



AWS Academy Cloud Security Foundations  
(LA)

Introduction to Security on AWS Student Guide

Versión 1.0.1

100-ACSECF-10-LA-SG

© 2023, Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

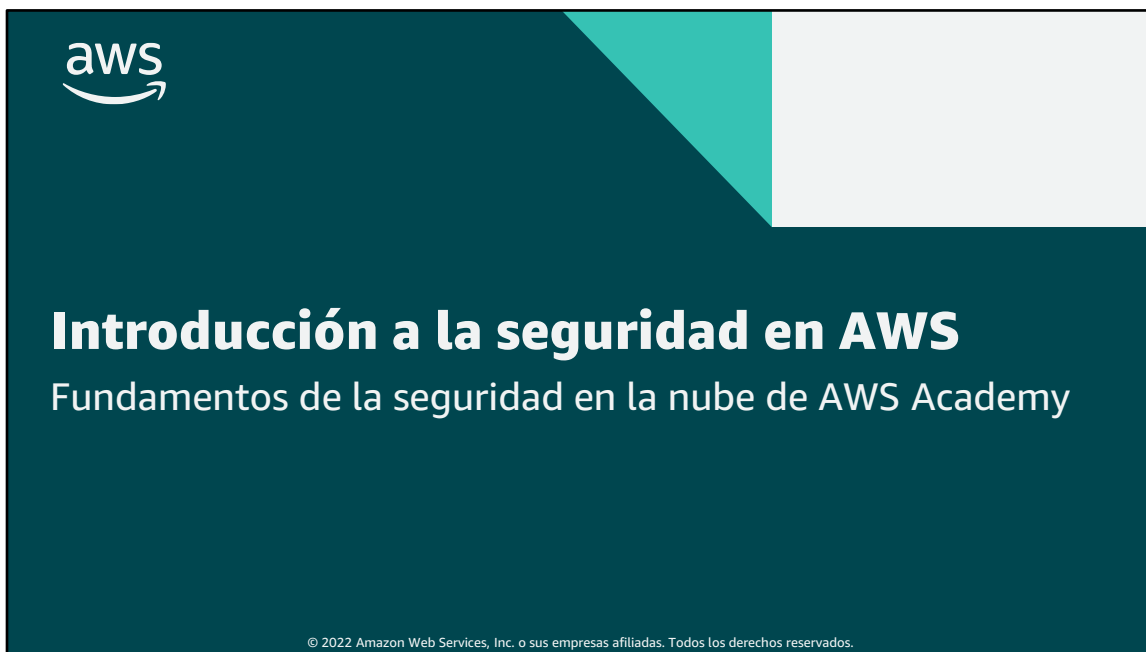
Este contenido no puede reproducirse ni redistribuirse, total ni parcialmente, sin el permiso previo por escrito de Amazon Web Services, Inc. Queda prohibida la copia, el préstamo o la venta de carácter comercial.

Todas las marcas comerciales pertenecen a sus propietarios.

# Contenido

[Introducción a la seguridad en AWS](#)

4



Le damos la bienvenida al módulo Introducción a la seguridad en AWS.



En esta primera sección, se proporciona una introducción al módulo.

## Objetivos del módulo

---

Al finalizar este módulo, podrá hacer lo siguiente:

- Identificar las funciones y beneficios del cómputo en la nube.
- Identificar los principios de seguridad sobre los que está creada la nube de AWS.
- Identificar de qué parte de una aplicación es responsable el usuario para asegurar la nube.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

3

Al finalizar este módulo, podrá hacer lo siguiente:

- Identificar las funciones y beneficios del cómputo en la nube.
- Identificar los principios de seguridad sobre los que está creada la nube de AWS.
- Identificar de qué parte de una aplicación es responsable el usuario para asegurar la nube.

## Información general sobre el módulo

### Secciones

- Seguridad en la nube de AWS
- Principios de diseño para la seguridad
- Modelo de responsabilidad compartida

### Actividad

- Modelo de responsabilidad compartida

### Evaluación de conocimientos



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

4

Este módulo incluye las siguientes secciones:

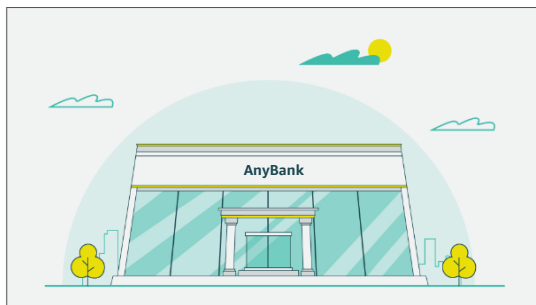
- Seguridad en la nube de AWS
- Principios de diseño para la seguridad
- Modelo de responsabilidad compartida

Este módulo también incluye una actividad sobre el modelo de responsabilidad compartida.

Finalmente, se le pedirá que complete una evaluación de conocimientos que pondrá a prueba su comprensión de los conceptos clave que se abordaron en este módulo.

## Escenario empresarial bancario (1 de 3)

---



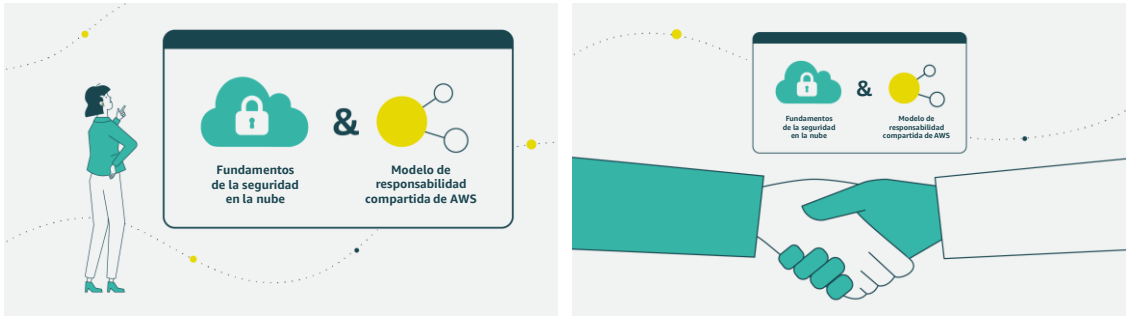
© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

5

Analicemos cómo los conceptos de este módulo se aplican al escenario empresarial bancario.



## Escenario empresarial bancario (2 de 3)



Fundamentos de la seguridad en la nube & Modelo de responsabilidad compartida de AWS

aws

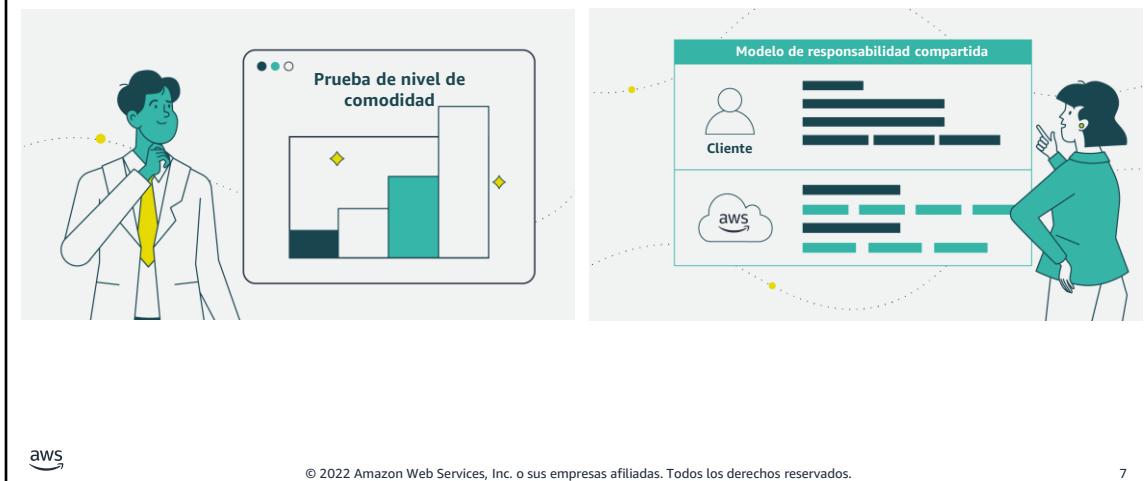
© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

6

Para su primer encuentro con John, María decide presentar información sobre los fundamentos de la seguridad en la nube y el modelo de responsabilidad compartida de AWS.

Esta será una excelente manera de generar confianza y una buena relación con su nuevo supervisor.

## Escenario empresarial bancario (3 de 3)









Al comenzar con los fundamentos de la seguridad en la nube, puede evaluar el nivel de comodidad de John con el tema mientras brinda la información necesaria para presentar su caso de negocios.


María decide presentar el modelo de responsabilidad compartida para explicar cómo tanto el banco como AWS protegerán los recursos del banco con múltiples capas de seguridad. Tiene la intención de utilizar el modelo para demostrar las áreas en las que el banco o AWS serían responsables.



Esta sección cubre la seguridad en la nube de AWS.

## Beneficios de la nube

-  Operar con gastos variables en lugar de gastos fijos.
-  Obtener beneficios de las grandes economías de escala.
-  Dejar de hacer conjeturas sobre las necesidades de capacidad.
-  Aumentar la velocidad y la agilidad.
-  Deje de gastar dinero en la ejecución y el mantenimiento de centros de datos.
-  Convertirse en una empresa global en minutos.


 © 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados. 9

Las empresas pueden obtener los siguientes beneficios al migrar a la nube:


- **Cambie los gastos fijos por gastos variables:** en lugar de tener que invertir mucho en centros de datos y servidores antes de saber cómo los utilizará, pague solo cuando consuma recursos informáticos y pague solo por cuánto consume.
- **Benefíciense de las economías de escala masivas:** mediante el uso de cómputo en la nube, puede lograr un costo variable más bajo que el que puede obtener por su cuenta. Debido a que el uso de cientos de miles de clientes se agrega en la nube, los proveedores como AWS pueden lograr mayores economías de escala, lo que se traduce en precios de pago por uso más bajos.
- **Deje de adivinar sus necesidades de capacidad:** deje de adivinar sus necesidades de capacidad de infraestructura. Cuando toma una decisión sobre la capacidad antes de implementar una aplicación, a menudo utiliza recursos inactivos costosos o se enfrenta a una capacidad limitada. Con el cómputo en la nube, estos problemas desaparecen. Puede acceder a cuanto capacidad necesite, y escalar hacia arriba o hacia abajo según sea necesario con solo unos minutos de antelación.
- **Aumente la velocidad y la agilidad:** en un entorno de cómputo en la nube, los nuevos recursos de TI están a solo un clic de distancia. Esto significa que reduce el tiempo para que esos recursos estén disponibles para sus desarrolladores de semanas a minutos. Esto da como resultado un aumento dramático en la agilidad de la organización, porque el costo y el tiempo que lleva experimentar y desarrollar es significativamente menor.
- **Deje de gastar dinero para ejecutar y mantener centros de datos:** concéntrese en proyectos que diferencien su negocio en lugar de centrarse en la infraestructura. Con cómputo en la nube, puede concentrarse en sus propios clientes, en lugar de en el trabajo pesado de almacenar, apilar y alimentar servidores.
- **Globalícese en minutos:** implemente fácilmente su aplicación en varias regiones del mundo con unos pocos clics. Esto significa que puede proporcionar una latencia más baja y una mejor experiencia para sus clientes a un costo mínimo.

Para más información, consulte ¿Qué es la computación en la nube? en <https://aws.amazon.com/what-is-cloud-computing>.

## La seguridad es familiar



Confidencialidad	Integridad	Disponibilidad
<ul style="list-style-type: none"><li>• Limitar el acceso y la divulgación a usuarios autorizados</li><li>• Evitar el acceso a personas no autorizadas</li></ul>	<ul style="list-style-type: none"><li>• Mantener la uniformidad de los datos a lo largo del ciclo de vida</li><li>• Conservar los datos en reposo y los datos en tránsito</li></ul>	<ul style="list-style-type: none"><li>• Tener acceso a los recursos de información cuando es necesario</li></ul>

 © 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados. 10

La *seguridad* es la práctica de proteger su propiedad intelectual del acceso, uso o modificación no autorizados. La tríada de confidencialidad, integridad y disponibilidad, o CIA, se desarrolló originalmente para resaltar los aspectos importantes de la seguridad de la información dentro de una organización.

*Confidencialidad* hace referencia a limitar el acceso a la información y la divulgación a usuarios autorizados y evitar el acceso a personas no autorizadas.

*Integridad* hace referencia a mantener la consistencia, exactitud y fiabilidad de los datos en todo su ciclo de vida. Esto incluye el “origen” o la “integridad de la fuente”, que es una garantía de que el remitente de esa información es quien se supone que es. La integridad puede significar asegurarse de que la persona o entidad en cuestión ingresó la información correcta. Sin embargo, la integridad de un sistema de información solo puede significar preservar los datos sin corrupción de lo que se transmitió o ingresó al sistema.

*Disponibilidad* hace referencia a la preparación de los recursos de información. Un sistema de información que no está disponible cuando usted lo necesita es casi tan inútil como no tener un sistema de información. Los entornos de TI modernos presentan desafíos para la tríada CIA debido al volumen de información que debe protegerse, la multiplicidad de fuentes de las que provienen los datos y la variedad de formatos.

## Seguridad en la nube de AWS: objetivos

---

- Capacidad de control
- Auditabilidad
- Visibilidad
- Agilidad
- Automatización



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

11

La seguridad en la nube es similar a la seguridad de los centros de datos en las instalaciones: solo que sin los costos y las complejidades de proteger las instalaciones y el hardware. Debido a que la nube no tiene servidores físicos ni dispositivos de almacenamiento, utiliza herramientas de seguridad basadas en software para supervisar y proteger el flujo de información que entra y sale de sus recursos de AWS.

En AWS, nos esforzamos por hacer que la seguridad sea tan familiar como lo que está haciendo hoy. Puede traer los mismos modelos de seguridad que utiliza hoy en su entorno a la nube. Esto incluye proporcionar visibilidad, auditabilidad y capacidad de control a sus recursos en la nube. Además, AWS ofrece varios servicios y herramientas para equiparlo con la agilidad y la automatización que necesita para adaptarse al escalado a nivel de la nube con el objetivo de llevar la seguridad al siguiente nivel.

## Seguridad en la nube de AWS: capacidad de control

- ¿Puedo administrar usuarios de manera efectiva?
- ¿Cómo puedo proporcionar credenciales temporales?
- ¿Puedo usar mis propias claves?



**AWS Identity and Access Management (IAM)**



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

12

AWS proporciona métodos y herramientas para administrar el control de acceso de usuarios, grupos y roles; proporcionar credenciales de seguridad temporales y controlar las claves de cifrado.

El servicio AWS Identity and Access Management (IAM) lo ayuda a controlar de forma segura el acceso a los recursos de AWS para sus usuarios. IAM se emplea para controlar quién puede utilizar los recursos de AWS (autenticación), qué recursos se pueden utilizar y de qué formas (autorización). Puede definir permisos granulares para entidades, como usuarios, grupos o roles. Esto permite que las entidades administren y utilicen recursos en su cuenta de AWS sin tener que compartir su contraseña o clave de acceso.

Puede conceder diferentes permisos a diferentes personas para distintos recursos. Por ejemplo, puede permitir que algunos usuarios tengan acceso completo a Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3) y otros servicios de AWS. Para otros usuarios, puede permitir acceso de solo lectura a algunos buckets de S3, conceder permiso para administrar solo algunas instancias de EC2 o acceder a su información de facturación, y restringir lo demás. Con IAM, también puede permitir que los usuarios que ya tienen contraseñas en otro lugar accedan a su cuenta de AWS. Por ejemplo, los usuarios con contraseñas en su red corporativa o con un proveedor de identidades de Internet pueden obtener acceso a la cuenta de AWS.

Puede utilizar el servicio de token de seguridad de AWS (AWS STS) para crear y proporcionar a los usuarios de confianza credenciales de seguridad temporales que pueden controlar el acceso a sus recursos de AWS. Las credenciales de seguridad temporales funcionan casi de manera idéntica a las credenciales de clave de acceso a largo plazo que pueden usar sus usuarios de IAM.

Con AWS CloudHSM, puede proteger sus claves de cifrado dentro de módulos de seguridad de hardware (HSM) que están diseñados y validados según los estándares gubernamentales para la administración segura de claves. Puede generar, almacenar y administrar de forma segura las claves criptográficas utilizadas para el cifrado de datos de una manera que garantice que solo usted tenga acceso a las claves. CloudHSM lo ayuda a cumplir con los estrictos requisitos de administración de claves en la nube de AWS sin sacrificar el rendimiento de la aplicación.



## Seguridad en la nube de AWS: auditabilidad

- ¿Quién tiene acceso a este recurso?
- ¿Quién realizó qué acción?
- ¿Cuándo se realizó la acción y desde dónde?
- ¿Dónde está la evidencia?



AWS CloudTrail



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

13

Es importante probar y validar sus medidas de protección para asegurarse de que cumplan con los requisitos de cumplimiento y funcionen según lo previsto. Las organizaciones suelen depender de auditorías periódicas, ya sean internas o externas, de sus entornos para garantizar la conformidad con las políticas y normativas.

Los servicios de AWS, como AWS CloudTrail, pueden ayudarlo a responder preguntas como, por ejemplo, ¿qué acciones realizó un usuario específico durante un periodo de tiempo determinado? Para un recurso específico, ¿qué usuario ha realizado acciones en él durante un periodo de tiempo determinado? ¿Cuál es la dirección IP de origen de una actividad específica?

## Seguridad en la nube de AWS: visibilidad

---

- ¿Qué hay en mi entorno?
- ¿Qué impacto tuvo una acción en particular?
- ¿Qué ha cambiado?
- ¿Dónde está la evidencia?



AWS Config



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

14

El primer paso para asegurar sus activos es saber cuáles son. No debería necesitar adivinar en qué consiste su inventario de TI, quién accede a sus recursos y qué acciones ha ejecutado alguien en sus recursos.

AWS ofrece herramientas para realizar un seguimiento y supervisar sus recursos de AWS, de modo que tenga una visibilidad instantánea de su inventario y de la actividad de sus usuarios y aplicaciones. Por ejemplo, al usar AWS Config, puede descubrir recursos de AWS existentes, exportar un inventario completo de sus recursos de AWS con todos los detalles de configuración y determinar cómo se configuró un recurso en cualquier momento. Estas capacidades pueden ayudarlo con la auditoría de cumplimiento, el análisis de seguridad, el seguimiento de cambios de recursos y la resolución de problemas.

## Seguridad en la nube de AWS: agilidad y automatización

- ¿Cómo garantizo una alta disponibilidad?
- ¿Puedo implementar automáticamente aplicaciones con configuraciones relacionadas con la seguridad y el cumplimiento?
- ¿Cómo puedo aplicar comprobaciones de seguridad de manera reproducible?



**AWS CloudFormation**



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

15

El aumento de la agilidad y la capacidad de realizar acciones más rápido, a mayor escala y a menor costo, no invalida los principios bien establecidos de seguridad de la información. El escalado automático para garantizar una alta disponibilidad durante un ataque de seguridad es una de las formas en que AWS brinda agilidad para satisfacer las necesidades. AWS diseña centros de datos con exceso de ancho de banda, de modo que, si se produce una interrupción importante, haya suficiente capacidad disponible para equilibrar la carga del tráfico y direccionarlo a los sitios restantes, a fin de minimizar el impacto en nuestros clientes. Los clientes también utilizan esta estrategia de múltiples regiones y múltiples zonas de disponibilidad para crear aplicaciones altamente resistentes a un costo disruptivamente bajo, para replicar y respaldar datos con facilidad, y para implementar controles de seguridad globales de manera uniforme en toda su empresa.

Las herramientas de AWS están especialmente diseñadas y adaptadas a su entorno, tamaño y requisitos globales exclusivos. Al crear herramientas de seguridad desde cero, AWS puede automatizar muchas de las tareas rutinarias en las que los expertos en seguridad normalmente dedican tiempo. Esto significa que los expertos en seguridad de AWS pueden dedicar más tiempo a centrarse en medidas para aumentar la seguridad de su entorno en la nube de AWS. Los clientes también pueden automatizar las funciones de ingeniería y operaciones de seguridad mediante el uso de un conjunto integral de API y herramientas.

Cuando automatiza mediante el uso de servicios de AWS como AWS CloudFormation, en lugar de implementar manualmente un entorno para la resolución de problemas forenses, por ejemplo, puede hacer que AWS implemente un entorno de manera segura y reproducible.

## **Aprendizajes clave: seguridad en la nube de AWS**



- La tríada de confidencialidad, integridad y disponibilidad, o CIA, se desarrolló originalmente para resaltar los aspectos importantes de la seguridad de la información dentro de una organización.
- AWS ofrece varias herramientas y funciones para ayudarlo a cumplir los objetivos de seguridad relacionados con la capacidad de control, la auditabilidad, la visibilidad, la agilidad y la automatización.

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

16

Estos son algunos aprendizajes clave de esta sección del módulo:

- La tríada de confidencialidad, integridad y disponibilidad, o CIA, se desarrolló originalmente para resaltar los aspectos importantes de la seguridad de la información dentro de una organización.
- AWS ofrece varias herramientas y funciones para ayudarlo a cumplir los objetivos de seguridad relacionados con la capacidad de control, la auditabilidad, la visibilidad, la agilidad y la automatización.



En esta sección, se describen los principios de diseño de seguridad.

## 1. Aplicar el principio de mínimo privilegio



- Conceder acceso según sea necesario
- Hacer cumplir la división de controles
- Evitar las credenciales a largo plazo



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

18

Se describen los siete principios de diseño del pilar de seguridad del Marco de AWS Well-Architected. Seguir estos principios puede ayudarlo a fortalecer la seguridad de su carga de trabajo y puede ayudarlo a guiar sus conversaciones sobre seguridad y cumplimiento.

–Una cultura de seguridad organizacional debe construirse sobre el principio del mínimo privilegio. Solo conceda acceso a los datos y otros recursos a las personas que realmente lo necesitan. Puede comenzar por denegar el acceso a todo y otorgar acceso según sea necesario en función de los roles de trabajo.

–

–Una práctica recomendada de seguridad es hacer cumplir la separación de funciones con la autorización adecuada para cada interacción con sus recursos de AWS. Establezca expectativas sobre cómo se delegará la autoridad a través de los ingenieros de software, el personal de operaciones y otras funciones laborales que están involucradas en la adopción de la nube.

–

–Al reducir o incluso eliminar la dependencia de las credenciales a largo plazo, puede disminuir su área de superficie de ataque. Puede usar credenciales temporales y requerir identidades para adquirirlas dinámicamente. Para las identidades de la fuerza laboral, use AWS Single Sign-On o la federación con IAM para acceder a las cuentas de AWS. Para las identidades de máquinas, como las instancias de EC2 o las funciones de AWS Lambda, se requiere el uso de roles de IAM, en lugar de usuarios de IAM con claves de acceso a largo plazo.

–

–Identity and Access Management son partes clave de un programa de seguridad de la información para garantizar que solo los usuarios y componentes autorizados y autenticados puedan acceder a sus recursos, y solo de la manera que usted desea. En AWS, IAM es el servicio principal para la administración de permisos. El servicio proporciona la capacidad de controlar el acceso programático y de usuarios a los servicios y recursos de AWS.

Con IAM, puede definir entidades principales (es decir, cuentas, usuarios, funciones y servicios que pueden realizar acciones en su cuenta) y desarrollar políticas granulares alineadas con estas entidades. También tiene la capacidad de exigir prácticas sólidas de contraseña, como establecer un nivel de complejidad, evitar la

reutilización y hacer cumplir la autenticación multifactor (MFA). Puede usar la federación con su servicio de Directory Service Para las cargas de trabajo que requieren que los sistemas tengan acceso a AWS, IAM puede proporcionar acceso seguro a través de funciones, perfiles de instancia, identidad federada y credenciales temporales.

## 2. Habilitar la trazabilidad



- Supervisar las acciones y los cambios
- Usar registros y métricas
- Auditar los recursos de la nube



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

19

Con AWS, puede supervisar y auditar las acciones y los cambios en su entorno en tiempo real, y alertar sobre ellos. AWS proporciona registro nativo, así como servicios que puede utilizar para proporcionar una mayor visibilidad casi en tiempo real de las ocurrencias en su entorno. Integre estas herramientas con sus soluciones existentes de registro y supervisión. Conozca qué cargas de trabajo están implementadas y operativas, de modo que pueda auditar y asegurarse de que el entorno esté funcionando en los niveles de gobierno de seguridad esperados y cumpla con los estándares de seguridad requeridos.

En AWS, puede implementar controles de detección procesando registros y eventos, y supervisando, lo que permite la auditoría, el análisis automatizado y las alarmas. Los registros de CloudTrail, las llamadas API de AWS y Amazon CloudWatch brindan supervisión de métricas con alarmas, y AWS Config brinda el historial de configuración. Amazon GuardDuty es un servicio administrado de detección de amenazas que supervisa continuamente comportamientos malintencionados o no autorizados para ayudarlo a proteger sus cuentas y cargas de trabajo de AWS. Los registros de nivel de servicio también están disponibles; por ejemplo, puede usar Amazon S3 para registrar solicitudes de acceso.



### 3. Proteger todas las capas



- Utilizar un enfoque de defensa en profundidad
- Utilizar diferentes servicios de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

20

En lugar de centrarse únicamente en la protección de una sola capa exterior, aplique un enfoque de defensa en profundidad con otros controles de seguridad. Esto significa aplicar seguridad a todas las capas, como su red, aplicación y almacén de datos. Por ejemplo, puede solicitar a los usuarios que se autenticuen fuertemente en una aplicación. Además, asegúrese de que los usuarios provengan de una ruta de red confiable y requieran acceso a las claves de descifrado para procesar los datos cifrados. Uno de los beneficios de utilizar AWS es que nuestros servicios también están diseñados para la integración. Puede utilizar varios servicios de AWS juntos a fin de proporcionar el entorno más seguro para sus datos y recursos.

Los clientes de AWS pueden adaptar o reforzar la configuración de una instancia de EC2, un contenedor de Amazon Elastic Container Service (Amazon ECS) o una instancia de AWS Elastic Beanstalk y conservar esta configuración en una imagen de máquina de Amazon (AMI) inmutable. Luego, todos los nuevos servidores virtuales (instancias) lanzados con esta AMI reciben la configuración reforzada, ya sea que se lancen manualmente o mediante escalado automático.

## 4. Automatizar la seguridad



- Automatizar las tareas de seguridad de rutina con las API
- Implementar infraestructura como código



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

21

AWS desarrolla herramientas de seguridad especialmente diseñadas que pueden ayudarlo a automatizar muchas de las tareas rutinarias a las que los expertos en seguridad normalmente dedican tiempo. Esto significa que los expertos en seguridad pueden dedicar más tiempo a centrarse en las medidas para aumentar la seguridad de su entorno en la nube de AWS.

Puede automatizar las funciones de ingeniería y operaciones de seguridad mediante el uso de un conjunto integral de API y herramientas. Puede automatizar por completo la administración de identidades, la seguridad de la red y la protección de datos, y las capacidades de supervisión, y entregarlas mediante el uso de métodos de desarrollo de software populares que ya tiene implementados. En lugar de tener personas que supervisen su posición de seguridad y reaccionen ante un evento, con la automatización, su sistema puede supervisar, revisar e iniciar una respuesta.

En la nube de AWS, puede convertir su infraestructura en código. Con esta capacidad, puede automatizar la creación de entornos confiables para realizar investigaciones y análisis forenses más profundos. Puede ejecutar simulaciones de respuesta a incidentes y utilizar herramientas con automatización para aumentar la velocidad de la detección, la investigación y la recuperación. Al automatizar las implementaciones y el mantenimiento, puede eliminar el acceso del operador para reducir la superficie de ataque.

## 5. Proteger los datos en tránsito y los datos en reposo



- Utilizar los controles de acceso y cifrado
- Clasificar los datos con etiquetas
- Aprovechar las conexiones de VPN y TLS



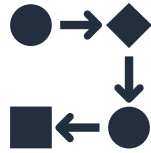
© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

22

La protección de los datos es una parte fundamental de la creación y la operación de los sistemas de información. AWS proporciona servicios y características que lo ayudan a proteger sus datos en reposo y en tránsito. Las medidas de seguridad incluyen controles de acceso detallados a los objetos, la creación y el control de las claves de cifrado que se utilizan para cifrar sus datos, la selección de métodos de cifrado apropiados, la validación de la integridad y la retención de datos adecuada. Para ayudarlo a administrar la protección, implemente un esquema de etiquetado para clasificar sus datos en niveles de confidencialidad. Otra práctica recomendada de seguridad es construir mecanismos para proteger los datos en tránsito, como el uso de conexiones de red privada virtual (VPN) y Transport Layer Security (TLS).

AWS proporciona varios medios para cifrar datos en reposo y datos en tránsito. Creamos funciones en nuestros servicios que facilitan el cifrado de sus datos. Por ejemplo, hemos implementado el cifrado del lado del servidor (SSE) para Amazon S3 para que le resulte más fácil almacenar sus datos de forma cifrada. También puede hacer arreglos para que Elastic Load Balancing (ELB) maneje todo el proceso de cifrado y descifrado de HTTPS (generalmente conocido como terminación SSL).

## 6. Prepararse para los eventos de seguridad



- Mitigar el impacto de los incidentes de seguridad
- Crear procesos para aislar los incidentes y restaurar las operaciones



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

23

Incluso con controles preventivos y de detección maduros, debe implementar procesos para responder y mitigar el impacto potencial de los incidentes de seguridad. La arquitectura de la carga de trabajo afecta fuertemente su capacidad de operar de modo eficaz durante un incidente, aislar o contener los sistemas y restaurar las operaciones a un estado correcto conocido. Instale las herramientas y el acceso antes de un incidente de seguridad. Luego, practique rutinariamente la respuesta a incidentes durante los días de juego. Esto lo ayudará a garantizar que su arquitectura pueda adaptarse a una investigación y recuperación oportunas. En otro módulo de este curso, se describe una variedad de enfoques para la respuesta ante incidentes.

En AWS, las siguientes prácticas facilitan una respuesta eficaz ante incidentes:

- El registro detallado está disponible. Los registros contienen contenido importante, como acceso a archivos y cambios.
- Los eventos se pueden procesar automáticamente y pueden invocar herramientas que automaticen las respuestas mediante el uso de las API de AWS.
- Puede preaprovisionar herramientas y una "sala limpia" mediante AWS CloudFormation. Esto proporciona la capacidad de llevar a cabo análisis forenses en un entorno seguro y aislado.

## 7. Minimizar la superficie de ataque



- Prepararse para escalar y absorber el ataque
- Defender los recursos expuestos



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

24

Generalmente, un ciberataque se cierra debido a dos razones: o los atacantes se agotan y se dan por vencidos o los atacantes logran su objetivo. Reduzca su exposición al acceso no deseado fortaleciendo los sistemas operativos y minimizando los componentes, las bibliotecas y los servicios consumibles externos en uso. Comience por reducir los componentes no utilizados, como los paquetes y las aplicaciones del sistema operativo. Configure grupos de seguridad y listas de control de acceso a la red (ACL) en Amazon Virtual Private Cloud (Amazon VPC) para ayudar a reducir la superficie de ataque de sus aplicaciones.

Ciertos servicios de AWS, como AWS Auto Scaling y Amazon CloudFront, brindan a las aplicaciones la capacidad de escalar para absorber ataques comunes a la capa de infraestructura. Un ataque de reflexión UDP tiene lugar cuando el atacante solicita información al equipo objetivo utilizando una dirección de origen falsificada. Una inundación SYN es un tipo de ataque por denegación de servicio distribuido (DDoS) que tiene como objetivo hacer que un servidor no esté disponible para el tráfico legítimo al consumir todos los recursos disponibles del servidor. Mediante el uso de técnicas como el escalado automático, puede absorber mayores volúmenes de ataques a la capa de aplicación.

Para más información, consulte el documento técnico Pilar de seguridad: Marco de AWS Well-Architected en <https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html>.

## **Aprendizajes clave: principios de diseño de seguridad**



Los principios de diseño para la seguridad en la nube son los siguientes:

- Aplicar el principio de mínimo privilegio.
- Habilitar la trazabilidad.
- Proteger todas las capas.
- Automatizar la seguridad.
- Proteger los datos en tránsito y los datos en reposo.
- Prepararse para los eventos de seguridad.
- Minimizar la superficie de ataque.

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

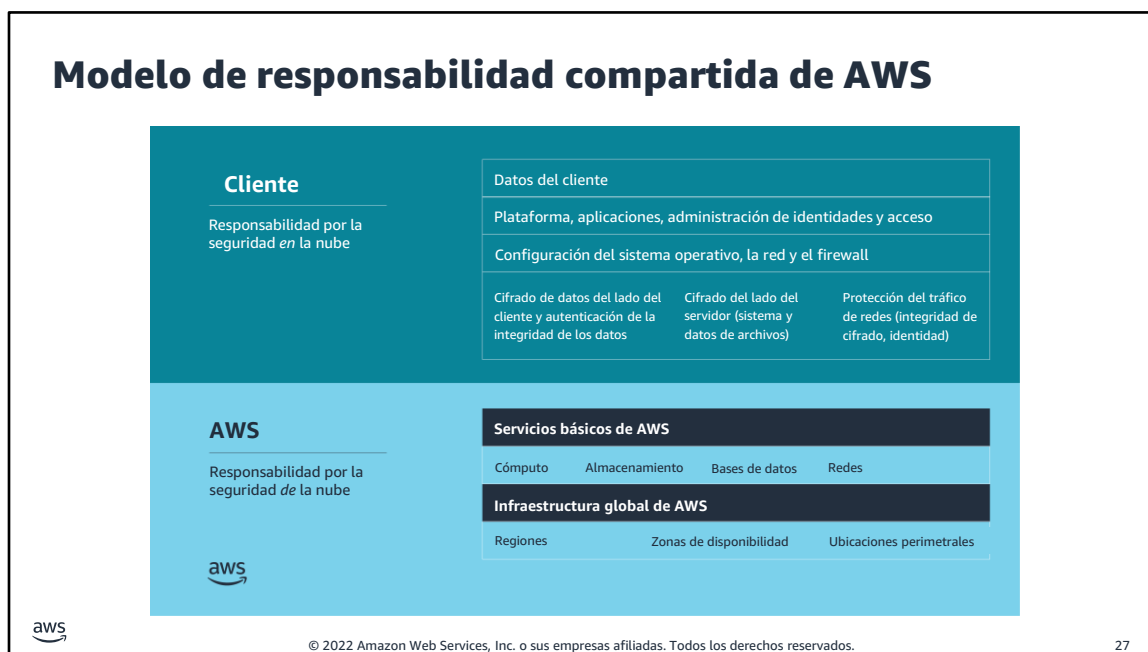
25

Los puntos clave de esta sección del módulo son los principios de diseño para la seguridad en la nube:

- Aplicar el principio de mínimo privilegio.
- Habilitar la trazabilidad.
- Proteger todas las capas.
- Automatizar la seguridad.
- Proteger los datos en tránsito y los datos en reposo.
- Prepararse para los eventos de seguridad.
- Minimizar la superficie de ataque.



En esta sección, se analiza el modelo de responsabilidad compartida.



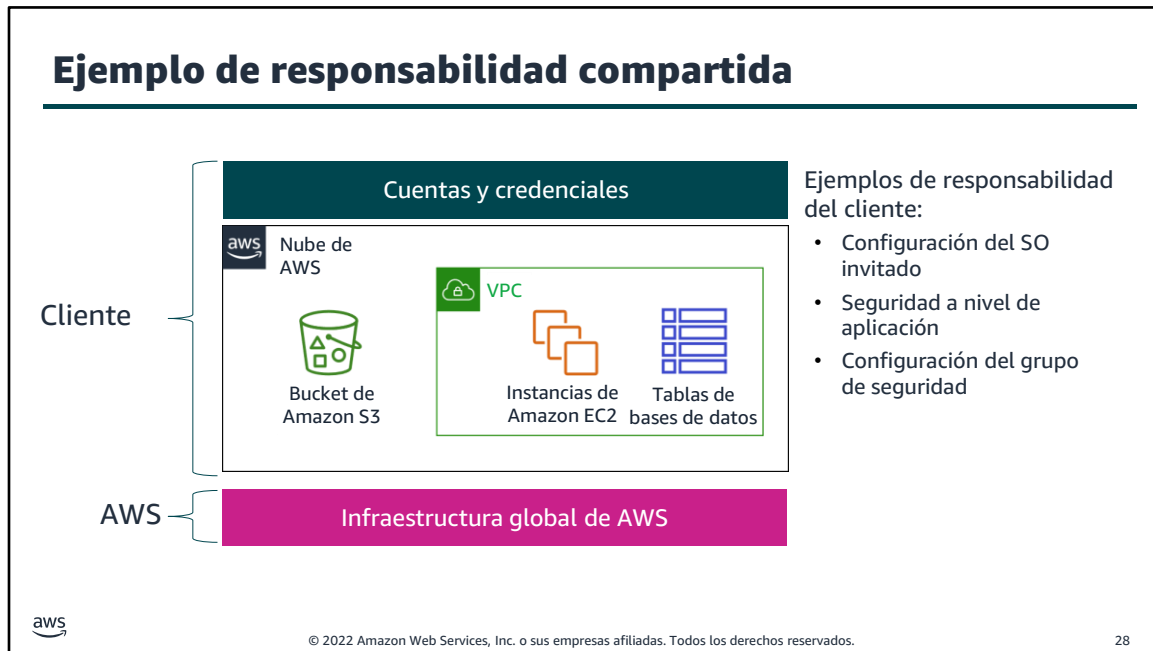
**Para la accesibilidad:** modelo de responsabilidad compartida en el que se enumeran las responsabilidades del cliente y de AWS. El cliente es responsable de la seguridad *en* la nube. Esto incluye los datos del cliente. Administración de accesos, identidades, plataforma y aplicaciones. Configuración de firewall, red y sistema operativo. Cifrado de datos del lado del cliente e integridad de datos, autenticación. Cifrado del lado del servidor del sistema de archivos y datos. Protección del tráfico de redes, incluidos el cifrado, la integridad y la identidad. AWS es responsable de la seguridad *de* la nube. Esto incluye los servicios básicos de AWS para cómputo, almacenamiento, bases de datos y redes. Además, incluye la infraestructura global de AWS, que abarca las regiones, las zonas de disponibilidad y las ubicaciones perimetrales. **Fin de la descripción de accesibilidad.**

La seguridad y el cumplimiento son responsabilidades compartidas entre AWS y los clientes. AWS opera, administra y controla la seguridad *de* la nube. Esta responsabilidad incluye asegurar los componentes, desde el sistema operativo del host y la capa de virtualización hasta la seguridad física de las instalaciones donde opera el servicio. AWS es responsable de proteger la infraestructura global que ejecuta todos los servicios que se ofrecen en la nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

Usted asume la responsabilidad y la administración *en* la nube. Los pasos de seguridad que deben seguir dependen de los servicios que utilizan y de la complejidad de su sistema. Las responsabilidades del cliente incluyen seleccionar y proteger los sistemas operativos que se ejecutan en instancias EC2 y proteger las aplicaciones que se lanzan en los recursos de AWS. Los clientes también deben seleccionar y manejar configuraciones de grupos de seguridad, configuraciones de firewall, configuraciones de red y administración segura de cuentas. Los clientes también son responsables de administrar sus datos, incluidas las opciones de cifrado.

Para reiterar, AWS protege el hardware, el software, las instalaciones y las redes que ejecutan todos los productos y servicios de AWS. Usted es responsable de lo que implemente mediante el uso de productos y servicios de AWS, y de las aplicaciones que conecte a AWS. Los pasos de seguridad que deben seguir dependen de los servicios que utilizan y de la complejidad de su sistema.



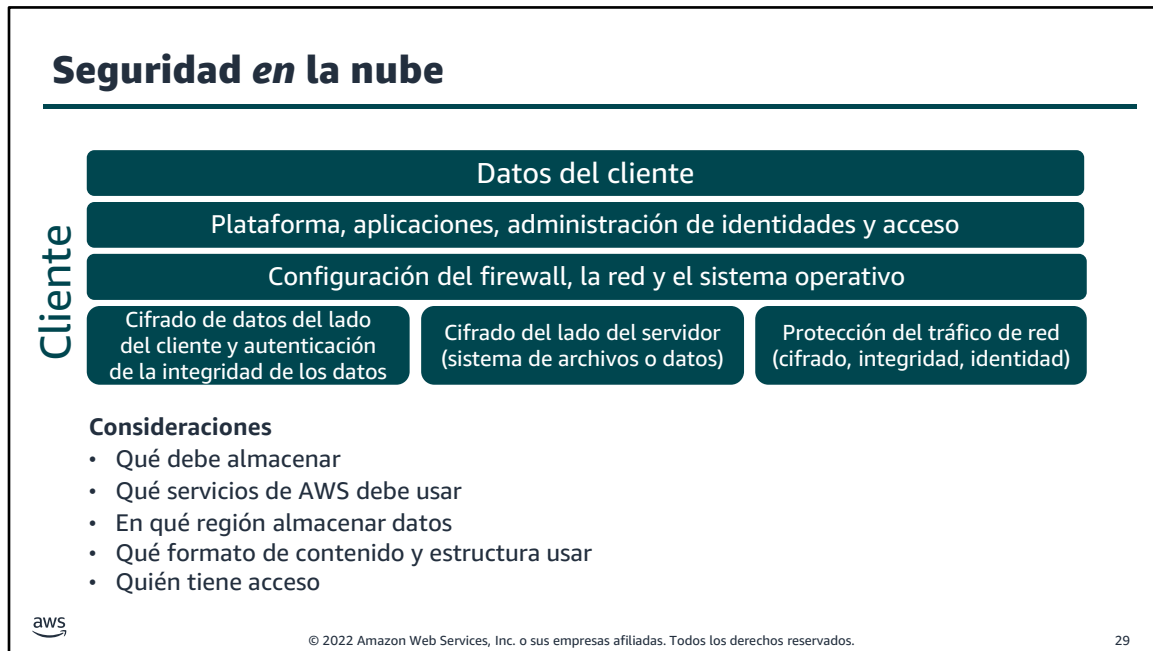


Considere un ejemplo en el que su empresa utiliza Amazon S3 para almacenar datos. Su entorno de AWS también incluye instancias de EC2 y una instancia de Amazon Relational Database Service (Amazon RDS). Estos recursos ejecutan una base de datos MySQL, que se implementa dentro de una nube virtual privada (VPC). Una instancia de EC2 aloja un servidor web y la aplicación web que se ejecuta en ella utiliza la base de datos para almacenar datos de la aplicación.

En este escenario, AWS es responsable de proteger la infraestructura global, que contiene los servidores físicos que alojan las máquinas virtuales y el hardware de almacenamiento. Estas máquinas virtuales y hardware de almacenamiento alojan su bucket de S3, instancias de EC2 e instancia de base de datos. AWS es responsable de la seguridad de la infraestructura de red física que garantiza que se pueda acceder a estos componentes. AWS también es responsable de la seguridad de la capa del hipervisor que aloja las instancias de EC2. (El hipervisor es el sistema operativo del host que ejecuta las instancias de EC2, que son máquinas virtuales que ejecutan sistemas operativos invitados).

Usted (el cliente) es responsable de administrar el sistema operativo huésped que se ejecuta en las instancias de EC2 (incluidas las actualizaciones y los parches de seguridad del sistema operativo Microsoft Windows o Linux). También es responsable de administrar cualquier software de aplicación o utilidades que instale. Además, es responsable de la configuración de los grupos de seguridad que controlan el acceso a la red a cada instancia de EC2 y a la instancia de la base de datos RDS. También es responsable de configurar la seguridad en el bucket de S3 y los objetos que almacena en él. Por ejemplo, podría usar una o más de las funciones de seguridad que proporciona AWS, como políticas de buckets, cifrado de datos y acceso público a buckets de S3.

Para más información, consulte el Modelo de responsabilidad compartida en <https://aws.amazon.com/compliance/shared-responsibility-model>.



Si bien AWS asegura y mantiene la infraestructura de la nube, usted es responsable de proteger todo lo que coloca *EN* la nube.

Antes de diseñar cualquier carga de trabajo, debe implementar prácticas que influyan en la seguridad. Querrá controlar quién puede hacer qué. Además, desea poder identificar incidentes de seguridad, proteger sus sistemas y servicios y mantener la confidencialidad e integridad de los datos a través de la protección de datos. Debe tener un proceso bien definido y practicado para responder a los incidentes de seguridad. Estas herramientas y técnicas son importantes porque respaldan objetivos, como la prevención de pérdidas financieras o el cumplimiento de obligaciones normativas.

Debido a que AWS protege físicamente la infraestructura que admite nuestros servicios en la nube, como cliente de AWS puede concentrarse en usar los servicios para lograr sus objetivos. La nube de AWS también proporciona un mayor acceso a los datos de seguridad y un enfoque automatizado para responder a los eventos de seguridad.

Al utilizar los servicios de AWS, usted mantiene un control total sobre su contenido y es responsable de administrar los requisitos de seguridad críticos, incluidos los siguientes:

- El contenido que elige almacenar en AWS
- Los servicios de AWS que se utilizan con el contenido
- El país en el que se almacena ese contenido
- El formato y la estructura de ese contenido, y si está enmascarado, anónimo o cifrado
- Quién tiene acceso a ese contenido y cómo se otorgan, administran y revocan esos derechos de acceso

Usted conserva el control de la seguridad que elige implementar para proteger sus propios datos, plataforma, aplicaciones, administración de acceso e identidad y sistema operativo. Esto significa que el modelo de responsabilidad compartida cambia según los servicios de AWS que utilice.

## Actividad: Modelo de responsabilidad compartida



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

30

Ahora completará una actividad sobre el modelo de responsabilidad compartida y las responsabilidades de AWS y el cliente.

## Actividad: Escenario 1 de 2

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



1. ¿Actualizaciones y parches del sistema operativo en la instancia de EC2?
2. ¿Seguridad física de los centros de datos?
3. ¿Infraestructura de virtualización?
4. ¿Configuración del grupo de seguridad EC2?
5. ¿Configuración de aplicaciones que se ejecutan en la instancia de 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?



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

31

**Para la accesibilidad:** el diagrama arquitectónico muestra un cuadro de la nube de AWS que contiene un área de infraestructura global de AWS, así como un bucket de Amazon S3 y, finalmente, una VPC que contiene una instancia de Amazon EC2 y una instancia de Oracle. **Fin de la descripción de accesibilidad.**

Considere el caso en el que un cliente utiliza los recursos y servicios de AWS que se muestran aquí. El cliente utiliza Amazon S3 para almacenar datos. El cliente administra una VPC que contiene una instancia de EC2 y una instancia de Amazon RDS para Oracle Database.

¿Quién es responsable de mantener la seguridad de cada componente? ¿AWS o el cliente?

## Actividad: Respuestas de Escenario 1 de 2

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



1. ¿Actualizaciones y parches del sistema operativo en la instancia de EC2?

**Respuesta: El cliente**

2. ¿Seguridad física de los centros de datos?

**Respuesta: AWS**

3. ¿Infraestructura de virtualización?

**Respuesta: AWS**

4. ¿Configuración del grupo de seguridad EC2?

**Respuesta: El cliente**

5. ¿Configuración de aplicaciones que se ejecutan en la instancia de EC2?

**Respuesta: El cliente**

6. ¿Actualizaciones o parches de Oracle si la instancia de Oracle se ejecuta como una instancia de Amazon RDS?

**Respuesta: AWS**

7. ¿Actualizaciones o parches de Oracle si Oracle se ejecuta en una instancia de EC2?

**Respuesta: El cliente**

8. ¿Configuración de acceso al bucket de S3?

**Respuesta: El cliente**



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

32

**Para la accesibilidad:** el diagrama arquitectónico muestra un cuadro de la nube de AWS que contiene un área de infraestructura global de AWS, así como un bucket de Amazon S3 y, finalmente, una VPC que contiene una instancia de Amazon EC2 y una instancia de Oracle. **Fin de la descripción de accesibilidad.**

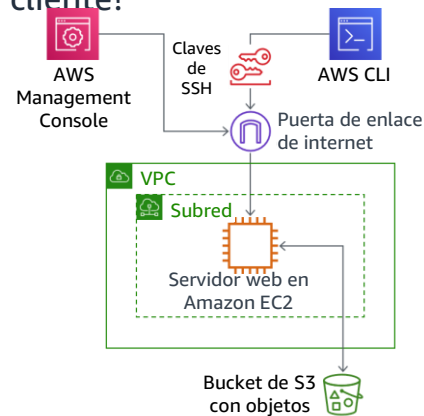
El cliente controla la seguridad *en* la nube. En el escenario anterior, esto incluye actualizar y parchear el sistema operativo huésped y el software de la aplicación asociada en la instancia de EC2, y la configuración del firewall del grupo de seguridad proporcionado por AWS. Debido a que la responsabilidad del cliente está determinada por los servicios de la nube de AWS que seleccione, las actualizaciones o los parches de Oracle serán responsabilidad del cliente si ejecuta la base de datos de Oracle en una instancia de EC2. El cliente también es responsable de utilizar las herramientas de IAM para aplicar los permisos correctos en el nivel de la plataforma, como para los buckets de S3, y en el nivel de usuario o grupo de IAM.

AWS administra la seguridad *de* la nube al garantizar que la infraestructura de AWS cumpla con los requisitos reglamentarios y las prácticas recomendadas globales y regionales. AWS opera, administra y controla los componentes desde el sistema operativo del host y la capa de virtualización hasta la seguridad física de las instalaciones en las que opera el servicio.

En este ejemplo, AWS es responsable de la seguridad física del centro de datos y la infraestructura de virtualización. Si la instancia de Oracle se ejecuta como una instancia de Amazon RDS, AWS es responsable de las actualizaciones y los parches de Oracle. Amazon RDS automatiza tareas administrativas comunes, como realizar copias de seguridad y aplicar parches al software que alimenta su base de datos.

## Actividad: Escenario 2 de 2

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



1. ¿Se asegura de que la Consola de administración de AWS no sea pirateada?
2. ¿Configurando la subred?
3. ¿Configurando la VPC?
4. ¿Protección contra las interrupciones de la red en las regiones de AWS?
5. ¿Proteger las claves SSH?
6. ¿Garantizar el aislamiento de la 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. ¿Hacer cumplir la autenticación multifactor para todos los inicios de sesión de los usuarios?



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

33

**Para la accesibilidad:** diagrama arquitectónico en el que se muestra un servidor web que se ejecuta en EC2 dentro de una subred y VPC. El servidor web se conecta a un bucket de S3. Se puede acceder al servidor web a través de una puerta de enlace de Internet, ya sea mediante la consola de administración de AWS o mediante la Command Line Interface de AWS, que utiliza claves SSH. **Fin de la descripción de accesibilidad.**

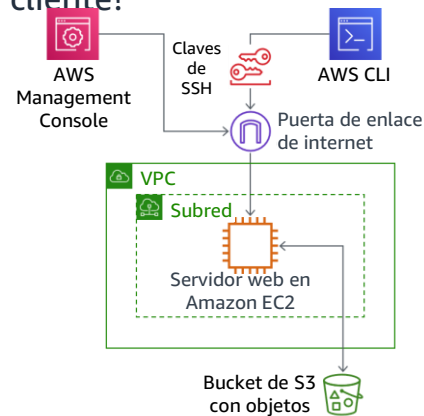
Ahora, considere este caso adicional en el que un cliente utiliza los servicios y recursos de AWS que se muestran aquí.

Un cliente utiliza Amazon S3 para almacenar datos. El cliente configuró una nube virtual privada (VPC) con Amazon VPC y está ejecutando un servidor web en una instancia de EC2 en la VPC. El cliente configuró una puerta de enlace de Internet como parte de la VPC para que se pueda acceder al servidor web mediante la consola de administración de AWS o Command Line Interface de AWS (AWS CLI). Cuando el cliente utiliza la AWS CLI, la conexión requiere el uso de claves de Secure Shell (SSH).

¿Quién es responsable de mantener la seguridad de cada componente? ¿AWS o el cliente?

## Actividad: Respuestas de Escenario 2 de 2

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



1. ¿Se asegura de que la Consola de administración de AWS no sea pirateada?

**Respuesta: AWS**

2. ¿Configurando la subred?

**Respuesta: El cliente**

3. ¿Configurando la VPC?

**Respuesta: El cliente**

4. ¿Protección contra las interrupciones de la red en las regiones de AWS?

**Respuesta: AWS**

5. ¿Proteger las claves SSH?

**Respuesta: El cliente**

6. ¿Garantizar el aislamiento de la red entre los datos de los clientes de AWS?

**Respuesta: AWS**

7. ¿Garantizar una conexión de red de baja latencia entre el servidor web y el bucket de S3?

**Respuesta: AWS**

8. ¿Hacer cumplir la autenticación multifactor para todos los inicios de sesión de los usuarios?

**Respuesta: El cliente**



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

34

**Para la accesibilidad:** diagrama arquitectónico en el que se muestra un servidor web que se ejecuta en EC2 dentro de una subred y VPC. El servidor web se conecta a un bucket de S3. Se puede acceder al servidor web a través de una puerta de enlace de Internet, ya sea mediante la consola de administración de AWS o mediante la Command Line Interface de AWS, que utiliza claves SSH. **Fin de la descripción de accesibilidad.**

En el modelo de responsabilidad compartida, el cliente es responsable de lo que implementa al usar AWS y de las aplicaciones que están conectadas a la nube de AWS. En este ejemplo, el cliente es responsable de configurar la VPC y la subred, proteger las claves SSH y aplicar la autenticación multifactor para todos los inicios de sesión de los usuarios.

Recuerde que los clientes son responsables de la seguridad del contenido que colocan en la nube de AWS o que conectan a su infraestructura de AWS. Esto incluye contenido almacenado y procesado en almacenamiento, bases de datos u otros servicios de AWS. Como cliente de AWS, usted controla todo el ciclo de vida de su contenido en AWS y puede administrar su contenido de acuerdo con sus necesidades específicas, incluida la clasificación de contenido, el control de acceso, la retención y la eliminación.

Como se describe en el modelo de responsabilidad compartida, AWS es responsable de proteger la infraestructura global que ejecuta toda la nube de AWS. Esto incluye la infraestructura física que aloja sus recursos. En este ejemplo, AWS es responsable de lo siguiente:

- Asegurarse de que la consola no esté pirateada
- Proteger la infraestructura contra interrupciones de la red en las regiones de AWS
- Garantizar el aislamiento de la red entre los datos de los clientes de AWS
- Garantizar una conexión de red de baja latencia entre el servidor web y el bucket de S3

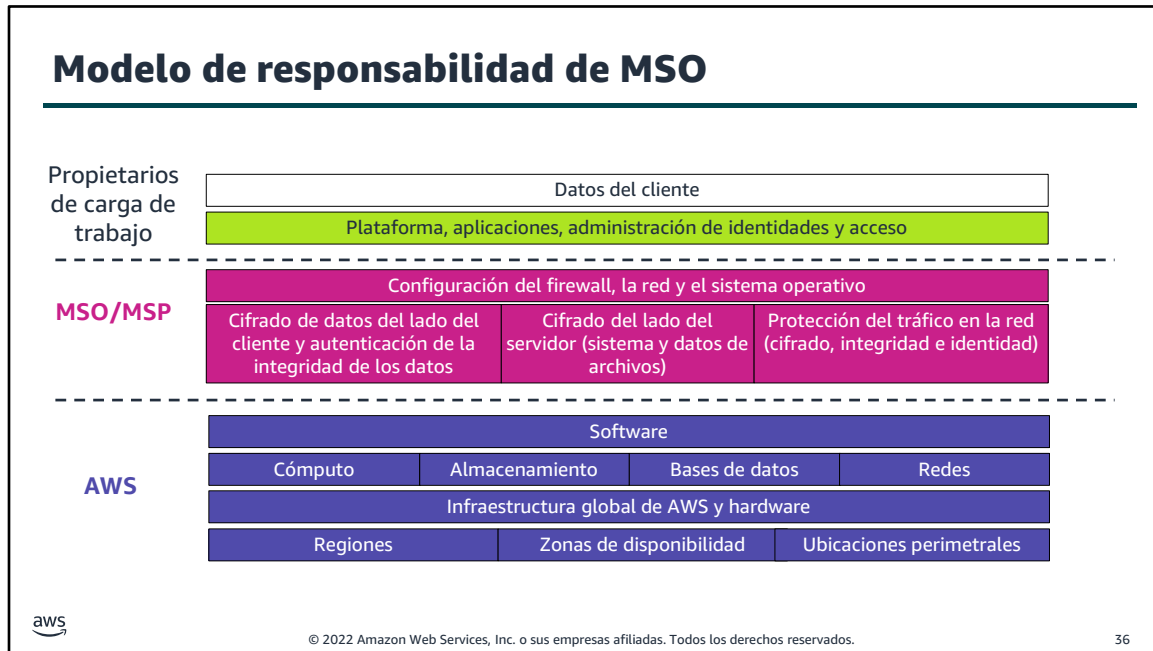


Un enfoque para implementar la seguridad y la gobernanza es crear un equipo centralizado que sea responsable de establecer procesos y plantillas repetibles para implementar aplicaciones en AWS mientras se mantiene el control organizacional sobre las implementaciones. Tal equipo puede ser interno o externo (proveedores externos) y, a menudo, se lo denomina equipo de aprovisionamiento, centro de excelencia u organización de servicios gestionados (MSO). Los proveedores externos se conocen comúnmente como proveedores de servicios administrados (MSP). AWS valida a los socios de AWS en el marco del programa Proveedor de servicios administrados (MSP) de AWS.

Los MSO o MSP suelen ser responsables de las cuentas de aprovisionamiento; establecer procesos repetibles para el despliegue; auditar las implementaciones de los propietarios de la carga de trabajo; y alojamiento de servicios compartidos para seguridad, supervisión continua, conectividad y autenticación. En un sentido básico, los MSO crean las protecciones para la seguridad, la protección de los datos y la recuperación ante desastres en la empresa.

Para más información, consulte el programa Proveedor de servicios administrados (MSP) de AWS en <https://aws.amazon.com/partners/programs/msp>.





En el modelo MSO, los propietarios de la carga de trabajo manejan la implementación, el desarrollo y el mantenimiento reales de las aplicaciones. Los propietarios de cargas de trabajo suelen incluir administradores de sistemas, desarrolladores y otras personas que son directamente responsables de una o más aplicaciones. La incorporación de un MSO permite garantizar que las aplicaciones se implementen de forma segura y conforme a la normativa mediante la aplicación automatizada de los requisitos de seguridad de la organización. Tener un MSO también significa que el propietario de la carga de trabajo puede reducir su documentación de autorización solo a la configuración e instalación del software que es específico para una aplicación en particular. Esto se debe a que el propietario de la carga de trabajo hereda una parte significativa de la implementación del control de seguridad del MSO.

Los MSO clientes de AWS suelen ocuparse de las siguientes actividades:

**Aprovisionamiento de cuentas:** tras revisar el caso práctico del propietario de la carga de trabajo, el MSO establece la cuenta inicial, la conecta con la cuenta correspondiente para la facturación unificada y configura la funcionalidad de seguridad básica antes de otorgarle acceso al propietario de la carga de trabajo.

**Supervisión de la seguridad:** con el aprovisionamiento de cuentas centralizado, el MSO puede implementar funciones que permiten al personal de seguridad supervisar la aplicación a medida que se implementa y administra. El MSO puede realizar actividades como establecer un grupo de auditores con acceso entre cuentas y vincular la VPC de la aplicación a una VPC de servicios compartidos que controla el MSO.

**Configuración de Amazon VPC:** una configuración de Amazon VPC incluye la VPC y sus subredes, configuraciones de grupos de seguridad y listas de control de acceso a la red (ACL). Para ejercer un control más estricto sobre las VPC de la aplicación, el MSO también puede conservar el control sobre la configuración de la VPC y exigir que el propietario de la carga de trabajo solicite los cambios deseados para la seguridad de la red.

**Configuración de IAM:** el MSO puede crear grupos de usuarios y asignar permisos. Esto puede incluir la creación de grupos para auditores internos, un superusuario de IAM y grupos administrativos de aplicaciones que están

segregados por funcionalidad (por ejemplo, administradores de bases de datos y Unix).

**Desarrollo y aprobación de plantillas:** el MSO puede crear plantillas de CloudFormation preaprobadas para casos de uso comunes. Mediante el uso de plantillas, los propietarios de la carga de trabajo heredan la implementación de seguridad de la plantilla aprobada, lo que limita su documentación de autorización a las características que son exclusivas de su aplicación. Pueden reutilizarse las plantillas para acortar el tiempo necesario para aprobar e implementar nuevas aplicaciones.

**Creación y gestión de AMI:** el MSO puede crear una biblioteca de AMI comunes y aprobadas para la organización, lo que proporciona una gestión y actualización centralizadas de las imágenes de las máquinas. Al crear plantillas frecuentes, los MSO pueden exigir el uso de AMI aprobadas.

**Desarrollo de una VPC de servicios compartidos:** con una VPC de servicios compartidos, el MSO puede recibir fuentes de supervisión casi continuas de la VPC de la aplicación de la organización y los servicios compartidos comunes que se requieren para su organización. Esto suele incluir una plataforma de administración de acceso compartido, puntos de enlace de registros y acumulación de información sobre la configuración.

## **Aprendizajes clave: modelo de responsabilidad compartida**



- El modelo de responsabilidad compartida de AWS ayuda a las organizaciones que adoptan la nube a lograr sus objetivos de seguridad y cumplimiento.
- Los clientes son responsables de proteger todo lo que colocan en la nube.
- Un MSO esencialmente crea las barandillas para la seguridad, la protección de datos y la recuperación ante desastres.

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

37

Estos son algunos aprendizajes clave de esta sección del módulo:

- El modelo de responsabilidad compartida de AWS ayuda a las organizaciones que adoptan la nube a lograr sus objetivos de seguridad y cumplimiento.
- Los clientes son responsables de proteger todo lo que colocan EN la nube.
- Un MSO esencialmente crea las barandillas para la seguridad, la protección de datos y la recuperación ante desastres.



Ahora es el momento de revisar el módulo y concluir con una evaluación de conocimientos y una discusión sobre una pregunta del examen de certificación de práctica.

## Resumen del módulo

---

En este módulo, aprendió a hacer lo siguiente:

- Identificar las funciones y beneficios del cómputo en la nube.
- Identificar los principios de seguridad sobre los que está creada la nube de AWS.
- Identificar de qué parte de una aplicación es responsable el usuario para asegurar la nube.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

39

En este módulo, aprendió a hacer lo siguiente:

- Identificar las funciones y beneficios del cómputo en la nube
- Identificar los principios de seguridad sobre los que está creada la nube de AWS.
- Identificar de qué parte de una aplicación es responsable el usuario para asegurar la nube.

## Completar la evaluación de conocimientos

---



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

40

Ahora es el momento de completar la evaluación de conocimientos para este módulo.

## Pregunta de examen de ejemplo



Según el modelo de responsabilidad compartida, ¿quién es responsable de configurar reglas de grupo de seguridad para determinar qué puertos están abiertos para una instancia de EC2 para Linux?

Opción	Respuesta
<b>A</b>	AWS es responsable de configurar las reglas del grupo de seguridad.
<b>B</b>	El cliente es responsable de configurar las reglas del grupo de seguridad.
<b>C</b>	Las reglas del grupo de seguridad no son necesarias.
<b>D</b>	AWS es responsable de configurar las reglas del grupo de seguridad y el cliente debe abrir los puertos a la instancia.

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

41

Mire las opciones de respuesta y descártelas según las palabras clave.

## Respuesta a la pregunta de examen de ejemplo

Copie y pegue la misma pregunta aquí.

La respuesta correcta es la B.

Las palabras clave de la pregunta son **configurar las reglas del grupo de seguridad**.

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

42

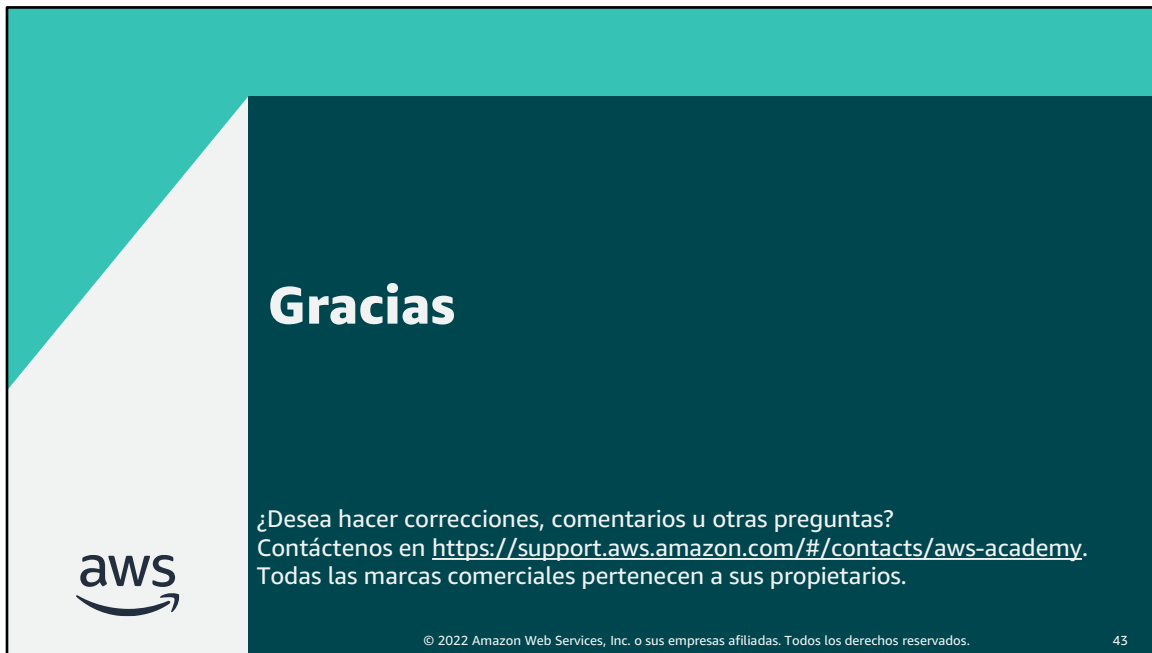
Las siguientes son las palabras clave que se deben reconocer: **configurar las reglas del grupo de seguridad**.

**La respuesta correcta es la B.** El cliente es responsable de controlar el acceso a la red a las instancias de EC2.

Respuestas incorrectas:

- Respuesta A: AWS mantiene la configuración de sus dispositivos de infraestructura, pero el cliente es responsable de configurar sus propios sistemas operativos invitados (incluida la protección del tráfico de red), las bases de datos y las aplicaciones.
- Respuesta C: Las reglas del grupo de seguridad filtran el tráfico según los protocolos y los números de puerto, y el cliente es responsable de configurar la protección del tráfico de red.
- Respuesta D: AWS mantiene la configuración de sus dispositivos de infraestructura, pero el cliente es responsable de configurar sus propios sistemas operativos invitados (incluida la protección del tráfico de red), las bases de datos y las aplicaciones.





Gracias por completar este módulo.