Tecnológico de Monterrey

INTELIGENCIA ARTIFICIAL AVANZADA
PARA LA CIENCIA DE DATOS II

TC3007C

Reporte de Seguridad en la Nube

Autor:
Héctor Hibran Tapia Fernández - A01661114

30 de noviembre de 2024

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

A continuación, se presenta una comparación de los principales proveedores de servicios en la nube: **AWS**, **Google Cloud** y **Azure**. Se presentan sus características de seguridad y prácticas de confidencialidad, estás están clasificadas en relación con los principios éticos (confidencialidad, integridad y disponibilidad) y normas internacionales como ISO/IEC 27001, NIST y GDPR.

Proveedor	Características de Seguridad	Prácticas de Confidencialidad	Principios Éticos	Normas Internacionales
AWS	▪ **Cifrado de datos en reposo y en tránsito** mediante SSL/TLS y opciones de cifrado del lado del servidor y cliente. ▪ **Herramientas de seguridad avanzadas** como AWS KMS y AWS Shield.	▪ **Control de acceso basado en permisos** con AWS IAM. ▪ **Auditorías de acceso** a través de AWS CloudTrail. ▪ **Autenticación multifactor (MFA)** para mayor seguridad.	▪ **Confidencialidad**: Protección de datos y acceso restringido. ▪ **Integridad**: Monitoreo constante y registro de actividades. ▪ **Disponibilidad**: Infraestructura redundante y escalable.	▪ **ISO/IEC 27001**: Certificado. ▪ **NIST**: Cumple con NIST SP 800-53. ▪ **GDPR**: Ofrece recursos para el cumplimiento.
Google Cloud	▪ **Cifrado de datos en reposo por defecto** y en tránsito con TLS. ▪ **Seguridad de la red** mediante VPC y Cloud Armor.	▪ **Políticas de acceso detalladas** con Cloud IAM. ▪ **Registro y monitoreo** con Cloud Logging y Monitoring. ▪ **MFA** con verificación en dos pasos.	▪ **Confidencialidad**: Control de acceso granular y cifrado robusto. ▪ **Integridad**: Auditorías y seguimiento en tiempo real. ▪ **Disponibilidad**: Servicios globales con alta redundancia.	▪ **ISO/IEC 27001**: Certificado. ▪ **NIST**: Mapas de cumplimiento disponibles. ▪ **GDPR**: Recursos para el cumplimiento.
Microsoft Azure	▪ **Cifrado en reposo** con Azure Storage Encryption. ▪ **Cifrado en tránsito** con HTTPS/TLS. ▪ **Protección avanzada** con Security Center.	▪ **Gestión de identidades y acceso** con Azure AD y RBAC. ▪ **Auditorías de acceso** con Monitor Logs. ▪ **MFA** con Azure MFA.	▪ **Confidencialidad**: Acceso seguro y cifrado. ▪ **Integridad**: Monitoreo y alertas continuas. ▪ **Disponibilidad**: Alta disponibilidad y recuperación.	▪ **ISO/IEC 27001**: Certificado. ▪ **NIST**: Cumple con SP 800-53 y CSF. ▪ **GDPR**: Herramientas para el cumplimiento.

2. Selección de Prácticas y Herramientas de Seguridad/Confidencialidad

Basádonos en la matriz de comparación, seleccioné siguientes prácticas y herramientas de seguridad para proteger los datos en la nube, no necesariamente todas pertenecen al mismo proveedor:

1. **AWS Key Management Service (KMS)**

   AWS KMS es un servicio de gestión de claves que permite crear y controlar claves de cifrado para proteger datos. Ofrece integración con otros servicios de AWS y facilita el cifrado avanzado de datos sensibles. Su ventaja principal es la gestión centralizada de claves con altos niveles de seguridad y cumplimiento, además de la alta disponibilidad con la que AWS se diferencia de la competencia.

2. **Google Cloud Identity and Access Management (IAM)**

   Cloud IAM proporciona control detallado sobre quién puede hacer qué en la plataforma de Google Cloud. Implementa el principio de mínimo privilegio, permitiendo definir permisos específicos para usuarios y recursos. Esto mejora la confidencialidad al limitar el acceso únicamente a lo necesario.

3. **Azure Active Directory (Azure Entra ID)**

   Azure Entra ID es un servicio de gestión de identidades y accesos que ofrece autenticación multifactor y control de acceso basado en roles. Facilita el manejo seguro de identidades y la aplicación de políticas de seguridad, fortaleciendo la integridad y confidencialidad de los datos.

4. **AWS CloudTrail**

   AWS CloudTrail registra y monitorea las actividades y llamadas a las APIs dentro de la cuenta de AWS. Proporciona registros de auditoría detallados, lo que permite revisar accesos y acciones realizadas.

5. **Azure Security Center**

   Azure Security Center es una herramienta de gestión central de seguridad que ayuda a prevenir, detectar y responder a amenazas. Ofrece recomendaciones de seguridad, evaluación de configuraciones y detección de amenazas.

3. Establecimiento de un Proceso o Estándar de Validación

Para asegurar el manejo ético y seguro de los datos en la nube, propongo el siguiente proceso de validación:

1. **Evaluación Periódica de Permisos y Accesos**

   Realizar revisiones regulares de los permisos asignados a usuarios y roles, asegurando que se mantengan alineados el principio de mínimo privilegio. Esto incluye:

   - Identificar y revocar accesos innecesarios o caducados.
   - Validar que los nuevos permisos otorgados sean adecuados y justificados.
   - Documentar cambios en los permisos para seguimiento y auditoría.

2. **Monitoreo Continuo de la Seguridad con Auditorías y Reportes de Acceso**

   - Configurar alertas para actividades sospechosas o no autorizadas.
   - Generar informes periódicos sobre accesos y acciones realizadas.
   - Analizar los registros de auditoría para identificar patrones o amenazas potenciales.

3. **Revisión y Actualización de Políticas de Acceso y Uso de Datos**

   - Revisar las políticas de acceso y uso de datos al menos una vez al año o después de cambios significativos.
   - Asegurar el cumplimiento con normativas vigentes como GDPR, ISO/IEC 27001 y NIST.
   - Comunicar y capacitar al personal sobre las políticas y procedimientos actualizados.

4. Conclusión

Los tres proveedores son opciones realmente sólidas, y la elección dependerá en gran medida de las necesidades específicas de cada cliente. Cada uno cuenta con clientes de talla mundial, como AWS con Netflix, Google Cloud con Spotify y Azure con GitHub. Todos ofrecen características de seguridad y prácticas de confidencialidad alineadas con los principios éticos de confidencialidad, integridad y disponibilidad. La selección de las herramientas mencionadas proporciona el enfoque necesario para proteger los datos en la nube, garantiza el cifrado avanzado, el control de acceso y el monitoreo continuo, cumpliendo con normativas como ISO/IEC 27001, NIST y GDPR.

Referencias

[1] Amazon Web Services (AWS). (n.d.). *AWS Identity and Access Management (IAM)*. Recuperado de https://aws.amazon.com/es/iam/

[2] Amazon Web Services (AWS). (n.d.). *AWS CloudTrail*. Recuperado de https://aws.amazon.com/es/cloudtrail/

[3] Amazon Web Services (AWS). (n.d.). *AWS ISO 27001*. Recuperado de https://aws.amazon.com/es/compliance/iso-27001-faqs/

[4] Amazon Web Services (AWS). (n.d.). *AWS NIST Compliance*. Recuperado de https://aws.amazon.com/es/compliance/nist/

[5] Amazon Web Services (AWS). (n.d.). *Centro de Cumplimiento GDPR de AWS*. Recuperado de https://aws.amazon.com/es/compliance/gdpr-center/

[6] Google Cloud. (n.d.). *Cifrado en Google Cloud*. Recuperado de https://cloud.google.com/security/encryption-at-rest/?hl=es

[7] Google Cloud. (n.d.). *Identidad y Gestión de Acceso*. Recuperado de https://cloud.google.com/iam/?hl=es

[8] Google Cloud. (n.d.). *Google Cloud Logging*. Recuperado de https://cloud.google.com/logging/?hl=es

[9] Google Cloud. (n.d.). *Google Cloud ISO 27001*. Recuperado de https://cloud.google.com/security/compliance/iso-27001/?hl=es

[10] Google Cloud. (n.d.). *Google Cloud NIST*. Recuperado de https://cloud.google.com/security/compliance/nist800-53?hl=es-419

[11] Google Cloud. (n.d.). *Cumplimiento GDPR*. Recuperado de https://cloud.google.com/security/gdpr/?hl=es

[12] Microsoft Azure. (n.d.). *Cifrado de Almacenamiento de Azure*. Recuperado de https://docs.microsoft.com/es-es/azure/storage/common/storage-service-encryption

[13] Microsoft Azure. (n.d.). *Azure Active Directory*. Recuperado de https://azure.microsoft.com/es-es/services/active-directory/

[14] Microsoft Azure. (n.d.). *Azure Monitor Logs*. Recuperado de https://docs.microsoft.com/es-es/azure/azure-monitor/logs/log-query-overview

[15] Microsoft Azure. (n.d.). *Azure ISO 27001*. Recuperado de https://www.microsoft.com/es-es/trustcenter/compliance/iso-iec-27001

[16] Microsoft Azure. (n.d.). *Azure NIST SP 800-53*. Recuperado de https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

[17] Microsoft Azure. (n.d.). *Cumplimiento GDPR en Azure*. Recuperado de https://www.microsoft.com/es-es/trustcenter/privacy/gdpr/solutions