

Tus dispositivos almacenan mucha **información privada** ¿Te habías parado a pensarlo?

“Estaba junto a la puerta del tren volviendo del trabajo aprovechando el viaje para hacer unas gestiones con la app de mi banco cuando el tren se detuvo en una estación y justo antes de que reemprendiera su marcha, en el momento en que las puertas comenzaban a cerrarse, alguien cogió mi móvil y me lo arrancó de las manos.”



Uno de los principales motivos para proteger nuestros dispositivos móviles es salvaguardar nuestra información personal y la de aquellas personas con las que nos comunicamos: contactos, fotografías, vídeos, correos electrónicos, etc., y que no nos gustaría perder o que cayesen en manos de terceros.

Debes proteger adecuadamente tus dispositivos



- ◆ Es obvio que **si pierdes o te roban** el móvil te quedas sin la información.
- ◆ Una **app maliciosa** puede ser capaz de eliminar o utilizar tus datos sin que lo sepas.
- ◆ Las **redes wifi públicas** (aeropuertos, cafeterías, bibliotecas, etc.) pueden no ser seguras ya que, o no cifran la información que se transmite a través de ellas, por lo que cualquier usuario conectado con ciertos conocimientos podría hacerse con ella, o porque desconocemos quién está conectado a esa misma red y con qué fines.

Consejos y recomendaciones



El riesgo de pérdida o robo siempre va a existir. Por tanto:

- ◆ Utiliza un método de bloqueo de la pantalla (código numérico o patrón) y **cifra la información** para que si esta situación se produce, dificultes el acceso a la persona que acabe con el dispositivo en sus manos.
- ◆ Haz uso de **herramientas de seguridad** que te ayudarán a localizar el dispositivo, bloquearlo e incluso eliminar la información almacenada en él.
- ◆ Realiza **copias de seguridad** en otro soporte para que, pase lo que pase, no pierdas la información almacenada en el móvil o tableta.

En el dispositivo, sólo aplicaciones seguras:

- ◆ Descárgalas únicamente a través de las **tiendas de apps oficiales**. Así te aseguras que éstas han sido revisadas tanto por ellos como por los usuarios.
- ◆ Revisa previamente la **valoración y los comentarios** que los usuarios han hecho sobre una determinada app. Cuando se comporta mal o de manera sospechosa, los propios usuarios se encargan de reflejarlo en los comentarios.
 - ◆ Instala una **herramienta antivirus** para que detecte posibles apps maliciosas que intenten colarse en tu dispositivo.



Cuidado con las redes **wifi públicas a las que te conectas. Si las usas:**

- ◆ No intercambies información privada o confidencial.
- ◆ No te conectes al servicio de banca online.
- ◆ No realices compras.