Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia artificial avanzada para la ciencia de datos I (Gpo 101)

Cloud computing | Evidencia portafolio

Saul Francisco Vázquez del Río A01198261

Campus Monterrey **Fecha: 4/11/2024**

Tabla de características de seguridad

Característica de Seguridad	AWS	Google Cloud	Azure
Cifrado de datos en tránsito	TLS/SSL y VPN para cifrado en tránsito y certificado de seguridad para APIs y servicios	HTTPS y TLS para proteger datos en tránsito; seguridad de red con protocolos de VPN y TLS	TLS/SSL en tráfico; VPN y ExpressRoute para conexión segura con redes empresariales;
Cifrado de datos en reposo	Cifrado automático con AES-256 en la mayoría de los servicios; claves gestionados por el cliente o AWS	Cifrado AES-256 para datos en reposo; opciones claves gestionadas por cliente y Google	Cifrado AES-256 para datos en reposo; opción de administrar claves con Azure Key Vault o generar claves propias
Gestión de claves (KMS)	AWS Key Management Service para crear, administrar y controlar Keys	Google Cloud Key Management (Cloud KMS) para gestionar y proteger Keys	Azure Key Vault para gestionar y generar Keys
Monitoreo y auditoría de seguridad	AWS CloudTrail para la auditoría de actividades, y AWS GuardDuty para detección de amenazas	Google Audit Logs y Google Cloud Security Command Center para alertas de seguridad	Azure Security Center y Azure Monitor para detección de amenazas y alertas
Protección contra DDoS	AWS Shield y AWS WAF para la protección de ataques DDoS y control de tráfico malicioso	Google Cloud Armor y Cloud CDN para la protección de ataques DDoS y filtrado de tráfico	Azure DDoS Protección y Azure WAF para la protección de ataques DDoS y control de tráfico malicioso

Tablas de prácticas de seguridad

Prácticas de Confidencialidad	AWS	Google Cloud	Azure

Policías de acceso basada en permisos	Control de acceso detallado mediante AWS Identity and Access Management (IAM)	Cloud Identity and Access Management (IAM)	Azure Active Directory (AD) y Role Based Access Control (RBAC)
Auditorías de acceso	AWS CloudTrail permite rastrear y auditar el acceso a los recursos de AWS generando log de actividad	Cloud Audit Logs para rastreo de accesos y cambio en recursos, con reportes	Azure Monitor y Azure AD Logs para registros de auditoría de actividades
Autentificador multifactor (MFA)	MFA integrado en IAM; autentificador multifactor para usuario y admin	Soporte en MFA en cuentas de usuario autenticación a través de google authenticator	MFA a través de Azure AD, compatible con aplicaciones y celulares para acceso seguro
Control de identidad de usuario y session	AWS Single Sign-On (SSO) y gestión de sesiones con políticas de duración y control de accesos	Identity-Aware Proxy (IAP) y SSO para proteger accesos y controlar sesiones de usuarios	Azure AD ofrece SSO y control de session, con opciones de duración y autentificación
Políticas de acceso incondicional	IAM permite políticas basadas en condiciones como ubicación, IP y horario para restringir accesos	Condiciones en Cloud IAM basadas en atributos como IP y tiempo	Azure AD Condicional Access para definir políticas basadas en contexto, ubicación y riesgo del usuario.

1. AWS Key Management
   Proveedor: Amazon Web Services
   Ventajas:
   - Ofrece un servicio centralizado para la creación y gestión de claves, compatible con el cifrado AES-256
   - Permite integrar las claves creadas con otros servicios de AWS para proteger datos automáticamente
   - Cumple con regulaciones como FIPS 140-2 y es compatible con auditorias bajo normas como ISO 27001

Funcionamiento:

- Los usuarios pueden elegir entre claves creadas por AWS o gestionar las sus claves propias, al igual que facilita la rotación automática de claves y permite establecer políticas detalladas de acceso.

2. Google Cloud Armor

   Proveedor: Google Cloud

   Ventajas:

   - Proporciona protección avanzada contra ataques DDoS mediante políticas de seguridad basadas en reglas
   - Integra la inteligencia artificial para detectar patrones de tráfico maliciosos en tiempo real
   - Es compatible con el filtrado geográfico y protege aplicaciones web y servicios API

   Funcionamiento:

   - Configura políticas de acceso basado en el nivel de riesgo y atributos de tráfico como IPS o encabezados HTTP, además de ofrecer visibilidad completa del tráfico mediante Google Cloud Security Command Center

3. Azure Active Directory (AD)
   Proveedor: Azure
   Ventajas:
   - Proporciona control de acceso detallado basado en roles y tiene un autentificador multifactor
   - Incluye políticas de acceso condicional que permiten restringir accesos según contexto como ubicación, riesgo o dispositivo
   - Compatible con SSO (Single Sign On) para facilitar la gestión de usuarios

   Funcionamiento:
   - Los administradores configuran roles y permisos específicos para cada usuario o grupo, además se integra con aplicaciones empresariales y servicios en la nube para simplificar el acceso seguro.

4. AWS CloudTrail
   Proveedor: Amazon Web Services:
   Ventajas:
   - Permite monitorear y restringir actividades en el entorno de AWS, ayudando a rastrear el accesos de datos y controlar estos.
   - Genera logs detallados que pueden exportarse para auditorías o integrarse con herramientas SIEM
   - Compatible con la normativa GDPR y normas de seguridad como NIST y ISO 27001

Funcionamiento:

- Registra cada solicitud realizada dentro de AWS, incluyendo la identidad del solicitante, la acción realizada y los recursos que se vieron usados o afectados. Facilitando la configuración de alarmas para actividades sospechosas a través de AWS CloudWatch

5. Azure Key Vault
   Proveedor: Azure
   Ventajas:
   - Almacena y gestiona claves, contraseñas y certificados en un entorno seguro
   - Compatible con el cifrado AES-256 y cumple revelaciones como GDPR
   - Ofrece opciones para integrar las claves y aplicaciones empresariales y bases de datos en la nube

   Funcionalidades:
   - Los administradores pueden generar y administrar claves directamente desde Azure Key Vault, además de proporcionar un entorno seguro y aislado para reducir el riesgo de exposición de datos.

Evaluación periódica de permisos y accesos

La evaluación periódica de permisos y accesos tienen como objetivo garantizar que solo las personas autorizadas o con roles específicos accedan a los datos. Este proceso debe de realizarse trimestralmente o según la capacidad de los datos. Es fundamental generar reportes de accesos desde sistemas IAM para compararlos con las funciones asignadas a cada usuario dentro de la organización. Esto permite identificar y revocar accesos innecesarios. Todos los cambios deben resignarse, y un informe debe enviarse al equipo de cumplimiento para garantizar transparencia. Las herramientas necesarias como AWS IAM Access Analyzer, Google Cloud IAM Policy Analyzer, o Azure AD Access Reviews son ideales para llevar a cabo este tipo de revisiones.

Monitoreo continuo de la seguridad con auditorías y reportes de acceso

El monitoreo continuo es esencial para detectar y mitigar incidentes de seguridad en tiempo real. Este proceso incluye la configuración de monitoreo constante, acompañada de auditorías mensuales o registros. Es necesario activar registros detallados, como logs y cambios, para analizar anomalías. Finalmente un informe mensual debe presentarse a la dirección, destacando incidentes y medidas correctivas. Las herramientas recomendadas son AWS CloudTrail, Google Cloud Audit Logs y Azure Monitor.

Revisión y actualización de políticas de acceso y uso de datos, garantizando que solo el equipo autorizado tenga acceso, cumpliendo con la normativa vigente

La revisión y actualización de políticas de acceso y uso de datos asegura que están alineadas con las regulaciones vigentes y las necesidades organizacionales. Este

proceso debe de realizarse después de actualizaciones importantes o semestralmente para tener un control. Se debe colaborar con el equipo de cumplimiento para garantizar que las políticas cumplan con las regulaciones necesarias. Los cambios deben de ser documentados o comunicados a los empleados que estén designados capacitaciones y los documentos que cumplan con una documentación clara. Además es recomendable hacer simulacros para afirmar que las políticas se están cumpliendo. Las herramientas recomendadas son Azure Policy o AWS Config.

Conclusión

Mediante la actividad realizada se puede observar que la hacer una implementación de este tipo no solamente protege los datos y ayuda a cumplir las normativas vigentes, la combinación de evaluaciones periódicas de permisos y accesos más el monitoreo continuo de la seguridad, y la actualización regular de políticas garantiza que los datos estén disponibles únicamente para personal autorizado, reduciendo riesgos y posibles brechas de seguridad.

El usos de las herramientas de cloud, como AWS, Google o Azure brindan la capacidad para las compañías de poder identificar brechas de seguridad, responder a alertas en tiempo real y adaptarse a cambios.

Referencias

- *Seguridad en la Nube - Amazon Web Services (AWS)*. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/es/security/
- *Identity and Access Management documentation | IAM Documentation | Google Cloud*. (n.d.). Google Cloud. https://cloud.google.com/iam/docs
- Msmbaldwin. (n.d.). *Azure security documentation*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/security/
- *ISO/IEC 27001:2022*. (n.d.). ISO. https://www.iso.org/isoiec-27001-information-security.html
- Rboucher. (n.d.). *Azure Monitor documentation - Azure Monitor*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/azure-monitor/