# Introducción a la auditoría del uso de AWS

*Octubre de 2015*


amazon
web services

# Avisos

Este documento se proporciona únicamente con fines informativos. Representa la oferta actual de productos y prácticas de AWS a partir de la fecha de publicación de este documento. Dichas prácticas y productos pueden modificarse sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece “tal cual”, sin garantía de ningún tipo, ya sea explícita o implícita. Este documento no genera ninguna garantía, declaración, compromiso contractual, condición ni certeza por parte de AWS, sus filiales, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS para con sus clientes están sujetas a los acuerdos de AWS. Este documento no forma parte de ningún acuerdo entre AWS y sus clientes ni modifica acuerdo alguno.

# Contenido

# Resumen

La seguridad en AWS no requiere ninguna tarea. Todos los clientes de AWS se benefician de una arquitectura de red y un centro de datos diseñados para satisfacer las necesidades de seguridad de las organizaciones más exigentes. Para ello, la conformidad de AWS permite a los clientes conocer los potentes controles de AWS para mantener la seguridad y la protección de datos en la nube.

A medida que se van creando sistemas en la infraestructura de nube de AWS, se deberán compartir las responsabilidades relativas a la conformidad. Mediante la combinación de características de servicio centradas en la gobernanza y la auditoría con los estándares aplicables de conformidad o auditoría, los habilitadores de conformidad de AWS crean programas tradicionales que ayudan a los clientes a establecerse y trabajar en un entorno de control de seguridad de AWS.

AWS administra la infraestructura subyacente, y usted administra la seguridad de todo lo que implementa en AWS. Al ser una plataforma moderna, AWS permite formalizar el diseño de la seguridad, así como los controles de auditoría, mediante unos procesos operativos y técnicos verificables, automatizados y fiables incorporados a las cuentas de todos los clientes de AWS. La nube simplifica el uso del sistema para los administradores y los responsables de TI, y hace que sea mucho más fácil auditar pruebas de muestreo del entorno de AWS, ya que AWS puede convertir las auditorías en una verificación del 100% frente a las pruebas de muestreo tradicionales.

Asimismo, las herramientas creadas expresamente de AWS pueden adaptarse a los requisitos y los objetivos de auditoría y escalado de los clientes, además de permitir la verificación en tiempo real y la generación de informes mediante el uso de herramientas internas como AWS CloudTrail, Config y CloudWatch. Estas herramientas se han creado para ayudarle a maximizar la protección de sus servicios, datos y aplicaciones. Esto significa que los clientes de AWS pueden dedicar menos tiempo a realizar tareas rutinarias de auditoría y seguridad, y pueden centrarse más en adoptar medidas proactivas que pueden seguir mejorando las funciones de auditoría y seguridad de sus entornos de AWS.

# Introducción

A medida que los clientes implementan más cargas de trabajo en la nube, los auditores no solo necesitan entender mejor cómo funciona la nube, sino también cómo sacar el máximo partido de la eficacia que ofrece la informática en la nube a la hora de realizar auditorías. Gracias a la nube de AWS, los auditores pueden pasar de unas pruebas de muestreo basadas en porcentajes hacia una vista de auditoría integral en tiempo real, lo que permite disponer de una auditabilidad del 100% del entorno de los clientes y de una administración de riesgos en tiempo real.

La consola de administración de AWS, junto con la interfaz de línea de comandos (CLI), pueden generar resultados excelentes para los auditores ante varias autoridades del sector, de estándares y reguladoras. Ello obedece a que AWS admite multitud de configuraciones de seguridad para establecer funciones de seguridad, conformidad por diseño y auditoría en tiempo real mediante el uso de lo siguiente:

- **Automatización**: la infraestructura para la que pueden crearse scripts (es decir, Infraestructura como código) permite crear sistemas de implementación seguros, fiables y repetibles aprovechando implementaciones programables (mediante API) de los servicios.

- **Arquitecturas para las que pueden crearse scripts**: se pueden implementar imágenes de máquina de Amazon (AMI) y entornos "maestros" para conseguir servicios auditables y fiables, y se les pueden aplicar restricciones para asegurar una administración de riesgos en tiempo real.

- **Distribución**: las funciones que AWS CloudFormation ofrece proporcionan a los administradores de sistemas una forma sencilla de crear una colección de recursos relacionados de AWS y de provisionarlos de una manera ordenada y predecible.

- **Verificable**: el uso de AWS CloudTrail, Amazon CloudWatch, AWS OpsWorks y AWS CloudHSM proporciona funciones de recopilación de pruebas.

# Enfoques para el uso de las guías de auditoría de AWS

## Examinadores

Al evaluar las organizaciones que utilizan servicios de AWS, es fundamental entender el modelo de "responsabilidad compartida" entre AWS y el cliente. La guía de auditoría organiza los requisitos en controles del programa de seguridad y áreas de control comunes. Cada control hace referencia a los requisitos de auditoría aplicables.

En general, los servicios de AWS deben tratarse de manera similar a los servicios de infraestructura locales que los clientes han utilizado tradicionalmente para los servicios y las aplicaciones. También deben aplicarse políticas y procesos a los dispositivos y servidores cuando es AWS quien suministra esas funciones. Los controles que incumben solamente a la política o el procedimiento suelen ser de la entera responsabilidad del cliente. Del mismo modo, la administración de AWS, ya sea mediante la consola de AWS o la API de línea de comandos, debe tratarse como cualquier otro acceso de administrador con privilegios. Consulte el apéndice y los puntos mencionados para obtener más información.

## Pruebas proporcionadas por AWS

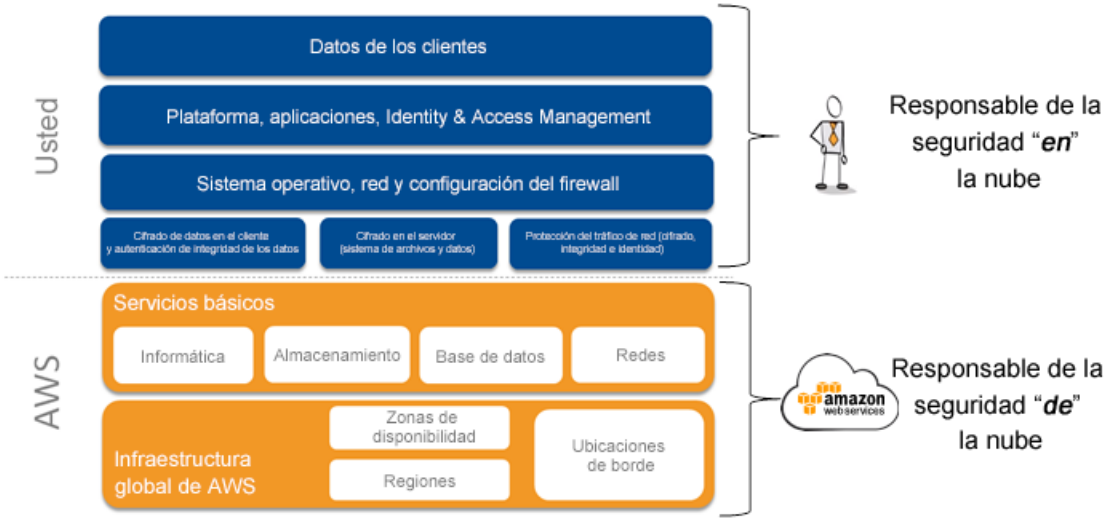
La conformidad en la nube de Amazon Web Services permite a los clientes conocer los potentes controles de AWS para mantener la seguridad y la protección de datos en la nube. A medida que se van creando sistemas en la infraestructura de nube de AWS, se deberán compartir las responsabilidades relativas a la conformidad. Cada certificación significa que un auditor ha verificado que se han establecido determinados controles de seguridad y funcionan según lo previsto. Puede ver los informes de conformidad aplicables poniéndose en contacto con el representante de su cuenta de AWS. Para obtener más información acerca de las regulaciones y los estándares de seguridad con los que cumple AWS, visite la página web Conformidad en la nube de AWS. Para ayudar a satisfacer las regulaciones y los estándares de seguridad gubernamentales, del sector y de la empresa, AWS proporciona informes de certificación en los que se describe cómo la infraestructura de la nube de AWS satisface los requisitos de una extensa lista de estándares de seguridad globales, incluidos los siguientes: ISO 27001, SOC, el estándar de seguridad de datos de PCI, FedRAMP, el Manual de seguridad de la información de la Dirección de Señales Australiana (ASD) y el Estándar de seguridad de la nube multinivel de Singapur (MTCS SS 584). Para obtener más información acerca de las regulaciones y los estándares de seguridad con los que cumple AWS, visite la página web Conformidad en la nube de AWS.

# Conceptos de auditoría del uso de AWS

Durante una auditoría de seguridad de los sistemas y los datos de AWS de una organización, hay que tener en cuenta los conceptos siguientes:

- Las medidas de seguridad que el proveedor de servicios en la nube (AWS) implementa y opera: "seguridad de la nube"
- Las medidas de seguridad que el cliente implementa y opera, relacionadas con la seguridad del contenido y las aplicaciones del cliente que utilizan los servicios de AWS: "seguridad en la nube "

Aunque AWS administra la seguridad **de** la nube, la seguridad **en** la nube es responsabilidad del cliente. El cliente mantiene el control de las medidas de seguridad que decide implementar para proteger su contenido, plataforma, aplicaciones, sistemas y redes, del mismo modo que lo haría en el caso de aplicaciones ubicadas en un centro de datos en sus propias instalaciones.




Hay información adicional en el Centro de seguridad de AWS, en Conformidad en la nube de AWS y en los documentos técnicos de AWS publicados en: Documentos técnicos de AWS

## Identificación de los activos en AWS

Los activos de AWS de un cliente pueden ser instancias, almacenes de datos, aplicaciones y los propios datos. La auditoría del uso de AWS suele comenzar con la identificación de activos. Los activos de una infraestructura de nube pública *no* son muy diferentes que los activos de los entornos internos, y en algunos casos puede ser menos complejo hacer un inventario de ellos porque AWS proporciona visibilidad a los activos que administra.

## Identificadores de cuenta de AWS

AWS asigna dos ID únicos a cada cuenta de AWS: un ID de cuenta de AWS y un ID de usuario canónico. El ID de cuenta de AWS es un número de 12 dígitos, como 123456789012, que se usa para crear nombres de recursos de Amazon (ARN). Cuando se hace referencia a recursos, como un usuario de IAM o un almacén de Amazon Glacier, el ID de cuenta distingue sus recursos de los recursos existentes en otras cuentas de AWS.

### Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS

Los nombres de recursos de Amazon (ARN) identifican de forma exclusiva los recursos de AWS. Exigimos un ARN cuando tiene que especificar un recurso de manera inequívoca en todo AWS, como en políticas de IAM, etiquetas de Amazon Relational Database Service (Amazon RDS) y llamadas API.

### Ejemplo de formato de ARN:

```
    <!-- Elastic Beanstalk application version -->
arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/My App/MyEnvironment

<!-- IAM user name -->
arn:aws:iam::123456789012:user/David

<!-- Amazon RDS tag -->
arn:aws:rds:eu-west-1:001234567890:db:mysql-db

<!-- Amazon S3 bucket (and all objects in it)-->
arn:aws:s3:::my_corporate_bucket/*
```

Además de los identificadores de cuenta, nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS, cada servicio de AWS crea un identificador único de servicio, por ejemplo, el ID de instancia de Amazon Elastic Compute Cloud (Amazon EC2): i-3d68c5cb o el ID de volumen de Amazon Elastic Block Store (Amazon EBS) vol-ecd8c122 que puede utilizarse para crear un inventario de activos del entorno y emplearse dentro de los documentos de trabajo para indicar el ámbito de aplicación de la auditoría y el inventario.

Cada certificación significa que un auditor ha verificado que se han establecido determinados controles de seguridad y funcionan según lo previsto.

# 1. Gobernanza

**Definición:** la gobernanza garantiza que la orientación e intención del cliente se reflejan en la postura del cliente sobre la seguridad. Para ello se utiliza un enfoque estructurado destinado a implementar un programa de seguridad de la información. A efectos de este plan de auditoría, significa entender qué servicios de AWS se han comprado, qué tipos de sistemas e información piensa utilizar con el servicio de AWS, y qué políticas, procedimientos y planes se aplican a estos servicios.

**Objetivo principal de la auditoría:** entender qué servicios y recursos de AWS se utilizan y asegurarse de que su programa de administración de riesgos o de la seguridad ha tenido en cuenta el uso del entorno de nube pública.

**Enfoque de auditoría:** como parte de esta auditoría, determine quién es propietario de una cuenta de AWS y propietario de recursos en su organización, así como los tipos de servicios y recursos de AWS que utilizan. Verifique que las políticas, los planes y los procedimientos incluyen conceptos de nube y que la nube está incluida en el ámbito del programa de auditoría del cliente.

### Lista de comprobación de gobernanza

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | Entender el uso de AWS dentro de su organización. Los enfoques pueden incluir:<br>• Encuestar o entrevistar a los equipos de TI y de desarrollo.<br>• Realizar escaneos de red o una prueba de intrusión más exhaustiva.<br>▪ Revisar los informes de gastos o los pagos de pedidos (PO) relacionados con Amazon.com o AWS para entender qué servicios se utilizan. Los cargos de la tarjeta de crédito aparecen como “AMAZON WEB SERVICES AWS.AMAZON.CO WA” o algo similar.<br>Nota: algunas personas de su organización pueden haber solicitado una cuenta de AWS en sus cuentas personales; por tanto, contemple la posibilidad de plantear esta pregunta si es el caso cuando encueste o entreviste a los equipos de TI y de desarrollo. |
| ☐ | **Identificar los activos.** Cada cuenta de AWS tiene una dirección de correo electrónico de contacto asociada y se puede utilizar para identificar a los propietarios de cuentas. Es importante entender que esta dirección de correo electrónico puede proceder de un proveedor público de servicios de correo electrónico, según lo que especificara el usuario al registrarse. |

| | **Elemento de la lista de comprobación** |
|---|---|
| | • Se puede mantener una reunión formal con cada propietario de una cuenta o de un activo de AWS para entender lo que se implementa en AWS, cómo se administra y cómo se ha integrado con las políticas, los procedimientos y los estándares de seguridad de su organización.<br><br>**Nota**: el propietario de una cuenta de AWS puede ser alguien del departamento financiero o de compras, pero la persona que *implementa* el uso que hace la organización de los recursos de AWS puede pertenecer al departamento de TI. Puede que deba entrevistarse con ambos. |
| ☐ | **Definir los límites de AWS para las revisiones.** La revisión debe tener un ámbito definido. Entienda los procesos empresariales básicos de su organización y su adecuación con TI, tanto fuera de la nube como en las implementaciones actuales o futuras en la nube.<br><br>• Obtenga una descripción de los servicios de AWS que se utilizan o que se plantea utilizar.<br><br>• Después de identificar los tipos de servicios de AWS que se utilizan o se piensa utilizar, determine los servicios y las soluciones empresariales que se incluirán en la revisión.<br><br>• Obtenga y revise los informes de auditoría anteriores con planes de corrección.<br><br>• Identifique los problemas pendientes de los informes de auditoría anteriores y evalúe las actualizaciones de los documentos con respecto a estos problemas. |
| ☐ | **Evaluar las políticas.** Evalúe y revise las políticas de seguridad, privacidad y clasificación de datos de la organización para determinar qué políticas se aplican al entorno de servicios de AWS.<br><br>• Verifique si existe una política o un proceso formales para la adquisición de servicios de AWS con el fin de determinar cómo se autoriza la compra de servicios de AWS.<br><br>• Verifique si los procesos y las políticas de administración de cambios de la organización incluyen la consideración de los servicios de AWS. |

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Identificar los riesgos.** Determine si se ha realizado una evaluación de riesgos de los activos aplicables. |
| ☐ | **Revisar los riesgos.** Obtenga una copia de los informes de evaluación de riesgos y determine si reflejan el entorno actual y describen exactamente el entorno de riesgo residual. |
| ☐ | **Revisar la documentación de riesgos.** Para cada elemento de la revisión, revise los planes de tratamiento de riesgos y sus plazos o hitos según las políticas y los procedimientos de administración de riesgos. |
| ☐ | **Documentación e inventario.** Verifique que la red de AWS está totalmente documentada y que todos los sistemas esenciales de AWS están incluidos en la documentación de inventario, a la que hay un acceso limitado.<br>• Revise AWS Config para ver un inventario de los recursos de AWS y el historial de configuración de esos recursos *(ejemplo de llamada API 1)*.<br>• Asegúrese de que los recursos están debidamente etiquetados y asociados a datos de aplicación.<br>• Examine la arquitectura de las aplicaciones para identificar los flujos de datos, la conectividad prevista entre los componentes de las aplicaciones y los recursos que contienen datos.<br>• Examine lo siguiente para revisar toda la conectividad entre su red y la plataforma de AWS:<br>▪ Conexiones de VPN en las que las direcciones IP públicas locales de los clientes se asignan a gateways de cliente en todas las VPC que son propiedad del cliente. *(Ejemplo de llamadas API 2 y 3)*. Conexiones privadas de Direct Connect, que pueden asignarse a 1 o varias VPC que son propiedad del cliente. *(Ejemplo de llamada API 4)* |

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Evaluar los riesgos.** Evalúe la importancia de los datos implementados en AWS para el perfil de riesgos y la tolerancia a riesgos globales de la organización. Asegúrese de que estos activos de AWS están integrados en el programa formal de evaluación de riesgos de la organización.<br><br>• Se deben identificar los activos de AWS y asociarles objetivos de protección en función de sus perfiles de riesgo. |
| ☐ | **Incorporar el uso de AWS en la evaluación de riesgos.** Realice procesos de evaluación de riesgos de la organización e incorpore en ellos elementos de servicio de AWS. Los riesgos clave pueden incluir:<br><br>• Identificar el riesgo empresarial asociado al uso de AWS e identificar los propietarios y los agentes clave del negocio.<br>• Verificar que los riesgos empresariales se alinean, valoran o clasifican dentro de su uso de los servicios de AWS y de los criterios de seguridad de la organización en cuanto a protección de la confidencialidad, integridad y disponibilidad.<br>• Revisar las auditorías anteriores relacionadas con los servicios de AWS (SOC, PCI, auditorías relacionadas con NIST 800-53, etc.).<br>• Determinar si los riesgos identificados previamente se han abordado convenientemente.<br>• Evaluar el factor de riesgo global para realizar la revisión de AWS.<br>• Según la evaluación de riesgos, identificar los cambios en el ámbito de auditoría.<br>• Hablar sobre los riesgos con la dirección de TI y ajustar la evaluación de riesgos. |
| ☐ | **Política y programa de seguridad de TI.** Verifique que el cliente incluye los servicios de AWS en sus procedimientos y políticas de seguridad, incluidas las prácticas recomendadas de AWS a nivel de cuenta de AWS como se destaca en el servicio AWS Trusted Advisor, que ofrece prácticas recomendadas y directrices sobre 4 temas: seguridad, costos, desempeño y tolerancia a errores.<br><br>• Revise las políticas de seguridad de la información y asegúrese de que incluyen los servicios de AWS.<br><br>• Confirme que ha designado a uno o varios empleados como autoridad para el uso y la seguridad de los servicios de AWS y que se han definido roles para esos roles clave indicados, incluido un oficial principal de seguridad de la información. |

| | Elemento de la lista de comprobación |
|---|---|
| | **Nota:** todos los estándares de procesos de administración de riesgos de ciberseguridad publicados que haya utilizado para modelar los procesos y la arquitectura de seguridad de la información.<br><br>• Asegúrese de que mantiene la documentación de apoyo a las auditorías realizadas en los servicios de AWS, incluida su revisión de las certificaciones independientes de AWS.<br>• Verifique que los registros de capacitación internos incluyen la seguridad de AWS, como el uso de Amazon IAM, los grupos de seguridad de Amazon EC2 y el acceso remoto a instancias Amazon EC2.<br>• Confirme que se mantiene una política de respuesta a la ciberseguridad y capacitación para los servicios de AWS.<br><br>**Nota**: todas las protecciones relacionadas específicamente con el uso que hacen los clientes de los servicios de AWS y todas las reclamaciones derivadas de las pérdidas y los gastos atribuidos a eventos de ciberseguridad resultantes. |
| ☐ | **Supervisión de los proveedores de servicios.** Compruebe que el contrato con AWS incluye un requisito para implementar y mantener medidas preventivas de seguridad y privacidad para los requisitos de ciberseguridad. |

## 2. Configuración y administración de redes

**Definición:** la administración de redes en AWS es muy parecida a la administración de redes local, salvo que los componentes de red como firewalls y enrutadores son virtuales. Los clientes deben asegurarse de que la arquitectura de red sigue los requisitos de seguridad de su organización, incluido el uso de zonas desmilitarizadas (DMZ) para separar los recursos públicos y privados (de confianza y que no son de confianza), la segregación de recursos mediante subredes y tablas de enrutamiento, la configuración segura de DNS, si se necesita una protección adicional de la transmisión en forma de VPN, y si se va a limitar el tráfico de entrada y salida. Los clientes que deben monitorizar la red pueden hacerlo mediante sistemas de monitorización y detección de intrusiones basados en host.

**Objetivo principal de la auditoría:** la falta de controles de seguridad o la existencia de controles de seguridad configurados incorrectamente relacionados con la seguridad de la red y el acceso externo que podría suponer un riesgo para la seguridad.

**Enfoque de auditoría:** entienda la arquitectura de red de los recursos de AWS del cliente, y cómo se configuran los recursos para permitir el acceso externo desde Internet y desde redes privadas del cliente. Nota: se puede utilizar AWS Trusted Advisor para validar y verificar los parámetros de configuración de AWS.

### Lista de comprobación de configuración y administración de redes

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Controles de red.** Identifique cómo se aplica la segmentación de red en el entorno de AWS.<br>• Revise la implementación de grupos de seguridad de AWS, la configuración de AWS Direct Connect y Amazon VPN para ver si se ha implementado correctamente la segmentación de la red y la configuración de ACL y firewall o los servicios de AWS *(ejemplo de llamadas API 5 - 8)*.<br>• Verifique que dispone de un procedimiento para conceder acceso remoto, de Internet o de VPN a los empleados para el acceso a la consola de AWS y el acceso remoto a los sistemas y redes de Amazon EC2.<br>• Revise lo siguiente para mantener un entorno de pruebas y desarrollo de software y de aplicaciones que esté separado de su entorno empresarial:<br>▪ Existe aislamiento de VPC entre el entorno empresarial y los entornos empleados para tareas de pruebas y desarrollo.<br>▪ Examine la interconexión entre las VPC para asegurarse de que existe aislamiento de red entre las VPC<br>▪ Existe aislamiento de subred entre el entorno empresarial y los entornos empleados para tareas de pruebas y desarrollo.<br>▪ Examinando las NACL asociadas a las subredes en las que se encuentran los entornos empresarial y de pruebas o desarrollo para garantizar que existe aislamiento de red.<br>▪ Existe aislamiento de instancias Amazon EC2 entre el entorno empresarial y los entornos empleados para tareas de pruebas y desarrollo.<br>▪ Examinando los grupos de seguridad asociados a 1 o varias instancias que están asociadas a los entornos empresarial, de pruebas o desarrollo para garantizar que existe aislamiento de red entre las instancias Amazon EC2 |

| | **Elemento de la lista de comprobación** |
|---|---|
| | ▪ Examine la solución de defensa organizada en capas contra ataques de DDoS que se está ejecutando y que opera directamente en AWS, revisando los componentes que se utilizan como parte de una solución de DDoS como:<br>▪ Configuración de Amazon CloudFront<br>▪ Configuración de Amazon S3<br>▪ Amazon Route 53<br>▪ Configuración de ELB<br>▪ Nota: los servicios anteriores no utilizan direcciones IP públicas que son propiedad del cliente y ofrecen características de mitigación de DoS heredadas de AWS.<br>▪ Uso de Amazon EC2 para proxy o WAF<br>Encontrará orientaciones más detalladas en el documento técnico "AWS Best Practices for DDoS Resiliency Whitepaper" |
| ☐ | **Controles de código malintencionado.** Evalúe la implementación y administración de software antimalware para las instancias Amazon EC2 de un modo similar al de los sistemas físicos. |

## 3. Configuración y administración de activos

**Definición:** los clientes de AWS son responsables de mantener la seguridad de todo lo que hay instalado en sus recursos de AWS o que conectan con sus recursos de AWS. La administración segura de los recursos de AWS del cliente supone saber qué recursos está utilizando (inventario de activos), configurar de forma segura el SO invitado y las aplicaciones en los recursos (parámetros de configuración segura, parches y antimalware) y controlar los cambios en los recursos (administración de cambios).

**Objetivo principal de la auditoría:** administre las vulnerabilidades de seguridad del sistema operativo y de las aplicaciones para proteger la seguridad, estabilidad e integridad de los activos.

**Enfoque de auditoría:** valide que el SO y las aplicaciones están diseñados, configurados, con los parches aplicados y protegidos de acuerdo con sus políticas, procedimientos y estándares. Todas las prácticas de administración del SO y de las aplicaciones pueden ser comunes a los sistemas y servicios locales y de AWS.

### Lista de comprobación de configuración y administración de activos

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Evaluar la administración de la configuración.** Verifique su uso de las prácticas de administración de la configuración para todos los componentes del sistema de AWS y valide que estos estándares coinciden con las configuraciones de referencia.<br>• Revise el procedimiento para realizar un borrado especializado antes de eliminar el volumen, a fin de cumplir con los requisitos que estableció.<br>• Examine el sistema de Identity and Access Management (que puede utilizarse para permitir el acceso autenticado a las aplicaciones alojadas en servicios de AWS).<br>• Confirme que se han completado las pruebas de intrusión. |
| ☐ | **Controles de administración de cambios.** Asegúrese de que el uso de los servicios de AWS sigue los mismos procesos de control de cambios que las series internas.<br>• Verifique que los servicios de AWS están incluidos en un proceso interno de administración de parches. Revise el proceso documentado para la configuración y aplicación de parches de instancias Amazon EC2:<br>▪ Imágenes de máquina de Amazon (AMI) *(ejemplo de llamadas API 9 - 10)*<br>▪ Sistemas operativos<br>▪ Aplicaciones<br>• Revise las llamadas API de los servicios que recaen dentro del ámbito de aplicación para eliminar las llamadas a fin de asegurarse de que los activos de TI se han eliminado correctamente. |

# 4. Control de acceso lógico

**Definición:** los controles de acceso lógico determinan no solo quién o qué puede tener acceso a un recurso específico del sistema, sino también el tipo de acciones que se pueden realizar en el recurso (lectura, escritura, etc.). Como parte del control de acceso a los recursos de AWS, los usuarios y los procesos deben presentar credenciales para confirmar que tienen autorización para realizar determinadas funciones o que tienen acceso a recursos concretos. Las credenciales que AWS solicita varían en función del tipo de servicio y el método de acceso, e incluyen contraseñas, claves de cifrado y certificados. El acceso a los recursos de AWS se puede habilitar mediante la cuenta de AWS, cuentas de usuario individuales de AWS Identify and Access Management (IAM) creadas bajo la cuenta de AWS o federación de identidades con el directorio corporativo del cliente (inicio de sesión único). AWS Identity and Access Management (IAM) permite a los usuarios controlar de forma segura el acceso a los servicios y recursos de AWS. Con IAM puede crear y administrar usuarios y grupos de AWS, así como utilizar permisos para aceptar y denegar permisos para los recursos de AWS.

**Objetivo principal de la auditoría:** esta parte de la auditoría se centra en la identificación de cómo se configuran los usuarios y permisos en AWS para los servicios. También es importante asegurarse de que administra de forma segura las credenciales asociadas a todas las cuentas de AWS.

**Enfoque de auditoría:** valide que los permisos de los activos de AWS se administran de acuerdo con las políticas, los procedimientos y los procesos de la organización. Nota: se puede utilizar AWS Trusted Advisor para validar y verificar las configuraciones de usuarios, grupos y roles de IAM.

## Lista de comprobación de control de acceso lógico

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Administración, autenticación y autorización de accesos.** Asegúrese de que existan políticas y procedimientos internos para administrar el acceso a los servicios de AWS y las instancias Amazon EC2.<br>• Garantice la documentación del uso y la configuración de los controles de acceso de AWS, ejemplos y opciones que se indican a continuación:<br>▪ Descripción de cómo se utiliza Amazon IAM para la administración de accesos.<br>▪ Lista de controles en los que se utiliza Amazon IAM para administrar recursos, grupos de seguridad, VPN, permisos de objetos, etc.<br>▪ Uso de controles de acceso a AWS nativos, o si el acceso se administra mediante autenticación federada, que utiliza el estándar abierto lenguaje de marcado para confirmaciones de seguridad (SAML, Security Assertion Markup Language) 2.0.<br>▪ Lista de cuentas, roles, grupos y usuarios de AWS, políticas y asociaciones de políticas para usuarios, grupos y roles *(ejemplo de llamada API 11)*.<br>▪ Una descripción de los métodos de monitorización y las cuentas y los roles de Amazon IAM.<br>▪ Una descripción y configuración de los sistemas de EC2. |
| ☐ | **Acceso remoto.** Asegúrese de que exista un proceso de aprobación o de registro, o controles para impedir el acceso remoto no autorizado. Nota: todo acceso a AWS y a instancias Amazon EC2 es “acceso remoto” por definición, a menos que se haya configurado Direct Connect.<br>• Revise el proceso para impedir el acceso no autorizado, lo que puede incluir:<br>▪ AWS CloudTrail para registrar las llamadas API de nivel de servicio.<br>▪ Registros de Amazon CloudWatch para cumplir los objetivos de registro.<br>▪ Políticas de IAM, políticas de bucket de S3, grupos de seguridad para los controles que impiden el acceso no autorizado. |

| | **Elemento de la lista de comprobación** |
|---|---|
| | ▪ Revise la conectividad entre la red de la compañía y AWS:<br>▪ Conexión de VPN entre la VPC y la red de la compañía.<br>▪ Direct Connect (conexión cruzada e interfaces privadas) entre la compañía y AWS.<br>▪ Grupos de seguridad definidos, listas de control de acceso de red y tablas de enrutamiento para controlar el acceso entre AWS y la red. |
| ☐ | **Control de personal.** Restrinja los usuarios a aquellos servicios de AWS que sean estrictamente necesarios para su función empresarial *(ejemplo de llamada API 12)*.<br>• Revise el tipo de control de acceso existente en relación con los servicios de AWS.<br>▪ Control de acceso a AWS en un nivel de AWS mediante IAM y etiquetado para controlar la administración de instancias Amazon EC2 (inicio, parada, terminación) dentro de las redes<br>▪ Control de acceso de los clientes mediante IAM (solución LDAP) para administrar el acceso a los recursos existentes en las redes en las capas de aplicación y sistema operativo<br>▪ Control de acceso a la red mediante grupos de seguridad (SG) de AWS, listas de control de acceso a la red (NACL), tablas de enrutamiento, conexiones de VPN e interconexión de VPC para controlar el acceso de red a los recursos dentro de las VPC que son propiedad de los clientes. |

## 5. Cifrado de datos

**Definición:** los datos almacenados en AWS son seguros de forma predeterminada; solo los propietarios de AWS tienen acceso a los recursos de AWS que crean. Sin embargo, los clientes que tienen datos confidenciales pueden requerir protección adicional cifrando los datos cuando están almacenados en AWS. Actualmente solo el servicio Amazon S3 ofrece una función automatizada de cifrado en el servidor además de permitir que los clientes cifren los datos en el lado del cliente antes de almacenarlos. En las demás opciones de almacenamiento de datos de AWS, es el cliente el que tiene que cifrar los datos.

**Objetivo principal de la auditoría:** los datos en reposo se deben cifrar de la misma forma en que se protegen los datos locales. Además, muchas políticas de seguridad consideran que Internet es un medio de comunicación inseguro y requerirán el cifrado de los datos en tránsito. La protección incorrecta de los datos puede suponer un riesgo de seguridad.

**Enfoque de auditoría:** entienda dónde se encuentran los datos y valide los métodos empleados para proteger los datos que se encuentran en reposo y en tránsito (denominados también "datos en vuelo"). Nota: se puede utilizar AWS Trusted Advisor para validar y verificar los permisos y el acceso a activos de datos.

**Lista de comprobación de cifrado de datos**

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Controles de cifrado.** Asegúrese de que existan los controles adecuados para proteger la información confidencial que se transporta mientras se utilizan los servicios de AWS.<br>▪ Revise los métodos de conexión a la consola de AWS, administración de API, S3, RDS y VPN de Amazon EC2 para exigir el cifrado.<br>▪ Revise las políticas y los procedimientos internos para la administración de claves, incluidos los servicios de AWS y las instancias Amazon EC2.<br>▪ Revise los métodos de cifrado empleados, si hay alguno, para proteger los PIN en reposo; AWS ofrece diversos servicios de administración de claves como KMS, CloudHSM y Cifrado en el servidor de Amazon S3 que pueden utilizarse como ayuda para el cifrado de datos en reposo *(ejemplo de llamadas API 13-15)*. |

## 6. Registro y monitorización de la seguridad

**Definición:** los registros de auditoría contienen una gran variedad de eventos que se producen dentro de sus sistemas de información y redes. Los registros de auditoría se emplean para identificar las actividades que pueden afectar a la seguridad de esos sistemas, ya sea en tiempo real o después de los hechos en cuestión, por lo que es importante realizar una configuración y protección adecuadas de los registros.

**Objetivo principal de la auditoría:** los sistemas se deben registrar y monitorizar del mismo modo que los sistemas locales. Si los sistemas de AWS no están incluidos en el plan global de seguridad de la empresa, pueden quedar fuera del ámbito de los esfuerzos de monitorización de los sistemas importantes.

**Enfoque de auditoría:** valide que se está realizando el registro de auditoría en el SO invitado y las aplicaciones esenciales instaladas en las instancias Amazon EC2, y que la implementación es conforme con sus políticas y procedimientos, especialmente lo que está relacionado con el almacenamiento, la protección y el análisis de los registros.

**Lista de comprobación de registro y monitorización de la seguridad:**

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Monitorización y seguimientos de evaluación de registro.** Revise las políticas y los procedimientos de registro y monitorización en términos de idoneidad, retención, umbrales definidos y mantenimiento seguro, específicamente para detectar actividades no autorizadas en servicios de AWS.<br>• Revise las políticas y los procedimientos de registro y monitorización, y compruebe que figuran los servicios de AWS, incluidas las instancias Amazon EC2, para ver eventos relacionados con la seguridad.<br>• Verifique que los mecanismos de registro están configurados para enviar los registros a un servidor centralizado, y compruebe que en el caso de las instancias Amazon EC2 se conservan el tipo y el formato adecuado de los registros, de un modo similar al de los sistemas físicos.<br>• Para los clientes que utilizan AWS CloudWatch, examine el proceso y el registro del uso de la monitorización de red.<br>• Asegúrese de que se emplean análisis de eventos para mejorar las medidas y políticas defensivas.<br>• Examine el informe de credenciales de IAM de AWS para ver si hay usuarios no autorizados, AWS Config y el etiquetado de recursos para ver si hay dispositivos no autorizados *(ejemplo de llamada API 16)*.<br>• Confirme la agregación y la correlación de datos de eventos procedentes de diversos orígenes mediante servicios de AWS como los siguientes:<br>▪ Registros de flujo de VPC para identificar los paquetes de red aceptados y rechazados que entran en la VPC.<br>▪ AWS CloudTrail para identificar las llamadas API autenticadas y sin autenticar a los servicios de AWS<br>▪ Registro de ELB: registro del balanceador de carga.<br>▪ Registro de AWS CloudFront: registro de las distribuciones de CDN. |
| ☐ | **Detección y respuesta ante intrusiones.** Revise los IDS basados en host en las instancias Amazon EC2 de un modo similar al de los sistemas físicos.<br>• Examine las pruebas proporcionadas por AWS para ver qué información de los procesos de detección de intrusiones se puede revisar. |

# 7. Respuesta ante incidencias de seguridad

**Definición:** en un modelo de responsabilidad compartida, los eventos de seguridad se pueden monitorizar con la interacción de AWS y el cliente de AWS. AWS detecta y responde a los eventos que afectan al hipervisor y a la infraestructura subyacente. Los clientes administran los eventos desde el sistema operativo invitado hasta la aplicación. Debe comprender las responsabilidades de respuesta ante incidencias que tiene y adaptar las herramientas y los procesos de monitorización de la seguridad, alertas y auditoría para sus recursos de AWS.

**Objetivo principal de la auditoría:** se deben monitorizar los eventos de seguridad independientemente de dónde se encuentren los activos. El auditor puede evaluar la coherencia de implementar controles de administración de incidencias en todos los entornos y validar una cobertura total mediante pruebas.

**Enfoque de auditoría:** evalúe la existencia y la eficacia operativa de los controles de administración de incidencias de los sistemas del entorno de AWS.

**Lista de comprobación de respuesta ante incidencias de seguridad:**

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Informes sobre incidencias.** Asegúrese de que el plan de respuesta ante incidencias de seguridad y la política de incidencias de ciberseguridad incluyen los servicios de AWS y contemplan controles que mitigan las incidencias de ciberseguridad y ayudan a la recuperación.<br>• Asegúrese de que se utilizan las herramientas existentes de monitorización de incidencias, así como las herramientas disponibles en AWS para monitorizar el uso de los servicios de AWS.<br>• Verifique que el plan de respuesta ante incidencias está sometido a una revisión periódica y que los cambios relativos a AWS se realizan cuando es necesario.<br>• Compruebe si el plan de respuesta ante incidencias incluye procedimientos de notificación y cómo el cliente aborda la responsabilidad en relación con las pérdidas asociadas a los ataques o cómo afectan a las instrucciones. |

# 8. Recuperación de desastres

**Definición:** AWS ofrece una infraestructura de alta disponibilidad que permite a los clientes diseñar aplicaciones resistentes y responder rápidamente ante incidencias graves o en situaciones de desastre. No obstante, los clientes deben asegurarse de configurar los sistemas que requieren tiempos rápidos de recuperación o alta disponibilidad de manera que se beneficien de las diversas regiones y zonas de disponibilidad que ofrece AWS.

**Objetivo principal de la auditoría:** un punto único de error no identificado o una planificación inadecuada para afrontar situaciones de recuperación de desastres puede tener repercusiones importantes. Si bien AWS ofrece acuerdos de nivel de servicios (SLA) en el nivel de instancia y servicio individual, no deben confundirse con los objetivos de continuidad del negocio (BC) y de recuperación de desastres (DR) del cliente, como un objetivo de tiempo de recuperación (RTO) y un objetivo de punto de recuperación (RPO). Los parámetros de BC y DR están asociados al diseño de la solución. Normalmente, un diseño más flexible utiliza varios componentes de diferentes zonas de disponibilidad de AWS e incluye replicación de datos.

**Enfoque de auditoría:** entienda la estrategia de DR y determine la arquitectura tolerante a errores empleada para los activos esenciales. Nota: se puede utilizar AWS Trusted Advisor para validar y verificar algunos aspectos de las funciones de resistencia del cliente.

**Lista de comprobación de recuperación de desastres**:

| | **Elemento de la lista de comprobación** |
|---|---|
| ☐ | **Plan de continuidad del negocio (BCP).** Asegúrese de que existe un BCP integral, para los servicios de AWS utilizados, que aborde la mitigación de los efectos que una incidencia de ciberseguridad puede tener y la recuperación de una incidencia de ese tipo.<br>• Dentro del plan, compruebe que AWS se ha incluido en los elementos de preparación en caso de emergencia y de administración de crisis, las responsabilidades de supervisión de la alta dirección y el plan de pruebas. |

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Controles de almacenamiento y copia de seguridad.** Revise las pruebas periódicas que hace el cliente de sus sistemas de copia de seguridad para los servicios de AWS *(ejemplo de llamadas API 17-18)*.<br>1. Revise el inventario de los datos de los que se ha hecho copia de seguridad en servicios de AWS como copias de seguridad externas. |

## 9. Controles heredados

**Definición:** Amazon tiene muchos años de experiencia en el diseño, la construcción y el funcionamiento de centros de datos a gran escala. Esta experiencia se ha aplicado a la plataforma y a la infraestructura de AWS. Los centros de datos de AWS se alojan en instalaciones sin identificación externa. El acceso físico está estrictamente controlado en el perímetro y en los puntos de acceso del edificio por personal de seguridad profesional mediante videovigilancia, sistemas de detección de intrusiones y otros recursos electrónicos. El personal autorizado debe confirmar dos veces como mínimo una autenticación de dos factores para acceder a las plantas del centro de datos. Todos los visitantes y contratistas deben presentar su identificación, firmar el registro de entrada e ir acompañados en todo momento de personal autorizado.

AWS solo ofrece acceso al centro de datos y solo facilita información a los empleados y contratistas que tengan una necesidad empresarial legítima de tales privilegios. Cuando un empleado deja de tener una necesidad empresarial de tales privilegios, su acceso se revoca inmediatamente, incluso aunque continúe siendo empleado de Amazon o de Amazon Web Services. El acceso físico a los centros de datos por parte de los empleados de AWS está sujeto a registros y auditorías rutinarios.

**Objetivo principal de la auditoría:** la finalidad de esta sección de auditoría es demostrar la diligencia debida adecuada en la selección de los proveedores de servicios.

**Enfoque de auditoría:** entienda cómo puede solicitar y evaluar certificaciones y acreditaciones independientes para obtener garantías razonables en relación con el diseño y la eficacia operativa de los controles y objetivos de control.

**Lista de comprobación de controles heredados**

| | Elemento de la lista de comprobación |
|---|---|
| ☐ | **Controles ambientales y de seguridad física.** Examine las pruebas proporcionadas por AWS para ver detalles sobre qué información de los procesos de detección de intrusiones se puede revisar que esté administrada por AWS en lo referente a los controles de seguridad física. |

# Conclusión

Existen muchas herramientas de terceros que pueden ayudarle con la evaluación. Puesto que los clientes de AWS tienen pleno control de sus sistemas operativos, la configuración de red y el direccionamiento del tráfico, se pueden utilizar la mayoría de herramientas empleadas internamente para evaluar y auditar los activos de AWS.

AWS proporciona una herramienta útil denominada AWS Trusted Advisor. AWS Trusted Advisor aprovecha las prácticas recomendadas aprendidas gracias al ingente historial operativo de atender a cientos de miles de clientes de AWS. AWS Trusted Advisor efectúa varias comprobaciones fundamentales del entorno de AWS y realiza recomendaciones cuando surge la oportunidad de ahorrar dinero, mejorar el desempeño del sistema o solucionar errores de seguridad.

Esta herramienta puede utilizarse para comprobar algunos elementos de la lista de comprobación de auditoría a fin de mejorar y respaldar los procesos de auditoría y evaluación de las organizaciones.

# Apéndice A: Referencias y documentación adicional

1. Amazon Web Services: Información general sobre los procesos de seguridad: https://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

2. Documento técnico sobre riesgos y conformidad de Amazon Web Services: https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
3. Cuaderno para AWS OCIE Cybersecurity Initiative: https://d0.awsstatic.com/whitepapers/compliance/AWS_SEC_Workbook.pdf
4. Using Amazon Web Services for Disaster Recovery: http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
5. Identity federation sample application for an Active Directory use case: http://aws.amazon.com/code/1288653099190193
6. Single Sign-on with Windows ADFS to Amazon EC2 .NET Applications: http://aws.amazon.com/articles/3698?_encoding=UTF8&queryArg=searchQuery&x=20&y=25&fromSearch=1&searchPath=all&searchQuery=identity%20federation
7. Authenticating Users of AWS Mobile Applications with a Token Vending Machine http://aws.amazon.com/articles/4611615499399490?_encoding=UTF8&queryArg=searchQuery&fromSearch=1&searchQuery=Token%20Vending%20machine
8. Client-Side Data Encryption with the AWS SDK for Java and Amazon S3: http://aws.amazon.com/articles/2850096021478074
9. AWS Command Line Interface: http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html
10. Política de uso aceptable de Amazon Web Services: http://aws.amazon.com/aup/

# Apéndice B: Glosario de términos

**Autenticación:** la autenticación es el proceso por el que se determina si alguien o algo es realmente lo que se supone que es.

**EC2:** Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona capacidad de cómputo de tamaño ajustable en la nube. Está diseñado para facilitar a los desarrolladores la informática en la nube en la Web.

**Hipervisor:** un hipervisor, también denominado monitor de máquina virtual (VMM), es un software de virtualización de plataformas de software y hardware que permite que varios sistemas operativos se ejecuten en un equipo host de forma simultánea.

**IAM:** AWS Identity and Access Management (IAM) permite que un cliente cree múltiples usuarios y administre los permisos para cada uno de ellos dentro de su cuenta de AWS.

**Objeto:** las entidades fundamentales almacenadas en Amazon S3. Los objetos se componen de datos de objetos y metadatos. La parte de datos es opaca para Amazon S3. Los metadatos son conjuntos de pares de nombre y valor que describen el objeto. Estos incluyen algunos metadatos predeterminados como la fecha de la última modificación y los metadatos HTTP estándar como el tipo de contenido. El desarrollador también puede especificar metadatos personalizados en el momento en que se almacena el objeto.

**Servicio:** software o capacidad informática que se presta a través de una red (por ejemplo, EC2, S3, VPC, etc.).

**Zona de disponibilidad:** las ubicaciones de Amazon EC2 se componen de regiones y zonas de disponibilidad. Las zonas de disponibilidad son regiones diferentes que están diseñadas para estar aisladas de errores que se produzcan en otras zonas de disponibilidad, y que proporcionan conectividad de red económica de baja latencia a otras zonas de disponibilidad de la misma región.

# Apéndice C: Llamadas API

La interfaz de línea de comandos de AWS es una herramienta unificada para la administración de los servicios de AWS.
http://docs.aws.amazon.com/cli/latest/reference/index.html#cli-aws

1. Enumerar todos los recursos que tienen etiquetas
    - aws ec2 describe-tags

http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-tags.html

2. Enumerar todas las gateways de cliente existentes en la cuenta de AWS de los clientes:
    - aws ec2 describe-customer-gateways –output table
3. Enumerar todas las conexiones de VPN de la cuenta de AWS de los clientes
    - aws ec2 describe-vpn-connections
4. Enumerar todas las conexiones de Direct Connect de los clientes
    - aws directconnect describe-connections
    - aws directconnect describe-interconnects
    - aws directconnect describe-connections-on-interconnect
    - aws directconnect describe-virtual-interfaces
5. Enumerar todas las gateways de cliente existentes en la cuenta de AWS de los clientes:
    - aws ec2 describe-customer-gateways –output table
6. Enumerar todas las conexiones de VPN de la cuenta de AWS de los clientes
    - aws ec2 describe-vpn-connections
7. Enumerar todas las conexiones de Direct Connect de los clientes
    - aws directconnect describe-connections
    - aws directconnect describe-interconnects
    - aws directconnect describe-connections-on-interconnect
    - aws directconnect describe-virtual-interfaces
8. Utilizar también la CLI centrada en los grupos de seguridad:
    - aws ec2 describe-security-groups
9. Enumerar las AMI que son propiedad del cliente o que este tiene registradas actualmente
    - aws ec2 describe-images –owners self

10. Enumerar todas las instancias lanzadas con una AMI específica
    - aws ec2-describe-instances --filters “Name=image-id,Values=XXXXX” (donde XXXX = image-id value por ejemplo, ami-12345a12)
11. Enumerar los roles, grupos y usuarios de IAM
    - aws iam list-roles
    - aws iam list-groups
    - aws iam list-users
12. Enumerar las políticas asignadas a grupos, roles y usuarios:
    - aws iam list-attached-role-policies --role-name XXXX
    - aws iam list-attached-group-policies --group-name XXXX
    - aws iam list-attached-user-policies --user-name XXXX

    donde XXXX es un nombre de recurso dentro de la cuenta de AWS del cliente
13. Enumerar las claves de KMS
    - aws kms list-aliases
14. Enumerar las políticas de rotación de claves
    - aws kms get-key-rotation-status –key-id XXX (donde XXX = key-id de la cuenta de AWS)
15. Enumerar los volúmenes de EBS cifrados con claves de KMS
    - aws ec2 describe-volumes "Name=encrypted,Values=true"
    - targeted por ejemplo, us-east-1)
16. Informes de credenciales
    - aws iam generate-credential-report
    - aws iam get-credential-report
17. Crear instantánea o copia de seguridad de un volumen de EBS
    - aws ec2 create-snapshot --volume-id XXXXXXX
    - (donde XXXXXX = ID del volumen dentro de la cuenta de AWS)
18. Confirmar la creación de una instantánea o copia de seguridad
    - aws ec2 describe-snapshots --filters “Name=volume-id,Values=XXXXXX)