Instituto Tecnológico y de Estudios Superiores de Monterrey

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

Cloud computing | Evidencia portafolio

Eliezer Cavazos Rochin A00835194

Campus Monterrey **Fecha: 26/11/2024**

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

Características	AWS	Google Cloud	Microsoft Azure
Cifrado de datos en tránsito y en reposo	- Cifrado AES-256 por defecto. - TLS 1.2 para datos en tránsito.	- Cifrado AES-256 y TLS 1.2 por defecto. - Google Cloud Key Management Service para claves de cifrado personalizadas.	- Cifrado AES-256 para datos en reposo y en tránsito. - Azure Disk Encryption utiliza BitLocker para Windows y DM-Crypt para Linux.
Confidencialidad	- La ISO 27017 para la seguridad en la nube, - La ISO 27701 para la administración de la información sobre la privacidad - La ISO 27018 para la privacidad en la nube.	- IAM con control detallado de permisos. - Cloud Audit Logs para seguimiento de accesos. - MFA como estándar.	- Active Directory y control de roles detallados. - Azure Monitor Logs y Azure Security Center para auditorías. - MFA para acceso.
Integridad	- Control de versiones en S3 para datos críticos. - Monitoreo con Amazon GuardDuty para detectar actividad sospechosa.	- Verificación de integridad con checksums en servicios de almacenamiento. - Detección de amenazas con Cloud Security Command Center.	- Verificación de integridad automática en Azure Blob Storage. - Monitoreo y alertas con Microsoft Defender for Cloud.
Disponibilidad	- SLA del 99.99% para servicios principales. - Redundancia en múltiples zonas de disponibilidad.	- SLA del 99.95% para servicios estándares. - Redundancia geográfica y recuperación ante desastres.	- SLA del 99.95% para servicios estándares. - Funciones avanzadas de recuperación ante desastres.
Normas	- Certificaciones ISO/IEC 27001, NIST, GDPR.	- Certificaciones ISO/IEC 27001, NIST, GDPR.	- Certificaciones ISO/IEC 27001, NIST, GDPR.

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

1. Cifrado avanzado: Implementar cifrado AES-256 en reposo y TLS 1.2 o superior en tránsito.
2. Control de acceso basado en el principio de mínimo privilegio: Configurar políticas estrictas en IAM para limitar accesos según roles.
3. MFA obligatorio: Establecer autenticación multifactor para todos los usuarios.
4. Auditoría continua: Usar servicios como AWS CloudTrail o Google Cloud Audit Logs para registrar y revisar accesos.
5. Monitoreo de amenazas: Implementar herramientas como Amazon GuardDuty o Microsoft Defender.

Herramientas/Componentes:

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

Ventajas: Gestión centralizada de claves de cifrado; integración con otros servicios de AWS.
Función: Genera y administra claves criptográficas con alta disponibilidad.

2. **Google Cloud Security Command Center**

Ventajas: Consolida alertas de seguridad; identifica configuraciones erróneas y vulnerabilidades.
Función: Proporciona una visión general del estado de seguridad.

3. **Azure Active Directory (AAD)**

Ventajas: Soporte para MFA y SSO; integración con aplicaciones de terceros.
Función: Gestiona accesos y usuarios en la nube.

4. **AWS CloudTrail**

Ventajas: Registro completo de las actividades realizadas en AWS.
Función: Facilita auditorías y revisiones de cumplimiento.

5. **Google Cloud Key Management**

Ventajas: Soporte para claves personalizadas y auditoría del uso de claves.
Función: Gestiona claves de cifrado para proteger datos en reposo.

3. Establecimiento de un Proceso o Estándar de Validación

Proceso de Validación:

1. **Evaluación Periódica de Permisos y Accesos**
    - Su objetivo es garantizar que solo las personas autorizadas o con roles específicos accedan a los datos.
    - Revisar trimestralmente las políticas de acceso en IAM.
    - Identificar y revocar accesos innecesarios o inactivos.
    - Para todo cambio se deben generar informes para garantizar transparencia
2. **Monitoreo Continuo de Seguridad**
    - Su objetivo es detectar y mitigar incidentes de seguridad en tiempo real.
    - Configurar alertas automáticas en herramientas de monitoreo como Azure Monitor o Google Cloud Security Command Center.
    - Realizar auditorías semestrales utilizando los registros de acceso con las siguientes herramientas dependiendo del servidor AWS CloudTrail, Google Cloud Audit Logs y Azure Monitor.
3. **Revisión y Actualización de Políticas de Acceso**
    - Su objetivo es la revisión y actualización de políticas de acceso y uso de datos asegura que están alineadas con las regulaciones vigentes y las necesidades organizacionales
    - Establecer reuniones mensuales para actualizar prácticas según nuevas amenazas o requerimientos normativos.

Conclusion

En esta actividad pude entendender mejor el funcionamiento de seguridad de los diferentes proveedores de nube que existen de empresas como Amazon, Google y Microsoft, muchas de estas herramientas ayudan a mantener un nivel de seguridad alto que cualquier empresa deberia tener para administrar usuarios, datos, archivos, etc. También el conocer diferentes estrategias que se implementan para mantener la seguridad de contraseñas y los registros de acciones realizadas ayudan cuando se tiene que trabajar con cualquiera de estas tecnologias ya que aunque sean compañías distintas siguen los mismos principios.

Bibliografia

Msmbaldwin. (2023, 25 marzo). Cifrado en reposo de datos de Azure: seguridad de

Azure.Microsoft Learn.

https://learn.microsoft.com/es-es/azure/security/fundamentals/encryption-atrest

Opciones de cifrado para Amazon EMR - Amazon EMR. (s. f.).
https://docs.aws.amazon.com/es_es/emr/latest/ManagementGuide/emr-data-encryption-options.html

Encriptación en tránsito. (s. f.). Google Cloud.
https://cloud.google.com/docs/security/encryption-in-transit?hl=es-419

Transparencia y protección de datos. (s. f.). Google Cloud.
https://cloud.google.com/transparency?hl=es

Privacidad de datos en la nube de confianza | Microsoft Azure. (s. f.).
https://azure.microsoft.com/es-mx/explore/trusted-cloud/privacy

Computación criptográfica de AWS (2:05). (s. f.). [Vídeo]. Amazon Web Services, Inc.
https://aws.amazon.com/es/compliance/data-privacy/

Firma criptográfica de cifrado - AWS Key Management Service - AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/kms/

Security Command Center. (s. f.). Google Cloud.
https://cloud.google.com/security/products/security-command-center?hl=es_419

Microsoft Entra ID (anteriormente, Azure Active Directory) | Seguridad de Microsoft. (s. f.).
https://www.microsoft.com/es-es/security/business/identity-access/microsoft-entra-id

Registros de API - Servicio de registro estandarizado de seguridad - AWS CloudTrail - AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/cloudtrail/

Cloud Key Management. (s. f.). Google Cloud.
https://cloud.google.com/security/products/security-key-management?hl=es_419

¿En qué consiste la revisión de acceso de usuario? - ADM Cloud Services. (s. f.). ADM Cloud Services.
https://admcloudservices.com/en-que-consiste-la-revision-de-acceso-de-usuario/

Monitoreo continuo de la seguridad (DE.MC). (s. f.). Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.
https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad/detectar/monitoreo-continuo-seguridad-demc
¿En qué consiste la revisión de acceso de usuario? - ADM Cloud Services. (s. f.-b). ADM Cloud Services.
https://admcloudservices.com/en-que-consiste-la-revision-de-acceso-de-usuario