Campus Monterrey

Materia

Inteligencia artificial avanzada para la ciencia de datos II

Tarea

Evidencia Portafolio Cloud Computing

Estudiantes

Jacobo Hirsch Rodríguez - A00829679

Profesor

Félix Ricardo Botello Urrutia

Indice

Matriz Comparativa de Prácticas de Seguridad en la Nube..... 3
Selección de Prácticas y Herramientas de Seguridad y Confidencialidad..... 4
AWS Key Management Service (KMS):.....4
Google Cloud Identity and Access Management (IAM):..... 4
Azure Active Directory (Azure AD):.....4
AWS CloudTrail:.....4
Google Cloud Data Loss Prevention (DLP):.....5
Estableciendo un Proceso o Estándar de Validación.....5
1. Evaluación Periódica de Permisos y Accesos..... 5
2. Monitoreo Continuo de Seguridad con Auditorías y Reportes de Acceso.....6
3. Revisión y Actualización de Políticas de Acceso y Uso de Datos..... 6
Integración del Proceso..... 7
1. Frecuencia de Validaciones:..... 7
2. Automatización con AWS:..... 7
3. Centralización de Reportes:.....7
Conclusiones..... 7
Referencias..... 8

Matriz Comparativa de Prácticas de Seguridad 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 (MFA)	Cumplimiento con Normativas (ISO/IEC 27001, NIST, GDPR)
AWS	Sí, mediante TLS/SS	Sí, con opciones como AWS KMS	IAM permite políticas detalladas	AWS CloudTrail para auditorías	MFA disponible para usuarios	Cumple con ISO/IEC 27001, NIST y GDPR
Google Cloud	Sí, cifrado en tránsito por defecto	Sí, cifrado en reposo por defecto	IAM para gestión de permisos	Auditorías mediante Cloud Audit Logs	MFA disponible para usuarios	Cumple con ISO/IEC 27001, NIST y GDPR
Azure	Sí, mediante TLS/SSL	Sí, con Azure Storage Service Encryption	Azure AD para control de acceso	Azure Monitor y Log Analytics	MFA disponible para usuarios	Cumple con ISO/IEC 27001, NIST y GDPR

Sobre la **confidencialidad**, **integridad** y **disponibilidad** de los datos al usar cualquiera de los proveedores comparados:

Confidencialidad: Todos los proveedores implementan cifrado en tránsito y en reposo, políticas de acceso basadas en permisos y MFA, garantizando que solo usuarios autorizados accedan a los datos.

Integridad: Mediante auditorías de acceso y registros detallados, se asegura que cualquier modificación o acceso a los datos sea rastreable, manteniendo la integridad de la información.

Disponibilidad: Los proveedores ofrecen infraestructuras redundantes y servicios de alta disponibilidad, asegurando el acceso continuo a los datos y servicios.

Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

AWS Key Management Service (KMS):

Es una herramienta diseñada para gestionar claves criptográficas que protegen datos en reposo y en tránsito mediante el estándar AES-256, un cifrado simétrico robusto. Esta herramienta permite generar, rotar y eliminar claves de manera automática o personalizada, además de integrarse con servicios como Amazon S3 para aplicar cifrado automático. KMS utiliza módulos de seguridad de hardware (HSMs) que aseguran que las claves nunca abandonen un entorno seguro, minimizando el riesgo de exposición. Funciona en conjunto con AWS Identity and Access Management (IAM), lo que permite aplicar principios de mínimo privilegio y políticas detalladas de acceso. Gracias a su soporte para Bring Your Own Key (BYOK), las organizaciones tienen control adicional sobre la seguridad de sus datos, asegurando un cifrado avanzado para cualquier tipo de información sensible.

Google Cloud Identity and Access Management (IAM):

Esta herramienta proporciona control detallado sobre permisos y acceso mediante RBAC (Role-Based Access Control) y se basa en principios de mínimo privilegio, garantizando que los usuarios solo puedan acceder a lo estrictamente necesario. Utiliza protocolos como OAuth 2.0 y OpenID Connect (OIDC) para autenticar usuarios de forma segura, y todo el tráfico entre IAM y los servicios está cifrado mediante TLS 1.2 o superior para evitar ataques de intermediarios (MITM). IAM también admite autenticación multifactor (MFA) para añadir una capa extra de seguridad a los accesos críticos. Además, su integración con Google Cloud Audit Logs permite registrar y rastrear cada acción realizada, facilitando auditorías exhaustivas y la identificación de actividades sospechosas. Esta herramienta asegura una administración eficiente y segura de permisos en entornos de nube.

Azure Active Directory (Azure AD):

Combina autenticación segura y control de acceso granular utilizando estándares como Kerberos, NTLM, SAML y OAuth 2.0, lo que lo convierte en una herramienta versátil para gestionar identidades locales y en la nube. Además, incorpora autenticación multifactor (MFA) con opciones avanzadas como reconocimiento biométrico y tokens físicos. Una de sus características más destacadas es el acceso condicional, que evalúa en tiempo real factores como la ubicación, el dispositivo y el riesgo del usuario antes de permitir el acceso. Los datos y accesos están protegidos mediante TLS 1.2+ en tránsito, y la herramienta integra análisis de seguridad con Azure Sentinel, lo que permite detectar y responder rápidamente a amenazas.

AWS CloudTrail:

Registra de forma inalterable todas las acciones realizadas en una cuenta de AWS, desde llamadas a API hasta cambios en la configuración de los servicios. Los registros están protegidos mediante cifrado AES-256 y pueden cifrarse adicionalmente usando claves gestionadas por AWS KMS para mayor seguridad. Este sistema de auditoría permite enviar registros a Amazon S3, donde se aplican políticas de acceso detalladas para restringir el acceso no autorizado.

Google Cloud Data Loss Prevention (DLP):

Google Cloud DLP protege datos sensibles mediante la identificación y clasificación automatizada de información como números de tarjetas de crédito, identificaciones personales y direcciones IP, utilizando patrones predefinidos, algoritmos de aprendizaje automático y expresiones regulares avanzadas. Es capaz de procesar datos estructurados y no estructurados en múltiples formatos, como texto, JSON, imágenes y CSV, lo que lo convierte en una herramienta versátil para diferentes aplicaciones. Además, permite aplicar técnicas avanzadas como tokenización y pseudonimización para proteger los datos sin comprometer su utilidad, garantizando así que la información confidencial permanezca segura incluso mientras se analiza. Los datos en tránsito están protegidos mediante TLS 1.2 o superior, y las herramientas de redacción eliminan información confidencial de conjuntos de datos visibles para reducir riesgos de exposición.

Estableciendo un Proceso o Estándar de Validación

Todo el proceso se hizo considerando una arquitectura hecha con AWS debido ya que es la herramienta con la que más estoy familiarizado y que considero más completa.

1. Evaluación Periódica de Permisos y Accesos

La gestión de accesos en AWS se realiza mediante **AWS Identity and Access Management (IAM)**, que permite definir roles y asignar permisos detallados bajo el principio de mínimo privilegio. Para iniciar, se debe configurar una política centralizada que asigne permisos estrictos basados en funciones, garantizando que los usuarios solo puedan acceder a los datos necesarios para sus tareas. De manera trimestral, se pueden utilizar los informes de acceso generados por IAM Access Analyzer para auditar los permisos activos, identificando accesos innecesarios o riesgosos, como cuentas inactivas con permisos elevados. La herramienta permite verificar si las configuraciones de acceso cumplen con las mejores prácticas de seguridad y normativas relevantes. En caso de irregularidades,

se pueden ajustar las políticas directamente desde la consola de IAM o mediante AWS Organizations, que facilita la administración centralizada de permisos en múltiples cuentas de AWS.

Resultado esperado: Un control granular y actualizado de los permisos que garantice un acceso limitado y seguro a los datos.

2. Monitoreo Continuo de Seguridad con Auditorías y Reportes de Acceso

Para realizar auditorías continuas, **AWS CloudTrail** es una herramienta esencial que registra todas las actividades en una cuenta de AWS, incluidas llamadas a API y cambios en la configuración de servicios. Los registros generados por CloudTrail están protegidos mediante cifrado AES-256 y se pueden integrar con Amazon S3 para almacenamiento seguro o Amazon CloudWatch para crear alertas en tiempo real sobre actividades sospechosas, como intentos de acceso no autorizados o patrones inusuales de uso. Además, la integración con **Amazon GuardDuty** permite detectar amenazas avanzadas al analizar los registros de CloudTrail y otros flujos de datos, como logs de VPC o DNS, utilizando aprendizaje automático. Para mantener un monitoreo eficiente, se recomienda establecer auditorías mensuales de los reportes generados, revisando los eventos registrados y asegurando que las acciones sean consistentes con las políticas de acceso definidas.

Resultado esperado: Identificación oportuna de actividades irregulares mediante auditorías continuas, alertas en tiempo real y análisis de amenazas.

3. Revisión y Actualización de Políticas de Acceso y Uso de Datos

La herramienta **AWS Config** es clave para garantizar que las políticas de acceso y uso de datos estén alineadas con las normativas vigentes. AWS Config monitorea continuamente los recursos de AWS y verifica si cumplen con las reglas predefinidas, como la aplicación de cifrado en reposo mediante AWS Key Management Service (KMS) o el uso de conexiones seguras (TLS 1.2+) para datos en tránsito. Además, se pueden configurar políticas dinámicas utilizando **AWS Service Control Policies (SCPs)** a través de AWS Organizations, lo que permite implementar restricciones globales a nivel de cuenta o servicio, como bloquear accesos no cifrados o desde ubicaciones no aprobadas. Estas políticas deben revisarse semestralmente para adaptarse a cambios normativos o en la estructura organizacional. También se debe capacitar al personal autorizado en el manejo seguro de datos utilizando guías y simulaciones proporcionadas por AWS Security Hub, una herramienta que centraliza las mejores prácticas de seguridad.

Resultado esperado: Políticas de acceso y uso actualizadas que cumplan con normativas internacionales y aseguren el manejo ético de los datos.

Integración del Proceso

1. **Frecuencia de Validaciones**:
    - **IAM**: Evaluaciones trimestrales de permisos y acceso.
    - **CloudTrail y Guard Duty**: Auditorías mensuales y alertas en tiempo real.
    - **Config y SCPs**: Revisión semestral de políticas de acceso y cumplimiento normativo.
2. **Automatización con AWS**:
    - Configurar AWS Config para monitorear reglas automáticamente y activar alertas en caso de incumplimiento.
    - Usar Amazon Event Bridge para coordinar acciones correctivas automáticas basadas en eventos de CloudTrail.
3. **Centralización de Reportes**:
    - Consolidar auditorías y métricas de seguridad en AWS Security Hub, generando informes para la alta dirección y equipos de cumplimiento.

Conclusiones

Cuando se comparan los principales proveedores de servicios en la nube, AWS, Google Cloud y Azure, queda claro que todos cumplen con estándares internacionales como ISO/IEC 27001, NIST y GDPR. Utilizan tecnologías avanzadas como cifrado AES-256, autenticación multifactor (MFA) y auditorías detalladas para garantizar la seguridad de los datos. Entre ellos, AWS sobresale por su completo conjunto de herramientas que simplifican la gestión de accesos, protegen datos sensibles y permiten auditorías continuas de manera eficiente.

Cada proveedor ofrece soluciones únicas: AWS KMS garantiza un cifrado robusto con claves gestionadas de forma segura, Google Cloud DLP emplea inteligencia artificial para identificar y proteger datos sensibles, y Azure AD fortalece la seguridad con acceso condicional y autenticación avanzada. Herramientas como AWS CloudTrail y Google Cloud IAM brindan control granular y auditorías exhaustivas, ofreciendo a las organizaciones la flexibilidad de implementar estrategias de seguridad adaptadas a sus necesidades.

El sistema de validación basado en herramientas de AWS propone un enfoque estructurado que incluye monitoreo continuo con CloudTrail y GuardDuty, revisión de permisos con IAM y ajuste de políticas con Config y SCPs. Este modelo asegura tanto la protección de datos sensibles como el cumplimiento de normativas y buenas prácticas de seguridad.

En definitiva, integrar herramientas avanzadas con procesos bien diseñados permite gestionar datos en la nube de manera segura, ética y escalable. AWS lidera con su ecosistema interconectado, ofreciendo una solución confiable y replicable, que refuerza la confianza en el manejo responsable de la información.

Referencias

Amazon Web Services. (n.d.). Encrypt data in transit. En *AWS Documentation*. Recuperado el 25 de noviembre de 2024, de https://docs.aws.amazon.com/es_es/whitepapers/latest/navigating-gdpr-compliance/encrypt-data-in-transit.html

Amazon Web Services. (n.d.). What is MFA? En *AWS*. Recuperado el 25 de noviembre de 2024, de https://aws.amazon.com/es/what-is/mfa/

Google Cloud. (n.d.). Preguntas frecuentes sobre la seguridad de Cloud. En *Google Support*. Recuperado el 25 de noviembre de 2024, de https://support.google.com/cloud/answer/6262505?hl=es

Revista Seguridad. (2024). Autenticación multifactor en Google Cloud. Recuperado el 25 de noviembre de 2024, de https://revistaseguridad.cl/2024/11/16/autenticacion-multifactor-google-cloud/

Microsoft. (n.d.). Cifrado de datos en reposo en Azure. En *Microsoft Learn*. Recuperado el 25 de noviembre de 2024, de https://learn.microsoft.com/es-es/azure/security/fundamentals/encryption-atrest

Microsoft. (n.d.). Microsoft Entra MFA. En *Microsoft Security*. Recuperado el 25 de noviembre de 2024, de https://www.microsoft.com/es-es/security/business/identity-access/microsoft-entra-mfa-multi-factor-authentication