escenarios de reversión.
 - Utilice [estrategias de AWS etiquetado](#) para realizar un seguimiento de las versiones y los atributos de las imágenes.
 - Actualizaciones incrementales:
 - Realice cambios pequeños e incrementales en las aplicaciones o configuraciones.
 - Pruebe minuciosamente las actualizaciones en el generador de imágenes antes de crear una imagen nueva.
 - Documente todos los cambios que haya realizado en cada nueva versión de la imagen.
- Para actualizar la flota de control:
 - Cree nuevas flotas con imágenes actualizadas para realizar pruebas.
 - Modifique los atributos de la flota existente sin interrumpir las sesiones activas.
- Establezca procedimientos de gestión de cambios para la documentación, los protocolos de pruebas, los flujos de trabajo de aprobación y los procesos de supervisión.
 - Documentación:

- Mantenga registros de cambios detallados para todas las actualizaciones de imagen y flota.
- Documente los procedimientos de prueba y los resultados de cada cambio.
- Se utiliza [AWS CloudTrail](#) para realizar un seguimiento de los cambios de configuración y auditarlos.
- Protocolos de prueba:
 - Establezca un proceso de prueba integral para todos los cambios.
 - Incluya pruebas de funcionalidad, rendimiento y experiencia del usuario de las aplicaciones.
 - Realice pruebas en el generador de imágenes antes de crear nuevas imágenes.
 - Realice pruebas adicionales en flotas que no estén en producción antes del despliegue completo.
- Flujos de trabajo de aprobación:
 - Implemente un proceso de aprobación para los cambios en los entornos de producción.
 - Defina los criterios para los cambios que requieren aprobación en comparación con las actualizaciones estándar.
 - Establezca las funciones y responsabilidades para la aprobación de los cambios.
- Supervisión y validación:
 - Usa [Amazon CloudWatch](#) para monitorear el rendimiento de la flota y las aplicaciones después de los cambios.
 - Configura alertas para las métricas clave a fin de identificar rápidamente los problemas después de las actualizaciones.
 - Realice revisiones posteriores a la implementación para validar el éxito del cambio y recopilar información.

Refina los procedimientos de operaciones con frecuencia

Mejore continuamente los procedimientos operativos mediante revisiones y actualizaciones periódicas y la participación del equipo para mantener a todas las partes interesadas informadas y alineadas con las mejores prácticas.

- Gestión de la documentación. Mantenga la documentación actualizada y controlada por versiones de los procedimientos de WorkSpaces las aplicaciones en una ubicación central para garantizar la coherencia operativa y el intercambio de conocimientos entre los equipos.

- Documentación requerida: mantenga la up-to-date documentación de WorkSpaces las operaciones de aplicaciones críticas para la creación y administración de imágenes, las operaciones de la flota y la solución de problemas.
- Revisiones operativas: supervise y revise los aspectos operativos clave, incluidas las métricas de rendimiento y la gestión de incidentes.
- Mejora continua. Mejore sistemáticamente las operaciones de las WorkSpaces aplicaciones incorporando Servicio de AWS actualizaciones, métricas operativas y las mejores prácticas aprendidas en los procedimientos estándar.
 - Actualizaciones del servicio: supervise las notas de la versión de WorkSpaces las aplicaciones para conocer las nuevas funciones, las mejoras del servicio, las actualizaciones de seguridad y la disponibilidad regional.
 - Mejores prácticas: revise e incorpore las actualizaciones de AWS Well-Architected Framework, las mejores prácticas de aplicaciones WorkSpaces , las arquitecturas de referencia AWS y las recomendaciones de seguridad. AWS
 - Gestión del conocimiento: mantenga y actualice los procedimientos operativos estándar, los manuales de instrucciones, las guías de solución de problemas y la documentación de soporte al usuario.

Anticipe el fracaso

Realice pruebas periódicas de los escenarios de fallo para comprender los riesgos, validar los procedimientos de respuesta y mejorar la preparación del equipo para gestionar incidentes reales.

- Pruebas de fallos. Simule y pruebe con regularidad fallos como el agotamiento de la capacidad de la flota, los fallos en el lanzamiento de las aplicaciones y los problemas de conectividad de la red.
 - Agotamiento de la capacidad de la flota:
 - Supervise y pruebe el comportamiento de escalado de la flota cuando se acerque a los límites de capacidad.
 - Configure CloudWatch las alarmas CapacityUtilization y AvailableCapacity las métricas.
 - Implemente procedimientos para gestionar las restricciones de capacidad durante los picos de uso.
 - Fallos en el inicio de la aplicación:
 - Pruebe el comportamiento de inicio de la aplicación en instancias de streaming.

- Valide el acceso y el rendimiento de las aplicaciones en diferentes configuraciones de flota.
- Problemas de conectividad de red:
 - Pruebe el rendimiento de la sesión de streaming en diferentes condiciones de red.
 - `StreamingSessionLatencySupervisa` si hay problemas de calidad de conexión.
 - Asegúrese de que los ajustes de la VPC y los grupos de seguridad estén correctamente configurados.
- Procedimientos de recuperación. Desarrolle y pruebe procedimientos para:
 - Conmutación por error de la flota entre Zonas de disponibilidad de AWS. Además, documente los procedimientos para ampliar la capacidad de la flota, gestionar las actualizaciones de la flota y responder a los problemas de estado de las instancias.
 - Gestión de datos de usuario:
 - Configure y pruebe las soluciones de [persistencia y almacenamiento de los ajustes de la aplicación](#) para las carpetas principales de las flotas de Amazon Simple Storage Service (Amazon S3) para Windows y los sistemas de archivos compartidos de Amazon Elastic File System (Amazon EFS) para flotas de Linux.
 - Valide la sincronización de datos entre sesiones.
 - Continuidad del servicio. Mantenga los procedimientos para crear nuevas instancias de flota, gestionar las actualizaciones de imágenes y gestionar las desconexiones de las sesiones.
- Gestión de riesgos. Identifique y mitigue:
 - Las restricciones de capacidad estableciendo la capacidad mínima de la flota adecuada, configurando políticas de escalado automático en función de los patrones de demanda y monitoreando las tendencias de utilización de la flota mediante CloudWatch métricas como `CapacityUtilizationInUseCapacity`, y `AvailableCapacity`.
 - Los cuellos de botella en el rendimiento mediante el seguimiento de las métricas clave, por ejemplo, `StreamingSessionLatency` y la configuración de las alarmas adecuadas. CloudWatch

Aprenda de todos los eventos y métricas operativos

Fomente una cultura de mejora continua compartiendo las lecciones aprendidas de los eventos y fracasos operativos en toda la organización. Haga hincapié en su impacto en los resultados empresariales.

- **Análisis de eventos.** Documente y analice las interrupciones del servicio, la degradación del rendimiento, las quejas de los usuarios y los problemas de capacidad.
- **Revisión de métricas.** Analice los patrones de uso, las tendencias de rendimiento, las métricas de costes y los datos de satisfacción de los usuarios de forma periódica.
- **Intercambio de conocimientos.** Establezca procesos para las sesiones de aprendizaje en equipo, la documentación sobre las mejores prácticas, la transferencia de conocimientos entre los equipos y las retrospectivas de los incidentes.

Utilice servicios gestionados

Minimice los gastos operativos mediante el uso de servicios AWS gestionados y la creación de procedimientos estandarizados en torno a ellos. Intégrelo con los siguientes servicios AWS gestionados:

- [AWS Systems Manager](#) para la automatización
- [Amazon CloudWatch](#) para monitoreo
- [AWS Identity and Access Management \(IAM\)](#) para el control de acceso
- [Amazon S3](#) para almacenamiento de usuarios para flotas de Windows
- [Amazon EFS](#) para almacenamiento de usuarios para flotas de Linux
- [AWS Directory Service](#) para la autenticación de usuarios

Pilar de seguridad

El [pilar de seguridad](#) de AWS Well-Architected Framework se centra en aprovechar las capacidades de la nube para ayudar a establecer mecanismos de protección sólidos para su información, infraestructura y recursos. Estos principios ayudan a mejorar su postura general de seguridad y, al mismo tiempo, permiten la innovación.

Áreas de enfoque clave para aplicar este pilar a su entorno de streaming de WorkSpaces aplicaciones:

- Integridad y confidencialidad de los datos
- Administración de permisos de usuario
- Establecer controles para detectar eventos de seguridad

Implemente una base de identidad sólida

Utilice los permisos mínimos necesarios para acceder a los AWS recursos y, al mismo tiempo, centralice la administración de identidades y evite las credenciales a largo plazo.

- Otorgue los permisos menos privilegiados para los recursos de WorkSpaces las aplicaciones:
 - Cree funciones de IAM específicas para WorkSpaces las flotas de aplicaciones con los permisos mínimos requeridos.
 - Configure permisos de IAM limitados para los creadores de imágenes.
 - Restrinja el acceso administrativo a WorkSpaces las funciones de administración de aplicaciones.
 - Defina permisos detallados para la gestión de pilas y flotas.
- Implemente los mecanismos de autenticación de usuarios adecuados:
 - Configure la federación SAML 2.0 para la integración de los proveedores de identidad empresariales.
 - Configure [AWS IAM Identity Center](#) para la administración de usuarios.
 - Utilice agentes de identidad personalizados solo cuando sea necesario para escenarios de autenticación específicos.
 - Implemente la autenticación multifactor (MFA) cuando sea compatible.
- Controle el acceso de los usuarios a las aplicaciones:

- Configure los derechos de las aplicaciones para restringir el acceso a aplicaciones específicas.
- Cree grupos de asignación de aplicaciones en función de las funciones de los usuarios.
- Gestione el acceso a las aplicaciones mediante permisos apilados.
- Implemente políticas de sesión para controlar el comportamiento de las aplicaciones.
- Proteja las sesiones de los usuarios con los controles adecuados:
 - Configure las políticas de tiempo de espera de las sesiones.
 - Establezca acciones de tiempo de espera de desconexión.
 - Implemente los requisitos de persistencia de la sesión.
 - Controle los permisos de redireccionamiento del sistema de archivos.
- Configure la autenticación basada en certificados para las aplicaciones. WorkSpaces Para obtener más información, consulte la entrada del AWS blog [Simplifique la autenticación basada en certificados para WorkSpaces aplicaciones y WorkSpaces con Autoridad de certificación privada de AWS Connector for Active Directory](#).
- Utilice etiquetas de sesión para implementar un control de acceso detallado. Para obtener más información, consulte la AWS entrada del blog [Use etiquetas de sesión para simplificar WorkSpaces los permisos de las aplicaciones](#).

Mantenga la trazabilidad

Implemente sistemas de monitoreo en tiempo real y respuesta automatizada para todos los cambios y actividades del entorno.

- Configure el [CloudWatch registro](#) de los registros de las aplicaciones para monitorear los eventos específicos de la aplicación, incluidos los lanzamientos, bloqueos y errores de la aplicación. Configure los registros de sesión para realizar un seguimiento de la información de las sesiones de streaming, incluidos los inicios y paradas de las sesiones y los eventos de conexión de los usuarios.
- [CloudTrail Actívelos para registrar todas WorkSpaces las llamadas a la API de aplicaciones](#) y realizar un seguimiento de los eventos de administración, como la creación y modificación de la flota, las operaciones del generador de imágenes, las configuraciones de las pilas y las actividades de administración de usuarios.
- Supervisa la actividad de WorkSpaces las instancias de Applications
 - Configure el registro de instancias para capturar los eventos a nivel del sistema.

- Realice un seguimiento de los lanzamientos y errores de las aplicaciones.
- Supervise el uso y el rendimiento de los recursos del sistema.
- Realice un seguimiento de la actividad del usuario:
 - Supervise los intentos y los errores de autenticación de los usuarios. Utilice CloudWatch métricas y CloudWatch registros para rastrear los intentos de inicio de sesión de los usuarios, las horas de inicio y finalización de la sesión y los eventos de desconexión de la sesión.
 - Rastrea los patrones de uso de las aplicaciones. [Habilite los informes de uso de WorkSpaces las aplicaciones](#) para recuperar información como la duración de la sesión, las horas de inicio y finalización, los tipos de instancias utilizadas y las aplicaciones a las que se ha accedido.
 - Registre las actividades del sistema de archivos a través de las carpetas de inicio habilitadas.
 - Configure los ajustes del portapapeles y las operaciones de impresión para lograr sus objetivos de prevención de la pérdida de datos.
- Configure [CloudWatchalarms](#) para métricas relacionadas con la seguridad, como las autenticaciones de usuarios fallidas, los patrones de sesión inusuales y las infracciones de acceso a los recursos.
- Utilice el kit de herramientas EUC para realizar un seguimiento de las sesiones y los estados activos, supervisar las direcciones IP de las sesiones activas en uso y exportar los datos de las sesiones para su auditoría. Para obtener más información, consulta la entrada del AWS blog [Usa el kit de herramientas EUC para gestionar Amazon WorkSpaces Applications y Amazon WorkSpaces](#)

Aplica la seguridad en todos los niveles

Implemente varios niveles de controles de seguridad en todos los componentes de su infraestructura, desde el perímetro de la red hasta el código de la aplicación.

- Configure la seguridad de la capa de red:
 - Implemente reglas estrictas para los grupos de seguridad.
 - Coloque WorkSpaces las instancias de la flota de aplicaciones en subredes privadas que no tengan acceso directo a Internet. Controle el acceso a Internet a través de dispositivos NAT.
 - Utilice puntos finales de nube privada virtual (VPC) para acceder a los dispositivos compatibles Servicios de AWS (como Amazon S3).

- Implemente listas de control de acceso a la red (ACLs) como capa de seguridad de red adicional.
- Restrinja el acceso al puerto de transmisión (TCP 8443 para HTTPS y WebSocket Secure) a rangos de IP específicos.
- Configure la seguridad de la capa de acceso:
 - Implemente políticas de tiempo de espera de sesión para desconectar automáticamente a los usuarios inactivos.
 - Implemente un control de acceso basado en atributos mediante etiquetas de sesión. Para obtener más información, consulta la AWS entrada del blog [Usa etiquetas de sesión para simplificar los permisos de WorkSpaces las aplicaciones.](#)
- Configure la seguridad de la capa de aplicaciones:
 - Configure los derechos de las aplicaciones para controlar qué usuarios pueden acceder a aplicaciones específicas.
 - Habilite los controles de redirección del sistema de archivos para restringir el acceso a las unidades locales.
 - Configure los permisos de portapapeles, transferencia de archivos e impresión en función de los requisitos de seguridad.
 - Configure los controles de acceso a los dispositivos USB de acuerdo con las políticas de seguridad.
- Configure la seguridad de la capa de imágenes:
 - Cree y mantenga imágenes base reforzadas que cumplan con los requisitos de seguridad.
 - Mantenga las imágenes base actualizadas con los últimos parches de seguridad.
 - Configure los ajustes de seguridad de Windows en las imágenes base.
 - Deshabilite los servicios y funciones de Windows innecesarios en las imágenes base.

Automatice las prácticas recomendadas de seguridad

Utilice controles de seguridad automatizados y definidos por código en plantillas controladas por versiones para permitir una implementación de infraestructura segura y escalable.

- Utilice la infraestructura como código (IaC) mediante el uso de servicios, por ejemplo, AWS CloudFormation para implementar configuraciones de seguridad uniformes en todos los despliegues de la flota. Para obtener más información, consulte la entrada del AWS blog [Adjuntar](#)

[automáticamente grupos de seguridad adicionales a Amazon WorkSpaces Applications y Amazon WorkSpaces.](#)

- Automatice los procesos de seguridad de creación de imágenes mediante la CLI de Image Assistant.
- Configure las respuestas automatizadas para los umbrales de utilización de la capacidad superados, los intentos de acceso no autorizado y los cambios en los grupos de seguridad mediante las CloudWatch alarmas de Amazon, EventBridge las reglas de Amazon y las AWS Lambda funciones de las respuestas automatizadas.

Mantenga a las personas alejadas de los datos

Automatice los procesos de manejo de datos para minimizar el acceso humano directo y reducir el riesgo de errores o mal manejo.

- Configure los derechos de las aplicaciones para controlar qué usuarios pueden acceder a aplicaciones específicas.
- Utilice el [marco de aplicaciones dinámicas](#) para crear un proveedor de aplicaciones dinámicas que permita que las aplicaciones estén disponibles de forma dinámica en función de los atributos del usuario.
- Configure la redirección del sistema de archivos para controlar a qué unidades locales pueden acceder los usuarios, restringir el acceso a carpetas específicas y administrar los permisos de transferencia de archivos entre las sesiones locales y de streaming.
- Implemente restricciones en el portapapeles para impedir que se comparta el portapapeles entre sesiones locales y de streaming, habilite el flujo unidireccional del portapapeles cuando sea necesario e impida la copia de datos no autorizada.
- Configure la persistencia de los ajustes de las aplicaciones para guardar y restaurar automáticamente las configuraciones de las aplicaciones, eliminar las necesidades de configuración manual y mantener una experiencia de usuario uniforme.

Prepárese para los eventos de seguridad

Desarrolle y ponga en práctica planes de respuesta a incidentes mediante el uso de herramientas automatizadas que permitan detectar, investigar y recuperarse rápidamente de los eventos de seguridad.

- Configure CloudWatch alarmas para los intentos de autenticación fallidos, los cambios en los grupos de seguridad de la flota, las modificaciones en las configuraciones de las imágenes y los patrones inusuales de las sesiones de streaming.
- Documente los procedimientos de respuesta para los escenarios de seguridad comunes de WorkSpaces las aplicaciones, como:
 - Intentos de acceso no autorizados
 - Detección: supervise los errores de autenticación.
 - Respuesta: revoque los derechos de los usuarios, revise los registros de sesión y actualice las políticas de acceso.
 - Instancias de streaming comprometidas
 - Detección: supervisa el comportamiento de las instancias.
 - Respuesta: finalice las sesiones afectadas, sustituya las instancias de la flota y revise las configuraciones de los grupos de seguridad.
 - Intentos de exfiltración de datos
 - Detección: supervise las actividades de transferencia de archivos.
 - Respuesta: revise los registros del portapapeles y de las transferencias de archivos, ajuste los permisos de transferencia de archivos y actualice las políticas de protección de datos.
- Implemente procesos de recuperación automatizados para reemplazar las instancias de la flota, restaurar los grupos de seguridad, reconfigurar el acceso de los usuarios y recuperar la configuración de las aplicaciones.
- Úselo Servicios de AWS para la gestión de la seguridad, como AWS Security Hub CSPM para los hallazgos de seguridad, y Amazon GuardDuty para la detección de amenazas.

Pilar de fiabilidad

El [pilar de confiabilidad](#) del Marco de AWS Buena Arquitectura aborda qué tan bien un sistema mantiene la funcionalidad y los niveles de rendimiento previstos durante los períodos operativos esperados a lo largo de su vida útil. Proporciona directrices exhaustivas para crear y mantener sistemas fiables AWS, incluidas estrategias para las pruebas y la validación en todas las etapas del ciclo de vida de la carga de trabajo.

Áreas de enfoque clave para aplicar este pilar a su entorno de streaming de WorkSpaces aplicaciones:

- Gestión y escalado de la flota
- Fiabilidad de las sesiones
- Disponibilidad de aplicaciones
- Procedimientos de recuperación

Recuperación automática de errores

Supervise el valor empresarial KPIs para activar respuestas automatizadas que puedan predecir, prevenir o recuperarse de las fallas antes de que afecten a las operaciones.

- Asegúrese de que la asignación de subredes IP tenga en cuenta la ampliación y la disponibilidad.
- Supervise CloudWatch las métricas críticas para garantizar la disponibilidad y el rendimiento del servicio, incluidas las métricas de capacidad de la flota (por ejemplo `InUseCapacity`, `AvailableCapacity` y las métricas de calidad del streaming) `StreamingSessionLatency`.
- Configure alertas para los umbrales de capacidad, las métricas del estado de las sesiones, la degradación del rendimiento y los cambios en el estado de la flota.
- Utilice las funciones de escalado automático integradas en las WorkSpaces aplicaciones para:
 - Configure la capacidad mínima y máxima de la flota.
 - Establezca políticas de escalado en función de la utilización de la capacidad.
 - Defina los umbrales de escalamiento horizontal y horizontal en función de las métricas de la experiencia del usuario y los requisitos empresariales, en lugar de solo las métricas técnicas.

- Cree un entorno de recuperación ante desastres para su entorno de aplicaciones. WorkSpaces Para obtener más información, consulte la AWS entrada del blog [Consideraciones sobre la recuperación ante desastres con Amazon WorkSpaces Applications](#).

Prueba de los procedimientos de recuperación

Los entornos en la nube permiten realizar pruebas automatizadas de los escenarios de fallo y los procedimientos de recuperación. Estas capacidades le ayudan a identificar y corregir las vulnerabilidades antes de que se produzcan fallos reales.

- Pruebas de recuperación de flota. Implemente pruebas exhaustivas de recuperación de la flota en varios escenarios:
 - Simule la terminación de la instancia para verificar la respuesta de escalado automática.
 - Valide el mantenimiento de la capacidad mínima de la flota.
 - Pruebe el tiempo de reemplazo de la instancia y el redireccionamiento de los usuarios.
 - Valide la eficacia de las políticas de escalado.
 - Pruebe los límites de capacidad de la flota y la gestión de desbordamientos.
- Pruebas de recuperación de sesiones. Implemente procedimientos de validación de la recuperación de sesiones:
 - Pruebe los escenarios de desconexión y reconexión.
 - Verifique la conservación del estado de la aplicación.
 - Pruebe varios escenarios de interrupción de la red.
 - Valide los comportamientos de tiempo de espera de las sesiones.
 - Compruebe la persistencia de la autenticación de los usuarios.
 - Compruebe la gestión del almacenamiento temporal.

Escale horizontalmente para aumentar la disponibilidad de la carga de trabajo agregada

Distribuya su carga de trabajo entre varios recursos más pequeños para minimizar el impacto de las fallas individuales y eliminar los puntos únicos de falla.

- **Implemente instancias de flota en varias zonas de disponibilidad.**

- Configure la capacidad mínima de flota adecuada.
- Configure el escalado automático para las flotas y establezca los umbrales de escalado adecuados.
- Supervise la utilización de la capacidad en toda la flota.
- Implemente pilas de WorkSpaces aplicaciones en varias regiones. Para obtener más información, consulta la entrada del AWS blog [Optimiza la experiencia del usuario con el enrutamiento basado en la latencia para Amazon Applications](#). WorkSpaces

Deja de adivinar la capacidad

Utilice las capacidades de escalado automático de la nube para ajustar los recursos de forma dinámica en función de la demanda. Esto ayuda a evitar la saturación de los recursos y, al mismo tiempo, a mantener una eficiencia óptima.

- Supervise las métricas clave `CapacityUtilization`, como `AvailableCapacity`, y comprenda `InUseCapacity` las necesidades de capacidad.
- Realice un seguimiento de las tendencias de utilización de la flota en diferentes períodos de tiempo. Supervise los patrones diarios, las variaciones semanales, las tendencias mensuales y los picos estacionales.
- Configure políticas de escalado y configure umbrales de escalado.
- Asegúrese de que exista una diferencia suficiente entre las cuotas actuales y el uso máximo para permitir la conmutación por error.
- Adapte las cuotas de servicio fijas y las restricciones a través de la arquitectura.

Gestione los cambios mediante la automatización

Implemente cambios en la infraestructura mediante la automatización, incluidos los cambios controlados por versiones en el propio código de automatización.

- Utilice iAC para configurar la flota.
- Implemente políticas de escalado consistentes.
- Utilice la [CLI de Image Assistant](#) para crear imágenes de forma coherente.

Pilar de eficiencia de rendimiento

El [pilar de eficiencia del rendimiento](#) del AWS Well-Architected Framework se centra en optimizar el uso de los recursos de la nube para cumplir o superar los objetivos de rendimiento y, al mismo tiempo, garantizar la adaptabilidad a las demandas fluctuantes y a las tecnologías emergentes. Hace hincapié en la importancia de ajustar continuamente los sistemas para mantener la máxima eficiencia en un entorno de nube dinámico.

Áreas de enfoque clave para aplicar este pilar a su entorno de streaming de WorkSpaces aplicaciones:

- Selección y optimización del tipo de instancia
- Optimización del rendimiento de streaming
- Gestión de la capacidad de la flota

Democratice las tecnologías avanzadas

Aproveche los servicios de nube gestionados por el proveedor para tecnologías complejas, de modo que su equipo pueda centrarse en el desarrollo de productos en lugar de en la gestión de la infraestructura.

- Configure los tipos de instancias adecuados en función de los requisitos de la aplicación:
 - Seleccione instancias habilitadas para GPU para aplicaciones con uso intensivo de gráficos.
 - Elija [las familias de GPU](#) adecuadas (como Graphics G4dn o Graphics G5) en función de las necesidades de la aplicación.
- Elija y configure uno de los siguientes métodos de autenticación:
 - Configure la integración con un proveedor de identidades basado en SAML 2.0.
 - Configure los ajustes del grupo de usuarios.
 - Integre con [AWS Directory Service](#).
- Habilite y configure las opciones de almacenamiento según las necesidades del usuario:
 - Configure las carpetas principales en [Amazon S3](#) para flotas basadas en Windows.
 - Configure sistemas de archivos compartidos en [Amazon EFS](#) para flotas basadas en Linux.
 - Configure los permisos de almacenamiento persistente.
 - Habilite la persistencia de los ajustes de la aplicación.

Globalícese en cuestión de minutos

Utilice la implementación en varias regiones para mejorar las experiencias de los usuarios globales mediante la reducción de la latencia.

- Configure flotas en varias regiones de AWS desplegando flotas en las regiones más cercanas a sus usuarios y creando pilas independientes para cada región.
- Implemente la redirección entre regiones para redirigir automáticamente a los usuarios de WorkSpaces las aplicaciones a las AppStream pilas más cercanas a su ubicación actual.
- Si utiliza alguna de las funciones opcionales de las WorkSpaces aplicaciones, como la persistencia de la configuración de la aplicación, las carpetas principales o las flotas elásticas, debe configurar la replicación entre regiones de Amazon S3 para los datos de usuario de las flotas basadas en Windows y la replicación entre regiones para las flotas basadas en Linux.
- Replique imágenes en todas las regiones. Para obtener más información, consulta [Copiar una imagen de tu propiedad a otra Región de AWS en Amazon WorkSpaces Applications](#) en la AWS documentación.
- En el caso de las flotas unidas a un dominio, asegúrese de que la infraestructura de Active Directory, incluidos los Servicios de federación de Active Directory (AD FS) (a menos que utilice SAML 2.0 y Amazon Cognito como alternativa), esté configurada correctamente en las demás regiones y de que la utilice para las capacidades de replicación multirregional. [AWS Directory Service for Microsoft Active Directory](#)
- Dirija a los usuarios a los puntos finales de aplicaciones con la latencia más baja. WorkSpaces Para obtener más información, consulta la entrada del AWS blog [Optimiza la experiencia del usuario con el enrutamiento basado en la latencia para Amazon Applications](#). WorkSpaces

Utilice arquitecturas sin servidor

Las arquitecturas sin servidor eliminan la sobrecarga de administración de servidores y reducen los costos mediante el uso de servicios administrados en la nube para las funciones informáticas.

Utilice servicios AWS sin servidor como los siguientes:

- [AWS Lambda](#) para automatizar tareas e integrar una lógica personalizada mediante funciones basadas en eventos
- [Amazon S3](#) proporcionará almacenamiento escalable para WorkSpaces aplicaciones, datos de usuario, archivos de aplicaciones y artefactos de sesión

- [Amazon CloudWatch](#) proporcionará monitoreo, registro y alertas para WorkSpaces las métricas de rendimiento y uso de las aplicaciones
- [Amazon Cognito facilitará la](#) autenticación de los usuarios y el control de acceso a las aplicaciones WorkSpaces
- [Amazon API Gateway](#) RESTful APIs para crear una interfaz entre WorkSpaces aplicaciones y otros servicios o aplicaciones personalizadas

Experimenta con más frecuencia

La infraestructura en la nube permite realizar pruebas rápidas de diversas configuraciones de recursos para optimizar el rendimiento y los costes.

- Pruebe diferentes tipos de instancias para optimizar el rendimiento y los costes:
 - Compare el rendimiento de las transmisiones en diferentes familias de instancias.
 - Evalúe las instancias con GPU y las que no lo son para aplicaciones gráficas.
 - Pruebe instancias optimizadas con memoria para aplicaciones con uso intensivo de memoria.
- Pruebe las configuraciones de las aplicaciones mediante Image Builder:
 - Cree imágenes de prueba con diferentes configuraciones de aplicaciones.
 - Valide el rendimiento de las aplicaciones antes del despliegue.
 - Pruebe la compatibilidad de las aplicaciones con distintos tipos de instancias.
- Pruebe la configuración de la flota mediante configuraciones de capacidad de la flota, como la capacidad mínima y máxima, las políticas de escalado, las configuraciones de sesión, como la duración máxima de la sesión, y la configuración de tiempo de espera de desconexión.

Considera la simpatía mecánica

Elija los servicios en la nube en función de los requisitos y patrones de uso específicos de su carga de trabajo para garantizar un rendimiento y una eficiencia óptimos.

- Elija las instancias Graphics G5 para aplicaciones con uso intensivo de gráficos, aplicaciones que requieran DirectX, OpenGL, OpenCL o software de visualización 3D.
- Seleccione `stream.standard` instancias para aplicaciones empresariales, navegadores web y aplicaciones de gráficos ligeros

- Supervise y ajuste el protocolo de transmisión en función de CloudWatch métricas como `StreamingSessionLatency`.
- Configure WorkSpaces las aplicaciones de VPCs forma que estén más cerca de sus usuarios y utilice el ancho de banda de red adecuado en función de los requisitos de la aplicación.
- Elija el tipo de flota adecuado en función del comportamiento de la aplicación. Por ejemplo, elija flotas de sesión única para aplicaciones que requieran recursos dedicados y flotas de sesiones múltiples para aplicaciones que puedan compartir recursos de manera eficiente.
- Considere la compatibilidad de las aplicaciones con entornos de varias sesiones.
- Utilice la [función de redireccionamiento del sistema de archivos](#) para gestionar las interacciones entre las aplicaciones remotas y locales. Para obtener más información, consulte la entrada del AWS blog [Lanzamiento de aplicaciones locales desde una sesión de streaming de Amazon WorkSpaces Applications](#).

Pilar de optimización de costos

El [pilar de optimización de costes del AWS Well-Architected Framework](#) se centra en maximizar el valor empresarial y, al mismo tiempo, minimizar los gastos. Ayuda a garantizar que cada dólar que gaste en recursos de la nube contribuya de manera efectiva al logro de los objetivos de su organización.

Áreas de enfoque clave para aplicar este pilar a su entorno de streaming de WorkSpaces aplicaciones:

- Gestión de la capacidad de la flota y selección del tipo de instancia
- Optimización del escalado y la programación
- Supervisión y análisis de los patrones de uso
- Asignación y seguimiento de costos

Implementación de la administración financiera en la nube

Desarrolle una capacidad organizativa dedicada a la gestión financiera y la optimización de costes en la nube mediante programas y procesos estructurados para maximizar el valor y la eficiencia de la nube.

- Supervise los costes de WorkSpaces las aplicaciones mediante [AWS Cost Explorer](#) el uso de informes de uso para realizar un seguimiento del uso de las horas de streaming, analizar los costes de las instancias de flota y supervisar la distribución regional de los costes.
- Planifique y establezca controles de costos mediante [AWS Budgets](#) el uso de alertas para los costos generales del servicio de WorkSpaces aplicaciones, establezca umbrales presupuestarios para el servicio y controle los gastos reales comparándolos con los montos presupuestados. Para obtener más información, consulta la entrada del AWS blog [Cómo utilizar la automatización para optimizar y controlar el coste de Amazon WorkSpaces Applications](#).

Añada un modelo de consumo

Amplíe los recursos y los costes informáticos en función de los patrones de uso reales. Por ejemplo, puede cerrar los entornos que no son de producción fuera del horario laboral para optimizar los gastos.

- Elija el modelo de precios adecuado. Por ejemplo, utilice flotas siempre activas para un uso uniforme y flotas bajo demanda para cargas de trabajo variables.
- Seleccione los tipos de instancias óptimos. Por ejemplo, use `stream.standard` instancias para aplicaciones generales y use instancias gráficas (G4dn) solo cuando sea necesario.

Mida la eficiencia general

Calcule y realice un seguimiento cost-per-unit de la producción empresarial para cuantificar las mejoras de eficiencia y orientar los esfuerzos de optimización.

- Realice un seguimiento de la eficiencia de las sesiones
- Supervise la utilización de la flota mediante las siguientes CloudWatch métricas:
 - `AvailableCapacity` para realizar un seguimiento de la capacidad no utilizada
 - `InUseCapacity` para medir el uso real
- Calcule y realice un seguimiento de los costes por sesión, como el coste por hora de streaming, el coste por usuario y el coste por aplicación.
- Implemente el [optimizador de costos para WorkSpaces aplicaciones para](#) monitorear a sus creadores.
- Compare los costos entre los tipos de flota. Por ejemplo, compare:
 - Costos de licencia para sesiones individuales y sesiones múltiples
 - Tasas de utilización de recursos
 - Densidad de usuarios por instancia
- Utilice los datos de seguimiento de procesos para identificar aplicaciones infrautilizadas o innecesarias. Para obtener más información, consulte la entrada del AWS blog [Seguimiento de los procesos de los usuarios en WorkSpaces las sesiones de Amazon Applications](#).

Deje de gastar dinero en levantar objetos pesados indiferenciados

AWS gestiona las operaciones de infraestructura y ofrece servicios gestionados para que su organización pueda centrarse en los objetivos empresariales y no en el mantenimiento de la TI.

- Cree y mantenga imágenes de aplicaciones mediante Image Builder para empaquetar las aplicaciones, configurar los ajustes de las aplicaciones y probar la compatibilidad de las aplicaciones.

- Configure las especificaciones de la flota seleccionando los tipos de instancias adecuados, definiendo los umbrales de escalado y estableciendo los límites de capacidad deseados.
- Configure las opciones de almacenamiento persistente configurando las carpetas principales en [Amazon S3](#) para las flotas basadas en Windows y los sistemas de archivos compartidos en Amazon [EFS](#) para las flotas basadas en Linux. Establezca los permisos de almacenamiento y defina las políticas de retención.

Analice y atribuya los gastos

La nube permite realizar un seguimiento preciso del uso de los recursos y los costes por carga de trabajo, lo que permite medir con precisión el retorno de la inversión (ROI) y ofrecer oportunidades de optimización específicas.

- Implemente una estrategia integral de etiquetado para las flotas para la asignación de costes, las imágenes para el seguimiento de los activos, los generadores de imágenes para la designación del entorno y las pilas para la agrupación organizacional.
- Utilice [los informes de AWS costos y uso \(AWS CUR\)](#) para desglosar los costos de WorkSpaces las aplicaciones por recursos etiquetados y analice los costos por flota, pila e imagen.
- Úselos [AWS Cost Explorer](#) para visualizar las tendencias de gasto en WorkSpaces aplicaciones y comparar los costos en diferentes dimensiones, como las regiones y los tipos de instancias.
- Supervise y analice las tasas de utilización de la flota, la eficiencia del tipo de instancia y las horas de streaming por aplicación.
- Realice un seguimiento de la capacidad reservada no utilizada, de las flotas o parques infrautilizados y de los períodos de inactividad durante el uso de la flota.
- Calcule y realice un seguimiento del costo por usuario de cada aplicación, las horas de transmisión por aplicación y las tasas de adopción por parte de los usuarios de las aplicaciones transmitidas.
- Configure un análisis de uso detallado mediante la configuración de los informes de uso de WorkSpaces las aplicaciones, el uso de [Amazon Athena](#) para consultar los datos de uso y la creación de visualizaciones en [Amazon Quick](#) para obtener información sobre los costes y el uso.
- Evalúe las consideraciones de costo total, como las licencias de Windows Server, los modelos de licencias de aplicaciones y las licencias por usuario, en comparación con las licencias por dispositivo.
- Use Amazon Athena para consultar y analizar los costos de almacenamiento de las carpetas de inicio y los patrones de uso por usuario. Para obtener más información, consulte la entrada del

AWS blog [Cómo denunciar el uso de la carpeta principal de WorkSpaces las aplicaciones de Amazon con Amazon Athena.](#)

Pilar de sostenibilidad

El [pilar de sostenibilidad](#) del AWS Well-Architected Framework hace hincapié en minimizar la huella ambiental y optimizar el uso y la eficiencia de la energía. Guía a los arquitectos para que tomen decisiones respetuosas con el medio ambiente en sus diseños de sistemas y estrategias de asignación de recursos.

Áreas de enfoque clave para aplicar este pilar a su entorno de streaming de WorkSpaces aplicaciones:

- Comprender y optimizar la asignación de recursos para adaptarla a la demanda real y minimizar el desperdicio en los entornos de streaming
- Analizar y adaptarse a los patrones de consumo de los usuarios para mejorar la eficiencia de la entrega de aplicaciones y las sesiones de streaming
- Seleccionar y usar las configuraciones de hardware adecuadas para maximizar la eficiencia energética y, al mismo tiempo, cumplir con los requisitos de rendimiento
- Utilizar las capacidades de los servicios AWS gestionados para beneficiarse de las economías de escala y las funciones de eficiencia integradas que ofrecen estos servicios

Comprensión del impacto

Supervise y optimice el impacto ambiental de su carga de trabajo midiendo la eficiencia de los recursos y las emisiones por unidad de producción. Utilice estos datos para establecer KPIs y guiar las mejoras en materia de sostenibilidad.

- Supervise los patrones de utilización de la flota.
- Realice un seguimiento de las horas de transmisión por usuario.
- Analice las tendencias de uso de la capacidad de la flota.

Establezca objetivos de sostenibilidad

Establezca metas de sostenibilidad mensurables para cada carga de trabajo que se alineen con los objetivos de la organización. Concéntrese en reducir la intensidad de los recursos por transacción a medida que vaya escalando.

- Establezca objetivos para las tasas de utilización de la flota, la eficiencia de los tipos de instancias y la optimización de las horas de streaming.
- Planifique la capacidad en función de los patrones de uso reales.

Maximizar el uso

Optimice la eficiencia de la carga de trabajo al dimensionar correctamente los recursos y maximizar la utilización. Reduzca la capacidad inactiva para minimizar el consumo de energía y mejorar la sostenibilidad.

- Configure el escalado automático para que se adapte a la demanda real.
- Dimensione la capacidad de la flota de forma adecuada en función de los patrones de uso.
- Implemente los límites de capacidad mínima y máxima adecuados.
- Elija los tipos de instancias adecuados para las cargas de trabajo.
- Supervisa y optimiza la densidad de las sesiones de streaming.
- Reduzca la capacidad inactiva durante las horas de menor actividad.

Anticipe y adopte ofertas de hardware y software nuevas y más eficientes

Manténgase informado sobre las nuevas tecnologías eficientes de socios y proveedores y adopte rápidamente dichas tecnologías para mejorar continuamente el impacto ambiental de su carga de trabajo.

- Utilice los tipos de instancias de la generación actual.
- Actualice a tipos de instancias más nuevos cuando estén disponibles.
- Optimice la configuración de streaming de aplicaciones.
- Configure los protocolos de transmisión adecuados.
- Actualícese a las funciones más recientes de las WorkSpaces aplicaciones.

Servicios gestionados usados

Aproveche los servicios en la nube compartidos y las soluciones gestionadas para maximizar la eficiencia en la utilización de los recursos y, al mismo tiempo, minimizar el impacto ambiental mediante la escalabilidad automatizada y la gestión del ciclo de vida.

- Utilice [Amazon S3](#) para el almacenamiento de usuarios para flotas basadas en Windows y [Amazon EFS](#) para sistemas de archivos compartidos para flotas basadas en Linux.
- Implemente para la supervisión. [CloudWatch](#)
- Configure la [IAM](#) para la administración del acceso.

Reduzca el impacto descendente de sus cargas de trabajo en la nube

Diseñe servicios para minimizar los requisitos de recursos del lado del cliente, reducir el consumo de energía y prolongar la vida útil de los dispositivos para los usuarios.

- Ajuste la duración máxima de la sesión para evitar el consumo innecesario de recursos.
- Configure los tiempos de espera de sesión adecuados.
- Establezca políticas de tiempos de espera de desconexión.
- Implemente políticas de persistencia de sesiones cuando sea necesario.

Recursos

AWS documentación

- [AWS Marco de buena arquitectura](#)
- [Guía de administración WorkSpaces de aplicaciones de Amazon](#)
- [Guía CloudWatch del usuario de Amazon](#)
- [Guía del usuario de Amazon EFSS](#)
- [Guía del usuario de Amazon S3](#)
- [Guía del usuario de IAM](#)

AWS publicaciones de blog

- [WorkSpaces Aplicaciones basadas en la pertenencia a grupos de Active Directory, segmentación de aplicaciones](#)
- [Cree un único proveedor de identidad para todas sus pilas de WorkSpaces aplicaciones de Amazon con Azure AD](#)
- [Configuración de la asistencia remota de Windows para Amazon WorkSpaces y Amazon WorkSpaces Applications](#)
- [Crear un registro TXT de AS2 TrustedDomains DNS para redirigir el cliente nativo de Amazon WorkSpaces Applications a un proveedor de identidad externo](#)
- [Creación de registros personalizados y CloudWatch alertas de Amazon en Amazon Applications WorkSpaces](#)
- [Redireccionamiento entre regiones con Geo Targetly y Amazon Applications WorkSpaces](#)
- [Recursos multicuenta y aplicaciones de Amazon WorkSpaces](#)
- [Habilite la federación con Bio-key PortalGuard y Amazon Applications WorkSpaces](#)
- [Habilitación de la federación con WorkSpaces aplicaciones simples SAMLphp y de Amazon](#)
- [Habilitar la federación de identidades con Duo Single Sign-On y Amazon Applications WorkSpaces](#)
- [Habilitación de la federación de identidades con las aplicaciones Shibboleth y Amazon WorkSpaces](#)
- [Estrategias de conmutación por error para VDI local con Amazon End User Computing](#)

- [Cómo utiliza Amazon WorkSpaces Applications para proporcionar a los científicos y analistas de datos acceso a datos confidenciales](#)
- [Cómo configurar la autenticación basada en certificados para las aplicaciones de Amazon WorkSpaces](#)
- [Cómo utilizar las reclamaciones de Okta con los derechos de solicitud para Amazon Applications WorkSpaces](#)
- [Gestión de laboratorios de computación en WorkSpaces aplicaciones de Amazon con administración de aplicaciones virtuales de código abierto](#)
- [Métodos para asignar los costos de sus WorkSpaces aplicaciones a sus unidades de negocio](#)
- [Supervisión de WorkSpaces aplicaciones de Amazon con Amazon OpenSearch Service y Amazon Kinesis Data Firehose](#)
- [Separación de redes y saneamiento de datos mediante Amazon WorkSpaces, Amazon WorkSpaces Applications y Amazon Macie](#)
- [OneLogin SSO con Amazon Applications WorkSpaces](#)
- [Optimice la ruta de audio de sus llamadas de Amazon Connect con Amazon WorkSpaces Applications](#)
- [Almacenamiento persistente para las flotas de Linux de Amazon WorkSpaces Applications en Amazon Elastic File System](#)
- [Redirigir una aplicación SAML de Okta al cliente nativo de Amazon WorkSpaces Applications](#)
- [Simplifique la gestión de imágenes de Amazon WorkSpaces Applications con el enmascaramiento de aplicaciones](#)
- [Transmita aplicaciones a un costo menor gracias a la compatibilidad con Amazon WorkSpaces Applications, flotas elásticas y Linux](#)
- [Transmisión desde puntos finales de VPC de interfaz para entornos regulados con aplicaciones WorkSpaces](#)
- [Utilice los derechos de WorkSpaces las aplicaciones de Amazon Applications con Azure AD](#)
- [Reportero de problemas de usuario para Amazon WorkSpaces Applications](#)
- [Uso de los derechos de WorkSpaces aplicaciones de Amazon Applications con Google Workspace](#)
- [Uso de Auth0 con Microsoft Active Directory en aplicaciones de Amazon WorkSpaces](#)
- [Uso de Microsoft AppLocker para gestionar la experiencia de las aplicaciones en Amazon WorkSpaces Applications](#)
- [Uso de Python para impulsar una GUI de WorkSpaces Applications Linux Imaging Assistant](#)

- [Opciones de redireccionamiento de aplicaciones web para el cliente de WorkSpaces aplicaciones](#)

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
Publicación inicial	—	23 de julio de 2025

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:

- **Refactorizar/rediseñar:** traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en 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: Migrar la base de datos de Oracle en las instalaciones a Amazon Aurora PostgreSQL-Compatible Edition.
- **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: Migrar el sistema de administración de las relaciones con los clientes (CRM) a Salesforce.com.
- **Volver a alojar (migrar mediante lift-and-shift):** traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades 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

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.

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 AIOps se utiliza en la estrategia de AWS migración, 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.

implementación azul/verde

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 más información, consulte el indicador [Implement break-glass procedures](#) en la guía de AWS Well-Architected.

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.

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: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCoE, establecer un modelo de operaciones)

- Migración: migración de aplicaciones individuales
- Reinención: optimización de productos y servicios e innovación en la nube

Stephen Orban definió estas etapas en la entrada del blog [The Journey Toward Cloud-First & the Stages of Adoption en el](#) 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 canalización de CI/CD 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 (CI/CD)

El proceso de automatización de las etapas de origen, compilación, 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 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.

malla 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.

defense-in-depth

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 defense-in-depth enfoque podría combinar la autenticación multifactorial, 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 ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework](#).

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. Este concepto lo introdujo Eric Evans en su libro, *Diseño impulsado por el dominio: abordando la complejidad en el corazón del 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 Microsoft ASP.NET \(ASMX\) 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. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian 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 AWS PrivateLink y conceder permisos a otras Cuentas de AWS o a responsables AWS Identity and Access Management (de IAM). 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, mediante el que los modelos aprenden a partir de ejemplos (pasos) incrustados en las peticiones. La técnica de peticiones con pocos pasos puede ser eficaz para las 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)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMs son capaces de realizar 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?](#)

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 [la sección 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 el cumplimiento en todas las unidades organizativas (OUs). 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.

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.

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 de DevOps publicación típico.

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

IaC

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 más información, consulte la práctica recomendada [Implementación mediante una infraestructura inmutable](#) en el Marco de 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 AWS de referencia de seguridad](#) recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

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

Término que introdujo [Klaus Schwab](#) en 2016 para referirse a la modernización de los procesos de fabricación mediante los avances en la conectividad, los datos en tiempo real, la automatización, el análisis, la IA y el 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 de la Internet de las cosas \(IIoT\) industrial](#).

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red VPCs entre Internet y las redes locales (en una misma o Regiones de AWS diferente). La [arquitectura AWS de referencia de seguridad](#) recomienda configurar su cuenta de red con entrada, salida e inspección VPCs para proteger la interfaz bidireccional entre la 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 obtener más información, consulte Qué son. LLMs](#)

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 para lo cual 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](#).

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 Framework.

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 machine-to-machine \(M2M\), basado en el patrón de publicación/suscripción, para dispositivos de IoT con recursos limitados.](#)

microservicio

Un servicio pequeño e independiente que se comunica a través de una red bien definida APIs 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 AWS servicios sin servidor](#).

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 un uso ligero. APIs 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

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de las fábricas de migración suelen incluir a analistas y propietarios de operaciones, empresas, 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 fiabilidad y la previsibilidad, el AWS Well-Architected Framework 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](#).

Open Process Communications: arquitectura unificada (OPC-UA)

Un protocolo de machine-to-machine comunicación (M2M) para la automatización industrial. OPC-UA establece un estándar de interoperabilidad con esquemas de autenticación, autorización y cifrado 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 más información, consulte [Operational Readiness Reviews \(ORR\)](#) en el Marco de AWS Well-Architected.

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 para todos los miembros 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 AWS KMS (SSE-KMS) y las solicitudes dinámicas PUT y DELETE dirigidas 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 AWS de referencia de seguridad](#) recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la 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

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno o más VPCs. 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 la sección 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 Regions 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)

Política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPs defina barreras o establezca límites a las acciones que un administrador puede delegar en usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados para especificar qué servicios o acciones están permitidos o prohibidos. Para obtener más información, consulte [las políticas de control de servicios](#) 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](#).

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](#).

split-and-seed modelo

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 dismantelar 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 con la aplicación de 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

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS 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.

puerta de enlace de tránsito

Un centro de tránsito de red que puede usar para interconectar sus redes con VPCs las locales. 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. Para más información, consulte la guía [Cuantificación de la incertidumbre en los sistemas de aprendizaje profundo](#).

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

Una conexión entre dos VPCs que le 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.