

## 10 Consejos para proteger nuestro teléfono móvil

Los usuarios que poseen teléfonos inteligentes, por lo general, utilizan sus dispositivos para prácticamente cualquier cosa. Desde compras y tareas laborales, hasta entretenimiento y comunicaciones. Es por ello que te indicaré algunos consejos útiles que puedes aplicar para **proteger móvil**.

Es fácil olvidar que estos dispositivos pueden contener gran cantidad de información completamente confidencial, y peor aún, que pueden ser hackeados muy fácilmente si no se toman medidas a tiempo.

Si este es tu caso, o sencillamente quieres proteger aún más tu móvil, la información que te proporcionaré te será de gran ayuda.

### 10 consejos a tomar en cuenta sobre proteger móvil

Existen ciertos pasos clave que puedes seguir para cuidar correctamente tu teléfono inteligente de cualquier pirata informático. Del mismo modo, hay hábitos que te ayudarán a que tus datos se encuentren bien protegidos.

#### 1. Aplica una contraseña para el teléfono con un PIN



Si, sé que suena muy obvio, pero la verdad es que no todas personas tienen este método de bloqueo en sus dispositivos móviles. Este PIN, también conocido como número de identificación personal, se encuentra registrado en la tarjeta SIM.

## Perit Girona

Esto es una medida de seguridad que permite que se protejan los datos en caso de que se reinicie el dispositivo, o si se le cambia el chip al móvil. Al momento en que eso ocurre, se activa un menú que solicita el PIN. Allí radica la importancia de usar este método.

### **No abandones la tarjeta que venía con el SIM**

Si vas a aplicar esta técnica es preciso que guardes en un lugar seguro la tarjeta plástica con la que venía el chip al momento de ser comprado. La razón de esto es que allí también se ubica el código PUK, por si el equipo se bloquea.

### **2. Realiza una copia de seguridad de los datos que estén en el móvil**

Respalda tu información es sumamente importante, ya que permite que guardes toda tu información valiosa, en caso de que exista una pérdida de datos por algún motivo. Puedes hacerlo directamente desde alguna aplicación que viene directamente con el celular, o a través de servicios en la nube.



En cualquiera de los dos casos puedes guardar distintos datos como contactos, archivos, imágenes, fotografías, etc.

### **3. Activa el bluetooth y el Wi-Fi únicamente cuando vayas a utilizarlos**

Sin lugar a dudas el bluetooth y el Wi-Fi tienen una infinidad de ventajas, pero la realidad es que tener encendidas estas dos herramientas del móvil todo el tiempo puede traer dos consecuencias.

## Perit Girona

La primera es que sencillamente se te acaba más rápido la batería de tu dispositivo, y la segunda, es que puedes tener riesgo de que haya una fuga de datos. Esto sucede ya que al estar abierta una señal de un móvil sin usar, cualquier usuario malintencionado puede aprovechar para enviar virus o conectarse a tu dispositivo.

### **4. Verifica que la información que recibes esté libre de malware**

Dependiendo del software u OS que tenga tu celular, puede afectarle uno u otro malware. Para combatir este riesgo, solo debes instalar una App de antivirus que compruebe todos los archivos que descargues o te transfieran.

Del mismo modo, estas apps son capaces de cuidar los archivos que se instalan en el teléfono. Por ello, un análisis con antivirus nunca está de más.

### *Qué puede hacer por ti un perito calígrafo*

### **5. Descarga aplicaciones únicamente de sitios confiables**

Existen aplicaciones que lo único que buscan es extraer tus datos personales. Estas poseen funciones ocultas que pueden enviar preferencias y hábitos de consumo de la persona para agentes publicitarios, e incluso crear desperfectos en el móvil.



Es por ello que te recomiendo siempre instalar aplicaciones solo si las conoces y confías en su procedencia. Las aplicaciones confiables las puedes obtener desde la tienda de aplicaciones que viene con tu equipo, y sus descargas son gratuitas, o al menos la mayoría.

## Perit Girona

### Aplicaciones crackeadas

Por otra parte, descargar aplicaciones que traen ya una licencia cargada en el software puede traer consecuencias para tu móvil. Algunas de ellas es que puedes llenar tu teléfono de programas [espías](#) o incluso de programas maliciosos.

### No abrir enlaces desconocidos

Dentro de este punto existe algo que también resulta relevante, y es que por ningún motivo debes abrir enlaces que no conozcas, o que te lleguen por medio de SMS. Por lo general estos implican la descarga de alguna aplicación para el equipo, y al hacerlo es posible que se dañe tu móvil.

### [¿Puedo presentar un WhatsApp como una prueba en un juicio?](#)

## 6. Cierra todas las sesiones luego de que termines de utilizar tus apps

La realidad es que nunca se sabe cuándo tu teléfono puede caer en las manos equivocadas, incluso por unos cuantos minutos. Alguien que usa tu teléfono con las sesiones de redes sociales abiertas, tiene toda la facilidad de acceder a ellas y a tu información.



Si no quieres cerrar las sesiones, no te preocupes, puedes asignar una contraseña para abrirlas, desde tu dispositivo. En el caso de que tu móvil no posea esta opción, puedes optar por descargar una App confiable para este fin.

## 7. Mantén tu sistema operativo siempre actualizado

Al mantenerlo siempre actualizado puedes evitar cualquier fallo de seguridad, además de que se añaden y optimizan distintas características que pueden ayudarte a evitar problemas de protección. Casi siempre las actualizaciones van destinadas a resolver cualquier tipo de fallo que ponga en riesgo tus datos.

### [Perito arquitecto en Girona](#)

## 8. Instala una App de borrado de datos de forma remota

Esta es una muy buena idea si te roban o llegases a extraviar el teléfono. Con este tipo de aplicaciones puedes activar el celular por un mensaje de texto, y así puedes proceder a borrar la información privada. Dependiendo de la aplicación incluso puedes localizar el móvil, aunque el GPS se encuentre desactivado.

## 9. Guarda muy bien el número IMEI

Una excelente manera de ayudar a detener el robo de móviles es haciendo uso del código IMEI. Este es un número que cada celular tiene pregrabado de fábrica, y lo identifica como único a nivel mundial.

Es transmitido por red con el operador de telefonía que poseas, y puedes mandar a que lo bloqueen para que nadie pueda acceder a tus datos y al móvil en general.



[¿Se pueden recuperar mensajes borrados de WhatsApp?](#)

## 10. Ten cuidado sobre a quién le prestas tu móvil

Finalmente, es importante que cuides a quién le vas a prestar tu teléfono, sin importar que sea por unos pocos minutos. Donde quiera que te ubiques, una “inocente” llamada puede involucrar la extracción de toda tu información o datos personales, secuestro virtual, o incluso robo, en caso de que el sujeto salga corriendo.

Es importante aclarar que todos estos consejos sobre proteger móvil deben aplicarse tanto a teléfonos inteligentes, como a dispositivos tradicionales, en la medida de lo posible. Las amenazas de seguridad en estos casos siempre se encuentran latentes, pero aplicando ciertas recomendaciones puedes reducir riesgos.

Lógicamente nada es infalible, pero con unas cuantas acciones puedes evitar muchos malos ratos. Proteger tus datos es algo que deberías hacer constantemente.

Mi nombre es José Luis Martir Millán, soy perito informático, y puedo ayudarte en cualquier inconveniente que presentes en cuanto a cualquier plataforma digital, o dispositivo electrónico, que requiera de mis servicios ante un juzgado. Me puedes contactar a través de mi email [lluis@peritinformatic.com](mailto:lluis@peritinformatic.com) o mediante mi web [www.peritinformatic.com](http://www.peritinformatic.com).