Tecnológico de Monterrey

Inteligencia artificial avanzada para la ciencia de datos II

(Gpo 101)

Evidencia Portafolio - Módulo cloud computing

Ricardo Salinas Quiroga

A01284657

Noviembre del 2024

1. Evaluación de Prácticas de Almacenamiento y Procesamiento en AWS

AWS es uno de los proveedores más completos en cuanto a seguridad en la nube. Algunas de sus principales prácticas incluyen:

- Cifrado avanzado: Utilizan TLS para proteger datos en tránsito y KMS para cifrarlos en reposo.
- Control de accesos: IAM permite establecer roles y políticas para garantizar que cada usuario o servicio tenga únicamente los permisos necesarios.
- Monitoreo continuo: CloudTrail registra toda la actividad en la cuenta, lo que facilita la identificación de accesos no autorizados o configuraciones incorrectas.

Matriz Comparativa de Seguridad en AWS

Aspecto Evaluado	**Práctica Implementada**	**Normativas Relacionadas**
Cifrado	TLS (en tránsito), KMS (en reposo)	ISO/IEC 27001, GDPR
Control de Accesos	IAM con permisos mínimos	NIST 800-53
Monitoreo	CloudTrail para auditorías	ISO/IEC 27001

2. Selección de Herramientas y Prácticas de AWS

De las herramientas disponibles en AWS, se seleccionaron las siguientes cinco por ser las más útiles para proteger datos en la nube:

1. IAM: Permite gestionar quién accede a qué, aplicando el principio de menor privilegio.
2. AWS KMS: Facilita el cifrado de datos sensibles y la gestión de claves de seguridad.
3. CloudTrail: Registra todas las actividades en la cuenta para facilitar auditorías y el rastreo de incidentes.
4. GuardDuty: Detecta posibles amenazas o comportamientos anómalos en la infraestructura.
5. AWS Config: Evalúa las configuraciones para garantizar que cumplen con los estándares establecidos.

3. Procedimiento para el Manejo Seguro de Datos

A continuación, se describe un procedimiento simple y efectivo para gestionar datos de forma segura utilizando AWS:

Nombre: Proceso de Seguridad y Validación en la Nube

Objetivo: Proteger los datos almacenados en la nube, garantizar accesos controlados y asegurar el cumplimiento de normativas internacionales.

Pasos:

1. Definición de Roles y Permisos: Configurar IAM para asignar accesos específicos según el rol de cada usuario o servicio.
2. Cifrado de Información: Implementar AWS KMS para cifrar datos en reposo y asegurar que toda la comunicación esté protegida con TLS.
3. Monitoreo de Actividades: Activar CloudTrail para registrar cada acción dentro de la cuenta de AWS.
4. Supervisión Constante: Usar AWS Config para identificar configuraciones incorrectas o desviaciones de los estándares de seguridad.
5. Auditorías Periódicas: Revisar trimestralmente los permisos y los registros de CloudTrail para detectar anomalías.

Conclusión

AWS ofrece las herramientas necesarias para implementar un entorno seguro y confiable en la nube, con prácticas básicas como el cifrado de datos, la gestión de accesos y el monitoreo continuo, se puede garantizar que los datos estén protegidos. La clave está en mantener procesos de auditoría regulares y aprovechar al máximo las herramientas que AWS ya ofrece para evitar riesgos innecesarios.