Instituto Tecnológico y de Estudios Superiores de Monterrey

“Evidencia Portafolio - Módulo Cloud Computing”

Inteligencia Artificial Avanzada para la Ciencia de Datos II (Gpo 101)

25/11/2024

Mtro. Félix Ricardo Botello Urrutia

Estudiante:

Eryk Elizondo González A01284899

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

Políticas / Proveedor	AWS	GCP	Azure
Cifrado en Tránsito	TLS 1.2 https://docs.aws.amazon.com/es_es/efs/latest/ug/encryption-in-transit.html	TLS 1.2/1.3 https://cloud.google.com/docs/security/encryption-in-transit?hl=es-419	TLS 1.2 https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tls-support
Cifrado en Reposo	AES-256 https://docs.aws.amazon.com/es_es/efs/latest/ug/encryption-at-rest.html	AES-256 https://cloud.google.com/docs/security/encryption/default-encryption?hl=es-419	AES-256 https://learn.microsoft.com/es-es/azure/security/fundamentals/encryption-atrest
Políticas de Acceso	IAM con roles y principios de mínimo privilegio https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/access_policies.html	IAM con principios de seguridad Zero Trust https://cloud.google.com/beyondcorp?hl=es-419	RBAC con políticas personalizadas https://learn.microsoft.com/en-us/azure/role-based-access-control/overview
Auditorías de Acceso	AWS CloudTrail https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/security-audit-guide.html	Cloud Audit Logs https://cloud.google.com/logging/docs/audit?hl=es-419	Azure Monitor y Log Analytics https://learn.microsoft.com/es-es/azure/azure-monitor/logs/log-analytics-tutorial
Autenticación Multifactor	MFA con hardware y software https://aws.amazon.com/es/iam/features/mfa/	MFA integrado con soporte para U2F https://cloud.google.com/identity-platform/docs/web/mfa?hl=es-419	MFA con Azure AD https://www.microsoft.com/es-mx/security/business/identity-access/microsoft-entra-id
Cumplimiento de ISO/IEC 27001	Cumple con ISO/IEC 27001	Cumple con ISO/IEC 27001	Cumple con ISO/IEC 27001

	https://aws.amazon.com/es/compliance/iso-27001-faqs/	https://cloud.google.com/security/compliance/iso-27001?hl=es-419	https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001
Cumplimiento de GDPR	Cumple con GDPR https://aws.amazon.com/es/compliance/gdpr-center/	Cumple con GDPR https://cloud.google.com/privacy/gdpr?hl=es-419	Cumple con GDPR https://azure.microsoft.com/de-de/blog/protecting-privacy-in-microsoft-azure-gdpr-azure-policy-updates/
Cumplimiento de NIST	Compatible con NIST 800-53 https://aws.amazon.com/es/compliance/nist/	Compatible con NIST 800-53 https://cloud.google.com/security/compliance/nist800-53?hl=es-419	Compatible con NIST 800-53 https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

a) AWS CloudTrail

i) **Ventaja:** Ofrece registros detallados de actividad en la cuenta.

ii) **Función:** Monitorea cambios en recursos y detecta accesos no autorizados.

iii) https://aws.amazon.com/es/cloudtrail/

b) Google Cloud IAM

i) **Ventaja:** Gestión centralizada de permisos basada en roles.

ii) **Función:** Garantiza el acceso limitado a los recursos necesarios.

iii) https://cloud.google.com/security/products/iam?hl=es-419

c) Azure Key Vault

i) **Ventaja:** Almacena y gestiona claves, certificados y secretos de forma segura.

ii) **Función:** Protege credenciales sensibles usadas por aplicaciones.

iii) https://azure.microsoft.com/en-us/products/key-vault

d) AWS GuardDuty

i) **Ventaja:** Detección de amenazas basadas en inteligencia artificial.

ii) **Función:** Monitorea patrones inusuales de actividad.

iii) https://aws.amazon.com/es/guardduty/

e) Google Cloud DLP

i) **Ventaja:** Identifica y protege datos sensibles automáticamente.

ii) **Función:** Escanea datos para prevenir filtraciones.

iii) https://cloud.google.com/security/products/dlp?hl=es-419

3. Establecimiento de un Proceso o Estándar de Validación

- **Procedimiento:** Política de Manejo Ético y Seguro de Datos
- **Alcance**: Aplicable a todas las operaciones que involucren datos sensibles almacenados o procesados en la nube.
- **Pasos del Procedimiento:**

1. Evaluación inicial de accesos:
    - Identificar usuarios y permisos actuales.
    - Comparar configuraciones con principios de mínimo privilegio.
2. Monitoreo continuo:
    - Implementar herramientas como AWS GuardDuty o Azure Monitor.
    - Realizar auditorías automáticas cada semana.
3. Actualización de políticas:
    - Revisar cada tres meses las políticas de IAM/RBAC.

    - Asegurar que cumplen con ISO/IEC 27001 y GDPR.

4. Pruebas de seguridad:
    - Ejecutar simulaciones de ataque (penetration testing).
    - Validar la efectividad de las medidas implementadas.
5. Capacitación y comunicación:
    - Entrenar al equipo sobre nuevas amenazas y herramientas.
    - Establecer canales claros para reportar incidentes.

- **Diagrama:**
    - Evaluación inicial → Monitoreo continuo → Actualización de políticas → Pruebas de seguridad → Capacitación.

4. Conclusiones

- AWS, Google Cloud y Azure tienen capacidades robustas para garantizar seguridad, confidencialidad e integridad.
- La selección de herramientas adecuadas asegura un balance entre protección y eficiencia.
- Implementar un proceso de validación continuo y revisable garantiza el cumplimiento de normativas y reduce riesgos operativos.