PRIVACY PROTECTION IN CLOUD PLATAFORMS

Jaider Daniel Gonzalez Ariza – 2205563

Ricardo Svensson Jaimes Estupiñan – 22020007

UNIVERSIDAD INDUSTRIAL DE SANTANDER

Diciembre 1, 2023

INTRODUCCIÓN

El Cloud computing es un modelo de entrega de servicios de almacenamiento, servidores, redes, etc.., a gran escala, donde las empresas que lo contratan pueden acceder a estos servicios sin infraestructura local. En los últimos años ha tenido una adopción masiva y aunque cuente con muchos sectores y tecnologías que serían interesantes revisar, se buscó estudiar el más importante, la seguridad. Los métodos de seguridad en la nube juegan un papel crucial para salvaguardar la integridad, confidencialidad y disponibilidad de la información.

El tema de la seguridad de la información es algo crucial en las empresas, tan solo en el año 2020 las vulnerabilidades reportadas superan en cantidad a las reportadas 10 años atrás. En el pasado las únicas compañías que podían contar con seguridad eran las compañías grandes, sin embargo, esto con el tiempo ha cambiado y tecnologías como el Cloud computing permiten que incluso compañías que estén empezando cuenten con varios servicios con una gran seguridad y una capacidad de sostener procesos bastante alta.

En este informe nos centraremos en las tecnologías de seguridad empleadas por AWS (Amazon Web Services) ya que es una de las nubes más usadas en la actualidad y con mayores avances tecnológicos, analizaremos viabilidad y ventajas frente a otros métodos y compañías que protegen la información en el uso de datos.

OBJETIVO GENERAL

Analizar los componentes de seguridad implementados en el AWS y estudiar su viabilidad en entornos corporativos.

OBJETIVOS ESPECÍFICOS

- Entender cómo operan los servidores de la nube.
- Exponer las tecnologías en privacidad y seguridad usadas por la nube de Amazon (AWS).
- Hallar las ventajas y desventajas respecto a seguridad en el AWS frente a otras empresas y servidores físicos.
- Concluir la viabilidad de AWS y su sector objetivo.

METODOLOGÍA

1. Se buscó un tema relevante en el sector tecnológico, para el cual se escogió “Privacy protection in Cloud plataforms”.
2. Se expusieron las tecnologías usadas en seguridad de AWS.

3. Se comparó las tecnologías del numeral anterior con la seguridad de servidores físicos de pequeñas y grandes empresas.
4. Se comparó las tecnologías del numeral (2) con otras empresas con servicio de nube del sector, como Microsoft Azure y GSP (Google).
5. Se analizaron casos externos de problemas en la nube de compañías en el pasado y su impacto en la industria.
6. Se concluyó la viabilidad del servicio de AWS respecto a la seguridad.

CONTENIDO

1. Seguridad en AWS

La seguridad en AWS es un factor clave para su éxito, esta plataforma de servicios se esfuerza por proporcionar un entorno seguro y confiable para los datos, aplicaciones y recursos que los usuarios despliegan en la nube.

Opera en centro de datos altamente seguros, con medidas físicas robustas y confiables como lo son cámaras de seguridad en la planta física, control de acceso, y procesos básicos para el mantenimiento de los equipos, pero, aquí no nos centraremos en la parte física, vamos a desglosar con detenimiento todas las tecnologías de las cuales podemos hacer uso cuando adquirimos algún servicio de AWS.

1.1. AWS Identity and Access Management (IAM):

IAM (Identity and Access Management) es un servicio de AWS que te permite gestionar el acceso a los recursos y servicios de AWS de manera segura. IAM se centra en la administración de identidades, políticas y permisos dentro de tu entorno en la nube de AWS. Algunos aspectos clave de IAM incluyen:

1.1.1. Usuarios y Grupos: Puedes crear usuarios individuales y organizarlos en grupos lógicos.

1.1.2. Políticas de Acceso: Establece políticas de acceso granulares para controlar qué acciones pueden realizar los usuarios, grupos o roles en los diferentes servicios y recursos de AWS.

1.1.3. Autenticación Multifactor (MFA): IAM es compatible con la autenticación multifactor, lo que añade una capa adicional de seguridad al requerir múltiples formas de autenticación para acceder a una cuenta.

Este servicio es común en las plataformas Cloud, donde casi todas las empresas cuentan con los mismos aspectos, solo que varían algunas cosas de alcance para las personas que tienen gestión en la nube.

1.2. AWS Key Management Service (KMS):

KMS facilita la creación, gestión y protección de claves de encriptación. Permitiendo generar y controlar claves criptográficas para encriptar y desencriptar datos de forma segura.

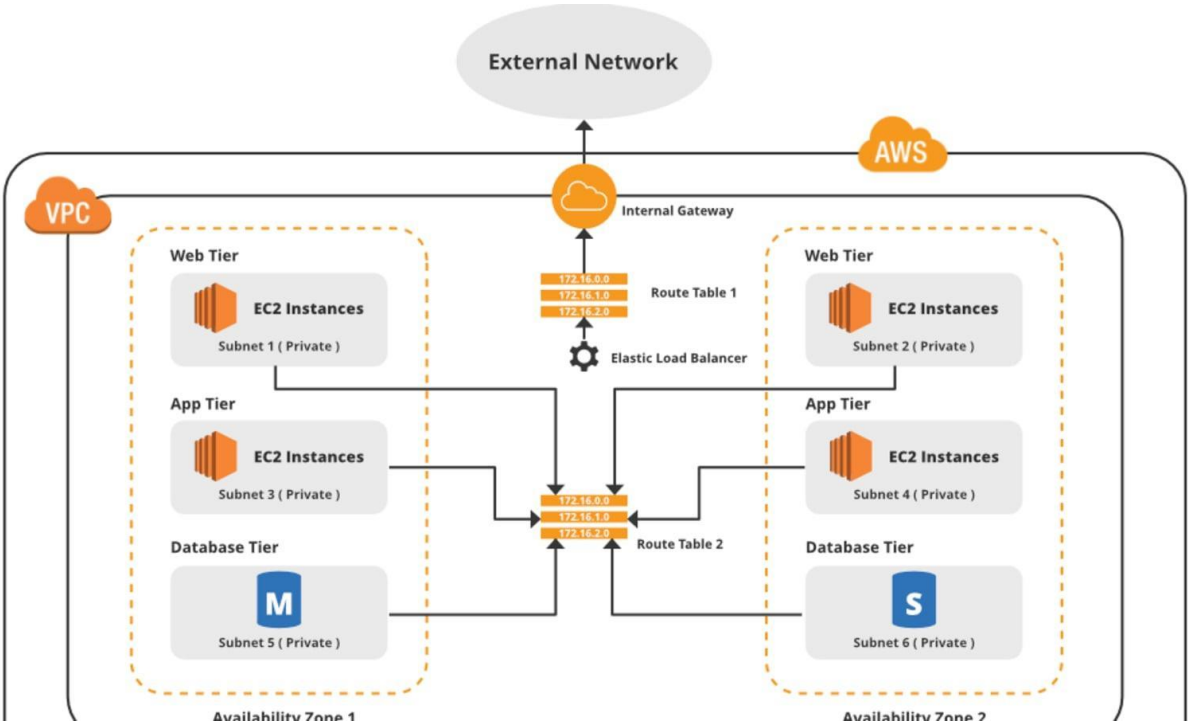
Se utiliza para proteger datos en reposo y en tránsito y permite a los usuarios crear políticas para el acceso a las claves y asegura la confidencialidad de los datos en la nube.

Microsoft y Google también cuentan con una tecnología similar en la nube, como lo es Azure Key Bault y Google Cloud KMS, respectivamente. Ofrecen una solución de gestión de claves similar, permitiendo generar, usar y controlar claves de cifrado de manera segura para proteger datos y recursos en la nube.

1.3. Amazon Virtual Private Cloud (VPC):

VPC es un servicio que te permite crear una red virtual personalizada dentro de AWS. Con VPC, puedes controlar de manera precisa la configuración de redes, subredes, tablas de enrutamiento y puertas de enlace, lo que te brinda un alto nivel de aislamiento y seguridad para tus recursos en la nube. Algunos aspectos clave de VPC incluyen:

Puedes configurar listas de control de acceso (ACL) y grupos de seguridad para controlar el tráfico de red y la comunicación entre los recursos dentro de la VPC.



Podemos encontrar alternativas en el sector como lo es la Virtual Network (VNet) de Microsoft Azure que es similar a VPC VNet permite crear redes aisladas y definir la topología de red, subredes, enrutamiento y configuración de seguridad en Microsoft Azure.

1.4. AWS WAF (Web Application Firewall):

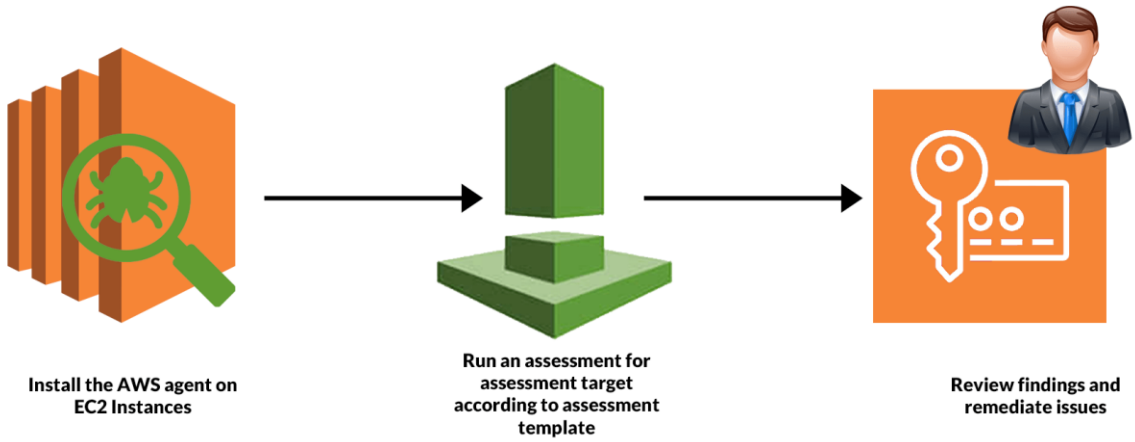
AWS WAF lo ayuda a protegerse de los exploits y bots web comunes que podrían afectar la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos.

AWS WAF le permite crear reglas de seguridad que controlan el tráfico de bots y bloquean los patrones de ataque comunes, como la inyección de código SQL o el scripting entre sitios (XSS). Además se puede superviasr la página de inicio de sesión de su aplicación para detectar el acceso no autorizado a las cuentas de usuario utilizando credenciales comprometidas.

Microsoft Azure ofrece un servicio similar al AWS WAF a través del Application Gateway WAF. Proporciona firewall de aplicaciones web con capacidades de protección contra ataques comunes a nivel de aplicación.

1.5. Amazon Inspector:

Amazon Inspector es un servicio de administración automatizada de vulnerabilidades que analiza continuamente las cargas de trabajo de AWS en busca de vulnerabilidades de software y exposición involuntaria a la red. Descubre automáticamente cargas de trabajo, como las instancias de Amazon EC2, contenedores y funciones de Lambda, y los escanea para encontrar vulnerabilidades de software y exposición involuntaria de red.



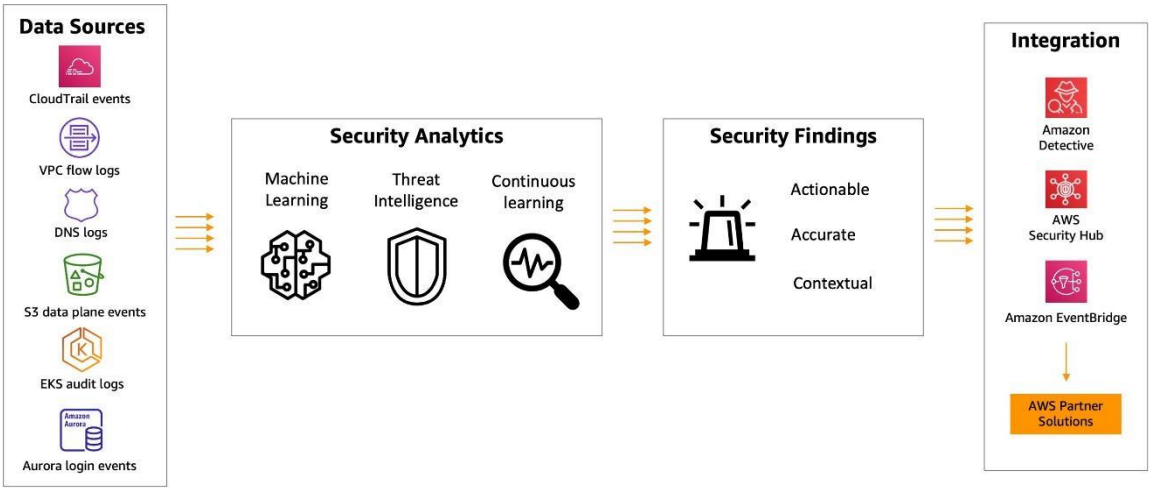
Google Cloud Security Command Center (Google Cloud Platform): Proporciona herramientas de seguridad que permiten identificar y analizar las amenazas de seguridad, realizar escaneos de vulnerabilidades y recibir recomendaciones para mejorar la seguridad de los recursos en GCP.

1.6. Amazon GuardDuty:

GuardDuty analiza los registros y la actividad de la red en busca de patrones sospechosos o comportamientos anómalos. Utiliza análisis de comportamiento y aprendizaje automático para identificar posibles amenazas, como actividades de hacking, intentos de intrusión, comportamientos de malware, etc.

Esta tecnología se integra con varios servicios de AWS, como CloudTrail, VPC Flow Logs y DNS logs, para obtener información sobre la actividad de la cuenta y la red.

Cuando se detecta una actividad sospechosa, GuardDuty genera alertas en tiempo real, lo que permite una respuesta rápida a posibles amenazas.



1.7. AWS Security Hub:

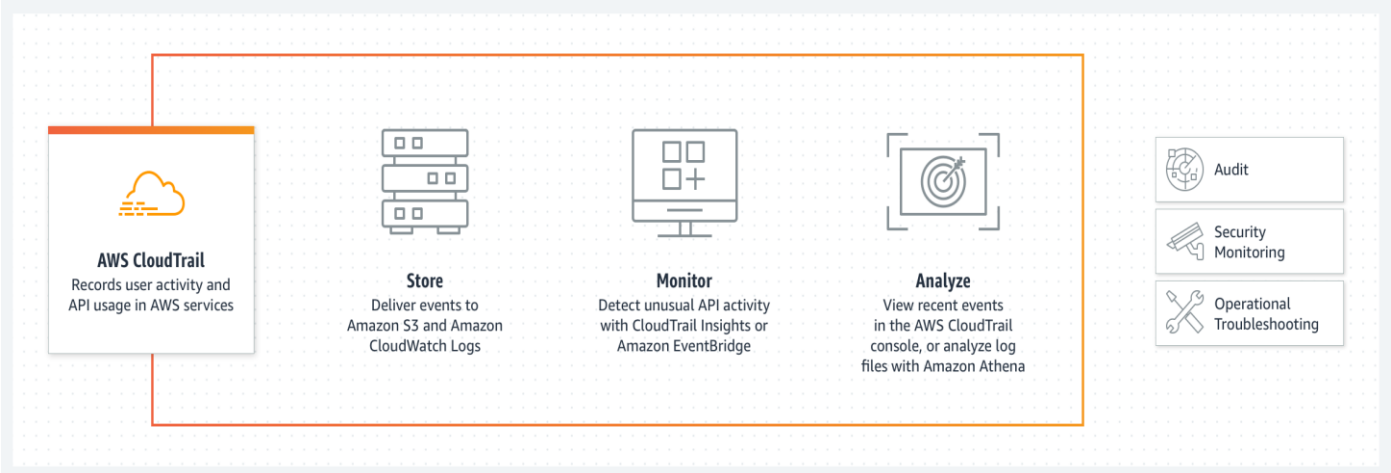
Security Hub ofrece una vista centralizada de la seguridad en AWS. Recopila y analiza datos de seguridad de múltiples servicios de AWS para identificar y priorizar amenazas, vulnerabilidades y desviaciones de las mejores prácticas de seguridad.

Proporciona información consolidada para la gestión y corrección proactiva de riesgos de seguridad.

1.8. AWS CloudTrail:

CloudTrail registra y audita actividades en la cuenta de AWS. Captura registros detallados de eventos y actividades realizadas en la cuenta de AWS, incluyendo acciones de usuarios, cambios en recursos y acceso a servicios.

Proporciona visibilidad y registros para auditorías de seguridad, cumplimiento de normativas y detección de posibles amenazas



2. Comparativa entre AWS y infraestructura física

Al considerar AWS (Amazon Web Services), una plataforma en la nube, frente a compañías que mantienen infraestructura física (on-premise), es esencial analizar diversos aspectos:

1. Costos:

AWS: Ofrece un modelo de pago por uso, lo que puede resultar más rentable para muchas empresas al eliminar la necesidad de invertir en hardware costoso y gastos continuos de mantenimiento de la infraestructura.

Infraestructura Física: Requiere una inversión inicial en servidores, equipos de red y almacenamiento, además de gastos recurrentes por mantenimiento, actualizaciones y gestión.

2. Escalabilidad y Flexibilidad:

AWS: Permite una escalabilidad instantánea, con la capacidad de ajustar recursos de manera rápida y sencilla según las necesidades. Ofrece una amplia gama de servicios adaptables.

Infraestructura Física: Requiere planificación anticipada y tiempo para expandir o reducir recursos, además de estar limitada por las restricciones de recursos físicos existentes.

3. Seguridad:

AWS: Garantiza una serie de medidas de seguridad y cumplimiento, con centros de datos altamente seguros y herramientas integradas para la seguridad.

Infraestructura Física: La seguridad depende en gran medida de las implementaciones internas y puede ser más desafiante mantener y asegurar de manera efectiva.

Si bien la infraestructura física ofrece control directo, el modelo de pago por uso de AWS provee flexibilidad y ahorro de costos significativos. La escalabilidad instantánea y las medidas de seguridad integradas de AWS representan ventajas claras sobre las limitaciones y los desafíos de seguridad asociados con la infraestructura física. En última instancia, la elección entre AWS y la infraestructura física depende de las necesidades específicas de cada empresa, considerando factores como costos, escalabilidad y seguridad.

3. Controversias del Cloud Computing

El desarrollo del cloud computing estuvo marcado por diversas polémicas que impactaron su percepción pública. Sin embargo, pese a estos desafíos, el avance tecnológico continuó redefiniendo la gestión de datos y servicios.

- Brecha de seguridad de Dropbox (2012): Esta situación se originó cuando Dropbox sufrió una brecha de seguridad, exponiendo las contraseñas y cuentas de sus usuarios. Este incidente planteó serias inquietudes sobre la seguridad de los datos almacenados en la nube, destacando la necesidad de medidas de protección más sólidas en estos entornos.
- Interrupción de Amazon Web Services (2017): Durante este evento, Amazon Web Services (AWS) experimentó una caída masiva que afectó a servicios populares como Netflix, Spotify y Reddit. Esta interrupción evidenció la fragilidad de depender exclusivamente de

un proveedor en la nube y generó debates sobre la fiabilidad y la gestión de crisis en estos entornos tecnológicos.

4. Análisis de ventajas y desventajas

Aunque Amazon sea una empresa líder en el sector tecnológico, presenta algunas desventajas al ser una empresa tan global, al igual que muchas ventajas debido a su amplio grupo de expertos que trabajan con ellos.

Ventajas

- Al ser una empresa tan grande, si adquirimos sus servicios contamos con toda su infraestructura con un gran soporte.
- AWS está en constante evolución, lanzando nuevos servicios y actualizaciones para satisfacer las necesidades cambiantes del mercado y los avances tecnológicos, por lo que siempre tendremos lo último en seguridad del sector.
- Cuenta con una amplia comunidad debido a los aportes que hace con cursos, documentación, recursos y partners, por lo que si nuevas personas quieren adentrarse al sector de seguridad, tendrán mucha información disponible.

Desventajas

- A pesar de su amplia oferta, algunas personalizaciones pueden ser complejas o limitadas en comparación con otros proveedores.
- No todos los servicios de AWS están disponibles en todas las regiones, lo que puede limitar las opciones para algunas implementaciones específicas.
- Varias configuraciones de los servicios de Amazon pueden resultar más costosos que los de su competencia, por lo que hay que evaluar la viabilidad y beneficio de su uso antes de empezar

CONCLUSIONES

AWS demostró por qué es una de las nubes más usadas por todas las ventajas que tiene, al ser una compañía líder presenta los último en tecnología, es seguro que las empresas que adquieran sus servicios van a estar en buenas manos.

AWS puede brindar a empresas pequeñas una mayor flexibilidad lo cual les permite acarrear solo con los problemas necesarios para su empresa, lo que permitiría que muchas empresas nuevas ingresen al sector, sin embargo, se tendría que estudiar más a fondo la viabilidad de esta plataforma u otras en cada caso.

Las grandes empresas pueden aprovechar la escala de AWS para obtener descuentos por volumen y, a menudo, pueden optimizar sus costos mediante acuerdos de precios personalizados.

Es crucial que las empresas permanezcan atentas a las evoluciones tecnológicas y los cambios en las políticas de seguridad en la nube, ajustándose constantemente para asegurar la salvaguarda de sus datos y para cumplir con las regulaciones en constante cambio.

BIBLIOGRAFIA

[1] “AWS | Informática En La Nube. Ventajas y Beneficios.” Amazon Web Services, Inc., 15 Nov. 2023, https://aws.amazon.com/es/what-is-cloud-computing/?nc2=h_ql_le_int_cc.

[2] ChatGPT [Información sobre la nube AWS]. Recuperado de https://chat.openai.com/?model=text-davinci-002-render-sha

[3] Antoniony, Brismark. “Amazon Web Services: Ventajas, Desventajas y Alternativas.” Ambit BST | Consultoría Regulatoria y de Calidad En Sector Salud, https://www.ambit-bst.com/blog/amazon-web-services-ventajas-desventajas. Accessed 1 Dec. 2023.

[3] River, Heubert. “Infraestructura Digital y Seguridad Física de Datos: Buenas Prácticas.” Cirion Technologies, https://www.facebook.com/LumenLATAM/, 3 Mar. 2023, https://blog.ciriontechnologies.com/es/infraestructura-digital-seguridad-fisica/.