

## **Actividad 03. Amenazas,** **vulnerabilidades e incidentes de** **seguridad informática**

- [1. Describe con tus propias palabras estos tres conceptos y pon algún ejemplo de cada uno de ellos.](#)
- [2. En la carpeta compartida por el docente añade, al menos, dos amenazas, las posibles vulnerabilidades y contramedidas de las mismas.](#)

### **1. Describe con tus propias palabras estos tres conceptos y pon algún ejemplo de cada uno de ellos.**

#### **AMENAZAS**

Cualquier cosa que pueda potencialmente causar daño a una red informática o sistema. Pueden ser intencionadas (hackers) o accidentales (error humano, desastre natural, etc.)

EJEMPLO: Hacker que intenta acceder a la red de una empresa para robar datos sensibles de la misma. Puede usar técnicas como el phishing para obtener credenciales de empleados o lanzar un ataque de fuerza bruta para así romper contraseñas y acceder fácilmente.

#### **VULNERABILIDADES**

Debilidades o fallos en un sistema informático que pueden ser explotados por amenazas que pueden causar daño o para acceder a la información no autorizada. Pueden estar presentes el hardware, software, redes o incluso en las políticas y procedimientos.

EJEMPLO: Software sin actualizar que contiene un bug conocido y que permite la ejecución de código malicioso. Si el software no se parchea mediante actualizaciones de seguridad proporcionadas por el proveedor, un atacante podría explotar esa vulnerabilidad para tomar el control del sistema.

**INCIDENTES DE SEGURIDAD**

Eventos que comprometen a la integridad, confidencialidad o disponibilidad de la información. Pueden resultar de amenazas que puedan explotar vulnerabilidades del sistema.

EJEMPLO: Ataque de ransomware en el que el atacante logra cifrar los datos de la empresa y exige un rescate para proporcionar la clave de descifrado. El incidente ha comprometido la disponibilidad de la información de la empresa, afectando así a las operaciones hasta que se resuelva dicho problema.

**2. En la carpeta compartida por el docente  
añade, al menos, dos amenazas, las  
posibles vulnerabilidades y contramedidas  
de las mismas.**

**AMENAZA:** Ataque por canal lateral

**VULNERABILIDAD:** Dispositivos que emiten señales y pueden ser analizados-hackeados

**CONTRAMEDIDA:** Blinding (encriptar temporalmente los datos y consumiendo tiempo de ejecución a las operaciones para dificultar al atacante)

**AMENAZA:** Clickjacking

**VULNERABILIDAD:** Aplicaciones web fraudulentas para "falsificar" el producto

**CONTRAMEDIDA:** Verificar que los encabezados de las páginas utilicen la seguridad "HTTPS"