Hackers

Lo que muestran las películas y lo que pasa en la realidad.

El hacker de las películas no es toda la historia

Cuando pensamos en un hacker, solemos imaginar a alguien encapuchado, frente a una pantalla llena de código, que entra a sistemas en segundos. Esa escena tiene algo de real, pero es solo una pequeña parte de la historia.

En su origen, la palabra *hacker* no tenía que ver con el delito: se refería a personas con un conocimiento profundo de la tecnología, que disfrutan entender cómo funcionan los sistemas y resolver problemas complejos.

La diferencia no está en lo que saben hacer, sino en **cómo usan ese conocimiento**. Por eso, bajo la misma palabra conviven perfiles muy distintos: desde quienes protegen sistemas hasta quienes intentan vulnerarlos.

Los que protegen: hackers éticos

Muchos profesionales trabajan del lado de la seguridad. Se los conoce como **hackers éticos** o especialistas en ciberseguridad. Su trabajo es:

- Analizar sistemas, aplicaciones e infraestructuras.
- Detectar vulnerabilidades antes de que alguien las aproveche.
- Reportar los hallazgos para que se corrijan.

Empresas, bancos y organismos públicos recurren a estos perfiles para fortalecer sus sistemas. Gracias a ese trabajo, muchas veces invisible, los servicios digitales que usás todos los días son más seguros. Es una actividad profesional, con formación específica, metodologías definidas y marcos legales claros.

Los que atacan: ciberdelincuentes

En el otro extremo están los **ciberdelincuentes**, que entran a sistemas sin autorización para robar información, obtener dinero o extorsionar a personas y organizaciones.

No siempre actúan solos: muchas veces operan en grupos organizados, con roles definidos y herramientas creadas para atacar a gran escala. Gran parte de las amenazas actuales se basa en:

- **Procesos automatizados** que recorren Internet en busca de dispositivos vulnerables.
- **Engaños,** como correos o sitios falsos, para que las personas entreguen información sin darse cuenta.

Por eso, no hace falta ser un objetivo específico: cualquier dispositivo desprotegido puede ser aprovechado.

Zonas grises

Hay casos intermedios: personas que entran a sistemas sin autorización pero sin intención de causar daño, por curiosidad o para reportar una falla. Aun así:

- El acceso sin permiso sigue siendo ilegal.
- Puede exponer vulnerabilidades antes de que se corrijan.
- Puede facilitar que terceros malintencionados usen esa información.

La investigación de seguridad siempre tiene que hacerse dentro de marcos legales y autorizados.

¿Qué tiene que ver esto con vos?

Cualquier dispositivo conectado puede interesarle a un atacante, aunque no tenga información sensible. Un equipo comprometido puede usarse para:

- Sumarse a redes de dispositivos controlados a distancia (**botnets**).
- Consumir recursos para actividades como la minería de criptomonedas.
- Servir de intermediario para ocultar otras acciones maliciosas.

Esto incluye computadoras y celulares, pero también routers, cámaras, televisores inteligentes y otros dispositivos del Internet de las cosas (IoT).

Cómo protegerte sin ser experto

- Mantené actualizados tus dispositivos y aplicaciones.
- Usá contraseñas robustas y distintas para cada servicio.
- Activá la autenticación en dos pasos (2FA) siempre que puedas.
- Cambiá las contraseñas que vienen de fábrica, sobre todo en routers y dispositivos IoT.
- Desconfiá de mensajes, enlaces o archivos inesperados, aunque parezcan venir de contactos conocidos.

La figura del hacker de las películas es una simplificación: el conocimiento técnico puede usarse para proteger o para atacar. La seguridad no depende solo de especialistas; el uso responsable de la tecnología es clave para reducir incidentes. Desde **BA-CSIRT** te acompañamos.