GUÍA DE PROTECCIÓN

USB Killer: la memoria que fríe tu equipo en segundos.

Se ve exactamente igual a una memoria USB normal. Pero en vez de guardar archivos, carga capacitores internos y descarga hasta -220V directo a los puertos de tu equipo — sin necesitar ningún software, ningún clic, ningún permiso.

01 — CÓMO FUNCIONA REALMENTE

⚡ **Carga y descarga en ciclos, no una sola vez**

Al conectarse, el dispositivo usa la energía del propio puerto USB para cargar capacitores internos, y los descarga de inmediato hacia las líneas de datos — repitiendo el ciclo varias veces por segundo.

🔥 **No es un ataque de software — es daño físico directo**

No hay virus, no hay malware que detectar. El voltaje inverso destruye directamente los componentes electrónicos del puerto y, en la mayoría de los casos, la tarjeta madre completa.

💀 **El daño suele ser irreversible y no cubierto por garantía**

Al ser daño físico intencional por una fuente externa, la mayoría de las garantías de fabricante no lo cubren — es pérdida total del equipo en la mayoría de los casos.

02 — DÓNDE APLICA ESTE RIESGO

RIESGO 01

Equipos públicos o compartidos

Cafés internet, kioscos de renta de equipo, computadoras de uso común en oficinas u hoteles — cualquier puerto USB accesible a desconocidos.

RIESGO 02

Estaciones de carga públicas

Puertos USB de carga en aeropuertos, cafeterías o transporte público pueden estar comprometidos con este mismo principio de descarga.

RIESGO 03

Sabotaje interno o competencia desleal

Un empleado descontento o un tercero con acceso físico puede destruir equipo de cómputo sin dejar rastro de malware ni acceso remoto.

RIESGO 04

Se consigue sin restricción en línea

Estos dispositivos se venden abiertamente como "probadores de puertos USB" en tiendas en línea internacionales, sin control real de para qué se usan.

03 — CÓMO PROTEGERTE (INVERSIÓN MÍNIMA)

✓ **Nunca conectes USBs desconocidas** — ni siquiera "para ver qué tiene", así empezó la mayoría de estos casos documentados.

✓ **Usa bloqueadores de datos USB ("USB condoms")** en puertos de carga públicos — permiten energía pero bloquean líneas de datos.

✓ **Restringe físicamente los puertos USB** en equipos de acceso público de tu negocio con candados de puerto o deshabilitación por software.

✓ **Capacita a tu personal** — la mayoría de los ataques exitosos ocurren porque alguien encontró la memoria "tirada" y la conectó por curiosidad.

// REGLA DE ORO

Una memoria USB que encontraste tirada nunca debe conectarse — ni para ver de quién es.

Es la forma más común en que este ataque llega a oficinas y equipos personales.