Evidencia de Portafolio

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

Prácticas	AWS	GCP	Azure
Cifrado en tránsito	TLS para el tránsito de datos entre un punto y otro.	TLS para el tránsito de datos entre un punto y otro.	TLS para el tránsito de datos entre un punto y otro.
Cifrado en reposo	Cifrado de metadatos usando AES 256.	Cifrado de datos usando AES.	Cifrado de metadatos usando AES 256.
Autenticación	MFA mandatorio para el usuario root, y SSO	MFA y SSO	MFA y SSO
Políticas de Acceso	IAM, y AWS KMS para gestionar el control de acceso a los servicios.	Políticas IAM para gestionar el control de acceso a los servicios.	Políticas IAM para gestionar el control de acceso a los servicios.
Auditoría	AWS Audit Manager	Cloud Audit Logs	Azure Monitor

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

1. Cifrado avanzado de datos

   AWS KMS (Key Management Service) permite gestionar y controlar el uso de claves de cifrado para proteger datos en tránsito y en reposo. Se integra con múltiples servicios de AWS, garantizando cifrado con estándares como AES-256. La ventaja de este servicio es que tiene una gestión centralizada y una escalabilidad para proteger grandes volumen de datos

2. Control de acceso basado en permisos

   IAM (Identity and Access Management) proporciona herramientas para aplicar el principio de mínimo privilegio mediante políticas personalizables. La ventaja de este servicio es que permite una gran granularidad para asignar permisos a usuarios, roles y recursos.

3. Registros de auditoría

   Cloud Audit Logs rastrea la actividad de las cuentas y servicios en GCP proporcionando un registro detallado de los cambios realizados. La ventaja de este servicio es que ofrece una visibilidad completa sobre las acciones en la infraestructura para auditorías y cumplimiento normativo.

4. Monitoreo Continuo

   Azure Monitor ofrece capacidades avanzadas para recopilar, analizar y actuar sobre métricas en tiempo real relacionadas con el estado de seguridad de los datos. La principal ventaja de este servicio es que mejora la detección de anomalías y posibles brechas de seguridad.

5. Autenticación Multifactorial

   La MFA con SSO ofrece la facilidad de un acceso centralizado para las empresas que utilicen los servicios de la nube. La ventaja de usar una MFA es que aumenta la seguridad contra accesos no autorizados, incluso en el caso de contraseñas comprometidas.

3. Establecimiento de un Proceso o Estándar de Validación

1. Evaluación periódica de permisos y accesos
   - Realizar revisiones periódicas de las políticas de accesos en IAM y eliminar permisos que ya no se utilicen.
   - Garantizar que se sigan los principios de mínimo privilegio y que los accesos se restrinjan temporalmente cuando sea necesario.
2. Monitoreo continuo de la seguridad con auditorías y reportes de acceso
   - Implementar herramientas como AWS CloudTrail o Azure Monitor para registrar y alertar sobre actividades anómalas.
   - Generar reportes mensuales con el uso de estas herramientas para identificar riesgos.
3. Revisión y actualización de políticas de acceso y uso de datos
   - Revisar las políticas IAM cada semestre, asegurándonos de que estas sigan cumpliendo las necesidades.
   - Asegurar que las cuentas con roles importantes esten protegidos bajo un MFA
4. Pruebas de vulnerabilidad
   - Realizar pruebas de seguridad periódicas usando herramientas como AWS Inspector para detectar configuraciones inseguras.

Conclusiones

La nube es actualmente parte fundamental del proceso de desarrollo de un software. Permite tener una arquitectura confiable y elástica, asegurándonos la seguridad de nuestros datos, y que estemos pagando únicamente por el uso que le estemos dado. El estar enterado de todas estas herramientas, y de los distintos proveedores de estas, nos permite escoger mejor cuál herramienta se ajusta mejor a nuestras necesidades y nuestro presupuesto, así haciendo una decisión más educada sobre que servicio de nube contratar.