



Evaluación de Competencias Técnicas y Habilidades Personales en Seguridad Cloud

Parte 1: Preguntas Teóricas (4 puntos)

Responde las siguientes preguntas basadas en el contenido visto en clase:

1. Gestión de Identidades y Acceso (IAM) (1 punto):
 - ¿Qué es la autenticación multifactor (MFA) y por qué es importante en la seguridad cloud?

2. Protección de Datos y Cifrado (1 punto):
 - Explica la diferencia entre cifrado en reposo y cifrado en tránsito.

3. Seguridad de Redes en la Nube (1 punto):
 - ¿Qué es la segmentación de redes y cómo contribuye a la seguridad cloud?

4. Habilidades Personales (1 punto):
 - ¿Por qué es importante la comunicación efectiva para un profesional de seguridad cloud?



Parte 2: Caso Práctico (6 puntos)

Escenario:

Eres un profesional de seguridad cloud contratado por una empresa de servicios financieros que está migrando su infraestructura a la nube. La empresa necesita proteger sus datos sensibles y cumplir con regulaciones como PCI DSS. Tu tarea es diseñar una estrategia de seguridad cloud que incluya:

1. Gestión de Identidades y Acceso (IAM) (2 puntos)
 - Propón una solución para gestionar los accesos de los empleados y clientes a los sistemas en la nube.
2. Protección de Datos y Cifrado (2 puntos):
 - Describe cómo protegerías los datos financieros de la empresa, tanto en reposo como en tránsito.
3. Seguridad de Redes (2 puntos):
 - Explica cómo configurarías la seguridad de la red para proteger la infraestructura cloud de la empresa.

Instrucciones:

- Puntaje total: 10 puntos.
- Entregables: Un documento en formato PDF con las respuestas a las preguntas y la solución del caso práctico.