Instituto Tecnológico y de Estudios Superiores de Monterrey

Construyendo cuerpo y mente (Gpo 120)

Actividad Integradora 1 - Reporte

Facundo Colasurdo Caldironi A01198015

Campus Monterrey **Fecha: 25/11/2024**

Para este trabajo, en lugar de una explicación detallada, se realizaron distintas tablas comparativas para comparar las características de tres proveedores de servicios de la nube: AWS (Amazon Web Services), Google Cloud y Microsoft Azure.

Característica	AWS (Amazon Web Services)	Google Cloud	Microsoft Azure
Cifrado de datos en tránsito	Usa Transport Layer Security (TLS) al montar el sistema de archivos mediante el asistente de EFS.	Usa TLS/SSL para datos entre centros de datos, el cifrado se realiza de manera automática.	Utiliza TLS para los datos en tráfico, compatible con IPsec y SSL.
Cifrado de datos en reposo	Usa AES (Advanced Encryption Standard) para encriptar los datos en reposo, dando protección avanzada.	Usa AES para encriptar los datos en reposo, lo que los muestra como una clase	Implementa AES , aplicable a servicios como Azure Blob y File Storage.
Autenticación multifactor	MFA (Autenticación Multifactor) en IAM, soporta Google Authenticator y dispositivos de hardware.	MFA con opciones de verificación en dos pasos para usuarios de GCP.	MFA con Azure Active Directory, permite autenticación biométrica y múltiples factores de autenticación.
Herramientas de gestión de claves	AWS Key Management Service (KMS) y AWS CloudHSM para almacenamiento y control de claves.	Google Cloud Key Management Service y soporte para claves propias y módulos HSM.	Azure Key Vault para la gestión de claves, certificados y secretos con HSM integrado.
Detección de amenazas	Amazon GuardDuty para detectar amenazas mediante machine learning y análisis de patrones de tráfico.	Google Cloud Security Command Center para la detección de amenazas y evaluación de seguridad.	Azure Security Center y Azure Sentinel para la detección y análisis de amenazas.

Cada uno de los proveedores utiliza distintas técnicas y herramientas para tener un manejo seguro de sus datos, esta matriz comparativa evalúa las prácticas de seguridad de datos en la nube de de cada uno de los proveedores anteriores,

clasificándolas según los principios de confidencialidad, integridad y disponibilidad y su cumplimiento con normas de seguridad y privacidad, incluyendo ISO/IEC 27001, NIST, y GDPR.

Prácticas	AWS (Amazon Web Services)	Google Cloud	Microsoft Azure
Confidencialidad	Utiliza AES para datos de reposo y TLS para aquellos en tránsito, también, usa Identity access management, (IAM) para controlar permisos.	Utiliza TLS para datos en movimiento, y AES para los de reposo, también usa IAM para restringir accesos.	Utiliza AES para datos en reposo, y TLS para los de movimiento,al mismo tiempo que usa Azure AD para control de acceso.
Integridad	Mediante AWS Key Management Service (KMS) y Amazon Guard Duty, mantiene la seguridad de datos y registros.	Ofrece Cloud KMS y Security Command Center para monitorear la integridad, así como auditorías automáticas.	Azure Key Vault y Security Center proporcionan control de claves y análisis de integridad de los datos.
Disponibilidad	Cuenta con múltiples zonas de disponibilidad y recuperación ante desastres, además de Elastic Load Balancing.	El uso de google cloud proporciona un balance de carga y recuperación ante fallos.	Azure garantiza alta disponibilidad y copias de datos en centros de datos globales.
ISO/IEC 27001	AWS está certificado en ISO/IEC 27001, cumpliendo con los requisitos de seguridad.	Google Cloud cuenta con certificación ISO/IEC 27001 para su infraestructura y servicios en la nube.	Azure cumple con ISO/IEC 27001 en todos sus centros de datos.
NIST	Cumple con el NIST SP 800-53 y NIST Cybersecurity Framework, con controles para la	Compatible con los estándares NIST y provee controles de seguridad.	Se adhiere al NIST SP 800-53, con auditorías y prácticas de protección de datos.

	gestión de riesgos y protección de datos.		
GDPR	AWS cumple con el GDPR, logrando la gestión de datos, control de acceso y privacidad en la Unión Europea.	Google Cloud cumple con el GDPR, dando herramientas para la protección de datos personales en Europa.	Microsoft Azure cumple con el GDPR, proporcionando gestión de privacidad de datos en la UE.

Basado en la matriz anterior, se seleccionaron las siguientes herramientas y prácticas como componentes clave para garantizar la protección de los datos en la nube. Estas prácticas y herramientas fueron seleccionadas por su capacidad para reforzar la confidencialidad, integridad y disponibilidad de los datos, así como para cumplir con estándares de seguridad reconocidos como ISO/IEC 27001, NIST y GDPR.

1. AWS Key Management Service (KMS)

Su principal objetivo es el controlar las claves de AWS, lo cual permite poder crear, almacenar y gestionar de manera segura claves usadas para cifrar datos en AWS

Las principales ventajas de este servicio son que incluye su integración con otros productos de AWS como S3 y RDS, la personalización de políticas de acceso y el cumplimiento con estándares de seguridad como NIST y FIPS 140-2, lo que asegura una protección sólida y adaptada a las normativas.

2. Google Cloud Identity and Access Management (IAM)

Su objetivo es la asignación de roles y permisos a usuarios y grupos, asegurando que cada entidad solo tenga acceso a los recursos necesarios en Google Cloud.

Las ventajas de este servicio incluyen la implementación de políticas de mínimo privilegio para mejorar la seguridad, su integración con herramientas de monitoreo que permiten mantener registros de accesos, y su compatibilidad con múltiples protocolos de autenticación y roles predefinidos, los cuales simplifican la gestión de permisos.

3. Microsoft Azure Key Vault

Busca almacenar y gestionar claves criptográficas, certificados y secretos de aplicaciones en un entorno seguro.

Este servicio incluye almacenamiento de módulos de seguridad de hardware (HSM) para una protección de claves altamente seguras, su integración nativa con otros servicios de Azure y herramientas de administración de identidades, así como la automatización en la renovación de certificados, permite simplificar la administración y asegura la confidencialidad de datos críticos.

4. AWS CloudTrail

Su función principal es registrar y monitorear todas las actividades en la cuenta de AWS, incluyendo accesos y modificaciones en recursos, lo cual resulta útil para auditorías y cumplimiento de normativas.

Incluye la habilidad de poder observar las actividades en la cuenta, lo que facilita la detección de intrusos, ya que monitoreo continuo de seguridad, también, cuenta con la capacidad de configurar alertas y almacenar registros, lo cual es muy útil para las auditorías, todo bajo cumplimiento con estándares internacionales como ISO 27001 y GDPR.

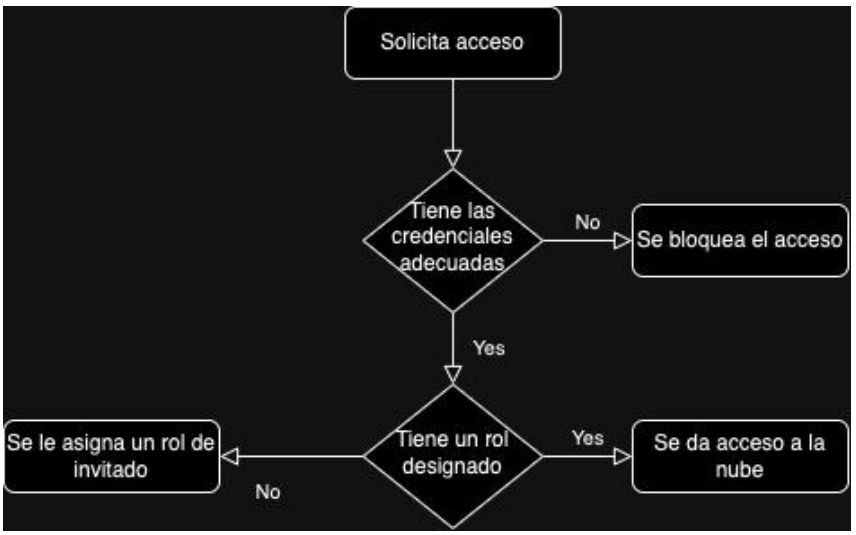
5. Google Cloud

Su principal papel es brindar una visión centralizada de la seguridad de los recursos de Google Cloud, permitiendo identificar amenazas, vulnerabilidades y configuraciones riesgosas.

Las principales ventajas de este servicio incluyen la detección temprana de amenazas y notificaciones de actividad sospechosa en tiempo real, la integración de capacidades de escaneo, lo cual ayuda a cumplir con estándares internacionales como NIST e ISO 27001..

Después de haber analizado las prácticas anteriores, se decidió definir los estándares de validación, para poder asegurarse que se estén manejando los datos adecuadamente, logrando alinearse con las mejores prácticas de desarrollo.

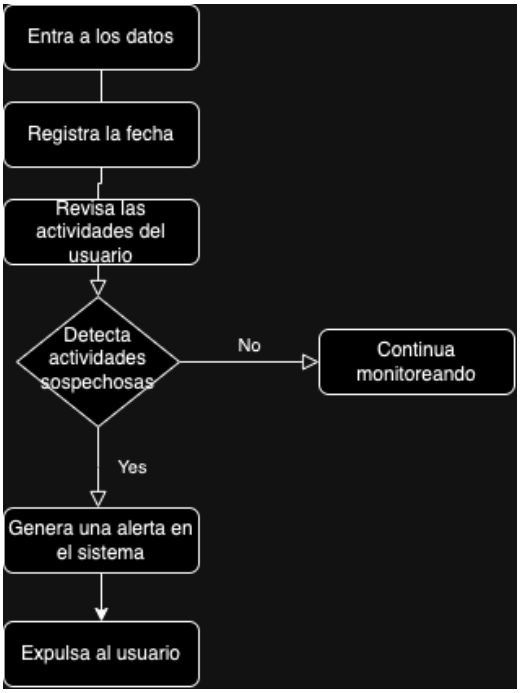
El primer estándar de validación definido fue el mismo proceso de valoración y acceso a la nube, en donde se busca asegurar que el acceso a la nube sea controlado y medido, usando revisiones y reglas para asegurarse de la privacidad y seguridad de la información.



Explicación del diagrama de flujo:

- Solicitud de acceso: El usuario solicita acceso a un recurso específico de datos en la nube.
- Tiene las credenciales adecuadas: Se evalúan los permisos basados en la necesidad, se le da lo mínimo necesario para evitar posibles peligros de fallas de información, si no tiene permiso, se es denegado.
- Tiene un rol adecuado: Dependiendo de rol, este se le designa las habilidades que tiene dentro de la nube.

El segundo estándar definido fue el monitoreo continuo de seguridad, en donde se garantiza que todos los accesos quedan registrados y sean revisados de manera continua, para poder detectar actividad sospechosa.



Explicación del diagrama de flujo:

- Detectar actividades sospechosas: Si detecta que el usuario está haciendo alguna actividad sospechosa, el sistema lo detecta y lo expulsa del mismo, por otra parte, si el usuario no genera actividades sospechosas, el sistema le permite seguir dentro.

Una vez explicados los estándares de validación, también es necesario dejar en claro las políticas de acceso, verificando que se encontraban actualizadas para el proyecto.

Primeramente fue necesario entender que la revisión y el cuidado de las políticas de acceso son un elemento fundamental para asegurarse que las políticas de seguridad sean respetadas, al mismo tiempo, que no solo asegura la seguridad de los datos, sino también de los colaboradores.

Esto fue debido a que permite mantener un control adecuado de los sistemas, donde no solo se aseguran los mismos, sino que al mismo tiempo que se implementa el cifrado de tránsito y en reposo, se puede tener la exactitud que toda la información esté segura, a su vez, la gestión de las contraseñas y certificados, ya que estos son importantes para proteger las comunicaciones entre los datos.

Conclusiones

En conclusión, gracias al documento anterior fue posible ver como cada proveedor utiliza diferentes estrategias y herramientas para poder asegurar que la confidencialidad e integrada de los datos sea asegurada, todo lo anterior debido a que estas prácticas se crearon con el objetivo de cumplira con las normativas internacionales de seguridad tales como ISO/IEC 27001, NIST y GDPR, lo que se asegura que los datos se encuentren asegurados, por otra parte, la evaluación de sus servicios clave, como AWS Key Management Service (KMS), Google Cloud IAM y Microsoft Azure Key Vault, nos ayudan a entender como estos logran gestionar de manera segura la información sensible.

Además, las herramientas de monitoreo usadas por estas compañías ofrecen vitales ventajas para poder prevenir y detectar actividades sospechosas en tiempo real, lo cual no solo ayuda a prevenir ingresos no deseados, sino que también ayudan a identificar cuando estos ocurren de manera precisa, la integración de estas soluciones con otros servicios nativos de cada proveedor simplifica en gran manera la administración y mejora la respuesta ante incidentes, al mismo tiempo, la implementación de estándares de validación, como el control del acceso y el monitoreo continuo de la seguridad, refuerza la protección de los datos en la nube, lo cual sirve para asegurarse que solo usuarios autorizados accedan, mientras se supervisan las actividades para detectar y prevenir posibles amenazas.

En resumen , las prácticas seleccionadas y los estándares definidos no solamente cumplen con las normativas internacionales de seguridad, sino que también ayudan a controlar los datos en la nube, lo cual es vital para las organizaciones no solamente para asegurarse de la seguridad de los mismos, sino también para hacerlos dinámicos.

Referencia bibliográfica:

Amazon. (2020). Cifrado de datos en tránsito. Recuperado de https://docs.aws.amazon.com/es_es/efs/latest/ug/encryption-in-transit.html

Amazon (2024) AWS Key Management Service. Recuperado de https://aws.amazon.com/es/kms/

Google. (2022). Encriptación en tránsito. Recuperado de https://cloud.google.com/docs/security/encryption-in-transit?hl=es-419

Microsoft. (2024). Microsoft Azure Portal. Recuperado de https://azure.microsoft.com/es-es/get-started/azure-portal/

ISO. (2023) SO/IEC 27001:2022. Recuperado de https://www.iso.org/es/contents/data/standard/08/28/82875.html