



Tecnológico de Monterrey

Inteligencia artificial avanzada para la ciencia de datos II (Gpo 101)

Profesor: Félix Ricardo Botello Urrutia

Evidencia Portafolio

Sofía Cantú Talamantes

A01571120

Noviembre 2024

Índice

1. Evaluación de Prácticas de Almacenamiento y Procesamiento en la Nube.....	2
2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad.....	3
3. Establecimiento de un Proceso o Estándar de Validación.....	4
4. Conclusiones.....	5

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

Características	AWS	Azure	Google Cloud	Principios Éticos	Normas
Cifrado en reposo	AWS KMS	Azure SSE	Cloud KMS	Confidencialidad	ISO/IEC 27001, GDPR
Curado en tránsito	SSL/TLS	SSL/TLS	HTTPS, TLS	Confidencialidad	ISO(IEC 27001, GDPR
Control de acceso basado en permisos	AWS IAM	Azure RBAC	Cloud IAM	Confidencialidad	ISO/IEC 27001
Auditorías de acceso	AWS CloudTrail	Azure Monitor Logs	Cloud Audit Logs	Integridad	NIST
Autenticación multifactor (MFA)	MFA en AWS IAM	MFA en Azure AD	MFA en Cloud Identity	Confidencialidad	ISO/IEC 2701

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

1. AWS Key Management Service (KMS):
 - Ventajas: Proporciona gestión centralizada de claves de cifrado, integración con otros servicios de AWS.
 - Funcionamiento: Permite crear, administrar y controlar claves de cifrado utilizadas para proteger datos.
2. Azure Active Directory (Azure AD):
 - Ventajas: Servicio de gestión de identidades y accesos, soporta MFA y SSO.
 - Funcionamiento: Controla el acceso a recursos y aplicaciones mediante autenticación y autorización centralizadas.
3. Google Cloud Identity and Access Management (IAM):
 - Ventajas: Ofrece control granular sobre quién puede hacer qué en los recursos de Google Cloud.
 - Funcionamiento: Define políticas basadas en roles para otorgar permisos a usuarios y grupos.
4. AWS CloudTrail:
 - Ventajas: Registro detallado de llamadas a API y actividad de la cuenta.
 - Funcionamiento: Monitorea y registra acciones en la cuenta AWS para auditorías y detección de anomalías.
5. Azure Security Center:
 - Ventajas: Proporciona visibilidad unificada de la seguridad, recomendaciones y gestión de políticas.
 - Funcionamiento: Supervisa el estado de seguridad de los recursos, detecta amenazas y sugiere mejoras.

2. Establecimiento de un Proceso o Estándar de Validación

El proceso de validación será “Proceso de Validación y Gestión Segura de Datos en la Nube”. Este procedimiento aplica a todo el personal y sistemas que manejan datos sensibles en la organización. Los pasos son los siguientes:

1. Evaluación Periódica de Permisos y Accesos: Revisar trimestralmente los permisos asignados a usuarios y roles.
 - Generar un informe de usuarios y sus permisos actuales.
 - Verificar que los permisos correspondan con las responsabilidades actuales.
 - Revocar accesos innecesarios o modificar según sea necesario.
2. Monitoreo Continuo de la Seguridad: Implementar auditorías y monitoreo en tiempo real.
 - Configurar registros de auditoría (logs) en los servicios de nube.
 - Analizar logs regularmente para detectar actividades sospechosas.
 - Utilizar alertas automáticas para eventos críticos.
3. Revisión y Actualización de Políticas de Acceso y Uso de Datos: Mantener las políticas alineadas con las normativas vigentes y mejores prácticas.
 - Revisar semestralmente las políticas de seguridad y acceso.
 - Actualizar políticas para reflejar cambios regulatorios o internos.
 - Comunicar cambios al personal y ofrecer capacitación si es necesario.

2. Conclusiones

La seguridad y confidencialidad de los datos en la nube es fundamental para proteger la información sensible de la organización y de sus clientes. Al comparar las prácticas de los principales proveedores de servicios en la nube, es evidente que todos ofrecen herramientas robustas para garantizar la seguridad. Sin embargo, es responsabilidad de la organización implementar correctamente estas herramientas y mantener procesos activos de validación y mejora continua. Adoptar un enfoque proactivo en la gestión de la seguridad no solo asegura el cumplimiento normativo, sino que también fortalece la confianza de los clientes y mejora la reputación de la empresa en el mercado.