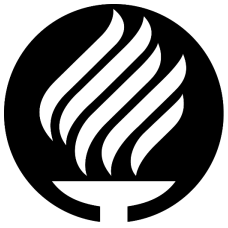

Tecnológico de Monterrey

CAMPUS MONTERREY

INTELIGENCIA ARTIFICIAL AVANZADA PARA LA CIENCIA DE DATOS II

TC3007C

Evidencia Portafolio

Modulo Cloud Computing

Prof. Félix Ricardo Botello

Lautaro Gabriel Coteja - A01571214

I. Introducción

En la actualidad, el almacenamiento y procesamiento de datos en la nube se ha convertido en una práctica esencial para empresas y organizaciones que buscan aprovechar la flexibilidad, escalabilidad y accesibilidad que ofrecen los proveedores de servicios en la nube. Sin embargo, esta transición hacia entornos digitales plantea desafíos significativos relacionados con la seguridad y el manejo ético de los datos.

Para garantizar la confidencialidad, integridad y disponibilidad de la información, es fundamental evaluar las prácticas de seguridad implementadas por los principales proveedores en la nube, como Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure. Estas prácticas deben estar alineadas con estándares reconocidos internacionalmente, como ISO/IEC 27001, NIST y GDPR, para asegurar el cumplimiento normativo y la protección adecuada de los datos sensibles.

El presente análisis tiene como objetivo comparar las prácticas de seguridad y confidencialidad de los principales proveedores de servicios en la nube, identificar herramientas clave que pueden ser adoptadas para fortalecer la protección de datos y establecer un procedimiento que garantice el manejo ético y seguro de la información. Esto permitirá a las organizaciones tomar decisiones informadas al seleccionar un proveedor y definir estrategias para gestionar los riesgos asociados al almacenamiento y procesamiento en la nube.

II. Desarrollo

Matriz Comparativa de Prácticas de Seguridad en la Nube

Proveedor	Cifrado de Datos	Control de Accesos	Auditorias	Autenticacion Multifactor (MFA)	Normas Cumplidas
AWS	Cifrado AES-256 en tránsito y en reposo	IAM para control granular basado en roles; principio de menor privilegio	AWS CloudTrail para registro de auditorías detallado	Compatible con MFA (hardware/software)	ISO/IEC 27001, NIST, GDPR
Google Cloud	Cifrado AES-256 en tránsito y en reposo	IAM con soporte para jerarquías y políticas específicas	Cloud Audit Logs para monitoreo de eventos	Soporte MFA con seguridad avanzada	ISO/IEC 27001, NIST, GDPR

Azure	Cifrado AES-256 en tránsito y en reposo	Azure AD para control de accesos con RBAC; privilegios mínimos	Azure Monitor Logs y Defender para auditorías	MFA integrado con autenticación biométrica	ISO/IEC 27001, NIST, GDPR

Selección de Prácticas y Herramientas de Seguridad

Herramientas Seleccionadas

AWS Key Management Service (KMS)

- Ventaja
  Permite administrar claves de cifrado de manera segura con rotación automática y control granular.

- Funcionamiento
  Cifra datos en reposo y en tránsito, integra servicios como S3 y DynamoDB.

Google Cloud IAM

- Ventaja
  Jerarquía clara de permisos para garantizar el acceso mínimo necesario.

- Funcionamiento
  Permite gestionar accesos por usuario, proyecto o recurso, con auditorías automáticas.

Azure Security Center

- Ventaja
  Monitoreo proactivo de amenazas y recomendaciones para mejorar la seguridad.

- Funcionamiento
  Escanea configuraciones y datos en tiempo real, emitiendo alertas en caso de vulnerabilidades.

AWS CloudTrail

- Ventaja
  Registro detallado de cada acción realizada en la nube.

- Funcionamiento
  Captura eventos de usuario, API y consola, facilitando auditorías y revisiones.

Google Cloud Audit Logs

- Ventaja
  Registra actividades de administración, acceso a datos y eventos del sistema.

- Funcionamiento
  Proporciona visibilidad completa de todas las acciones realizadas en la plataforma.

Procedimiento para el Manejo Seguro de Datos

Nombre del Procedimiento

- Gestión Ética y Segura de Datos en la Nube

Alcance

- Aplica a todas las operaciones relacionadas con el manejo de datos sensibles almacenados en plataformas de servicios en la nube.

Paso a Paso del Proceso

1. Evaluación Inicial de Permisos
2. Implementación de Medidas de Seguridad
3. Monitoreo y Auditoría
4. Actualizacion de Politicas
5. Revisión Periódica

Explicación del Paso a Paso del Proceso

1. Identificación de datos sensibles y establecimiento de acceso basado en principios de menor privilegio

2. Configuración de cifrado AES-256 en tránsito y reposo y activación MFA para todos los usuarios.

3. Uso de herramientas como AWS CloudTrail o Google Cloud Audit Logs, y detectar accesos sospechosos o no autorizados.

4. Revisar regularmente las políticas de acceso y asegurarse de que cumplan con normativas como GDPR.

5. Realizar auditorías mensuales y ajustar configuraciones basadas en cambios en el entorno o normativa.

Conclusión

La elección del proveedor de nube debe basarse en prácticas sólidas de seguridad, como el cifrado avanzado y políticas de control de acceso detalladas. La implementación de herramientas de monitoreo continuo, como AWS CloudTrail o Google Audit Logs, es crucial para detectar posibles amenazas. Establecer un procedimiento claro asegura el manejo ético y seguro de los datos, promoviendo la confidencialidad, integridad y disponibilidad. Finalmente, la revisión periódica y la alineación con normativas como ISO/IEC 27001 y GDPR fortalecen la seguridad y el cumplimiento regulatorio.

III. Referencias

- **Amazon Web Services (AWS):** Amazon Web Services. (n.d.). *Security in the cloud*. Retrieved from https://aws.amazon.com/security/
- **Google Cloud Platform (GCP):** Google Cloud. (n.d.). *Security overview*. Retrieved from https://cloud.google.com/security
- **Microsoft Azure:** Microsoft Azure. (n.d.). *Azure security*. Retrieved from https://azure.microsoft.com/en-us/solutions/security/