



Migración de servidores locales a redes AWS privadas mediante AWS Application Migration Service

# AWS Guía prescriptiva



# AWS Guía prescriptiva: Migración de servidores locales a redes AWS privadas mediante AWS Application Migration Service

Copyright © 2024 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
Escenarios .....	2
Replicación únicamente a través de redes privadas .....	2
Recursos públicos de salida HTTPS en la fuente y del área de almacenamiento privada .....	4
Recursos públicos de salida HTTPS en la fuente y del área de almacenamiento pública .....	5
Componentes y requisitos de arquitectura para la replicación restringida .....	7
Subred provisional .....	7
subred de origen .....	8
subred de destino .....	8
Prácticas recomendadas de la gateway .....	10
Configuraciones de enrutamiento y subredes .....	10
Configuración de enlace de la VPC de gateway .....	11
Puntos de enlace de interfaz de VPC .....	12
VPC enlace de la gateway .....	13
Terminales entrantes del solucionador de DNS .....	14
Grupos de enlace de interfaz de red elástica .....	14
Instalación del agente del servicio de migración de aplicaciones en los servidores de origen .....	15
Implementación del entorno PoC .....	17
Despliegue manual .....	17
Automatización de las implementaciones de agentes .....	19
Supervisión y problemas de problemas de problemas .....	21
Probar la conectividad y la resolución de nombres desde el servidor de origen .....	21
Probar la conectividad y la resolución de nombres desde la red de área de ensayo .....	22
Conclusión .....	24
Recursos .....	25
Historial de documentos .....	26
Glosario .....	27
# .....	27
A .....	28
B .....	31
C .....	33
D .....	36
E .....	41
F .....	43

---

G .....	44
H .....	45
I .....	46
L .....	49
M .....	50
O .....	54
P .....	57
Q .....	60
R .....	60
S .....	63
T .....	67
U .....	68
V .....	69
W .....	69
Z .....	71
.....	lxxii

# Migración de servidores locales a redes AWS privadas mediante el uso de AWS Application Migration Service

Mike Kuznetsov y Dipin Jain, Amazon Web Services (AWS)

Marzo de 2023 ([historial del documento](#))

Muchas empresas migran a entornos AWS de red aislados o semiaislados, como centros de datos locales u otras infraestructuras híbridas o en la nube. Estas redes aisladas normalmente no permiten ningún tráfico de salida a puntos finales externos, lo cual es necesario para la migración a través de la red. Otras empresas permiten el tráfico de salida HTTPS desde sus redes internas, pero no permiten las comunicaciones específicas en [los puertos de red](#) requeridos por [AWS Application Migration Service](#), que es el principal Servicio de AWS para [lift-and-shift las migraciones de gran tamaño](#). En un tercer escenario, se permite el tráfico HTTPS desde las áreas de origen y de ensayo, pero el tráfico de replicación de datos debe pasar por el canal privado por motivos de cumplimiento.

El Servicio de migración de aplicaciones [admite estos casos de uso](#) y le permite migrar desde entornos aislados y seguros utilizando únicamente conectividad de red privada o híbrida privada/pública. Esta guía describe estos tres escenarios, que van desde los dos modelos híbridos público/privado hasta el completamente aislado, y se centra en los pasos detallados y los requisitos de infraestructura para la opción más restrictiva y exclusiva para uso privado. Se basa en el patrón de orientación AWS prescriptiva [Connect a los planos de datos y control del servicio de migración de aplicaciones a través de una red privada](#) y proporciona:

- Detalles adicionales sobre la conectividad requerida en cada escenario
- Explicaciones de AWS los recursos que deben crearse
- Opciones de automatización para crear la infraestructura de pruebas AWS e implementarla durante la fase de migración
- Opciones para monitorear y solucionar problemas de conectividad para cada caso de uso

Para obtener más información sobre el funcionamiento del servicio de migración de aplicaciones, consulte estas publicaciones de blog.

- [Acelere su migración con AWS Application Migration Service](#)
- [Cómo utilizar lo nuevo AWS Application Migration Service para migraciones de Lift and Shift](#)

# Escenarios

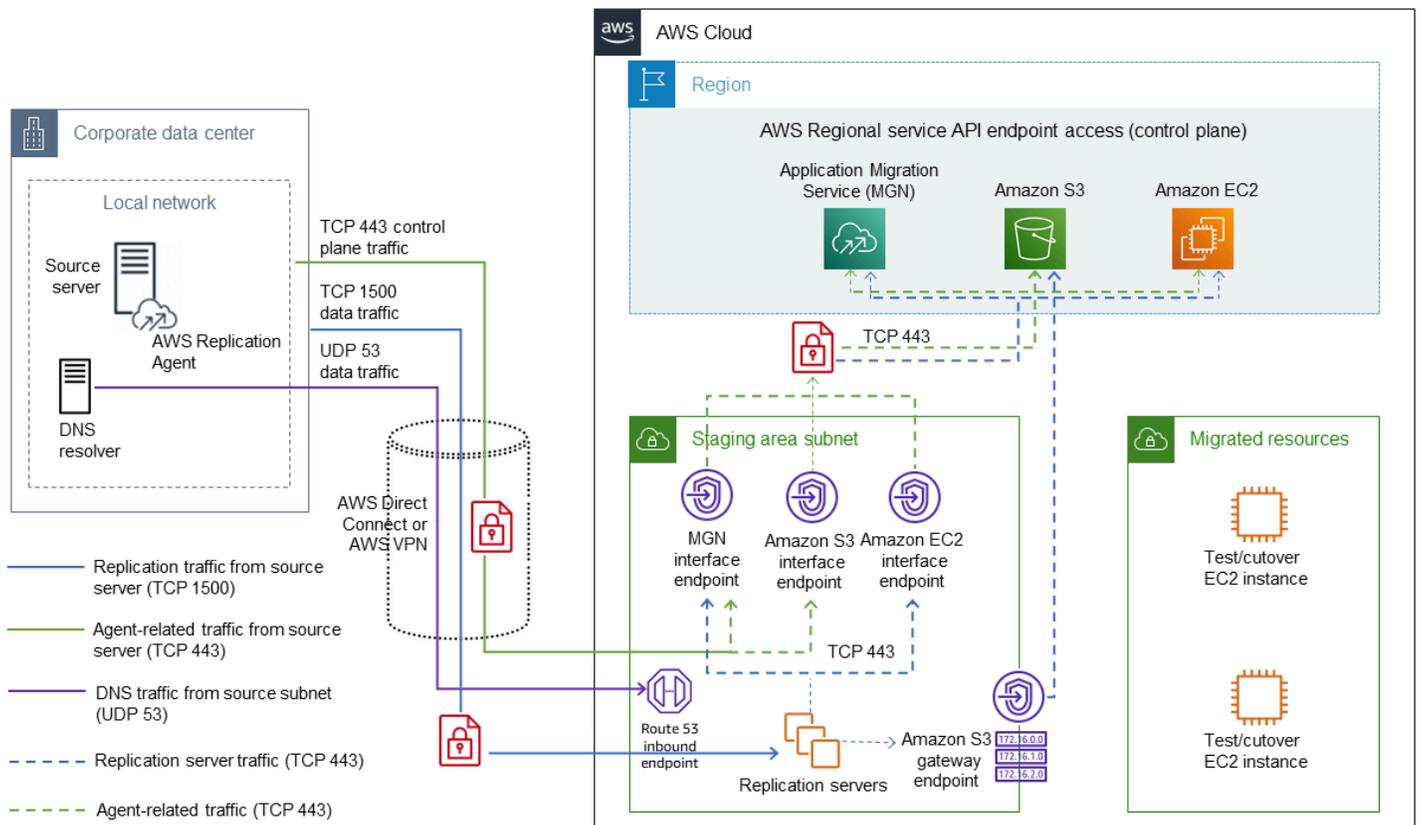
Esta guía describe los componentes de infraestructura necesarios que se deben crear para completar la migración en los siguientes escenarios:

- [Replicación únicamente a través de redes privadas](#), que es el escenario más común y restrictivo.
- Escenario híbrido en el que se permite la comunicación de salida mediante HTTPS pero se restringe el resto del tráfico. Este escenario consta de dos opciones:
  - [Recursos públicos de salida HTTPS en la fuente y del área de almacenamiento privada](#)
  - [Recursos públicos de salida HTTPS en la fuente y del área de almacenamiento pública](#)

Para cada escenario, la guía proporciona un ejemplo de configuración y la lista completa de AWS los componentes necesarios.

## Replicación únicamente a través de redes privadas

El siguiente diagrama muestra la arquitectura del escenario más restrictivo, en el que todo el tráfico pasa por el canal privado (AWS VPNoAWS Direct Connect) entre el entorno de origen y AWS.



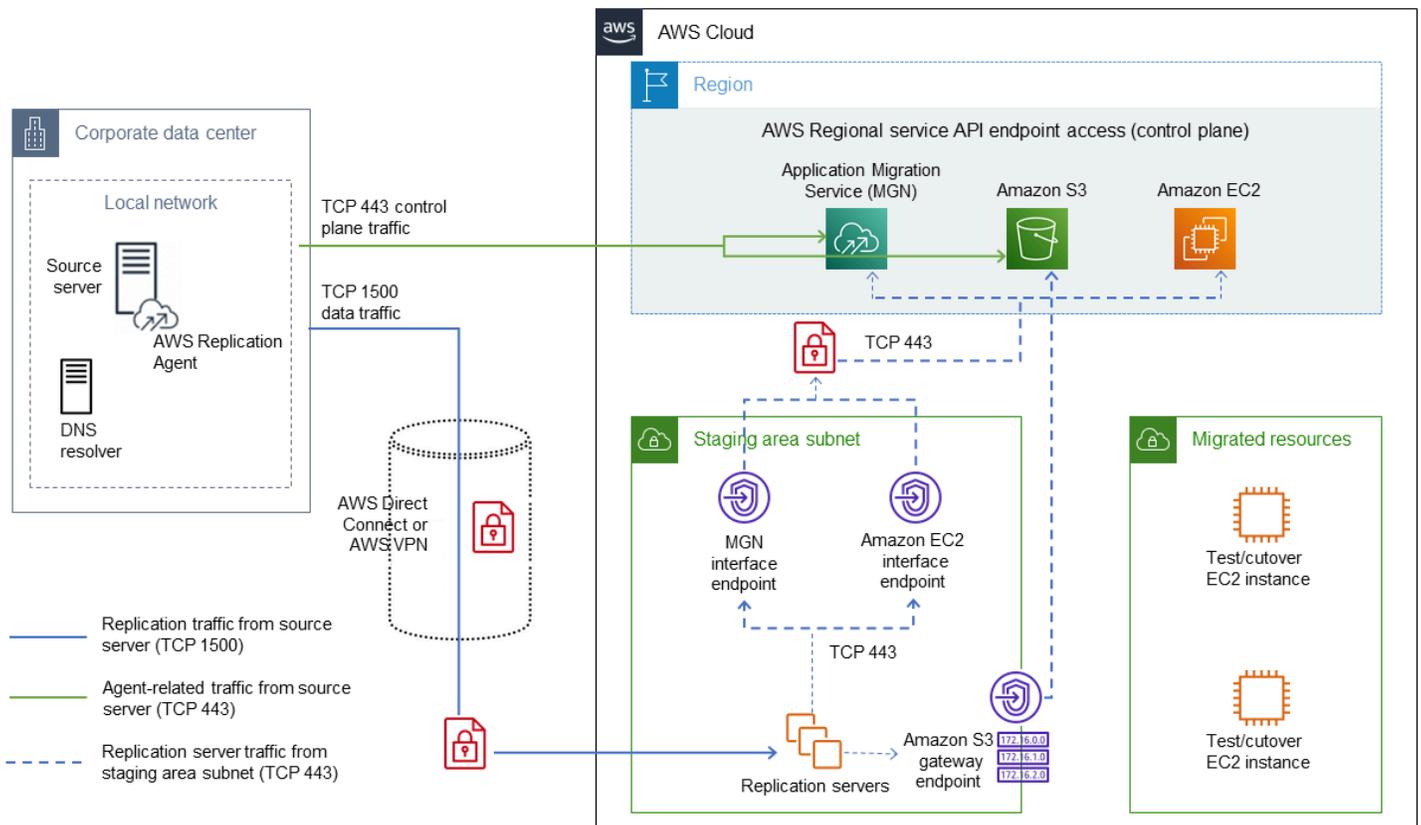
Los principales componentes de esta arquitectura son:

- Entorno de origen en el centro de datos corporativo (a la izquierda). Este es el entorno desde el que hay que migrar.
- Entorno de ensayo AWS con nube privada virtual privada (VPC) y subred (en el centro). Este es el entorno que utilizará el Servicio de migración de aplicaciones para crear recursos relacionados con la replicación. Estos recursos pueden incluir servidores de replicación, servidores de conversión y volúmenes relacionados de Amazon Elastic Block Store (Amazon EBS) y sus instantáneas de Amazon Simple Storage Service (Amazon S3).
- Conexión VPN desde el entorno de origen a la VPC provisional y a las subredes para gestionar tres tipos de tráfico:
  - Puerto HTTPS/TCP 443 para comunicación de API
  - Puerto TCP 1500 para transferencia de datos
  - tráfico del sistema de nombres de dominio (DNS)

- Entorno objetivo enAWS (a la derecha). Puede ser una VPC completamente aislada o una subred en el entorno de ensayo. (Nota: No hay ningún requisito de conectividad de red desde la subred del entorno de ensayo hasta las subredes de destino).
- Puntos de enlace de la interfaz Amazon VPC para Application Migration Service, Amazon Elastic Compute Cloud (Amazon EC2) y Amazon S3 creados en el entorno de ensayo, y un punto final de puerta de enlace de VPC de Amazon S3 al que se puede acceder desde la subred provisional.
- Y, por último, el [punto final entrante del solucionador de DNS](#) en la subred provisional. Esto es necesario para que los sistemas de origen puedan convertir los nombres de dominio completos (FQDN) de los puntos finales de la VPC en IP privadas.

## Recursos públicos de salida HTTPS en la fuente y del área de almacenamiento privada

El siguiente diagrama ilustra la arquitectura en el escenario híbrido, en el que se permite el tráfico de salida HTTPS desde cualquier servidor de origen y se utiliza para comunicarse con los puntos finales del Servicio de Migración de Aplicaciones y Amazon S3, mientras que los datos de replicación del puerto TCP 1500 pasan por el canal privado (AWS VPNoAWS Direct Connect) entre el entorno de origen yAWS.

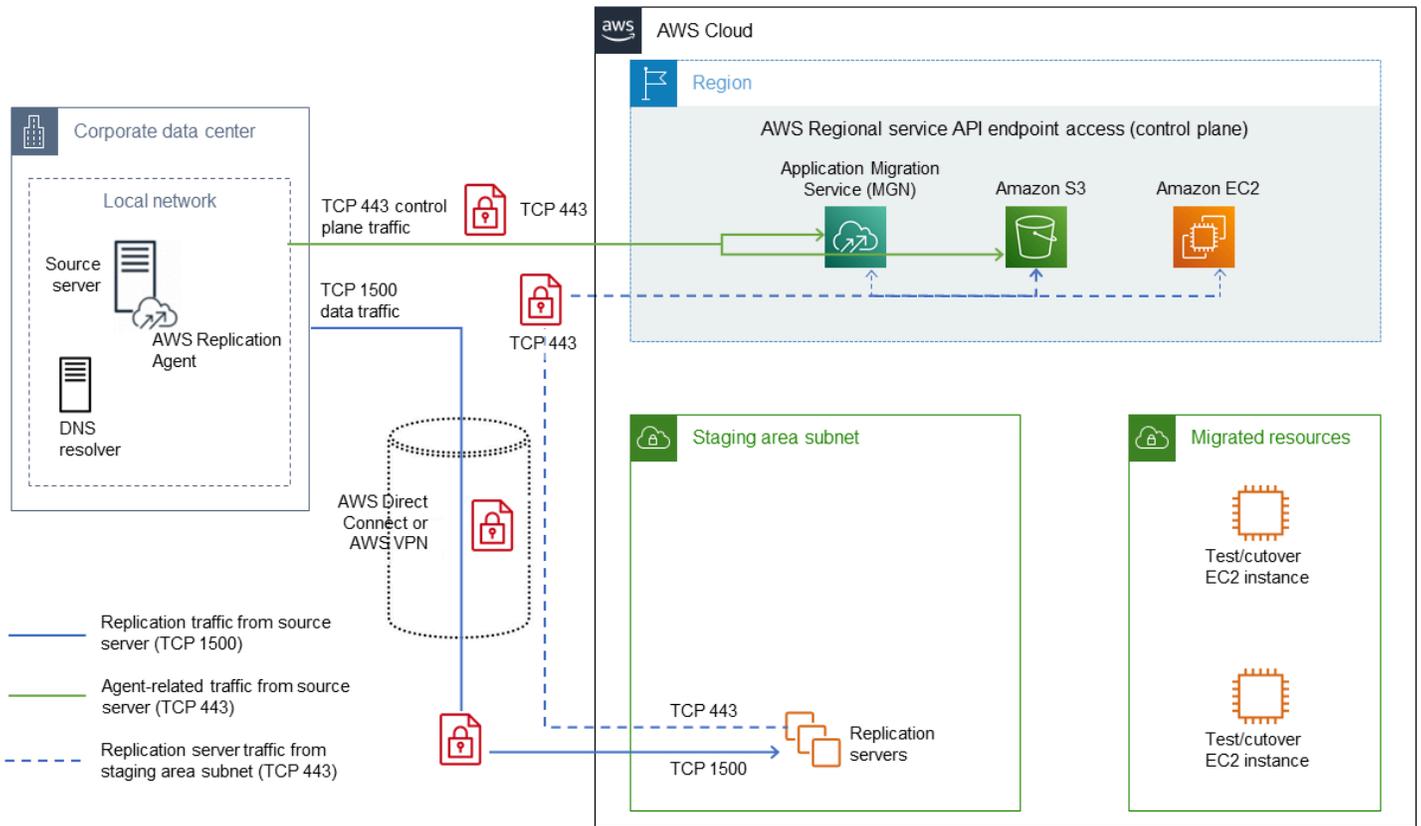


Esta arquitectura simplifica los requisitos de la subred del área de ensayo, ya que las comunicaciones HTTPS de los agentes no viajan a través del canal privado. Además, no es necesario crear puntos finales de VPC de la interfaz Amazon S3 o puntos de resolución de entrada de Amazon Route 53 adicionales para el tráfico de DNS, ya que los servidores de origen utilizarán sus servidores DNS tradicionales para resolver los nombres DNS públicos y estándar de Application Migration Service y los puntos de enlace de Amazon S3.

Sin embargo, en este escenario, los recursos de la subred del área de ensayo siguen ejecutándose en una red privada y completamente aislada y no tienen acceso público a ningún extremo de HTTPS, por lo que necesitan crear puntos finales de interfaz Amazon EC2 y del servicio de migración de aplicaciones, así como un punto final de Amazon S3 gateway.

## Recursos públicos de salida HTTPS en la fuente y del área de almacenamiento pública

En los casos en los que no sea necesario que los recursos del área de ensayo estén en una subred completamente aislada, puede utilizar la alternativa híbrida que se muestra en el siguiente diagrama.



En este escenario, solo el tráfico de replicación de datos en el puerto TCP 1500 pasa por el canal privado. El resto de la comunicación, tanto de la subred de origen como de la subred provisional, se realiza a través de la red pública y se dirige a los extremos HTTPS públicos estándar.

# Componentes y requisitos de arquitectura para la replicación restringida

Esta sección proporciona una descripción detallada del escenario más restrictivo, en el que toda la comunicación se produce únicamente a través del canal privado, e incluye una explicación detallada de los requisitos y los componentes correspondientes que se crearán para cada área.

## Subred provisional

La [subred provisional](#) es la parte más importante de la infraestructura de replicación. Aquí es donde se lanzarán todos los [servidores de replicación](#) del Servicio de migración de aplicaciones y contiene las direcciones IP a las que se dirigirá el tráfico de replicación. Para la replicación de datos privados entrantes, configure los [parámetros del servidor de replicación](#) para el Servicio de migración de aplicaciones con la [opción Usar IP privada](#).

Para [los requisitos de salida](#), puede utilizar la opción [Crear IP pública](#) para elegir si los servidores de replicación se comunicarán con AWS los servicios necesarios (Amazon S3, Application Migration Service, Amazon EC2) a través de una IP privada o pública. Las opciones estándar para proporcionar conectividad a Internet saliente se enumeran en la [documentación del Servicio de migración de aplicaciones](#): una dirección IP pública con una puerta de enlace a Internet o una dirección IP privada con una puerta de enlace NAT. Ambas opciones permiten implementar un escenario híbrido simplificado en el que el tráfico de replicación de datos pasa por una conexión privada (AWS VPNoAWS Direct Connect) mientras los servidores de replicación se comunican con AWS los servicios a través de la red pública.

Sin embargo, tener conectividad pública de salida suele estar prohibido en entornos corporativos cerrados, y este es el escenario más restrictivo que se analiza en la siguiente sección. En este caso, utilice AWS PrivateLink y configure los siguientes extremos de VPC al organizar subredes para los servidores de replicación:

- Punto de enlace de la VPC para comunicarse con Amazon S3
- Terminales de interfaz de VPC para comunicarse con Application Migration Service y Amazon EC2

Para obtener más información acerca de los puntos de enlace de la VPC, consulte la [AWS PrivateLink](#) documentación de.

## subred de origen

La subred de origen es cualquier subred desde la que se esté replicando. Aquí es donde se encuentran los [servidores de origen](#) y donde instalará el Agente de AWS Replicación en estos servidores. Los [requisitos de red](#) para un agente incluyen:

- Comunicación a través del puerto HTTPS/TCP 443 con Servicios de AWS Amazon S3 y Application Migration Service
- Comunicación con la dirección IP del servidor de replicación (privada o pública, según su configuración)

El agente también admite escenarios híbridos en los que la comunicación con Servicios de AWS puede realizarse a través de la red pública (mediante tráfico HTTPS estándar) mientras que los datos de replicación se envían a través de redes privadas a la IP privada del servidor de replicación.

Esta guía se centra en un escenario más restrictivo en el que ni Servicios de AWS siquiera se permite el tráfico HTTPS desde los sistemas de origen, por lo que los siguientes puntos finales se configuran en la subred provisional:

- Terminales de interfaz de VPC para Application Migration Service y Amazon S3 (punto final de interfaz regional, no el punto final de puerta de enlace que se requiere para los servidores de replicación)
- Un [punto final de resolución de DNS entrante](#), que permite que las fuentes locales y los servidores DNS resuelvan las direcciones IP privadas de los puntos finales de la VPC, ubicados en la subred provisional

## subred de destino

La subred de destino es cualquier subred en la que planea lanzar sus servidores, incluidas las instancias de prueba y de transición. Estas subredes no requieren conectividad de red en absoluto y podrían estar ubicadas en cualquier otra VPC de la misma Cuenta de AWS región. Esto se debe a que Application Migration Service utiliza las API de Amazon EC2 para crear nuevas instancias de prueba o transición (razón por la cual los servidores de replicación de la subred provisional requieren conectividad HTTPS de salida con Amazon EC2) y accede a las instantáneas regionales de S3 creadas a partir de volúmenes de EBS replicados. Ninguna de estas operaciones requiere acceso

---

directo a la red hacia o desde la subred de destino, por lo que podría tratarse incluso de una subred privada completamente aislada.

Sin embargo, el Servicio de migración de aplicaciones también [instala automáticamente](#) varias herramientas, como EC2Config o AWS Systems Manager Agents (agentes SSM), en las instancias de destino, y estas actividades requieren la conectividad del puerto HTTPS/TCP 443 de salida desde las instancias y subredes de destino.

## Prácticas recomendadas de la gateway

Esta sección proporciona una descripción detallada del escenario más restrictivo, en el que toda la comunicación se produce únicamente a través del canal privado, e incluye una explicación detallada de los requisitos y los componentes correspondientes que se crearán para cada área.

En esta sección se describe la configuración para el escenario más restrictivo (replicación únicamente en redes privadas), tal como se muestra en el [primer diagrama](#), basándose en las consideraciones expuestas anteriormente. Puede configurar ambos escenarios híbridos omitiendo partes de la configuración más restrictiva:

- Para el escenario híbrido que admite la salida pública de HTTPS en los recursos del área de ensayo de origen y privada, no se requiere el punto final de VPC de la interfaz Amazon S3.
- Para el escenario híbrido que admite la salida pública de HTTPS en los recursos del área de ensayo pública y de origen, no se requieren puntos finales de VPC en la subred del área de ensayo.

En las siguientes secciones se parte del supuesto de que la configuración inicial del Servicio de migración de aplicaciones ya está completa, tal como se describe en las entradas del blog ([Acelere la migración con AWS Application Migration Service y cómo utilizar lo nuevo AWS Application Migration Service para migraciones de Lift-and-Shift](#)). Este análisis se centra en los componentes que son específicos del escenario restrictivo y asume que se trata de una subred provisional privada que no tiene conectividad a Internet.

## Configuraciones de enrutamiento y subredes

Para el escenario restrictivo, configura los AWS recursos necesarios en la subred privada de una VPC provisional. Esta subred no tiene conectividad a Internet (no hay ninguna puerta de enlace de Internet conectada a la tabla de enrutamiento como ruta predeterminada). En cambio, utiliza una puerta de enlace virtual asociada a una [AWS Site-to-Site VPN](#) puerta de enlace (conectada a través de un túnel IPsec a una puerta de enlace local) o está conectada a una puerta de enlace de transferencia o a AWS Direct Connect servicios para proporcionar interconectividad privada a los centros de datos locales.

Utilizará esa subred privada como subred provisional para los recursos relacionados con la replicación gestionados por el Servicio de migración de aplicaciones y configurará todo el acceso a la

red necesario a través de esta subred mediante puntos de conexión de VPC, como se explica en la siguiente sección.

## Configuración de enlace de la VPC de gateway

Ahora debe crear puntos de conexión de VPC en la subred provisional para proporcionar conectividad a los servidores de replicación y a los agentes del servicio de migración de aplicaciones desde las subredes locales.

Aquí tienes una lista completa de los puntos de conexión de VPC que necesitas:

- Los puntos finales de interfaz de Amazon EC2 y Application Migration Service proporcionan sus propias interfaces de red elásticas con direcciones IP privadas y nombres DNS privados para que los utilicen tanto los servidores de replicación como los agentes. (Los agentes usarán únicamente el punto final del Servicio de migración de aplicaciones).
- Punto final de Amazon S3 Gateway que proporciona una ruta específica en la tabla de rutas de subred (a través de una lista de prefijos). Esto lo utilizarán los servidores de replicación.
- Punto final de interfaz Amazon S3 que proporciona una elastic network interface específica con una dirección IP privada dedicada en la subred privada. Los agentes del servicio de migración de aplicaciones utilizarán esta dirección a través de un nombre DNS específico.

En las siguientes secciones se ofrece información más detallada sobre el funcionamiento de los puntos de conexión de VPC. La siguiente tabla muestra todos los extremos creados para la subred privada provisional. (Tenga en cuenta que el punto final de Amazon S3 Gateway no tiene aprovisionadas interfaces de red, pero sí listas de prefijos específicas aprovisionadas en la tabla de rutas de la subred, como se describirá más adelante en esta guía).

Servicio de AWS	VPC endpoint type	Private DNS	Related subnet
Amazon EC2	Interfaz	Habilitado	Intersubnet subnet subnet subnet subnet
Servicio de migración de aplicaciones de gateway	Interfaz	Habilitado	Intersubnet subnet subnet subnet subnet

Servicio de AWS	VPC endpoint type	Private DNS	Related subnet
Amazon S3	Interfaz	No disponible	Intersubnet subnet subnet subnet subnet
Amazon S3	Puerta de enlace	No disponible	Connect a la tabla de enrutamiento de la subred privada provisional

Puede crear puntos de enlace de VPC opcionales para permitir el acceso a las instancias de EC2 en subredes privadas aisladas mediante AWS Systems Manager, como se explica en [Creación de puntos de enlace de VPC](#) en la documentación de Systems Manager.

Servicio de AWS	VPC endpoint type	Private DNS	Related subnet
Systems Manager	Interfaz	Habilitado	Intersubnet subnet subnet subnet subnet
mensajes ssm de gateway	Interfaz	Habilitado	Intersubnet subnet subnet subnet subnet
mensajes de la gateway	Interfaz	Habilitado	Intersubnet subnet subnet subnet subnet
AWS Key Management Service (AWS KMS)	Interfaz	Habilitado	Intersubnet subnet subnet subnet subnet
Logs (Registros)	Interfaz	Habilitado	Intersubnet subnet subnet subnet subnet

## Puntos de enlace de interfaz de VPC

Al crear un extremo de interfaz también se crea una elastic network interface específica para cada subred para la que se aprovisiona el punto final de la interfaz determinado. Por ejemplo, el extremo de la interfaz del Servicio de migración de aplicaciones se aprovisiona en una subred privada de la

VPC provisional con una elastic network interface que está asociada a la dirección IP de esa subred y también tiene tres nombres DNS que se pueden resolver desde la subred a esta dirección IP:

- Private de enlace de DNS `subnet,mgn.<region>.amazonaws.com`
- Dos nombres de DNS que se basan en el ID del punto de enlace (`vpce-xxx`), con y sin la región incluida en el nombre: `vpce-xxx-<region>.<service-name>` y `vpce-xxx.<service-name>`

Esto permite que cualquier instancia que se ejecute en la subred que utilice la configuración predeterminada del [conjunto de opciones del Protocolo de configuración dinámica de host \(DHCP\)](#) en la VPC, que tenga ambos [atributos de DNS](#) `enableDnsHostnames` y `enableDnsSupport` esté habilitada, pueda:

- Resuelva el nombre DNS del Servicio de migración de aplicaciones (`mgn.<region>.amazonaws.com`) a una dirección IP privada asignada a la elastic network interface.
- Connect al Servicio de migración de aplicaciones únicamente mediante la red local.

Esto corrige la conectividad de cualquier instancia que se ejecute en la subred provisional (como el servidor de replicación o el servidor de conversión del Servicio de migración de aplicaciones) de cualquier instancia Servicio de AWS que tenga aprovisionados puntos de enlace de interfaz en la subred (como Amazon EC2, Application Migration Service AWS KMS, Systems Manager, etc.).

## VPC enlace de la gateway

Para servicios como Amazon S3, no se puede aprovisionar ningún nombre DNS fijo porque cada bucket tiene su propio nombre DNS. Para este escenario, utilizará puntos finales de puerta de enlace de VPC.

Al crear un punto final de puerta de enlace de Amazon S3, también se crea un objeto de lista de prefijos específico con una lista de destinos de subred (en notación CIDR), que se puede añadir a la tabla de rutas de subred. Por lo tanto, los nombres DNS de los buckets de S3 resueltos a las direcciones IP incluidas en esta lista estarían accesibles a través de la conectividad interna.

Al aprovisionar un punto final de Amazon S3 Gateway, puede especificar las subredes en las tablas de rutas que deben incluir ese ID de lista de prefijos (`PL-<id>`). La tabla de enrutamiento resultante para la subred privada provisional debe incluir ese ID de lista de prefijos, como en este ejemplo de tabla de enrutamiento:

Destination	Target
<code>p1-&lt;id&gt;</code>	<code>vpce-&lt;id-of-S3-Gateway-VPC-endpoint&gt;</code>
Cualquier otra ruta (por ejemplo, los CIDR de la subred de origen)	Cualquier objetivo, como los ID de puerta de enlace virtual
CIDR de la gateway	<code>"local"</code>

## Terminales entrantes del solucionador de DNS

La configuración descrita en la sección anterior es suficiente para las instancias que se ejecutan dentro de las AWS subredes, porque ya están configuradas para usar servidores DNS internos de Amazon Route 53. Sin embargo, los servidores de origen locales requieren pasos adicionales para poder comunicarse de Servicios de AWS forma privada. En particular, el agente del servicio de migración de aplicaciones debe descargar el instalador de Amazon S3 y, a continuación, comunicarse con el servicio de migración de aplicaciones mediante los nombres DNS que se proporcionan en la [documentación](#). Los servidores locales utilizan sus servidores DNS predeterminados para resolver estos nombres DNS, lo que da como resultado direcciones IP públicas. Los firewalls corporativos eventualmente bloquean las comunicaciones con estas direcciones a través del puerto HTTPS/TCP 443.

Para evitarlo, debe configurar los servidores de origen o sus servidores DNS predeterminados [Amazon Route 53 Resolver](#) para usarlos en la resolución de estos nombres DNS específicos o de una zona de subdominio (es decir, la `*.<region>.amazonaws.com` zona completa). Esto se puede configurar creando un [punto final de entrada de Route 53 Resolver](#) que, como un extremo de la interfaz de VPC, tenga una elastic network interface dedicada creada en la subred privada dedicada y AWS, por lo tanto, a la que pueda reenviar solicitudes de DNS Amazon Route 53 Resolver.

## Grupos de enlace de interfaz de red elástica

Cada elastic network interface tiene un grupo de seguridad dedicado asociado, que debe permitir el tráfico esperado para esta elastic network interface y el punto final correspondiente. Por lo tanto, el grupo de seguridad del punto final de la resolución de DNS debe permitir el puerto UDP 53 de entrada (y, a veces, el puerto TCP 53) para las solicitudes de DNS, y los grupos de seguridad de

puntos finales de la mayoría de los demás servicios (Application Migration Service, Amazon EC2, Systems Manager, etc.) necesitan habilitar el puerto HTTPS/TCP de entrada 443.

## Instalación del agente del servicio de migración de aplicaciones en los servidores de origen

Para instalar el agente del servicio de migración de aplicaciones en los servidores de origen, debe proporcionar los nombres DNS de los extremos del servicio de migración de aplicaciones y los puntos finales de la interfaz Amazon S3 a los parámetros de la línea de comandos del agente (consulte [Instalación del agente en una red segura](#) en la documentación del servicio de migración de aplicaciones).

Para el extremo del Servicio de migración de aplicaciones, puede usar cualquiera de los nombres DNS asociados a él (un campo DNS privado (`mgn.<region>.amazonaws.com`) o un nombre DNS específico de VPC (`vpce-<VPC-id>-<suffix>.mgn.<region>.vpce.amazonaws.com`) y proporcionar un argumento: `--endpoint <FQDN>`. De hecho, si omite este argumento, el agente usa el especificado Región de AWS para reconstruir el FQDN DNS predeterminado (`mgn.<region>.amazonaws.com`) y usa el FQDN para acceder al plano de control del Servicio de migración de aplicaciones. En la mayoría de los casos, ese comportamiento predeterminado debería bastar, siempre y cuando el FQDN se resuelva correctamente desde el servidor de origen a la dirección IP privada de la elastic network interface del punto final de VPC del Servicio de migración de aplicaciones creado en la subred provisional.

El extremo de la interfaz de Amazon S3 no tendrá un solo nombre DNS privado (porque cada bucket de S3 tendrá el suyo propio), por lo que no se admite esa opción. Sin embargo, un extremo de la interfaz de Amazon S3 todavía tiene una elastic network interface asociada. También tiene una IP privada específica y nombres DNS comodín (en formato `.vpce-<VPC-ID>-<suffix>.s3.<region>.vpce.amazonaws.com` o región específicos). `vpce-<VPC-ID>-<suffix>-<region>.s3.<region>.vpce.amazonaws.com`) que se pueden resolver en esta IP privada.

Ese nombre DNS comodín se puede utilizar para el `--s3-endpoint` argumento, de la siguiente manera:

```
aws-replication-installer-init.py --region <region> --aws-access-key-id  
<MGN_IAM_ACCESS_KEY> --aws-secret-access-key <MGN_IAM_SECRET> --no-prompt \
```

```
--endpoint vpce-<VPC-id>-<suffix>.mgn.<region>.vpce.amazonaws.com --s3-endpoint  
vpce-<VPC-ID>-<suffix>-<region>.s3.<region>.vpce.amazonaws.com
```

La siguiente sección proporciona un ejemplo de cómo configurar el Servicio de migración de aplicaciones, incluidos todos los puntos de enlace de VPC necesarios, e implementar los agentes mediante puntos de enlace de VPC en los servidores de origen de Windows y Linux. La sección abarca tanto la implementación manual como la automatizada.

# Implementación del entorno PoC

Muchos usuarios prefieren probar minuciosamente todos los canales de comunicación y los pasos de migración con antelación. Probar la migración desde redes aisladas podría ser un desafío. Para abordar esa necesidad, AWS ofrece dos opciones:

- Una [CloudFormation plantilla](#) en la que se preparan todos los recursos necesarios AWS. La plantilla crea un entorno de prueba de concepto (PoC) que emula los componentes del entorno del centro de datos y configura la AWS infraestructura. Incluye VPC de origen y destino aisladas, subredes y puntos de conexión de VPC.
- Un taller específico ([Migra de forma Well-Architected](#)) con step-by-step instrucciones detalladas para crear tu entorno de prueba (consulta el paso [Crear puntos de conexión de VPC](#)).

Como alternativa, puede implementar su entorno de PoC siguiendo los pasos de las siguientes secciones.

## Despliegue manual

La siguiente lista describe los pasos principales para las implementaciones manuales en su entorno. Para obtener más información, consulte el patrón de orientación AWS prescriptiva [Connect a los planos de datos y control del Servicio de migración de aplicaciones a través de una red privada](#).

1. Cree las VPC de subredes privadas.
2. Cree los siguientes extremos de VPC en la subred del área de ensayo:
  - Servicio de migración de aplicaciones y habilite el nombre DNS privado (compartido por el servidor de replicación y el servidor de origen).
  - Amazon EC2 y habilite el nombre DNS privado (compartido por el servidor de replicación y el servidor de origen).
  - Amazon S3 (no se admite el nombre DNS privado). Los puntos finales de la interfaz son compatibles con Direct Connect y el emparejamiento de VPC. AWS VPN Por lo tanto, esto solo es necesario para que los servidores de origen (y pueden estar ubicados en las instalaciones) se conecten al plano de control del Servicio de migración de aplicaciones a través de una red privada.

**Note**

Los extremos de ssm y ssmmessages son opcionales y actualmente se crean para conectar el servidor de origen a través del administrador de sesiones SSM.

- Amazon S3 enlace de búfer de la subredes de subredes. El servidor de replicación lo requiere para conectarse a Amazon S3. Debe actualizar las rutas de la subred del área de ensayo.
3. Cree un punto final de resolución entrante en la VPC del área de ensayo para permitir la resolución del registro DNS privado (para los extremos de la interfaz de VPC) desde la VPC de origen.
  4. Actualice las opciones de DHCP de la VPC de origen con el extremo de resolución entrante de la VPC del área de ensayo como IP del servidor DNS.
  5. Habilite el intercambio entre las VPC de origen y de almacenamiento y actualice ambas tablas de enrutamiento de VPC.
  6. Cree un grupo de seguridad en las VPC de origen y de almacenamiento para permitir los siguientes puertos.

Source	Destination	Port	Description
Centro de datos de origen	URL de servicios Amazon S3	443 (TCP)	<a href="#">Comunicación a través del puerto TCP 443</a>
Centro de datos de origen	La dirección de consolaRegión de AWS específica del Servicio de migración de aplicaciones	443 (TCP)	<a href="#">Comunicación entre los servidores de origen y el Servicio de migración de aplicaciones a través del puerto TCP 443</a>
Centro de datos de origen	subredes de áreas de búfer	1500 (TCP)	<a href="#">Comunicación entre los servidores de origen y la subred del área de ensayo</a>

Source	Destination	Port	Description
			<a href="#">a través del puerto TCP 1500</a>
Subred del área de ensayo	La dirección de consolaRegión de AWS específica del Servicio de migración de aplicaciones	443 (TCP)	<a href="#">Comunicación entre la subred del área de ensayo y el Servicio de migración de aplicaciones a través del puerto TCP 443</a>
Subred del área de ensayo	URL de servicios Amazon S3	443 (TCP)	<a href="#">Comunicación a través del puerto TCP 443</a>
Subred del área de ensayo	Punto de conexión Amazon EC2 de suRegión de AWS	443 (TCP)	<a href="#">Comunicación a través del puerto TCP 443</a>

7. Inicialice el servicio de migración de aplicaciones en el área de ensayoRegión de AWS actualizando los detalles de la subred del área de ensayo y habilitando la comunicación a través de IP privada.
8. Cree un rolAWS Identity and Access Management (IAM) para instalar el agente del servicio de migración de aplicaciones. Adjunte políticas gestionadas y genere claves de acceso y una clave secreta.
9. Cree un perfil de IAM para conectar Amazon EC2 a través del administrador de sesiones SSM.
- 10Instale un agente en las máquinas de origen.

## Automatizar las implementaciones de agentes con Cloud Migration Factory

[Cloud Migration Factory onAWS](#) automatiza la implementación del agente del servicio de migración de aplicaciones para el escenario de redes privadas, con parámetros de línea de comandos adicionales. Al implementar esta solución (consulte las opciones de [implementación automática](#)), puede usar estos scripts y una de las siguientes opciones:

- Ejecuta estos [scripts](#) de forma manual desde la línea de comandos, tal y como se describe en la sección [Ejecutar automatizaciones desde la línea de comandos](#) de la [Guía de implementación de Cloud Migration Factory](#)
- Agregue los [scripts](#) a Migration Factory siguiendo las instrucciones de la sección [Administración de scripts](#) para lograr una integración completa con Cloud Migration Factory

Estos scripts automatizan lo siguiente:

- Instalación del agente de servicio de migración de aplicaciones en un servidor Windows mediante puntos finales privados
- Instalación del agente de servicio de migración de aplicaciones en servidores Linux mediante puntos finales privados

# Supervisión y problemas de problemas de problemas

Puede supervisar el Servicio de migración de aplicaciones mediante [Amazon CloudWatch](#), [Amazon](#) y EventBridge [AWS CloudTrail](#), que recopilan datos sin procesar y los procesan para convertirlos en near-real-time métricas legibles. Para obtener más información, consulte [Monitorear el servicio de migración de aplicaciones](#) en laAWS documentación.

Si encuentras algún problema y quieres lanzar nuevas instancias de prueba o transición, puedes revertir la acción de prueba o transición. Esto revertirá el estado del ciclo de vida de los servidores de origen a la etapa anterior, lo que indicará que estos servidores no se han sometido a una transición. Durante una reversión, también tendrá la opción de eliminar las instancias de prueba o de transición para ahorrar costes. Para obtener más información, consulte [Solución problemas en la documentación del servicio de problemas de problemas de problemas](#) en la documentación del servicio de problemas.

Cuando se haya instalado el agente, el servidor de origen aparece en la consola del Servicio de migración de aplicaciones y puede ver los detalles del servidor para comprobar el progreso de la replicación.

## Probar la conectividad y la resolución de nombres desde el servidor de origen

Inicie sesión en el servidor de origen mediante el protocolo de escritorio remoto de Windows (RDP), Secure Shell (SSH) o el Administrador deAWS sesiones y pruebe lo siguiente:

- Conectividad a través de HTTPS en el puerto TCP 443 con el extremo del servicio de migración de aplicaciones.

- En Windows (en PowerShell):

```
Test-NetConnection -ComputerName mgn.<aws_region>.amazonaws.com -Port 443
```

- En Linux o Windows (cmd):

```
Telnet mgn.<aws_region>.amazonaws.com 443
```

- Conectividad a través de HTTPS en el puerto TCP 443 con el endpoint de Amazon S3.

- En Windows (en PowerShell):

```
Test-NetConnection -ComputerName <s3_endpoint_name> -Port 443
```

- En Linux o Windows (cmd):

```
Telnet <s3_endpoint_name> 443
```

- Conectividad en el puerto TCP 1500 con la IP del servidor de replicación:

- En Windows (en PowerShell):

```
Test-NetConnection -ComputerName <Replication_Server_Private_IP> -Port 1500
```

- En Linux o Windows (cmd):

```
Telnet <Replication_Server_Private_IP> 1500
```

Además, asegúrese de que los extremos de la API de Amazon EC2 y Application Migration Service se dirijan a IP privadas mediante los siguientes comandos. (Puede usar los mismos comandos en Windows y Linux).

- nslookup ec2.<aws\_region>.amazonaws.com
- nslookup mgn.<aws\_region>.amazonaws.com

## Probar la conectividad y la resolución de nombres desde la red de área de ensayo

Para probar la conectividad desde el área de ensayo, inicie una instancia EC2 temporal en la subred de ensayo y pruebe lo siguiente:

- Conectividad a través de HTTPS en el puerto TCP 443 con el extremo del servicio de migración de aplicaciones.
- En Windows (en PowerShell):

```
Test-NetConnection -ComputerName mgn.<aws_region>.amazonaws.com -Port 443
```

- En Linux o Windows (cmd):

```
Telnet mgn.<aws_region>.amazonaws.com 443
```

- Conectividad a través de HTTPS en el puerto TCP 443 con el endpoint de Amazon EC2.
- En Windows (en PowerShell):

```
Test-NetConnection -ComputerName ec2.<aws_region>.amazonaws.com -Port 443
```

- En Linux o Windows (cmd):

```
Telnet ec2.<aws_region>.amazonaws.com 443
```

Si la inicialización de la replicación se detiene en el paso «Descargar el software de replicación» después de instalar el agente en el servidor de origen, compruebe lo siguiente.

- Resolución de problemas de problemas:

```
nslookup s3.<aws_region>.amazonaws.com
```

#### Note

El punto de enlace de Amazon S3 se resolverá en una IP pública, pero se conectará de forma privada a través del punto de enlace de Amazon S3.

- Conectividad a través del protocolo HTTPS en el puerto TCP/443.
- En Windows:

```
Test-NetConnection -ComputerName s3.<aws_region>.amazonaws.com -Port 443
```

- En Linux:

```
Telnet s3.<aws_region>.amazonaws.com 443
```

## Conclusión

Esta guía cubría los requisitos y proporcionaba un ejemplo de configuración para utilizar el Servicio de lift-and-shift migración de aplicaciones para la migración de servidores de redes locales seguras aAWS una conectividad privada (AWS VPNoAWS Direct Connect). Este es un escenario típico de muchas migraciones corporativas. La guía también proporcionó orientación sobre las formas de realizar pruebas mediante la implementación automática o manual, y sobre cómo monitorear y solucionar los problemas de conectividad si surgieran.

# Recursos

## Publicaciones de blog

- [Acelere su migración conAWS Application Migration Service](#)
- [Cómo utilizar lo nuevoAWS Application Migration Service para migraciones de Lift and Shift](#)

## Guías y patrones

- [Connect a los planos de datos y control deAWS MGN a través de una red privada](#)
- [AWSestrategia de migración a gran escala y mejores prácticas](#)
- [Automatiza las migraciones de servidores a gran escala con Cloud Migration Factory](#)

## Soluciones

- [Coordine y automatice las migraciones a gran escala aNube de AWS través de laAWS solución Cloud Migration Factory on](#)

## Historial de documentos

En la siguiente tabla se describen los cambios importantes de esta guía. Si quieres recibir notificaciones sobre future actualizaciones, puedes suscribirte a una fuente [RSS](#).

Cambio	Descripción	Fecha
<a href="#">Publicación inicial</a>	—	10 de marzo de 2023

# AWS Glosario de orientación prescriptiva

Los siguientes son términos de uso común en las estrategias, guías y patrones proporcionados por AWS Prescriptive Guidance. 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: migre su base de datos Oracle local a la edición compatible con PostgreSQL de Amazon Aurora.
- **Redefinir la plataforma (transportar y redefinir):** traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Amazon Relational Database Service (Amazon RDS) para Oracle en el Nube de AWS
- **Recomprar (readquirir):** cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: migre su sistema de gestión de relaciones con los clientes (CRM) a Salesforce.com.
- **Volver a alojar (migrar mediante lift-and-shift):** traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Oracle en una instancia EC2 del 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 local 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 gestionados](#).

### ACID

Consulte [atomicidad, consistencia, aislamiento y 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 la 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 base de datos de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la base de datos de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función agregada

Función SQL que opera en un grupo de filas y calcula un único valor de retorno para el grupo. Entre los ejemplos de funciones agregadas se incluyen SUM y MAX.

## IA

Véase [inteligencia artificial](#).

AIOps

Consulte las [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

Un enfoque de seguridad que permite el uso únicamente de aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

## cartera de aplicaciones

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

## inteligencia artificial (IA)

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

## operaciones de inteligencia artificial (AIOps)

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

## cifrado asimétrico

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

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

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

## control de acceso basado en atributos (ABAC)

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

## origen de datos fidedigno

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

## Zona de disponibilidad

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

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

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la [Página web de AWS CAF](#) y el [Documento técnico de AWS CAF](#).

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

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQF se incluye con AWS

Schema Conversion Tool ( ). AWS SCT Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

## B

Un bot malo

Un [bot](#) destinado a interrumpir o causar daño a personas u organizaciones.

BCP

Consulte la [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. Véase también [endianness](#).

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

Una estrategia de despliegue 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 en el otro entorno (verde). Esta estrategia le ayuda a revertirla rápidamente 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 información en Internet. Algunos otros bots, conocidos como bots malos, tienen como objetivo interrumpir o causar daños a personas u organizaciones.

## botnet

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

## rama

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 con cristales rotos

En circunstancias excepcionales y mediante un proceso aprobado, un usuario puede acceder rápidamente a un sitio para el Cuenta de AWS que normalmente no tiene permisos de acceso. Para obtener más información, consulte el indicador [Implemente procedimientos de rotura de cristales en la guía Well-Architected AWS](#) .

## 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 el marco AWS de adopción de la nube.](#)

## despliegue canario

El lanzamiento lento e incremental de una versión para los usuarios finales. Cuando se tiene confianza, se despliega la nueva versión y se reemplaza la versión actual en su totalidad.

## CCoE

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

## CDC

Consulte la [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

Introducir intencionalmente 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 la [integración continua y la 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 conectada a la tecnología de [computación perimetral](#).

### 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 cuatro fases por las que suelen pasar las organizaciones cuando migran a Nube de AWS:

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

- 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 del](#) blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de [preparación para la migración](#).

## CMDB

Consulte la [base de datos de administración de la 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. Los repositorios en la nube más comunes incluyen GitHub o AWS CodeCommit. 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 aprendizaje automático para analizar y extraer información de formatos visuales, como imágenes y vídeos digitales. Por ejemplo, AWS Panorama ofrece dispositivos que añaden CV a las redes de cámaras locales, y Amazon SageMaker proporciona algoritmos de procesamiento de imágenes para CV.

## desviación de configuración

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

## 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

Conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus comprobaciones 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, presentación y producción del proceso de lanzamiento del software. La CI/CD se describe comúnmente como una canalización. La CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. 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](#).

#### desviación 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 desviación de los 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

Un marco arquitectónico que proporciona una propiedad de datos distribuida y descentralizada con administración y gobierno centralizados.

#### 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

Un sistema de administración de datos que respalde la inteligencia empresarial, como el análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para consultas y 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 el [lenguaje de definición de bases de datos](#) 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 de 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 utilizan habitualmente para restringir consultas, filtrar y etiquetar 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)

La estrategia y el proceso que se utilizan para minimizar el tiempo de inactividad y la pérdida de datos ocasionados por 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 el 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 de referencia. 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 [el mapeo del flujo de valor del desarrollo](#).

## E

### EDA

Consulte el [análisis exploratorio 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 nube, la computación](#) perimetral puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

### cifrado

Proceso informático que transforma datos de texto plano, 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 el punto final del 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 otros directores Cuentas de AWS o a AWS Identity and Access Management (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)

Un sistema que automatiza y gestiona los procesos empresariales clave (como la contabilidad, el [MES](#) y la gestión 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).

## environment

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 una canalización de CI/CD, 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](#).

## PERP

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 datos

La tabla central de un [esquema en forma de estrella](#). Almacena datos cuantitativos sobre las operaciones comerciales. Normalmente, 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.

### fallan rápidamente

Una filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de un enfoque ágil.

### límite de aislamiento de fallas

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 obtener más información, consulte [Límites de AWS aislamiento de errores](#).

### rama de característica

Consulte la [sucursal](#).

### 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.

## FGAC

Consulte el 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 modificados](#) 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.

## G

### bloqueo geográfico

Consulta [las restricciones geográficas](#).

### restricciones geográficas (bloqueo geográfico)

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

### Flujo de trabajo de Gitflow

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

## estrategia de implementación desde cero

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

## barrera de protección

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

# H

## JA

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.

## 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, las revisiones suelen realizarse fuera del flujo de trabajo habitual de las DevOps versiones.

## periodo de hiperatención

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

|

## laC

Vea [la infraestructura como código](#).

## políticas basadas en identidad

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

|

## 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.

## IloT

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

## infraestructura inmutable

Un modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, aplicar parches o modificar la infraestructura existente. [Las infraestructuras inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables](#). Para obtener más información, consulte las prácticas recomendadas para [implementar con una infraestructura inmutable](#) en Well-Architected Framework AWS .

## VPC entrante (de entrada)

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

## migración gradual

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

## Industria 4.0

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

## infraestructura

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

## infraestructura como código (IaC)

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

## Internet de las cosas industrial (IIoT)

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

## VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red entre las VPC (iguales o Regiones de AWS diferentes), Internet y las redes locales. La [Arquitectura de referencia de seguridad de AWS](#) recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

## Internet de las cosas (IoT)

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

## interpretabilidad

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

### migración grande

Migración de 300 servidores o más.

## LBAC

Consulte el 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

Ver [7 Rs](#).

## sistema little-endian

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

## entornos inferiores

[Véase 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

Ver [sucursal](#).

## malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware puede 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 gestionados

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

## sistema de ejecución de fabricación (MES)

Un sistema de software para rastrear, monitorear, documentar y controlar los procesos de producción que convierten las materias primas en productos terminados en el taller.

## MAP

Consulte [Migration Acceleration Program](#).

## mecanismo

Un proceso completo en el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para realizar ajustes. Un mecanismo es un ciclo que se refuerza y mejora a 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 el [sistema de ejecución de la fabricación](#).

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

## arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de

una interfaz bien definida mediante API ligeras. Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte [Implementación de microservicios](#) en. AWS

## Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

## migración a escala

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

## fábrica de migración

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)

Una herramienta en línea que proporciona información para validar el modelo de negocio para migrar a. 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 asociados 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

El enfoque utilizado para migrar una carga de trabajo a. Nube de AWS Para obtener más información, consulte la entrada de las [7 R](#) de este glosario y consulte [Movilice a su organización para acelerar las migraciones a gran escala](#).

## ML

[Consulte el aprendizaje automático.](#)

## 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 obtener más información, consulte [Estrategia para modernizar las aplicaciones en el 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 obtener más información, consulte [Evaluación de la preparación para la modernización de las aplicaciones en el 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](#).

## MAPA

Consulte [la evaluación de la cartera de migración](#).

## MQTT

Consulte [Message Queue Queue Telemetría](#) y Transporte.

## 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

Un modelo que actualiza y modifica la infraestructura existente 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 el control de acceso de origen](#).

### OAI

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

### OCM

Consulte [gestión 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

Véase el [acuerdo a nivel operativo](#).

## migración en línea

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

### OPC-UA

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

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

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

## acuerdo de nivel operativo (OLA)

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

## revisión de la preparación operativa (ORR)

Una lista de preguntas y las mejores prácticas asociadas que le ayudan a comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles fallos. Para obtener más información, consulte [Operational Readiness Reviews \(ORR\)](#) en AWS Well-Architected Framework.

## tecnología operativa (OT)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En la industria manufacturera, 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 el AWS CloudTrail que se registran todos los eventos para todos Cuentas de AWS los miembros 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.

## O

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

## NO

Consulte [tecnología operativa](#).

## VPC saliente (de salida)

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

## P

### límite de permisos

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

### información de identificación personal (PII)

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

## PII

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

### política

Un objeto que puede definir los permisos (consulte la [política basada en la identidad](#)), especifique las condiciones de acceso (consulte la [política basada en los recursos](#)) o defina los permisos máximos para todas las cuentas de una organización AWS Organizations (consulte la política de control de [servicios](#)).

### 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. Para obtener más información, consulte [Habilitación de la persistencia de datos en los microservicios](#).

### 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

Una condición de consulta que devuelve true o false, por lo general, se encuentra en una cláusula. WHERE

### pulsar un predicado

Técnica de optimización de consultas de bases de datos que filtra los datos de la consulta antes de transferirlos. Esto reduce la cantidad de datos que se deben recuperar y procesar de la base de datos relacional y 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

Un enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de ingeniería.

## zonas alojadas privadas

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

## control proactivo

Un [control de seguridad](#) diseñado para evitar el despliegue de recursos no conformes. Estos controles escanean los recursos antes de aprovisionarlos. Si el recurso no cumple con el control, significa que no está aprovisionado. Para obtener más información, consulte la [guía de referencia de controles](#) en la AWS Control Tower documentación y consulte [Controles proactivos](#) en Implementación de controles de seguridad en AWS.

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

La gestión 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 el rechazo y la retirada.

## entorno de producción

Consulte [el entorno](#).

## controlador lógico programable (PLC)

En la fabricación, una computadora adaptable y altamente confiable que monitorea las máquinas y automatiza los procesos de fabricación.

## 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.

## publicar/suscribirse (pub/sub)

Un patrón que permite las 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 puedan suscribir otros microservicios. El sistema puede añadir 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

Véase [responsable, responsable, consultado, informado \(RACI\)](#).

### 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

Véase [responsable, responsable, consultado, informado \(RACI\)](#).

### RCAC

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

## read replica

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

Ver [7 Rs.](#)

## 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

Ver [7 Rs.](#)

## Región

Una colección 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 obtener más información, consulte [Regiones de AWS Especificar qué cuenta puede usar.](#)

## 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 [7 Rs.](#)

## versión

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

## trasladarse

Ver [7 Rs.](#)

---

## redefinir la plataforma

Ver [7 Rs.](#)

## recompra

Ver [7 Rs.](#)

## resiliencia

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

## 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 [7 Rs.](#)

## jubilarse

Ver [7 Rs.](#)

## rotación

Proceso de actualizar periódicamente un [secreto](#) para dificultar el acceso de un atacante 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 el [objetivo del punto de recuperación](#).

## RTO

Consulte el [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 AWS Management Console 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 el [control de supervisión y la adquisición de datos](#).

## SCP

Consulte la [política de control de servicios](#).

## secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus

metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener más información, consulta [¿Qué hay en un secreto de Secrets Manager?](#) en la documentación de Secrets Manager.

## 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. Hay cuatro tipos principales de controles de seguridad: [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

Una acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o remediarlo. Estas automatizaciones sirven como controles de seguridad [detectables](#) o [adaptables](#) que le ayudan a implementar las mejores prácticas AWS de seguridad. Algunos ejemplos de acciones de respuesta automatizadas incluyen la modificación de un grupo de seguridad de VPC, la aplicación de parches a una instancia de Amazon EC2 o la rotación de credenciales.

## cifrado del servidor

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

## política de control de servicio (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. Las SCP definen barreras de protección o establecen límites a las acciones que un administrador puede delegar en los usuarios o roles. Puede utilizar las SCP como listas de permitidos o rechazados, para especificar qué servicios o acciones se

encuentra permitidos o prohibidos. Para obtener más información, consulte [las políticas de control 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)

[Una 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 que compartes con respecto a la seguridad y AWS 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 [la información de seguridad y el sistema de gestión de eventos](#).

#### punto único de fallo (SPOF)

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

#### SLA

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

#### SLI

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

## ASÍ QUE

Consulte el 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 obtener más información, consulte [Enfoque gradual para modernizar las aplicaciones en el. Nube de AWS](#)

### SPOT

Consulte el [punto único de falla](#).

### esquema en forma de estrella

Estructura organizativa de una base de datos que utiliza una tabla de datos grande para almacenar datos transaccionales o medidos y una o más tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para usarse 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.

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

En la industria manufacturera, un sistema que utiliza hardware y software para monitorear 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

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

# T

## etiquetas

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. 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

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

## flujo de trabajo basado en enlaces troncales

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

## acceso de confianza

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

## ajuste

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

## equipo de dos pizzas

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

# U

## incertidumbre

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

Ver [entorno](#).

## V

### succión

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

### control de versión

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

### Emparejamiento de VPC

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

### vulnerabilidad

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

## W

### caché caliente

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

## datos templados

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

## función de ventana

Función SQL que realiza un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para procesar tareas, 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.

## GUSANO

Mira, [escribe una vez, lee muchas](#).

## WQF

Consulte el [marco de calificación de cargas de trabajo de AWS](#).

## escribe una vez, lee muchas (WORM)

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

## Z

### ataque de día cero

Un ataque, normalmente de malware, que aprovecha 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.

### 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.