

Todo lo que tenés que hacer si te robaron o perdiste el celular para proteger tu privacidad

11/03/2024



Hoy en día, las personas usan sus celulares para realizar una gran cantidad de tareas, como pagos, acceso a cuentas bancarias y comunicarse. Debido a la gran cantidad de datos personales que poseen los móviles, perderlo o sufrir un robo puede ser un grave problema.

Es por eso que los usuarios de smartphones tienen que estar preparados para que la pérdida del teléfono no sea un daño mayor a su tiempo, finanzas y reputación.

Algunas precauciones a tomar si te

robaron o perdiste el celular

Un informe de la compañía de ciberseguridad **Eset** explica los pasos que hay que seguir para tener los **datos personales seguros** y evitar **problemas serios** luego de perder un **teléfono**.

Establecer una protección robusta para el acceso

El primer paso para proteger tu smartphone es implementar una sólida medida de **seguridad en la pantalla**. Hay distintos tipos de **bloqueos de pantalla**, como contraseñas, patrones, PIN y biometría. Las contraseñas fuertes son esenciales para resguardar tanto tus **cuentas** como tus **dispositivos** contra accesos no autorizados.


Una **contraseña segura** debe tener al menos **8 caracteres** y que incluyan una combinación de **letras, números y caracteres especiales**, ya que esto dificultará enormemente cualquier intento de descifrado.

Configurar la función de borrado remoto de datos

Hay que verificar que esté **activada y configurada** la función de borrado remoto de datos. Así, se podrá **eliminar toda la información** de tu teléfono en caso de robo o pérdida. La forma de hacerlo va a depender del sistema operativo que posea el móvil.

Habilitar la autenticación de dos factores

La **autenticación de dos factores** agrega un adicional de **seguridad** a tus cuentas. Al activar esta opción, se te solicitará ingresar un **código de verificación**, además de tu **contraseña para iniciar sesión**.

 **La autenticación en dos pasos es una buena forma de proteger la privacidad. Foto Unsplash.**

Se puede activar esta opción en la mayoría de las cuentas importantes, como las **bancarias**, las de **redes sociales** y las de servicios de **correo electrónico**.

Realizar copias de seguridad periódicas de tus datos

Es fundamental contar con **copias de seguridad** de tus datos para facilitar la **recuperación de información** como fotos, videos, contactos y mensajes.

Se puede hacer **manualmente** transfiriendo archivos desde tu smartphone a una computadora o disco duro externo o usar diferentes **servicios de respaldo en la nube**, como Google Drive, iCloud o OneDrive.

Guardar el número de IMEI de tu dispositivo

El **IMEI** es un **código único** que identifica cada dispositivo. Es fundamental conservar el IMEI de tu smartphone en un lugar seguro para, en caso de robo o pérdida, proporcionarlo a las **autoridades** y facilitar la **recuperación o bloqueo** del dispositivo. Se encuentra en la **caja del smartphone**, en la **configuración del dispositivo** o marcando **#06#** en el teclado del teléfono.

Robo o pérdida: ¿qué hacer en estos casos?

En caso de **pérdida o robo** de tu smartphone, lo primero que hay que hacer es **informar a las autoridades**. Puede ser en una **comisaría** o realizando un **informe en línea**, esto aumentará

las posibilidades de **recuperar tu dispositivo**.

✘ *Si perdiste tu celular, realizar la denuncia es muy importante. Foto Unsplash.*

Si extravías tu smartphone, podés usar la función «**Encontrar mi dispositivo**» proporcionada por tu operador o fabricante. Así, podrás **localizar tu smartphone** en un mapa y enviarle un mensaje con un enlace para **bloquearlo o borrar sus datos**.

Eset detallo los **pasos a seguir** en caso de **pérdida o robo** para **proteger tus datos**:

Bloquear el dispositivo

El primer paso es **bloquear el dispositivo** para impedir que el **delincuente** acceda a tu información. Podés lograrlo contactando a tu operador y solicitando la **cancelación del chip**, o mediante el **IMEI**, el código único que identifica tu dispositivo.

Cambiar la contraseña y cerrar sesión en tus aplicaciones

Una vez que hayas bloqueado el dispositivo, es crucial **cambiar las contraseñas** de las aplicaciones instaladas y **cerrar sesión en el dispositivo**, si es posible. Esto resguardará tu información personal y financiera contra cualquier persona que intente acceder al dispositivo.

Informar a tus instituciones financieras

Notificar a tus **instituciones financieras** sobre el robo de tu smartphone fortalecerá la **seguridad de tus cuentas bancarias y tarjetas de crédito**, previniendo cualquier actividad fraudulenta.

✘ *Si perdiste el celular es muy importante cambiar las*

contraseñas. Foto: Unsplash.

Avisar a familiares y amigos

Alertar a tus **familiares y amigos** para evitar que el delincuente intente **contactarlos** para obtener **información o dinero**.

Presentar una denuncia ante las autoridades

Presentar la denuncia en la policía facilitará la **investigación del delito**, la identificación del agresor y te permitirá ser contactado en caso de recuperar tu dispositivo.

Fuente: Canal 26