Evidencia Portafolio - Cloud Computing

Daniela Jiménez Téllez A01654798

1 Evaluación de Prácticas de Almacenamiento y Procesamiento en la Nube

1.1 Características de Seguridad

- **AWS**: Ofrece cifrado de datos en tránsito y en reposo. Utiliza servicios como AWS Key Management Service (KMS) para la gestión de claves y soporta protocolos de seguridad estándar para la protección de datos.
- **Google Cloud**: Implementa cifrado de datos en tránsito y en reposo de forma predeterminada. Utiliza Google Cloud Key Management Service para la gestión de claves y emplea protocolos de seguridad avanzados.
- **Azure**: Proporciona cifrado de datos en tránsito y en reposo. Utiliza Azure Key Vault para la gestión de claves y soporta una variedad de protocolos de seguridad para proteger los datos.

1.2 Prácticas de Confidencialidad

- **AWS**: Implementa políticas de acceso basadas en permisos a través de AWS Identity and Access Management (IAM), auditorías de acceso y autenticación multifactor (MFA) para reforzar la seguridad.
- **Google Cloud**: Utiliza Google Cloud IAM para gestionar permisos, realiza auditorías de acceso y ofrece autenticación multifactor para proteger los recursos.
- **Azure**: Emplea Azure Active Directory para la gestión de identidades y accesos, realiza auditorías de acceso y soporta autenticación multifactor para garantizar la seguridad.

1.3 Matriz Comparativa

Aspecto	AWS	Google Cloud	Azure
Confidencialidad	• Cifrado AES-256 en reposo y TLS en tránsito. • Políticas de acceso detalladas con AWS IAM. • Autenticación multifactor (MFA) opcional.	• Cifrado AES-256 por defecto y TLS 1.3 en tránsito. • IAM con roles personalizables y políticas. • MFA con claves de hardware y software.	• Cifrado AES-256 en reposo y en tránsito. • Gestión de accesos con Azure Active Directory. • MFA integrada con aplicaciones de Microsoft.

Integridad	• Auditorías de acceso con AWS CloudTrail. • Supervisión constante y alertas.	• Registro y monitoreo con Cloud Logging. • Auditorías en tiempo real.	• Monitoreo con Azure Monitor. • Auditorías automáticas con Security Center.
Disponibilidad	• Infraestructura escalable y redundante. • Recuperación ante desastres integrada.	• Alta disponibilidad global con servicios redundantes. • Recuperación rápida y eficiente.	• Recuperación de desastres integrada. • Alta disponibilidad en todas las regiones.
Cumplimiento Normativo	• ISO/IEC 27001, GDPR, NIST 800-53, PCI DSS, HIPAA. • Recursos para el cumplimiento normativo.	• ISO/IEC 27001, GDPR, NIST 800-53, PCI DSS. • Mapas de cumplimiento detallados.	• ISO/IEC 27001, GDPR, NIST 800-53, PCI DSS. • Herramientas avanzadas de cumplimiento.

2 Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

En esta sección se presentan las mejores prácticas seleccionadas de la matriz comparativa para proteger los datos en la nube:

1. Cifrado avanzado de datos sensibles: Implementar cifrado avanzado, como AES-256, para proteger datos sensibles tanto en reposo como en tránsito. Esto asegura que los datos estén seguros frente a accesos no autorizados incluso si se interceptan.

2. Control de acceso basado en permisos y principio de mínimo privilegio: Configurar políticas detalladas de acceso utilizando herramientas como AWS IAM, Google Cloud IAM o Azure Active Directory, asegurando que los usuarios solo tengan los permisos estrictamente necesarios para sus tareas.

3. Registros de auditoría y monitoreo constante: Utilizar registros de auditoría, como AWS CloudTrail, Google Cloud Logging y Azure Monitor, para supervisar los accesos y detectar actividades sospechosas. Esto permite identificar y mitigar riesgos de seguridad.

4. Autenticación multifactor (MFA): Habilitar MFA para agregar una capa adicional de seguridad en la autenticación de usuarios, protegiendo contra accesos no autorizados incluso si se comprometen las credenciales.

5. Infraestructura escalable y redundante: Garantizar alta disponibilidad y recuperación ante desastres mediante arquitecturas redundantes proporcionadas por los principales proveedores de nube.

2.1 Herramientas y Componentes de los Proveedores

Habiendo dicho lo anterior, se describen cinco herramientas clave de los principales proveedores de servicios en la nube y sus ventajas:

1. AWS Key Management Service (KMS): KMS permite administrar claves criptográficas para cifrar datos. Ofrece escalabilidad, integración con otros servicios de AWS y soporte para cifrado transparente. Ideal para proteger datos sensibles de manera centralizada.

2. Google Cloud IAM: IAM ofrece control detallado de los accesos a recursos, permitiendo asignar permisos personalizados según lo que necesiten. Es esencial para implementar el principio de mínimo privilegio y proteger recursos críticos.

3. Azure Security Center: Esta herramienta proporciona visibilidad centralizada, detección de amenazas y recomendaciones de seguridad. Además, permite la integración con otras soluciones de seguridad para proteger cargas de trabajo en la nube.

4. AWS CloudTrail: CloudTrail registra acciones realizadas en la cuenta de AWS, lo que permite monitorear y auditar actividades de acceso. Es útil para cumplir con requisitos normativos y detectar anomalías.

5. Google Cloud Logging: Esta herramienta recopila y analiza registros de actividad en tiempo real, ofreciendo un monitoreo detallado para detectar amenazas y garantizar la integridad de los sistemas.

3 Establecimiento de un Proceso o Estándar de Validación

Para garantizar el manejo ético y seguro de los datos, se necesita un proceso de validación que aborde tres áreas clave: la evaluación periódica de permisos, el monitoreo continuo de la seguridad y la actualización de políticas de acceso. A continuación se muestra el proceso:

3.1 Evaluación periódica de permisos y accesos

Revisar configuraciones de acceso para garantizar:

- Solo usuarios autorizados acceden a datos sensibles.
- Aplicación del principio de mínimo privilegio.
- Eliminación de permisos temporales al vencimiento.

Frecuencia: Trimestral o tras cambios en roles.

3.2 Monitoreo continuo de la seguridad

Implementar monitoreo con herramientas como AWS CloudTrail, Google Cloud Logging o Azure Monitor para:

- Registrar y auditar accesos.
- Generar alertas ante intentos no autorizados.
- Supervisar actividades sospechosas en tiempo real.

3.3 Revisión y actualización de políticas de acceso y uso de datos

Asegurar que las políticas de acceso:

- Estén alineadas con normativas como ISO/IEC 27001 y GDPR.
- Reflejen cambios organizacionales o regulatorios.
- Garanticen que solo personal autorizado pueda acceder a los datos sensibles.

Frecuencia: Anual o al introducir nuevos servicios en la nube.

4 Conclusiones

En conclusión, los resultados de la actividad reflejan un análisis sólido de las prácticas de seguridad y herramientas más relevantes ofrecidas por AWS, Google Cloud y Azure. Se pudo observar cómo estas plataformas cumplen con principios éticos como la confidencialidad, integridad y disponibilidad, además de alinearse con normativas internacionales como ISO/IEC 27001, NIST y GDPR. La matriz comparativa permitió identificar las mejores opciones en términos de cifrado avanzado, control de accesos y monitoreo continuo, destacando el potencial de herramientas específicas como AWS CloudTrail, Google Cloud Logging y Azure Monitor.

Además, al definir un proceso de validación, se establecieron pasos claros y estratégicos para garantizar la seguridad de los datos en la nube, desde auditorías periódicas hasta la actualización de políticas de acceso. Este enfoque no solo mejora la gestión de la seguridad, sino que también asegura el cumplimiento normativo. Creo que esta actividad resalta la importancia de implementar prácticas sólidas y herramientas específicas para proteger los datos, y los resultados obtenidos proporcionan una base práctica y estructurada para futuros proyectos relacionados con la seguridad en la nube.

Referencias

1. Amazon Web Services. (n.d.). *AWS Key Management Service (KMS)*. Recuperado de `https://aws.amazon.com/kms/`
2. Amazon Web Services. (n.d.). *AWS CloudTrail*. Recuperado de `https://aws.amazon.com/cloudtrail/`
3. Google Cloud. (n.d.). *Cloud Identity and Access Management (IAM)*. Recuperado de `https://cloud.google.com/iam`
4. Google Cloud. (n.d.). *Cloud Logging*. Recuperado de `https://cloud.google.com/logging`
5. Microsoft Azure. (n.d.). *Azure Active Directory*. Recuperado de `https://azure.microsoft.com/en-us/services/active-directory/`
6. Microsoft Azure. (n.d.). *Azure Security Center*. Recuperado de `https://azure.microsoft.com/en-us/services/security-center/`
7. International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Recuperado de `https://www.iso.org/standard/54534.html`
8. National Institute of Standards and Technology. (2013). *NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations*. Recuperado de `https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final`
9. The European Parliament and the Council of the European Union. (2016). *General Data Protection Regulation (GDPR)*. Recuperado de `https://gdpr-info.eu/`