Universitat Oberta de Catalunya

Guía para proteger y usar de forma segura su móvil en la empresa

Guía del trabajador

INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDICE

1 Introducción

La capacidad tecnológica en movilidad actual: wifis, 3G, 4G… las necesidades empresariales: movilidad de los trabajadores, inmediatez en la obtención de datos… y las capacidades de los dispositivos móviles de los usuarios: tabletas y teléfonos móviles con altas prestaciones, están acelerando el crecimiento del denominado BYOD (*Bring Your Own Device*).

El BYOD es una forma de trabajo en la que las empresas permiten a los trabajadores utilizar sus dispositivos móviles personales para llevar a cabo tareas del trabajo accediendo a los recursos de la compañía.

Este nuevo concepto en el uso de los dispositivos de los propios trabajadores abre un nuevo campo en cuanto a la capacidad del trabajador para realizar tareas laborales desde sus dispositivos móviles personales. Conforme aumentan las capacidades tecnológicas de los dispositivos móviles también aumenta su uso en el puesto de trabajo. Los números y las estadísticas reflejan una claro aumento en el número de dispositivos móviles a nivel mundial y un mayor uso de estos dentro del mundo laboral.

Esta nueva forma de relación laboral lleva implícita muchas ventajas, pero también sus desventajas.

Como ventajas destacan las siguientes:

Ventajas del uso de BYOD
Incremento en la satisfacción del trabajador ya que le permite trabajar con más flexibilidad.
Incremento de la productividad de los empleados debido a que los trabajadores se encuentran más cómodos trabajando con sus aplicaciones y dispositivos.
Mejora en la atención al cliente al poder responder ante cualquier petición en cualquier momento.
Ahorro en los costes de adquisición de tecnología por parte de la empresa debido a que los trabajadores pagan parcial o totalmente sus dispositivos y se pueden utilizar programas gratuitos de la nube.

No obstante, diversos estudios[1] demuestran que empleados y empresas cometen imprudencias que ponen en peligro los datos que contienen o a los que acceden los dispositivos móviles personales. Estas imprudencias pasan por usuarios que prestan sus dispositivos a otras personas, usuarios que guardan contraseñas en el móvil, dispositivos que no tienen activas las opciones de bloqueo, falta de implementación de políticas y administración en las empresas para el uso del móvil personal en la empresa, uso de redes wifi de forma insegura, mezcla de correos personales con laborales.

Estos actos provocan que sean varias las desventajas del uso del BYOD:

Desventajas del uso de BYOD
Riesgo para la seguridad de los datos, tanto de la empresa como del propio trabajador.
Posibilidad de infección de la red si un usuario se conecta infectado con malware[2].
Mayor consumo de los recursos de la red.
Necesidad de reforzar los departamentos y políticas de soporte informático y de Tecnologías de la Información (TI) para dar respuesta a las problemáticas generadas por la multitud de dispositivos y programas.

Esta nueva forma de relación trabajador-empresa implica riesgos para la información de la empresa y los datos personales del trabajador (cuentas de correo, usuario de banca online, cuentas corrientes…) si no se realizan las acciones adecuadas en cuanto a la protección de los mismos. Esto provoca que sea de especial interés el estudio de las debilidades del uso de los dispositivos móviles tanto para garantizar la

[1] http://www.ribbit.net/frogtalk/id/143/byod-stats-what-business-leaders-need-to-know-right-now http://www.forbes.com/sites/markfidelman/2012/05/02/the-latest-infographics-mobile-business-statistics-for-2012/

[2] Programas maliciosos creados para manipular el funcionamiento normal de los sistemas sin el conocimiento ni consentimiento de los usuarios. Estos programas tratan de alterar el funcionamiento normal del equipo así como la información que contienen o manejan. El objetivo de estos ataques pueden ser múltiples: reconocimiento público, uso del sistema para realizar actos delictivos, obtención de datos…

seguridad de los datos personales como los de la empresa prestando atención a las siguientes vulnerabilidades:

Vulnerabilidades de los dispositivos móviles	
Robo o pérdida de móviles.	Cada vez que un móvil es robado los datos que contiene y aquellos datos accesibles desde aplicaciones instaladas en el móvil pueden ser robadas y usadas con fines desconocidos.
Instalación de aplicaciones infectadas con capacidad para robar datos.	La utilización de markets de aplicaciones sin ningún proceso de validación, han hecho que los ciberdelincuentes publiquen aplicaciones con malware insertado que permiten realizar cualquier tipo de actividad maliciosa.[3]
Instalación de aplicaciones con capacidad de acceso a datos.	Existen aplicaciones que utilizan más permisos de los realmente necesarios para su uso y funcionamiento con el objeto de extraer todo tipo de información del dispositivo. Este tipo de aplicaciones podría poner en riesgo la información de la empresa.
Análisis de envío y recepción de datos a través de conexiones inseguras (WIFI de un bar, bluetooth mal configurado...).	Puntos de acceso gratuitos, pero sin medidas de seguridad adecuadas que pueden permitir a terceras personas analizar nuestro tráfico de red y obtener datos relevantes.
Préstamo del móvil a otra persona.	El hecho de dejar el móvil a terceros, si dentro del dispositivo gestionamos información y credenciales relacionadas con nuestra empresa, se considera una práctica de alto riesgo por los posibles usos que se pudiera hacer de la misma consciente o inconscientemente.
Ataques de ingeniería social.	Un atacante podría instar a realizar alguna acción en el dispositivo móvil poniendo en peligro los datos almacenados o accesibles desde él: ejecutar fichero (con malware) u obtener datos de forma directa (simulando un pago al banco, intentado sacar más respuestas de las debidas a través del envío de

[3] En un estudio reciente realizado por Alcatel-Lucent publicado el 9 de septiembre de 2014 muestra que las amenazas a dispositivos móviles y equipos de escritorio aumentaron considerablemente durante el primer semestre de 2014. En el informe se asegura que los casos de malware en dispositivos móviles se vieron incrementados en un 17% durante ese primer semestre de 2014.

	correos....).
Tipo de acceso permitido a los datos de empresa.	Una mala gestión de los accesos y permisos otorgados a los datos de empresa accesibles desde los dispositivos móviles podría facilitar la obtención y acceso a estos datos por parte de un atacante.

2 Problemas y ataques en el uso de los dispositivos móviles

A través de ataques a dispositivos móviles que son utilizados en el entorno empresarial, un atacante podría obtener información tanto del propio usuario como de la propia entidad en la que trabaja.

Por lo tanto y de forma resumida estos ataques implican básicamente dos riesgos:

Riesgos del uso de BYOD para la empresa
Pérdida de datos directa desde el dispositivo: Robo/eliminación/ modificación de ficheros accesibles desde el dispositivo.
Robo de identidad que permita el acceso a diferentes servicios/ficheros de la empresa.

Estos riesgos hacen que a la hora de gestionar los datos se deban controlar distintos parámetros referentes a la seguridad de los datos de la empresa teniendo en cuenta:

Factores de seguridad a tener en cuenta
A qué datos se tiene acceso desde los dispositivos móviles
Donde pueden estar almacenados los datos
Como se transfieren los datos
La posibilidad de fuga de datos
El uso personal y de negocio de forma simultánea
La capacidad y configuración de seguridad del dispositivo
Qué hacer si el propietario del dispositivo cesa en su puesto de trabajo
Como tratar la pérdida, robo… de un dispositivo

2.1 Tipos de ataques

Los diferentes tipos de ataque han sido en muchos casos una adaptación a la tecnología móvil de los ya existentes. Pueden realizarse a través de dispositivos móviles o hacia ellos y que pueden comprometer los datos del trabajador y de la empresa son:

- **Malware:** (virus, código malicioso…): Programas maliciosos creados para manipular el funcionamiento normal de los sistemas sin el conocimiento ni consentimiento de los usuarios. Estos programas tratan de alterar el funcionamiento normal del equipo así como la información que contienen o manejan. El objetivo puede ser múltiple: uso del sistema para realizar actos delictivos, obtención de datos… actualmente la mayoría de ataques tienen un fin económico, aunque en ocasiones puede buscarse un reconocimiento público. El malware trata de ser los

más silencioso posible para poder actuar el máximo tiempo posible. A través de un ataque malware al dispositivo móvil un atacante podría:

- Robar información sensible (datos o credenciales).
- Usar el móvil dentro de una red zombie[4].
- Cifrar, borrar o modificar ficheros.
- Infectar la red corporativa.

El malware puede infectar un dispositivo móvil de diversas formas: explotando una vulnerabilidad de cualquier aplicación instalada en el sistema, usando ingeniería social, a través del envío de archivos maliciosos (adjuntos a un mensaje, fichero en una web, APPs maliciosas…), a través de dispositivos extraíbles infectados… Actualmente el malware es un tipo de ataque en crecimiento por lo que hay que tener mucho cuidado con este tipo de ataque.

- **Privilegios y permisos de las aplicaciones:** Cuando se instala una aplicación en un dispositivo móvil la aplicación requiere que se acepten una serie de permisos que, supuestamente, son necesarios para funcionar correctamente. En caso de no aceptar estos permisos la aplicación no se instalará. La mayoría de veces, los usuarios, suelen aceptar estos permisos sin ni siquiera haberlos leído, por lo que no se analiza dónde tendrá acceso la aplicación que se está instalando. Como una aplicación puede solicitar permisos para prácticamente cualquier función del dispositivo (acceso a las herramientas del sistema, acceso a la red de datos, acceso a la lista de contactos, acceso al historial web…) un programador podría encubrir en una simple aplicación algo más que lo que se cree que se está instalando. Simplemente aceptando este exceso de permisos y privilegios en una aplicación podemos provocar que la aplicación ayude a un atacante a:
  - Robar información sensible (datos o credenciales).
  - Cifrar, borrar o modificar ficheros.
  - Usar el dispositivo móvil usando cualquiera de sus capacidades (envío de mensajes, conexión a internet…).

- **Ataques a través de redes wifi:** La flexibilidad y movilidad que aportan las redes inalámbricas ha hecho que actualmente sea el sistema wifi el sistema más elegido para la conexión de datos en edificios y espacios abiertos. El uso del aire como medio de transmisión provoca que la señal enviada llegue no solo al dispositivo destino sino a muchos otros que puedan estar dentro del alcance. Tanto los dispositivos que se conectan a los puntos de acceso de una red wifi, como los

[4] Red formada por un conjunto de equipos infectados con un tipo de software malicioso que permite al atacante controlar los equipos sin el consentimiento ni el conocimiento del propietario. Normalmente se usan para realizar acciones ilegítimas o ilegales de forma conjunta.

dispositivos que sostienen esta red y las señales de comunicaciones que se transfieren están expuestos a diversos ataques (sniffing[5], spoofing[6] , modificación de los datos enviados…) que pueden permitir a un atacante leer, insertar y modificar mensajes entre dos usuarios o sistemas.

Este ataque podría realizarse cuando el usuario de la empresa esté usando su dispositivo móvil desde alguna red desconocida y quizás insegura como podría ser la wifi de un bar o de un aeropuerto.

Atacando a una red wifi un atacante podría afectar al dispositivo del trabajador y a la empresa:

- Robando información sensible (datos o credenciales).
- Desviando correos a otro destino, modificarlos y enviarlos o no al destinatario, con el perjuicio que comportarían estos actos para la empresa. Con esto podría perjudicar la relación con clientes o conocidos, añadir malware a los correos…

- **Ataques a bluethoth:** Como en el caso anterior el uso del aire como medio de transmisión hace que la señal enviada no solo llegue al destino sino también a los dispositivos dentro de un determinado alcance. Un atacante puede aprovechar el uso del bluethooh para realizar diversos ataques (bluebug[7], blueSnarf[8]) a los dispositivos que lo tengan activo.

Como en los casos anteriores nos encontramos con un tipo de ataque que puede acarrear problemas para al dispositivo del usuario y la empresa, ya que un atacante podría:

- Robar información.
- Enviar mensajes o realizar llamadas no deseadas.

- **Ingeniería social:** Un ataque de este tipo consiste en la manipulación de las víctimas con el fin de obtener información confidencial o para convencerles de que realicen alguna acción que comprometa su sistema. Gracias a las formas de

[5] Es uno de los ataques más sencillos consistente en la intercepción de datos inalámbricos que se está emitiendo en una red wifi. La forma más habitual es a través de un software que captura la información de red pese a que también puede realizarse por hardware. Aquel tráfico que no esté cifrado, o lo esté con un sistema débil será accesible para el atacante.

[6] El atacante se hace pasar por un punto de acceso y el cliente piensa estar conectándose a una red WLAN verdadera.

[7] Ataque que permite ejecutar comandos AT (instrucciones codificadas que conforman un lenguaje de comunicación entre el hombre y un terminal móvil o módem) en el terminal sin necesidad de autenticación donde el atacante podría obtener del celular: la agenda telefónica, calendario, modificar o borrar entradas en los contactos, enviar SMS…

[8] Ataque que permite extraer archivos de un teléfono móvil sin previa autorización del propietario. Con este ataque un atacante puede obtener los contactos, el calendario y otros datos de otro usuario.

comunicación en línea que hay actualmente (redes sociales, correo…) este tipo de ataques están en aumento. La ingeniería social se sustenta en el principio de que "el usuario es el eslabón débil".

Aparte de la adaptación de lo ya existente fuera de la tecnología móvil, como por ejemplo, recibir llamadas suplantando nuestro departamento de informática solicitando nuestras credenciales , podemos encontrarnos con otros ataques más adaptados como los phishing attacks, uno de los métodos más usados. Un phishing attack es un fraude informático que utiliza el email, SMS, web… para convencer a la víctima de que revele cierta información (pin bancario, usuarios de redes sociales…) o realice cierta actividad (entrar en una web falsa y realizar un pago…).

A través de un ataque de ingeniería social un atacante podría:

- Obtener información sensible (datos o credenciales).
- Infectar con malware el dispositivo móvil y este a la red corporativa.
- Obtener un pago de la empresa o del usuario.

- **Ataques a 2G/3G/4G:** A través de estos estándares de comunicación de telefonía comunes, también se pueden llevar ciertos ataques con el objetivo de perjudicar al propietario del dispositivo móvil o bien a la empresa donde trabaja.

Aunque esta tecnología es totalmente obsoleta, en 2G la seguridad es prácticamente nula y sus protocolos y algoritmos de cifrado presentan multitud de vulnerabilidades permitiendo a un atacante una serie de ataques (ataques de escucha pasiva[9], ataques de escucha activa[10], ataques de denegación de servicio[11]).

En 3G la seguridad es más elevada, pese a ello se puede llevar un ataque de denegación de servicio (hacer que la red 3G no esté disponible) que obligue al dispositivo móvil a cambiarse a 2G y una vez conectado a 2G se podría llevar a cabo algún tipo de ataque a 2G. También es vulnerable a otro tipos de ataques (man-in-the-middle[12], eavesdropping[13]).

Para 4G, basada en tecnología IP, existen también una serie de ataques (man-in-the-middle, eavesdropping y ataques a los recursos de radio para provocar una denegación de servicio) que no hacen de esta tecnología una tecnología libre de vulnerabilidades.

[9] Permiten la intercepción, escucha de llamadas, suplantación de identidad y obtención de SMS.

[10] El atacante actúa como una estación base falsa que actúa sustituyendo a la del operador sin que la víctima detecte anomalía.

[11] Ataques de denegación de servicio a ciertos usuarios y semipermanentes haciendo que esos usuarios no puedan hacer uso de la red 2G.

[12] Permiten permanecer en medio de una conversación y escucharla.

[13] Consistente en la escucha pasiva de una comunicación de forma que un atacante puede capturar información privilegiada y claves para acceder con posterioridad a más información.

A través de los ataques que se pueden llevar a cabo a través de 2G, 3G y 4G un atacante podría:

- Denegar el servicio a un dispositivo concreto.
- Obtener información sensible (datos o credenciales) a través de escuchas telefónicas.

- **Ataques a NFC (Near field communication):** Esta tecnología permite la transmisión e intercambio de datos de forma inalámbrica entre dispositivos móviles próximos (20 cm) de forma instantánea y sin necesidad de emparejamiento entre ellos. Se usa mayoritariamente para realizar pagos sin necesidad de usar tarjetas o dinero en efectivo, intercambio de datos y automatización de tareas como ejecutar aplicaciones o realizar llamadas. NFC tiene una serie de vulnerabilidades con las que un atacante podría:
  - Robar información sensible (datos o credenciales).
  - Cifrar, borrar o modificar el contenido de los ficheros o los propios ficheros.
  - Descargar malware e infectar el equipo.
  - Intercepción, lectura y modificación de los datos que se transmiten entre dispositivos mediante un ataque man-in-the-middle.

- **Robo o pérdida del dispositivo móvil:** A partir del robo de un dispositivo móvil un atacante podría acceder a todos los datos del dispositivo móvil y a todos aquellos datos remotos accesibles desde el propio terminal.

Así pues, podemos afirmar que en las tecnologías inalámbricas que podemos encontrar en un dispositivo móvil existen una serie de riesgos. En mayor o menor medida podrían permitir a un atacante obtener información y datos del mismo dispositivo móvil o de otras ubicaciones (bien a través de credenciales robadas o de aplicaciones que hagan de puente desde el dispositivo móvil).

Para mitigar el riesgo, se hace indispensable un correcto uso del dispositivo por parte de los usuarios (que pueden ser víctimas directas o puentes para otros ataques). Para ello, la empresa debe aportar recursos para la protección de sus datos, así como concienciar y formar a sus trabajadores para la correcta gestión y uso de los dispositivos móviles personales en los entornos empresariales. Una correcta política en los aspectos anteriores permitirá a la empresa y a los trabajadores tener un nivel elevado de seguridad tanto en sus datos personales como en los empresariales.

3 Situaciones de riesgo

Como se ha visto en los apartados anteriores el BYOD trae consigo ventajas y desventajas. Dentro de las situaciones de riesgo con las que nos podemos encontrar se encuentran las siguientes:

Situaciones de riesgo	
Conexiones a wifis públicas (bares, hoteles, aeropuertos)	Cuando un usuario realiza conexiones de este tipo se está exponiendo a recibir ataques a través de este medio. Si el usuario no tiene en cuenta esto y no aplica medidas de seguridad o preventivas podría recibir ataques en los que podría ver comprometida sus datos (como por ejemplo el PIN bancario) o los de la empresa (identidad del correo).
Abrir un archivo adjunto de un correo desconocido	Puede provocar la infección con malware del dispositivo. Este malware puede tener varios objetivos, entre ellos, el robo o borrado de datos disponibles en el dispositivo móvil.
Tener activo el bluetooth	Incrementa las posibilidades de recibir un ataque que aproveche el dispositivo móvil para realizar/desviar llamadas de voz, enviar/borrar/leer mensajes, modificar la agenda. Por ejemplo, se podría usar el dispositivo atacado como un dispositivo espía: el dispositivo móvil atacado podría recibir la orden de realizar una llamada a otro dispositivo desde el cual se descolgaría la llamada y se podría escuchar la conversación que esté teniendo el propietario del dispositivo atacado.
Descarga de aplicaciones desde markets no oficiales, o de aplicaciones con mala reputación.	Descargar una aplicación aparentemente simple (por ejemplo una aplicación con función de linterna) puede provocar que estemos instalando en el dispositivo una aplicación con malware con fines desconocidos. Instalar aplicaciones de

	dudosa fiabilidad podría provocar que estuviésemos dando el control del dispositivo a algún atacante.
No usar el bloqueo de pantalla	Puede provocar que en caso de robo o pérdida del terminal el acceso a los datos alojados en él sea más rápido y sencillo.
Aceptar el guardado de una contaseña	Facilita la obtención de esa contraseña por parte de un atacante.
Guardar usuarios y contraseñas en el navegador	Puede provocar que se le facilite la tarea a un atacante a la hora de obtener credenciales del usuario del dispositivo móvil (por ejemplo: robo de la identidad para acceso a las cuentas bancarias, obtención de la cuenta de correo, del usuario de acceso a un ftp…)
Realizar jailbreak[14] en iOS o root[15] en Android	Puede provocar que se facilite el robo de información del dispositivo. Al realizar estas acciones se le dan al usuario opciones que no tendría si no las llevara a cabo y vuelven el dispositivo en más vulnerable.
Guardar un número PIN o contraseña en una nota de la aplicación	Facilita la obtención de datos a un atacante.

[14] Proceso de suprimir algunas limitaciones impuestas por Apple en los dispositivos que utilitzan iOS permitiendo a los usuarios acceder por completo al sistema operativo. De este modo, el usuario puede descargar aplicaciones, extensiones… no disponibles a través de la App Store oficial. Con esto, el usuario puede correr software no autorizado por Apple.

[15] Modificación del sistema operativo Android para tener total control de éste. Con esto, se pueden superar todas las limitaciones que el fabricante pone sobre el dispositivo móvil, pudiendo, incluso, cambiar el sistema operativo del dispositivo.

4 Recomendación para el uso del dispositivo móvil

Para minimizar el riesgo de recibir algún ataque que provoque algún mal funcionamiento de nuestro dispositivo móvil o provoque algún robo de datos personal o empresarial debemos tomar una serie de medidas a la hora de utilizar el dispositivo móvil.

El usuario del dispositivo deberá controlar sus acciones y tener cura de que los datos y credenciales almacenados en el dispositivo estén solo disponibles para él. La empresa deberá facilitar herramientas para que el usuario pueda interactuar de forma segura con los datos de la empresa y hacer de su dispositivo un dispositivo lo más seguro posible.

A continuación se detallan una serie de recomendaciones que permiten hacer un uso seguro del dispositivo protegiendo el máximo posible los datos que contiene y las credenciales que tiene almacenadas.

Recomendaciones para el uso del dispositivo móvil	
Bloquear el dispositivo móvil y habilitar un mecanismo de autenticación para su acceso	Además del número PIN de la tarjeta SIM es necesario añadir una contraseña (numérica o de patrón) en el dispositivo para evitar el acceso de terceros.
Habilitar el bloqueo automático cuando el dispositivo lleve un cierto tiempo inactivo	Con esto conseguiremos que tras unos pocos minutos (configurados en el terminal) de inactividad el terminal se bloquee por sí mismo haciendo necesario el uso del PIN de desbloqueo del punto anterior para volver a acceder. En caso de robo o pérdida mitigamos en parte el riesgo de acceso a la información.
Desconectar el bluetooth	Desconectar el bluetooth cuando no se esté utilizando y activarlo sólo cuando sea necesario para mitigar el riesgo de acceso al dispositivo móvil.
Desconectar el GPS	Desconectar el GPS cuando no se esté utilizando y activarlo sólo cuando sea necesario para no facilitar nuestro geoposicionamiento.
Realizar copias de seguridad	Con esto conseguiremos recuperar nuestros datos en caso de pérdida o fallo del dispositivo.
Instalar aplicaciones de markets de confianza oficiales	Descargar aplicaciones siempre del market oficial y revisar comentarios.
Vigilar privilegios y permisos que algunas aplicaciones solicitan	Un exceso de permisos para las aplicaciones instaladas puede suponer una pérdida de privacidad haciendo al

para ser instaladas	dispositivo más vulnerable frente al acceso de información de la empresa.
Uso del cifrado	Cifrar la información importante corporativa para prevenir ante un acceso, robo o pérdida por parte de un atacante.
Uso de versiones actualizadas	Mantener el software y el sistema operativo actualizado evitando posibles vulnerabilidades que permitan acceder al dispositivo y la información almacenada en el mismo.
Instalar antivirus	Instalar un antivirus para mitigar el riesgo de infección por parte del malware.
Evitar jailbreak o rooteado del dispositivo	Llevando a cabo estas acciones la seguridad del dispositivo disminuirá y los riesgos serán mayores.
Instalar alguna aplicación de localización del dispositivo	Estas aplicaciones permiten el acceso remoto al terminal en caso de robo o pérdida para tal de encontrar su ubicación, borrar los datos…
Encriptación de llamadas y mensajes	Para aquellos casos más extremos de intercambio de información muy confidencial, es posible encriptar las llamadas y los mensajes con aplicaciones haciendo que solo los interlocutores puedan escuchar la llamada o leer el intercambio de mensajes.
Evitar el uso de wifis públicas o hacerlo con algún método cifrado	Evitará que terceras personas no autorizadas puedan acceder a nuestra información. En caso de que no sea posible utilizar métodos a través de VPN-SSL que permitan un intercambio de información segura.
No abrir correos con origen desconocido ni hipervínculos sospechosos	Este tipo de correos o hipervínculos pueden ser ataques de ingeniería social o contener malware.
Usar contraseñas robustas	Siempre debemos elegir una contraseña robusta: longitud mínima de ocho caracteres, que combine mayúsculas, minúsculas, números y símbolo. No comparta las contraseñas, no use la misma contraseña para diferentes servicios y es recomendables cambiarla cada cierto tiempo.

Ser cuidadoso con el dispositivo para evitar su pérdida o robo	

4.1 Medidas legales

Hay otro aspecto de gran importancia que debemos de considerar y que es igual de importante que las medidas técnicas y organizativas que se implantan en un entorno BYOD. Para llevar a cabo una correcta estrategia BYOD trabajador y empresa deberán firmar un acuerdo de consentimiento del trabajador que regule el uso de dispositivos privados en la empresa.

Este acuerdo debe contemplar la aceptación de las medidas de seguridad y los controles que establezca la empresa para la protección de la información corporativa y de los datos personales que lleguen a tratarse o que estén almacenados en el dispositivo móvil.

El acuerdo o acuerdos deberán regular:

- Confidencialidad y secreto.
- Regulación del uso de BYOD: condiciones de uso, establecimiento de posibles responsabilidades del uso de la información corporativa, medidas a adoptar por parte del trabajador, definición de los datos que pueden, que sucede al finalizar la relación laboral …

La capacidad de control por parte de la empresa debería limitarse a las áreas, aplicaciones y contenedores de información corporativa, sin perjudicar un posible análisis forense de todo el contenido del terminal móvil.

5 Aplicaciones útiles

En este apartado se muestran una serie de aplicaciones de seguridad para dispositivos móviles. Estas aplicaciones solo son una muestra de las diferentes aplicaciones de seguridad que podemos encontrar en los markets oficiales de las diferentes plataformas (Android, IOS, Windows…).

Antes de instalar cualquier aplicación deberemos:

- Consultar con nuestra empresa si dispone de aplicaciones similares o si por administración y uso de la red empresarial nos recomienda uno u otro programa.
- Buscar entre las diferentes opciones disponibles de los markets la opción más interesante para el uso que queramos. Es interesante mirar si el sistema operativo instalado ya dispone de alguna aplicación para realizar la función deseada.
- Evaluar la fiabilidad de la aplicación a través de la nota y los comentarios que otros usuarios hayan podido darle.

Para cada dispositivo se han diferenciado las aplicaciones según el ámbito de actuación. Los diferentes ámbitos permiten luchar contra los diferentes tipos de ataque considerados anteriormente. Se han divido las aplicaciones en 7 ámbitos:

- **Protección y bloqueo de aplicaciones, fotos, contactos, llamadas…:** Aplicaciones útiles para bloquear y encriptar datos, documentos y otros del dispositivo móvil con el fin de hacer más difícil el acceso a esos datos protegidos. Suelen usarse de forma que protegen un grupo de aplicaciones, ficheros… a través de un PIN o contraseña de acceso.
- **Comprobación de estado de seguridad:** Aplicaciones que ayudan al usuario a detectar debilidades en la seguridad de su dispositivo móvil ofreciendo, además, posibles soluciones a esas debilidades. Por ejemplo, puede avisar de que el usuario tiene permanentemente activo el bluetooth recomendándole activarlo solo en caso de necesidad, o bien avisarle de que no tiene instalado ningún antimalware.
- **Protección de identidades:** Aseguran el almacenado de contraseñas, datos bancarios, tarjetas de crédito… de forma que sea más difícil el acceso por parte de un atacante. Normalmente realizan esto a través del cifrado de datos y el uso de PIN.
- **Antimalware:** Aplicaciones destinadas a la protección contra todo tipo de malware incluyendo protección contra amenazas procedentes de Internet (navegación web, correo electrónico, mensajería instantánea, descargas de

ficheros, banca online) y del uso de dispositivos externos (USB, discos duros externos…).

- **Comunicaciones seguras:** Aplicaciones que permiten encriptar los datos que se envían para comunicarnos con otros usuarios haciendo que pese a ser interceptados no puedan ser leídos.
- **Robo y pérdida:** Aplicaciones que en caso de pérdida o robo del móvil pueden ayudar al usuario a encontrarlo, a saber quién lo tiene o en caso necesario de llevar a cabo un borrado total del dispositivo para evitar el acceso a los datos que contiene.
- **Copias de seguridad:** Estas aplicaciones ayudan al usuario a recuperar datos, ficheros, imágenes… que haya podido perder por cualquier tipo de ataque recibido o extravío del dispositivo móvil almacenando una copia de estos datos fuera de su ubicación habitual.

Así pues, los ataques y ámbitos en los que actúan son los siguientes, valorados del 0 al 5, siendo 5 un ámbito de actuación alto para ese tipo de ataque (una aplicación con 5 en un ataque es una aplicación de seguridad muy útil para ese tipo de ataque y con un 0 será una aplicación con nula capacidad de lucha contra ese ataque):

Ámbito de actuación	**Ataques contra los que protegen**				
	Malware y Privilegios y permisos de las aplicaciones	**Ataques a redes wifi, 2G, 3G, 4G y NFC**	**Ingeniería social**	**Ataque bluetooth**	**Robo y pérdida**
Protección y bloqueo de aplicaciones, fotos, contactos, llamadas…	3	3	2	3	5
Comprobación de estado de seguridad	No ofrece una seguridad directa pero si muestra errores de configuración que perjudican a la seguridad. Podemos decir que actúa contra todos los ataques ayudando y dando opciones para mejorar la seguridad del dispositivo.				
Protección de	5	5	5	5	5

identidades					
Antimalware	5	3	3	3	0
Comunicaciones seguras	0	5	1	5	0
Robos y pérdidas	0	0	0	0	5
Copias de seguridad	No ofrece seguridad frente al robo de datos ni credenciales pero ofrece la opción de recuperar datos perdidos en caso de robo, virus, borrado de ficheros…				

A continuación, una muestra de aplicaciones que pueden actuar en cada sistema operativo para aumentar la seguridad en cada ámbito:

Android	
Protección y bloqueo de aplicaciones, fotos, contactos…	
AppLock	Permite bloquear mensajes, SMS, contactos, Facebook, galería, llamadas y cualquier aplicación con abundantes opciones protegiendo la privacidad. Con esta aplicación se puede crear una lista de aplicaciones protegidas, que al ser lanzadas, AppLock solicita una contraseña para continuar con la ejecución. Permite almacenar fotos y vídeos en una galería protegida por una contraseña. Tiene más opciones como por ejemplo: - Bloqueo automático en cierta posición. - Teclado aleatorio. - Bloqueo de llamadas entrantes o salientes. - Bloqueo de la configuración del sistema. - Evitar la desinstalación de aplicaciones.
EDS	Aplicación similar a la anterior pero que en lugar de actuar fichero a fichero lo hace por contenedores (agrupación de ficheros, aplicaciones…). Los ficheros que se quieren proteger se almacenan en un contenedor accesible solo desde la aplicación mediante una contraseña. Así se evita tener que poner la contraseña cada vez

	para cada fichero.
Folder Lock	Mantiene los datos personales y ficheros bajo una contraseña. Permite: - Proteger fotos privadas, ocultar fotos y vídeos, proteger mediante contraseña un audio, bloqueo de documentos, escritura de notas seguras… - Guardar de forma protegida tarjetas de crédito, cuentas bancarias, licencias, ID de la seguridad social, pasaporte,… - Uso sin trazas y con privacidad del navegador de ficheros. - Prevención de ataques de fuerza bruta, copia de seguridad en caso de contraseñas olvidadas, medidas preventivas para múltiples intentos de inicio de sesión no válidos…
KeepSafe	Permite mantener la privacidad de fotos y vídeos bloqueándolas con un PIN y haciéndolas no visibles desde la galería de fotos públicas.
Safe Notes	Permite guardar notas de forma segura protegiéndolas con un PIN.
App Protector Pro	Protege la privacidad mediante el bloqueo de aplicaciones. Permite bloquear, por ejemplo, el acceso a los SMS a través de una contraseña.
BoxCryptor	Permite la encriptación de los ficheros.
Comprobación de estado de seguridad	
CONAN mobile	Comprueba el estado de seguridad y las aplicaciones instaladas en un dispositivo comprobando diferentes parámetros e indicando al usuario que puede hacer en cada caso. Como ejemplos de comprobaciones realiza: - Análisis de la configuración del dispositivo evaluando los parámetros de configuración del dispositivo, redes WI-FI y dispositivos bluetooth. - Análisis de aplicaciones instaladas clasificándolas en base a su estado o peligrosidad. - Clasificación de aplicaciones por permisos clasificadas por categoría de riesgos.

	- Servicio Proactivo realizando un seguimiento en tiempo real de eventos de seguridad y notificaciones en la barra de estado para determinados eventos: conexiones a redes WI-FI inseguras, detección de llamadas y SMS a números de tarificación especial…
Protección de identidades	
SplashID Password Manager	Almacena de forma segura toda la información personal como inicios de sesión de red, tarjetas de crédito, PINs, configuración de correo…
Password Box	Permite la gestión de contraseñas y códigos guardándolos y haciendo copias de seguridad de forma cifrada para que nadie pueda acceder excepto el propietario.
1Password	Asegura el almacenado de las contraseñas, datos bancarios, tarjetas de crédito… de forma segura. Permite la sincronización de la información contenida con un PC.
Antimalware	
Kaspersky Internet Security	Protege el dispositivo de intrusos o vulnerabilidades de seguridad. Protege de amenazas de internet, sitios de phishing, spyware y spam. Además, también permite encontrar un dispositivo perdido emitiendo una señal acústica, bloquear el terminal, borrar los datos de forma remota, encontrar el teléfono vía GPS, sacar una foto… Proporciona una alta seguridad contra ataques malware.
Comunicaciones seguras	
Kryptos y RedPhone	Aplicación para cifrar comunicaciones de voz protegiendo las conversaciones que se realizan sobre 3G, 4G o wifi. Solo emisor y receptor pueden descifrar la comunicación.
Telegram	Con su opción de chats secretos permite establecer una comunicación instantánea de forma similar a WhatsApp con la ventaja de que los mensajes se envían de forma cifrada ofreciendo seguridad frente a ataques que intenten espiar la comunicación.

	Solo emisor y receptor pueden descifrar estos mensajes.
VPN One Click, Hotspot Shield y SpeedVPN.	Aplicaciones VPN[16] que permiten crear una conexión segura entre el dispositivo móvil y un servidor que nos dará el acceso a los servicios de internet. Esta conexión se realiza de forma segura, por lo que evita que cualquier ataque de intercepción de datos consiga descifrar los datos. Ideales para el uso de wifis no seguras.
Robos y pérdidas	
Prey	Agente que permanece activo de forma silenciosa en el dispositivo. A través de una señal remota enviada desde otro dispositivo permite saber donde se encuentra el dispositivo robado o perdido. Además de facilitar la ubicación permite: - Tomar fotos con la cámara - Bloquear el terminal - Activar una alarma sonora en el dispositivo - Mostrar un mensaje en pantalla Incluye un panel de control desde el que se pueden controlar hasta tres dispositivos.
Copias de seguridad	
MyBackup	Aplicación para copias de seguridad que se pueden almacenar en la tarjeta SD o en la nube de MyBackup. Trata de guardar todos los componentes del sistema: aplicaciones, música, contactos, registro de llamadas, SMS, calendario, alarmas…

iPhone	
Protección y bloqueo de aplicaciones, fotos, contactos …	
Lock My Folder Free	Mantiene los datos personales y ficheros bajo una contraseña. Permite:

[16] Tecnología de red que permite una extensión de una red local de forma segura. Permite que un dispositivo móvil alejado de una red privada pueda enviar y recibir datos de esa red privada como si estuviese conectado físicamente a ella. Con esto se obtiene completa funcionalidad y seguridad. Se realiza estableciendo una conexión virtual que aporta seguridad frente ataques.

	- Proteger fotos privadas, ocultar vídeos, proteger mediante contraseña un audio, bloqueo de documentos, escritura de notas seguras… - Guardar de forma protegida tarjetas de crédito, cuentas bancarias, licencias, ID de la seguridad social, pasaporte,… - Uso sin trazas y con privacidad del navegador de ficheros. - Prevención de ataques de fuerza bruta, copia de seguridad en caso de contraseñas olvidadas, medidas preventivas para múltiples intentos de inicio de sesión no válidos…
KeepSafe	Permite mantener la privacidad de fotos y vídeos bloqueándolas con un PIN y haciéndolas no visibles desde la galería de fotos públicas.
Wickr	Permite proteger los mensajes de texto cifrándolos, haciendo que se borren solos, haciéndolos anónimos o quitando la información de fecha, hora o lugar de envío. Si el receptor no tiene la aplicación instalada no podrá descifrar el mensaje.
Locktopus	Asignan una contraseña de acceso necesario para abrir las aplicaciones que bloqueemos.
iDiscrete	Aplicación útil para mantener lejos de los demás aquello que se quiera mantener oculto en el dispositivo. Permite guardar cualquier tipo de archivo en la aplicación, que al abrirla muestra una pantalla que necesita desbloqueo para acceder a los ficheros.
Secretum	Ofrece la posibilidad a través de una contraseña de acceder a un perfil diferente en el que sólo se muestre la información que hayamos seleccionado previamente.
iCaughtU	Permite controlar quién intenta acceder a nuestro teléfono sin permiso. También permite localizar el dispositivo en caso de robo o pérdida. Entre sus opciones podemos determinar un número máximo de intentos de acceso antes de que la aplicación haga una foto de la persona que está intentando acceder, enviándola posteriormente al email indicado con la localización y la hora.
Keepsafe	Permite guardar de forma cifrada (solo permite el acceso previa petición de PIN) una carpeta de imágenes.

Protección de identidades	
SplashID Password Manager	Almacena de forma segura toda la información personal como inicios de sesión de red, tarjetas de crédito, PINs, configuración de correo…
1Password	Asegura el almacenado de las contraseñas, datos bancarios, tarjetas de crédito… de forma segura. Permite la sincronización de la información contenida con un PC.
Antimalware	
Anti-Virus Detective	Ofrece protección contra los malwares. Explora las aplicaciones de malwares y otras vulnerabilidades.
Kaspersky Safe Browser	Protege los dispositivos de las amenazas móviles. Permite filtrar contenido. Especialmente diseñado para la navegación web, bloqueando las páginas web maliciosas e inapropiadas.
Comunicaciones seguras	
Kryptos	Aplicación para encriptar comunicaciones de voz protegiendo las conversaciones que se realizan sobre 3G, 4G o wifi.
Silent Phone	Permite el envío de vídeos y mensajes de audio cifrados de forma que solo emisor y receptor puedan ver su contenido.
TunnelBear VPN, Hot Spot Shiel VPN, VPN Express	Aplicaciones VPN que permiten crear una conexión segura entre el dispositivo móvil y un servidor que nos dará el acceso a los servicios de internet. Esta conexión se realiza de forma segura, por lo que evita que cualquier ataque de intercepción de datos consiga descifrar los datos. Ideal para el uso de wifis no seguras.
Robos y pérdidas	
Lookot Mobile Security	Permite la localización del dispositivo en caso de robo o pérdida mediante sincronización con el servicio GPS.
Prey	Agente que permanece activo de forma silenciosa en el dispositivo. A través de una señal remota enviada desde otro dispositivo

	permite saber donde se encuentra el dispositivo robado o perdido. Además de facilitar la ubicación permite: - Tomar fotos con la cámara - Bloquear el terminal - Activar una alarma sonora en el dispositivo - Mostrar un mensaje en pantalla Incluye un panel de control desde el que se pueden controlar hasta tres dispositivos.
Find My IPhone, Gadget Track	Aplicaciones que permiten conocer la ubicación del dispositivo móvil, enviar un mensaje, hacer que suene un pitido o borrar de forma remota toda la información que contenga. Estas aplicaciones son interesantes en caso de robo o pérdida del dispositivo.

Windows Phone	
Protección y bloqueo de aplicaciones, fotos, contactos …	
4UrEyezOnly	Permite a un usuario la posibilidad de proteger los archivos multimedia, mensajes… a través de cifrado de datos.
Lock & Hide	Pone todas las fotos bajo la protección de una clave.
File Locker	Protege los datos y permite cifrar la información a través de un PIN.
Protección de identidades	
1Password	Asegura el almacenado de las contraseñas, datos bancarios, tarjetas de crédito… de forma segura. Permite la sincronización de la información contenida con un PC.
Keeper	Gestor de contraseñas para cada una de tus cuentas online. Ayuda a iniciar sesión en varias cuentas de forma automática, sincroniza dispositivos Windows, ofrece copias de seguridad en la nube y cifra la información sensible.
Password Padlock	Permite la gestión de contraseñas de forma segura. A través de una contraseña maestra se cifrarán todas las contraseñas que tengamos. Puede realizarse una copia de seguridad desde SkyDrive.

Antimalware	
Kaspersky Safe Browser	Protege los dispositivos de las amenazas móviles. Permite filtrar contenido. Especialmente diseñado para la navegación web, bloqueando las páginas web maliciosas e inapropiadas.
Comunicaciones seguras	
SplashID	Permite proteger la información personal que circula por internet cuando navegamos por internet. Provoca que los datos, como los bancarios, no puedan ser vistos por usuarios malignos.
VyprVPN, Hot Spot Shiel VPN, HideMyAss, ExpressVPN	Aplicaciones VPN que permiten crear una conexión segura entre el dispositivo móvil y un servidor que nos dará el acceso a los servicios de internet. Esta conexión se realiza de forma segura, por lo que evita que cualquier ataque de intercepción de datos consiga descifrar los datos. Ideal para el uso de wifis no seguras.
Robos y pérdidas	
Prey	Agente que permanece activo de forma silenciosa en el dispositivo. A través de una señal remota enviada desde otro dispositivo permite saber donde se encuentra el dispositivo robado o perdido. Además de facilitar la ubicación permite: - Tomar fotos con la càmera - Bloquear el terminal - Activar una alarma sonora en el dispositivo - Mostrar un mensaje en pantalla Incluye un panel de control desde el que se pueden controlar hasta tres dispositivos.
Best Phone Security	Activa una alarma y guarda el sitio y hora cuando se produjeron intentos de acceso al dispositivo móvil.
My WP	Ayuda a encontrar un dispositivo perdido o robado mediante localización. Permite llamar, bloquear o eliminar información del terminal.