Julio 2025

Boletín Asociados de negocio

THOR LTDA
SEGURIDAD PRIVADA

Ciberdelincuencia

La ciberdelincuencia es una actividad delictiva que tiene como objetivo principal un ordenador, una red asociada a este o un dispositivo conectado. No obstante, aunque la creencia más arraigada en la sociedad es que es llevada a cabo por individuos o ciberdelincuentes, la ciberdelincuencia también puede ser practicada por organizaciones.

¿Cuál es su objetivo?

Su objetivo principal es, eso sí, el mismo: dañar dispositivos o sistemas de usuarios u organizaciones con fines de lucro, personales o políticos.

Tipos de ciberdelitos

- **Ciberdelincuencia pura o contra la seguridad:**
Aquellos actos dirigidos contra sistemas informáticos de particulares, empresas o gobiernos con el objetivo de vulnerar la integridad del sistema y la confidencialidad de los datos que se almacenan y gestionan.

- **Ciberdelincuencia clásica:**
Aquellos ataques que se sirven de medios digitales para cometer delitos tradicionales, como la estafa, amenazas, acoso, extorsión, fraude, venta de productos falsos, entre otros.

- Fraudes por correo electrónico e Internet, conocido como phishing.

- Ciberextorsión para exigir dinero para evitar una amenaza o recuperar información robada.

- Cryptojacking, donde los ciberatacantes minan criptodivisas utilizando recursos que no les pertenecen.

- Malware, y entre él el más extendido y que más afecta a las organizaciones de todo el mundo: el ransomware.

¿ Cómo evitar la Ciberdelincuencia?

La mejor manera de protegerse es **adoptar hábitos digitales cuidadosos y sensatos.**

1. Desconfiar de los correos electrónicos con archivos adjuntos o enlaces dudosos.

2. No descargar los archivos de los correos ni pinchar en dichos enlaces a menos que se conozca el emisor, ya que pueden contener malware.

3. No instalar aplicaciones de fuentes desconocidas.

4. Evitar la conexión a redes WiFi públicas o gratuitas.

5. Utilizar contraseñas robustas y no reutilizar la misma en varias cuentas.

6. Tener instalado y actualizado el sistema antivirus.

7. Realizar simulacros periódicos.