Seguridad a escala: Inicio de sesión en AWS

Cómo AWS CloudTrail puede ayudarle a alcanzar la conformidad registrando llamadas API y cambios en los recursos

Octubre de 2015

(Consulte https://aws.amazon.com/compliance/aws-whitepapers/

para obtener la versión más reciente de este documento)

Índice

Resumen

El registro y la monitorización de las llamadas API son componentes clave de las prácticas recomendadas de seguridad y operativas, así como requisitos de conformidad del sector y normativo. AWS CloudTrail es un servicio web que registra las llamadas API a servicios de AWS admitidos en su cuenta de AWS y deja un archivo de registro en el bucket de Amazon Simple Storage Service (Amazon S3). AWS CloudTrail alivia los problemas habituales propios de un entorno local y, además de que resulta más sencillo demostrar conformidad con las políticas o los estándares normativos, el servicio permite mejorar fácilmente los procesos de seguridad y operativos.

En este documento se ofrece información general acerca de los requisitos de conformidad relacionados con el registro y detalles sobre las características de AWS CloudTrail que pueden ayudar a satisfacer estos requisitos. Aparte de los cargos estándar de S3 para el almacenamiento de registros y el uso de SNS para las notificaciones opcionales, AWS CloudTrail se ofrece sin cargo adicional.

Introducción

Amazon Web Services (AWS) ofrece recursos y servicios de TI bajo demanda muy diversos que puede lanzar y gestionar con un modelo de precios de pago por uso. El registro de las llamadas API de AWS y los cambios asociados en la configuración de los recursos es un componente esencial de la gobernanza, la seguridad y la conformidad de TI. AWS CloudTrail ofrece una solución sencilla para registrar las llamadas API y los cambios en los recursos de AWS que contribuye a reducir la carga que suponen los problemas de la infraestructura y el almacenamiento locales al ayudarle a crear controles de seguridad preventivos y de detección mejorados para el entorno de AWS. Las soluciones de registro local requieren la instalación de agentes, el ajuste de archivos de configuración y servidores de registro centralizados, así como la creación y el mantenimiento de costosos almacenes de datos de larga duración para almacenar los datos. AWS CloudTrail elimina esta configuración de infraestructura excesivamente costosa y permite activar el registro con solo dos clics y tener mayor visibilidad de todas las llamadas API en su cuenta de AWS. CloudTrail captura continuamente las llamadas API de varios servidores en una canalización de procesamiento de alta disponibilidad. Para activar CloudTrail, basta con iniciar sesión en la consola de administración de AWS, navegar hasta la consola de CloudTrail y hacer clic para habilitar el registro. Para obtener más información acerca de los servicios y las regiones disponibles con AWS CloudTrail, visite el sitio web de AWS CloudTrail.

Para elaborar este documento se ha realizado un inventario de los requisitos de registro de los marcos de conformidad más frecuentes (como ISO 27001:2005, PCI DSS v2.0, FedRAMP, etc.) y se han combinado con los controles y dominios de registro generalizados. Puede aprovechar este documento para una amplia variedad de casos de uso, como prácticas recomendadas de seguridad y operativas, conformidad con políticas internas, estándares del sector, normativas legales y mucho más. El presente documento se ha escrito de forma genérica para que todos los usuarios entiendan cómo AWS CloudTrail puede mejorar sus actividades actuales de registro y monitorización.

Control del acceso a los archivos de registro

Para mantener la integridad de los datos de registro, es importante gestionar racionalmente el acceso en lo referente a la generación y el almacenamiento de los archivos de registro. La capacidad de ver o modificar los datos de registro debe restringirse a los usuarios autorizados exclusivamente. En los entornos locales, un problema frecuente relacionado con el registro es la capacidad de demostrar a los reguladores que el acceso a los datos de registro está restringido a los usuarios autorizados. Este control puede llevar mucho tiempo y ser difícil de demostrar eficazmente porque la mayoría de los entornos locales no cuentan con una solución única de registro o una seguridad de registro coherente en todos los sistemas.

Con AWS CloudTrail, el acceso a los archivos de registro de Amazon S3 se controla de forma centralizada en AWS, lo que le permite controlar fácilmente el acceso a los archivos de registro y ayuda a demostrar la integridad y la confidencialidad de los datos de registro.

	Requisitos de registro comunes	Cómo AWS CloudTrail puede ayudarle a alcanzar la conformidad con los requisitos
Control del acceso a los archivos de registro	Existen controles para impedir el acceso no autorizado a los registros.	AWS CloudTrail le ofrece la posibilidad de restringir el acceso a los archivos de registro. Para impedir y controlar el acceso a fin de realizar cambios en los datos de los archivos de registro, puede configurar roles de AWS Identity and Access Management (IAM) y políticas de bucket de Amazon S3 para aplicar el acceso de solo lectura a los archivos de registro. Más información. Además, puede reforzar los controles de autenticación y autorización si habilita AWS Multi-Factor Authentication (AWS MFA) en los buckets de Amazon S3 en los que se almacenan los registros de AWS CloudTrail. Más información.
	Existen controles para garantizar que el acceso a los registros se basa en roles.	AWS CloudTrail ofrece la posibilidad de controlar el acceso de los usuarios a sus archivos de registro según un aprovisionamiento detallado basado en roles. AWS Identity and Access Management (IAM) permite controlar de forma segura el acceso a AWS CloudTrail de los usuarios; además, mediante roles de IAM y políticas de bucket de Amazon S3, se puede aplicar el acceso basado en roles al bucket de S3 donde se almacenan los archivos de registro de AWS CloudTrail. Más información.

Obtención de alertas sobre la creación y configuración errónea de los archivos de registro

Las alertas casi en tiempo real para indicar configuraciones erróneas en los registros que detallan las llamadas API o los cambios en los recursos son muy importantes para lograr una gobernanza de TI eficaz y la conformidad con los requisitos tanto internos como externos. Incluso desde una perspectiva operativa, es imprescindible que el registro esté configurado correctamente para que pueda supervisar las actividades de sus usuarios y recursos. No obstante, dada la variabilidad y la amplia gama de infraestructuras de registro presentes en los entornos locales, la monitorización y la notificación activas cuando hay errores de configuración o cambios en la configuración de registro son tareas abrumadoras.

Una vez habilitado AWS CloudTrail para su cuenta, el servicio entrega los archivos de registro en su bucket de S3. Si lo prefiere, CloudTrail publicará notificaciones de entrega de archivos de registro en un tema de SNS para que pueda tomar alguna medida al respecto. Estas alertas incluyen la dirección de los archivos de registro en el bucket de Amazon S3 para que pueda acceder rápidamente a los metadatos de los objetos sobre el evento en los archivos de registro de origen. Además, la consola de administración de AWS le avisará si los archivos de registro están mal configurados y, por tanto, se va a dejar de realizar el registro.

	Requisitos de registro comunes	Cómo AWS CloudTrail puede ayudarle a alcanzar la conformidad con los requisitos
Recepción de alertas sobre la creación y configuración errónea de los archivos de registro	Proporcionar alertas cuando se crean o no se crean registros y seguir las medidas definidas por la organización en caso de que haya una configuración errónea.	AWS CloudTrail le ofrece notificaciones inmediatas relacionadas con la existencia de problemas en la configuración del registro a través de la consola de administración de AWS. Más información.
	Las alertas relacionadas con una configuración errónea del registro remitirán a los usuarios a los registros pertinentes para obtener más información (y no divulgarán una cantidad innecesaria de detalles).	AWS CloudTrail registra la dirección de los archivos de registro del bucket de Amazon S3 cada vez que se escribe un nuevo archivo de registro. AWS CloudTrail publica notificaciones sobre la creación de archivos de registro de forma que los clientes puedan tomar medidas casi en tiempo real cuando se crean estos archivos. La notificación se entrega al bucket de Amazon S3 y se muestra en la consola de administración de AWS. Si lo prefiere, se pueden enviar mensajes de Amazon SNS a dispositivos móviles o servicios distribuidos, configurados a través de API o de la consola de administración de AWS. El mensaje de SNS sobre la creación de un archivo de registro incluye la dirección del archivo de registro, que solo divulga la cantidad de información necesaria y también le permite seguir fácilmente un enlace para obtener detalles adicionales del evento. Más información.

Administración de cambios en los recursos y los archivos de registro de AWS

Un componente esencial de la gobernanza y la seguridad de TI consiste en comprender los cambios realizados en los recursos. Además, la prevención de cambios y accesos no autorizados a estos datos de registro afecta directamente a la integridad de los procesos de gestión de cambios y a su capacidad para cumplir con los requisitos internos, del sector y normativos sobre la gestión de cambios. Un problema grave al que se enfrentan los entornos locales es la capacidad de registrar los cambios en los recursos o en los registros, ya que solo se dispone de recursos finitos para monitorizar lo que parece una cantidad infinita de datos.

AWS CloudTrail permite hacer un seguimiento de los cambios realizados en un recurso de AWS, incluida su creación, modificación y eliminación. Además, al examinar el historial de registro de llamadas API, AWS CloudTrail ayuda a investigar un evento para determinar si se realizaron cambios no autorizados o inesperados viendo quién los inició, cuándo se hicieron y dónde se originaron. Si lo prefiere, cuando llegue un nuevo archivo de registro a su bucket de Amazon S3, CloudTrail publicará notificaciones en un tema de SNS para que pueda tomar alguna medida al respecto.

	Requisitos de registro comunes	Cómo AWS CloudTrail puede ayudarle a alcanzar la conformidad con los requisitos
Administración de cambios en los recursos de TI y los archivos de registro	Proporcionar un registro de cambios en los componentes del sistema (incluida la creación y eliminación de objetos de nivel del sistema).	AWS CloudTrail genera datos de registro sobre los eventos de cambios en el sistema para permitir hacer un seguimiento de los cambios realizados en los recursos de AWS. AWS CloudTrail permite ver los cambios realizados en los recursos de AWS desde su creación hasta su eliminación; para ello, registra los cambios efectuados mediante llamadas API a través de la consola de administración de AWS, la interfaz de línea de comandos (CLI) de AWS o los kits de desarrollo de software (SDK) de AWS. Más información.
	Existen controles para impedir modificaciones a los registros de cambios o errores asociados a los registros.	De forma predeterminada, los archivos de registro de llamadas API se cifran mediante Cifrado en el servidor (SSE) de S3 y se colocan en su bucket de S3. Se pueden controlar las modificaciones a los datos de registro mediante el uso de IAM y MFA para aplicar acceso de solo lectura al bucket de Amazon S3 en el que se almacenan los archivos de registro de AWS CloudTrail. Más información.

Almacenamiento de archivos de registro

Los estándares del sector y las normativas legales pueden requerir que los archivos de registro se almacenen durante distintos períodos de tiempo. Por ejemplo, PCI DSS exige almacenar los registros durante un año, HIPAA requiere que los registros se conserven seis años como mínimo y otros requisitos exigen períodos de almacenamiento más largos o variables en función de los datos que se registran. Por tanto, la gestión de los requisitos de almacenamiento de archivos de registro para diferentes datos en distintos sistemas puede suponer una carga administrativa y tecnológica. Además, el almacenamiento y archivado de grandes volúmenes de datos de registro de forma persistente y segura puede suponer un problema para muchas organizaciones.

AWS CloudTrail está diseñado para integrarse a la perfección con Amazon S3 y Amazon Glacier, lo que permite personalizar los buckets y las reglas del ciclo de vida de S3 según sus necesidades de almacenamiento. AWS CloudTrail ofrece un período de vencimiento indefinido para los registros, de forma que puede personalizar el período de tiempo durante el que almacena los registros para cumplir los requisitos de los reguladores.

	Requisitos de registro comunes	Cómo AWS CloudTrail puede ayudarle a alcanzar la conformidad con los requisitos
Almacenamiento de archivos de registro	Los registros se almacenan durante un año como mínimo.	Para facilitar el almacenamiento de archivos de registro, puede configurar AWS CloudTrail para agregar los archivos de registro de todas las regiones o de varias cuentas en un único bucket de S3. AWS CloudTrail ofrece la posibilidad de personalizar el período de almacenamiento de registros configurando los períodos de vencimiento deseados en los archivos de registro que se graban en su bucket de Amazon S3. Usted es quien controla las políticas de retención de los archivos de registro de CloudTrail. Puede conservar los archivos de registro durante el período de tiempo que desee o de forma indefinida. De forma predeterminada, los archivos de registro se almacenan indefinidamente. Si desea un ahorro mayor en los costos asociados al almacenamiento en frío, también puede mover los datos de los archivos de registro a Amazon Glacier. Más información.
	Almacenar los registros durante un período de tiempo definido por la organización.	
	Almacenar los registros en tiempo real para obtener una mayor resistencia.	AWS CloudTrail ofrece resistencia de los archivos de registro al utilizar Amazon S3, una infraestructura de almacenamiento de larga duración. El almacenamiento estándar de Amazon S3 está diseñado para tener una durabilidad del 99,999999999% y una disponibilidad de los objetos del 99,99% durante un año concreto. Más información.

Generación de informes personalizados de datos de registro

Desde una perspectiva operativa y de seguridad, el registro de llamadas API ofrece los datos y el contexto necesarios para analizar el comportamiento de los usuarios y entender determinados eventos. Las llamadas API y los registros de cambios en los recursos de TI pueden utilizarse también para demostrar que solo los usuarios autorizados han realizado determinadas tareas en su entorno, como exigen los requisitos de conformidad. Sin embargo, dado el volumen y la variabilidad asociados a los registros de diferentes sistemas, en un entorno local puede ser difícil hacerse una idea clara de las actividades que los usuarios han realizado y los cambios que se han efectuado en los recursos de TI.

AWS CloudTrail genera datos que puede utilizar para detectar comportamientos anormales, recuperar actividades de eventos asociadas a determinados objetos o proporcionar un seguimiento de auditoría simple para su cuenta. Puede desarrollar los análisis de registro actuales con los más de 25 campos diferentes de los datos de eventos que AWS CloudTrail ofrece para crear consultas y crear informes personalizados centrados en investigaciones internas, conformidad externa, etc. AWS CloudTrail le permite monitorizar las llamadas API para ver si hay determinados comportamientos no deseados conocidos y generar alarmas mediante la gestión de registros o soluciones de gestión de eventos e incidencias de seguridad (SIEM). Los datos enriquecidos que AWS CloudTrail proporciona pueden acelerar el tiempo de investigación y reducir el tiempo de respuesta ante incidencias. Además, los datos proporcionados por AWS CloudTrail le permiten realizar un análisis de seguridad más profundo en las llamadas API para identificar comportamientos sospechosos y patrones latentes que no activan alarmas inmediatas pero que pueden representar un problema para la seguridad.
Por último, AWS CloudTrail colabora con una gran variedad de socios que disponen de soluciones listas para ejecutar de seguridad, análisis y alertas. Hay más información acerca de las soluciones de nuestros socios en el sitio web de AWS CloudTrail.

Generación de informes personalizados de datos de registro	**Requisitos de registro comunes**	**Cómo AWS CloudTrail puede ayudarle a alcanzar la conformidad con los requisitos**
	Registrar el acceso de los usuarios individuales a los recursos, por sistema al que han accedido y medidas tomadas. “Acceso de los usuarios individuales” incluye el acceso por parte de los administradores del sistema y los operadores del sistema; “Recursos” incluye los registros de seguimiento de auditoría.	AWS CloudTrail ofrece la posibilidad de generar informes de llamadas API completos y detallados al registrar las actividades que realizan todos los usuarios que acceden a sus recursos registrados de AWS, incluido el raíz, usuarios de IAM, usuarios federados y cualquier usuario o servicio que lleve a cabo actividades en nombre de otros usuarios, mediante cualquier método de acceso. Más información.
	Producir registros con una frecuencia definida por la organización.	AWS CloudTrail ofrece la posibilidad de utilizar herramientas de análisis de registros para recuperar datos de los archivos de registro con frecuencias personalizadas mediante la creación de registros en tiempo casi real y la entrega de los datos de registro en el bucket de Amazon S3 15 minutos después de la llamada API. Puede utilizar los archivos de registro como entrada en las principales soluciones de análisis y gestión de registros del sector para realizar análisis. Más información.
	Proporcionar un registro de cuándo se inició la actividad de registro.	AWS CloudTrail registra todas las llamadas API, incluida las empleadas para habilitar y deshabilitar el registro de AWS CloudTrail. Esto le permite hacer un seguimiento de cuándo se activó o desactivó el propio CloudTrail. Más información.
	Generar registros sincronizados con un único reloj interno del sistema para proporcionar información coherente de marca de tiempo.	AWS CloudTrail produce datos de registro a partir de un único reloj interno del sistema generando marcas de tiempo de eventos según la Hora universal coordinada (UTC), coherente con el estándar ISO 8601 de formato de hora y fecha básico. Más información.

Proporcionar registros que pueden mostrar si se ha realizado alguna actividad inadecuada o inusual.	Con AWS CloudTrail se puede monitorizar las llamadas API registrando los errores de autorización en su cuenta de AWS, lo que le permite hacer un seguimiento de los intentos de acceso a recursos restringidos o de otras actividades inusuales. Más información.
Proporcionar registros con detalles de eventos suficientes.	AWS CloudTrail ofrece información detallada de las llamadas API como el tipo, la fecha y la hora, la ubicación, el origen, el resultado (incluidas excepciones, errores e información de eventos de seguridad), el recurso afectado (datos, sistema, etc.) y el usuario asociado. AWS CloudTrail puede ayudarle a identificar el usuario, la hora del evento, la dirección IP del usuario, los parámetros de solicitud proporcionados por el usuario, los elementos de respuesta devueltos por el servicio, y el código y el mensaje de error opcionales. Más información.

Conclusión

En AWS se puede ejecutar prácticamente todo lo que se ejecuta de forma local: sitios web, aplicaciones, bases de datos, aplicaciones móviles, campañas de correo electrónico, análisis de datos distribuidos, almacenamiento y redes privadas. Los servicios que AWS ofrece están diseñados para funcionar conjuntamente, por lo que puede crear soluciones completas. AWS CloudTrail ofrece una solución simple para registrar la actividad de los usuarios, lo que ayuda a reducir la carga que supone gestionar un sistema de registro complejo. Otro beneficio de la migración de cargas de trabajo a AWS es la posibilidad de conseguir un nivel superior de seguridad, a escala, utilizando las numerosas características de gobernanza que se ofrecen. Por los mismos motivos que la entrega de infraestructura en la nube tiene beneficios respecto a la entrega local, la gobernanza basada en la nube ofrece un costo menor de entrada, operaciones más sencillas y mayor agilidad al proporcionar más visibilidad, control de seguridad y automatización central. AWS CloudTrail es uno de los servicios que puede utilizar para conseguir un alto nivel de gobernanza de los recursos de TI que utilizan AWS.

Recursos adicionales

A continuación se incluyen unos enlaces que dan respuesta a las preguntas frecuentes relacionadas con el registro en AWS:

- ¿Qué puedo hacer con AWS? Más información.
- ¿Cómo puedo empezar a utilizar AWS? Más información.
- ¿Cómo puedo empezar a utilizar AWS CloudTrail? Más información.
- ¿Tiene AWS CloudTrail una lista de preguntas frecuentes? Más información.
- ¿Cómo puedo conseguir la conformidad cuando utilizo AWS? Más información.
- ¿Cómo puedo prepararme para una auditoría mientras utilizo AWS? Más información.

Apéndice: Índice del programa de conformidad

La información del documento técnico anterior se presentaba por dominios de requisitos de registro. Para su referencia, en la tabla siguiente se enumeran los requisitos de registro por marcos comunes de conformidad:

Programa de conformidad de AWS	Requisito de conformidad
Nivel 1 del estándar de seguridad de datos (DSS) del sector de las tarjetas de pago (PCI) AWS ha alcanzado el Nivel 1 de conformidad con el estándar PCI DSS. Puede ejecutar aplicaciones en nuestra infraestructura tecnológica conforme a PCI para almacenar, procesar y transmitir información de tarjetas de crédito en la nube. Más información.	**PCI 5.2:** Asegurarse de que todos los mecanismos antivirus están actualizados, se ejecutan de forma activa y generan registros de auditoría.
	PCI 10.1: Establecer un proceso para enlazar todos los accesos a los componentes del sistema (especialmente los accesos realizados con privilegios administrativos como el raíz) a cada usuario individual.
	PCI 10.2: Implementar seguimientos de auditoría automatizados para todos los componentes del sistema a fin de reconstruir los eventos siguientes: **10.2.1:** Todos los accesos individuales a datos de titulares de tarjetas **10.2.2:** Todas las medidas que adopta un usuario que tiene privilegios raíz o administrativos **10.2.3:** Acceso a todos los seguimientos de auditoría **10.2.4:** Intentos no válidos de acceso lógico **10.2.5:** Uso de mecanismos de identificación y autenticación **10.2.6:** Inicialización de los registros de auditoría **10.2.7:** Creación y eliminación de objetos de nivel del sistema
	PCI 10.3: Para cada evento, registrar al menos las entradas siguientes de seguimiento de auditoría para todos los componentes del sistema: **10.3.1:** Identificación del usuario **10.3.2:** Tipo de evento **10.3.3:** Fecha y hora **10.3.4:** Indicación de éxito o de error **10.3.5:** Origen del evento **10.3.6:** Identidad o nombre de los datos, componente del sistema o recurso afectados
	PCI 10.4.2: Los datos de hora están protegidos.
	PCI 10.5: Proteger los seguimientos de auditoría para que no se puedan alterar.
	PCI 10.5.1: Limitar la visualización de seguimientos de auditoría a las necesidades relacionadas con el trabajo.
	PCI 10.5.2: Proteger los archivos de seguimiento de auditoría frente a modificaciones no autorizadas.
	PCI 10.5.3: Hacer rápidamente copia de seguridad de los archivos de seguimiento de auditoría en un servidor centralizado de registros o en medios que son difíciles de alterar.

Programa de conformidad de AWS	Requisito de conformidad
Nivel 1 del estándar de seguridad de datos (DSS) del sector de las tarjetas de pago (PCI) AWS ha alcanzado el Nivel 1 de conformidad con el estándar PCI DSS. Puede ejecutar aplicaciones en nuestra infraestructura tecnológica conforme a PCI para almacenar, procesar y transmitir información de tarjetas de crédito en la nube. Más información.	**PCI 10.5.4:** Escribir los registros de tecnologías externas en un servidor de registros de la LAN interna.
	PCI 10.5.5: Utilizar software de monitorización de la integridad de los archivos o de detección de cambios en los registros para garantizar que los datos de registro existentes no se pueden modificar sin que se generen alertas (aunque los nuevos datos que se añadan no deben provocar una alerta).
	PCI 10.6: Revisar los registros de todos los componentes del sistema una vez al día como mínimo. Las revisiones de los registros deben incluir aquellos servidores que realizan funciones de seguridad como el sistema de detección de intrusiones (IDS) y los servidores de protocolos de autenticación, autorización y contabilidad (AAA) (por ejemplo, RADIUS).
	PCI 10.7: Conservar el historial de seguimientos de auditoría durante un año al menos; debe haber un mínimo de tres meses de disponibilidad inmediata para realizar análisis (por ejemplo, en línea, archivado o que se pueda restaurar a partir de la copia de seguridad).
	PCI 11.5: Implementar herramientas de monitorización de la integridad de los archivos que avisen al personal en caso de alguna modificación no autorizada de los archivos del sistema, archivos de configuración o archivos de contenido esenciales; y configurar el software para que realice comparaciones de los archivos esenciales una vez a la semana por lo menos.
	PCI 12.2: Elaborar procedimientos diarios de seguridad operativa que sean coherentes con los requisitos de esta especificación (por ejemplo, procedimientos de mantenimiento de cuentas de usuario y procedimientos de revisión de registros).
	PCI A.1.2.d: Restringir el acceso y los privilegios de cada entidad al propio entorno de datos de titulares de tarjetas únicamente.
	PCI A.1.3: Asegurarse de que el registro y los seguimientos de auditoría están habilitados y son únicos del entorno de datos de titulares de tarjeta de cada entidad, y que son coherentes con el Requisito 10 de PCI DSS.

Programa de conformidad de AWS	Requisito de conformidad
Nivel 1 del estándar de seguridad de datos (DSS) del sector de las tarjetas de pago (PCI) AWS ha alcanzado el Nivel 1 de conformidad con el estándar PCI DSS. Puede ejecutar aplicaciones en nuestra infraestructura tecnológica conforme a PCI para almacenar, procesar y transmitir información de tarjetas de crédito en la nube. Más información.	**PCI 11.4:** Utilizar sistemas de detección y prevención de intrusiones para monitorizar todo el tráfico en el perímetro del entorno de datos de titulares de tarjetas y en los puntos importantes dentro del entorno de datos de titulares de tarjetas, y avisar al personal ante sospechas de riesgos para la seguridad. Mantener actualizados todos los motores, bases de referencia y firmas de detección y prevención de intrusiones.
	PCI 11.5: Implementar herramientas de monitorización de la integridad de los archivos que avisen al personal en caso de alguna modificación no autorizada de los archivos del sistema, archivos de configuración o archivos de contenido esenciales; y configurar el software para que realice comparaciones de los archivos esenciales una vez a la semana por lo menos.
Controles de las organizaciones de servicios 2 (SOC 2) El informe SOC 2 es un informe de certificación que amplía la evaluación de los controles conforme a los criterios establecidos por los Principios de los servicios de confianza del American Institute of Certified Public Accountants (AICPA). Estos principios definen controles de prácticas principales relacionados con la seguridad, la disponibilidad, la integridad durante el procesamiento, la confidencialidad y la privacidad, aplicables a las organizaciones de servicios, como AWS. Más información.	**Seguridad 3.2.g de SOC 2:** Existen procedimientos para restringir el acceso lógico al sistema definido incluidos, entre otros, los aspectos siguientes: Restricción de acceso a las configuraciones del sistema, funcionalidad de superusuario, contraseñas maestras, utilidades eficaces y dispositivos de seguridad (por ejemplo, firewalls).
	Seguridad 3.3 de SOC 2: Existen procedimientos para restringir el acceso físico al sistema definido incluidos, entre otros, las instalaciones, medios de copia de seguridad y otros componentes del sistema como firewalls, enrutadores y servidores.
	Seguridad 3.7 de SOC 2: Existen procedimientos para identificar, notificar y actuar en caso de infracciones de seguridad del sistema y otras incidencias.
	Disponibilidad 3.5.f de SOC 2: Existen procedimientos para restringir el acceso lógico al sistema definido incluidos, entre otros, los aspectos siguientes: Restricción de acceso a las configuraciones del sistema, funcionalidad de superusuario, contraseñas maestras, utilidades eficaces y dispositivos de seguridad (por ejemplo, firewalls).
	Disponibilidad 3.6 de SOC 2: Existen procedimientos para restringir el acceso físico al sistema definido incluidos, entre otros, las instalaciones, medios de copia de seguridad y otros componentes del sistema como firewalls, enrutadores y servidores.

Programa de conformidad de AWS	Requisito de conformidad
Controles de las organizaciones de servicios 2 (SOC 2) El informe SOC 2 es un informe de certificación que amplía la evaluación de los controles conforme a los criterios establecidos por los Principios de los servicios de confianza del American Institute of Certified Public Accountants (AICPA). Estos principios definen controles de prácticas principales relacionados con la seguridad, la disponibilidad, la integridad durante el procesamiento, la confidencialidad y la privacidad, aplicables a las organizaciones de servicios, como AWS. Más información.	**Disponibilidad 3.10 de SOC 2:** Existen procedimientos para identificar, notificar y actuar en caso de problemas de disponibilidad del sistema e infracciones de seguridad relacionadas y otras incidencias.
	Confidencialidad 3.3 de SOC 2: Los procedimientos del sistema relacionados con la confidencialidad del procesamiento de datos son coherentes con las políticas de confidencialidad documentadas.
	Confidencialidad 3.8.1 de SOC 2: Existen procedimientos para restringir el acceso lógico al sistema y a los recursos de información confidencial que se mantienen en el sistema incluidos, entre otros, los aspectos siguientes: Restricción de acceso a las configuraciones del sistema, funcionalidad de superusuario, contraseñas maestras, utilidades eficaces y dispositivos de seguridad (por ejemplo, firewalls).
	Confidencialidad 3.13 de SOC 2: Existen procedimientos para identificar, notificar y actuar en caso de infracciones de la seguridad y confidencialidad del sistema y otras incidencias.
	Confidencialidad 4.2 de SOC 2: Existe un proceso para identificar y abordar posibles deficiencias en la capacidad continua de la entidad de conseguir sus objetivos de acuerdo con sus políticas de confidencialidad del sistema y las políticas de seguridad relacionadas.
	Integridad 3.6.g de SOC 2: Existen procedimientos para restringir el acceso lógico al sistema definido incluidos, entre otros, los aspectos siguientes: Restricción de acceso a las configuraciones del sistema, funcionalidad de superusuario, contraseñas maestras, utilidades eficaces y dispositivos de seguridad (por ejemplo, firewalls)
	Integridad 4.1 de SOC 2: Los resultados de la seguridad e integridad durante el procesamiento del sistema se revisan y comparan periódicamente con las políticas de integridad durante el procesamiento del sistema definidas y las políticas de seguridad relacionadas.
	Integridad 4.2 de SOC 2: Existe un proceso para identificar y abordar posibles deficiencias en la capacidad continua de la entidad de conseguir sus objetivos de acuerdo con sus políticas de integridad durante el procesamiento del sistema definidas y las políticas de seguridad relacionadas.

Programa de conformidad de AWS	Requisito de conformidad
Organización Internacional de Normalización (ISO 27001) ISO 27001 es una norma de seguridad global muy extendida que fija los requisitos de los sistemas de gestión 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. Más información.	*Debido a las leyes de propiedad intelectual, AWS no puede proporcionar las descripciones de los requisitos de ISO 27001. Puede adquirir una copia del estándar ISO 27001 en diferentes lugares de Internet, incluido ISO.org*
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP es un programa de ámbito gubernamental de EE. UU. que ofrece un planteamiento estandarizado para la evaluación de la seguridad, la autorización y la monitorización continua de productos y servicios en la nube hasta un nivel moderado. Más información.	**Rev 3 AU-2 de NIST 800-53 de FedRAMP:** La organización: a. Determina, en función de una evaluación de riesgos y las necesidades de una misión o un negocio, que el sistema de información debe ser capaz de auditar los eventos siguientes: [Asignación: lista de eventos auditables definida por la organización]; b. Coordina la función de auditoría de seguridad con otras entidades organizativas que requieren información relacionada con la auditoría para mejorar el apoyo mutuo y ayudar a seleccionar los eventos auditables; c. Ofrece un análisis razonado de por qué se cree que la lista de eventos auditables es suficiente para apoyar las investigaciones de las incidencias de seguridad una vez que se han producido; y d. Determina, en función de la información actual sobre amenazas y la evaluación continua de riesgos, que se deben auditar los siguientes eventos en el sistema de información: [Asignación: subconjunto definido por la organización de los eventos auditables definidos en AU-2 a. que se van a auditar junto con la frecuencia (o la situación que requiere) de auditoría para cada evento identificado].
	Rev 4 AU-2 de NIST 800-53 de FedRAMP: La organización: a. Determina que el sistema de información debe ser capaz de auditar los eventos siguientes: [Asignación: eventos auditables definidos por la organización]; b. Coordina la función de auditoría de seguridad con otras entidades organizativas que requieren información relacionada con la auditoría para mejorar el apoyo mutuo y ayudar a seleccionar los eventos auditables; c. Ofrece un análisis razonado de por qué se cree que los eventos auditables son suficientes para apoyar las investigaciones de los incidentes de seguridad una vez que se han producido; y d. Determina que se deben auditar los siguientes eventos en el sistema de información: [Asignación: subconjunto definido por la organización de los eventos auditables definidos en AU-2 a. que se van a auditar junto con la frecuencia (o la situación que requiere) de auditoría para cada evento identificado].

Programa de conformidad de AWS	Requisito de conformidad
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP es un programa de ámbito gubernamental de EE. UU. que ofrece un planteamiento estandarizado para la evaluación de la seguridad, la autorización y la monitorización continua de productos y servicios en la nube hasta un nivel moderado. Más información.	**Rev 3 AU-3 de NIST 800-53 de FedRAMP:** El sistema de información genera registros de auditoría que contienen suficiente información para, como mínimo, establecer qué tipo de evento se produjo, cuándo (fecha y hora) ocurrió el evento, dónde se produjo, el origen del evento, el resultado (éxito o error) del evento y la identidad de cualquier usuario o asunto asociado al evento.
	Rev 4 AU-3 de NIST 800-53 de FedRAMP: El sistema de información genera registros de auditoría que contienen información que, como mínimo, establece qué tipo de evento se produjo, cuándo ocurrió el evento, dónde se produjo, el origen del evento, el resultado del evento y la identidad de cualquier usuario o asunto asociado al evento.
	Rev 3 AU-4 de NIST 800-53 de FedRAMP: La organización asigna capacidad de almacenamiento para los registros de auditoría y configura la auditoría a fin de reducir la probabilidad de que se supere esa capacidad.
	Rev 4 AU-4 de NIST 800-53 de FedRAMP: La organización asigna capacidad de almacenamiento para los registros de auditoría de acuerdo con [Asignación: requisitos de almacenamiento de registros de auditoría definidos por la organización].
	Rev 3 AU-5 de NIST 800-53 de FedRAMP: El sistema de información: a. Alerta a los empleados de la organización designados en caso de que se produzca un error en el procesamiento de auditoría; y b. Adopta las medidas adicionales siguientes: [Asignación: medidas definidas por la organización que se tomarán (por ejemplo, apagar el sistema de información, sobrescribir los registros de auditoría más antiguos, dejar de generar registros de auditoría)].
	Rev 4 AU-5 de NIST 800-53 de FedRAMP: El sistema de información: a. Alerta [Asignación: personal definido por la organización] en caso de que se produzca un error en el procesamiento de auditoría; y b. Adopta las medidas adicionales siguientes: [Asignación: medidas definidas por la organización que se tomarán (por ejemplo, apagar el sistema de información, sobrescribir los registros de auditoría más antiguos, dejar de generar registros de auditoría)].
	Rev 3 AU-6 de NIST 800-53 de FedRAMP: La organización: a. Revisa y analiza los registros de auditoría del sistema de información [Asignación: frecuencia definida por la organización] para obtener indicaciones de actividades inadecuadas o inusuales y notifica los resultados al personal designado por la organización; y b. Ajusta el nivel de revisión, análisis e informes de auditoría dentro del sistema de información cuando haya un cambio en el riesgo para las operaciones o los activos de la organización, los usuarios, otras organizaciones, o la Nación en función de la información de aplicación de la ley, información de inteligencia u otras fuentes de información creíbles.

Programa de conformidad de AWS	Requisito de conformidad
	Rev 3 AU-6 de NIST 800-53 de FedRAMP: La organización: a. Revisa y analiza los registros de auditoría del sistema de información [Asignación: frecuencia definida por la organización] para obtener indicaciones de [Asignación: actividades inadecuadas o inusuales definidas por la organización]; y b. Notifica los resultados al [Asignación: personal o funciones designados por la organización].
	Rev 3 AU-8 de NIST 800-53 de FedRAMP: El sistema de información utiliza los relojes internos del sistema con el fin de generar marcas temporales para los registros de auditoría.
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP es un programa de ámbito gubernamental de EE. UU. que ofrece un planteamiento estandarizado para la evaluación de la seguridad, la autorización y la monitorización continua de productos y servicios en la nube hasta un nivel moderado. Más información.	**Rev 4 AU-8 de NIST 800-53 de FedRAMP:** El sistema de información: a. Utiliza los relojes internos del sistema con el fin de generar marcas temporales para los registros de auditoría; y b. Genera la hora en las marcas temporales que se puede asignar a la hora universal coordinada (UTC) o a la hora del meridiano de Greenwich (GMT) y cumple con el [Asignación: grado de detalle definido por la organización para la medida del tiempo].
	Rev 3 AU-9 de NIST 800-53 de FedRAMP: El sistema de información protege la información de auditoría y las herramientas de auditoría frente al acceso, modificación y eliminación no autorizados.
	Rev 4 AU-9 de NIST 800-53 de FedRAMP: El sistema de información protege la información de auditoría y las herramientas de auditoría frente al acceso, modificación y eliminación no autorizados.
	Rev 3 AU-10 de NIST 800-53 de FedRAMP: El sistema de información protege frente a un usuario que niega falsamente haber realizado una acción determinada.
	Rev 4 AU-10 de NIST 800-53 de FedRAMP: El sistema de información protege frente a un usuario (o proceso que actúa en nombre de un usuario) que niega falsamente haber realizado [Asignación: acciones definidas por la organización que estarán cubiertas por el no repudio].
	Rev 3 AU-11 de NIST 800-53 de FedRAMP: La organización conserva los registros de auditoría durante [Asignación: período de tiempo definido por la organización coherente con la política de retención de registros] para apoyar las investigaciones de las incidencias de seguridad una vez que se han producido, y para cumplir los requisitos normativos y de la organización para la retención de información.
	Rev 4 AU-11 de NIST 800-53 de FedRAMP: La organización conserva los registros de auditoría durante [Asignación: período de tiempo definido por la organización coherente con la política de retención de registros] para apoyar las investigaciones de las incidencias de seguridad una vez que se han producido, y para cumplir los requisitos normativos y de la organización para la retención de información.