Nadia Arellano G.
Ingeniera en Informática

Actividad – Sesión 1: Fundamentos de Seguridad Cloud

Parte 1: Preguntas Teóricas

1. **¿Qué es la autenticación multifactor (MFA) y por qué es importante en la seguridad cloud?**

(R). La autenticación MFA es un tipo de seguridad en donde el usuario debe proporcionar como mínimo 2 factores de verificación diferentes para acceder a un servicio o sistema. Por ejemplo: una contraseña más un código temporal en su celular o una huella digital o un reconocimiento facial. Es importante porque añade una capa adicional de protección a accesos no autorizados, incluso si una contraseña fue robada o filtrada.

2. **Explica la diferencia entre cifrado en reposo y cifrado en tránsito.**

(R). El Cifrado en Reposo protege los datos que están almacenados en discos duros, bases de datos, etc., en comparación con el Cifrado en Tránsito que protege los datos que se están transmitiendo entre sistemas como entre un servidor y un usuario o entre servicios cloud.

3. **¿Qué es la segmentación de redes y cómo contribuye a la seguridad cloud?**

(R). La segmentación de redes es cuando se divide una gran red en partes más pequeñas, teniendo cada una de estas partes reglas específicas de acceso y comunicación. Contribuye a la seguridad cloud limitando el acceso de los atacantes, ya que si logran entrar a una parte no pueden moverse con facilidad a otras que pueden ser importantes en la red. También ayuda a reducir el impacto de incidentes porque sólo afecta un área limitada y permite aplicar controles específicos por área.

4. **¿Por qué es importante la comunicación efectiva para un profesional de seguridad cloud?**

(R). Es importante la comunicación efectiva porque el profesional de seguridad cloud puede explicar los riesgos técnicos complejos de manera comprensible a personas que no tienen esa competencia técnica, por ejemplo, a gerentes o equipos de otras áreas. Esto ayuda a tomar mejores decisiones, a trabajar en un ambiente colaborativo y a fortalecer las respuestas ante incidentes de seguridad.

Parte 2: Caso Práctico

1. **Propón una solución para gestionar los accesos de los empleados y clientes a los sistemas en la nube.**

(R). Para gestionar el acceso de los empleados y clientes en la nube propongo usar autenticación MFA para que los empleados y clientes, además de su contraseña, deban ingresar un código adicional que les llegará a su celular. También permisos por rol en donde se asignarán permisos de acuerdo con el trabajo que realiza cada persona. Crear inicio de sesión único para varias plataformas, pero siempre con MFA activado, y finalmente realizar revisión de accesos para detectar intrusiones sospechosas.

Nadia Arellano G.
Ingeniera en Informática

2. **Describe cómo protegerías los datos financieros de la empresa, tanto en reposo como en tránsito.**

(R). Protegería los datos financieros aplicando cifrado en reposo, cifrado en tránsito y gestionando claves de forma segura, guardándolas y controlándolas adecuadamente con sistemas como KMS (Key Management System).

3. **Explica cómo configurarías la seguridad de la red para proteger la infraestructura cloud de la empresa.**

(R). También aplicaría reglas de acceso que permitan solo los accesos necesarios por zona. Activaría VPN para acceso remoto, asegurando conexiones seguras desde otras ubicaciones, y finalmente protegería contra ataques como DDoS activando herramientas que provee el servicio cloud para detectar y bloquear amenazas.