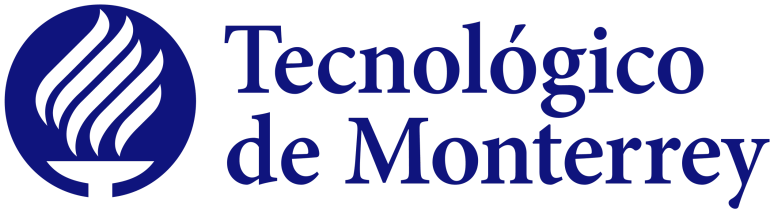
Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Monterrey



Inteligencia artificial avanzada para la ciencia de datos II
TC3007C, Grupo 101

Nombre del profesor: Félix Ricardo Botello Urrutia

Cloud computing | Evidencia - Portafolio

Marcelo de Luna | A00832239

Noviembre 2024

1. Amazon Web Services (AWS)

- **Cifrado de datos**:
  - **En tránsito**: TLS/SSL para asegurar las comunicaciones.
  - **En reposo**: Cifrado AES-256. Ofrece control de claves mediante AWS Key Management Service (KMS).
- **Prácticas de confidencialidad**:
  - Políticas de acceso basadas en permisos mediante IAM (Identity and Access Management).
  - Auditorías de acceso con AWS CloudTrail.
  - Autenticación multifactor (MFA) opcional para todas las cuentas y servicios críticos.

2. Google Cloud Platform (GCP)

- **Cifrado de datos**:
  - **En tránsito**: Usa TLS 1.3 para la mayoría de las comunicaciones.
  - **En reposo**: AES-256 predeterminado y opciones avanzadas para control de claves con Cloud KMS.
- **Prácticas de confidencialidad**:
  - IAM granular con roles personalizados.
  - Auditorías de acceso a través de Cloud Audit Logs.
  - MFA y soporte para hardware keys (como FIDO).

3. Microsoft Azure

- **Cifrado de datos**:
  - **En tránsito**: TLS/SSL.
  - **En reposo**: Cifrado predeterminado con AES-256 y soporte para Bring Your Own Key (BYOK) con Azure Key Vault.
- **Prácticas de confidencialidad**:
  - IAM y Azure Active Directory (Azure AD) para acceso basado en roles.
  - Auditorías con Azure Monitor y Azure Security Center.
  - Autenticación multifactor incluida para entornos críticos.

Aspecto	AWS	GCP	Azure	Principios Éticos	Normas
Cifrado de datos en tránsito	TLS/SSL	TLS 1.3	TLS/SSL	Confidencialidad	ISO 27001, GDPR
Cifrado de datos en reposo	AES-256, control de claves	AES-256, control de claves	AES-256, control de claves	Confidencialidad, Integridad	ISO 27001, GDPR
Políticas de acceso	IAM granular	IAM granular	IAM con Azure AD	Confidencialidad	ISO 27001, NIST
Auditorías de acceso	AWS CloudTrail	Cloud Audit Logs	Azure Monitor	Integridad, Confidencialidad	NIST, GDPR
Autenticación multifactor	MFA para cuentas y servicios	MFA con hardware keys	MFA con Azure AD	Confidencialidad	ISO 27001
Disponibilidad	Alta disponibilidad regional	Alta disponibilidad regional	Alta disponibilidad regional	Disponibilidad	NIST

AWS Key Management Service (KMS)

- **Descripción**: Proporciona administración centralizada de claves de cifrado para proteger datos en reposo y en tránsito. Compatible con estándares AES-256.
- **Ventajas**:
    - Control total sobre las claves (rotación, eliminación, auditoría).
    - Integración con otros servicios de AWS como S3, RDS y EBS.
    - Compatible con Bring Your Own Key (BYOK).
- **Uso recomendado**: Protección avanzada de datos confidenciales mediante cifrado personalizado.

Google Cloud IAM (Identity and Access Management)

- **Descripción**: Gestiona el acceso a los recursos de GCP mediante roles y permisos granulares.
- **Ventajas**:
    - Roles personalizados y predefinidos para un control detallado.
    - Implementación del principio de mínimo privilegio.
    - Integración con auditorías en Cloud Audit Logs.
- **Uso recomendado**: Control preciso del acceso a recursos críticos para minimizar riesgos de exposición de datos.

Azure Active Directory (Azure AD)

- **Descripción**: Servicio de identidad y control de acceso que permite gestionar usuarios y dispositivos en entornos de Azure.
- **Ventajas**:
    - Autenticación multifactor (MFA) integrada.
    - Compatibilidad con Single Sign-On (SSO) y autenticación de aplicaciones SaaS.
    - Detección de amenazas mediante inteligencia de seguridad.
- **Uso recomendado**: Administración centralizada de identidades y control de accesos en entornos híbridos o multi-nube.

AWS CloudTrail

- **Descripción**: Servicio de auditoría que registra toda la actividad en la cuenta de AWS, incluyendo acciones de usuarios y servicios.
- **Ventajas**:
    - Registros detallados para cumplir con normativas como GDPR y NIST.
    - Integración con servicios de análisis como Amazon CloudWatch.
    - Soporte para alertas en tiempo real sobre actividades sospechosas.
- **Uso recomendado**: Monitoreo continuo de accesos y auditorías para identificar anomalías.

Google Cloud Key Management Service (Cloud KMS)

- **Descripción**: Solución de gestión de claves para cifrado en reposo y en tránsito. Admite integraciones con API de encriptación personalizada.
- **Ventajas**:
    - Claves administradas por el cliente o proporcionadas por Google.
    - Opciones de auditoría mediante Cloud Logging.
    - Soporte para cifrado de disco persistente, almacenamiento y bases de datos.
- **Uso recomendado**: Encriptación avanzada de datos sensibles con control y visibilidad de las claves.

Evaluación Periódica de Permisos y Accesos

Pasos clave

1. **Inventario de usuarios y permisos**:
    - Generar un listado de todos los usuarios y roles con acceso a sistemas críticos.
    - Identificar permisos asignados y evaluar su adecuación según funciones laborales.
2. **Auditoría de permisos**:
    - Comparar los permisos existentes con el principio de mínimo privilegio.
    - Revocar permisos innecesarios o excesivos.
3. **Validación de roles**:
    - Revisar la configuración de roles predefinidos o personalizados en IAM (AWS, GCP, Azure).
    - Garantizar que los permisos no excedan lo requerido para cada rol.
4. **Frecuencia recomendada**:
    - Realizar evaluaciones trimestrales.

Monitoreo Continuo de Seguridad con Auditorías y Reportes de Acceso

Pasos clave

1. **Habilitar registros de auditoría**:
    - Activar herramientas como AWS CloudTrail, Google Cloud Audit Logs o Azure Monitor.
    - Asegurar que los registros incluyan actividades de lectura, escritura y eliminación de datos.
2. **Análisis automatizado de accesos**:
    - Utilizar herramientas SIEM (Security Information and Event Management) para detectar actividades anómalas.
    - Generar alertas automáticas para accesos no autorizados o cambios críticos en la configuración.
3. **Reporte de actividades**:
    - Generar informes mensuales que incluyan métricas de acceso, eventos sospechosos y tendencias.
    - Presentar los informes al equipo de seguridad y a responsables de cumplimiento.
4. **Frecuencia recomendada**:
    - Monitoreo continuo con revisiones semanales de los reportes.

Revisión y Actualización de Políticas de Acceso y Uso de Datos

Pasos clave

1. **Evaluar políticas actuales**:
    - Verificar que las políticas de acceso cumplan con normativas como GDPR (consentimiento y propósito específico) e ISO/IEC 27001 (gestión de seguridad de la información).
    - Revisar los procedimientos documentados para la gestión de accesos.
2. **Actualizar según necesidades**:
    - Ajustar políticas en función de cambios organizacionales (nuevas áreas, roles, proyectos).
    - Incorporar nuevos requisitos legales o estándares de la industria.
3. **Validación de equipo autorizado**:
    - Confirmar que solo personal autorizado tenga acceso a datos sensibles.
    - Establecer un proceso de aprobación para otorgar nuevos accesos.
4. **Capacitación y concienciación**:
    - Realizar entrenamientos anuales para el personal sobre manejo ético y seguro de datos.
    - Asegurar que el equipo esté al tanto de las actualizaciones normativas.
5. **Frecuencia recomendada**:
    - Revisiones semestrales o cuando ocurran cambios significativos.

Conclusión

El manejo ético y seguro de datos en la nube exige combinar herramientas avanzadas, buenas prácticas y cumplimiento normativo. AWS, GCP y Azure ofrecen soluciones sólidas para cifrado, gestión de accesos y auditorías, esenciales para proteger los datos y cumplir estándares como ISO/IEC 27001 y GDPR.

Un proceso de validación periódico que evalúe permisos, monitoree accesos y actualice políticas asegura la confidencialidad, integridad y disponibilidad de la información. Este enfoque fortalece la seguridad, fomenta la confianza y garantiza un manejo ético de los datos.