Tecnológico de Monterrey

CAMPUS MONTERREY

INTELIGENCIA ARTIFICIAL AVANZADA PARA LA CIENCIA DE DATOS II

TC3007C

Diseño de Arquitectura en la Nube

Cloud Computing

Evidencia Portafolio

Prof. Felix Ricardo Botello

Andrés Villareal González - A00833915

Evaluación de Prácticas de Almacenamiento y Procesamiento en la Nube

Proveedor	Cifrado de datos en tránsito	Cifrado de datos en reposo	Políticas de acceso basadas en permisos	Auditorías de acceso	Autenticación multifactor
AWS	TLS/SSL para datos en tránsito	Cifrado AES-256 para datos en reposo	IAM para gestión de permisos detallados	AWS CloudTrail para auditorías	Soporte para MFA
Azure	TLS/SSL para datos en tránsito	Cifrado AES-256 para datos en reposo	Azure RBAC para control de acceso	Azure Monitor y Log Analytics para auditorías	Soporte para MFA
GCP	TLS/SSL para datos en tránsito	Cifrado AES-256 para datos en reposo	IAM para gestión de permisos detallados	Cloud Audit Logs para auditorías	Soporte para MFA

Proveedor	Confidencialidad	Integridad	Disponibilidad	Cumplimiento ISO/IEC 27001	Cumplimiento NIST
AWS	Alta	Alta	Alta	Certificado	Cumple con NIST SP 800-53
Azure	Alta	Alta	Alta	Certificado	Cumple con NIST CSF
GCP	Alta	Alta	Alta	Certificado	Cumple con NIST SP 800-53

AWS, Azure y GCP ofrecen sólidas prácticas de seguridad y confidencialidad, implementando cifrado robusto, controles de acceso detallados, auditorías exhaustivas y autenticación multifactor. Además, cumplen con estándares internacionales como ISO/IEC 27001, NIST y GDPR, asegurando que sus servicios en la nube mantienen altos niveles de confidencialidad, integridad y disponibilidad de la información.

Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

Prácticas seleccionadas:

1. Cifrado avanzado de datos sensibles:
    - Utilizar cifrado AES-256 para datos en reposo.
    - Usar protocolos de transporte seguro (TLS/SSL) para proteger los datos en tránsito.

2. Control de acceso basado en permisos y principios de mínimo privilegio:
    - Configurar roles y permisos específicos para usuarios mediante Identity Access Management (IAM).

3. Registros de auditoría:
    - Implementar herramientas que monitoreen continuamente el acceso a datos, generen reportes y rastreen incidentes.

4. Autenticación multifactor (MFA):
    - Exigir MFA para añadir una capa adicional de seguridad al inicio de sesión.

5. Cumplimiento de normativas de seguridad (ISO/IEC 27001, GDPR):
    - Adoptar configuraciones y herramientas que permitan el cumplimiento automatizado de estándares internacionales.

Herramientas y Componentes Seleccionados

1. AWS Key Management Service (KMS)
    - Proveedor: AWS
    - Ventajas: Permite crear y controlar claves de cifrado para proteger datos en reposo y en tránsito. Se integra con otros servicios de AWS para proporcionar cifrado de extremo a extremo.
    - Funcionamiento: Genera, almacena y administra claves de cifrado; además, permite automatizar el ciclo de vida de estas claves.

2. Azure Role-Based Access Control (RBAC)
    - Proveedor: Azure
    - Ventajas: Facilita la gestión granular de permisos al asignar roles específicos a usuarios o grupos, siguiendo el principio de mínimo privilegio.
    - Funcionamiento: Permite definir roles personalizados que se adaptan a las necesidades específicas de acceso a los datos y recursos en la nube.

3. Google Cloud Audit Logs
    - Proveedor: Google Cloud Platform
    - Ventajas: Ofrece auditorías exhaustivas para rastrear actividades de acceso y cambios en los recursos, lo que ayuda en el cumplimiento normativo y la detección de amenazas.
    - Funcionamiento: Registra eventos administrativos, de acceso a datos y de eventos del sistema, lo que proporciona un historial detallado para la revisión.

4. AWS Identity and Access Management (IAM)
    - Proveedor: AWS
    - Ventajas: Administra de forma centralizada quién tiene acceso a qué recursos y bajo qué condiciones. Incluye opciones como autenticación basada en políticas y atributos.
    - Funcionamiento: Crea políticas detalladas para restringir el acceso según roles, IP, tiempo, o incluso atributos específicos de usuario.

5. Azure Security Center
    - Proveedor: Azure
    - Ventajas: Proporciona análisis continuo y recomendaciones de seguridad. Permite monitorear vulnerabilidades y activar soluciones para mantener el cumplimiento normativo.
    - Funcionamiento: Usa inteligencia artificial para evaluar configuraciones y detectar posibles amenazas en la infraestructura de la nube

Establecimiento de un Proceso o Estándar de Validación

Nombre del Procedimiento:

Proceso de Validación de Seguridad y Ética en el Manejo de Datos

Alcance:
Este procedimiento aplica a todos los sistemas y datos almacenados o procesados en la nube por la organización. Cubre a empleados, contratistas y terceros con acceso autorizado, asegurando la confidencialidad, integridad y disponibilidad de los datos según estándares como ISO/IEC 27001, GDPR y NIST.

Diagrama del proceso:

Inicio
↓
Evaluación de Accesos y Permisos
↓
Monitoreo Continuo de Seguridad
↓
Generación de Auditorías y Reportes
↓
Revisión de Políticas de Acceso
↓
Implementación de Mejoras
↓
Fin

Explicación de Cada Paso:

1. Evaluación de Accesos y Permisos
   - Descripción: Realizar una revisión de los permisos asignados en sistemas y servicios en la nube para garantizar que solo personas autorizadas accedan a datos específicos.
   - Acciones:
     -Generar un informe con los usuarios y roles asignados.
     -Verificar que los accesos sigan alineados con el principio de mínimo privilegio.
     -Revocar accesos innecesarios o no utilizados.

2. Monitoreo Continuo de Seguridad
   - Descripción: Implementar herramientas automatizadas para monitorear la seguridad en tiempo real.
   - Acciones:
     -Configurar alertas automáticas para detectar accesos sospechosos o fuera de horario.
     -Utilizar herramientas como AWS CloudTrail, Azure Security Center o Google Cloud Audit Logs.
     -Registrar actividades críticas como accesos administrativos, cambios en permisos o intentos fallidos de autenticación.

3. Generación de Auditorías y Reportes
   - Descripción: Producir reportes que documenten los accesos, actividades sospechosas y cambios en los permisos.
   - Acciones:
     -Revisar los registros de acceso generados por las herramientas de monitoreo.
     -Identificar patrones inusuales de actividad.
     -Compartir los hallazgos con el equipo de seguridad y cumplimiento.

4. Revisión de Políticas de Acceso y Uso de Datos
   - Descripción: Actualizar políticas de acceso según cambios normativos, tecnológicos o estructurales de la organización.
   - Acciones:
     -Revisar políticas existentes y alinearlas con normas internacionales (ej., GDPR, ISO/IEC 27001).
     -Realizar capacitaciones para empleados sobre las actualizaciones.
     -Implementar nuevos roles o restricciones según sea necesario.

5. Implementación de Mejoras
   - Descripción: Basado en auditorías y monitoreos, realizar cambios para mejorar la seguridad de los datos.
   - Acciones:
     -Integrar nuevas herramientas o procesos que refuercen las medidas de seguridad.
     -Reforzar autenticación multifactor o cifrado en áreas vulnerables.
     -Documentar y comunicar los cambios a las partes interesadas.

Referencias

Amazon Web Services. (n.d.). Security Documentation. Retrieved from https://aws.amazon.com/security/

Microsoft Azure. (n.d.). Security, Privacy, and Compliance. Retrieved from https://azure.microsoft.com/en-us/overview/trusted-cloud/

Google Cloud Platform. (n.d.). Security and Compliance. Retrieved from https://cloud.google.com/security/

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information security management systems — Requirements. Geneva, Switzerland: ISO. Retrieved from https://www.iso.org/standard/54534.html

National Institute of Standards and Technology. (2020). NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: NIST. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

European Union. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj