Nadia Arellano G.
Ingeniera en Informática

Evaluación Final – Módulo 2: Fundamentos de Seguridad

Sección 1: Preguntas de Verdadero o Falso con justificación

1. Los principios CIA son independientes entre sí y no requieren consideración conjunta en entornos de nube.
   (Falso). Los principios de Confidencialidad, Integridad y Disponibilidad forman una triada interrelacionada que debe aplicarse de forma conjunta. Una debilidad en uno afecta a los otros. Por ejemplo, si un sistema pierde disponibilidad, no se puede verificar la integridad ni acceder a datos confidenciales.

2. El modelo de responsabilidad compartida establece que la configuración de cifrado de datos en una base de datos gestionada en un modelo PaaS es responsabilidad del cliente.
   (Verdadero). En el modelo PaaS, el proveedor se encarga de la gestión general de la base de datos. Sin embargo, el cliente es responsable de los datos, incluyendo su cifrado, configuración de accesos y administración de usuarios.

3. Las normativas como HIPAA e ISO/IEC 27001 no tienen impacto directo en la adopción de servicios en la nube.
   (Falso). Normativas como HIPAA e ISO/IEC 27001 sí tienen un impacto directo en la adopción y uso de servicios en la nube, ya que imponen requisitos específicos de seguridad, control y cumplimiento normativo. Las organizaciones que almacenan o procesan datos sensibles deben asegurarse de que sus proveedores cloud cumplan con estas normativas.

Sección 2: Análisis de Caso Práctico

Una empresa financiera utiliza un modelo de nube híbrida para gestionar datos de sus clientes. Recientemente, la empresa experimentó una filtración de datos confidenciales debido a configuraciones incorrectas de permisos en su nube pública. Además, el sistema estuvo fuera de servicio durante 8 horas debido a un ataque de denegación de servicio (DDoS).

1. Identifique qué principios CIA se vieron comprometidos en este incidente y justifique.
   (R). Se vieron comprometidos dos principios de la triada CIA: Confidencialidad, porque fue afectada por la filtración de datos confidenciales debido a configuraciones incorrectas de permisos en la nube pública y Disponibilidad, porque provocó una interrupción del sistema durante 8 horas impidiendo que los servicios estuvieran accesibles para los usuarios legítimos.

2. ¿Qué medidas de mitigación podría implementar la empresa para evitar configuraciones incorrectas de permisos?
   (R). Capacitación del personal en el modelo de responsabilidad compartida porque el equipo de TI debe comprender cuáles son sus responsabilidades al operar en la nube híbrida e implementación de herramientas de monitoreo automatizado para identificar configuraciones incorrectas en tiempo real.

Nadia Arellano G.
Ingeniera en Informática

3. ¿Qué estrategia recomendaría para minimizar los efectos de futuros ataques DDoS?
(R). Recomendaría una estrategia basada en: Uso de servicios de mitigación DDoS ofrecidos por el proveedor cloud junto con: Balanceo de carga, escalabilidad automática y monitoreo en tiempo real.