Evidencia final: Evaluación de prácticas de almacenamiento y procesamiento en la nube

Trabajo realizado por:

Rogelio Lizárraga Escobar

Cómputo en la nube

Profesor: Félix Ricardo Botello Urrutia

27 de noviembre de 2024

Instituto Tecnológico y de Estudios Superiores de Monterrey
Monterrey, Nuevo León

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

En el trabajo posterior, se presenta un análisis detallado de las prácticas de almacenamiento y procesamiento en la nube de los principales proveedores de servicios: Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure. La evaluación se centra en características de seguridad esenciales, como el cifrado de datos en tránsito y en reposo, así como prácticas de confidencialidad relacionadas con control de accesos, auditorías y autenticación multifactor.

Amazon Web Services (AWS)

Características de seguridad:

- **Cifrado de datos en tránsito:** AWS utiliza el protocolo TLS 1.2 para garantizar la protección de los datos que se transfieren entre sus servicios y los usuarios [1].
- **Cifrado de datos en reposo:** Emplea cifrado avanzado AES-256 en servicios como Amazon S3, RDS y DynamoDB. Las claves de cifrado se gestionan de forma centralizada a través de AWS Key Management Service (KMS), garantizando una gestión segura y eficiente [2].

Prácticas de confidencialidad:

- **Control de acceso:** AWS implementa Amazon Identity and Access Management (IAM), un sistema robusto que permite asignar permisos precisos basados en roles y políticas, alineado con el principio de menor privilegio [3].
- **Auditorías de acceso:** AWS CloudTrail registra todas las acciones realizadas sobre los servicios, facilitando auditorías y la identificación de accesos no autorizados [4].
- **Autenticación multifactor:** La autenticación multifactor (MFA) puede activarse para todas las cuentas de usuario y accesos administrativos, proporcionando una capa adicional de seguridad frente a intentos de acceso no autorizados [1].

Google Cloud Platform (GCP)

Características de seguridad:

- **Cifrado de datos en tránsito:** GCP garantiza la seguridad en la transferencia de datos mediante el uso del protocolo TLS 1.3, el cual ofrece una mayor rapidez y robustez frente a ataques [5].
- **Cifrado de datos en reposo:** Todos los datos almacenados en GCP están cifrados automáticamente con AES-256. La gestión de claves se realiza a través de Google Cloud Key Management, que asegura un control eficiente y seguro [6].

Prácticas de confidencialidad:

- **Control de acceso:** GCP emplea Cloud Identity and Access Management (IAM), que aplica estrictamente el principio de menor privilegio, limitando los permisos a lo estrictamente necesario [7].
- **Auditorías de acceso:** Las actividades realizadas en los servicios de GCP son monitoreadas mediante Cloud Audit Logs, lo que permite un rastreo exhaustivo para identificar posibles irregularidades [8].
- **Autenticación multifactor:** GCP es compatible con sistemas de autenticación multifactor (MFA), añadiendo un nivel adicional de seguridad para los accesos sensibles [5].

Microsoft Azure

Características de seguridad:

- **Cifrado de datos en tránsito:** Azure emplea el protocolo TLS 1.2 para garantizar que todas las conexiones entre usuarios y servicios estén protegidas contra intercepciones [9].
- **Cifrado de datos en reposo:** Los datos almacenados en Azure se protegen mediante cifrado AES-256, con claves gestionadas a través de Azure Key Vault, lo que asegura una administración confiable [10].

Prácticas de confidencialidad:

- **Control de acceso:** Azure utiliza Role-Based Access Control (RBAC) para implementar permisos detallados según roles, promoviendo un control de acceso eficiente [11].
- **Auditorías de acceso:** Las actividades y accesos a los servicios son supervisados mediante Azure Monitor y Log Analytics, herramientas avanzadas que permiten detectar posibles anomalías [12].
- **Autenticación multifactor:** Azure integra su autenticación multifactor (MFA) con Azure Active Directory, fortaleciendo los accesos administrativos y reduciendo riesgos [9].

Matriz Comparativa de Prácticas en Relación con Principios Éticos y Normas

Proveedor	Confidencialidad	Integridad	Disponibilidad
AWS	- Control de acceso mediante AWS IAM. - Uso de autenticación multifactor (MFA). - Auditorías con AWS CloudTrail.	- Cifrado avanzado (AES-256) para datos en reposo. - TLS 1.2 para datos en tránsito.	- Múltiples zonas de disponibilidad. - Balanceo de carga y replicación. - Recuperación ante desastres.
Google Cloud	- Control de acceso granular con Cloud IAM. - Auditorías con Cloud Audit Logs. - Autenticación multifactor (MFA).	- Cifrado automático AES-256 en reposo. - TLS 1.3 para datos en tránsito.	- Balanceo de carga global. - Replicación geográfica. - Alta disponibilidad garantizada por SLA.
Microsoft Azure	- Gestión de permisos con RBAC. - Integración con Azure Active Directory para MFA. - Auditorías con Azure Monitor.	- Cifrado AES-256 en reposo con Azure Key Vault. - TLS 1.2 para datos en tránsito.	- Réplica geográfica de datos. - Balanceo de carga global. - Recuperación ante desastres con Azure Backup.

Table 1: Prácticas de los principales proveedores clasificadas por principios éticos.

Cumplimiento de Normas Internacionales

Proveedor	Normas Cumplidas	Descripción del Cumplimiento
AWS	ISO/IEC 27001, NIST 800-53, GDPR	AWS cumple con los estándares internacionales de seguridad mediante auditorías periódicas y cumplimiento de marcos regulatorios.
Google Cloud	ISO/IEC 27001, ISO/IEC 27701, NIST 800-53, GDPR	GCP asegura conformidad con normativas internacionales a través de herramientas integradas para auditorías y gestión de datos.
Microsoft Azure	ISO/IEC 27001, NIST 800-53, GDPR	Azure se alinea con los principales estándares de seguridad mediante la implementación de herramientas avanzadas de control y cumplimiento.

Table 2: Cumplimiento de normas internacionales por proveedor.

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

Con base en la matriz comparativa, se seleccionaron las mejores prácticas y herramientas de seguridad de los principales proveedores de nube (AWS, Google Cloud, Azure) para garantizar la protección de los datos. Estas herramientas se enfocan en cifrado avanzado, control de acceso y auditorías, fundamentales para asegurar la confidencialidad, integridad y disponibilidad de la información.

Prácticas Seleccionadas

1. **Cifrado avanzado de datos sensibles:** Todas las plataformas seleccionadas utilizan cifrado AES-256 para datos en reposo y protocolos TLS para datos en tránsito, asegurando protección frente a accesos no autorizados.

2. **Control de accesos basados en permisos y principios de menor privilegio:** Herramientas como AWS IAM, Cloud IAM de Google, y RBAC de Azure permiten configurar permisos específicos basados en roles, limitando los accesos al mínimo necesario.

3. **Registros de auditoría:** Plataformas como AWS CloudTrail, Cloud Audit Logs y Azure Monitor facilitan el monitoreo y la revisión de actividades, garantizando trazabilidad y cumplimiento normativo.

Herramientas Seleccionadas y su Descripción

De esta manera, se seleecionarion cinco herramientas y componentes de los proveedores, con base en su funcionamiento y las ventajas que estos proporcionaron:

1. **AWS Identity and Access Management (IAM):**
   - **Función:** Gestiona accesos a los servicios y recursos de AWS mediante permisos específicos asignados a usuarios, roles o grupos.
   - **Ventajas:**
     - Implementa el principio de menor privilegio.
     - Soporta autenticación multifactor (MFA) para mayor seguridad.
     - Escalable para grandes organizaciones con múltiples usuarios y servicios.
2. **Google Cloud Key Management Service (KMS):**
   - **Función:** Permite generar, gestionar y rotar claves criptográficas para cifrar datos almacenados en los servicios de GCP.
   - **Ventajas:**
     - Integración nativa con servicios como Cloud Storage y BigQuery.
     - Simplifica el cumplimiento de regulaciones como GDPR al ofrecer un control total de claves.
3. **Azure Role-Based Access Control (RBAC):**
   - **Función:** Asigna permisos basados en roles a usuarios, grupos y aplicaciones para gestionar recursos de Azure.
   - **Ventajas:**
     - Alta granularidad en la configuración de permisos.
     - Integración con Azure Active Directory para autenticación centralizada.
     - Reducción de riesgos mediante el principio de menor privilegio.
4. **AWS CloudTrail:**
   - **Función:** Proporciona registros detallados de las acciones realizadas sobre los servicios de AWS.
   - **Ventajas:**
     - Facilita auditorías y cumplimiento de normativas como ISO/IEC 27001.
     - Detecta actividades sospechosas mediante análisis de registros.
5. **Azure Key Vault:**
   - **Función:** Almacena y gestiona claves de cifrado, certificados y secretos utilizados en aplicaciones y servicios.

- **Ventajas:**
  - Protección avanzada de claves mediante módulos de seguridad de hardware (HSM).
  - Integración con otros servicios de Azure para automatizar el cifrado.
  - Mejora la seguridad al centralizar la gestión de secretos y credenciales.

3. Establecimiento de un Proceso o Estándar de Validación

Para garantizar el manejo ético y seguro de los datos en la nube, se propone un proceso de validación basado en evaluaciones periódicas, monitoreo continuo y revisiones de políticas. Este proceso asegura el cumplimiento de normativas como ISO/IEC 27001, NIST y GDPR, alineándose con los principios de confidencialidad, integridad y disponibilidad.

Este proceso de validación tiene como objetivo asegurarse que los datos almacenados y procesados en la nube sean gestionados de forma ética y segura, limitando los accesos a personal autorizado y garantizando la conformidad con la normativa vigente.

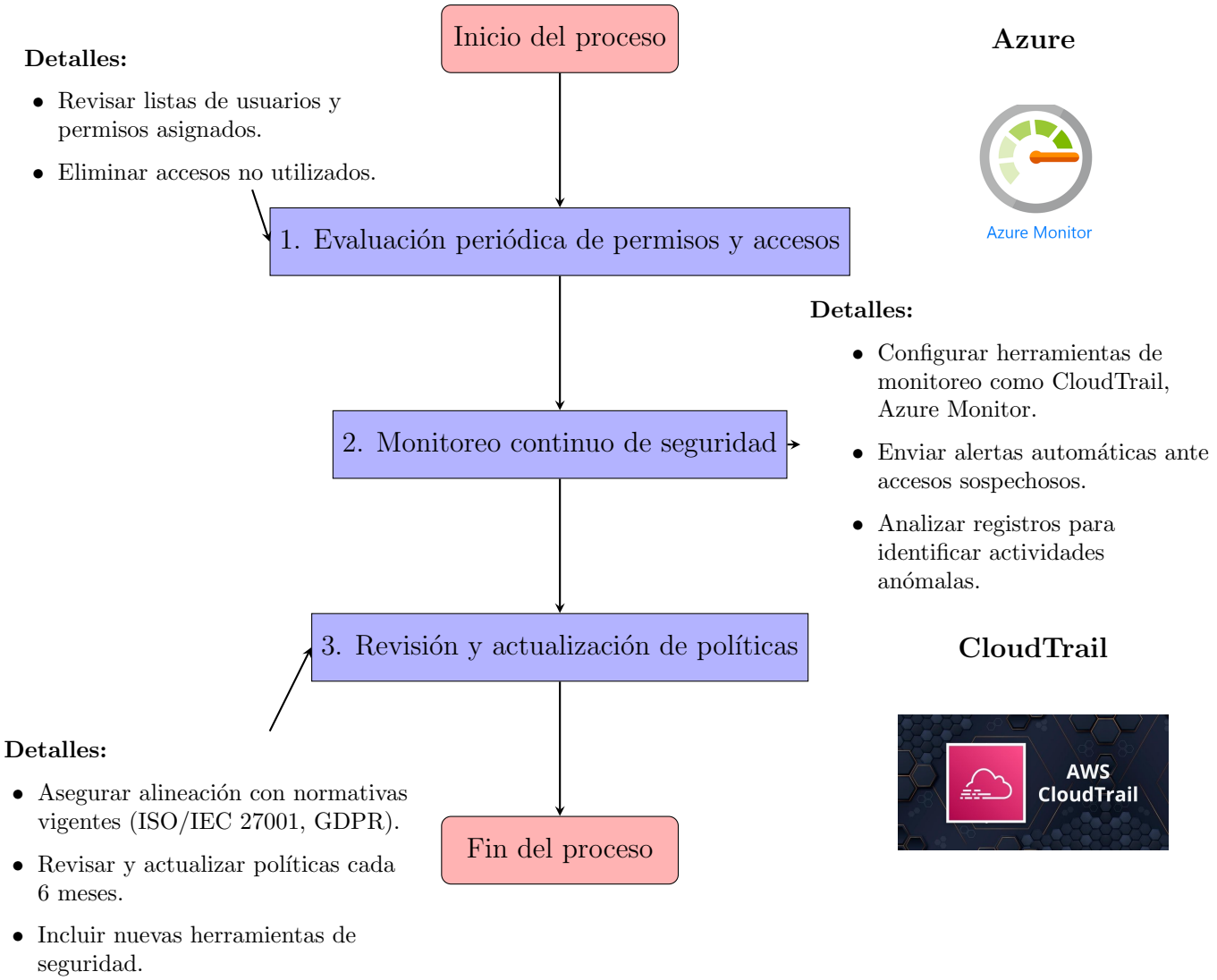
Además, este proceso es aplicable a todas las áreas de la organización que gestionen datos sensibles almacenados en servicios en la nube, incluyendo la evaluación de accesos, la implementación de auditorías y la actualización constante de políticas de seguridad.

Pasos del Proceso de Validación

1. **Evaluación periódica de permisos y accesos:**
   - Realizar revisiones trimestrales de las listas de usuarios con acceso a los servicios en la nube.
   - Validar que los permisos asignados correspondan a las responsabilidades actuales de los usuarios.
   - Revocar accesos innecesarios o inactivos para minimizar riesgos.
2. **Monitoreo continuo de la seguridad:**
   - Implementar herramientas como AWS CloudTrail, Google Cloud Audit Logs o Azure Monitor para registrar y supervisar las actividades en tiempo real.
   - Generar reportes semanales sobre accesos y actividades inusuales.
   - Configurar alertas automáticas para identificar actividades sospechosas o no autorizadas.
3. **Revisión y actualización de políticas de acceso y uso de datos:**
   - Revisar semestralmente las políticas de acceso, asegurando que estén alineadas con las mejores prácticas y normativas vigentes.

- Actualizar las políticas para incluir nuevas tecnologías, herramientas o cambios en la estructura organizacional.
- Implementar controles adicionales como autenticación multifactor (MFA) para accesos administrativos.

Diagrama del Proceso



Conclusiones

- **Relevancia del cumplimiento normativo:** La alineación con estándares internacionales como ISO/IEC 27001 y GDPR no solo protege los datos, sino que fortalece la credibilidad de las organizaciones frente a clientes y reguladores.
- **Importancia del enfoque integral en seguridad:** La combinación de herramientas avanzadas, como AWS IAM, Azure RBAC y Google Cloud KMS, demuestra que la seguridad efectiva requiere implementar controles específicos para confidencialidad, integridad y disponibilidad.
- **Eficiencia del proceso propuesto:** La validación periódica de accesos, junto con el monitoreo continuo, asegura que los sistemas se mantengan seguros y actualizados frente a amenazas emergentes.
- **Mejora en la resiliencia organizacional:** El diseño e implementación de un proceso estructurado para la gestión de datos en la nube permite a las empresas responder proactivamente ante riesgos, garantizando una operación confiable y ética.

Referencias

[1] Amazon Web Services. (n.d.). *AWS Security Overview*. Recuperado de `https://aws.amazon.com/security/`.

[2] Amazon Web Services. (n.d.). *AWS Key Management Service*. Recuperado de `https://aws.amazon.com/kms/`.

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

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

[5] Google Cloud. (n.d.). *Google Cloud Security*. Recuperado de `https://cloud.google.com/security`.

[6] Google Cloud. (n.d.). *Google Cloud Key Management*. Recuperado de `https://cloud.google.com/kms/`.

[7] Google Cloud. (n.d.). *Cloud IAM Overview*. Recuperado de `https://cloud.google.com/iam`.

[8] Google Cloud. (n.d.). *Cloud Audit Logs*. Recuperado de `https://cloud.google.com/logging/audit`.

[9] Microsoft Azure. (n.d.). *Azure Security Overview*. Recuperado de `https://azure.microsoft.com/en-us/overview/security/`.

[10] Microsoft Azure. (n.d.). *Azure Key Vault*. Recuperado de `https://azure.microsoft.com/en-us/services/key-vault/`.

[11] Microsoft Azure. (n.d.). *Role-Based Access Control*. Recuperado de `https://learn.microsoft.com/en-us/azure/role-based-access-control/`.

[12] Microsoft Azure. (n.d.). *Azure Monitor*. Recuperado de `https://azure.microsoft.com/en-us/services/monitor/`.