Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Monterrey

Materia

Inteligencia artificial avanzada para la ciencia de datos II

Tarea

Cloud Computing | Evidencia Portafolio

Estudiantes

Cleber Gerardo Pérez Galicia - A01236390

Profesor

Félix Ricardo Botello Urrutia

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

Proveedor	Confidencialidad	Integridad	Disponibilidad	Cumplimiento Normativo
AWS	Cifrado AES-256 en reposo, TLS 1.2 en tránsito, IAM para control detallado de accesos.	Firmas digitales en S3, validación de integridad en API Gateway.	SLA de monitoreo con CloudWatch, redundancia en varias regiones.	Certificaciones ISO/IEC 27001, SOC 2, GDPR, cumplimiento con NIST 800-53.
Google Cloud	Cifrado predeterminado en reposo y en tránsito, gestión de claves (CMEK) para cifrado avanzado.	Verificación de integridad en Cloud Storage, registros de auditoría detallados con Cloud Audit Logs.	SLA de arquitectura multiregión, redundancia activa-activa.	Certificaciones ISO/IEC 27001, SOC 2, GDPR, cumplimiento con NIST 800-53.
Azure	Cifrado en reposo con Azure Disk Encryption, TLS/SSL en tránsito, Azure Active Directory (AAD) para gestión.	Monitoreo de integridad con Azure Monitor, Azure Policy para evitar configuraciones erróneas.	SLA de replicación geográfica con Azure Site Recovery.	Certificaciones ISO/IEC 27001, SOC 2, GDPR, cumplimiento con NIST 800-53.

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

- **Cifrado avanzado de datos sensibles.**

Se implementa el cifrado de datos tanto en tránsito como en reposo para garantizar la confidencialidad e integridad de la información. El estándar AES-256 de AWS es utilizado ampliamente debido a su nivel de seguridad, el cual se basa en una clave de 256 bits que protege los datos contra accesos no autorizados. Además, se emplean mecanismos

complementarios como claves rotativas y cifrado de extremos a extremo en las comunicaciones más críticas.

- **Registros de auditoría y monitoreo continuo.**

Se habilitan servicios como CloudTrail en AWS o Cloud Audit Logs en Google Cloud para rastrear todas las actividades relacionadas con el acceso, configuración y operaciones críticas en la infraestructura. Estos registros permiten realizar análisis forenses en caso de incidentes y asegurar el cumplimiento de normativas. También se configuran alertas en tiempo real para identificar patrones inusuales que puedan indicar intentos de acceso malintencionados.

- **Autenticación Multifactor.**

Se requiere la autenticación multifactor (MFA) para todos los accesos administrativos y transacciones sensibles en todas las plataformas, reduciendo significativamente el riesgo de accesos no autorizados incluso si las credenciales son comprometidas. Se favorecen métodos robustos como aplicaciones autenticadoras y tokens físicos sobre métodos más vulnerables como mensajes SMS.

- **Segmentación de red y monitoreo avanzado.**

Se implementa una arquitectura de red segmentada para minimizar la superficie de ataque y contener posibles brechas. Esto incluye el uso de firewalls virtuales, redes privadas virtuales (VPN) y herramientas avanzadas de detección y prevención de intrusiones (IDS/IPS). Los sistemas están configurados para analizar el tráfico en busca de comportamientos anómalos y responder automáticamente ante posibles amenazas.

- **Control de accesos basados en permisos.**

Se adopta el principio de privilegios mínimos utilizando sistemas de gestión de identidades como IAM en AWS o Azure Active Directory (AAD). Cada usuario o entidad tiene acceso únicamente a los recursos necesarios para realizar sus funciones, y los permisos son revisados periódicamente para garantizar su adecuación. Además, se registran todas las solicitudes de acceso y cambios en permisos para auditorías posteriores.

3. Establecimiento de un Proceso o Estándar de Validación

Evaluación Periódica de Permisos y Accesos (Trimestral)

Realizar una revisión detallada de los roles y permisos asignados en herramientas como IAM (AWS, Google Cloud) o AAD (Azure). Esto incluye la identificación y eliminación de permisos no utilizados, caducados o que excedan los requerimientos mínimos para cada usuario o aplicación. Adicionalmente, implementar un proceso de notificación y

validación con los responsables de cada área para asegurar que los cambios no afecten las operaciones críticas.

Monitoreo Continuo de Seguridad

Configurar herramientas como AWS CloudWatch, Google Cloud Operations Suite, o Azure Monitor para supervisar constantemente las actividades, métricas de desempeño y posibles anomalías en el entorno. Generar informes mensuales de seguridad que incluyan análisis de tendencias, indicadores clave de rendimiento (KPI) y recomendaciones para mitigar riesgos detectados. Complementar este monitoreo con alertas automatizadas para responder rápidamente a incidentes de seguridad.

Revisión y Actualización de Políticas de Acceso y Uso de Datos (Semestral)

Actualizar las políticas de acceso y uso de datos para alinearlas con los cambios tecnológicos, operativos y regulatorios. Esto incluye asegurarse de que las políticas sean compatibles con normativas como GDPR, ISO/IEC 27001, HIPAA (si aplica), o cualquier otra regulación específica del sector. Las actualizaciones deben ser comunicadas a todos los usuarios relevantes y acompañadas de capacitaciones necesarias para su correcta implementación.

Auditorías de Cumplimiento Normativo (Anual)

Contratar servicios de auditoría externa para realizar evaluaciones integrales de conformidad con estándares como ISO/IEC 27001, GDPR, SOC 2, u otras regulaciones aplicables. Estas auditorías deben incluir la revisión de los procesos internos, políticas de seguridad, configuraciones de infraestructura y controles implementados. Además, documentar los hallazgos y planes de acción para abordar cualquier incumplimiento identificado.

Pruebas de Penetración y Escaneos de Vulnerabilidades (Bianual)

Realizar pruebas de penetración (pentesting) semestralmente o después de cambios significativos en el entorno. Contratar expertos certificados para simular ataques reales y descubrir vulnerabilidades en aplicaciones, redes, y configuraciones. Complementar estas pruebas con escaneos automatizados de vulnerabilidades para identificar riesgos recurrentes. Documentar los resultados y garantizar que las vulnerabilidades detectadas sean mitigadas de manera oportuna.