Ciberataque

Tus archivos, rehenes

Versión online y actualizada

08:31 · TU ESCRITORIO 08:31. Abres el portátil y el fondo de pantalla ya no es el tuyo. Letras rojas. Una cuenta atrás: 71:59:43. «Tus archivos han sido cifrados». Te acuerdas del correo de ayer, el que parecía del banco. El móvil vibra: un SMS pide «confirmar un código». Otro. Otro más. El ratón todavía se mueve. Tus fotos tienen extensiones que no reconoces. **El instinto te dice que pagues. No toques nada hasta leer esto.**

Lo primero

1. **Desconecta** de internet el dispositivo afectado (wifi y cable). No lo apagues si hay ransomware.
2. **No pagues** ningún rescate ni sigas instrucciones de los atacantes.
3. Llama a tu **banco** si puede haber acceso a tus cuentas o tarjetas.
4. Pide ayuda gratis al **017** (INCIBE, Tu Ayuda en Ciberseguridad).

1 Si el ataque es contra ti

PRIMEROS 30 MINUTOS

- [ ] **Aísla el equipo: desconecta wifi y cable de red. No conectes memorias USB ni discos de copia de seguridad a ese equipo.**
- [ ] **Desde otro dispositivo limpio, cambia la contraseña del correo electrónico primero (es la llave de todo) y después la del banco y las redes sociales. Activa la verificación en dos pasos.**
- [ ] Llama a tu banco por el teléfono oficial (el de la tarjeta o su web, nunca el de un SMS) para bloquear tarjetas y revisar movimientos.
- [ ] Haz capturas de pantalla de mensajes, correos y cargos: son pruebas.
- [ ] Avisa a tus contactos si te han suplantado en WhatsApp o redes.

2 Las horas siguientes

MISMO DÍA

- [ ] Llama al 017 o escribe a INCIBE para recibir orientación gratuita y confidencial.
- [ ] Denuncia ante la Policía Nacional o la Guardia Civil, sobre todo si hay pérdidas económicas.
- [ ] Restaura archivos solo desde copias de seguridad que no estuvieran conectadas durante el ataque.
- [ ] Revisa sesiones abiertas y dispositivos vinculados en tus cuentas principales y ciérralos.

3 Si el ataque es masivo

CAÍDA DE SERVICIOS

- [ ] Ten efectivo para unos días: tarjetas, Bizum y cajeros pueden fallar.
- [ ] **Desconfía de cualquier SMS, llamada o correo que «te ayude» con el problema: los estafadores aprovechan las crisis.**

- [ ] Infórmate solo por canales oficiales (INCIBE, tu banco, el Gobierno) y medios reconocidos.
- [ ] Si tienes citas médicas o trámites, llama o acude en persona antes de dar nada por perdido.

NO hagas

- ✕ Pagar rescates: no garantiza recuperar nada y financia nuevos ataques.
- ✕ Pulsar enlaces de SMS o correos que dicen venir de tu banco, Hacienda, Correos o la DGT.
- ✕ Dar códigos de verificación por teléfono a nadie, aunque diga ser del banco.
- ✕ Reinstalar o formatear sin guardar pruebas si vas a denunciar.

Teléfonos

España	**112**
México	**911**
Colombia	**123**
Chile	**131 · 132 · 133**
Argentina	**911**
Perú	**105 · 116 · 106**

Mis contactos: _____

Punto de encuentro: _____

Después

- [ ] Activa la verificación en dos pasos en correo, banco, redes y tienda online.
- [ ] Usa un gestor de contraseñas y contraseñas distintas en cada servicio.
- [ ] Haz copias de seguridad periódicas en un disco que desconectes después.
- [ ] Mantén actualizados el sistema y las apps.

modorefugio.com/playbook/ciberataque/ · Revisado el 22 de noviembre de 2026

Información divulgativa. Sigue siempre las indicaciones de Protección Civil y del 112.