



Robo o pérdida del *smartphone*

Prepárese y no entre en pánico

Contenido

- Riesgos ante el robo o pérdida del *smartphone*
- Prepárese y adopte buenas prácticas de prevención
- Consejos sobre qué hacer si sufre un robo o pérdida de su *smartphone*



A close-up photograph of a person's waist wearing dark trousers and a black leather belt. A hand is holding a black smartphone, positioning it near the waistband as if about to be placed in a pocket. The background is a plain, light color.

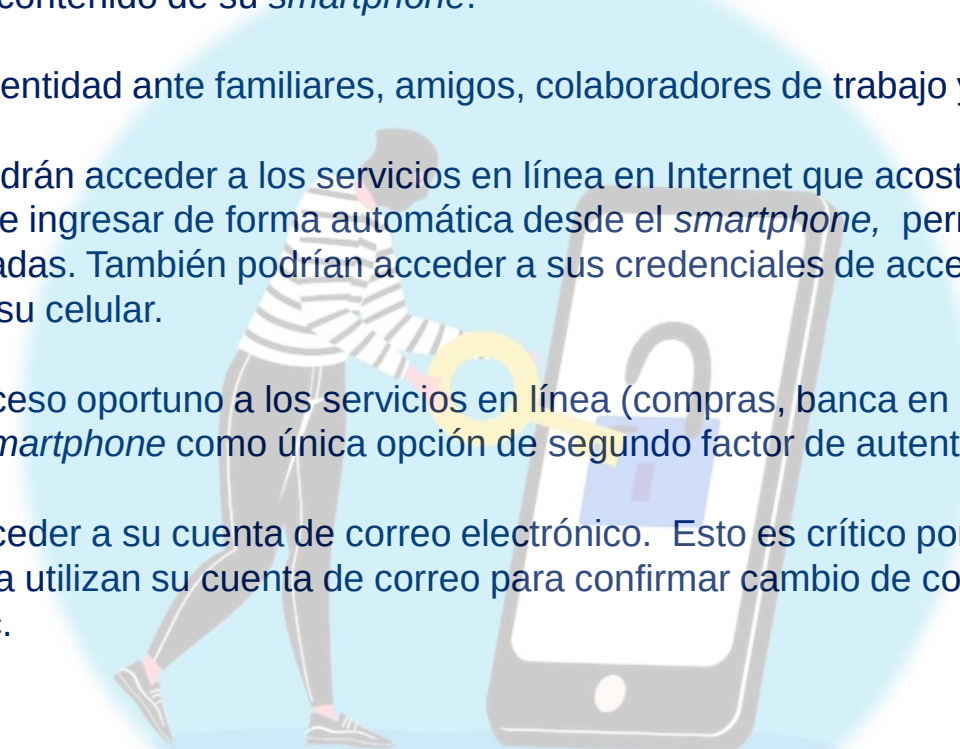
1. Riesgos ante el robo o pérdida del *smartphone*

Para muchos el *smartphone* es casi un artículo de primera necesidad. El robo o pérdida de un *smartphone* genera estrés o ansiedad. No solo es perder fotos-videos de reuniones familiares, sino de desconectarse del mundo digital y ser víctima de fraudes.

En la siguiente página, listamos algunos riesgos del robo o pérdida del *smartphone*:

Algunos riesgos sobre el robo o pérdida del *smartphone*

1. Los delincuentes podrán acceder a datos, fotos, videos, audios, conversaciones personales y credenciales de acceso a servicios en línea. Ser víctima de un robo de identidad y/o ser extorsionado por el contenido de su *smartphone*.
2. Que suplanten su identidad ante familiares, amigos, colaboradores de trabajo y/o clientes.
3. Los delincuentes podrán acceder a los servicios en línea en Internet que acostumbra a utilizar, si a los mismos se puede ingresar de forma automática desde el *smartphone*, permitiéndoles realizar compras no autorizadas. También podrían acceder a sus credenciales de acceso si están guardadas en notas o fotos en su celular.
4. Imposibilidad de acceso oportuno a los servicios en línea (compras, banca en línea, etc.) si solo tiene habilitado al *smartphone* como única opción de segundo factor de autenticación (2FA).
5. Imposibilidad de acceder a su cuenta de correo electrónico. Esto es crítico por que la mayoría de los servicios en línea utilizan su cuenta de correo para confirmar cambio de contraseña, autorizar una transacción, etc.

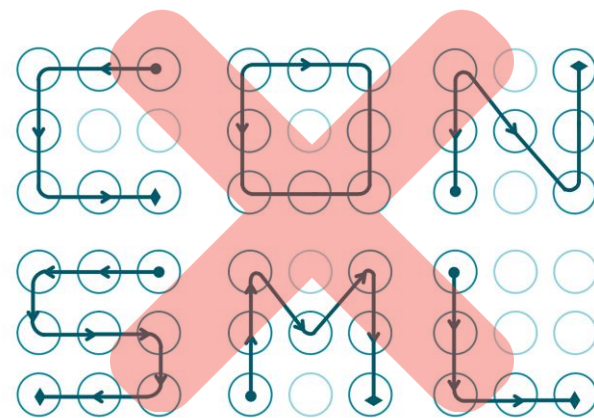


Tener habilitado el “auto-bloqueo de pantalla” no es garantía que el delincuente no tendrá acceso al *smartphone*. El criminal tratará de robar su teléfono mientras usted lo está usando, permitiéndole, deshabilitar la opción de “auto-bloqueo de pantalla” y acceder al *smartphone*.

2. Prepárese y adopte buenas prácticas de prevención

1. Habilitar una contraseña para acceder el *smartphone*, ya sea un PIN o mecanismo biométrico. Si utiliza *smartphones* Android, preferiblemente, que no sea un patrón predecible como letra “M”, “L”, “C”, “S”, y “O” (ver imagen a la derecha).
2. Habilitar que la opción de “auto-bloqueo de la pantalla” se active en un minuto o menos.
3. Habilitar la opción “*Find My iPhone*” (iPhone) o “*Find My Device*” (Android) y memorice las credenciales de acceso.
4. Tenga accesible (no en su *smartphone*) el número de teléfono de servicio al cliente para cancelar/suspender: a) su línea de teléfono b) sus tarjetas de crédito; c) la banca en línea.

En adición, memorice las credenciales de acceso a iCloud (iPhone) y su equivalente en Android.



5. Hace sentido que alguien cercano a usted tenga la información del punto No. 4. Memorice el número de teléfono de dicha persona para que pueda llamarlo.



Realice regularmente respaldos del contenido de su *smartphone*.



Ante el robo o pérdida del smartphone, cada minuto cuenta. Haberse preparado y actuar rápido, puede ser la diferencia entre pasar un mal rato o ser víctima de un fraude financiero o extorsión.

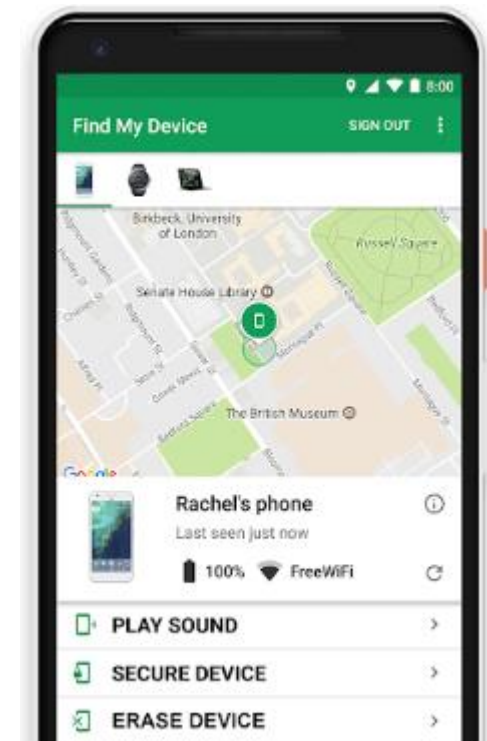
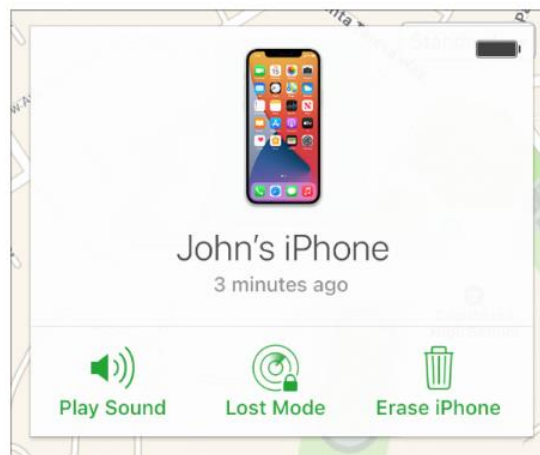
3. Consejos sobre qué hacer si sufre un robo o pérdida del *smartphone*

- a) Acceda el servicio “*Find My iPhone*” (iPhone) o “*Find My Device*” desde el teléfono o computador de alguna persona de confianza y:
 - 1. Verifique si su *smartphone* está aún cerca de donde usted se encuentra.
 - 2. Active la opción “*play sound*”. Aún cuando el teléfono esté en silencio, se escuchará el sonido al menos por dos minutos.
 - 3. Bloquee su *smartphone*.
- b) Cambie la contraseña de las cuentas de correo electrónicos configuradas en el *smartphone*.
- c) Llame desde otro teléfono a su *smartphone*. Puede ser que esté cerca o que alguien lo haya encontrado.
- d) Contacte al servicio al cliente de su operador de teléfono; tarjetas de crédito; banca en línea; y suspenda/cancele el servicio.



3. Consejos sobre qué hacer si sufre un robo o pérdida del *smartphone*

- e) Cambie las contraseñas de acceso a iCloud (iPhone) o su equivalente en Android.
- f) Acceda el servicio “*Find My iPhone*” (iPhone) o “*Find My Device*” y trate de borrar remotamente el contenido de su *smartphone*.
- g) Si recupera el *smartphone* algún tiempo después, es recomendable que borre los datos y restablezca el *smartphone* a las configuraciones de fábrica. Existe la posibilidad que le hayan instalado algún programa malicioso en el teléfono.



CONTACTOS

Panamá y CARICOM

Antonio Ayala I.
aayala@riscco.com

Rubén Fernández
rfernandez@riscco.com

República Dominicana y Puerto Rico

Rubén Fernández
rfernandez@riscco.com

Costa Rica y El Salvador

Roberto Delgado
rdelgado@riscco.com

Guatemala, Honduras y Nicaragua

Roberto Delgado
rdelgado@riscco.com

riscco.com

Es una compañía regional independiente y dedicada de manera exclusiva ayudar a organizaciones a enfrentar sus desafíos en GRC (*Governance, Risk & Compliance*) y ESG (*Environmental, Social & Governance*); compuesta por profesionales con el conocimiento y credibilidad necesaria para traducir aspectos muy técnicos a un lenguaje simple y con sentido de negocio. Con catorce (14) años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías privadas e Instituciones del Estado en la región líderes en su ramo.

