DEFINICION Y EJEMPLOS

Confidencialidad

Definición: Garantiza que solo las personas autorizadas puedan acceder a la información.

Ejemplo: En un hospital, los historiales médicos deben estar protegidos para que solo médicos autorizados puedan verlos.

Integridad

Definición: Asegura que la información no sea modificada de forma no autorizada.

Ejemplo: Un cambio no detectado en el diagnóstico médico o en una orden de compra online puede tener consecuencias graves.

Disponibilidad

Definición: Garantiza que la información esté accesible cuando se necesite.

Ejemplo: Si los sistemas de un hospital o tienda online están caídos, no se puede atender a los pacientes o procesar ventas.

Pregunta 1:

¿Qué concepto consideras más crítico en una empresa de salud? ¿Y en una empresa de comercio electrónico?

Empresa de salud:

Confidencialidad

Porque el acceso indebido a los datos de pacientes puede violar leyes como HIPAA (en EE.UU.) o la Ley de Protección de Datos (en otros países).

Empresa de comercio electrónico:

Disponibilidad

Porque si el sistema no está disponible, se pierden ventas y la reputación se daña rápidamente.

Pregunta 2:

¿Cómo podrías priorizar la implementación ?

Evaluar el tipo de datos y servicios críticos.

Confidencialidad primero si se manejan datos sensibles.

Integridad si los datos son operativos o de toma de decisiones.

Disponibilidad si la continuidad del negocio depende de sistemas en línea.

Ejemplo: En una clínica: primero Confidencialidad, luego Disponibilidad, y finalmente Integridad (aunque todos son importantes).

En un e-commerce: primero Disponibilidad, luego Integridad, y después Confidencialidad.

Definición: Código malicioso que se adjunta a un archivo legítimo y se propaga al ejecutarlo.

Ejemplo: Un virus adjunto a un documento de Word que se ejecuta al abrir el archivo.

**Gusano (Worm)**

Definición: Malware que se replica por sí solo a través de redes, sin necesidad de que el usuario lo ejecute.

Ejemplo: El gusano ILOVEYOU que se propagó por correo electrónico sin intervención del usuario.

**Troyano (Trojan)**

Definición: Se presenta como un programa legítimo pero contiene código malicioso oculto.

Ejemplo: Un supuesto “juego gratuito” que en realidad instala un keylogger.

**Ransomware**

Definición: Secuestra los datos del sistema cifrándolos y exige un pago (rescate) para devolver el acceso.

Ejemplo: El ransomware WannaCry que afectó a hospitales y empresas en todo el mundo.

**Spyware**

Definición: Programa que espía al usuario y recopila información sin su conocimiento.

Ejemplo: Software que registra pulsaciones de teclado o historial de navegación para enviarlo a un tercero.

CURSO CISCO

