# Seguridad en Dispositivos Móviles: Amenazas Desconocidas en las Empresas

**Cadena, Alejandra**[1]

[1]*Instituto Superior Tecnológico de Tecnologías Apropiadas INSTA, Quito, Ecuador*

**Resumen:** Los dispositivos móviles en la actualidad se han convertido en una herramienta fundamental no solo a nivel profesional, estos dispositivos móviles son empleados para diversos fines, redes sociales, telemática, comercio electrónico, banca móvil, empresarial, entre otros. Por ese motivo, foco de atención para actos ilícitos tales como, suplantación de identidad, robo de datos y otros. Los delincuentes, especialmente aprovechan el desconocimiento de la ciudadanía en general acerca de estos temas, el desconocimiento y el nivel de implicaciones para una empresa o nivel personal hace de las prácticas ilícitas una corriente cada vez más común. Un estudio revelo que en América Latina el 74% de las empresas han sufrido un ataque por un problema de seguridad móvil y como consecuencia el robo de información. En ese sentido, en el presente artículo se aborda información relevante, que debe ser tomada en cuanta para mitigar esto que se ha convertido en una amenaza para todos quienes empleamos un dispositivo móvil.

**Palabras clave: C**iberseguridad, robo de datos, malware.

# Movile Device Unknown Threat in Companies

**Abstract:** Mobile devices today have become a fundamental tool not only at a professional level, these mobile devices are used for various purposes, social networks, telematics, electronic commerce, mobile banking, business, among others. For this reason, the focus of attention for illegal acts such as identity theft, data theft and others. Criminals, especially take advantage of the general public's ignorance about these issues, the ignorance and the level of implications for a company or personal level makes illegal practices an increasingly common trend. A study revealed that in Latin America 74% of companies have suffered an attack due to a mobile security problem and as a consequence the theft of information. In this sense, this article addresses relevant information, which must be taken into account to mitigate this, which has become a threat to all of us who use a mobile device.

**Keywords:** Cybersecurity, data theft, malware.

## INTRODUCCIÓN

El uso de dispositivos móviles ha traído un gran beneficio a nivel empresarial pero claramente hay un riesgo por la manipulación de información, lo que conlleva el robo de datos para una posterior extorsión para la recuperación de los mismos, una gran vulnerabilidad es cuando en las empresas comparten vínculos corporativos para todos sus colaboradores. Un ciberataque conocido es una técnica que realiza la suplantación de identidad conocida como phishing, tiene como objetivo robar información confidencial y contraseñas para proporcionar accesos a la banca u otros archivos sensibles.
Los trabajadores de las empresas son los más vulnerables ya que cada uno dispone de un dispositivo móvil y pasa con el todo el día, a su vez la gran mayoría de personas desconoce de estas formas de ataque así como también no cuentan con recursos económicos para protegerse correctamente

Según datos del Instituto Nacional de Seguridad (Incibe), España sufrió el año pasado 123.000 ataques de ciberseguridad, un crecimiento exponencial si se tiene en cuenta que hace tres años se detectaron 18.000 delitos de este tipo, según expuso su director, Alberto Hernández Moreno.

Además, el vicepresidente de Cepyme, Gerardo Cuerva, precisó que el "53% de las pymes sufrieron un ataque cibernético en 2017″ y que nos encontramos "no sólo ante un problema empresarial, sino un problema estatal" (Ciberseguridad, 2018)

### El peligro de los USB

En la mayoría de ataques a nivel de seguridad han sido causados por el mal uso de dispositivos de almacenamiento los cuales son conectados a un ordenador o dispositivo móvil.

Toda la información guardada en estos dispositivos no son cifrados y cuando existe un ultraje, esta información esta vulnerable y la mejor forma de proteger estos datos es mediante un cifrado y una contraseña, el formateo de un dispositivo no asegura la desaparición de la información, la utilización de antivirus actualizados permite analizar de manera continua los archivos, los dispositivos USB pueden ser más que memorias puede incluir micrófonos, cámaras lo que

mayra.cadena@insta.edu.ec

no son detectados por el antivirus, cabe recalcar que el dispositivo es una herramienta útil y sencilla pero de exenta de peligros. (Ciberseguridad, 2018)

**Aplicaciones de Origen Desconocido**

Ten cuidado con las aplicaciones que descargas, a menudo los hacker's se molestan en duplicar aplicaciones conocidas de pago para sacar copias en versión gratuita que pueden generar brechas en nuestra seguridad. Cuando descargues una app, observa el rendimiento del móvil durante un par de días: si se calienta o va mucho más lento de lo habitual ten cuidado.

El malware puede llegar de todas partes, desde una inocente aplicación de fotos hasta una guía para tu juego favorito. Existen muchos mecanismos para evitar estas aplicaciones maliciosas pero al final la responsabilidad recae en el propio usuario, quien debe ser consciente de qué está instalado y cómo puede llegar a afectarle. (Tecnologia, 2018)

**Desventajas de Dispositivos Móviles**

El hecho de trabajar con dispositivos móviles conlleva una serie de riesgos importantes para la seguridad de las empresas, como por ejemplo: pérdida o robo de información, el mal uso que se pueda hacer de los dispositivos robo de los mismos, robo de credenciales, utilización de sistemas de conexión no seguros, etc. (Android, 2017)

**Ventajas de Dispositivos Móviles**

La utilización de dispositivos móviles personales para uso profesional, proporciona muchas ventajas para la empresa y para el empleado, entre ellas: reducción de costes y ahorro en inversión de dispositivos reducción de costes en desplazamientos aumento en la productividad y en el rendimiento de trabajo del empleado mayor satisfacción y flexibilidad de los empleados que hace que aumente su compromiso con la empresa eficiencia en el servicio al gestionarlo en tiempo real. (Android, 2017)

**Robo de Credenciales**

La utilización de los dispositivos personales para uso corporativo en lugares fuera de la oficina como hoteles, medios de transporte, estaciones de trenes o aeropuertos, bares, restaurantes, etc. o la propia casa del empleado, los hace especialmente sensibles al posible robo de sus credenciales de acceso. Cualquier descuido como: abandonar el equipo sin bloquear la sesión de usuario tener apuntada una contraseña a la vista de los demás en un papel, post-it, etc. teclear la contraseña a la vista de los demás tener memorizadas las contraseñas de las aplicaciones que utilizamos puede llevar a que se produzca el robo de nuestras credenciales de usuario, y a que un usuario no autorizado pueda acceder a los recursos de nuestra empresa. La utilización de estos dispositivos en situaciones fuera del entorno empresarial y la relajación en la aplicación de las normas básicas de seguridad, hace que sea más sencillo que se produzca un robo de credenciales. Por ejemplo, podemos eliminar temporalmente la contraseña de acceso a nuestro smartphone para que nuestro hijo juegue con él, y olvidarnos restituirla. (Guia de dispositivos móviles, 2017)

**Conexión A Redes Inseguras**

Habrá situaciones en las que el empleado deba conectar a la red los dispositivos móviles fuera de la protección que brindan las redes privadas del entorno laboral. Ya sea por ahorro en la tarifa de datos, por no tener cobertura, por no disponer de cobertura 3G o 4G, es habitual utilizar redes públicas abiertas o poco seguras para el intercambio de correo electrónico corporativo o acceder a aplicaciones de la empresa. Este tipo de redes podemos encontrarlas como servicio de cortesía en bares, restaurantes, hoteles, aeropuertos, etc. Debemos desconfiar de estas redes ya que no sabemos quién puede estar detrás de ellas o quien las administra. Antes de utilizarlas, debemos informarnos cuál es el nombre de la red (SSID) y si está debidamente protegida para que nos podamos conectar con un mínimo de confianza. Hay casos en los que los ciberdelincuentes crean una red wifi en zonas públicas con nombres similares al del lugar donde se encuentran con el objetivo de capturar conexiones y recopilar información. (Guia de dispositivos móviles, 2017)

**Medidas de Seguridad**

Tanto los dispositivos móviles personales para uso profesional como la información corporativa que manejan estos, deben estar protegidos convenientemente, estableciendo unas buenas medidas de seguridad que ayuden a reducir todo lo posible los riesgos a los que están expuestos. A continuación se detallan algunas medidas que deben tenerse en cuenta para mitigar los riesgos a los que nos enfrentamos. Medidas como: la debida protección de la información la correcta configuración de los dispositivos o la protección de la conexión a redes inalámbricas Para implementar estas medidas, podemos incorporar herramientas específicas que gestionan dispositivos móviles y el uso de la información corporativa que se realice desde estos. En el mercado, existen diversas soluciones como los programas de gestión de dispositivos móviles o MDM (del inglés Mobile Device Management) que administran y monitorizan los dispositivos móviles de nuestras empresas. De esta forma, tendremos controlados los dispositivos y podremos valorar el grado de implantación de las medidas de seguridad de nuestra política de seguridad. Con estas herramientas será posible gestionar y controlar: los dispositivos autorizados para acceder a aplicaciones y recursos las aplicaciones instaladas en los dispositivos las configuraciones de seguridad de los dispositivos, de su wifi y de su VPN las manipulaciones indebidas de los terminales como la detección de jailbreak en iOS o rooteo en Android el bloqueo remoto de dispositivos extraviados la destrucción/formateo remoto de datos de dispositivos extraviados o robados el cifrado de datos o del dispositivo la detección de malware la fortaleza y renovación de contraseñas, etc. En el caso especial de los dispositivos personales para uso en la empresa, debemos de tener especial cuidado. Para asegurarnos el éxito de la implementación de todas estas medidas, es esencial conseguir involucrar a los usuarios en la protección de sus dispositivos. Debemos incentivar, concienciar y formar al usuario para que tome medidas destinadas a proteger los datos corporativos y personales por igual. (Emprendedores, 2018)

### Autentificación Biométrica

En línea con las amenazas y la incipiente preocupación por la protección de la privacidad, el informe destaca la consolidación de los sistemas de autentificación biométrica como el elemento más habitual para el desbloqueo de estos dispositivos.

En definitiva, estas son solo algunas de las previsiones en cuanto a las amenazas a uno de los dispositivos más importantes para llevar a cabo las acciones del día a día en una sociedad cada vez más digitalizada.

Por ello, para no poner en peligro la sociedad del bienestar y las innovaciones tecnológicas, es necesario una investigación continua y la formación de profesionales en un área donde la oferta y la demanda aún no se encuentran para dar solución a los problemas en ciberseguridad. (Emprendedores, 2018)

### Análisis en datos de Ciberdelincuencia.

La ciberdelincuencia no tiene fronteras y la impunidad que proporciona la distancia, los delitos son perpetrados a miles de kilómetros, impide además actuar de manera contundente y precisa. La ciberseguridad es una ciencia viva, evoluciona a la vez que los riesgos y amenazas, requiere de un rápido aprendizaje y aportar soluciones también ágiles, y precisa de profesionales en constante observación y alerta.

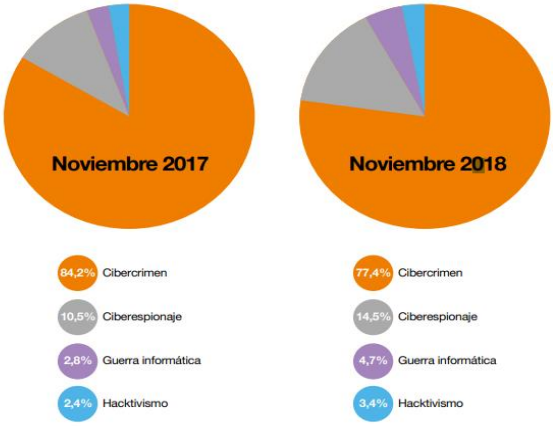


**Figura 1.** Motivaciones de la Ciberdelincuencia

Las amenazas son mayores que la capacidad de monitorizarlas: el 44% de las amenazas diarias no se investigan.

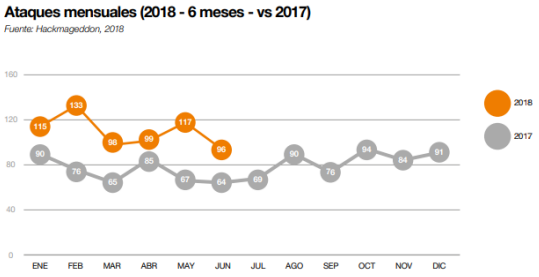


**Figura 2.** Ataques mensuales año 2017-2018

En el 69,9% de los ordenadores y el 77,9% de los teléfonos móviles analizados en España se han encontrado archivos maliciosos. Las empresas han pasado de sufrir 18.000 ciberataques a más de 100.000 desde 2014. La inversión en ciberseguridad de las empresas en España se ha duplicado desde 2012. La ciberseguridad con un ritmo de crecimiento anual del 13%, y creará más de 1 millón de puestos de trabajo en Europa. (Guia de dispositivos móviles, 2017)

### Conexión a Redes Inseguras

Habrá situaciones en las que el empleado deba conectar a la red los dispositivos móviles fuera de la protección que brindan las redes privadas del entorno laboral. Ya sea por ahorro en la tarifa de datos, por no tener cobertura, por no disponer de cobertura 3G o 4G, es habitual utilizar redes públicas abiertas o poco seguras para el intercambio de correo electrónico corporativo o acceder a aplicaciones de la empresa. Este tipo de redes podemos encontrarlas como servicio de cortesía en bares, restaurantes, hoteles, aeropuertos, etc. Debemos desconfiar de estas redes ya que no sabemos quién puede estar detrás de ellas o quien las administra. Antes de utilizarlas, debemos informarnos cuál es el nombre de la red (SSID) y si está debidamente protegida para que nos podamos conectar con un mínimo de confianza. Hay casos en los que los ciberdelincuentes crean una red wifi en zonas públicas con nombres similares al del lugar donde se encuentran con el objetivo de capturar conexiones y recopilar información. (Guia de dispositivos móviles, 2017)

### Medidas de Seguridad

Tanto los dispositivos móviles personales para uso profesional como la información corporativa que manejan estos, deben estar protegidos convenientemente, estableciendo unas buenas medidas de seguridad que ayuden a reducir todo lo posible los riesgos a los que están expuestos. A continuación se detallan algunas medidas que deben tenerse en cuenta para mitigar los riesgos a los que nos enfrentamos. Medidas como: la debida protección de la información la correcta configuración de los dispositivos o la protección de la conexión a redes inalámbricas Para implementar estas medidas, podemos incorporar herramientas específicas empresa. La utilización de los dispositivos personales para uso corporativo en lugares fuera de la oficina como hoteles, medios de transporte, estaciones de trenes o aeropuertos, bares, restaurantes, etc. o la propia casa del empleado, los hace especialmente sensibles al posible robo de sus credenciales de acceso. Cualquier descuido como: abandonar el equipo sin bloquear la sesión de usuario tener apuntada una contraseña a la vista de los demás en un papel, post-it, etc. teclear la contraseña a la vista de los demás tener memorizadas las contraseñas de las aplicaciones que utilizamos puede llevar a que se produzca el robo de nuestras credenciales de usuario, y a que un usuario no autorizado pueda acceder a los recursos de nuestra empresa. La utilización de estos dispositivos en situaciones fuera del entorno empresarial y la relajación en la aplicación de las normas básicas de seguridad, hace que sea más sencillo que se produzca un robo de credenciales. Por ejemplo, podemos eliminar temporalmente la contraseña de acceso a nuestro smartphone para que nuestro hijo juegue con él, y olvidarnos restituirla. (Guia de dispositivos móviles, 2017)

## CONCLUSIONES

Los dispositivos móviles sufren de constantes amenazas, debido a que guardan información personal y empresarial, en ese sentido, son el principal y punto de ataque. Con la evolución de la tecnología, los móviles están expuestos a redes externas poco seguras, así como, a aplicaciones de origen desconocido.

En el último año la ciberdelincuencia se ha incrementado más de lo habitual, debido a que el robo de información se ha convertido en un gran negocio, el phishing es un ejemplo de secuestro de información que pretende extorsionar a la víctima a cambio de la recuperación de datos.

## BIBLIOGRAFÌA

Android, K. (2017). *Seguridad en los androids.* Obtenido de https://www.xatakandroid.com/seguridad/he-instalado-todos-los-malware-de-android-esto-es-lo-que-ocurre-si-te-saltas-los-consejos-de-seguridad

Ciberseguridad. (2018). *Seguridad en dispositivos móviles: la mayor ciberamenaza está al alcance de tus manos.* Obtenido de [1]: https://www.iniseg.es/blog/ciberseguridad/seguridad-en-dispositivos-moviles/

Emprendedores. (2018). *Claves de seguridad para el móvil.* Obtenido de https://www.emprendedores.es/gestion/a27551265/claves-ciberseguridad-movil-seguridad-informatica-empresas/

móviles, G. d. (2017). *Dispositivos móviles personales para uso profesional BYOD.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

Tecnologia. (2018). *Peligro en los usb.* Obtenido de https://ticnegocios.camaravalencia.com/servicios/tendencias/guia-ciberseguridad-el-peligro-de-los-usb/