

## **Paso 1.**

### **Diferenciar entre confidencialidad Integridad y Disponibilidad.**

**Confidencialidad:** proceso que se debe llevar para datos e información sensible en el se debe cumplir con el control de acceso y autenticación para preservar la privacidad de los datos, también cifrarlos para evitar que puedan ser divulgados o robados.

**Integridad:** esta se refiere a la que los datos estén en perfectas condiciones, para lograr verificar que la integridad es correcta se usan diferentes métodos como los de Suma de verificación, hashes, firmas digitales y control de versiones esto para corroborar la integridad y si se encuentra comprometida el control de versiones será útil para ver en que momento el dato se volvió corrupto.

**Disponibilidad:** en esta se habla sobre que el servicio este disponible todo el tiempo un claro ejemplo es un banco debe tener una disponibilidad alta o una plataforma de rastreo vehicular deben tener una disponibilidad superior a un 99.5% para generar una confianza en sus clientes, la disponibilidad es algo esencial en cualquier sistema que tenga un flujo continuo, esto se logra con métodos como la redundancia, sistemas de respaldo y planificación ante cualquier tipo de desastres la creación de planes de respaldo y a seguir para estar online lo más rápido posible y con esto poder lograr una disponibilidad muy alta

## **Paso 2.**

### **Confidencialidad Ejemplo:**

Una empresa del sector salud debe proteger los **registros médicos de los pacientes**, ya que contienen información personal, diagnósticos, tratamientos y más datos altamente sensibles.

### **Aplicación práctica (cifrado):**

Para asegurar esta información, se implementa **cifrado de extremo a extremo**. Esto significa que cuando los datos son almacenados o transmitidos, son convertidos en un formato ilegible a menos que se tenga la **clave de descifrado adecuada**.

Solo el personal médico autorizado posee credenciales y permisos para acceder a esta información, lo cual se refuerza con mecanismos como:

- **Autenticación multifactor (MFA).**
- **Roles y permisos definidos en el sistema.**
- **Bitácoras de acceso** para rastrear quién vio qué y cuándo.

*Ejemplo técnico sería la implementación de Cifrado AES-256 en bases de datos y conexiones HTTPS/TLS para transmitir datos.*


**Ejemplo Integridad:** Una empresa de software como Microsoft o Red Hat necesita distribuir sus productos (como sistemas operativos o aplicaciones) de manera que los usuarios estén seguros de que **no han sido modificados maliciosamente**.

**Aplicación práctica (hashes):**

Cuando se descarga un archivo de instalación desde la web, también se proporciona un valor **hash**. Este valor es como una huella digital única del archivo original.

El usuario puede generar el hash del archivo que descargó y compararlo con el que proporciona la empresa:

- Si coinciden, el archivo **no ha sido alterado**.
- Si difieren, el archivo podría estar **corrupto o manipulado maliciosamente**.

 *Ejemplo técnico sería el sha256sum archivo.iso de Linux.*

**Disponibilidad Ejemplo:**

Un banco necesita garantizar que sus clientes puedan acceder a los servicios de **banca en línea 24/7**, sin importar si ocurre una falla de hardware o un ataque o un desastre.

**Aplicación práctica (redundancia y respaldo):**

El banco implementa:

- **Servidores redundantes.**
- **Balanceadores de carga**
- **Respaldos automáticos y constantes** de los datos críticos.
- **Planes de recuperación ante desastres**

*Ejemplo técnico:* tener respaldos múltiples y un plan de recuperación

## LAB 2.1

### Virus

**Definición:** Programa malicioso que **se adhiere a archivos legítimos** y se propaga al ejecutarlos

**Ejemplo:**

Un virus oculto en un archivo .exe descargado de un sitio pirata que, al ejecutarse, daña archivos del sistema.

### Gusano

**Definición:** Malware que se **reproduce automáticamente** y se propaga por redes.

**Ejemplo:**

El **gusano WannaCry** se propagó por redes Windows aprovechando una vulnerabilidad, infectando miles de equipos en horas.

### Troyano

**Definición:** Se hace pasar por un programa legítimo, pero en realidad es malicioso.

**Permite acceso remoto o robo de datos.**

**Ejemplo:**

Un supuesto "activador de Windows" que en realidad es un troyano que le da acceso al atacante para controlar tu PC.

### Ransomware

**Definición:** Malware que **cifra tus archivos** y pide un rescate para recuperarlos. Es un secuestro digital.

**Ejemplo:**

Te llega un correo con un archivo Word infectado. Lo abres, y todos tus documentos se cifran. Luego aparece un mensaje pidiendo bitcoins para liberarlos.

### Spyware

**Definición:** Software espía que **roba información** como contraseñas, historial, hábitos de navegación sin que el usuario lo sepa.

**Ejemplo:**

Instalas una app gratuita y sin saberlo empieza a registrar tus teclas (keylogger), robando tus datos.

Paso 3

Curso De Cisco

