El móvil más seguro del mundo

GUÍA COMPLETA PARA BLINDAR SU TELÉFONO

“En OCU trabajamos para ser útiles y facilitar su día a día.”

Índice

Introducción

Los actuales teléfonos móviles inteligentes o *smartphones* son casi una extensión de nosotros mismos. Se trata del dispositivo con el que pasamos más tiempo a lo largo del día. Lo utilizamos para comunicarnos, trabajar, aprender, entretenernos, comprar, viajar, investigar, etc.

Y aún así, muchos de los más de 6.500 millones de personas que utilizamos a diario nuestro *smartphone* no pensamos en lo que pasaría si todo lo que guardamos en él, fotos, conversaciones con amigos, contactos profesionales... desaparecieran en un minuto, aunque el impacto en nuestra vida sería considerable. Pero no tenemos por qué confiar simplemente en que este no ocurra; podemos anticiparnos y tomar medidas para proteger nuestro dispositivo más personal y, lo más importante, su información, tanto de accidentes o descuidos como de amenazas externas. Esto es lo que pretende esta guía: mostrar algunas de las acciones para lograrlo.

En el capítulo 1 se da una introducción sobre el concepto de seguridad móvil, describiendo las acciones que podemos realizar y cómo reconocer algunas de las amenazas más graves, como el *phishing*. También se habla de cómo conectarnos de forma segura y los riesgos de algunas redes Wi-Fi.

El capítulo 2 se centra en Android, el sistema operativo móvil más utilizado en el mundo. Nos adentramos en sus mecanismos de seguridad y en cómo configurarlos. Se describe cómo funciona la nube de Google y su tienda de aplicaciones, además de cómo realizar una copia de seguridad y la utilización de los antivirus dentro de esta plataforma.

El capítulo 3 está dedicado a iOS, el sistema con el que trabajan los populares iPhone de Apple. En él se explora cómo funcionan las opciones de seguridad, si es interesante utilizar iCloud para guardar nuestra información, los peligros de liberar nuestro *smartphone* y cómo hacerlo más seguro mediante las tecnologías más novedosas, como las llaves de seguridad.

Por último, el capítulo 4 propone algunas ideas para aplicar en el día a día, desde cómo gestionar las contraseñas hasta cómo comprar con nuestro móvil. Veremos qué hacer si lo perdemos o nos lo quitan, cómo localizarlo y poner a salvo su información. Y también cómo aprovechar las herramientas para el acompañamiento parental de nuestros hijos.

Esperamos que esta guía le resulte útil a la hora de disfrutar de todo lo bueno que nos aporta la tecnología móvil de la forma más segura.

La importancia de la seguridad

Aunque parece que todos entendemos el concepto de seguridad relacionado con nuestros dispositivos móviles, no está de más definirlo en toda su extensión para tener así una idea clara de qué trata esta guía.

¿Qué es la seguridad móvil?

La seguridad móvil abarca el conjunto de medidas y herramientas que se emplean para proteger de posibles amenazas tanto el dispositivo en sí como la información contenida en él. Por ejemplo, una medida básica de seguridad es el bloqueo de pantalla, de forma que sea necesario introducir una contraseña alfanumérica o un patrón de desbloqueo para poder acceder al dispositivo. Por otra parte, hay otro riesgo al que todos estamos expuestos: la pérdida o sustracción de nuestro *smartphone*.

Algunos de los aspectos más importantes que debemos tener presentes a nivel general son:

1. Cómo proteger el contenido del dispositivo

Esto incluye las medidas utilizadas para salvaguardar los datos almacenados en el equipo mediante el uso de contraseñas, autenticación de una huella dactilar o reconocimiento facial para acceder al dispositivo, así como la encriptación de datos sensibles. A este respecto, es importante emplear contraseñas que no sean demasiado simples y, a la vez, distintas de las utilizadas en los servicios a los que estamos suscritos, y cambiarlas regularmente.

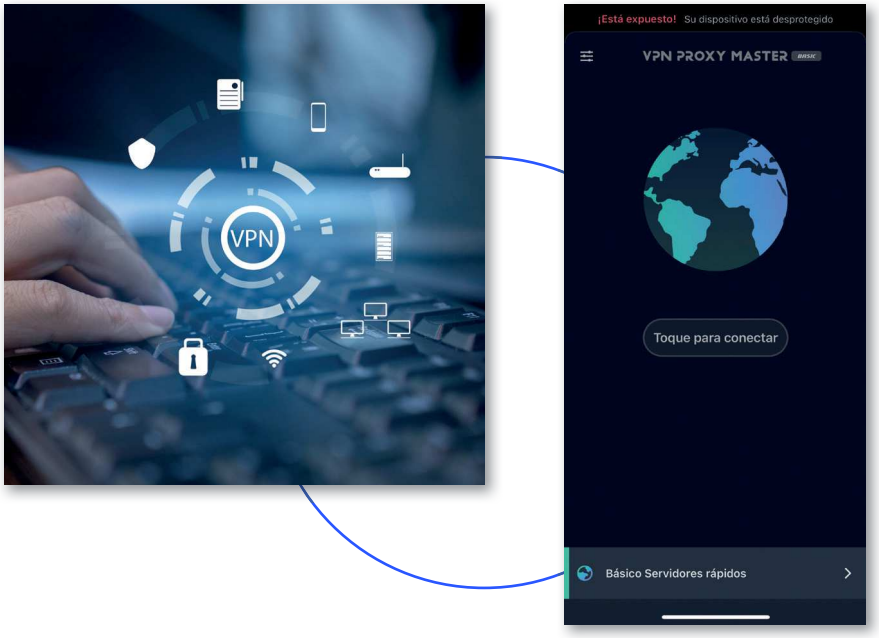
2. Los peligros de conectarse a una red Wi-FI pública o no suficientemente segura

El uso de redes inseguras o abiertas, como por ejemplo la red Wi-Fi que los centros comerciales suelen ofrecer a sus clientes, puede exponer a nuestros dispositivos móviles a riesgos tales como que un atacante pueda suplantar la identidad de la red, interceptar nuestras comunicaciones y acceder a nuestros mensajes de email o contraseñas de las páginas a las que nos conectemos. Es importante evitar, en lo posible, conectarse a redes públicas.

3. En el caso de que necesitemos utilizar una red Wi-Fi pública

Lo más recomendable es emplear una herramienta de acceso VPN (*Virtual Private Network*, o Red Privada Virtual). Se trata de una tecnología que pro-

porciona una capa adicional de seguridad al encriptar los datos que viajan entre nuestro móvil y la red a la que nos conectamos. De este modo, se evita que un atacante puede interceptar la información. Además, el uso de una VPN permite acceder a recursos y servicios restringidos que solo están disponibles en una red privada. Así podemos, por ejemplo, acceder a los archivos guardados en el disco duro de nuestro ordenador de casa o utilizar su impresora de forma remota y segura.



4. Las amenazas en forma de software malicioso

Los dispositivos móviles están expuestos cada vez a una mayor variedad de programas maliciosos (también conocidos como *malware*) tales como virus, troyanos y *spyware* que puede burlar su seguridad mientras navegamos por internet. Su finalidad puede ir desde apropiarse de nuestra información hasta incluso "secuestrar" el *smartphone*.

Por eso es tan importante mantener actualizado el sistema operativo del dispositivo. En especial, es recomendable instalar lo más rápidamente posible las actualizaciones de seguridad, ya que incluyen parches que solucionan las vulnerabilidades conocidas más graves. Además, puede emplearse alguna herramienta específica para aumentar su nivel de seguridad, como por ejemplo un antivirus.

5. Los riesgos derivados de la instalación de apps

Algunas de las aplicaciones disponibles en las tiendas de terceras partes (e incluso también en las oficiales de los desarrolladores de sistemas operativos, aunque en mucha menor medida) pueden contener un *malware*. Por ello, lo más recomendable es descargar las apps solo de fuentes fiables, como la App Store de Apple o Google Play Store, y actualizarlas regularmente para corregir cualquier amenaza potencial e intentar mantenerse al tanto sobre las vulnerabilidades que se van descubriendo.

6. La pérdida o robo del dispositivo

Es importante disponer de un plan que nos permita reducir, en la medida de lo posible, los problemas que acarrean la pérdida o sustracción de nuestro dispositivo. Dada la variedad de usos que le damos hoy en día, lo más probable es que contenga datos sensibles (como información de nuestra actividad profesional) y privados (fotos y vídeos personales, etc.).

Si lo planificamos con antelación, podremos rastrear la ubicación del dispositivo mediante la función de seguimiento del sistema operativo o de una app específica para este fin, lo que nos ayudará a localizarlo. También es importante tener la opción de inutilizarlo a distancia para evitar que cualquier persona pueda acceder a su contenido. En último extremo, si estamos seguros de que no vamos a poder recuperarlo, tendremos la posibilidad de eliminar remotamente la información guardada en él, y evitar que caiga en malas manos.

7. Realizar copias de seguridad de forma automática

Es muy recomendable que hagamos copias de seguridad de la información almacenada en el dispositivo para poder recuperarla en caso de pérdida, sustracción o daño físico. Tanto Android como iOS ofrecen opciones para ejecutar automáticamente una copia de seguridad de datos tales como nuestras queridas fotos y vídeos que suelen guardarse en las respectivas nubes de Google y Apple. También es posible realizar estas copias a mano en un dispositivo externo, como el disco duro de un ordenador, si tenemos alguna duda sobre el nivel de privacidad o deseamos tener una copia adicional que podamos recuperar sin necesidad de estar conectados a internet.

8. Dentro del ámbito empresarial

Se pueden tomar una serie de medidas avanzadas como establecer un control de acceso basado en las responsabilidades del trabajador. Algunas compañías

utilizan herramientas de protección en los dispositivos con el fin de garantizar que solo los usuarios autorizados tengan acceso a ciertos recursos y funcionalidades de estos. Por ejemplo, el departamento de informática podría tener un acceso completo a todas las opciones de configuración y datos del *smartphone*, mientras que su usuario habitual solo tendría capacidad de utilizar ciertas apps preinstaladas sin la posibilidad de descargar y ejecutar otras.

En resumen, la seguridad de nuestros dispositivos móviles supone un esfuerzo diario para preservar su integridad y salvaguardar la información que contienen. Esto implica adoptar medidas de protección tanto a nivel del propio dispositivo como al conectarnos a redes Wi-Fi externas y hacer uso de las apps. También conviene prever posibles accidentes, como la pérdida, sustracción o un daño accidental que lo inutilice. Es esencial mantener actualizados siempre tanto el sistema operativo como las aplicaciones, y obtener estas últimas solo de tiendas oficiales, ya sean las de Apple o Google o el fabricante del dispositivo.

Distintos dispositivos móviles

Gracias a la rápida evolución que ha experimentado la tecnología en los últimos años, hoy en día disponemos de una gran variedad de dispositivos móviles, algunos de ellos pensados para satisfacer unas necesidades muy concretas. Aunque esta guía está enfocada en el uso de los teléfonos inteligentes, no está de más echar un vistazo general a otros dispositivos móviles que comparten con los *smartphones* varias de sus funcionalidades y a los que, por tanto, se pueden aplicar muchos de los consejos que incluimos aquí.

Smartphone

Los teléfonos inteligentes, o *smartphones*, son dispositivos móviles provistos de una pantalla táctil cuya función original básica es la de comunicarse mediante voz con otras personas. Sin embargo, hoy en día, esta característica se ha visto relegada por la gran variedad de funciones que ofrecen: los empleamos como cámara de fotos y vídeo, navegador GPS, medio de acceso a internet, consola de videojuegos, para estudiar, trabajar y mucho más. Los *smartphones* se caracterizan por aunar la mayor portabilidad y una alta potencia, convirtiéndose en uno de los dispositivos tecnológicos actuales más versátiles y, de hecho, el único que poseen millones de personas.

Tableta

Como en el caso anterior, las tabletas, o *tablets*, son aparatos portátiles que disponen de una interfaz táctil, aunque el tamaño de su pantalla es mayor que el de los *smartphones*. A diferencia de estos, la mayoría de las tabletas no permiten realizar llamadas de voz a través de la red estándar de telefonía móvil, aunque sí a través de apps específicas. Sin embargo, cuentan con muchas de las funcionalidades que poseen los teléfonos inteligentes, tales como la conectividad a internet, la navegación a través de las redes satelitales (como GPS y otras) o su uso como cámara de fotos y vídeo.

Dispositivos híbridos

Existen también los llamados dispositivos híbridos. Se trata de equipos que combinan las características de las tabletas y los portátiles.

Quizás el ejemplo más popular es el Surface de Microsoft. Poseen una pantalla táctil y están diseñados para utilizarse fácilmente con un teclado y un ratón. Además, cuentan también con conectividad a internet, GPS y cámaras, al igual que las tabletas. La ventaja fundamental respecto a estas estriba en su compatibilidad con sistemas operativos de escritorio como Windows, por lo que es posible utilizar el software diseñado para este.

Portátil

Los clásicos portátiles suelen tener pantallas de mayor tamaño que las tabletas y los dispositivos híbridos, así como teclados completos y, en general, una mayor potencia de computación y gráfica. Por ello, es la opción ideal para trabajar de forma cómoda o realizar tareas más complejas, como la edición de vídeo o diseño industrial. A diferencia de las tabletas y los *smartphones*, la gran mayoría de los portátiles carecen de pantalla táctil. Se trata también del dispositivo donde existe una oferta más amplia de modelos, desde configuraciones básicas pero suficientes para muchas personas, hasta verdaderas estaciones de trabajo enfocadas a ejecutar las aplicaciones más complejas.

eReaders

En un apartado distinto, pero cada vez más utilizados, se encuentran los libros electrónicos y los relojes inteligentes. Dado que su complejidad está aumentando y muchos de sus modelos ofrecen conexión a internet, conviene tener en cuenta que se trata de dispositivos que también necesitan algunas medidas básicas de seguridad.

Los lectores de libros electrónicos, o lectores de *ebook*, están diseñados especialmente para la lectura. Sus pantallas cuentan con tecnologías distintas a las empleadas en el resto de dispositivos, optimizadas para ofrecer la mejor legibilidad posible. Además, suelen permitir su uso bajo la luz directa y su consumo de energía es mucho menor que el de, por ejemplo, una *tablet*. Esta característica hace que sean ideales para su función principal, la de replicar lo mejor posible la experiencia de estar leyendo un libro en papel. Asimismo, poseen un diseño ligero y delgado que facilita la lectura.

Relojes inteligentes

En cuanto a los relojes inteligentes, o *smartwatch*, son el equivalente electrónico de los relojes analógicos de toda la vida. Aunque cada vez son más independientes, suelen emplearse como un complemento de los teléfonos inteligentes, conectándose a ellos habitualmente a través de *Bluetooth*. Además, algunos dispoitivos suelen disponer de conectividad Wi-Fi, por lo que es posible vulnerar su seguridad e, incluso, comprometer al *smartphone* al que están enlazados. Incorporan también pantallas táctiles y otras características, como navegación GPS, notificaciones de mensajes y llamadas, monitorización de la actividad física e, incluso, funcionalidades avanzadas como la posibilidad de realizar un cardiograma o medir la saturación de oxígeno en sangre.

Precauciones al acceder a una Wi-Fi publíca

Muchas personas pasan varias horas al día navegando por la web, visualizando contenidos, comunicándose o utilizando múltiples apps que se conectan a internet. El tiempo que empleamos en la Red no deja de aumentar, ya sea por el uso de nuevas formas de ocio, como las plataformas de *streaming* de cine y series o los videojuegos, como por el teletrabajo o simplemente chateando. Y aunque no siempre nos lo planteemos directamente, lo cierto es que queremos asegurarnos de que todas estas actividades las hacemos