Leonis Manuel Diaz Pacheco

Laboratorio 2

**Parte 1**

**Definición:**

**Confidencialidad**: la confidencialidad es proteger información para que solo las personas que tengan acceso a esa información puedan verla.

**Integridad**: la información debe mantenerse sin modificación en el tiempo que este guardad en el sistema.

**Disponibilidad**: La disponibilidad es el hecho de que la información y los sistemas estén siempre accesibles cuando sean necesarias, sin interrupciones.

**Pregunta 1:** ¿Que concepto consideras más crítico en una empresa de salud? ¿Y en una empresa de comercio electrónico?

- En una empresa de salud el concepto más crítico seria la confidencialidad debido a que contiene información muy personal de las personas.
- En una empresa de comercio electrónico el concepto más crítico seria la Disponibilidad, porque los sistemas deben estar siempre accesibles y sin interrupciones, cuando los clientes decidan realizar compras.

**Pregunta 2**: ¿Cómo podrías priorizar la implementación a una empresa con recursos limitados?

Prioriza el pilar de la triada CIA más alineado al giro de tu negocio y comienza con controles simples pero impactantes.

**Parte 2**

Definición y Ejemplos (Malware):

- Virus: Es un programa malicioso que para funcionar requiere que un usuario active el archivo o programa legitimo al que esta adherido, una vez activado puede dañar archivos, ralentizar el sistema, mostrar mensajes molestos o borrar información.
    - Ejemplo: Melissa (1999) - Era un virus que infectaba documentos de Microsoft Word. Se propagaba por correo electrónico: cuando abrías el archivo, se enviaba automáticamente a los primeros 50 contactos de tu libreta de Outlook.

- Gusano: Es un Programa malicioso que se propaga solo sin necesidad de la interacción del usuario, este Malware se replica a través de redes o dispositivos conectados.
    - Colapsa redes, consume ancho de banda, instala puertas traseras, etc.
        - Ejemplo: *WannaCry* (2017) — se propagaba automáticamente a través de redes Windows vulnerables y cifraba los archivos.

- Troyano: Es un Programa legítimo que esconde un código Malicioso, engañando al usuario cuando los instala creyendo que es útil.
    - Permite el acceso remoto al atacante, roba información o instala más malware.
        - Ejemplo: *Emotet* — se presentaba como factura de Word o PDF, pero al abrirlo, robaba contraseñas y datos bancarios.

- Rasonware: Es un malware que bloquea los archivos o programas de un usuario exigiendo un rescate económico para desbloquearlos.
    - Inutiliza tu equipo o archivos hasta que pagues (en criptomonedas, generalmente).
        - Ejemplo: CryptoLocker (2013): Infectaba computadoras a través de correos electrónicos con archivos adjuntos falsos (como PDF o ZIP). Al abrir el archivo, cifraba todos los documentos del usuario y mostraba un mensaje pidiendo un rescate en bitcoins.
        - Fue uno de los primeros ransomware que popularizó el pago con criptomonedas y dio lugar a muchas variantes modernas.

- Spayware: Es un software que guarda tu actividad en internet y se instala en un computador sin que el usuario lo sepa.
    - Roba información personal, financiera o de comportamiento en línea.
        - Ejemplo: *CoolWebSearch* — un spyware que cambiaba la página de inicio del navegador redirigía búsquedas y espiaba la actividad del usuario.

**Parte 3**

Leonis Manuel Diaz Pacheco