# Seguridad y Alta Disponibilidad

T0 - Práctica- (Trabajo de investigación) Ampliación de amenazas y análisis de ataques al Internet de las Cosas (IoT)

## Parte 1: Ampliación de la lista de amenazas

Investiga y amplía la lista de amenazas cibernéticas, añadiendo otras que consideres relevantes o que hayas encontrado en noticias recientes. Las nuevas amenazas deben ser actuales y reflejar la evolución de los riesgos de seguridad en el entorno digital.

**Amenazas cibernéticas más comunes:**

- **Malware:** Virus, ransomware, troyanos que infectan dispositivos y sistemas.
- **Phishing:** Engaños por correo electrónico o mensajes para robar datos personales.
- **Ingeniería social:** Manipulación psicológica para obtener información confidencial.
- **Ataques DDoS:** Intentos de sobrecargar servidores para dejarlos fuera de servicio.

**Nuevas amenazas en auge:**

- **Ataques a la cadena de suministro:** Compromiso de proveedores para acceder a sistemas.
- **Ataques a la nube:** Explotación de vulnerabilidades en servicios en la nube.
- **Ataques a IoT:** Explotación de dispositivos conectados a internet.
- **Deepfakes:** Creación de contenido falso para engañar o difamar.
- **Ataques a 5G:** Explotación de vulnerabilidades en redes 5G.
- **Criptojacking:** Uso no autorizado de dispositivos para minar criptomonedas.

**Amenazas emergentes:**

- **Ataques basados en IA:** Uso de inteligencia artificial para crear malware más sofisticado.
- **Biometría sintética:** Creación de datos biométricos falsos para burlar sistemas de seguridad.
- **Ataques a blockchain:** Explotación de vulnerabilidades en redes blockchain.

## Parte 2: Investigación de ataques al Internet de las Cosas (IoT)

Realiza una investigación sobre ataques recientes a dispositivos del Internet de las Cosas (IoT). Encuentra noticias actuales que detallen incidentes de seguridad, brechas de privacidad o vulnerabilidades en dispositivos conectados como cámaras de seguridad, electrodomésticos inteligentes, automóviles conectados, etc.

Los dispositivos IoT son cada vez más vulnerables a ataques cibernéticos, esto se debe a varias razones:

- **Falta de seguridad:** Muchos dispositivos se diseñan con medidas de seguridad mínimas, como contraseñas débiles o sin actualizaciones de software regulares.
- **Gran cantidad de dispositivos:** La enorme cantidad de dispositivos conectados dificulta su protección individual.

**Tipos de ataques comunes:**

- **Ransomware:** Se encriptan los datos del dispositivo para exigir un pago.
- **Botnets:** Los dispositivos se utilizan para realizar ataques a gran escala.
- **Espionaje:** Los atacantes espían a los usuarios a través de las cámaras y micrófonos de los dispositivos.
- **Manipulación de datos:** Se alteran los datos que envía el dispositivo, como envenenar alimentos.

**Consecuencias de estos ataques:**

- **Pérdida de privacidad:** Los atacantes pueden acceder a información personal.
- **Pérdidas económicas:** Se pueden producir gastos por reparaciones o rescate de datos.
- **Daños físicos:** En algunos casos, los ataques pueden causar daños a personas o propiedades.
- **Disrupción de servicios:** Se pueden interrumpir servicios esenciales.

**Cómo protegerse:**

- **Cambia las contraseñas por defecto:** Utiliza contraseñas fuertes y únicas.
- **Mantén el software actualizado:** Instala todas las actualizaciones de seguridad disponibles.
- **Utiliza una red Wi-Fi segura:** Protege tu red con una contraseña fuerte y encriptación.
- **Segmenta tu red:** Crea una red separada para tus dispositivos IoT.

- **Investiga la reputación de los fabricantes:** Elige dispositivos de marcas confiables.

**En resumen,** la seguridad de los dispositivos IoT es un problema creciente. Es fundamental tomar medidas para proteger nuestros dispositivos y nuestra información personal.