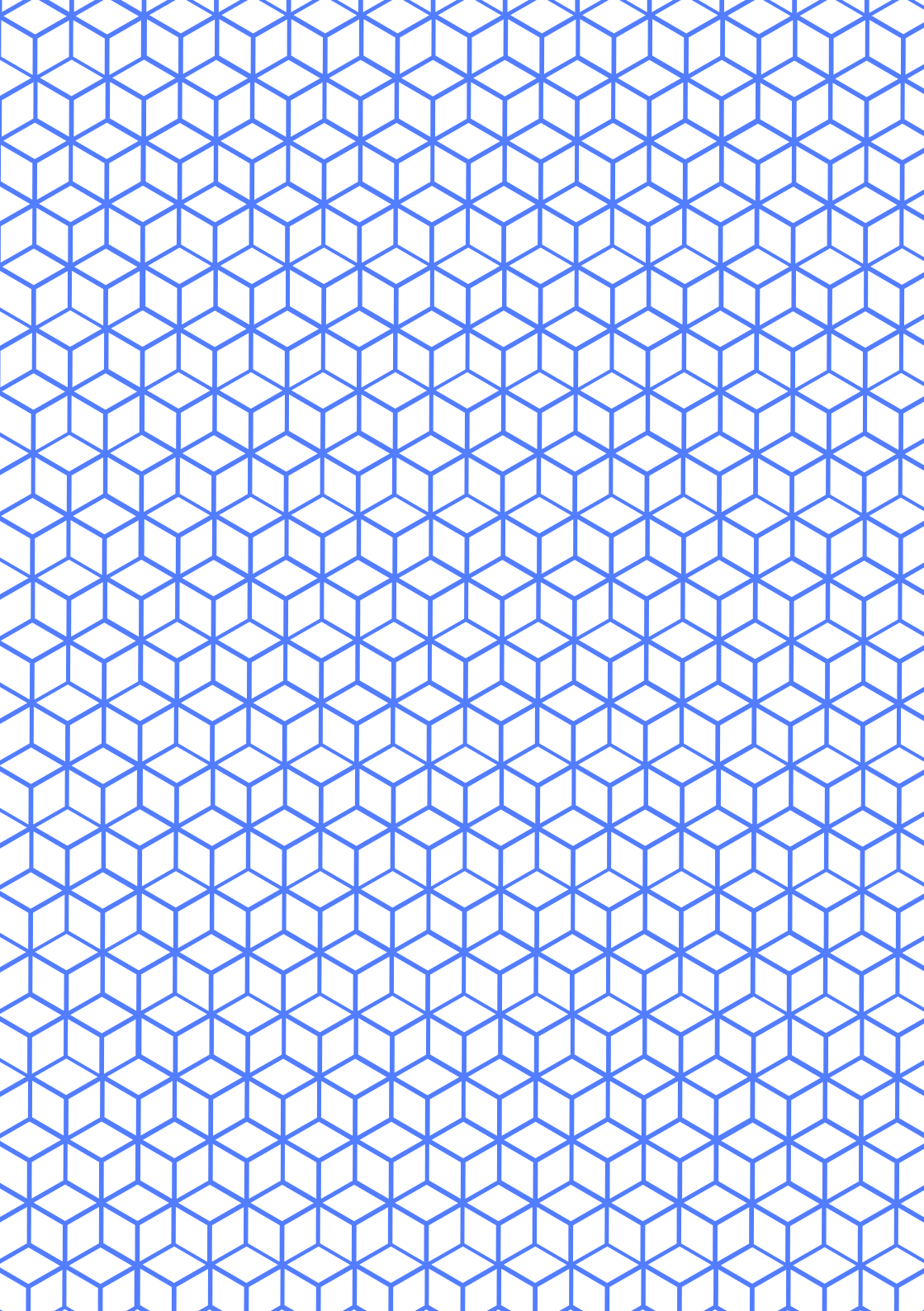
amazon web services

SEGURIDAD Y CONFORMIDAD DE AWS

GUÍA DE REFERENCIA RÁPIDA

2017



INFORMACIÓN GENERAL

INFORMACIÓN GENERAL

Al migrar a la nube sus cargas de trabajo reguladas, tiene acceso a muchas de nuestras características de gobernanza, que puede utilizar para conseguir un nivel superior de seguridad a escala. La gobernanza basada en la nube ofrece un costo menor de entrada, operaciones más sencillas y mayor agilidad al proporcionar más supervisión, control de seguridad y automatización central. La migración a la nube significa que podrá utilizar AWS para reducir el número de controles de seguridad que necesita mantener.

Un entorno conforme es fruto de un entorno debidamente protegido. Proporcionamos un sólido conjunto de controles de infraestructura que se han validado mediante numerosas certificaciones y acreditaciones. Cada certificación significa que un auditor ha verificado que se han establecido determinados controles de seguridad y funcionan según lo previsto. Encontrará más información acerca de todas las certificaciones y acreditaciones que tenemos en la página Programas de AWS Assurance.

También proporcionamos una amplia gama de herramientas y servicios que puede utilizar como ayuda para alcanzar la conformidad en la nube, incluidos Amazon Inspector, AWS Artifact, AWS Service Catalog, AWS CloudTrail, AWS Config y AWS Config Rules.

PROGRAMAS

PROGRAMAS

Nuestros entornos se auditan continuamente, y nuestra infraestructura y nuestros servicios cuentan con la aprobación para operar según varios estándares de conformidad y certificaciones del sector en distintos sectores y zonas geográficas. Puede utilizar estas certificaciones para validar la implementación y efectividad de nuestros controles de seguridad.

Figura 1: programas de AWS Assurance

Nota: añadimos continuamente programas. Para obtener la lista más actualizada de programas de AWS Assurance, visite el sitio web.

Las ***certificaciones y acreditaciones*** las realiza un auditor independiente externo. Nuestras certificaciones, informes de auditoría o acreditaciones de conformidad se basan en los resultados del trabajo del auditor.

Las ***leyes, regulaciones, privacidad*** y las ***homologaciones y los marcos reguladores*** son específicos de un sector o función determinados. Para apoyarle, proporcionamos funcionalidad (como características de seguridad) y habilitadores (incluidos cuadernos de trabajo, documentos de comparación y documentos

técnicos sobre conformidad). La certificación formal “directa” de estas leyes, regulaciones y programas 1) no está disponible para los proveedores de servicios en la nube o 2) representa un subconjunto más reducido de los requisitos ya demostrables por nuestros programas formales de certificación y acreditación actuales.

Estos son algunos de nuestros programas más populares:

PCI DSS: PCI DSS (siglas en inglés de estándar de seguridad de los datos del sector de tarjetas de pago) es un estándar de seguridad muy estricto para la prevención del fraude y la protección de datos de titulares de tarjetas para los comerciantes que procesan pagos con tarjetas de crédito.

ISO 27001: es un estándar de seguridad global muy extendido que fija los requisitos de los sistemas de administración de la seguridad de la información. Ofrece un enfoque sistemático para administrar la información de empresas y clientes que se basa en evaluaciones de riesgos periódicas.

SOC: los informes Service Organization Control (SOC, Control de organizaciones de servicios) de AWS son informes de análisis independientes de terceros que muestran cómo AWS logra los controles y objetivos clave de conformidad. La finalidad de estos informes es ayudarle a usted y a sus auditores a entender los controles de AWS que se han establecido como soporte a las operaciones y la conformidad. Hay cuatro tipos de informes SOC de AWS: Informe SOC 1 de AWS, Informe SOC 2 de AWS: Informe de seguridad y disponibilidad, Informe SOC 2 de AWS: Informe de confidencialidad e Informe SOC 3 de AWS: Informe de seguridad y disponibilidad.

FedRAMP: es un programa gubernamental estadounidense para asegurar que se cumplan los estándares en cuanto a la evaluación de la seguridad, así como la autorización y la monitorización continua. FedRAMP sigue los estándares de control de seguridad de NIST 800-53.

PROGRAMAS

Modelo de seguridad en la nube (CSM) del Departamento de Defensa (DoD): estándares para la informática en la nube emitidos por la Agencia de Sistemas de Información de Defensa (DISA) de Estados Unidos y documentados en la Guía de requisitos de seguridad (SRG) del Departamento de Defensa (DoD). Ofrece un proceso de autorización para los propietarios de cargas de trabajo del DoD que tienen requisitos arquitectónicos específicos en función del nivel de impacto.

HIPAA: la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) contiene estrictos estándares de seguridad y conformidad para las organizaciones que procesan o almacenan información sanitaria protegida (PHI).

Encontrará descripciones completas de cada programa que asumimos en la página web Programas de AWS Assurance.

AWS Artifact

El portal de AWS Artifact proporciona acceso previa petición a nuestros documentos de conformidad y seguridad, también conocidos como elementos de auditoría. Puede utilizar estos elementos para demostrar la seguridad y la conformidad de su infraestructura y sus servicios de AWS ante los auditores o las autoridades reguladoras.

Entre los ejemplos de elementos de auditoría se incluyen informes de Service Organization Control (SOC), informes de Payment Card Industry (PCI), y certificaciones de entidades de acreditación de todo el mundo y todos los sectores que validan la implementación y eficacia operativa de los controles de seguridad de AWS.

Puede obtener acceso al portal de AWS Artifact directamente desde la consola de administración de AWS.

SECTORES

SECTORES

Los clientes de los siguientes sectores utilizan AWS para satisfacer sus necesidades de conformidad con la normativa:

- Agricultura y minería
- Análisis y big data
- Informática y electrónica
- Comercio electrónico
- Educación
- Energía y servicios públicos
- Servicios financieros
- Alimentación y bebidas
- Juegos
- Sector público
- Sanidad y ciencias de la salud
- Seguros
- Fabricación
- Contenido multimedia y entretenimiento
- Organización sin ánimo de lucro
- Inmobiliarias y construcción
- Venta al por menor, venta al por mayor y distribución
- Software e Internet
- Telecomunicaciones
- Transporte y logística
- Viajes y hostelería

CÓMO COMPARTIMOS LA RESPONSABILIDAD

CÓMO COMPARTIMOS LA RESPONSABILIDAD

Al mover su infraestructura de TI a AWS, adoptará el modelo de responsabilidad compartida que se muestra en la figura 2. Puesto que AWS opera, administra y controla los componentes de TI, desde el sistema operativo host y la capa de virtualización hasta la seguridad física en las instalaciones en las que operan los servicios, este modelo compartido alivia su carga operativa.

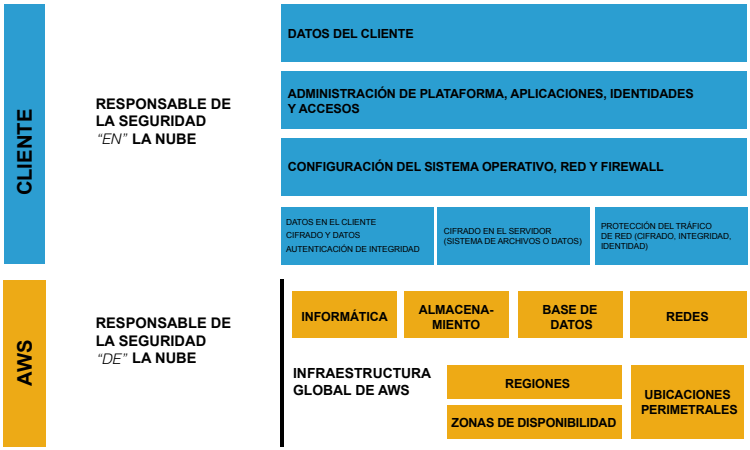


Figura 2: modelo de responsabilidad compartida

El modelo de responsabilidad compartida también abarca los controles de TI. De la misma forma que comparte con nosotros la responsabilidad de operar el entorno de TI, también la comparte en lo referente a la administración, operación y verificación de los controles de TI. Reducimos la carga que supone operar los controles, administrando los controles asociados con la infraestructura física implementada en el entorno de AWS. Puede utilizar la documentación de conformidad y control de AWS disponible para realizar sus procedimientos de evaluación y verificación de control según sea necesario, en virtud del estándar de conformidad aplicable.

AWS: CONFORMIDAD DE LA NUBE

Somos responsables de ayudarle a mantener un entorno conforme y seguro. En general, hacemos lo siguiente:

Validar que nuestros servicios e instalaciones de todo el mundo mantienen un entorno de control ubicuo que funciona con eficacia. Nuestro entorno de control comprende políticas, procesos y actividades de control que se benefician de varios aspectos del entorno de control global de Amazon.

El entorno de control colectivo comprende al personal, los procesos y la tecnología necesarios para crear y mantener un entorno que respalde la eficacia operativa de nuestro marco de control. Hemos integrado en nuestro marco de control los controles específicos de la nube aplicables que han identificado los principales organismos del sector de informática en la nube. Realizamos un seguimiento de estos grupos del sector a fin de identificar las prácticas principales que podemos aplicar y facilitarle aún más la administración de su entorno de control.

Demostrar nuestra actitud ante la conformidad para ayudarle a verificar la conformidad con los requisitos del sector y gubernamentales. Colaboramos con organismos de certificación externos y auditores independientes para ofrecerle una considerable cantidad de información acerca de las políticas, los procesos y los controles que establecemos y aplicamos.

Monitorizarlo; mediante el uso de miles de requisitos de control de seguridad, mantenemos la conformidad con estándares y prácticas recomendadas internacionales.

CLIENTE: CONFORMIDAD EN LA NUBE

Al igual que ocurre en un centro de datos tradicional, usted asume la responsabilidad de administrar el sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad), de cualquier otro software de aplicaciones asociadas y de la configuración del firewall del grupo de seguridad que ofrece AWS. Debe pensar detenidamente en los servicios que elige, ya que sus responsabilidades variarán en función de los servicios que utilice, la integración de estos servicios en su entorno de TI y la legislación y los reglamentos aplicables.

Para administrar de forma segura sus recursos de AWS, debe saber qué recursos está utilizando (inventario de activos), configurar de forma segura el SO invitado y las aplicaciones en sus recursos (parámetros de configuración segura, parches y antimalware) y controlar los cambios en los recursos (administración de cambios).

Puede utilizar la información que facilitamos acerca de nuestro programa de riesgos y conformidad para incorporarla a su marco de conformidad.

SU CONTENIDO

SU CONTENIDO

Por diseño, le otorgamos la propiedad y el control sobre su contenido. Mediante herramientas sencillas pero poderosas, puede determinar dónde se almacenará su contenido, proteger su contenido en tránsito o en reposo, y administrar el acceso a los servicios y recursos de AWS para sus usuarios.

> **Nota**: no obtenemos acceso a su contenido ni lo utilizamos para ningún otro fin que no sea proporcionarle a usted y a sus usuarios finales los servicios de AWS que han seleccionado. En ningún momento utilizamos su contenido para nuestros propios fines, incluidos marketing o publicidad.

Acceso: con nuestro conjunto avanzado de características de acceso, cifrado y registro (como AWS CloudTrail), puede administrar el acceso a su contenido y a los servicios y recursos de AWS. No obtenemos acceso a su contenido ni lo utilizamos para ningún fin distinto al exigido legalmente. Lo hacemos para mantener los servicios de AWS y proporcionarlos a usted y a sus usuarios finales.

Almacenamiento: puede elegir las regiones en las que desea almacenar su contenido. No trasladaremos ni replicaremos su contenido fuera de las regiones elegidas por el cliente, excepto en lo exigido legalmente o como sea necesario para el mantenimiento de los servicios de AWS y para proporcionarlos a usted y sus usuarios finales. Por ejemplo, si es un cliente europeo, puede decidir implementar sus servicios de AWS en la región UE (Alemania) exclusivamente.

SU CONTENIDO

Seguridad: usted elige cómo se protege su contenido. Le ofrecemos un cifrado seguro de su contenido en tránsito o en reposo y le ofrecemos la opción de administrar sus propias claves de cifrado.

Divulgación de su contenido: no divulgaremos su contenido a menos que sea necesario cumplir con la ley o con una orden válida y vinculante de un organismo gubernamental o regulador. Si nos vemos obligados a divulgar su contenido, se lo notificaremos antes a usted para que pueda buscar amparo frente a la divulgación de la información.

> **Importante**: si la ley prohíbe dicha notificación, o si hay una clara indicación de conducta ilegal relativa al uso de los productos o servicios de Amazon, se lo notificaremos antes de revelar su contenido.

Garantía de seguridad: para ayudarle a establecer, utilizar y aprovechar nuestro entorno de control de seguridad, hemos desarrollado un programa de garantía de seguridad que utiliza prácticas recomendadas internacionales sobre privacidad y protección de datos. Estos procesos de control y medidas de seguridad se someten a múltiples validaciones independientes externas.

> **Nota**: para validar que administramos la seguridad de la nube mediante controles físicos y técnicos diseñados para impedir accesos no autorizados o la divulgación de contenido de los clientes, un auditor independiente ha certificado que cumplimos con los estándares del sector.

DÓNDE SE ALMACENA SU CONTENIDO

Los centros de datos de AWS están agrupados en varios países del mundo. Nos referimos a cada uno de nuestros clústeres de centros de datos de un país determinado como “región”. Usted tiene acceso a numerosas regiones de AWS de todo el mundo, y puede utilizar una región, todas las regiones o cualquier combinación de regiones.

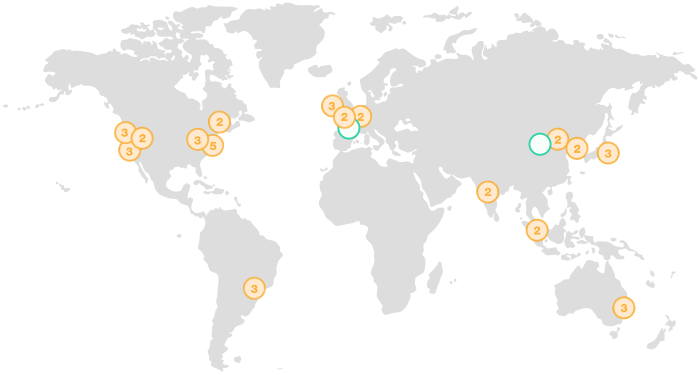


Figura 3: regiones

Usted ejerce el control y la propiedad total de la región en la que los datos se encuentran físicamente, lo que facilita el cumplimiento de los requisitos regionales de conformidad y residencia de datos. Puede elegir la región o las regiones de AWS en las que desea almacenar su contenido, lo que es útil si tiene requisitos geográficos específicos. Por ejemplo, si es un cliente europeo, puede decidir implementar sus servicios de AWS en la región UE (Alemania) exclusivamente. Si elige esta opción, su contenido se almacenará en Alemania a menos que seleccione otra región de AWS diferente.

CONTINUIDAD DEL NEGOCIO

Nuestra infraestructura presenta un alto nivel de disponibilidad y ofrecemos las características necesarias para implementar una arquitectura resistente de TI. Nuestros sistemas están diseñados para que toleren errores del sistema o del hardware con un impacto mínimo en los clientes.

> La **resistencia** se refiere a reducir la probabilidad de que los activos no estén disponibles.
>
> La **recuperación** se refiere a reducir el impacto cuando los activos no están disponibles.
>
> La **copia de seguridad** es una estrategia para abordar la pérdida de datos, ya sea accidental o intencionada.

La recuperación de desastres es el proceso de prepararse para poder recuperar los datos en caso de que se produzca un desastre. Cualquier acontecimiento que tenga un impacto negativo sobre la continuidad del negocio o sobre sus finanzas podría calificarse de desastre. La nube de AWS admite muchas arquitecturas populares de recuperación de desastres, desde entornos de "luz piloto" que están listos para ampliarse en cualquier momento a entornos de "espera activa" que permiten una rápida conmutación por error.

Para obtener más información acerca de la recuperación de desastres en AWS, visite **https://aws.amazon.com/disaster-recovery/**.

Nuestros centros de datos están agrupados en varias regiones del mundo. Todos los centros de datos están online y a disposición de los clientes, por lo que ninguno está "inactivo". En caso de error, los procesos automatizados desvían el tráfico de datos del cliente de la zona afectada.

CONTINUIDAD DEL NEGOCIO

Le ofrecemos la flexibilidad necesaria para colocar las instancias y almacenar datos en varias regiones geográficas, así como en varias zonas de disponibilidad dentro de cada región. Al distribuir las aplicaciones en varias zonas de disponibilidad, puede mantener la resistencia ante la mayoría de los modos de error, incluidos los desastres naturales o los errores del sistema.

Usted puede crear sistemas muy resistentes en la nube empleando varias instancias en diferentes zonas de disponibilidad y usando replicación de datos, a fin de alcanzar un tiempo de recuperación extremadamente rápido y objetivos de punto de recuperación altos.

Usted asume la responsabilidad de administrar y probar la copia de seguridad y la recuperación de su sistema de información creado en la infraestructura de AWS. Puede utilizar la infraestructura de AWS para poder realizar una recuperación de desastres más rápida de sus sistemas de TI fundamentales sin incurrir en los gastos adicionales de infraestructuras que supone disponer de un segundo sitio físico. La nube de AWS admite muchas arquitecturas populares de recuperación de desastres, desde entornos de "luz piloto" que están listos para ampliarse en cualquier momento a entornos de "espera activa" que permiten una rápida conmutación por error.

SEGURIDAD

SEGURIDAD

La seguridad de la nube de AWS es nuestra máxima prioridad. Puede encontrar información sobre la seguridad y conformidad de AWS en el Centro de seguridad de AWS.

Operamos la infraestructura en la nube global que usted usa para provisionar diversos recursos informáticos básicos como el procesamiento y el almacenamiento. Nuestra infraestructura global incluye las instalaciones, redes, hardware y software operativo (como el sistema operativo host, el software de virtualización, etc.) que permiten el provisionamiento y uso de estos recursos. Nuestra infraestructura global está diseñada y administrada de acuerdo con las prácticas recomendadas de seguridad y con arreglo a diversos estándares de conformidad relacionados con la seguridad. Como cliente de AWS, puede tener la certeza de que sus arquitecturas web se asientan sobre una de las infraestructuras informáticas más seguras del mundo.

RECURSOS

RECURSOS

Para obtener acceso a todas las páginas web y los documentos técnicos a los que se hace referencia en este documento, visite el AWS Security and Compliance Quick Reference Resource Hub, que está disponible en **https://aws.amazon.com/compliance/reference/**.

SOCIOS Y MARKETPLACE

La red de socios de AWS (APN) es el programa global de socios de AWS. Ayuda a los socios de APN a crear negocios o soluciones de éxito basados en AWS al ofrecer soporte empresarial, técnico, de marketing y de comercialización (GTM). Para obtener más información, visite **https://aws.amazon.com/partners/**.

AWS Marketplace es un canal de ventas que facilita a los vendedores de AWS la oferta de soluciones de software que se ejecutan en la nube de AWS. Para obtener más información, visite **https://aws.amazon.com/marketplace/**.

CAPACITACIÓN

Tanto si acaba de comenzar como si está consolidando los conocimientos de TI actuales o perfeccionando sus conocimientos de la nube, la capacitación de AWS puede ayudarle a usted y a su equipo a ampliar sus conocimientos para aprovechar la nube al máximo. Para obtener más información, visite **https://aws.amazon.com/training/**.


amazon
web services