Oskar Arturo Gamboa Reyes
A01173648
26 de noviembre de 2024

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

Aspecto	**AWS**	**Google Cloud**	**Azure**
Confidencialidad	- Cifrado: Soporte para cifrado en tránsito y en reposo (AES-256).	- Cifrado: Protección por defecto en tránsito y reposo (TLS 1.3 y AES-256).	- Cifrado: Implementación de Azure Key Vault para manejar claves.
	- IAM avanzado: Roles detallados, políticas y uso de MFA.	- IAM centralizado: Google Workspace y Cloud IAM.	- IAM: Soporte con Azure AD, MFA y políticas condicionales.
	- Herramientas: AWS KMS y Amazon Macie para detección de datos sensibles.	- Herramientas: DLP para protección de datos confidenciales.	- Seguridad adicional: Microsoft Purview para privacidad de datos.
Integridad	- Verificación: Logs detallados con AWS CloudTrail.	- Verificación: Cloud Audit Logs para rastrear actividades.	- Verificación: Monitorización en tiempo real con Azure Monitor.
	- Monitorización: AWS Config para seguimiento de cambios.	- Monitorización: Herramientas como Security Command Center.	- Auditoría: Azure Security Center para alertas y análisis.
	- Cumplimiento: Firmas digitales para datos críticos.	- Cumplimiento: Alertas automatizadas por cambios no autorizados.	- Cumplimiento: Políticas automatizadas con Azure Policy.

Oskar Arturo Gamboa Reyes
A01173648
26 de noviembre de 2024

Disponibilidad	- Alta disponibilidad: Servicios redundantes en múltiples regiones.	- Alta disponibilidad: SLA de 99.95% en múltiples regiones.	- Alta disponibilidad: SLA del 99.95% con múltiples zonas.
	- Resiliencia: Disaster Recovery con AWS Backup.	- Resiliencia: Soluciones como Google Backup and DR.	- Resiliencia: Servicios integrados para recuperación ante desastres.
	- Escalabilidad: Autoscaling para manejar cargas variables.	- Escalabilidad: Implementación dinámica de recursos según demanda.	- Escalabilidad: Uso de Elastic Scaling en entornos dinámicos.
ISO/IEC 27001	Certificado para múltiples servicios globales.	Certificación ISO 27001 para todos los servicios principales.	Certificación ISO 27001 abarcando infraestructura global.
NIST (800-53, 800-171)	Cumple con los controles recomendados por NIST, aplicables a GovCloud y entornos comerciales.	Compatible con NIST SP 800-53 y NIST SP 800-171, incluyendo controles específicos en herramientas.	Cumple con NIST 800-53, alineado a los marcos CMMC y FedRAMP para seguridad gubernamental.
GDPR	Ofrece control granular para cumplir GDPR, con Data Processing Addendum (DPA).	Soluciones prediseñadas para el cumplimiento de GDPR con opciones avanzadas de portabilidad de datos.	Implementación de herramientas como Compliance Manager para evaluar y ajustar cumplimiento de GDPR.

Oskar Arturo Gamboa Reyes
A01173648
26 de noviembre de 2024

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

1. Cifrado avanzado de datos sensibles

Funcionamiento:
El cifrado protege los datos tanto en tránsito (TLS) como en reposo (AES-256), haciendo que la información sea ilegible para atacantes que logren acceder sin las claves adecuadas. Herramientas como AWS KMS, Google Cloud Key Management y Azure Key Vault facilitan la gestión centralizada de claves.

Ventaja:
Cumple con normativas como GDPR y protege contra el robo de datos, incluso si son interceptados.

2. Control de accesos basados en permisos y principios de mínimo privilegio

Funcionamiento:
Implementar IAM (Identity and Access Management) asegura que cada usuario o sistema solo tenga los permisos necesarios para realizar su trabajo. Soluciones como AWS IAM, Google Cloud IAM, y Azure AD permiten configurar roles específicos y autenticación multifactorial (MFA).

Ventaja:
Reduce el riesgo de accesos no autorizados y posibles abusos internos.

3. Registros de auditoría para monitorear y revisar accesos a los datos

Funcionamiento:
Los registros de auditoría como AWS CloudTrail, Google Cloud Audit Logs, y Azure Monitor Logs documentan cada acceso, cambio o actividad en los sistemas, proporcionando un historial detallado para análisis forense o cumplimiento regulatorio.

Ventaja:
Ayuda a detectar actividades sospechosas en tiempo real y respalda investigaciones de seguridad.

Oskar Arturo Gamboa Reyes
A01173648
26 de noviembre de 2024

4. Monitorización activa y detección de amenazas

Funcionamiento:
Servicios como AWS Config, Google Security Command Center y Azure Security Center ofrecen monitorización continua, detectando configuraciones inseguras o actividades anómalas y proporcionando alertas automáticas.

Ventaja:
Mejora la capacidad de respuesta frente a incidentes y previene vulnerabilidades antes de que sean explotadas.

5. Evaluación y cumplimiento normativo automatizado

Funcionamiento:
Herramientas como Azure Compliance Manager, AWS Artifact, y soluciones específicas de Google ayudan a mapear las configuraciones de la nube contra marcos normativos como ISO/IEC 27001 y GDPR. Estas herramientas automatizan las evaluaciones de cumplimiento, sugiriendo ajustes para cumplir con las regulaciones.

Ventaja:
Simplifica el cumplimiento legal y evita penalizaciones por incumplimiento.

3. Establecimiento de un Proceso o Estándar de Validación

Nombre del procedimiento: Evaluación y Validación Ética de Seguridad de Datos

Alcance: Este procedimiento se aplica a todas las instancias de almacenamiento, procesamiento y transmisión de datos en los servicios de nube utilizados por la organización. Está diseñado para garantizar el cumplimiento normativo (GDPR, ISO/IEC 27001) y los principios éticos de confidencialidad, integridad y disponibilidad de los datos.

1. Inicio

- Se activa el proceso de validación periódica, programado según el ciclo de auditorías internas (e.g., trimestralmente).

- Identifica responsables de seguridad y define áreas prioritarias.

2. Evaluación de permisos y accesos

- Revisión de las políticas de acceso implementadas en IAM (AWS, Google Cloud, Azure AD).
- Validación de que los usuarios y sistemas tengan mínimo privilegio necesario.
- Deshabilitación de accesos caducados o inactivos.

3. Monitoreo continuo de seguridad

- Uso de herramientas de auditoría para detectar y reportar accesos no autorizados.
- Configuración de alertas automáticas para eventos sospechosos (e.g., cambios en permisos críticos).

4. Revisión y actualización de políticas

- Ajuste de las políticas de acceso y uso según normativas vigentes (e.g., GDPR, ISO/IEC 27001).
- Revisión de roles y permisos por parte de responsables de cumplimiento.
- Comunicación de cambios al equipo autorizado.

5. Generación de reportes y auditorías

- Consolidación de logs de seguridad en reportes accesibles para auditorías internas y externas.
- Identificación de patrones recurrentes en accesos y uso de datos.
- Validación del cumplimiento normativo.

6. Cierre y seguimiento

- Implementación de correcciones detectadas durante la evaluación.
- Retroalimentación al equipo para mejorar futuras validaciones.
- Registro formal de la auditoría para referencia.

4. Conclusión

Oskar Arturo Gamboa Reyes
A01173648
26 de noviembre de 2024

Las herramientas y prácticas de seguridad en la nube son fundamentales para garantizar el manejo ético y seguro de los datos en cualquier entorno digitalizado. Tecnologías como el cifrado avanzado, los controles de acceso basados en principios de mínimo privilegio y los registros de auditoría permiten proteger la confidencialidad, integridad y disponibilidad de la información. Su implementación no solo asegura el cumplimiento de normativas internacionales, sino que también refuerza la confianza de los usuarios al demostrar un compromiso con la transparencia y la ética en la gestión de datos.

5. Referencias

- Amazon Web Services. (n.d.). *AWS Key Management Service Documentation*. Retrieved November 29, 2024, from https://aws.amazon.com/kms/
- Google. (n.d.). *Google Cloud Key Management Service (KMS)*. Retrieved November 29, 2024, from https://cloud.google.com/security-key-management
- Microsoft. (n.d.). *Azure Key Vault Documentation*. Retrieved November 29, 2024, from https://learn.microsoft.com/en-us/azure/key-vault/
- International Organization for Standardization. (n.d.). *ISO/IEC 27001 Information Security Management*. Retrieved November 29, 2024, from https://www.iso.org/isoiec-27001-information-security.html
- National Institute of Standards and Technology (NIST). (n.d.). *Cybersecurity Framework*. Retrieved November 29, 2024, from https://www.nist.gov/cyberframework
- European Data Protection Board. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved November 29, 2024, from https://gdpr-info.eu/
- Cloud Security Alliance. (n.d.). *Cloud Security Guidance*. Retrieved November 29, 2024, from https://cloudsecurityalliance.org/
- Microsoft. (n.d.). *Compliance Documentation*. Retrieved November 29, 2024, from https://learn.microsoft.com/en-us/compliance/