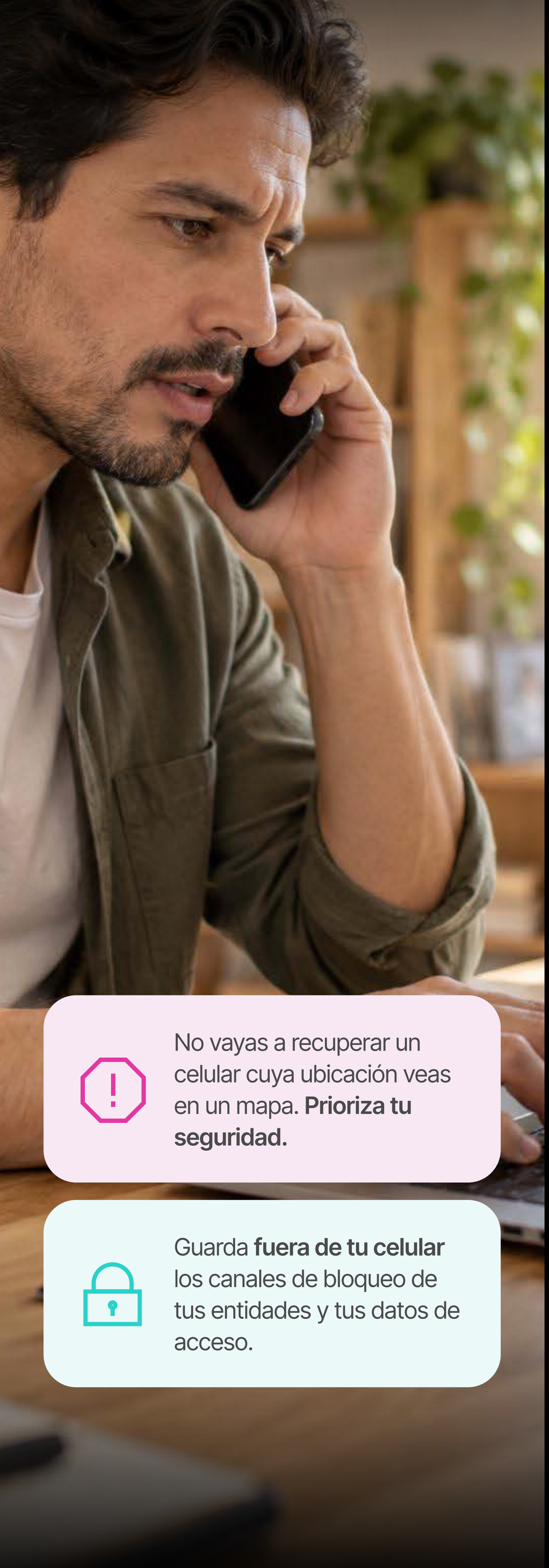
Ciber, en otras palabras

Colección Emergencias

6 guías · Hazlo así

Qué hacer, paso a paso, si **te roban el celular, entran a tu WhatsApp o a tu correo, pones tus datos en un enlace sospechoso, suplantan tu identidad** o **instalas una app sospechosa**.



Me robaron el celular. ¿Qué hago primero?

Protege **tu dinero y tus accesos** antes de intentar recuperar el equipo.

Hazlo así

01 **Protege tu dinero.** Desde otro equipo seguro, pide bloqueos preventivos a bancos y billeteras por sus números oficiales. No esperes la denuncia.

*En Perú, también: Bloqueo de Emergencia en los +10,000 Agentes BCP.

02 **Suspende tu línea y bloquea el equipo.** Pide al operador bloquear la SIM y el IMEI; usa la función oficial para localizar, bloquear o borrar.

*Ignora mensajes para “desbloquear” o “localizar”: entra solo desde la función oficial.

03 **Asegura tus cuentas.** Desde un equipo confiable, cambia claves (correo, redes y otras) y cierra sesiones desconocidas.

04 **Advierte a tus contactos:** que no atiendan pedidos de dinero ni entreguen códigos “de tu parte”.

05 **Revisa y denuncia.** Verifica movimientos, reporta operaciones desconocidas, guarda los números de atención y presenta la denuncia policial.

No vayas a recuperar un celular cuya ubicación veas en un mapa. **Prioriza tu seguridad.**

Guarda **fuera de tu celular** los canales de bloqueo de tus entidades y tus datos de acceso.

Entraron a mi WhatsApp. **¿Cómo recupero mi cuenta?**

Si otra persona tomó tu cuenta, **recupera el control** y avisa a quienes podrían recibir mensajes falsos.

Hazlo así

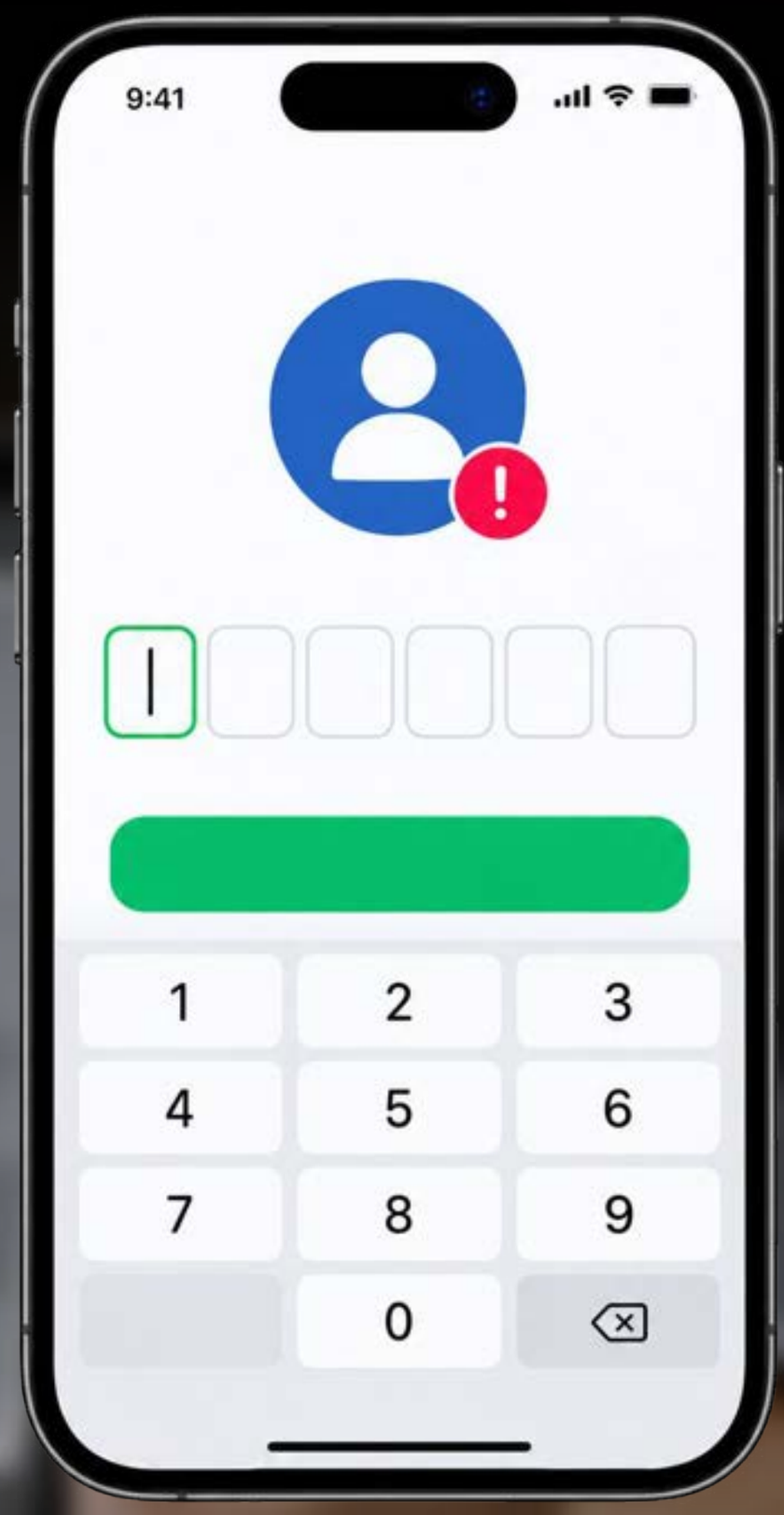
01 **Avisa por otra vía:** familia y contactos frecuentes no deben enviar dinero ni códigos por mensajes de tu cuenta.

02 **Vuelve a registrar tu número** en WhatsApp oficial con el código por SMS o llamada. Así se cierran las sesiones del registro anterior.

03 **¿Aparece un PIN que desconoces?** Sigue la recuperación oficial de la verificación en dos pasos; en algunos casos, hasta 7 días. No pagues a “recuperadores”.

04 **Revisa dispositivos vinculados** al recuperar el acceso y cierra las sesiones que no reconozcas.

05 **Refuerza la protección:** verificación en dos pasos con PIN y un correo de recuperación que controles.



Si también te robaron la SIM o el celular, pide primero a tu operador **una SIM de reemplazo con el mismo número.**

Nunca compartas **códigos SMS ni PIN de WhatsApp**, aunque te los pida un conocido.

Entré a un enlace sospechoso y puse mis datos. **¿Y ahora?**

El siguiente paso depende de **qué información ingresaste**.

Hazlo así

01 **No sigas interactuando:** cierra la página; no descargues archivos, no des permisos ni ingreses más códigos.

02 **¿Pusiste una contraseña?** Desde un equipo seguro, cámbiala ya en la página oficial y donde la reutilizabas; cierra sesiones desconocidas.

03 **¿Datos bancarios o códigos?** Contacta de inmediato a tu entidad para evaluar bloqueos y revisar movimientos: un código entregado puede facilitar operaciones.

04 **¿Descargaste o instalaste algo?** No uses ese equipo para banca ni para recuperar contraseñas. Desconéctalo de internet, extrae la SIM si es necesario y luego desinstala la app.

05 **Revisa y reporta:** comprueba la actividad de las cuentas implicadas y denuncia el enlace o mensaje por el canal oficial del servicio suplantado.

Entra a servicios importantes **escribiendo su dirección web o desde la app oficial**, no desde enlaces recibidos.

Si sospechas que tu celular está infectado, **no cambies contraseñas desde ese equipo** hasta asegurar otro dispositivo.

Hazlo así

01 **Si aún puedes entrar:** desde un dispositivo confiable, cambia la clave y activa o revisa la verificación en dos pasos.

02 **Si ya no puedes:** ve al proceso de recuperación del proveedor (Google, Microsoft u otro), no a supuestos servicios en redes sociales.

03 **Expulsa accesos desconocidos:** revisa actividad y dispositivos, cierra sesiones y elimina métodos de recuperación ajenos.

04 **Revisa cambios ocultos:** correos enviados, reglas de reenvío o eventos de calendario que no reconozcas.

05 **Protege otras cuentas:** cambia las claves de servicios importantes vinculados al correo y avisa a tus contactos si se enviaron mensajes fraudulentos desde tu dirección.

Alguien entró a mi correo. **¿Cómo lo protejo?**

Tu correo permite **restablecer contraseñas de otras cuentas:** protégelo cuanto antes.

Mantén un **método de recuperación actualizado** y usa **claves únicas** en servicios importantes.

Alguien se hace pasar por mí. **¿Cómo lo detengo?**

Reduce el riesgo de que alguien **engañe a tus contactos** usando tu identidad.

Hazlo así

01 **Avisa a tus contactos** por tus canales auténticos: que no transfieran dinero ni compartan códigos con la cuenta o número impostor.

02 **Conserva evidencia** antes de reportar: capturas del perfil falso, usuario, enlace, mensajes y pedidos de dinero.

03 **Reporta la suplantación** con la función oficial de WhatsApp o de la red social correspondiente.

04 **Protege tus cuentas reales:** revisa inicios de sesión y privacidad. Si hubo acceso no autorizado, cambia contraseñas desde un dispositivo seguro.



No publiques **fotos de documentos, direcciones ni datos personales** para “demostrar” que eres tú.

Revisa qué **datos públicos** de tus redes sociales pueden usar para hacerse pasar por ti.

Instalé una APK desconocida o creo que mi celular está infectado. **¿Qué hago?**

Si instalaste una app sospechosa, evita que siga accediendo a tus datos mientras **proteges tus cuentas**.

No todos los APK son maliciosos, pero instalar apps **desde internet o archivos enviados por WhatsApp o Telegram** aumenta el riesgo de encontrarte con uno.

Hazlo así

01 **Deja de hacer operaciones sensibles:** en el celular sospechoso no abras banca, billeteras ni correo, ni escribas contraseñas. Desconéctalo de Wi-Fi y datos móviles mientras consigues otro equipo seguro.

02 **Protege tu dinero desde otro equipo:** pide a tu banco el bloqueo preventivo de tus tarjetas de débito y crédito, y cambia contraseñas importantes (como la del correo) desde otro dispositivo confiable.

03 **Quita la app sospechosa.** Android: Ajustes > Aplicaciones, identifícala, desinstálala y revoca permisos especiales (Accesibilidad, administrador del dispositivo). iPhone: mantenla presionada y elige “eliminar”.

04 **Si el problema persiste,** busca soporte técnico confiable: podría ser necesario restablecer de fábrica. Antes, conserva solo tus archivos personales esenciales.

