Lección 1

Introducción a la seguridad en la nube

Analicemos cómo los conceptos de esta unidad se aplican al escenario empresarial bancario.

Fundamentos de la seguridad en la nube

Modelo de responsabilidad compartida AWS

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.

Prueba de nivel de comodidad

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.

Modelo de responsabilidad compartida

Seguridad en la nube de AWS

Introducción a la seguridad en 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.

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.

Benefíciese 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 cuanta 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.

La seguridad es familiar

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.

- Limitar el acceso y la divulgación a usuarios autorizados.
- Evitar el acceso a personas no autorizadas.

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.

- Mantener la uniformidad de los datos a lo largo del ciclo de vida.
- Conservar los datos en reposo y los datos en tránsito.

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.

- Tener acceso a los recursos de información cuando sea necesario.

Seguridad en la nube de AWS: OBJETIVOS

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

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 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 sólo 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?

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.

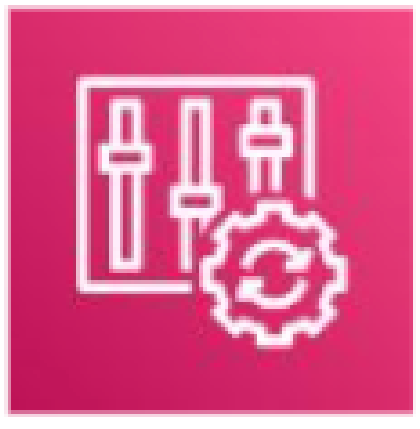
Los servicios de AWS, como AWS CloudTrail, pueden ayudarlo a responder preguntas como, por ejemplo, ¿qué acciones realizó un usuario específico durante un periodo de tiempo determinado? Para un recurso específico, ¿qué usuario ha realizado acciones en él durante un periodo de tiempo determinado? ¿Cuál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

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.



AWS Config

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: 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?

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.

AWS CloudFormation

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.

Estos son algunos aprendizajes clave de esta sección:

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, agilidad y automatización.