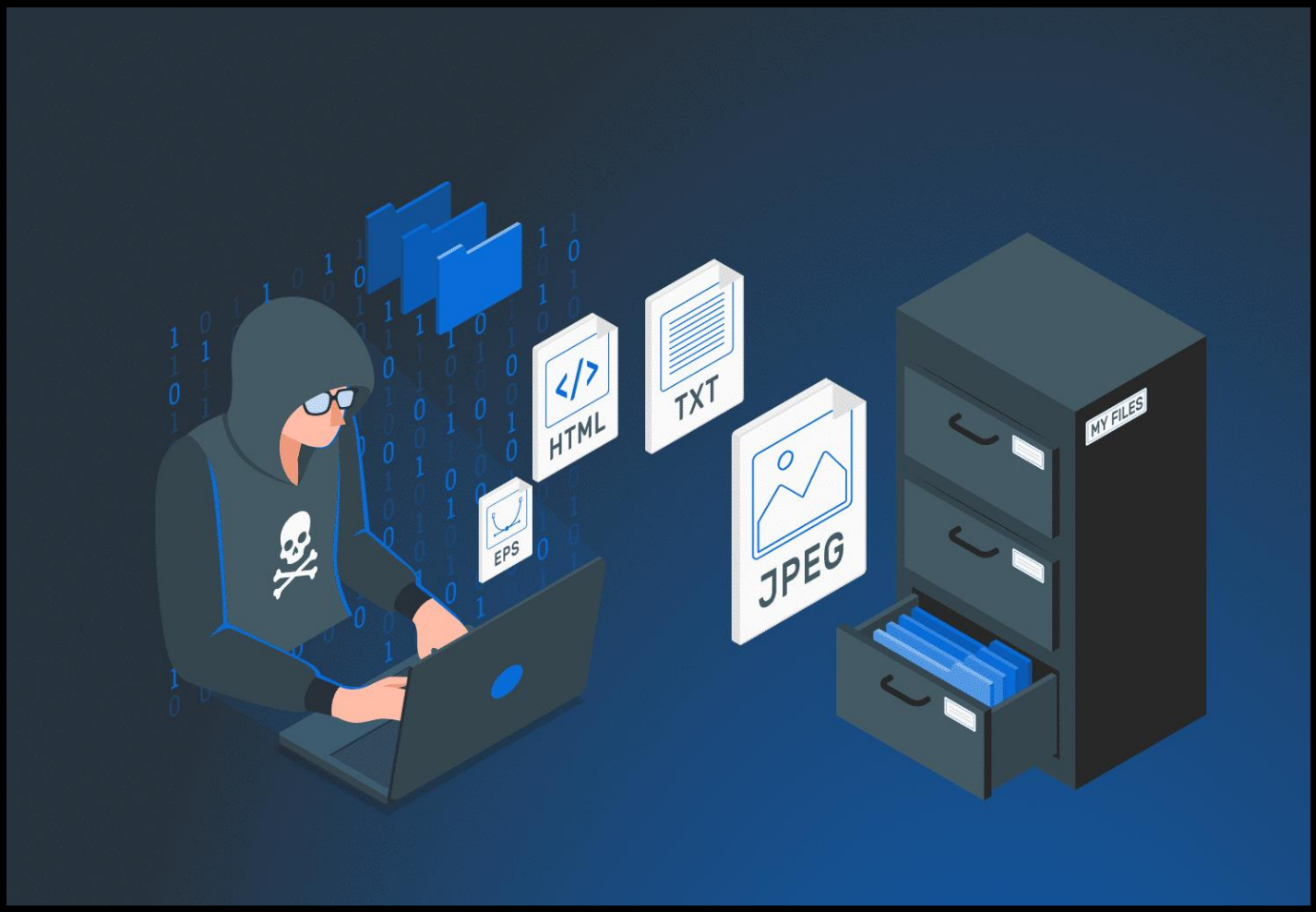

1.1 CASOS REALES

Hecho por: Izan Navarro

INDICE

EJERCICIO 1

Casos reales – Identifica el principio vulnerado

Lee las siguientes situaciones reales y marca qué principio de la ciberseguridad se vulnera en cada una. Después busca en la prensa digital un caso real reciente de cada uno de los principios.

1-Un hacker accede a la base de datos de un hospital y filtra los historiales médicos de los pacientes -->

Vulnera la **Confidencialidad** ya que expone al público datos que son confidenciales ya sea por acto intencionado o por fallo del sistema.

2-Un empleado cambia los datos de las nóminas para aumentarse el sueldo -->

Se vulnera la **integridad** de las nóminas ya que un empleado las modifica sin autorización previa.

3-Un ciberataque DDoS deja sin servicio la web del ayuntamiento durante dos días -->

Esta es una vulnerabilidad de **Disponibilidad** ya que deja al público sin posibilidad de acceso a una web, y así, sin poder mostrar los datos.

4-Se pierden los datos de un cliente porque el sistema no tenía copias de seguridad -->

Esta es otra vulnerabilidad de **Disponibilidad** ya que, al no realizarse copias de seguridad, los datos del cliente son irrecuperables

5-Una persona ajena a la empresa entra en la red Wi-Fi corporativa y lee los correos internos -->

Este caso vulnera la **Autenticación** de acceso al sistema, dejando entrar a una persona ajena a la empresa y también vulnera la **Confidencialidad**, ya que esta persona está accediendo a datos de la empresa sin autorización

EJERCICIO 2

Identifica la amenaza

Indica qué principio se ve amenazado en cada caso:

a) Un atacante roba contraseñas de usuarios -->

Este caso amenaza a la confidencialidad de la información y a la autenticación de acceso del sistema, ya sea de manera intencionada o no.

b) Un virus modifica los archivos del sistema -->

Este caso amenaza la Integridad de la información, modificando datos confidenciales que no deben ser tocados

c) Una tormenta provoca un corte eléctrico en el servidor -->

Esto genera una vulnerabilidad de Disponibilidad ya que esta falta de recursos va a generar problemas de accesibilidad de los usuarios.

d) Un empleado copia datos personales sin permiso -->

Este caso vulnera la confidencialidad de los datos ya que se cogen estos datos confidenciales y la persona no tiene esa autorización

e) Un ataque DDoS satura un sitio web y lo deja fuera de servicio -->

Este caso vulnera la Disponibilidad de los datos ya que deja al público sin acceso a la web y su información.

EJERCICIO 3

Medidas de protección

Empareja cada medida con el principio que protege principalmente:

Medida de seguridad	Principio protegido
Uso de copias de seguridad (backups)	**Disponibilidad**: acceso cuando quieras a la información.
Cifrado de datos (SSL/TLS, AES…)	**Confidencialidad**: Cifrado de la información para impedir la lectura en el acceso no autorizado
Control de acceso mediante contraseñas seguras	**Autenticación**: Solo pueden acceder usuarios autorizados
SAI (Sistema de Alimentación Ininterrumpida)	**Disponibilidad**: Permite al sistema no parar y trabajar de manera ininterrumpida
Verificación de integridad (hash, firmas digitales)	Integridad: Verificar que la información no ha sido alterada por ningún usuario

EJERCICIO 4

Reflexión

Responde brevemente:

1. ¿Por qué es importante aplicar medidas de seguridad en los tres principios a la vez?

Aplicar medidas de seguridad en los tres principios al mismo tiempo es importante porque están interrelacionados. Si uno falla, los demás pueden verse afectados. Por ejemplo:

- Si se protege la confidencialidad, pero no la disponibilidad, entonces los datos están seguros, pero no accesibles cuando se necesitan (lo que puede ser crítico en emergencias).
- Si se garantiza la disponibilidad, pero no la integridad, podrías tener acceso rápido a datos... pero alterados o corruptos.

2. Pon un ejemplo real (de tu entorno o de la actualidad) en el que se haya vulnerado alguno de ellos y qué medida de seguridad la habría evitado.

En 2021, el sistema de salud de Irlanda (HSE) sufrió un ciberataque tipo **ransomware** (malware que secuestra los archivos o sistemas) que afectó gravemente sus servicios.

- **¿Qué se vulneró?**
  - **Disponibilidad**: Muchos sistemas quedaron inactivos, citas médicas se cancelaron, y los hospitales no pudieron acceder a historiales clínicos.
  - **Confidencialidad**: Datos de pacientes fueron robados.
  - **Integridad**: Algunos archivos fueron alterados o bloqueados.
- **Medidas de seguridad que lo habrían evitado:**
  - Uso de **copias de seguridad (backups)** actualizadas y protegidas.
  - **Antivirus** y sistemas de detección de intrusos.
  - **Capacitación del personal** para evitar caer en correos maliciosos (phishing).
  - **Actualizaciones frecuentes** de software para corregir vulnerabilidades.