CiberConscientes
Creando nidos seguros en redes inseguras

PLAYBOOKS

# Te robaron el celular: las primeras 2 horas

Perder el celular ya no es perder un aparato: es perder la llave de tu mail, tu banco, tus billeteras virtuales y tu WhatsApp. Este playbook te da un orden claro para las primeras dos horas, que son las que definen cuánto daño te hacen. Guardalo impreso o en otro dispositivo: el día que lo necesites, no vas a tener el teléfono a mano para buscarlo.

Versión 1.1 · Agosto 2026

> ¿Ya te pasó?
> Si estás leyendo esto justo después del robo, saltá directo a la sección 2 y hacé los cuatro pasos en ese orden. Volvé después por el resto.

## 1. Antes de que pase: cinco minutos que te salvan

Todo lo que sigue después se hace mucho más fácil (o directamente se hace posible) si hoy dejás preparadas estas cosas.

- [ ] Anotá tu IMEI y guardalo fuera del teléfono. Marcá *#06# en el celular y te lo muestra: son 15 dígitos que identifican al equipo. Guardalo en un papel, en tu mail o en el gestor de contraseñas. Es lo primero que te van a pedir.
- [ ] Bloqueo de pantalla en serio. PIN de 6 dígitos o más, huella o rostro. Un patrón simple o un PIN de 4 se adivinan mirándote una vez en el colectivo.
- [ ] Activá el rastreo remoto. «Buscar mi dispositivo» en Android o «Buscar» en iPhone. Sirve para bloquear y borrar el equipo a distancia, no solo para encontrarlo.
- [ ] Sacá el segundo factor del SMS. Si tus códigos de verificación llegan por mensaje de texto, quien tenga tu chip los recibe. Pasá el segundo factor a una aplicación de códigos.
- [ ] Guardá los códigos de respaldo fuera del teléfono. Impresos, en el gestor de contraseñas o en otro dispositivo. Este paso es tan importante como el anterior: sin él, la aplicación de códigos te deja afuera a vos también.
- [ ] Poné PIN a la tarjeta SIM. Así, si mueven el chip a otro teléfono, no arranca. Está en los ajustes de seguridad de la SIM.
- [ ] Activá la verificación en dos pasos de WhatsApp (Ajustes > Cuenta > Verificación en dos pasos) y cargá un correo de recuperación.
- [ ] Tené el backup al día. Fotos y contactos en la nube o en la computadora, para que perder el equipo no sea perder los recuerdos.

> Ojo con esto: la app de códigos en el mismo teléfono
> Sacar el segundo factor del SMS te protege de que te clonen el chip, pero si la aplicación de códigos vive en el teléfono que te robaron, vos tampoco podés entrar. Por eso los dos pasos van juntos: la aplicación de códigos más los códigos de respaldo guardados en otro lado. Si tu aplicación permite copia de seguridad en la nube, activala también.

## 2. Los primeros 15 minutos: cortar el acceso

El orden importa. Primero se corta la línea, porque el chip es la llave que abre todo lo demás por SMS.

**PRIMEROS 15 MINUTOS — hacelo en este orden**

1. Llamá al *910 desde cualquier teléfono. Es la línea nacional para denunciar robo, hurto o extravío: da de baja la línea y dispara el bloqueo del equipo por IMEI. Si no podés, llamá a tu compañía y pedí lo mismo.
2. Bloqueá el equipo en remoto. Desde otro celular o una computadora, entrá a «Buscar mi dispositivo» (Android) o a iCloud «Buscar» (iPhone), marcalo como perdido y bloquealo. Dejá el borrado remoto para después de intentar ubicarlo.
3. Cerrá la sesión de WhatsApp. Instalá WhatsApp en otro teléfono con tu número y verificá con el código: al registrarte ahí, la sesión del equipo robado se cae sola.
4. Avisale a alguien de confianza que te robaron el celular y que no le crea a ningún mensaje tuyo pidiendo plata. Que lo replique en los grupos de familia.

> Esto no se hace
>
> No vayas a buscar el teléfono al lugar que marca el mapa. La aplicación te da una ubicación aproximada, no una dirección exacta, y hay casos de personas que terminaron en una situación mucho peor que perder un equipo. Esa información es para la denuncia, no para ir vos.

## 3. La primera hora: la plata y la cuenta madre

Con la línea cortada, el atacante ya no puede recibir tus SMS. Ahora hay que cerrarle las puertas que quedaron abiertas dentro del equipo.

- [ ] Cambiá la contraseña de tu correo electrónico. Empezá por acá aunque te parezca raro: el mail es la cuenta madre, desde ahí se recupera todo lo demás. Cambiala y cerrá todas las sesiones abiertas.
- [ ] Llamá a tu banco. Pedí el bloqueo del acceso desde ese dispositivo y, si tenés dudas, el bloqueo preventivo de las tarjetas. Preguntá expresamente si hay operaciones en curso o préstamos solicitados.
- [ ] Entrá a tus billeteras virtuales desde otro dispositivo: cambiá la clave, cerrá sesiones y revisá los movimientos.
- [ ] Revisá los préstamos preaprobados. Es el fraude más caro y el menos esperado: con la aplicación abierta se puede tomar un préstamo y transferirlo en minutos. Preguntá por esto en el banco y en cada billetera.
- [ ] Cerrá sesiones en las redes sociales y cambiá esas contraseñas. La mayoría tiene la opción de cerrar sesión en todos los dispositivos.
- [ ] Si el teléfono era también el del trabajo, avisá a tu área de sistemas o de seguridad ahora mismo, no mañana.

> Hacé todo esto desde una computadora o el teléfono de alguien de confianza, y escribiendo vos la dirección del sitio o desde la aplicación oficial. Nunca desde un link que te llegó.

## 4. Las primeras 2 horas: dejar registro

- Hacé la denuncia policial. Podés hacerla en cualquier comisaría y están obligadas a tomártela. Llevá el IMEI. En varias jurisdicciones se puede iniciar en línea: fijate en el sitio oficial de la policía de tu provincia o ciudad.
- Guardá la constancia. La vas a necesitar para el seguro, para el reclamo a la compañía y para desbloquear el equipo si aparece.
- Confirmá el bloqueo del IMEI. Si llamaste al *910 o a tu compañía, el equipo queda en la lista negativa y no puede usarse en las redes locales. Si tu compañía no lo hizo, ENACOM tiene un formulario de reclamo en su sitio.
- Si hubo fraude con tu plata, además de la denuncia podés reportar el caso a la UFECI, la unidad especializada en ciberdelincuencia del Ministerio Público Fiscal, escribiendo a denunciasufeci@mpf.gov.ar.
- Avisá en tus grupos. La estafa que sigue al robo es el mensaje pidiendo plata urgente a tus contactos. Un aviso a tiempo la corta.

## 5. La segunda estafa: lo que viene después

El robo del equipo suele ser solo la primera parte. Estas son las trampas más comunes de los días siguientes, y todas se aprovechan de que estás nervioso.

| Lo que te llega | Qué es en realidad |
|---|---|
| Un mail o SMS diciendo que «encontraron tu iPhone» con un link para ver la ubicación | Phishing. Buscan tu usuario y clave de iCloud para desbloquear el equipo y venderlo. Apple no manda links así. |
| Alguien que te escribe ofreciéndote devolverte el teléfono a cambio de plata | Extorsión. Pagar no garantiza nada y te marca como alguien que paga. |
| Un mensaje a tus contactos, desde tu número o uno nuevo, pidiendo una transferencia urgente | Suplantación. Por eso el aviso a tu entorno es uno de los primeros pasos. |
| Una llamada del «banco» pidiéndote datos o códigos para «asegurar tu cuenta» | Fraude. Ningún banco pide claves ni códigos. Cortá y llamá vos al número oficial. |

## 6. A la semana: cerrar el círculo

- [ ] Revisá los resúmenes del banco y de las tarjetas, movimiento por movimiento.
- [ ] Pedí tu informe crediticio para confirmar que nadie sacó un préstamo o una tarjeta a tu nombre.
- [ ] Cambiá las contraseñas que hayan quedado guardadas en el navegador del equipo robado.
- [ ] Revisá los dispositivos vinculados en WhatsApp, Google, Apple y las redes: sacá los que no reconozcas.
- [ ] Si comprás un equipo usado, pedí el IMEI antes y verificalo: si está bloqueado, no va a funcionar.
- [ ] Volvé a la sección 1 y dejá el teléfono nuevo preparado. Esta vez, antes.

## 7. Tu nido, cerrado a tiempo

Perder el equipo duele, pero lo caro es perder el acceso. Si cortás la línea, cambiás la clave del mail y avisás al banco dentro de la primera hora, el robo queda en un mal día y no en un problema de meses. Tenelo preparado hoy, que el día del apuro no se piensa.

## Esto no termina acá

Si querés enterarte de las estafas que están circulando de verdad, qué revisar y los documentos nuevos, sumate al correo de CiberConscientes. Sin vueltas y con baja en un clic. www.ciberconscientes.io

Material orientativo elaborado por CiberConscientes con fines educativos. No reemplaza el asesoramiento legal ni profesional para tu caso particular. Los números de contacto, organismos y procedimientos oficiales pueden cambiar: verificá siempre las fuentes oficiales vigentes (tu compañía de telefonía, ENACOM, la policía de tu jurisdicción y tu entidad bancaria) antes de actuar.

Versión 1.1 · Agosto 2026 · Próxima revisión: Febrero 2027 · www.ciberconscientes.io