Erika Martínez Meneses A01028621

Evidencia Portafolio - Módulo cloud computing

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

Investigación de Proveedores

Aspecto	AWS	Google Cloud	Microsoft Azure
Cifrado de datos	- Cifrado en tránsito con TLS. - Cifrado en reposo con AES-256. - Customer Key Management Service (KMS).	- TLS en tránsito. - AES-256 en reposo. - Cloud KMS para claves.	- TLS 1.2 en tránsito. - Cifrado AES-256 en reposo. - Azure Key Vault para gestión de claves.
Gestión de accesos	- IAM con políticas detalladas. - Autenticación multifactor (MFA). - Auditorías con AWS CloudTrail.	- IAM con roles y políticas detalladas. - MFA integrado. - Registros con Cloud Audit Logs.	- IAM y control detallado. - MFA mediante Azure AD. - Azure Monitor y Security Center para auditorías.
Monitoreo y Auditorías	AWS CloudTrail para auditorías; alertas automáticas.	Cloud Audit Logs para trazabilidad de eventos.	Azure Monitor y Security Center para monitoreo proactivo.
Cumplimiento normativo	ISO/IEC 27001, NIST, GDPR, HIPAA.	ISO/IEC 27001, NIST, GDPR, HIPAA.	ISO/IEC 27001, NIST, GDPR, HIPAA.

Matriz Comparativa: Principios Éticos y Normas

Proveedor	Confidencialidad	Integridad	Disponibilidad
AWS	IAM con políticas detalladas, MFA, Auditorías con AWS CloudTrail.	Verificación de integridad de datos con S3. Logging detallado con AWS CloudTrail.	SLA 99.99%, recuperación con AWS Backup.
Google Cloud	IAM con roles y políticas detalladas, MFA, Registros con Cloud Audit Logs.	Validación de integridad en Cloud Storage. Monitoreo constante con Cloud Operations.	SLA 99.95%, recuperación con Cloud Storage Archive.
Azure	IAM y control detallado, MFA con Azure AD, Azure Monitor y Security Center para auditorías.	Validación de integridad con Azure Blob Storage. Auditorías con Log Analytics.	SLA 99.99%, recuperación con Azure Backup.

Normas cumplidas desglose.

Proveedor	ISO/IEC 27001	NIST	GDPR	HIPAA
AWS	Certificación obtenida para varios de sus servicios.	Cumple con el marco NIST 800-53 y proporciona herramientas para alinearse con NIST CSF.	Ofrece funcionalidades específicas para el cumplimiento de GDPR, como cifrado, controles de acceso y AWS Artifact para informes de cumplimiento.	Certificado como apto para soluciones sujetas a HIPAA, con acuerdos de asociado comercial (BAA) disponibles.
Google Cloud	Certificado para servicios como Compute Engine, BigQuery y Cloud Storage.	Compatible con los controles de NIST SP 800-53 y NIST CSF para seguridad y privacidad.	Funciones diseñadas para la portabilidad y seguridad de datos según los requisitos de GDPR.	Certificación para servicios como GCP y Google Workspace, con soporte para cargas de trabajo sujetas a HIPAA.
Azure	Certificación que abarca múltiples servicios y centros de datos.	Compatible con los controles de NIST SP 800-53 y NIST CSF.	Proporciona herramientas específicas, como Azure Policy y Compliance Manager, para cumplir con GDPR.	Compatible con HIPAA para aplicaciones y datos relacionados con la salud, incluyendo acuerdos BAA.

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

Prácticas Seleccionadas:

A. Cifrado avanzado de datos sensibles

El cifrado asegura que los datos sean ilegibles para personas no autorizadas, tanto en tránsito como en reposo. Se implementa utilizando algoritmos robustos como **AES-256** o mediante hardware de seguridad (HSM).

Ventajas:

- Proporciona protección efectiva contra accesos no autorizados incluso si los datos son interceptados.
- Compatible con normativas como GDPR e HIPAA.

Ejemplo: Empresas del sector salud pueden cifrar datos de pacientes para cumplir con HIPAA, evitando violaciones de datos al transmitir información entre sistemas internos y externos.

B. Control de Accesos Basados en Permisos y Principios de Mínimo Privilegio

Limitar los accesos según roles y funciones específicas asegura que los empleados solo tengan acceso a los recursos necesarios para su trabajo.

Ventajas:

- Reduce riesgos al minimizar la exposición a datos sensibles.
- Ofrece trazabilidad detallada de las acciones realizadas por cada usuario.

Ejemplo: En un equipo de desarrollo, solo los líderes de proyecto pueden tener acceso a configuraciones críticas en el servidor, mientras que los desarrolladores tienen acceso restringido a sus áreas de trabajo específicas.

C. Registros de Auditoría para Monitorear y Revisar Accesos

Los registros de auditoría permiten monitorear quién accede a los recursos, cuándo lo hace y qué acciones realiza.

Ventajas:

- Identifica posibles amenazas internas o externas.
- Facilita cumplir con normativas que requieren trazabilidad, como ISO/IEC 27001.

Ejemplo: Una auditoría podría identificar accesos no autorizados a datos financieros y ayudar a prevenir violaciones futuras ajustando políticas de acceso.

D. Evaluaciones Periódicas de Seguridad

La revisión continua de permisos, configuraciones y políticas asegura que los sistemas se mantengan actualizados frente a amenazas emergentes.

Ventajas:

- Detecta configuraciones obsoletas o vulnerables.
- Garantiza el cumplimiento constante con regulaciones actualizadas.

Ejemplo: Una evaluación trimestral podría revelar que un conjunto de claves API antiguas sigue habilitado, mitigando riesgos de seguridad al deshabilitarlas.

E. Autenticación multifactor (MFA)

Requiere múltiples métodos de verificación, como contraseñas y dispositivos móviles, para acceder a sistemas o recursos. Para reforzar la seguridad de acceso.

Ventajas:

- Mejora significativamente la seguridad frente a intentos de acceso no autorizado.
- Aumenta la confianza en el manejo de datos críticos.

Ejemplo: En una organización financiera, el acceso al sistema de gestión de clientes está protegido por contraseñas y códigos generados por aplicaciones de autenticación.

F. Cumplimiento normativo

Garantizar que los servicios y políticas de seguridad cumplan con estándares internacionales y regulaciones locales como ISO/IEC 27001, GDPR, NIST, y HIPAA. Este cumplimiento asegura que los datos sean tratados de manera ética y que las operaciones en la nube se adhieran a requisitos legales.

Ventajas:

- Aumenta la confianza de los clientes y partes interesadas al demostrar un compromiso con la seguridad y privacidad de los datos.
- Reduce el riesgo de sanciones legales y costos asociados a violaciones regulatorias.
- Proporciona un marco claro para implementar políticas de seguridad coherentes y efectivas.

Ejemplo: Una empresa que maneja datos personales de clientes en Europa debe cumplir con el GDPR. Esto incluye proporcionar transparencia sobre cómo se recopilan, almacenan y procesan los datos, además de implementar el "derecho al olvido" para eliminar los datos cuando sea solicitado.

Herramientas Seleccionadas:

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

Ventajas**:**

- Gestión avanzada de claves con soporte para BYOK (Bring Your Own Key).
- Permite el cifrado avanzado de datos en tránsito y en reposo, gestionando claves de manera centralizada.
- Compatible con una amplia gama de servicios como S3, RDS y Lambda.
- Cumple con normativas como GDPR, NIST, e ISO/IEC 27001.

Uso**:** AWS KMS facilita la creación y rotación de claves de cifrado, permitiendo a los usuarios establecer permisos detallados sobre quién puede usar o gestionar

dichas claves. Esto es especialmente útil para datos sensibles almacenados en AWS, como registros financieros o personales.

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

Ventajas**:**

- Control granular de permisos basado en principios de acceso mínimo.
- Ofrece control detallado de acceso a recursos con políticas basadas en roles.
- Integración con herramientas como Google Workspace para una administración centralizada.
- Implementa autenticación multifactor (MFA) para acceso seguro.

Uso**:** IAM de Google Cloud es ideal para empresas con equipos grandes, ya que permite asignar permisos específicos basados en roles. Por ejemplo, un administrador de red puede limitar el acceso de un equipo a una base de datos mientras permite acceso completo a otro equipo.

3. **Azure Security Center:**

Ventajas**:**

- Proporciona análisis en tiempo real para detectar vulnerabilidades.
- Integra alertas de seguridad con recomendaciones automáticas de mitigación.
- Compatible con entornos híbridos y multi-nube.

Uso**:** Ideal para monitorear configuraciones de seguridad y proteger contra amenazas. Por ejemplo, un usuario puede recibir alertas sobre configuraciones incorrectas en máquinas virtuales y solucionarlas directamente desde el panel de control.

4. **AWS CloudTrail:**

Ventajas:

- Registra automáticamente todas las acciones realizadas en la infraestructura.
- Facilita auditorías de cumplimiento y monitoreo continuo.
- Permite configuraciones personalizadas de almacenamiento de registros.

Uso**:** AWS CloudTrail es útil para detectar y responder a incidentes de seguridad. Por ejemplo, una organización puede rastrear si un usuario no autorizado intentó acceder a recursos sensibles y tomar medidas inmediatas.

5. **Azure Key Vault:**

Ventajas**:**

- Almacén seguro para certificados y claves de cifrado.
- Integra el manejo de claves con servicios de Google Cloud como BigQuery y Cloud Storage.
- Ofrece cifrado avanzado con soporte para hardware de seguridad (HSM).
- Incluye capacidades de auditoría para verificar el uso de claves.

Uso: Es perfecto para empresas que necesitan cifrar grandes volúmenes de datos, como bases de datos de clientes. Además, permite importar claves propias, lo que asegura una mayor personalización en entornos sensibles.

3. Establecimiento de un Proceso o Estándar de Validación

El proceso de validación asegura que el manejo de datos en la nube sea seguro, ético y conforme a regulaciones internacionales. Este proceso debe ser continuo y adaptativo, incorporando controles técnicos y operativos que refuercen la protección de los datos.

Proceso de Validación

1. Evaluación Periódica de Permisos y Accesos:

Acción: Revisar los permisos asignados a usuarios y roles en los sistemas de gestión de identidad (IAM) cada seis meses.

Objetivo: Garantizar que los usuarios solo tengan los accesos estrictamente necesarios para desempeñar sus funciones.

Proceso:

- Identificar usuarios o roles con permisos excesivos y reducir privilegios según el principio de mínimo privilegio.
- Eliminar accesos obsoletos de excolaboradores o roles ya no utilizados.

Ejemplo: En un entorno con datos financieros sensibles, los permisos de un analista de datos que cambió de puesto deberían revocarse para evitar acceso innecesario.

2. Monitoreo Continuo de Seguridad:

Acción: Utilizar herramientas como AWS CloudTrail, Google Cloud Logging, o Azure Monitor para rastrear actividad en la nube y detectar anomalías.

Objetivo: Identificar y mitigar accesos no autorizados o actividades sospechosas en tiempo real.

Proceso:

- Configurar alertas automáticas para eventos críticos como intentos fallidos de inicio de sesión o cambios en configuraciones sensibles.
- Generar reportes mensuales que detallen patrones de uso y anomalías.

Ejemplo: Si un usuario intenta acceder repetidamente a una base de datos sin autorización, la herramienta debe alertar al administrador y bloquear el acceso.

3. Revisión y Actualización de Políticas:

Acción: Realizar una revisión anual de las políticas de acceso y uso de datos, incorporando cambios en las regulaciones aplicables como GDPR o ISO/IEC 27001.

Objetivo: Mantener las políticas alineadas con estándares globales y actualizadas frente a nuevas amenazas.

Proceso

- Implementar autenticación multifactor (MFA) como requisito estándar para accesos a datos sensibles.
- Incorporar cifrado avanzado (ej., AES-256) para proteger datos críticos en reposo y en tránsito.
- Revisar los contratos con proveedores para garantizar que sigan cumpliendo con normativas aplicables.

Ejemplo: Actualizar políticas para incluir el cifrado de datos almacenados en servicios de almacenamiento en la nube, asegurando que solo dispositivos autorizados puedan descifrarlos.

Resultado

Este proceso permite:

- Un manejo ético y seguro de los datos al limitar accesos no autorizados y garantizar la trazabilidad de todas las acciones realizadas.
- Cumplir con principios de confidencialidad, integridad y disponibilidad, asegurando que los datos estén siempre protegidos contra riesgos internos y externos.

- Alinear las operaciones con normativas internacionales, reduciendo el riesgo de sanciones legales y fortaleciendo la confianza de los usuarios y clientes.

Conclusión

La evaluación y comparación de prácticas de almacenamiento y procesamiento en la nube de proveedores como AWS, Google Cloud y Azure revelan un compromiso significativo con la seguridad, confidencialidad e integridad de los datos. Cada proveedor ofrece herramientas avanzadas para cifrado, control de acceso y monitoreo continuo, cumpliendo estándares internacionales como ISO/IEC 27001, NIST y GDPR.

La implementación de mejores prácticas, como el cifrado avanzado, el control de acceso basado en permisos y auditorías regulares, asegura una protección robusta de los datos sensibles. Además, las herramientas seleccionadas, como AWS KMS, Google Cloud IAM y Azure Security Center, destacan por su eficacia en la gestión de claves, permisos y monitoreo en tiempo real.

Establecer un proceso continuo de evaluación y validación garantiza un manejo ético y seguro de los datos en la nube, fortaleciendo la confidencialidad, integridad y disponibilidad. Este enfoque permite a las organizaciones mitigar riesgos, cumplir con normativas y mantener la confianza de sus usuarios y clientes.

Referencias

Amazon Web Services. (n.d.). *Security, identity, & compliance*. Recuperado de https://aws.amazon.com/security

Google Cloud. (n.d.). *Security and compliance*. Recuperado de https://cloud.google.com/security

Microsoft Azure. (n.d.). *Azure compliance offerings*. Recuperado de https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance

European Parliament. (2016). *General Data Protection Regulation (GDPR)*. Official Journal of the European Union. Recuperado de https://gdpr-info.eu

National Institute of Standards and Technology. (2017). *NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations*. Recuperado de https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final