Uso de AWS en el Contexto de Consideraciones Comunes de Privacidad y Protección de Datos

Primera publicación Mayo de 2022

Avisos

Los clientes son responsables de realizar su propia evaluación independiente de la información contenida en este documento. El presente documento: (a) es solo con fines informativos, (b) representa las ofertas y prácticas actuales de productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciatarios. Los productos o servicios de AWS se proporcionan "tal cual" sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con sus clientes están controladas por los acuerdos de AWS, y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Contenido

Resumen

Este documento proporciona información para ayudar a los clientes que desean utilizar Amazon Web Services (AWS) para almacenar o procesar contenido que contiene datos personales, en el contexto de consideraciones comunes de privacidad y protección de datos. Ayuda a los clientes a comprender:

- La forma en que funcionan los servicios de AWS, incluida la forma en que los clientes pueden abordar la seguridad y cifrar su contenido.
- Las ubicaciones geográficas donde los clientes pueden elegir almacenar contenido y otras consideraciones relevantes.
- Los roles respectivos que desempeñan el cliente y AWS en la administración y protección del contenido almacenado en AWS.

Introducción

Este documento técnico se centra en las preguntas típicas que hacen los clientes de AWS cuando están considerando los requisitos de privacidad y protección de datos relevantes para su uso de los servicios de AWS para almacenar o procesar contenido que contiene datos personales. Hay otras consideraciones relevantes para que cada cliente las aborde; por ejemplo, es posible que un cliente deba cumplir con los requisitos específicos de la industria, la legislación aplicable en otras jurisdicciones donde ese cliente realiza negocios o los compromisos contractuales que un cliente hace con un tercero.

Este documento técnico se proporciona únicamente con fines informativos. No es asesoría legal y no debe considerarse como asesoría legal. Dado que los requisitos de cada cliente difieren, AWS recomienda encarecidamente a sus clientes que obtengan asesoría adecuada sobre la implementación de los requisitos de privacidad y protección de datos, y sobre las leyes aplicables y otros requisitos relevantes para su negocio.

El término "contenido" en este documento técnico hace referencia al software (incluidas las imágenes de máquinas virtuales), datos, texto, audio, video, imágenes y otro contenido que un cliente, o cualquier usuario final, almacena o procesa mediante AWS. Por ejemplo, el contenido de un cliente incluye objetos que el cliente almacena usando Amazon Simple Storage Service (Amazon S3), archivos almacenados en un Amazon Elastic Block Store (Amazon EBS) o el contenido de un Amazon DynamoDB tabla de base de datos

Dicho contenido puede, pero no necesariamente, incluir datos personales relacionados con ese cliente, sus usuarios finales o terceros. Los términos del Acuerdo de Cliente de AWS, o cualquier otro acuerdo relevante con AWS que rija el uso de los servicios de AWS, se aplican al contenido del cliente. El contenido del cliente no incluye los datos que un cliente proporciona a AWS en relación con la creación o administración de sus cuentas de AWS, tales como los nombres, los números de teléfono, las direcciones de correo electrónico y la información de facturación del cliente. AWS se refiere a esto como *información de la cuenta*, y se rige por el Aviso de Privacidad de AWS.
AWS cambia constantemente, y el Aviso de Privacidad de AWS también puede cambiar. Visite el sitio web con frecuencia para ver los cambios recientes.

Consideraciones relevantes para la privacidad y la protección de datos

El almacenamiento de contenido presenta a todas las organizaciones una serie de asuntos prácticos comunes a considerar, que incluyen:

- ¿El contenido se encontrará seguro?
- ¿Dónde se almacenará el contenido?
- ¿Quién tendrá acceso al contenido?
- ¿Qué leyes y reglamentos se aplican al contenido y qué se necesita para cumplirlos?

Estas consideraciones no son nuevas y no son específicas a la nube. Son relevantes para los sistemas alojados y operados internamente, así como para los servicios tradicionales alojados por terceros. Cada uno puede implicar el almacenamiento de contenido en equipos de terceros o en instalaciones de terceros, con ese contenido administrado, accedido o utilizado por personal de terceros. Al utilizar los servicios de AWS, cada cliente de AWS mantiene la propiedad y el control de su contenido, incluido el control sobre:

- Qué contenido eligen almacenar o procesar utilizando los servicios de AWS
- Qué servicios de AWS utilizan con su contenido
- La(s) región(es) donde se almacena su contenido
- El formato, la estructura y la seguridad de su contenido, incluido si está enmascarado, anonimizado o encriptado
- Quién tiene acceso a sus cuentas y contenido de AWS y cómo se otorgan, administran y revocan esos derechos de acceso

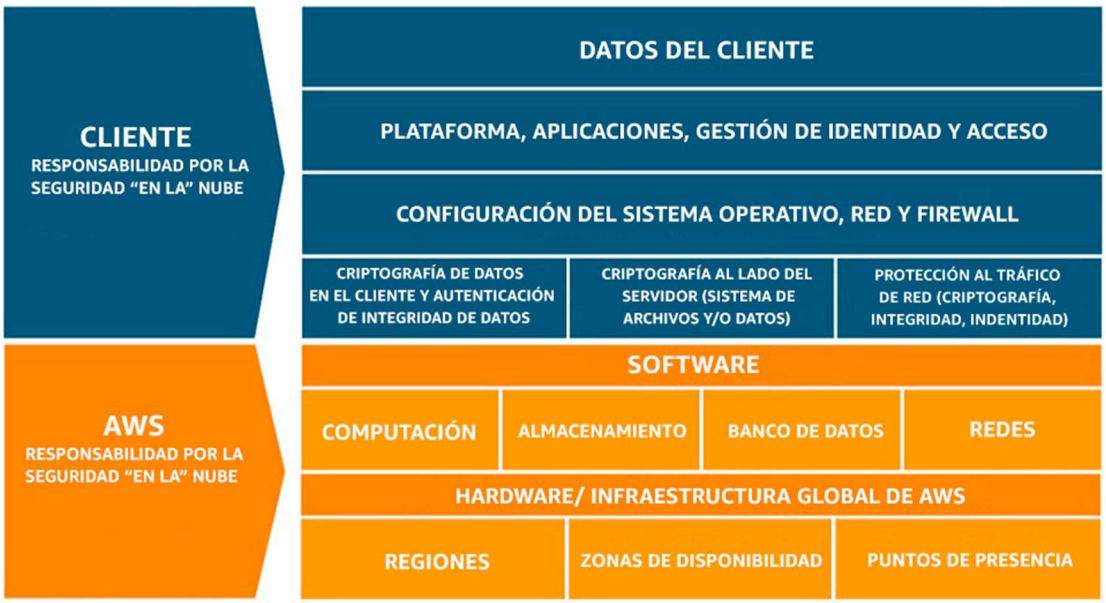
Debido a que los clientes de AWS conservan la propiedad y el control de su contenido dentro del entorno de AWS, también conservan las responsabilidades relacionadas con la seguridad de ese contenido como parte del modelo de "responsabilidad compartida" de AWS. Este modelo de responsabilidad compartida es fundamental para comprender las funciones respectivas del cliente y de AWS en el contexto de los requisitos de privacidad y protección de datos que pueden aplicarse al contenido que los clientes eligen almacenar o procesar mediante los servicios de AWS.

El modelo de responsabilidad compartida de AWS para administrar la seguridad en la nube

¿El contenido del cliente estará seguro?

Mover la infraestructura de TI a AWS crea un modelo de responsabilidad compartida entre el cliente y AWS, ya que tanto el cliente como AWS tienen roles importantes en la operación y administración de la seguridad. AWS opera, administra y controla los componentes desde el sistema operativo del host y la capa de virtualización hasta la seguridad física de las instalaciones en las que operan los servicios de AWS. El cliente es responsable de la administración del sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad) y el software de aplicaciones asociado, así como de la configuración del firewall del grupo de seguridad proporcionado por AWS y otras características relacionadas con la seguridad.

El cliente generalmente se conecta al entorno de AWS a través de servicios que el cliente adquiere de terceros (por ejemplo, proveedores de servicios de Internet). AWS no suministra estas conexiones; son parte del área de responsabilidad del cliente. Los clientes deben considerar la seguridad de estas conexiones y las responsabilidades de seguridad de dichos terceros en relación con sus sistemas. Los roles respectivos del cliente y AWS en el modelo de responsabilidad compartida se muestran en la siguiente figura:



El Modelo de Responsabilidad Compartida de AWS

¿Qué significa el modelo de responsabilidad compartida para la seguridad del contenido del cliente?

Al evaluar la seguridad de una solución en la nube, es importante que los clientes comprendan y distingan entre:

- Medidas de seguridad que implementa y opera el proveedor de servicios en la nube (AWS): “seguridad **de** la nube"
- Medidas de seguridad que el cliente implementa y opera, relacionadas con la seguridad del contenido del cliente y las aplicaciones que hacen uso de los servicios de AWS: “seguridad **en** la nube".

Si bien AWS gestiona la seguridad **de** la nube, la seguridad **en** la nube es responsabilidad del cliente, ya que los clientes conservan el control de la seguridad que eligen implementar para proteger su propio contenido, aplicaciones, sistemas y redes, de la misma manera que lo harían con las aplicaciones en un centro de datos en sitio.

Como entender la seguridad DE la nube

AWS es responsable de administrar la seguridad del entorno de nube subyacente. La infraestructura de la nube de AWS se ha diseñado para ser uno de los entornos de computación en la nube más flexibles y seguros disponibles, diseñado también para brindar una disponibilidad óptima al mismo tiempo que brinda una segregación completa de clientes. Brinda servicios extremadamente escalables y altamente confiables que permiten a los clientes implementar aplicaciones y contenido de manera rápida y segura, a escala global masiva si es necesario.

Los servicios de AWS son independientes del contenido, ya que ofrecen el mismo alto nivel de seguridad a todos los clientes, independientemente del tipo de contenido que se almacena o la región geográfica en la que almacenan su contenido. Los centros de datos altamente seguros y de clase mundial de AWS utilizan vigilancia electrónica de última generación y sistemas de control de acceso multifactorial. Los centro de datos tienen atención las 24 horas del día, los siete días de la semana por guardias de seguridad capacitados, y el acceso está autorizado estrictamente con base en el principio de mínimo privilegio. Para obtener una lista completa de todas las medidas de seguridad integradas en la infraestructura y los servicios centrales de la nube de AWS, consulte el documento técnico Introducción a la Seguridad de AWS .

AWS está atento a la seguridad de sus clientes y ha implementado medidas técnicas y físicas sofisticadas contra el acceso no autorizado. Los clientes pueden validar los controles de seguridad establecidos dentro del entorno de AWS a través de las certificaciones e informes de AWS, incluidos los informes Control de organizaciones y

sistemas de AWS (SOC) 1, 2 y 3 , certificaciones ISO 27001, 27017, 27018 , 27701 y 9001 , y la Declaración de cumplimiento de PCI DSS.

La certificación ISO 27018 de AWS demuestra que AWS cuenta con un sistema de controles que aborda específicamente la protección de la privacidad del contenido del cliente. Estos informes y certificaciones son elaborados por auditores externos independientes y dan fe del diseño y la eficacia operativa de los controles de seguridad de AWS.

Las certificaciones e informes de cumplimiento de AWS se pueden solicitar en AWS Artifact. Se puede encontrar más información sobre las certificaciones de cumplimiento de AWS, los informes y la alineación con las mejores prácticas y estándares en el sitio de Cumplimiento de AWS .

Como entender la seguridad EN la nube

Los clientes conservan la propiedad y el control de su contenido cuando utilizan los servicios de AWS. Los clientes, en lugar de AWS, determinan qué contenido almacenan o procesan utilizando los servicios de AWS. Debido a que es el cliente quien decide qué contenido almacenar o procesar con los servicios de AWS, solo el cliente puede determinar qué nivel de seguridad es apropiado para el contenido que almacena y procesa con AWS. Los clientes también tienen control total sobre qué servicios usan y a quién autorizan para acceder a su contenido y servicios, incluidas las credenciales requeridas.

Los clientes controlan cómo configuran sus entornos y protegen su contenido, incluido si cifran su contenido (en reposo y en tránsito), y qué otras funciones y herramientas de seguridad usan y cómo las usan. AWS no cambia los ajustes de configuración del cliente, ya que el cliente determina y controla estos ajustes. Los clientes de AWS tienen total libertad para diseñar su arquitectura de seguridad para satisfacer sus necesidades de cumplimiento. Esta es una diferencia clave con respecto a las soluciones de alojamiento tradicionales en las que el proveedor decide la arquitectura.

AWS permite y faculta al cliente para decidir cuándo y cómo se implementan las medidas de seguridad en la nube, de acuerdo con las necesidades comerciales de cada cliente. Por ejemplo, si se requiere una arquitectura de mayor disponibilidad para proteger el contenido del cliente, el cliente puede agregar sistemas redundantes, copias de seguridad, ubicaciones, enlaces ascendentes de red, etc. para crear una arquitectura de alta disponibilidad más resiliente. Si se requiere acceso restringido al contenido del cliente, AWS permite que el cliente implemente controles de administración de derechos de acceso tanto a nivel de sistemas como mediante cifrado a nivel de datos.

Para ayudar a los clientes a diseñar, implementar y operar su propio entorno seguro de

AWS, AWS ofrece una amplia selección de herramientas y características de seguridad que los clientes pueden usar. Los clientes también pueden usar sus propias herramientas y controles de seguridad, incluida una amplia variedad de soluciones de seguridad de terceros.

Los clientes pueden configurar sus servicios de AWS para aprovechar una variedad de características, herramientas y controles de seguridad para proteger su contenido, incluidas herramientas sofisticadas de administración de acceso e identidad, capacidades de seguridad, cifrado y seguridad de red.
Ejemplos de pasos que los clientes pueden tomar para ayudar a asegurar su contenido incluyen implementar:

- Políticas sólidas de contraseñas, asignación de permisos adecuados a los usuarios y adopción de medidas robustas para proteger sus claves de acceso.
- Firewalls y segmentación de red apropiados, encriptación de contenido y sistemas de arquitectura adecuados para disminuir el riesgo de pérdida de datos y acceso no autorizado.

Debido a que los clientes, en lugar de AWS, controlan estos factores importantes, los clientes conservan la responsabilidad de sus elecciones y de la seguridad del contenido que almacenan o procesan mediante los servicios de AWS o que conectan a su infraestructura de AWS, como el sistema operativo invitado, las aplicaciones en sus instancias informáticas y el contenido almacenado y procesado en almacenamiento, bases de datos u otros servicios de AWS.

AWS proporciona un conjunto avanzado de funciones de acceso, cifrado y registro para ayudar a los clientes a administrar su contenido de manera eficaz, incluido AWS Key Management Service (AWS KMS) y AWS CloudTrail.

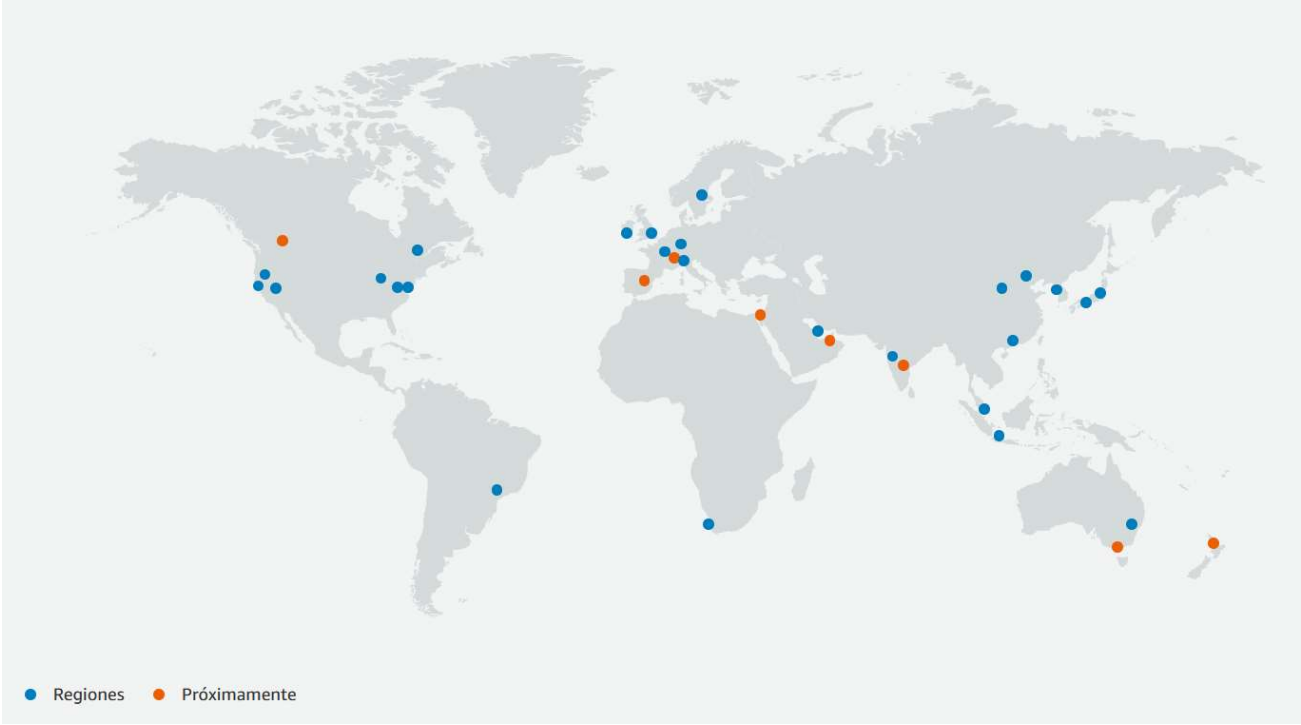
Para ayudar a los clientes a integrar los controles de seguridad de AWS en sus marcos de control existentes y ayudar a los clientes a diseñar y ejecutar evaluaciones de seguridad del uso de los servicios de AWS por parte de su organización, AWS publica una serie de documentos técnicos relacionados con la seguridad, la gobernanza, el riesgo y el cumplimiento; y una serie de listas de verificación y mejores prácticas.

Los clientes también son libres de diseñar y ejecutar evaluaciones de seguridad de acuerdo con sus propias preferencias, y pueden solicitar permiso para realizar exploraciones de su infraestructura en la nube, siempre que dichas exploraciones se limiten a las instancias informáticas del cliente y no infrinjan la Política de Uso Aceptable de AWS.

Para obtener más información sobre las pruebas de penetración, consulte la página Pruebas de Penetración .

Regiones de AWS: ¿Dónde se almacenará el contenido?

Los centro de datos de AWS están integrados en clústeres en varias Regiones. Cada uno de estos clústeres de centro de datos en un país determinado se denomina "Región de AWS". Los clientes tienen acceso a varias regiones de AWS en todo el mundo. Los clientes pueden optar por utilizar una región, todas las regiones o cualquier combinación de regiones de AWS. La siguiente figura muestra las Ubicaciones de Regiones AWS a partir de agosto 2021. Para obtener la información más actualizada sobre las regiones de AWS, consulte la página Infraestructura Global .



Regiones de AWS

Los clientes de AWS eligen la Región o Regiones de AWS en las que se localiza su contenido y servidores. Esto permite a los clientes con requisitos geográficos específicos establecer entornos en una ubicación o ubicaciones de su elección. Por ejemplo, los clientes de AWS en India pueden optar por implementar sus servicios de AWS exclusivamente en una región de AWS, como la región de Asia Pacífico (Mumbai), y almacenar su contenido en tierra en India, si esta es su ubicación preferida. Si el cliente elige esta opción, AWS no moverá su contenido desde la India sin el consentimiento del cliente, excepto cuando así lo exija la ley.

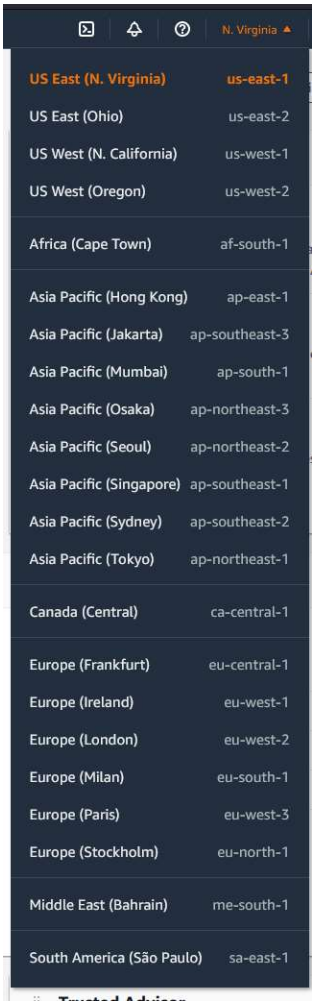
Los clientes siempre conservan el control de qué regiones de AWS se utilizan para

almacenar y procesar contenido. AWS almacena y procesa el contenido de cada cliente solo en las regiones de AWS elegidas por el cliente y, de otro modo, no moverá el contenido del cliente sin el consentimiento del cliente, excepto según lo exija la ley.

¿Cómo pueden seleccionar su(s) región(es) los clientes?

Al utilizar la Consola de Gestión de AWS, o al realizar una solicitud a través de una Interfaz de Programación de Aplicaciones (API) de AWS, el cliente identifica las regiones de AWS en particular donde desea utilizar los servicios de AWS.

La siguiente figura ofrece un ejemplo del menú de selección de región de AWS que se presenta a los clientes al cargar contenido en un servicio de almacenamiento de AWS o al aprovisionar recursos informáticos mediante la Consola de Gestión de AWS.



Selección de regiones de AWS en la Consola de administración de AWS

Los clientes también pueden prescribir la región de AWS que se usará para sus recursos informáticos aprovechando la capacidad de Amazon Virtual Private Cloud (VPC). Amazon VPC le permite al cliente aprovisionar una sección privada y aislada de la nube de AWS donde el cliente puede lanzar recursos de AWS en una red virtual que el cliente define.
Con Amazon VPC, los clientes pueden definir una topología de red virtual que se parece mucho a una red tradicional que podría operar en su propio centro de datos.

Cualquier compute y otros recursos lanzados por el cliente en la VPC se encuentran en la región de AWS designada por el cliente. Por ejemplo, al crear una VPC en la región de Asia Pacífico (Mumbai) y proporcionar un enlace (ya sea un vpn o Direct Connect) al centro de datos del cliente, todos los recursos informáticos lanzados en esa VPC solo residirían en la región de Asia Pacífico (Mumbai). Esta opción también se puede aprovechar para otras regiones de AWS.

Transferencia de datos personales transfronterizas

En 2016, la Comisión Europea aprobó y adoptó el nuevo Reglamento General de Protección de Datos (RGPD). El RGPD reemplazó la Directiva de Protección de Datos de la UE, así como todas las leyes locales relacionadas con esta. Todos los servicios de AWS cumplen con el RGPD. AWS proporciona a los clientes servicios y recursos para ayudarles a cumplir con los requisitos del RGPD que puedan aplicarse a sus operaciones. Estos incluyen el cumplimiento de AWS con el código de conducta de CISPE, controles de acceso a datos granulares, herramientas de monitoreo y registro, cifrado, administración de claves, capacidad de auditoría, cumplimiento de los estándares de seguridad de TI y atestaciones C5 de AWS. Para obtener información adicional, consulte el Centro de AWS del Reglamento General de Protección de Datos (GDPR) y el documento técnico Cómo Navegar el cumplimiento con el RGPD en AWS .

Al utilizar los servicios de AWS, los clientes pueden optar por transferir contenido que contenga datos personales entre países y deben tener en cuenta los requisitos legales que se aplican a dichas transferencias. AWS proporciona un Anexo de Procesamiento de Datos que incluye las Cláusulas Contractuales Tipo 2010/87/UE (a menudo denominadas "Cláusulas Tipo" o "SCC") para los clientes de AWS que transfieren contenido que contiene datos personales (como se define en el RGPD) desde la UE a un país fuera del Espacio Económico Europeo.

Con el Anexo de Procesamiento de Datos y las Cláusulas Tipo de AWS, los clientes de AWS, ya estén establecidos en Europa o sean una empresa global que opera en el Espacio Económico Europeo, pueden seguir gestionando sus operaciones globales usando AWS en pleno cumplimiento con el RGPD. El Anexo de Procesamiento de

Datos de AWS está incorporado en los Términos de Servicio de AWS y se aplica automáticamente en la medida en que el RGPD se aplica al procesamiento de datos personales del cliente en AWS.

¿Quién puede acceder al contenido del cliente?

Control del cliente sobre el contenido

Los clientes que utilizan AWS mantienen y que no liberan el control efectivo sobre su contenido dentro del entorno de AWS pueden:

- Determinar dónde se ubicará su contenido; por ejemplo, el tipo de almacenamiento que utilizan en AWS y la ubicación geográfica (por región de AWS) de ese almacenamiento.
- Controlar el formato, la estructura y la seguridad de su contenido, incluido si está enmascarado, anonimizado o encriptado AWS ofrece a los clientes opciones para implementar un cifrado sólido para el contenido de sus clientes en tránsito o en reposo, y también brinda a los clientes la opción de administrar sus propias claves de cifrado o utilizar mecanismos de cifrado de terceros de su elección.
- Administrar otros controles de acceso, como la administración del acceso a la identidad, los permisos y las credenciales de seguridad.

Esto permite a los clientes de AWS controlar todo el ciclo de vida de su contenido en AWS y administrar su contenido de acuerdo con sus propias necesidades específicas, incluida la clasificación de contenido, el control de acceso, la retención y la eliminación.

Acceso de AWS al contenido del cliente

AWS pone a disposición de cada cliente los servicios de cómputo, almacenamiento, base de datos, redes u otros, como se describe en nuestro sitio web. Los clientes tienen una serie de opciones para cifrar su contenido cuando usan los servicios, incluido el uso de funciones de cifrado de AWS (como AWS KMS), la administración de sus propias claves de cifrado o el uso de un mecanismo de cifrado de un tercero de su propia elección. AWS no accede a ni utiliza el contenido del cliente sin el consentimiento del cliente, excepto cuando así lo exija la ley. AWS nunca utiliza el contenido del cliente ni obtiene información de él para otros fines, como mercadeo o publicidad.

Derechos de acceso del gobierno

A menudo surgen consultas sobre los derechos de las agencias gubernamentales nacionales y extranjeras para acceder al contenido que se encuentra en los servicios en la nube. Los clientes con frecuencia están confundidos acerca de los problemas de soberanía de los datos, incluido si los gobiernos pueden tener acceso a su contenido y en qué circunstancias. Las leyes locales que se aplican en la jurisdicción donde se encuentra el contenido son una consideración importante para algunos clientes. Sin embargo, los clientes también deben considerar si las leyes de otras jurisdicciones pueden aplicarse a ellos. Los clientes deben buscar la asesoría de sus asesores para comprender la aplicación de las leyes pertinentes a sus negocios y operaciones.

Política de AWS sobre la concesión de acceso gubernamental

AWS está atento a la seguridad de los clientes y no divulga ni mueve datos en respuesta a una solicitud de los EE. UU. u otro gobierno, a menos que se le exija legalmente para cumplir con una orden legalmente válida y vinculante, como una citación o una orden judicial, o según lo requiera la ley aplicable. Los organismos reguladores o no gubernamentales generalmente deben usar procesos internacionales reconocidos, como los Tratados de Asistencia Legal Mutua con el gobierno de los EE. UU., para obtener órdenes válidas y vinculantes.

Además, AWS notifica a los clientes cuando es factible antes de divulgar su contenido para que los clientes puedan buscar protección contra la divulgación, a menos que AWS tenga prohibido hacerlo por ley o exista una clara indicación de conducta ilegal en relación con el uso de los servicios de AWS. Para obtener información adicional, consulte el Portal de Solicitudes de Información de Amazon en línea.

Consideraciones comunes de privacidad y protección de datos

Muchos países tienen leyes diseñadas para proteger la privacidad de los datos personales. Algunos países tienen una ley integral de protección de datos, mientras que otros abordan la protección de datos de una manera más comedida, a través de una variedad de leyes y reglamentos. Si bien los requisitos legales y reglamentarios difieren — incluido debido a los requisitos jurisdiccionales, los requisitos específicos de la industria y los requisitos específicos del contenido — existen algunas consideraciones comunes que surgen de varias leyes de protección de datos punteras. Estos pueden alinearse con el ciclo de vida típico de los datos personales.

Para ayudar a los clientes a analizar y abordar sus requisitos de privacidad y protección de datos cuando usan AWS para almacenar y procesar contenido que contiene datos personales, este documento técnico analiza varias etapas de este ciclo de vida de datos, identifica consideraciones clave relevantes para cada etapa y proporciona información relevante sobre cómo operan los servicios de AWS.

Muchas leyes de protección de datos asignan responsabilidades con respecto a cómo una parte interactúa con los datos personales y el nivel de acceso y control que tienen sobre esos datos personales. Un enfoque común es distinguir entre el responsable del tratamiento, el encargado del tratamiento y el titular de los datos. La terminología utilizada en diferentes jurisdicciones puede variar y algunas leyes hacen distinciones más sutiles.

AWS reconoce que sus servicios se utilizan en muchos contextos diferentes para diferentes fines comerciales y que puede haber varias partes involucradas en el ciclo de vida de los datos personales incluidos en el contenido del cliente almacenado o procesado mediante AWS. Para simplificar, la guía de la siguiente tabla asume que, en el contexto del contenido del cliente almacenado o procesado mediante AWS, el cliente:

- Recopila datos personales de sus usuarios finales u otras personas (los titulares de los datos) y determina el propósito para el cual el cliente requiere y utilizará los datos personales.
- Tiene la capacidad de controlar quién puede acceder, actualizar y utilizar los datos personales.
- Gestiona la relación con la persona a quien corresponden los datos personales (referido en esta sección como el titular de los datos), incluso comunicándose con el titular de los datos según sea necesario para cumplir con los requisitos

relevantes de divulgación y consentimiento.

Como tal, el cliente desempeña un papel similar al del responsable, ya que controla su contenido y toma decisiones sobre el tratamiento de ese contenido, incluido quién está autorizado para procesar ese contenido en su nombre. En comparación, AWS desempeña una función similar a la del encargado, porque AWS utiliza el contenido del cliente solo para proporcionar los servicios de AWS seleccionados por cada cliente a ese cliente y no utiliza el contenido del cliente para otros fines sin el consentimiento del cliente.

> Tenga en cuenta que los términos "responsable" y "encargado" tienen un significado muy distintivo bajo la legislación de la UE, y este documento técnico no pretende abordar los requisitos específicos de la UE.

Cuando un cliente procesa datos personales utilizando los servicios de AWS en nombre y de acuerdo con las instrucciones de un tercero (que puede ser el responsable del tratamiento de los datos personales u otro tercero con el que tenga una relación comercial), las responsabilidades del cliente a los que se hace referencia en la siguiente tabla serán compartidos y administrados entre el cliente y ese tercero.

Tabla 1: Resumen, ejemplos y consideraciones de la etapa del ciclo de vida de los datos

Etapa del ciclo de vida de los datos	Resumen y ejemplos	Consideraciones
Recopilación de datos personales	Puede ser apropiado o necesario informar a las personas (los titulares de los datos) o solicitar su consentimiento antes de recopilar sus datos personales. Esto puede incluir una notificación sobre el propósito para el cual se recopilará, utilizará o divulgará su información.	**Cliente**: El cliente determina y controla cuándo, cómo y por qué recopila datos personales de las personas y decide si incluirá esos datos personales en el contenido del cliente que almacena o procesa mediante los servicios de AWS. Es posible que el cliente deba revelar los fines para los que recopila esos datos a los interesados pertinentes, obtener los datos de una fuente permitida y utilizar los datos solo para un propósito permitido. Entre el cliente y AWS, el cliente tiene una relación con las personas cuyos datos personales almacena en AWS y, por lo tanto, el cliente puede comunicarse directamente con AWS sobre la recopilación y el tratamiento de sus datos personales.

Etapa del ciclo de vida de los datos	Resumen y ejemplos	Consideraciones
	Los requisitos pueden diferir según de quién se recopilan los datos personales (por ejemplo, los requisitos pueden diferir si los datos personales se recopilan de una fuente de terceros en lugar de directamente del individuo).	El cliente, en lugar de AWS, también conoce el alcance de las notificaciones enviadas o los consentimientos obtenidos por el cliente de dichas personas en relación con la recopilación de sus datos personales. **AWS**: AWS no recopila datos personales de individuos cuyos datos personales están incluidos en el contenido que un cliente almacena o procesa mediante AWS, y AWS no tiene contacto con esas personas. Por lo tanto, AWS no puede comunicarse con las personas pertinentes en estas circunstancias.
	La recopilación de datos personales solo puede permitirse si es para un propósito válido o razonable.	AWS utiliza el contenido del cliente solo para proporcionar los servicios de AWS seleccionados por cada cliente a ese cliente y no utiliza el contenido del cliente para otros fines sin el consentimiento del cliente.
Uso y divulgación de datos personales	Puede ser apropiado o necesario usar o divulgar datos personales solo para el propósito para el cual fueron recopilados.	**Cliente**: El cliente determina y controla por qué recopila datos personales, para qué se utilizarán, quién puede utilizarlos y a quién se divulgan. El cliente debe asegurarse de que solo lo hace para los fines permitidos. El cliente sabrá si utiliza los servicios de AWS para almacenar o procesar el contenido del cliente que contiene datos personales y, por lo tanto, está en mejores condiciones para informar a las personas que utilizará AWS como proveedor de servicios, si es necesario. **AWS**: AWS utiliza el contenido del cliente solo para proporcionar los servicios de AWS seleccionados por cada cliente a ese cliente y no utiliza el contenido del cliente para otros fines sin el consentimiento del cliente.

Etapa del ciclo de vida de los datos	Resumen y ejemplos	Consideraciones
Deslocalización de datos personales	Si se transfieren datos personales al extranjero, puede ser necesario o adecuado informar a las personas (los titulares de los datos) de los países en los que el cliente almacenará sus datos personales y/o solicitar el consentimiento para almacenar sus datos personales en esa ubicación. También puede ser importante considerar las protecciones comparables que ofrece el régimen de privacidad en el país pertinente donde residirán los datos personales.	**Cliente**: El cliente puede elegir la región o regiones de AWS en las que se ubicará su contenido y puede elegir implementar sus servicios de AWS exclusivamente en una sola región si lo prefiere. El cliente debe considerar si debe revelar a las personas las ubicaciones en las que almacena o procesa sus datos personales y obtener los consentimientos necesarios relacionados con dichas ubicaciones de las personas pertinentes, si es necesario. Igual que entre el cliente y AWS, el cliente tiene una relación con las personas cuyos datos personales almacena el cliente en AWS y, por lo tanto, el cliente puede comunicarse directamente con ellos acerca de dichos asuntos. **AWS**: AWS almacena y procesa el contenido de cada cliente solo en la(s) región(es) de AWS, y utilizando los servicios, elegidos por el cliente y, de otro modo, no moverá el contenido del cliente sin el consentimiento del cliente, excepto según lo exija la ley. Si un cliente elige almacenar contenido en más de una Región, o copiar o mover contenido entre Regiones, esa es la elección exclusiva del cliente, y el cliente continuará manteniendo un control efectivo de su contenido, donde sea que se almacene y procese. **General**: AWS cuenta con la Certificación ISO 27001 y ofrece sólidas funciones de seguridad a todos los clientes, independientemente de la región geográfica en la que almacenen su contenido.
Protección de datos personales	Es importante tomar medidas para proteger la seguridad de los datos personales.	**Cliente**: Los clientes son responsables de la seguridad *en* la nube, incluida la seguridad de su contenido (y los datos personales incluidos en su contenido).

Etapa del ciclo de vida de los datos	Resumen y ejemplos	Consideraciones
		Ejemplos de pasos que los clientes pueden tomar para ayudar a proteger su contenido incluyen implementar políticas de contraseñas seguras, asignar permisos apropiados a los usuarios y tomar medidas sólidas para proteger sus claves de acceso, así como firewalls y segmentación de red apropiados, encriptar contenido y diseñar adecuadamente los sistemas para reducir el riesgo de pérdida de datos y acceso no autorizado. **AWS**: AWS es responsable de administrar la seguridad *del* entorno de nube subyacente. Para obtener una lista completa de todas las medidas de seguridad integradas en la infraestructura y los servicios centrales de la nube de AWS, consulte el documento técnico Introducción a la Seguridad de AWS . Los clientes pueden validar los controles de seguridad establecidos dentro del entorno de AWS a través de las certificaciones e informes de AWS, incluidos los informes de Control de organizaciones y sistemas de AWS (SOC por sus siglas en inglés) 1, 2 y 3 , certificaciones ISO 27001, 27017, 27018, 27701 y Declaración de cumplimiento de PCI DSS.

Etapa del ciclo de vida de los datos	Resumen y ejemplos	Consideraciones
Acceso y corrección de datos personales	Las personas (los titulares de los datos) pueden tener derecho a acceder a sus datos personales, incluso con el fin de corregirlos.	**Cliente**: El cliente retiene el control del contenido almacenado o procesado mediante AWS, incluido el control sobre cómo se protege ese contenido y quién puede acceder y modificar ese contenido. Además, entre el cliente y AWS, el cliente tiene una relación con las personas cuyos datos personales se incluyen en el contenido del cliente almacenado o procesado mediante los servicios de AWS. Por lo tanto, el cliente, en lugar de AWS, puede trabajar con personas relevantes para brindarles acceso y la capacidad de corregir los datos personales incluidos en el contenido del cliente.

Etapa del ciclo de vida de los datos	Resumen y ejemplos	Consideraciones
		AWS: AWS utiliza el contenido del cliente solo para proporcionar los servicios de AWS seleccionados por cada cliente a ese cliente o según el consentimiento del cliente. AWS no tiene una relación directa con las personas cuyos datos personales se incluyen en el contenido que un cliente almacena o procesa mediante los servicios de AWS. Dado esto, y el nivel de control que los clientes disfrutan sobre el contenido del cliente, AWS no brinda a las personas acceso a sus datos personales ni la capacidad de corregirlos.
Mantenimiento de la calidad de los datos personales.	Puede ser importante garantizar que los datos personales sean precisos y que se mantenga la integridad de esos datos personales.	**Cliente**: Cuando un cliente elige almacenar o procesar contenido que contiene datos personales mediante AWS, el cliente tiene control sobre la calidad de ese contenido y conserva el acceso y puede corregirlo. Esto significa que el cliente puede mantener los datos personales incluidos en el contenido del cliente precisos, completos, no engañosos y actualizados. **AWS**: El informe AWS SOC 1, Tipo 2 incluye controles que brindan una garantía razonable de que la integridad de los datos se mantiene en todas las fases, incluida la transmisión, el almacenamiento y el procesamiento.
Eliminación o despersonalización de datos personales	Por lo general, los datos personales no deben conservarse durante más tiempo del razonablemente necesario y, de lo contrario, deben conservarse de acuerdo con las leyes de conservación de datos pertinentes.	**Cliente**: Solo el cliente sabe por qué se recopilaron los datos personales incluidos en el contenido del cliente almacenado en AWS, y solo el cliente sabe cuándo ya no es necesario conservar esos datos personales para fines legítimos. El cliente debe eliminar o anonimizar los datos personales cuando ya no los necesite. **AWS**: Los servicios de AWS brindan al cliente controles para permitirle eliminar contenido, como se describe en la Documentación de AWS.

Violaciones de privacidad

Dado que los clientes mantienen el control de su contenido cuando usan AWS, los clientes conservan la responsabilidad de monitorear su propio entorno en busca de violaciones de privacidad y notificar a los reguladores y a las personas afectadas según lo exige la ley aplicable. Sólo el cliente puede gestionar esta responsabilidad.

Por ejemplo, los clientes controlan las claves de acceso y determinan quién está autorizado para acceder a su cuenta de AWS. AWS no tiene visibilidad de las claves de acceso, o quién está y quién no está autorizado para iniciar sesión en una cuenta. Por lo tanto, el cliente es responsable de monitorear el uso, mal uso, distribución o pérdida de las claves de acceso.

En algunas jurisdicciones, es obligatorio notificar a las personas o a un regulador sobre el acceso no autorizado o la divulgación de sus datos personales. Hay circunstancias en las que notificar a las personas será el mejor enfoque para mitigar el riesgo, aunque no sea obligatorio según la ley aplicable. El cliente determina cuándo es apropiado o necesario para ellos notificar a las personas y el proceso de notificación que seguirán.

Consideraciones

Los clientes deben considerar los requisitos específicos que se les aplican, incluidos los requisitos específicos de la industria. Las leyes y regulaciones de privacidad y protección de datos relevantes aplicables a clientes individuales dependen de varios factores, incluido el lugar donde un cliente realiza negocios, la industria en la que opera, el tipo de contenido que desea almacenar, dónde o de quién se origina el contenido, y donde se almacenará el contenido.

Los clientes preocupados por sus obligaciones reglamentarias de privacidad primero deben asegurarse de identificar y comprender los requisitos que se les aplican y buscar el asesoramiento adecuado.

Conclusión

Para AWS, la seguridad es siempre la máxima prioridad. AWS brinda servicios a millones de clientes activos, incluidas empresas, instituciones educativas y agencias gubernamentales en más de 190 países. Los clientes de AWS incluyen proveedores de servicios financieros y prestadores de atención en salud, y confían en AWS con parte de su información más confidencial.

Los servicios de AWS están diseñados para brindar a los clientes flexibilidad sobre cómo configuran y despliegan sus soluciones y cómo controlan su contenido, incluido dónde se almacena, cómo se almacena y quién tiene acceso a él. Los clientes de AWS pueden crear sus propias aplicaciones seguras y almacenar contenido de forma segura en AWS.

Colaboradores

Los colaboradores de este documento incluyen:

- Simon Hollander, AWS Legal, Senior Corporate Counsel
- Jonathan Hatae, AWS Legal, Senior Corporate Counsel

Otras lecturas

Para ayudar a los clientes a comprender mejor cómo pueden abordar sus requisitos de privacidad y protección de datos, se recomienda a los clientes que lean los documentos técnicos, las mejores prácticas, las listas de verificación y la orientación sobre riesgo, cumplimiento y seguridad publicados en el sitio web de AWS. Este material se puede encontrar en:

- http://aws.amazon.com/compliance
- http://aws.amazon.com/security

A la fecha de este escrito, también están disponibles documentos técnicos específicos sobre consideraciones de privacidad y protección de datos para los siguientes países o regiones:

- California
- Unión Europea
- Alemania
- Australia
- Hong Kong
- Japón
- Malasia
- Nueva Zelanda

- Filipinas
- Singapur

AWS también ofrece capacitación para ayudar a los clientes a aprender cómo diseñar, desarrollar y operar aplicaciones disponibles, eficientes y seguras en la nube de AWS, y adquirir competencia con los servicios y soluciones de AWS. AWS ofrece videos instructivos gratuitos, laboratorios a su propio ritmo, y clases dirigidas por un instructor.

Más información sobre la capacitación de AWS está disponible en: http://aws.amazon.com/training/.

Las certificaciones de AWS certifican las habilidades técnicas y los conocimientos asociados con las mejores prácticas para crear aplicaciones seguras y confiables basadas en la nube mediante la tecnología de AWS.

Más información sobre las certificaciones de AWS está disponible en: http://aws.amazon.com/certification/.

Si requiere más información, comuníquese con AWS en: https://aws.amazon.com/contact-us/ o comuníquese con su representante local de cuentas de AWS.

Revisiones de documentos

Fecha	Descripción
Mayo, 2022	Primera Publicación en español