Lección 1

Modelo de responsabilidad compartida de AWS

La seguridad y la conformidad son compartidas entre AWS y el cliente, lo que implica que ambos tienen roles y responsabilidades definidos en el proceso. Este modelo de responsabilidad compartida busca aliviar la carga operativa del cliente, permitiendo flexibilidad y control en la implementación de soluciones en AWS. Se distingue entre la seguridad "de" la nube, manejada por AWS, y la seguridad "en" la nube, en la cual el cliente tiene un papel activo.

AWS se encarga de la gestión y seguridad de la infraestructura subyacente, desde la capa de virtualización hasta la seguridad física de las instalaciones. Esto incluye la protección del hardware, software, redes e instalaciones que soportan los servicios en la nube de AWS.

Por otro lado, el cliente es responsable del cifrado de datos en reposo y en tránsito, así como de garantizar la seguridad de la red y la gestión segura de credenciales y accesos. Además, debe configurar adecuadamente los grupos de seguridad y el sistema operativo en las instancias computacionales que utiliza, incluyendo actualizaciones y parches de seguridad.

Responsabilidad de AWS: seguridad de la nube

Responsabilidades de AWS:

- Seguridad física de los centros de datos
  - Acceso controlado basado en las necesidades

Infraestructura de hardware y software

- Baja de recursos de almacenamiento, registro de acceso del sistema operativo (SO) del host y auditoría

Infraestructura de red

- Detección de intrusiones

Infraestructura de virtualización

- Aislamiento de instancias

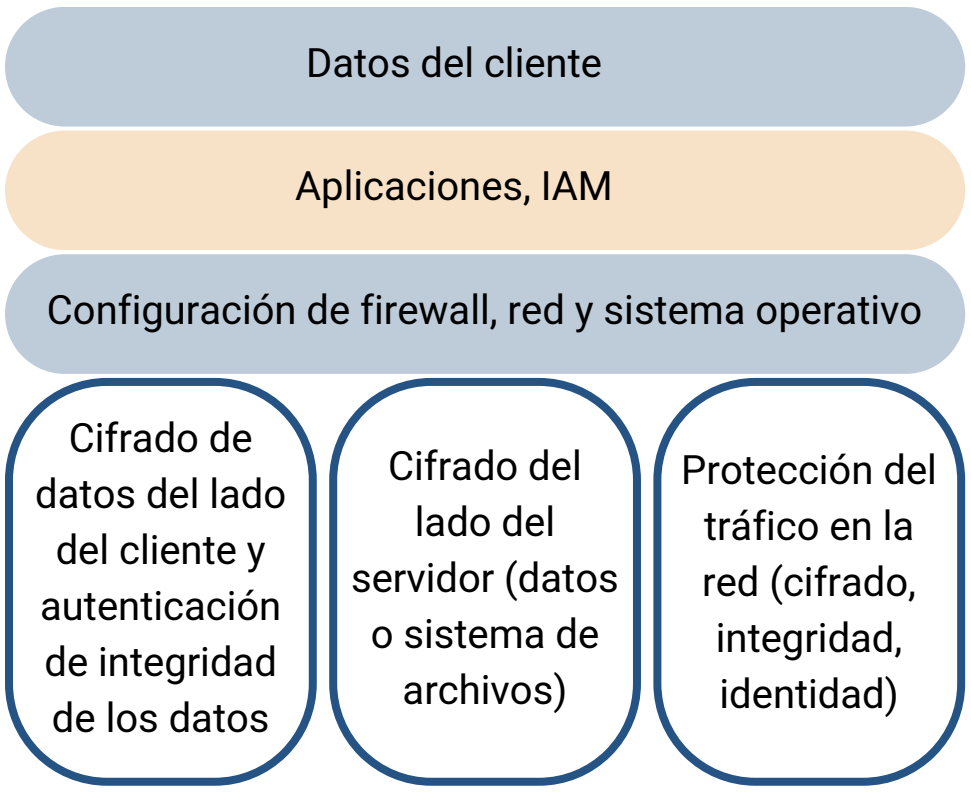
En el marco del modelo de responsabilidad compartida, AWS asume la responsabilidad de salvaguardar la seguridad de la infraestructura en la nube.

Esto implica que AWS gestiona y controla todos los componentes, desde el sistema operativo en el alojamiento bare metal hasta la capa de virtualización del hipervisor, y se extiende hasta la seguridad física de las instalaciones donde operan los servicios en la nube. En esencia, AWS se encarga de proteger la infraestructura global que sostiene todos los servicios ofrecidos en su plataforma.

Las responsabilidades de AWS incluyen garantizar la seguridad física de los centros de datos mediante medidas como el acceso controlado, la presencia de guardias de seguridad, la autenticación de dos factores y la vigilancia por vídeo. Además, AWS se encarga de mantener la infraestructura de hardware y software, que abarca desde servidores y dispositivos de almacenamiento hasta sistemas operativos y software de virtualización. También es responsable de gestionar la infraestructura de red, que incluye routers, switches, balanceadores de carga y firewalls, entre otros, y proporcionar monitoreo constante, protección contra intrusiones y redundancia en la infraestructura de red.

La seguridad de esta infraestructura es la máxima prioridad para AWS. Aunque los clientes no tienen acceso directo a los centros de datos o las instalaciones de AWS, la empresa ofrece informes exhaustivos de auditorías realizadas por terceros que certifican su conformidad con diversas normativas y estándares de seguridad informática.

Responsabilidad del cliente: seguridad en la nube



Responsabilidades de los clientes:

- Sistema operativo de la instancia de Amazon Elastic Compute Cloud (Amazon EC2)
  - Incluidos los parches y el mantenimiento
- Aplicaciones
  - Contraseñas, acceso basado en roles, etc.
- Configuración del grupo de seguridad
- SO o firewalls basados en host
  - Incluidos los sistemas de detección o prevención de instrucciones
- Configuraciones de red
- Administración de cuentas
  - Configuración de inicio de sesión y permisos para cada usuario

Aunque AWS se encarga de salvaguardar y mantener la infraestructura en la nube, los clientes tienen la responsabilidad de asegurar todo lo que implementan en ella. Esto abarca desde los servicios de AWS que utilizan hasta las aplicaciones que están conectadas a la plataforma. Las medidas de seguridad que deben tomar los clientes dependen de los servicios que utilicen y de la complejidad de su sistema.

Entre las responsabilidades de los clientes se encuentran la selección y protección del sistema operativo de las instancias, la seguridad de las aplicaciones desplegadas en los recursos de AWS, la configuración de los grupos de seguridad, el manejo de las configuraciones de firewall y de red, y la gestión segura de las cuentas.

Cuando los clientes hacen uso de los servicios de AWS, mantienen el control total sobre su contenido. Esto implica la gestión de los requisitos de seguridad de dicho contenido, incluyendo qué datos se almacenan en AWS, qué servicios de la plataforma se utilizan con dicho contenido, en qué ubicación geográfica se almacena, el formato y estructura del contenido, quién tiene acceso y cómo se gestionan los derechos de acceso.

Los usuarios conservan el control sobre la implementación de medidas de seguridad para proteger sus propios datos, entornos, aplicaciones, configuraciones de IAM y sistemas operativos.

Características del servicio y responsabilidad en materia de seguridad

Infraestructura como servicio (IaaS)

- El cliente tiene más flexibilidad en lo que respecta a la configuración de redes y almacenamiento.
- El cliente es responsable de administrar más aspectos de la seguridad.
- El cliente configura los controles de acceso.

Plataforma como servicio (PaaS)

- El cliente no necesita administrar la infraestructura subyacente.
- AWS gestiona el sistema operativo, la implementación de parches a la base de datos, la configuración del firewall y la recuperación de desastres.
- El cliente puede centrarse en la administración de código o datos.

La infraestructura como servicio (IaaS) se refiere a aquellos servicios en la nube que proporcionan los componentes básicos de TI, como redes configurables, máquinas virtuales o hardware dedicado, y almacenamiento de datos. Estos servicios ofrecen al cliente un alto nivel de flexibilidad y control sobre los recursos de TI, similares a los recursos informáticos tradicionales que muchos departamentos de TI ya están familiarizados.

Los servicios de AWS, como Amazon EC2, pueden ser considerados como IaaS, lo que implica que los clientes son responsables de configurar y administrar la seguridad. Esto incluye la gestión del sistema operativo de las instancias EC2, la instalación y mantenimiento de software de aplicación, así como la configuración de los grupos de seguridad proporcionados por AWS.

Por otro lado, la plataforma como servicio (PaaS) se refiere a servicios que eliminan la necesidad de que los clientes administren la infraestructura subyacente, como hardware y sistemas operativos. En lugar de eso, los clientes pueden enfocarse exclusivamente en la implementación y administración de aplicaciones. AWS ofrece servicios como AWS Lambda y Amazon RDS que se pueden clasificar como PaaS, ya que AWS gestiona la infraestructura, el sistema operativo y las plataformas. Los clientes solo necesitan acceder a los puntos de conexión para almacenar y recuperar datos.

Con los servicios PaaS, los clientes son responsables de administrar sus datos, organizar sus recursos y aplicar permisos adecuados. Sin embargo, estos servicios son más gestionados por AWS en comparación con los servicios IaaS. Por ejemplo, AWS se encarga de tareas de seguridad como la aplicación de parches en la base de datos y el sistema operativo, la configuración del firewall y la recuperación de desastres.

Software como servidor (SaaS)

- El software está alojado de forma centralizada.
- Cuenta con licencia según el modelo de suscripción o de pago por uso.
- Normalmente, el acceso a los servicios se realiza a través de una navegador web, una aplicación móvil o una interfaz de programación de aplicaciones (API).
- Los clientes no necesitan administrar la infraestructura que respalda el servicio.

El Software como Servicio (SaaS) se refiere a servicios que ofrecen software alojado de forma centralizada y accesible generalmente a través de un navegador web, una aplicación móvil o una interfaz de programación de aplicaciones (API). El modelo de licencia típico para estas ofertas es mediante suscripción o pago por uso. Con el SaaS, los clientes no necesitan preocuparse por administrar la infraestructura subyacente que respalda el servicio.

Algunos servicios de AWS, como AWS Trusted Advisor, AWS Shield y Amazon Chime, pueden clasificarse como ofertas de SaaS, dependiendo de sus características y funcionalidades.

AWS Trusted Advisor es una herramienta en línea que analiza el entorno de AWS de un cliente y ofrece orientación y recomendaciones en tiempo real para ayudar en la provisión de recursos siguiendo las mejores prácticas de AWS. Se ofrece como parte del plan de soporte de AWS, con ciertas características gratuitas y otras disponibles para clientes de Business Support y Enterprise Support.

AWS Shield es un servicio gestionado de protección contra ataques de denegación de servicio distribuido (DDoS) diseñado para proteger las aplicaciones que se ejecutan en AWS. Ofrece detección continua y mitigaciones automáticas que reducen el tiempo de inactividad y la latencia de las aplicaciones. AWS Shield Advanced está disponible para todos los clientes, mientras que el acceso al equipo de respuesta a DDoS requiere Business Support o Enterprise Support de AWS.

Amazon Chime es un servicio de comunicaciones que permite realizar reuniones, chats y llamadas empresariales tanto dentro como fuera de la organización, todo a través de una sola aplicación. Se trata de un servicio de comunicaciones de pago por uso, sin tarifas iniciales ni compromisos a largo plazo.

Actividad: escenario 1 de 2

Considere esta implementación

¿Quién es responsable? ¿AWS o el cliente?

1. ¿Actualizaciones y parches en el sistema operativo en la instancia EC2?
2. ¿Seguridad física del centro de datos?
3. ¿Infraestructura de virtualización?
4. ¿Configuración de grupos de seguridad de EC2?
5. ¿Configuración de las aplicaciones que se ejecutan en la instancia EC2?
6. ¿Actualizaciones o parches de Oracle si la instancia de Oracle se ejecuta como una instancia de Amazon RDS?
7. ¿Actualizaciones o parches de Oracle si Oracle se ejecuta en una instancia de EC2?
8. ¿Configuración de acceso al bucket de S3?

1 el cliente	5 el cliente
2 AWS	6 AWS
3 AWS	7 el cliente
4 el cliente	8 el cliente

En este escenario, la responsabilidad de mantener la seguridad recae tanto en AWS como en el cliente, dependiendo del servicio utilizado.

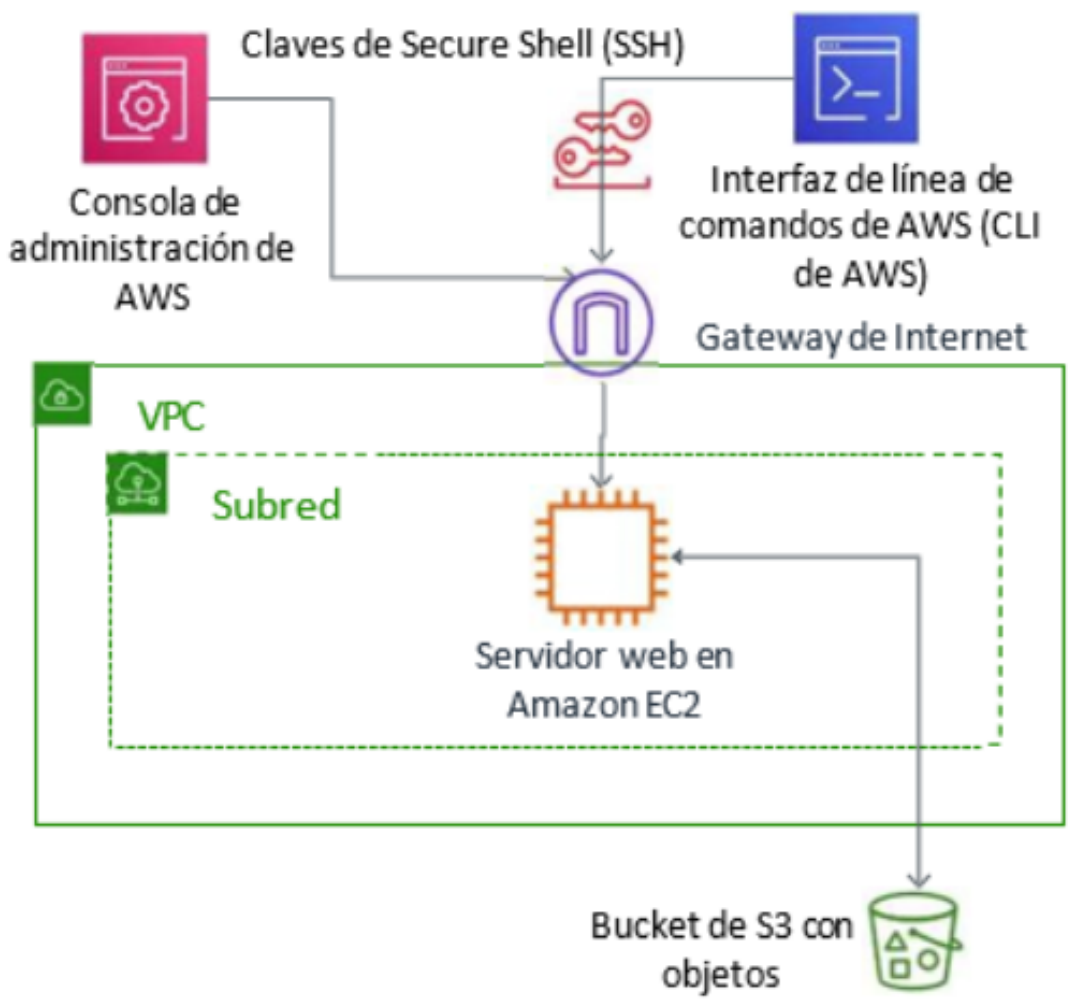
Para Amazon Simple Storage Service (Amazon S3), el cliente es responsable de configurar y gestionar los permisos de acceso adecuados a los datos almacenados en S3, así como de aplicar medidas de seguridad adicionales, como el cifrado de datos en reposo y en tránsito.

En cuanto a la configuración de la nube virtual privada (VPC) con Amazon Virtual Private Cloud (Amazon VPC), el cliente es responsable de definir las reglas de seguridad y acceso en la VPC, incluyendo la configuración de grupos de seguridad y las subredes.

En el caso de la instancia EC2 y la instancia de base de datos de Oracle, la responsabilidad varía dependiendo de si se ejecutan en una instancia EC2 estándar o en Amazon RDS. Si son instancias EC2 estándar, el cliente es responsable de administrar el sistema operativo invitado, aplicar parches de seguridad, mantener el software de aplicación y configurar el firewall (grupo de seguridad) y las reglas de red. Sin embargo, si la base de datos se ejecuta en Amazon RDS, AWS asume la responsabilidad de la administración de la base de datos, incluyendo el aprovisionamiento, las copias de seguridad, los parches de software, el monitoreo y el escalado de hardware.
Consulte las prácticas recomendadas para ejecutar la base de datos de Oracle en AWS.

Actividad: escenario 1 de 2

Considere esta implementación
¿Quién es responsable? ¿AWS o el cliente?



1. ¿Garantizar que la consola de administración de AWS no sea pirateada?
2. ¿Configurar la subred?
3. ¿Configurar la VPC?
4. ¿Proteger frente a interrupciones de red en las regiones de AWS?
5. ¿Proteger las claves SSH?
6. ¿Garantizar el aislamiento de red entre los datos de los clientes de AWS?
7. ¿Garantizar una conexión de red de baja latencia entre el servidor web y el bucket de S3?
8. ¿Requerir la autenticación multifactor para todos los inicios de sesión de los usuarios?

1 AWS	5 el cliente
2 el cliente	6 AWS
3 el cliente	7 AWS
4 AWS	8 el cliente

En este escenario adicional, la responsabilidad de mantener la seguridad recae tanto en AWS como en el cliente, dependiendo del servicio utilizado y las acciones realizadas.

Para el almacenamiento de datos en Amazon S3, el cliente es responsable de configurar adecuadamente los permisos de acceso a los datos almacenados y de aplicar medidas de seguridad, como el cifrado de datos en reposo y en tránsito.

En cuanto a la configuración de la nube virtual privada (VPC) con Amazon VPC, el cliente es responsable de definir las reglas de seguridad y acceso en la VPC, incluyendo la configuración de subredes y la gateway de Internet para permitir el acceso al servidor web.

Para la instancia EC2 que ejecuta el servidor web, el cliente es responsable de administrar el sistema operativo, aplicar parches de seguridad, mantener el software del servidor web actualizado y configurar los mecanismos de seguridad como las claves SSH para acceder al servidor.

En resumen, el cliente tiene la responsabilidad de garantizar la seguridad de los datos almacenados en S3, configurar correctamente la VPC y mantener seguro el servidor web en la instancia EC2. AWS, por su parte, proporciona herramientas y servicios para ayudar al cliente a implementar prácticas de seguridad sólidas y proteger su entorno en la nube.

Estos son algunos de los aprendizajes clave de esta lección:

- AWS y el cliente comparten responsabilidades en materia de seguridad:
  - AWS es responsable de la seguridad de la nube.
  - El cliente es responsable de la seguridad en la nube.
- AWS es responsable de proteger la infraestructura (incluido el hardware, el software, las redes y las instalaciones) que ejecuta los servicios en la nube de AWS.
- En el caso de los servicios clasificados como infraestructura como servicio (IaaS), el cliente es responsable de realizar las tareas de configuración y administración de seguridad necesarias.
  - Por ejemplo, actualizaciones del sistema operativo invitado y configuraciones de parches de seguridad, firewall y grupos de seguridad.