Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia Artificial Avanzada para la Ciencia de Datos II

Grupo 101

18 de noviembre 2024

Evidencia Portafolio - Módulo cloud computing

Autor:

Luis Maximiliano López Ramírez - A00833321

Profesor:

Félix Ricardo Botello Urrutia

Evaluación de Prácticas de Almacenamiento y Procesamiento en la Nube

1. Características de Seguridad: Cifrado de Datos en Tránsito y en Reposo

Amazon Web Services (AWS):

- *Cifrado en Tránsito*: AWS recomienda encarecidamente cifrar los datos en tránsito entre sistemas, tanto dentro como fuera de su infraestructura. Proporciona puntos de conexión HTTPS mediante el protocolo TLS para la comunicación segura.
- *Cifrado en Reposo*: Ofrece varias opciones para el cifrado en reposo y la administración de claves de cifrado, incluyendo el uso de AWS Key Management Service (KMS) y el SDK de cifrado de AWS.

Google Cloud Platform (GCP):

- *Cifrado en Tránsito*: GCP cifra automáticamente los datos en tránsito entre sus centros de datos y ofrece opciones para cifrar datos en tránsito hacia y desde sus servicios utilizando TLS.
- *Cifrado en Reposo*: GCP cifra de forma predeterminada todos los datos almacenados en reposo y proporciona Google Cloud Key Management Service (KMS) para la gestión de claves.

Microsoft Azure:

- *Cifrado en Tránsito*: Azure utiliza protocolos para el cifrado de los datos en tránsito, como HTTPS y SMB 3.0, y ofrece opciones para cifrar datos antes de su transferencia al almacenamiento.
- *Cifrado en Reposo*: Proporciona Azure Storage Service Encryption para cifrar datos almacenados en diversos servicios de almacenamiento y facilita la gestión de claves a través de Azure Key Vault.

2. Prácticas de Confidencialidad: Políticas de Acceso, Auditorías y Autenticación Multifactor

Amazon Web Services (AWS):

- *Políticas de Acceso*: Utiliza AWS Identity and Access Management (IAM) para definir políticas basadas en identidad y recursos, permitiendo un control granular de los permisos.
- *Auditorías de Acceso*: AWS CloudTrail registra las llamadas a la API para auditorías y monitoreo de seguridad.
- *Autenticación Multifactor (MFA)*: AWS recomienda habilitar MFA para el usuario raíz y los usuarios de IAM, ofreciendo soporte para dispositivos virtuales y físicos.

Google Cloud Platform (GCP):

- *Políticas de Acceso*: GCP ofrece Identity and Access Management (IAM) para gestionar permisos detallados y control de acceso basado en roles.
- *Auditorías de Acceso*: Cloud Audit Logs proporciona registros detallados de las actividades en GCP para auditorías y cumplimiento.
- *Autenticación Multifactor (MFA)*: GCP soporta MFA y ha anunciado que será obligatoria para todos los clientes a partir de 2025.

Microsoft Azure:

- *Políticas de Acceso*: Azure Active Directory (AD) permite la gestión de identidades y acceso con políticas detalladas y control de acceso basado en roles.
- *Auditorías de Acceso*: Azure Monitor y Azure AD proporcionan capacidades de auditoría y monitoreo de actividades.
- *Autenticación Multifactor (MFA)*: Azure AD ofrece MFA y planea hacerla obligatoria para accesos a portales de administración a partir de 2024.

3. Matriz Comparativa: Prácticas en Relación con Principios Éticos y Normas

Proveedor	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento de Normas**
AWS	Cifrado en tránsito y en reposo; IAM con políticas detalladas; MFA recomendada.	AWS CloudTrail para auditorías; gestión de claves con KMS.	Infraestructura redundante; opciones de alta disponibilidad.	Certificaciones ISO 27001; alineación con NIST; cumplimiento de GDPR.
GCP	Cifrado en tránsito y en reposo por defecto; IAM con control de acceso basado en roles; MFA obligatoria en 2025.	Cloud Audit Logs para auditorías; gestión de claves con KMS.	Infraestructura global; servicios con acuerdos de nivel de servicio (SLA) sólidos.	Certificaciones ISO 27001; alineación con NIST; cumplimiento de GDPR.
Azure	Cifrado en tránsito y en reposo; Azure AD con políticas detalladas; MFA obligatoria para portales de administración en 2024.	Azure Monitor y Azure AD para auditorías; gestión de claves con Key Vault.	Infraestructura redundante; opciones de alta disponibilidad y recuperación ante desastres.	Certificaciones ISO 27001; alineación con NIST; cumplimiento de GDPR.

Cuadro 1: Comparativa de prácticas de almacenamiento y procesamiento en la nube entre AWS, GCP y Azure.

Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

Prácticas seleccionadas

1. **Cifrado avanzado de datos sensibles**:

- Uso de algoritmos modernos como AES-256 y RSA.
- Gestión segura de claves mediante herramientas como AWS KMS, Google Cloud KMS y Azure Key Vault.

2. **Control de accesos basado en permisos y principios de mínimo privilegio**:
   - Configuración de roles específicos utilizando IAM para garantizar que los usuarios solo tengan acceso a los recursos necesarios.
3. **Registros de auditoría para monitorear accesos**:
   - Implementación de auditorías automáticas como AWS CloudTrail, Google Cloud Audit Logs y Azure Monitor.
4. **Autenticación multifactor (MFA)**:
   - Refuerza la protección mediante un segundo factor para verificar la identidad del usuario.
5. **Infraestructura redundante y mecanismos de recuperación ante desastres**:
   - Garantizar la disponibilidad de los datos con configuraciones de alta redundancia y replicación.

Herramientas y componentes seleccionados

1. **AWS Key Management Service (KMS)**
   - **Ventajas**:
     - Gestión centralizada de claves de cifrado con rotación automática.
     - Integración nativa con otros servicios de AWS (S3, DynamoDB, etc.).
   - **Funcionamiento**:
     - Permite cifrar y descifrar datos de manera automática mediante políticas de seguridad predefinidas y personalizables.
2. **Google Cloud Identity and Access Management (IAM)**
   - **Ventajas**:
     - Control granular de permisos basado en roles (RBAC).
     - Opciones avanzadas de auditoría de acceso.
   - **Funcionamiento**:
     - Los administradores pueden asignar roles específicos a usuarios y servicios para garantizar el principio de mínimo privilegio.
3. **Azure Active Directory (AD)**
   - **Ventajas**:
     - Soporta autenticación multifactor (MFA) y acceso condicional.

- Fácil integración con aplicaciones empresariales.

- **Funcionamiento**:
  - Proporciona un entorno centralizado para administrar identidades y accesos, reforzando la autenticación y limitando el acceso con base en condiciones específicas (ubicación, dispositivo).

4. **AWS CloudTrail**
   - **Ventajas**:
     - Proporciona registros detallados de todas las actividades realizadas en la cuenta de AWS.
     - Mejora la trazabilidad de accesos y modificaciones a recursos.
   - **Funcionamiento**:
     - Captura automáticamente llamadas a la API, cambios en recursos y configuraciones, permitiendo auditorías de seguridad y cumplimiento normativo.

5. **Google Cloud Audit Logs**
   - **Ventajas**:
     - Ofrece registros centralizados de todas las actividades administrativas y de acceso en la plataforma.
     - Compatible con herramientas de análisis como BigQuery para evaluaciones avanzadas.
   - **Funcionamiento**:
     - Los registros se generan automáticamente para los recursos de GCP y se pueden almacenar, analizar o configurar para alertas personalizadas.

Establecimiento de un Proceso o Estándar de Validación

Objetivo

Garantizar el manejo ético y seguro de los datos mediante la implementación de un proceso estructurado que evalúe de manera continua los accesos, políticas y normativas de seguridad en el entorno de datos en la nube.

Proceso de Validación

1. **Evaluación periódica de permisos y accesos**
   - Realizar una revisión trimestral de los permisos asignados a usuarios y servicios en la nube.
   - Identificar accesos innecesarios o caducados y revocarlos de inmediato para cumplir con el principio de mínimo privilegio.
   - Utilizar herramientas específicas de cada proveedor, como:

- AWS IAM Access Analyzer.
- Google Cloud Policy Troubleshooter.
- Azure Active Directory Privileged Identity Management (PIM).

2. **Monitoreo continuo de la seguridad con auditorías y reportes de acceso**
   - Configurar auditorías automáticas para registrar eventos relacionados con la seguridad, como accesos no autorizados o modificaciones de políticas.
   - Revisar reportes de acceso generados por:
     - AWS CloudTrail para actividades en cuentas y recursos de AWS.
     - Google Cloud Audit Logs para eventos de GCP.
     - Azure Monitor y Log Analytics para actividades en Microsoft Azure.
   - Implementar un sistema de alertas automáticas para detectar y responder a incidentes en tiempo real.
3. **Revisión y actualización de políticas de acceso y uso de datos**
   - Realizar una revisión semestral de las políticas de acceso y uso de datos para garantizar su alineación con normativas vigentes, como GDPR, ISO/IEC 27001 y NIST.
   - Asegurarse de que las políticas reflejen los siguientes principios:
     - Confidencialidad: Solo los usuarios autorizados pueden acceder a datos sensibles.
     - Integridad: Prevenir modificaciones no autorizadas en los datos.
     - Disponibilidad: Asegurar que los datos estén disponibles cuando se necesiten.
   - Actualizar las políticas para incorporar nuevos requisitos regulatorios o cambios en la infraestructura tecnológica.

Conclusión

Este proceso de validación garantiza un enfoque proactivo en la seguridad de los datos en la nube, protegiendo la información sensible mediante evaluaciones periódicas, monitoreo continuo y actualizaciones alineadas con estándares y normativas internacionales.

Referencias

[1] AWS (n.d.). Cifrado de los datos en tránsito. https://docs.aws.amazon.com/es_es/whitepapers/latest/navigating-gdpr-compliance/encrypt-data-in-transit.html.

[2] AWS (n.d.). Cifrado de los datos en reposo. https://nubax.com.ar/migracion-cloud-estrategias/.

[3] Políticas y permisos en AWS Identity and Access Management. https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/access_policies.html.

[4] Microsoft (n.d.). Información general del cifrado de Azure. https://learn.microsoft.com/es-es/azure/security/fundamentals/encryption-overview.

[5] Microsoft (n.d.). Principios y dependencias de diseño de acceso condicional. https://learn.microsoft.com/es-es/azure/architecture/guide/security/conditional-access-design.

[6] Microsoft (n.d.). Planificación para la autenticación multifactor obligatoria para Azure y otros portales de administración. https://learn.microsoft.com/es-es/entra/identity/authentication/concept-mandatory-multifactor-authentication.

[7] Microsoft (n.d.). Seguridad e identidad multinube con Azure y Amazon Web Services (AWS). https://learn.microsoft.com/es-es/azure/architecture/aws-professional/security-identity.

[8] Microsoft (n.d.). Comparación entre servicios de Google Cloud y Azure. https://learn.microsoft.com/es-es/azure/architecture/gcp-professional/services.

[9] Microsoft (n.d.). Administración de la posición de seguridad en la nube (CSPM). https://learn.microsoft.com/es-es/azure/defender-for-cloud/concept-cloud-security-posture-management.

[10] Microsoft (n.d.). Procedimientos recomendados de cifrado y seguridad de datos en Azure. https://learn.microsoft.com/es-es/azure/security/fundamentals/data-encryption-best-practices.