Campus Monterrey

Materia

Inteligencia artificial avanzada para la ciencia de datos II

Módulo

Cloud Computing

Tarea

Evidencia Portafolio - Módulo Cloud Computing

Estudiante

Juan Pablo Bernal Lafarga - A01742342

Profesor

Félix Ricardo Botello Urrutia

26 de noviembre del 2024

1.- Evaluación de Prácticas de Almacenamiento y Procesamiento en la Nube

- Investiga y compara proveedores de servicios en la nube conocidos (ej., AWS, Google Cloud, Azure) e identifica:
    - Características de seguridad como cifrado de datos en tránsito y en reposo.
    - Prácticas de confidencialidad, como políticas de acceso basadas en permisos, auditorías de acceso y autenticación multifactor.

- **Amazon Web Services**

AWS es la nube más adoptada y completa en el mundo, que ofrece más de 200 servicios integrales de centros de datos a nivel global. AWS cuenta con una cantidad de servicios y de características incluidas en ellos que supera la de cualquier otro proveedor de la nube, ofreciendo desde tecnologías de infraestructura como cómputo, almacenamiento y bases de datos hasta tecnologías emergentes como aprendizaje automático e inteligencia artificial, lagos de datos y análisis e internet de las cosas. Esto hace que llevar las aplicaciones existentes a la nube sea más rápido, fácil y rentable y permite crear casi cualquier cosa que se pueda imaginar.

AWS cifra datos en tránsito y en reposo de manera predeterminada utilizando protocolos TLS y su servicio AWS Key Management Service (KMS). Ofrece opciones avanzadas de control de claves entre otras opciones de seguridad que cubren desde el manejo de accesos, hasta la detección y respuesta de amenazas, y protección de redes y aplicaciones.

AWS IAM Proporciona control granular basado en roles con políticas detalladas en JSON. Apoya la segmentación de permisos a nivel de recursos. También registra actividades relacionadas con usuarios, recursos, y configuraciones, facilitando auditorías y cumplimiento normativo. Además, soporta autenticación multifactor (MFA), esencial para prevenir accesos no autorizados.

- **Google Cloud**

Google Cloud consiste en un conjunto de recursos físicos, como computadoras y unidades de disco duro, y recursos virtuales, como máquinas virtuales (VMs), que se encuentran en los centros de datos en todo el mundo.

Cuando hablamos de Google Cloud Platform (GCP), estamos ante todas las herramientas de Google disponibles en la nube que hasta ahora se ofrecían por separado. Este

conjunto de servicios ofrecen prestaciones muy dispares; desde machine learning hasta Inteligencia artificial pasando por el big data, todo englobado bajo el paraguas del cloud computing.

En cuanto a características de seguridad de Google Cloud, este implementa cifrado en tránsito y en reposo. Su red global segura mejora la protección, y su Key Management Service facilita el control de claves.

Google Cloud IAM ofrece roles predefinidos y personalizados, aunque con ciertas limitaciones en comparación con AWS. Y, al igual que AWS, Google Cloud registra actividades relacionadas con usuarios, recursos, y configuraciones, facilitando auditorías y cumplimiento normativo. Además, de contar con recursos de acceso como la autenticación multifactor.

- **Microsoft Azure**

La plataforma Azure está compuesta por más de 200 productos y servicios en la nube diseñados para ayudar a dar vida a nuevas soluciones que permitan resolver las dificultades actuales y crear el futuro. Crear, ejecutar y administrar aplicaciones en varias nubes, en el entorno local y en el perímetro, con las herramientas y los marcos que prefiera.

Microsoft Azure ofrece seguridad robusta con cifrado automático de datos en reposo (AES-256) y en tránsito (TLS/SSL), gestión de claves y secretos mediante Azure Key Vault con soporte para recuperación y BYOK. Integra Azure Active Directory con control de acceso basado en roles, autenticación multifactor y Privileged Identity Management para accesos privilegiados temporales. Protege redes con herramientas como DDoS Protection, firewalls y Network Security Groups. El Azure Security Center monitorea seguridad y asegura cumplimiento con estándares como GDPR e ISO 27001. Además, incluye computación confidencial para procesar datos sensibles en entornos protegidos y Microsoft Defender para detección avanzada de amenazas.

- Realiza una matriz comparativa donde clasifiques las prácticas de cada proveedor en relación con los principios éticos (confidencialidad, integridad y disponibilidad) y las normas como ISO/IEC 27001, NIST y GDPR.

Proveedor	Confidencialidad	Integridad	Disponibilidad	Norma cumplida
AWS	- Cifrado AES-256 en reposo y TLS en tránsito. - IAM con roles y políticas granulares. - MFA opcional.	- AWS CloudTrail para auditorías. - AWS Config asegura integridad de configuraciones .	- AWS Shield protege contra DDoS. - Alta disponibilidad en sus servicios (zonas de disponibilidad).	- Certificación ISO/IEC 27001. - Alineación con NIST 800-53. - Cumple con GDPR.
Google Cloud	- Cifrado predeterminado en reposo y tránsito. - IAM con autenticación granular y opciones de MFA.	- Cloud Audit Logs asegura transparencia en accesos. - Integrity Monitoring para configuraciones .	- Cloud Armor para DDoS. - Alta disponibilidad en su red global. - Redundancia en datos críticos.	- Certificación ISO/IEC 27001. - Cumple con NIST y GDPR. - Cumplimiento de HIPAA.
Azure	- Cifrado AES-256 en reposo y TLS/SSL en tránsito. - Key Vault para gestión de claves y secretos. - MFA.	- Azure Policy para asegurar configuraciones correctas. - Logs en Azure Security Center.	- Azure DDoS Protection y SLAs altos para servicios. - Respaldo geográfico en servicios clave.	- Certificación ISO/IEC 27001. - Cumple con NIST y GDPR. - Cumplimiento de HIPAA.

2.- Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

- Basado en la matriz comparativa, selecciona las mejores prácticas y herramientas de seguridad para proteger los datos en la nube. Considera prácticas como(pero no limitado a):

    - Cifrado avanzado de datos sensibles.
    - Control de accesos basados en permisos y principios de mínimo privilegio.
    - Registros de auditoría para monitorear y revisar accesos a los datos.

Para prácticas de cifrado de datos sensibles se podrían implementar herramientas como **AWS Key Management Service (KMS)**, **Azure Key Vault**, o **Google Cloud KMS** para la gestión segura de claves de cifrado. Estas herramientas permiten opciones avanzadas como BYOK (Bring Your Own Key) para mantener el control sobre las claves. Asimismo, se puede configurar certificados SSL/TLS usando servicios como **AWS Certificate Manager**, **Azure Application Gateway**, o **Google Certificate Authority Service**.

En cuanto al control de accesos y permisos se pueden implementar políticas basadas en **principios de privilegio mínimo** usando **IAM (Identity and Access Management)** de AWS, **Azure Active Directory (AAD)**, o **Google Cloud IAM**. De tal manera que se configuran **roles personalizados y predefinidos** para limitar el acceso solo a los recursos necesarios.

Para registros, se puede contar con **Google Cloud Audit Logs** que ofrece un registro completo de cambios, accesos y acciones en la infraestructura. Además, se pueden conectar los registros de auditoría con soluciones de SIEM (Security Information and Event Management) como Splunk para análisis más profundos.

Adicionalmente, se pueden usar servicios como **AWS Shield** para mitigar ataques DDoS y proteger datos accesibles públicamente, **Google Config Validator** para asegurar que los recursos cumplan con las políticas de seguridad establecidas o implementar entornos de ejecución confiables (TEE) como **Azure Confidential Computing** para proteger datos durante el procesamiento.

- (Seleccionar 5 herramientas/componentes de los proveedores de nube y realizar una breve explicación de sus ventajas/funcionamiento)

- **AWS Key Management Service (KMS)**

Facilita la creación, gestión y control de claves de cifrado utilizadas para proteger datos en reposo y en tránsito. Alguna de las ventajas que supone:

- Administre sus claves y defina políticas de manera centralizada en servicios y aplicaciones integradas desde un único punto.
- Cifre datos de sus aplicaciones con la biblioteca de cifrado de datos SDK de cifrado de AWS.
- Realice operaciones de firma con pares de claves asimétricas para validar firmas digitales.
- Genere de forma segura códigos de autenticación de mensajes basados en hash (HMAC) para garantizar la integridad y autenticidad de los mensajes.
- Es compatible con múltiples servicios de AWS (como S3, EBS, RDS), permite BYOK para mantener control sobre claves sensibles y se puede integrar con AWS CloudTrail para auditar el uso de claves.

- **Microsoft Entra ID (anteriormente Azure Active Directory)**

Es una solución integrada de identidad y acceso de la nube y un líder del mercado para administrar directorios, habilitar acceso a aplicaciones y proteger identidades. Entre sus ventajas se encuentra:

- Gestión de identidad y acceso que proporciona autenticación, control de acceso basado en roles (RBAC) y Single Sign-On (SSO).
- Compatible con MFA para mejorar la seguridad.
- Funcionalidades avanzadas como Privileged Identity Management (PIM) para gestionar accesos sensibles de manera temporal.
- Soporte para identidades híbridas (nube y on-premises).

- **AWS Shield**

Solución de protección contra ataques de denegación de servicio distribuido (DDoS) para aplicaciones web y servicios de AWS. Entre sus principales ventajas encontramos:

- Detección y mitigación automática de sofisticados eventos de denegación de servicio distribuidos a nivel de red (DDoS).
- Personalización de la protección de las aplicaciones contra los riesgos de DDoS mediante integraciones con el protocolo del equipo de respuesta Shield (SRT) o AWS WAF.
- Obtención de visibilidad, información y ahorro de costos para los eventos DDoS que afectan a los recursos de AWS.

- **Google Cloud Audit Logs**

Proporciona un registro completo de actividades en la infraestructura, incluyendo accesos a recursos, cambios en configuraciones y uso de API. Sus principales ventajas son:

- Transparencia total en accesos y actividades, pues registra auditoría de actividad del administrador, de acceso a los datos, de eventos del sistema y de política denegada.
- Compatible con GDPR y otros estándares de auditoría.
- Fácil integración con soluciones SIEM como Splunk para análisis detallados.

- Azure Confidential Computing

Permite procesar datos sensibles en entornos de ejecución confiables (Trusted Execution Environments, TEE) utilizando hardware especializado que protege los datos incluso durante el procesamiento. Y entre sus mayores ventajas y funciones tiene:

- Asegura que los datos permanezcan cifrados mientras están en reposo, en tránsito y durante su procesamiento en memoria.
- Está basado en tecnologías como enclaves Intel SGX o AMD SEV-SNP para garantizar la confidencialidad de los datos frente a usuarios no autorizados, incluso administradores de sistemas.
- Es compatible con servicios de Azure como Azure Kubernetes Service (AKS) para implementaciones modernas y escalables.

3.- Establecimiento de un Proceso o Estándar de Validación

- Define un proceso de validación que asegure el manejo ético y seguro de los datos mediante la evaluación de los siguientes puntos:
    - Evaluación periódica de permisos y accesos.

1. Revisión mensual:
    a. Identificar y eliminar accesos innecesarios o inactivos.
    b. Verificar la alineación de los roles y permisos con las responsabilidades actuales de los usuarios.
2. Herramientas automatizadas:
    a. Implementar herramientas como **Azure Active Directory Privileged Identity Management** para reportes y ajustes automáticos de accesos.
3. Registros de validación:
    a. Mantener un historial de cambios en permisos para auditorías futuras.
    - Monitoreo continuo de la seguridad con auditorías y reportes de acceso.

1. Auditorías automáticas:

    a. Utilizar **Google Cloud Audit Logs** para recopilar registros de acceso y actividad.
    b. Configurar alertas para detectar intentos de acceso no autorizados o anomalías.
2. Análisis periódico:
    a. Revisar manualmente los reportes generados por los sistemas automatizados al menos una vez al mes.
3. Informes de cumplimiento:
    a. Preparar informes regulares para cumplir con estándares como ISO/IEC 27001, GDPR o NIST.
    - Revisión y actualización de políticas de acceso y uso de datos, garantizando que solo el equipo autorizado tenga acceso, cumpliendo con la normativa vigente.

1. Evaluación regular de políticas:
    a. Revisar las políticas internas al menos una vez al año para alinearlas con la normativa vigente y las mejores prácticas del sector.
2. Control de Accesos Basados en Roles (RBAC):
    a. Diseñar roles específicos que limiten el acceso a los datos solo al personal autorizado. Y utilizar servicios como **Google Cloud IAM** o **Azure Role-Based Access Control (RBAC)** para implementar estas políticas.
3. Formación continua:
    a. Capacitar al personal en la correcta aplicación de las políticas y en el manejo ético de los datos.
4. Integración con regulaciones:
    a. Asegurar que las políticas cumplan con regulaciones como GDPR, HIPAA o CCPA según la jurisdicción aplicable.

Este proceso asegura el manejo ético y seguro de los datos mediante controles estrictos de acceso, monitoreo constante y políticas dinámicas actualizadas con las normativas vigentes. La implementación de herramientas de automatización y la capacitación constante del equipo complementan este enfoque para minimizar riesgos y garantizar cumplimiento.

4.- Conclusiones

El trabajo concluye que AWS, Google Cloud y Azure son plataformas de nube robustas con características avanzadas de seguridad, cada una destacándose en áreas específicas. AWS sobresale por la amplitud de servicios y herramientas como AWS KMS e IAM, que ofrecen control granular y opciones avanzadas de cifrado. Google Cloud destaca por su red global segura y simplicidad en el monitoreo mediante herramientas como Audit Logs. Por su parte, Azure combina seguridad avanzada con soluciones innovadoras como Azure Confidential Computing, que protege datos durante su procesamiento.

Se identificaron como mejores prácticas el cifrado avanzado de datos sensibles, controles de acceso basados en el principio de mínimo privilegio, y monitoreo continuo de accesos mediante auditorías automatizadas. Estas estrategias, apoyadas por herramientas específicas de cada proveedor, garantizan la seguridad de la información y el cumplimiento de normativas como GDPR e ISO/IEC 27001.

Finalmente, se propone un proceso de validación que incluye evaluaciones periódicas de permisos, monitoreo continuo y actualización de políticas de acceso, utilizando herramientas automatizadas. Este enfoque asegura el manejo ético y seguro de los datos, minimizando riesgos y mejorando la postura de seguridad en la nube.

Referencias

[1] *what-is-aws*. (s. f.). [Vídeo]. Amazon Web Services, Inc. https://aws.amazon.com/es/what-is-aws/?nc1=f_cc

[2] *Cloud Security, Identity, and Compliance Products – Amazon Web Services (AWS)*. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/products/security/

[3] *Qué es y para qué sirve Google Cloud Platform*. (2020, 19 agosto). Qué Es y Para Qué Sirve Google Cloud Platform. https://www.incentro.com/es-ES/blog/que-es-google-cloud-platform

[4] *Descripción general de Google Cloud*. (s. f.). Google Cloud. https://cloud.google.com/docs/overview?hl=es-419

[5] *Qué es Azure: Servicios en la nube de Microsoft | Microsoft Azure*. (s. f.). https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-azure/

[6] *Firma criptográfica de cifrado - AWS Key Management Service - AWS*. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/kms/

[7] *Microsoft Entra ID (anteriormente, Azure Active Directory) | Seguridad de Microsoft*. (s. f.). https://www.microsoft.com/es-co/security/business/identity-access/microsoft-entra-id#azure-capabilities

[8] *Protección DDoS administrada - AWS Shield - AWS*. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/shield/

[9] *Descripción general de los registros de auditoría de Cloud*. (s. f.). Google Cloud. https://cloud.google.com/logging/docs/audit?hl=es-419