Robo de celular

Producción:

cert.br nic.br cgi.br

TU CELULAR ES TU BILLETERA: CUIDA TU VIDA DIGITAL

Toda la comodidad que nos da el celular puede transformarse rápidamente en una pesadilla si cae en las manos equivocadas.

Aquí te explicamos cómo prepararte para reducir los daños y qué hacer en caso de robo.

CÓMO PREVENIR Y REDUCIR LOS DAÑOS

BLOQUEA SIEMPRE LA PANTALLA DE TU CELULAR CON UNA CONTRASEÑA FUERTE

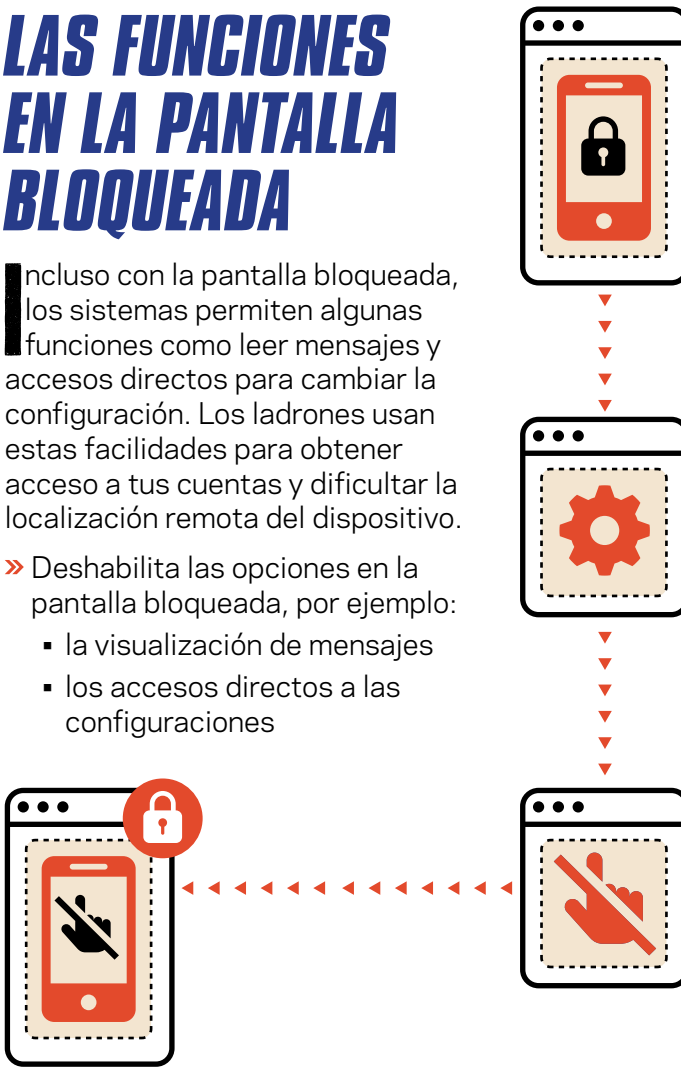
Si el teléfono está desbloqueado o si la contraseña es fácil de adivinar, el ladrón podría acceder a las aplicaciones instaladas, buscar contraseñas, modificar configuraciones y leer mensajes.

- Configura un método de autenticación para la pantalla de inicio
- Define una contraseña larga; si es alfanumérica, mejor
- Si usas un patrón de desbloqueo:
  - usa el mayor número de puntos posible
  - evita los diseños simples, como las letras
- Activa el bloqueo automático de la pantalla con el menor tiempo disponible

DESHABILITA LAS FUNCIONES EN LA PANTALLA BLOQUEADA

Incluso con la pantalla bloqueada, los sistemas permiten algunas funciones como leer mensajes y accesos directos para cambiar la configuración. Los ladrones usan estas facilidades para obtener acceso a tus cuentas y dificultar la localización remota del dispositivo.

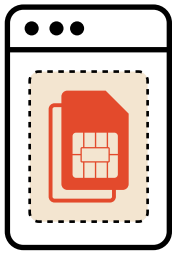
» Deshabilita las opciones en la pantalla bloqueada, por ejemplo:
- la visualización de mensajes
- los accesos directos a las configuraciones



BLOQUEA LA APLICACIÓN EN LA PANTALLA SI DEBES DEJARLA ABIERTA

Los ladrones suelen robar celulares desbloqueados. Fijar o anclar una aplicación en la pantalla permite mantenerla abierta y evita el acceso a otras funciones del teléfono. Fija una aplicación en la pantalla, por ejemplo, cuando navegues con el GPS, pidas un vehículo para transporte o intercambies mensajes.

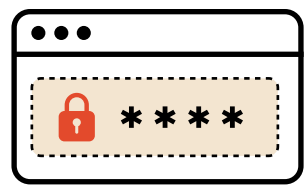
- Configura la opción de fijar una aplicación en la pantalla
  - función "Fijar pantalla" en Android o "Acceso guiado" en iOS
- Actívala cada vez que uses una aplicación en la vía pública



PROTEGE EL CHIP CON UNA CONTRASEÑA

Un *chip* o tarjeta SIM protegido por contraseña impide que el ladrón lo active en otro teléfono. Evita que el ladrón reciba mensajes SMS con códigos de verificación que le permitirían acceder a tus cuentas o restablecer tus contraseñas.

- » Activa el bloqueo del *chip*
- » Cambia el PIN predeterminado
  - verifica el de tu operadora

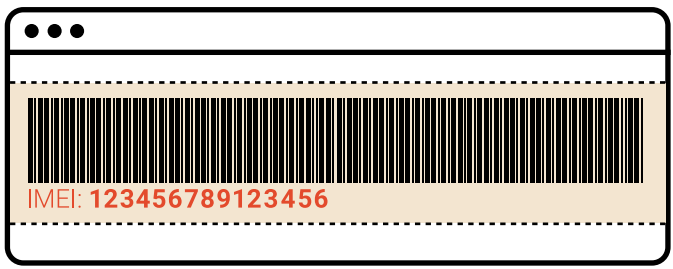


ANOTA EL IMEI DEL CELULAR

El IMEI es el código identificador del aparato y se necesita para pedir que el operador bloquee el teléfono o para informar un incidente. Con el IMEI bloqueado, el dispositivo no se puede utilizar en la red de telefonía móvil.

» Anota el IMEI y guárdalo en un lugar seguro. Este código se puede encontrar:

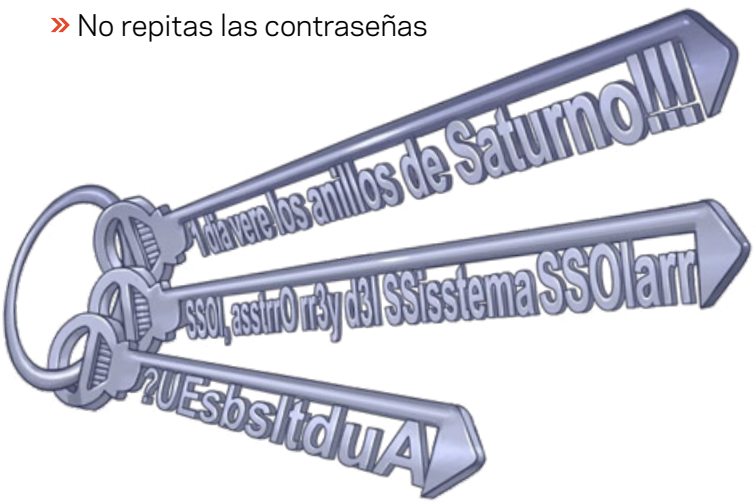
- en la factura
- en la caja del aparato
- en la configuración del sistema
- digitando *#06# directamente en el aparato



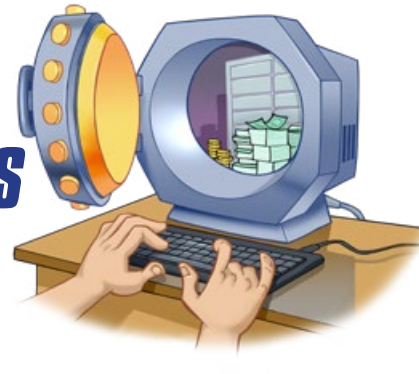
USA CONTRASEÑAS FUERTES PARA EVITAR ESTAFAS

Las secuencias conocidas o que se basan en información personal —como las fechas— son fáciles de adivinar. **Reutilizar las contraseñas también le facilita el trabajo al ladrón**, ya que le da acceso a todas las cuentas que usan la misma contraseña.

- » No uses información personal ni secuencias conocidas
- » No repitas las contraseñas



GUARDA TUS CONTRASEÑAS DE FORMA SEGURA



Los ladrones pueden encontrar las contraseñas que guardas en el celular usando mecanismos de búsqueda. No guardes contraseñas—especialmente de instituciones financieras— en aplicaciones de correo electrónico, notas, mensajes, contactos y fotos.

» Utiliza un gestor de contraseñas
  - configura una contraseña fuerte para acceder al gestor

» Si lo prefieres, usa otras opciones:
  - graba tus contraseñas en un archivo cifrado, o
  - anota las contraseñas en un papel y guárdalo en un lugar seguro

REDUCE LOS LÍMITES DE LAS TRANSACCIONES PARA MINIMIZAR LAS PÉRDIDAS

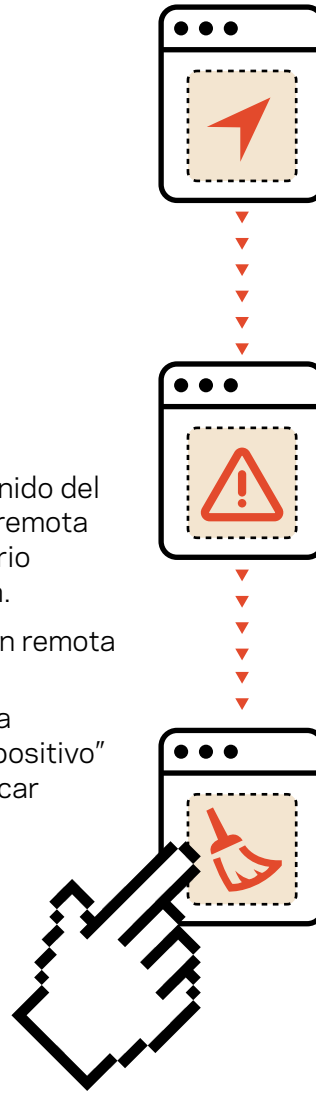
Una práctica bastante común entre los ladrones son las estafas por transferencias bancarias.

- Reduce los límites de las transferencias entre cuentas
- Revisa los límites de crédito preaprobados

PREPÁRATE PARA BORRAR EL TELÉFONO EN FORMA REMOTA

Para borrar el contenido del teléfono en forma remota primero es necesario activar su localización.

» Activa la localización remota del aparato
  - el recurso se llama “Encontrar mi dispositivo” en Android y “Buscar iPhone” en iOS



PLANIFICA CÓMO RECUPERAR TUS CUENTAS Y DATOS

Para recuperar tus cuentas y datos en otro dispositivo, antes de que ocurra el robo hay que implementar algunas acciones y configuraciones.

- Define un número de celular alternativo para recuperar tus cuentas, como la de Apple ID
- Genera y ten a mano los códigos de respaldo para las cuentas que usan verificación en dos pasos
- Haz copias de seguridad

Los códigos de respaldo son generados por la función de verificación en dos pasos para que los uses cuando los demás métodos de autenticación no están disponibles.

PROTEGE TUS DATOS PARA QUE NO LOS UTILICEN PARA ESTAFAR

Los ladrones pueden acceder fácilmente a los datos que se almacenan sin protección y los pueden usar para estafar.

» No guardes fotos de documentos, tarjetas ni contraseñas

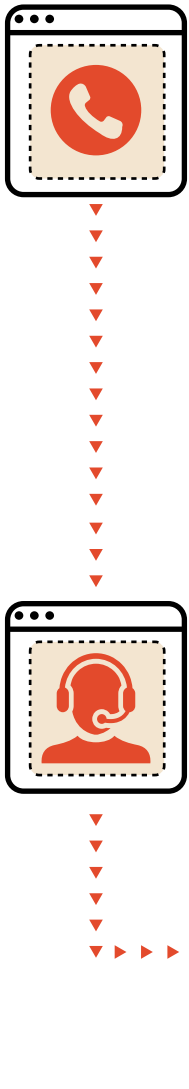
QUÉ HACER EN CASO DE ROBO

NOTIFICA A LAS INSTITUCIONES FINANCIERAS

Los ladrones pueden usar las aplicaciones de instituciones financieras y de comercio electrónico para cometer fraudes, como transferencias bancarias, préstamos, pagos de facturas y compras en línea.

» Notifica a las instituciones financieras a las que accedes a través de aplicaciones y solicita:

- el bloqueo del acceso a las cuentas por medio de la aplicación
- el bloqueo de las tarjetas que usas en el celular robado



COMUNÍCATE CON TU OPERADOR DE TELEFONÍA CELULAR

El operador puede desactivar el *chip* y bloquear el IMEI del aparato para evitar su conexión a la red de telefonía móvil. No poder hacer ni recibir llamadas y mensajes reduce las posibilidades de fraude, incluso contra tus contactos.

» Pide al operador que desactive el *chip* y que bloquee el código IMEI del aparato

HAZ LA DENUNCIA

La denuncia es el registro policial que te ayuda a defenderte, especialmente si el ladrón intenta hacerse pasar por ti. Por lo general, se exige para disputar un fraude o para reclamar un seguro.

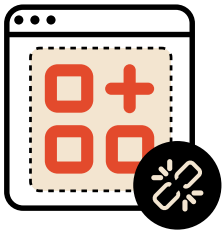
» Asegúrate de incluir el código IMEI y el número de serie del teléfono en la denuncia

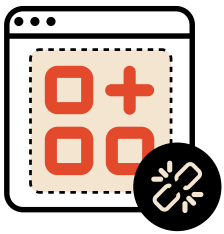
APAGA EL TELÉFONO DE FORMA REMOTA

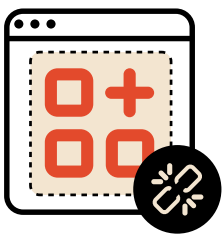
Un celular robado difícilmente se recupera. Para evitar el mal uso de tu teléfono y tus datos, borra todo el contenido de forma remota.

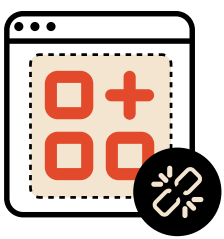
» Acceso al servicio de localización remota
  - servicio **https://android.com/find/** para Android y **https://icloud.com/find/** para iOS
  - recuerda activarlo previamente

» Borra todos los datos del dispositivo de forma remota









DESCONECTA LAS APLICACIONES Y CAMBIA LAS CONTRASEÑAS DE TUS CUENTAS

Muchas aplicaciones, como el correo electrónico y las redes sociales, mantienen la sesión abierta en tu teléfono sin que tengas que ingresar la contraseña cada vez que las usas. Si cierras las sesiones y cambias las contraseñas de las aplicaciones, el ladrón ya no podrá acceder a ellas.

- Cierra las sesiones en las aplicaciones instaladas en el celular (*logout*)
- Cambia las contraseñas de las cuentas que usas en el celular, en particular:
  - correo electrónico
  - *login* social (cuenta en una red social que se usa para registrarse en otras aplicaciones)
  - instituciones financieras
  - ID de sistema, como Apple ID y Google ID

DISPUTA LOS FRAUDES Y MONITOREA TU VIDA FINANCIERA

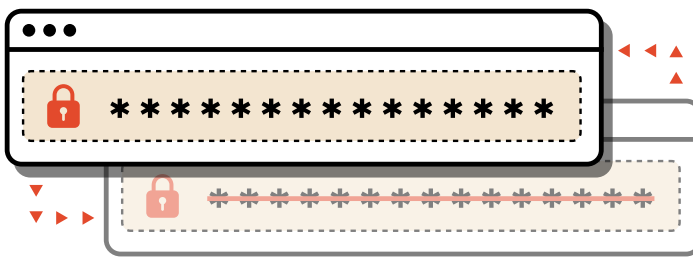
Incluso después que haya pasado el susto inicial, los problemas pueden continuar si tus datos y cuentas se usan en forma indebida.

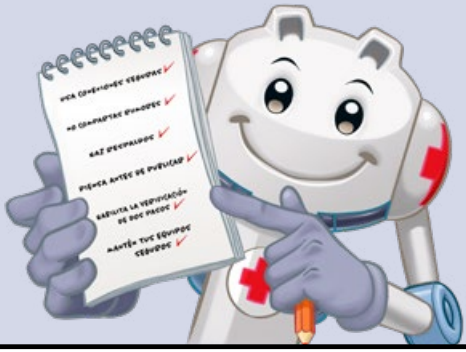
- Revisa los resúmenes y estados de cuenta de tus tarjetas en las entidades financieras y de telefonía
- Disputa las transacciones fraudulentas como transferencias, préstamos, pagos y compras
  - de ser necesario, presenta una denuncia ante el Banco Central

CAMBIA LAS CONTRASEÑAS USADAS EN DISPOSITIVOS DE TERCEROS

Es esencial actuar con rapidez para contener los daños y los accesos indebidos. Quizás hayas utilizado tus contraseñas en un dispositivo prestado, cuya seguridad no está garantizada.

» Restablece las contraseñas que usaste en el dispositivo prestado una vez que tengas acceso a un dispositivo confiable





MÁS INFORMACIÓN

» Para obtener más información sobre este y otros asuntos relacionados con los cuidados que debes tener en Internet, consulta los demás Fascículos de la Cartilla de Seguridad para Internet, disponibles en: **https://cartilla.cert.br/**

cert.br

CERT.br **(https://cert.br/)** es un Grupo de Respuesta a Incidentes de Seguridad (CSIRT) con jurisdicción nacional y de último recurso, mantenido por NIC.br. Además de la gestión de incidentes, también trabaja en la sensibilización en temas de seguridad, conciencia situacional y transferencia de conocimiento, siempre respaldado por una fuerte integración con las comunidades de los CSIRT nacionales e internacionales.

nic.br

El Núcleo de Información y Coordinación del Punto BR - NIC.br **(https://nic.br/)** es una entidad civil de derecho privado y sin fines de lucro, encargada de la operación del dominio .br, así como de la asignación de números IP y del registro de Sistemas Autónomos en Brasil. Lleva adelante acciones y proyectos que benefician la infraestructura de Internet en Brasil.

cgi.br

El Comité Gestor de Internet en Brasil **(https://cgi.br/)** es responsable por el establecimiento de directrices estratégicas relacionadas con el uso y el desarrollo de Internet en Brasil. Coordina e integra todas las iniciativas de servicios de Internet en Brasil, promoviendo la calidad técnica, la innovación y la difusión de los servicios ofrecidos.

septiembre de 2022