Tecnológico de Monterrey

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

Profesor: Félix Ricardo Botello Urrutia

Diseño de Arquitectura en la Nube

Evidencia Portafolio - Módulo cloud computing

Fernanda Perez A01742102

Noviembre 2024

Evidencia Portafolio - Módulo cloud computing

Instrucciones:

De manera individual realizar la actividad que se menciona a continuación:

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

- Investiga y compara proveedores de servicios en la nube conocidos (ej., AWS, Google Cloud, Azure) e identifica:
    - Características de seguridad como cifrado de datos en tránsito y en reposo.
    - Prácticas de confidencialidad, como políticas de acceso basadas en permisos, auditorías de acceso y autenticación multifactor.
- Realiza una matriz comparativa donde clasifiques las prácticas de cada proveedor en relación con los principios éticos (confidencialidad, integridad y disponibilidad) y las normas como ISO/IEC 27001, NIST y GDPR.

Después de una amplia investigación se realizó una comparación de los proveedores AWS, Google Cloud y Azure, con el fin de comparar y evaluar las características clave de seguridad, prácticas de confidencialidad y cumplimiento de normativas.

Aspecto	**AWS**	**Google Cloud**	**Azure**
Cifrado en tránsito y en reposo	Cifrado AES-256; TLS en tránsito	TLS 1.3 y cifrado AES-256	TLS y cifrado AES-256 en reposo y en tránsito
Políticas de acceso	IAM: Control de accesos detallado basado en roles y políticas	IAM: Roles personalizables y administración centralizada	Azure Active Directory para permisos y autenticación
Autenticación multifactor (MFA)	MFA opcional con integración de dispositivos físicos y software	Integración con claves de hardware y autenticación en dos pasos	MFA integrada con aplicaciones de Microsoft
Auditorías y monitoreo	AWS CloudTrail para monitoreo y generación de reportes	Cloud Logging para auditorías y supervisión en tiempo real	Azure Monitor y Security Center para auditorías y alertas
Cumplimiento normativo	ISO/IEC 27001, GDPR, NIST 800-53, PCI DSS,	ISO/IEC 27001, GDPR, NIST 800-53, PCI DSS	ISO/IEC 27001, GDPR, NIST 800-53, PCI DSS

	HIPAA		

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

- Basado en la matriz comparativa, selecciona las mejores prácticas y herramientas de seguridad para proteger los datos en la nube. Considera prácticas como(pero no limitado a):
    - Cifrado avanzado de datos sensibles.
    - Control de accesos basados en permisos y principios de mínimo privilegio.
    - Registros de auditoría para monitorear y revisar accesos a los datos.
- (Seleccionar 5 herramientas/componentes de los proveedores de nube y realizar una breve explicación de sus ventajas/funcionamiento)

Después de analizar la matriz comparativa (la tabla) las herramientas seleccionadas de acuerdo a las características solicitadas son:

1. AWS Key Management Service (KMS)

- Este es un servicio de gestiónn de claves de cifrado que le permite a los usuarios crear, administrar y poder utilizar claves criptográficas con el fin de proteger datos almacenados y en tránsito. Es decir administra claves de cifrado para datos almacenados y en tránsito.
- Ventajas:
    - AWS Key Management Service (KMS) ofrece seguridad de nivel avanzado al gestionar claves en un entorno protegido frente a accesos no autorizados, asegurando la confidencialidad de los datos. Al tener un manejo centralizado permite administrar todas las claves desde una única consola, con opciones como la rotación automática para mantener un nivel óptimo de seguridad. También KMS cumple con normativas internacionales como :GDPR, HIPAA y NIST, es por eso que es una herramienta confiable para garantizar el cumplimiento regulatorio y la protección de datos.

2. Google Cloud Identity and Access Management (IAM)

- Google Cloud (IAM) brinda un sistema centralizado para controlar el acceso a los recursos en la nube, permite asignar permisos detallados y específicos según roles, como : lectura, escritura o administrador, esto ayuda a segurar que cada usuario o servicio tenga el nivel de acceso mínimo necesario.
- Ventajas:
    - Google Cloud (IAM) se destaca por su fácil y sencilla integración con otros servicios de Google Cloud, como por ejemploo BigQuery y Google Cloud Storage, esto permite una administración fluida de los recursos. Mediante políticas y roles altamente personalizables proporciona un control granular lo

que garantiza un acceso preciso y seguro de acuerdo a las necesidades requeridas de cada cliente.

3. Azure Security Center

- Azure Security Center es una solución integral que ayuda en la gestión de la seguridad en entornos de Azure. Ayuda a proporcionarr monitoreo continuo, detección de amenazas, y análisis de vulnerabilidades, lo cual ayuda a los usuarios a mejorar la postura de seguridad de sus sistemas.
- Ventajas:
    - Azure Security Center es una solución integral que como ventaja ofrece monitoreo continuo con el fin de identificar y priorizar riesgos en tiempo real, como lo son configuraciones incorrectas o amenazas externas. Constantementte se hace un análisis de vulnerabilidades para detectar posibles debilidades en la infraestructura, garantizando una protección proactiva. Tambien otra de sus ventajas es que proporciona recomendaciones específicas y personalizadas que ayudan a los usuarios a mejorar la configuración de seguridad y optimizar la postura de protección de sus sistemas.

4. AWS CloudTrail

- AWS CloudTrail hace un registro de todas las actividades realizadas en una cuenta de AWS, genera los logs detallados sobre accesos y cambios en los recursos. Lo cual facilita la trazabilidad completa de las acciones, desde cambios de configuración hasta intentos de acceso no autorizados.
- Ventajas:
    - AWS CloudTrail es una herramienta esencial que sirve para garantizar la trazabilidad completa de las actividades en la nube, registrando información detallada de cada evento, como el usuario, la acción realizada y el momento en que ocurrió, lo cual resulta clave y util para auditorías. Como proporciona un historial de actividades contribuye al cumplimiento normativo de estándares como ISO 27001, otra ventaja es que integración con Amazon CloudWatch permite generar alertas y reportes sobre eventos críticos, mejorando la capacidad de respuesta ante incidentes de seguridad.

5. Google Cloud Logging

- Google Cloud Logging es un servicio centralizado que tiene la capacidad de permitir capturar, almacenar y analizar logs de eventos en tiempo real de todos los recursos de Google Cloud. Este ayuda a identificar problemas operativos y de seguridad.
- Ventajas:
    - Google Cloud Logging es una herramienta que se usa para la detección de incidentes, dada su buena capacidad para procesar grandes volúmenes de datos y generar alertas que permiten identificar rápidamente actividades alertantes sospechosas. Otra ventaja es que se puede integrar sencillamente con

herramientas externas como Google Cloud Monitoring y otras plataformas, ofreciendo una solución completa para la supervisión y gestión de logs. Ademas garantiza el cumplimiento normativo al almacenar los registros en formatos compatibles con estándares como GDPR y NIST lo cual asegura la seguridad y conformidad de los datos.

3. Establecimiento de un Proceso o Estándar de Validación

- Define un proceso de validación que asegure el manejo ético y seguro de los datos mediante la evaluación de los siguientes puntos:
    - Evaluación periódica de permisos y accesos.
    - Monitoreo continuo de la seguridad con auditorías y reportes de acceso.
    - Revisión y actualización de políticas de acceso y uso de datos, garantizando que solo el equipo autorizado tenga acceso, cumpliendo con la normativa vigente.

Proceso o Estandar de Validación:

Proceso de Validación de Seguridad en la Nube

Primeramente estableciendo el alcance, este procedimiento está diseñado para garantizar que el manejo de los datos almacenados en la nube sea seguro, ético y regulado , es válido y aplica a todas las cuentas y recursos gestionados mediante proveedores como AWS, Google Cloud y Azure, enfocándose en evaluar accesos, monitorear actividades y actualizar políticas de seguridad.

Definición de los Pasos del proceso:

1. Evaluación de Permisos y Accesos:
    - Se planean realizar auditorías trimestrales de los permisos otorgados a usuarios y servicios. Para lo cual, se pueden utilizar herramientas como AWS IAM Access Analyzer y Google Cloud Policy Troubleshooter, que ayudan a identificar permisos excesivos o mal configurados.
    - Verificar que cada usuario o servicio tenga asignado únicamente el acceso necesario y que no existan cuentas sin supervisión.
2. Monitoreo Continuo y Auditorías:
    - Se podrían implementar herramientas como : AWS CloudTrail y Google Cloud Logging para registrar y supervisar todas las actividades realizadas en los recursos de la nube.
    - Se configurarán alertas en tiempo real que puedan detectar actividades sospechosas o que sean no autorizadas.
3. Revisión y Actualización de Políticas de Uso y Acceso:

- Revisar las políticas de acceso y uso por lo menos una vez al año,
- Hacer uso obligatorio de autenticación multifactor (MFA) y cifrado en todos los niveles, tanto en tránsito como en reposo, para proteger los datos.

4. Validación de Reportes de Acceso:
    - Hacer una revisión periódica de los logs generados por herramientas como : Azure Security Center y Google Cloud Logging, con el fin de buscar y encontrar patrones de comportamiento sospechosos que puedan prender un foco rojo de riesgos o vulnerabilidades.
    - Documentar y/o llevar una bitácora de los hallazgos de las auditorías y establecer medidas correctivas para resolver cualquier problema que se identifique.
5. Entrenamiento al Personal:
    - Llevar a cabo capacitaciones anuales enfocadas en el manejo seguro de datos, las mejores prácticas de seguridad en la nube, y las actualizaciones en normativas como GDPR, ISO 27001 o NIST.
    - Asegurarse de que todas las personas del equipo que estén involucradas comprendan y sigan los procedimientos establecidos para evitar y/o minimizar errores humanos.

Diagrama de flujo:
Evaluación de permisos y accesos → Monitoreo continuo y auditorías → Revisión de políticas de acceso → Validación de reportes → Capacitación del personal

Conclusiones

Al hacer la evaluación de los proveedores nos demostró que AWS, Google Cloud y Azure cumplen con altos estándares de seguridad, pero destacan en aspectos diferentes como por ejemplo, monitoreo continuo en AWS y facilidad de uso en Google Cloud.

Las herramientas que fueron seleccionadas son esenciales y clave para garantizar la confidencialidad, integridad y disponibilidad de los datos.

El proceso diseñado nos asegura un manejo ético y seguro de los datos por medio de auditorías, monitoreo y actualizaciones continuas.

Al adoptar estas prácticas preestablecidas fortalece la confianza en la gestión de datos en la nube, cumpliendo con normativas internacionales como ISO/IEC 27001 y GDPR.

Referencias:

for, O. (2022). ISO/IEC 27001:2022. Retrieved November 29, 2024, from ISO website: https://www.iso.org/standard/27001

Security and Privacy Controls for Information Systems and Organizations. (2020). https://doi.org/10.6028/nist.sp.800-53r5

General Data Protection Regulation (GDPR) – Final text neatly arranged. (2024, April 22). Retrieved November 29, 2024, from General Data Protection Regulation (GDPR) website: https://gdpr-info.eu/

AWS re:Invent 2021: mejora continua de la seguridad; estrategias y tácticas. (2021). Retrieved November 29, 2024, from Amazon Web Services, Inc. website: https://aws.amazon.com/es/architecture/security-identity-compliance/?cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc&awsf.content-type=*all&awsf.methodology=*all

Documentación de la administración de identidades y accesos | IAM Documentation | Google Cloud. (2024). Retrieved November 29, 2024, from Google Cloud website: https://cloud.google.com/iam/docs?hl=es-419

ElazarK. (2024). Microsoft Defender for Cloud documentation - Microsoft Defender for Cloud. Retrieved November 29, 2024, from Microsoft.com website: https://learn.microsoft.com/en-us/azure/defender-for-cloud/

Registros de API - Servicio de registro estandarizado de seguridad - AWS CloudTrail - AWS. (2024). Retrieved November 29, 2024, from Amazon Web Services, Inc. website: https://aws.amazon.com/es/cloudtrail/

Gartner for Information Technology (IT) Leaders. (2024). Retrieved November 29, 2024, from Gartner website: https://www.gartner.com/en/information-technology

Home. (2020). Home | Ponemon Institute. Retrieved November 29, 2024, from Ponemon Institute website: https://www.ponemon.org/

CIS Controls Version 8. (2022, February 4). Retrieved November 29, 2024, from CIS website: https://www.cisecurity.org/controls/v8