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

Guía de empresa

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 abre un nuevo campo en cuanto a la capacidad del trabajador.

Conforme aumentan las capacidades tecnológicas de los dispositivos móviles también se incrementa su uso en el puesto de trabajo. Las estadísticas son claras en este sentido. Según datos de un estudio[1] de inicios de 2013 realizado por Gartner, Ovum, IBM, Vertic, Flurry, Magic Software, Motorola y Harris Pol:

- Existían un billón de *smartphones* en el mundo.
- El 81% de americanos usaba su dispositivo móvil para el trabajo.
- El aumento del número de usuarios de *smartphones* anual a nivel mundial es del 42%.
- En 2012 se vendieron 821 millones de *smartphones* y tabletas en todo el mundo.
- El incremento de la productividad laboral por el uso de las aplicaciones en móviles es del 45%.

Completando los datos anteriores, otro estudio[2] anterior publicado por Forbes indicaba que un 74% de las empresas a inicios de 2012 permitía algún tipo de uso de BYOD.

Por lo tanto el, BYOD está en aumento. Este método de trabajo lleva implícitas una serie de ventajas e inconvenientes:

Ventajas del uso de BYOD
Incremento de la productividad de los empleados debido a que los trabajadores se encuentran más cómodos trabajando con sus aplicaciones y dispositivos.
Incremento en la satisfacción del trabajador ya que le permite trabajar con más flexibilidad.
Mejora en la atención al cliente al poder responder ante cualquier petición

[1] http://www.ribbit.net/frogtalk/id/143/byod-stats-what-business-leaders-need-to-know-right-now

[2] http://www.forbes.com/sites/markfidelman/2012/05/02/the-latest-infographics-mobile-business-statistics-for-2012/

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.

En lo que a ciberseguridad se refiere, el primer estudio señala diferentes situaciones de riesgo en los dispositivos móviles personales que se utilizaban en entornos empresariales:

- El 46% de usuarios prestan sus dispositivos a otras personas.
- El 35% guardan su password del correo del trabajo en el móvil.
- El 37% no tienen activas las opciones de bloqueo.
- El 66% de trabajadores dice que su empresa no tiene implementadas políticas de BYOD.
- El 80% de la actividad a través del BYOD no está siendo administrada.
- El incremento de malware detectado en el año 2012 fue del 155%.

Completando los datos anteriores, según el estudio de Forbes, los datos perfilaban un gran desconocimiento en cuanto a movilidad y seguridad de las empresas:

- En 2012 menos del 10% de las empresas eran plenamente conscientes de los dispositivos que accedían a su red.
- El 55% de los trabajadores revelaron haber enviado correos o ficheros de empresa a sus cuentas personales usadas en el móvil.
- El 48% dicen conectarse a redes wi-fi inseguras.

Por tanto, podemos remarcar los siguientes inconvenientes en el uso del BYOD:

Desventajas del uso de BYOD
Riesgo para la seguridad de la red corporativa así como de la información de la empresa. Esto es muy crítico, ya que una fuga de datos podría incluso llevar al cierre a la empresa.
Posibilidad de infección de la red si un usuario se conecta infectado con malware[3].
Mayor consumo de los recursos de la red.
Necesidad de reforzar los departamentos de soporte y de tecnologías de la información para dar respuesta a las problemáticas generadas por la multitud de dispositivos y programas.

[3] 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, fines económicos…

Dentro de los riesgos señalados, el estudio realizado por Alcatel-Lucent muestra diferentes cifras que señalan un incremento en el número de dispositivos infectados por malware:

- El incremento durante el primer semestre de 2014 de dispositivos infectados por malware fue del 17%.
- Un 0,65% de equipos sufrió infección malware. Pese a representar un porcentaje pequeño, implica que 15 millones de dispositivos están infectados por malware en algún momento.
- Las infecciones por malware se han doblado con respecto a los datos de 2013.
- El estudio de Opswat advierte que casi un tercio de las aplicaciones de las tiendas ajenas a Google Play están infectadas.

Podemos afirmar que esta nueva forma de relación trabajador-empresa implica riesgos para la información de la empresa así como para los datos personales del trabajador si no se realizan las acciones adecuadas en cuanto a la protección de los mismos. Se debe centrar la atención en cualquier vulnerabilidad de los dispositivos móviles y los datos a los que acceden prestando atención a:

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.[4]
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	Puntos de acceso gratuitos, pero sin medidas de seguridad adecuadas que pueden permitir a terceras personas analizar nuestro tráfico de red y

[4] 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.

inseguras (WIFI de un bar, bluetooth mal configurado...).	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 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 del BYOD

Todos los riesgos del BYOD provienen principalmente del hecho de que es el propio usuario quién gestiona sus propios dispositivos personales. Esto implica que la empresa, propietaria de los datos, tiene menos control sobre el dispositivo que accede a estos datos que si éste fuera de la empresa.

Además, con el BYOD se amplía el espectro de dispositivos que pueden acceder a los datos, dificultando el control y administración de este tipo de tecnología. Por otro lado, ante la variedad de dispositivos que existen, hay que valorar el uso que se les da, sus características de seguridad implícitas y a qué datos pueden tener acceso. Así pues, a través de diferentes tipos de ataque a los dispositivos móviles personales un ciberdelincuente podría obtener usuarios y passwords de acceso a servidores, cuentas de correo, servicios ftp… o directamente obtener ficheros almacenados en el propio equipo o a algún otro dispositivo/recurso de red al que se tenga acceso. Estos ataques pueden producir:

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

Ahora se debe gestionar hasta dónde se permite al usuario acceder a los datos desde dispositivos más variados con tecnologías que no siempre estarán actualizadas y sin garantías de estar securizadas.

Las amenazas a dispositivos móviles y que pueden comprometer los activos de información de la empresa son las siguientes:

- **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 de estos ataques pueden ser múltiples: uso del sistema para realizar actos delictivos, obtención de datos… pero lo que en el trasfondo siempre estará presente en la mayoría de ataques es un fin económico. Por lo tanto, tratan de ser lo más silencioso para poder actuar el máximo tiempo posible. A través de un ataque malware al dispositivo móvil un atacante podría:
    - Acceder a información sensible (datos o credenciales).
    - Usar el móvil dentro de una red zombie[5].
    - Cifrar, borrar o modificar ficheros.
    - Infectar la red corporativa.

El malware puede infectar un dispositivo móvil de diversas formas:

- Explotando una vulnerabilidad de cualquier programa instalado en el sistema.
- Ingeniería social: Incitando al usuario a que realice algún tipo de acción. Se utiliza sobretodo en correos de phishing[6], aunque puede encontrarse en otro tipo de ataques de ingeniería social.
- A través de un archivo malicioso que puede llegar adjunto en un mensaje, fichero en una web, carpetas compartidas…
- Dispositivos extraíbles que contienen copias del malware que se ejecuta automáticamente una vez se conecta el dispositivo extraíble.

- **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.

[5] 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.

[6] Phishing o suplantación de identidad que se comete mediante el uso de ingeniería social para intentar adquirir información confidencial de forma fraudulenta.

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 se use el sistema wifi como 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 dispositivos que sostienen esta red y las señales de comunicaciones que se transfieren están expuestos a diversos ataques:
    - Sniffing: 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.
    - Análisis de tráfico: El atacante obtiene información con solo examinar el tráfico y sus patrones.
    - Spoofing: El atacante se hace pasar por un punto de acceso y el cliente piensa estar conectándose a una red WLAN verdadera.
    - Modificación: El atacante borra, manipula, añade o reordena los mensajes transmitidos.
    - Reactuación: El atacante inyecta en la red paquetes interceptados utilizando un sniffer[7] para repetir operaciones que ya habían sido realizadas.
    - Denegación de servicio: El atacante puede inutilizar el servicio wifi generando interferencias que produzcan errores en la transmisión hasta que la velocidad caiga hasta hacerla casi inutilizable.

A partir de estos ataques se podría leer, insertar y modificar mensajes entre dos usuarios o sistemas. Para el caso que nos ocupa este ataque podría realizarse cuando

[7] Programa informático que registra la información enviada por los periféricos.

el trabajador 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 se podría:

- Robar información sensible (datos o credenciales).
- Desviar 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, 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 alcance. Un atacante puede aprovechar el uso del bluethooh para realizar diversos ataques a los dispositivos que lo tengan activo. Con la redefinición del estándar de emparejamiento entre dispositivos bluethooh se ha conseguido rebajar en gran porcentaje el número de ataques a esta tecnología. Pese a ello aún es posible realizar ciertos ataques. Como ejemplo, algunos de ellos:

  - Bluebug: Ataque que permite ejecutar comandos AT (instrucciones codificadas que conforman un lenguaje de comunicación entre el hombre y un terminal móvil o modem) 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…
  - BlueSnarf: 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.

Como en los casos anteriores nos encontramos con un tipo de ataque que puede acarrear problemas serios para la empresa y sus datos, 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 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”. A través de los dispositivos móviles se pueden realizar diferentes tipos de ataque de ingeniería social, por ejemplo:

- Llamada suplantando identidad: Recibir una llamada de nuestro supuesto departamento IT que después de una serie de preguntas y de ganarnos nuestra confianza nos pregunte por nuestro password del correo.
- Phishing attacks: Uno de los métodos más usados. Fraude informático que utiliza el email, SMS, web… para convencer a la víctima de que revele cierta información (datos de la empresa, passwords…) o realice cierta actividad (entrar en una web falsa…).

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.

- **Ataques a 2G/3G/4G:** A través de estos estándares de comunicación de telefonía "tradicional" también pueden llevarse a cabo ciertos ataques para perjudicar al propietario del dispositivo móvil o bien a la empresa donde trabaja.

En 2G la seguridad es prácticamente nula y sus protocolos y algoritmos de cifrado presentan multitud de vulnerabilidades permitiendo a un atacante:

- Ataques de escucha pasiva que permiten la intercepción, escucha de llamadas, suplantación de identidad y obtención de SMS.
- Ataques de escucha activa donde el atacante actúa como una estación base falsa que actúa sustituyendo a la del operador sin que la víctima detecte anomalía.
- Ataques de denegación de servicio a ciertos usuarios y semipermanentes.

En 3G la seguridad es más elevada, pese a ello se puede llevar un ataque de denegación de servicio que obligue al dispositivo móvil a cambiarse a 2G y una vez conectado a 2G se podría llevar a cabo alguno de los ataques descritos anteriormente. También es vulnerable a ataques man-in-the-middle[8] y se ha demostrado que se puede acceder a datos e identidades a través del Eavesdropping, 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.

Para 4G, basada en tecnología IP, existen también una serie de ataques que no hacen de esta tecnología una tecnología libre de vulnerabilidades. Estos ataques son:

- Ataques a los recursos de radio, pudiendo provocar una denegación de servicio.

[8] Ataque en el que el atacante adquiere la capacidad para leer, insertar y modificar los mensajes entre dos partes sin que conozcan que el enlace entre ellas ha sido violado.

- Ataques man-in-the-middle.
- Ataques eavesdropping.

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:** 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 y la red corporativa.
  - 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 todos los tipos de tecnologías inalámbricas que podemos encontrar en un dispositivo móvil son vulnerables y que en mayor o menor medida permiten 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). Esto hace que se haga indispensable un correcto uso del dispositivo por parte de los usuarios (que pueden ser víctimas directas o puentes para otros ataques) y a que la empresa aporte el máximo de recursos posible a la protección de sus datos, a la concienciación de sus trabajadores y a la ayuda en la correcta administración y uso de los dispositivos móviles. Una correcta política en los aspectos anteriores permitirá a la empresa y a los trabajadores tener un nivel elevado de seguridad.

2.1 Impacto y posibilidades de éxito

A partir de las diferentes tecnologías que pueden recibir ataques se muestran las posibles consecuencias de un ataque, el impacto que puede implicar el éxito de un ataque y las posibilidades/facilidades de que un ataque tenga éxito si no se toman las medidas oportunas. El valor de impacto y las posibilidades de éxito están marcados con valores del 1 al 5, siendo 5 el mayor impacto o la posibilidad de éxito más elevada.

Ataque/Problema	Consecuencias	Impacto[9]	Posibilidades de éxito[10]
Malware	- Robo de información sensible (datos o credenciales). - Uso del móvil dentro de una red zombie. - Cifrado, borrado o modificación de ficheros. - Infección de la red corporativa.	5	4
Privilegios y permisos de las aplicaciones	- Robo de información sensible (datos o credenciales). - Cifrado, borrado o modificación de ficheros.	5	4
Ataque a 2G	- Robo, modificación, cifrado o borrado de información sensible (datos o credenciales). - Modificación, cancelación o realización de envíos de correos, SMS o llamadas indeseadas. - Denegación de servicio.	5	4
Ataque a 3G	- Robo, modificación, cifrado o borrado de información sensible (datos o credenciales). - Modificación, cancelación o realización de envíos de	5	3

[9] Criticidad del ataque en caso de llevarse a cabo de forma satisfactoria. A más datos/funciones accesibles una vez realizado el ataque más nivel de criticidad.

[10] Facilidad para llevar a cabo el ataque.

	correos, SMS o llamadas indeseadas. - Denegación de servicio.		
Ataque a 4G	- Robo, modificación, cifrado o borrado de información sensible (datos o credenciales). - Modificación, cancelación o realización de envíos de correos, SMS o llamadas indeseadas. - Denegación de servicio.	5	2
Ataque en wifis inseguras	- Robo, modificación, cifrado o borrado de información sensible (datos o credenciales). - Modificación, cancelación o realización de envíos de correos. - Denegación de servicio. - Descarga de malware al dispositivo y este a la red corporativa.	5	5
Ataque a NFS	- Robar información sensible (datos o credenciales). - Cifrado, borrado o modificación del contenido de los ficheros o los propios ficheros. - Descarga de malware e infección del equipo y la red corporativa. - Intercepción, lectura y modificación de los datos que se transmiten entre dispositivos mediante un ataque man-in-the-middle.	5	2
Ingeniería social	- Obtención de información sensible (datos o credenciales). - Infección con malware del dispositivo móvil y éste de la red corporativa.	5	4

	- Obtención de un pago de la empresa.		
Pérdida o robo del dispositivo móvil	- Peligro de ser usado por otras personas, pudiendo realizar cualquier tipo de acción (robo de datos, llamadas indeseadas, envío de datos, infección malware...)	5	4

3 Políticas de mitigación

Los dispositivos móviles pueden sufrir ataques que provoquen robo o pérdida de datos empresariales o personales, robo de identidades o denegaciones de servicio que impidan un uso normal del terminal. Además, si permitimos que cada usuario utilice su dispositivo, nos encontraremos con que la red corporativa ya no estará conformada por un conjunto de dispositivos uniformes (mismo hardware, mismo sistema operativo, mismo software…), sino que tendremos que gestionar dispositivos de diferentes marcas, con diferentes sistemas operativos, cada uno de ellos con diferentes aplicaciones desconocidas instaladas. Esto hace que la administración de la seguridad de cada dispositivo no se pueda hacer dispositivo a dispositivo y que se necesite centralizar este control de la seguridad.

Teniendo en cuenta las premisas anteriores la opción más interesante es la de controlar desde la red corporativa qué tipo de dispositivo está accediendo a la red, cómo lo está haciendo, qué aplicaciones tiene instaladas, qué sistemas de conexión tiene activados, si tiene activado el antivirus, si tiene alguna aplicación sospechosa, donde quiere acceder…

Con las necesidades que surgen hay unas líneas claras en las que la empresa debe trabajar para mantener una red de dispositivos móviles segura:

Políticas de mitigación
Definición de políticas de uso y gestión
Uso de aplicaciones Mobile Device Management
Concienciación del usuario

3.1 Definición de políticas de uso y gestión

A la hora de trabajar en conseguir que los accesos a la red corporativa desde dispositivos BYOD sean seguros y que los datos corporativos estén a salvo de ataques es necesario definir unas políticas que ayudarán a controlar los accesos a los datos y su uso. Estas políticas deberían ser claras y concisas, informando a aquellos que quieran hacer uso del BYOD de las condiciones de uso y haciéndoles firmar un documento claro y conciso con estas condiciones de uso.

Ejemplos de políticas de uso y seguridad
Definición de qué equipos y aplicaciones pueden acceder a la red corporativa.
Definición de qué funciones están permitidas con los datos. Por ejemplo, se puede prohibir que un fichero recibido por correo sea descargado al dispositivo móvil o renviado a una cuenta de correo no corporativa.
Prohibición de *jailbreak*[11] o *root*[12].
Habilitación del borrado remoto de los datos del dispositivo en caso de pérdida o robo.
Obligatoriedad de actualizar el sistema operativo y las aplicaciones a las nuevas versiones (en teoría, más seguras).

El incumplimiento por parte del trabajador de alguna de las políticas definidas puede acarrear problemas de seguridad a la empresa, por lo que dentro de las políticas de la empresa podría incluirse la posibilidad de revocar al trabajador el derecho de uso del BYOD.

La mayoría de las políticas definidas podrán ser controladas y realizadas desde una aplicación Mobile Device Management (MDM) que se verá en el siguiente apartado.

11 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.

12 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.

3.2 Mobile Device Management

Las herramientas *Mobile Device Management* (MDM), de uso indispensable para controlar las conexiones a la red corporativa por parte de los dispositivos móviles, ayudarán a las políticas de gestión y seguridad tradicionales (firewalls, antivirus, VPNs…) en su intento por lograr el máximo nivel de seguridad y gestión de los datos de la empresa desde dispositivos móviles. Se basan en el control de las aplicaciones y de sus funciones, en el control de los datos y en el comportamiento del usuario.

Estas herramientas permiten asegurar, monitorizar y administrar dispositivos móviles de forma que se garantice la seguridad de la información y de la red, ofreciendo, además, otras funciones interesantes para la empresa.

Aportan diferentes ventajas al entorno profesional dotando de una base sólida a la empresa para la administración de los dispositivos móviles no solo en cuestión de seguridad:

Ventajas del uso de MDM
Permiten realizar un seguimiento de los dispositivos móviles, líneas, usuarios y datos (por ejemplo manteniendo una lista de contactos actualizada de forma centralizada para todos los dispositivos).
Permiten elaborar informes (por ejemplo: informe de consumo de datos) que permitan tomar mejores decisiones para el futuro de la empresa.
Gestión de la información relacionada con el uso del dispositivo móvil.
Distribución y administración de aplicaciones corporativas, tanto empresariales como de IT (seguridad).
Control de las aplicaciones que pueden ser utilizadas evitando que los usuarios ejecuten aplicaciones que no son productivas para las empresas.
Facilitan la administración de los dispositivos.

A nivel de seguridad estos programas permiten asegurar, monitorizar y gestionar diversas funciones de forma remota desde un servidor centralizado en el que se definen las políticas o actuaciones a realizar (instalación software, cambios de passwords…) sobre un dispositivo concreto. Como ejemplo, con un sistema MDM, la empresa podría establecer la política de que un dispositivo con una aplicación concreta instalada no pueda acceder a la red.

En función de quién sea el propietario del dispositivo se podrán aplicar ciertas funcionalidades o no. Por ejemplo, en caso de que el propietario del dispositivo sea el propio usuario (como es el caso del BYOD), no se podrá negar al usuario la instalación de aplicaciones no productivas para la empresa. En cambio, el

departamento IT si podría controlar que aplicación del dispositivo particular puede acceder a datos corporativos y cual no.

Una empresa debería usar esta tecnología para controlar el uso de los dispositivos en cuanto al acceso que se realiza desde ellos a los datos corporativos, por ejemplo, creando políticas como las del apartado anterior. Esta tecnología le permitiría recuperar un dispositivo perdido o borrar todos los datos que tenga almacenado en caso de que el dispositivo sea robado evitando, así, la extracción de datos del dispositivo.

Políticas como las definidas en el apartado anterior aplicables desde los programas MDM hacen más seguros los accesos a los datos corporativos dificultando ataques que permitan su obtención además de permitir el borrado completo de un dispositivo en caso de pérdida (evitando robo de datos o de identidades).

A partir de una aplicación MDM la empresa puede controlar diferentes opciones específicas para mitigar los problemas reflejados a lo largo del documento.

Estas herramientas disponen de multitud de opciones que ayudarán a la empresa a controlar los riesgos de seguridad existentes con el BYOD.

La documentación de la solución MDM de Kaspersky [13]resume en 5 bloques la seguridad que se puede aplicar a cualquier entorno BYOD:

- Protección *antimalware*, *antiphishing* y *antispam*, usando antivirus u otras tecnologías.
- Controles de aplicaciones, de web y de dispositivos modificados, por ejemplo, a través del cumplimiento de políticas.
- Activación de cifrado para la protección de datos, como por ejemplo el uso de VPNs para el envío de datos o de contraseñas para la apertura de ficheros.
- Separación de datos corporativas y personales mediante contenedores (mantienen los datos de empresa separados de los personales, permitiendo, entre otras, un borrado selectivo) y restricción de acceso a datos.
- Seguridad en caso de pérdida o robo de dispositivos mediante el rastreo GPS o el bloqueo o borrado remoto.

Así pues, podemos diferenciar 5 grandes campos en los que se puede actuar desde una aplicación MDM en cuanto a la seguridad se refiere:

[13] http://www.kaspersky.es/software-seguridad-empresas/mobile-device-management

http://media.kaspersky.com/sp/business-security/endpoint-overview.pdf

Campos gestionables desde un MDM	
Gestión de aplicaciones	Gestionando, implementando, instalando, bloqueando…. las aplicaciones móviles de los dispositivos.
Gestión de políticas	Controlando identidades, sincronizaciones, integración de cuentas…
Gestión de seguridad	Aplicando las políticas de seguridad, de autenticación y encriptación definidas, del bloqueo o borrado del dispositivo, de la detección de *jailbreak*…
Gestión de inventario	Controlando el estado de los dispositivos y su ubicación.
Gestión de servicios de telecomunicaciones	Controlando consumos y usos de los servicios de telecomunicaciones.

Estas son algunas opciones/políticas de seguridad de ejemplo aplicables desde un *Mobile Device Management* a los dispositivos móviles para hacer segura su interacción con la red corporativa:

- Activar cifrado: Mediante esta opción se puede hacer que para acceder a un fichero (ubicado en el dispositivo móvil, enviado por correo…) se necesite introducir una clave. Con ello, dificultamos el acceso al fichero por parte de personas ajenas a la empresa.
- Borrado de los datos de un terminal: Permite borrar los datos de un terminal haciéndolos inaccesibles. Esta opción puede usarse en caso de robo o cese de la relación laboral con el trabajador para evitar una fuga o robo de datos.
- Bloqueo del terminal: Creando y distribuyendo a los dispositivos móviles reglas de bloqueo del terminal, como por ejemplo el tiempo máximo de inactividad antes de que el terminal se bloquee.
- Requerimiento de PIN: Obligando al usuario del terminal a marcar el número PIN para desbloquear el terminal.
- Establecimiento de una contraseña de bloqueo desde el servidor fijando la contraseña a usar.
- Localización y seguimiento de los dispositivos gracias al uso del GPS: permite localizar un terminal perdido o robado.
- Control de las aplicaciones que pueden acceder a los datos corporativos y cuales no. Controlando de esta forma qué aplicaciones pueden ser usadas de forma corporativa y descartando aquellas de dudosa fiabilidad (posible malware) o no corporativas.

- Detectar y restringir los dispositivos con jailbreak o pirateados, pudiendo denegarles el uso corporativo a sus propietarios o limitándoles ciertas acciones.
- Control de acciones sobre ficheros o correos: Permitiendo, por ejemplo, la visualización de un adjunto a un correo con un programa determinado pero denegar su descarga al terminal móvil o su renvío.
- Instalación, configuración y actualización de un antivirus o firewall a todos los equipos desde el MDM.
- Uso de VPNs en la conexión red empresa-dispositivo móvil, creando una conexión segura donde se evite que los datos enviados puedan ser interceptados.
- Establecimiento de políticas para establecer una contraseña.
- Configurar los dispositivos para que conecten a través de VPN en cualquier conexión que realicen con la red corporativa.

3.3 Concienciación del usuario

Para evitar ataques dirigidos al usuario del dispositivo móvil, sobretodo ataques de ingeniería social, hay que aplicar políticas de seguridad en la empresa destinadas a concienciar y educar a los trabajadores para evitar comportamientos que podrían introducir malware o exponer los datos empresariales a un riesgo no deseado.

A través de un conjunto de materiales y acciones formativas la empresa deberá de implementar un Plan de Concienciación con el objetivo de concienciar y fomentar hábitos cotidianos de seguridad en sus empleados.

Existen diferentes iniciativas que permiten poder implantar acciones de concienciación y formación en ciberseguridad para empleados. Entre aquellos que se encuentran disponibles de forma gratuita se encuentra el publicado por INCIBE.

3.4 Ejemplo de aplicación

Con el uso de las diferentes opciones de seguridad de las aplicaciones MDM y de la concienciación de los usuarios la empresa estará en condiciones de reducir el riesgo de que gran parte de las amenazas expuestas exploten las vulnerabilidades sobre los dispositivos móviles, sus datos y sus conexiones.

Para mantener la seguridad frente a las amenazas y vulnerabilidades vistas en el apartado anterior podemos realizar diferentes acciones de mitigación para cada tipo de ataque, siendo esta tabla representativa de algunas de las acciones que permiten las aplicaciones MDM a modo de ejemplo. Será necesario analizar las diferentes opciones de la aplicación MDM adoptada por la empresa para aplicar las más adecuadas y proporcionales:

Tipo de amenaza	Qué puede provocar	Medidas de mitigación
Malware	- Robar información sensible (datos o credenciales). - Usar el móvil dentro de una red zombie. - Cifrar, borrar o modificar ficheros. - Infectar la red corporativa.	- Concienciación del usuario. - Instalación de antimalware, antiphishing, y antispam, usando antivirus, firewall u otras tecnologías similares. - Uso del cifrado de datos, ficheros… - Uso de VPNs para las conexiones desde el terminal a un punto remoto. - Políticas de seguridad que eviten el trasvase de datos entre aplicaciones. Por ejemplo, haciendo que un tipo de fichero solo pueda ser abierto por determinada aplicación corporativa. - Detectar y restringir los dispositivos con jailbreak o pirateados.
Privilegios y permisos de las aplicaciones	- Robar información sensible (datos o credenciales). - Cifrar, borrar o modificar ficheros.	- Concienciación del usuario. - Uso del cifrado de datos, ficheros… - Políticas de seguridad que eviten el trasvase de datos entre aplicaciones. Por ejemplo, haciendo que un tipo de fichero solo pueda ser abierto por determinada aplicación

		corporativa.
Ataques a través de redes de datos (wifi, 2G, 3G, 4G, NFS, bluetoth...)	- Robo, modificación, cifrado o borrado de información sensible (datos o credenciales). - Modificación, cancelación o realización de envíos de correos, SMS o llamadas indeseadas. - Denegación de servicio. - Descarga de malware al dispositivo y éste a la red corporativa.	- Concienciación del usuario. - Activación de cifrado para la protección de datos, como por ejemplo el uso de VPNs para el envío de datos o de contraseñas para la apertura de ficheros. - Separación de datos corporativos y personales mediante contenedores (mantienen los datos de empresa separados de los personales, permitiendo, entre otras, un borrado selectivo) y restricción de acceso a datos. - Activar cifrado: Mediante esta opción se puede hacer que para acceder a un fichero (ubicado en el dispositivo móvil, enviado por correo…) se necesite introducir una clave. Con ello, dificultamos el acceso al fichero por parte de personas ajenas a la empresa. - Control de las aplicaciones que pueden acceder a los datos corporativos y cuales no, controlando de esta forma qué aplicaciones pueden ser usadas de forma corporativa y descartando aquellas de dudosa fiabilidad (posible malware) o no corporativas. - Configurar los dispositivos para que conecten a través de VPN en cualquier conexión que realicen con la red corporativa.
Ingeniería social	- Obtener información sensible (datos o credenciales). - Infectar con malware el dispositivo móvil y éste a la red corporativa. - Obtener un pago de la	- Concienciación del usuario - Activar cifrado: Mediante esta opción se puede hacer que para acceder a un fichero (ubicado en el dispositivo móvil, enviado por correo…) se necesite introducir una clave. Con ello, dificultamos

	empresa.	el acceso al fichero por parte de personas ajenas a la empresa. - Borrado de los datos de un terminal: Permite borrar los datos de un terminal haciéndolos inaccesibles. Esta opción puede usarse en caso de robo o cese de la relación laboral con el trabajador para evitar una fuga o robo de datos. - Bloqueo del terminal: Creando y distribuyendo a los dispositivos móviles reglas de bloqueo del terminal, como por ejemplo el tiempo máximo de inactividad antes de que el terminal se bloquee. - Requerimiento de PIN: Obligando al usuario del terminal a marcar el número PIN para desbloquear el terminal.
Pérdida o robo del dispositivo móvil	- Peligro de ser usado por otras personas, pudiendo realizar cualquier tipo de acción (robo de datos, llamadas indeseadas, envío de datos, infección malware...)	- Concienciación del usuario. - Activar cifrado: Mediante esta opción se puede hacer que para acceder a un fichero (ubicado en el dispositivo móvil, enviado por correo…) se necesite introducir una clave. Con ello, dificultamos el acceso al fichero por parte de personas ajenas a la empresa. - Borrado de los datos de un terminal: Permite borrar los datos de un terminal haciéndolos inaccesibles. Esta opción puede usarse en caso de robo o cese de la relación laboral con el trabajador para evitar una fuga o robo de datos. - Bloqueo del terminal: Creando y distribuyendo a los dispositivos móviles reglas de bloqueo del terminal, como por ejemplo el

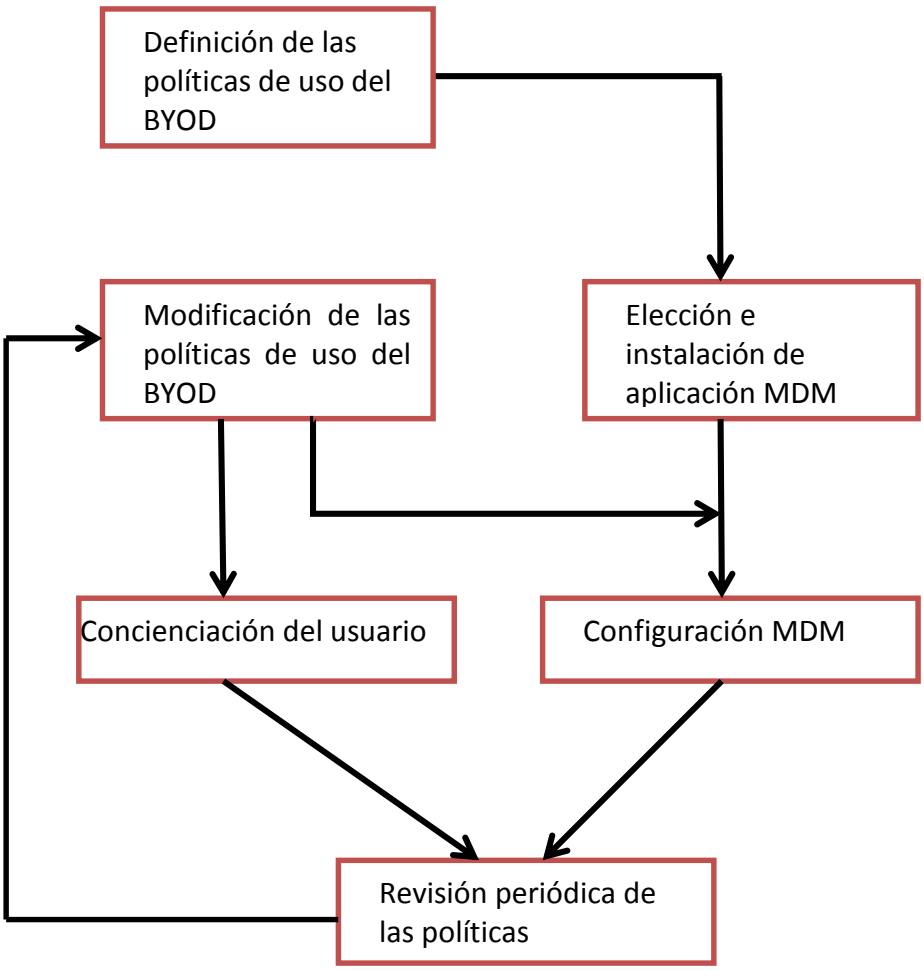
		tiempo máximo de inactividad antes de que el terminal se bloquee. - Requerimiento de PIN: Obligando al usuario del terminal a marcar el número PIN para desbloquear el terminal. - Establecimiento de una contraseña de bloqueo desde el servidor fijando la contraseña a usar. - Localización y seguimiento de los dispositivos gracias al uso del GPS: permite localizar un terminal perdido o robado.

Como hemos visto, la empresa debe actuar en la protección del uso de los dispositivos móviles en la empresa trabajando en tres líneas:

Definición de políticas de uso y gestión
Concienciación del usuario
Uso de aplicaciones Mobile Device Management

3.5 Ciclo de aplicación de la seguridad BYOD

El siguiente esquema es aquel que se debería seguir para implantar y mantener un sistema para el BYOD. Tras un conjunto de tareas relacionadas con la definición de las políticas e implementación de un sistema BYOD contiene un ciclo a repetir cada periodo de tiempo definido (según política de empresa) de revisión y actualización:



Con la actualización con la frecuencia definida (periodos de tiempo o cambios significativos de tecnología o algún tipo de incidente …) mantendremos actualizado el sistema de seguridad frente a nuevos parámetros a controlar de los dispositivos móviles, como podrían ser nuevos tipo de aplicaciones, nuevas tecnologías de comunicación…

4 Medidas legales

Las medidas organizativas son una de las tres piezas clave para mitigar los diferentes riesgos. Pero no debemos olvidar otra pieza importante para llevar a cabo una correcta estrategia BYOD: las medidas legales. Dentro de las mismas, trabajador y empresa deberán firmar un acuerdo de consentimiento 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 a los que pueden acceder, 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 MDM

La tercera pieza para la mitigación de riesgos en los entornos BYOD que completa las medidas organizativas y legales son las medidas técnicas.

Para ver las diferentes opciones en cuanto a las medidas técnicas dentro de una corporación, analizaremos las tecnologías *Mobile Device Management* (MDM). Para ello nos basaremos en el estudio de Gartner de diferentes aplicaciones MDM. La consultora IT Gartner analiza y separa en 4 cuadrantes los diferentes proveedores/fabricantes de aplicaciones MDM. En estos cuadrantes, reconocidos en el mundo empresarial, la consultoría IT Gartner coloca cada aplicación analizada en uno de los 4 cuadrantes disponibles, como forma de presentar sus investigaciones. El cuadrante es una representación de los resultados del estudio de mercado de un producto/servicio tecnológico en un momento concreto.

Para más información sobre los cuadrantes mágicos de Gartner y los criterios de elección de los productos analizados consultar el anexo I.

En el informe de Gartner, con fecha de 4 de Junio de 2014, las aplicaciones MDM son renombradas como aplicaciones Enterprise Mobility Management Suites debido a que ahora, estas aplicaciones, amplían su espectro de actuación, permitiendo una administración de contenido y aplicaciones que antes no permitían.

El informe de aplicaciones EMM (Enterprise Mobility Management) muestra el siguiente resultado gráfico:

Como se observa en el gráfico las empresas líderes en el sector de las aplicaciones MDM (en el informe EMM) son AirWatch, MobileIron, IBM, Good Technology, Citrix. Gartner, en sus informes, también comenta, según su estudio, cuáles son las debilidades y cuáles las "fuerzas" de cada aplicación/proveedor, además de una descripción de la empresa o el producto. Como resumen del informe sobre las aplicaciones MDM (en el informe EMM) podemos resumir lo siguiente para cada aplicación:

Absolute Software
Empresa canadiense, con gran presencia en los sectores educativos, gubernamentales y de la salud, ofrece su producto EMM Absolute Manage como una extensión de sus productos de seguimiento de dispositivos y gestión de clientes.
~~Empresa canadiense, con gran presencia en los sectores educativos, gubernamentales y de la salud, ofrece su producto EMM Absolute Manage como una extensión de sus productos de seguimiento de dispositivos y gestión de clientes.~~
Su producto Absolute Manage proporciona una amplia cobertura de sistemas operativos, soportando iOS, Android, Windows Phone, Mac OS X, Windows 7 y Windows 8. Mac OS X, Windows 7 y Windows 8 están siendo usados como

sistemas operativos también para dispositivos móviles, sobretodo en tabletas.
Se ofrece como producto con instalación local[14] (on-premise) o SaaS[15] (Software as a Service).

Puntos fuertes	Puntos débiles
Producto interesante para empresas que buscan gestionar Macs, PCs y dispositivos móviles desde una sola herramienta.	Débil administración del dispositivo y del contenido para Windows Phone.
Soporte para Mac OS X.	Carece de un portal para los usuarios para localizar, seguir y administrar sus propios dispositivos como sí hacen otros fabricantes.
Incorpora un agente en el firmware de determinados dispositivos, como por ejemplo en móviles Samsung, portátiles Lenovo…, para la localización y seguimiento en caso de robo. Esta tecnología se auto-reinstala en caso de que se intente eliminar del dispositivo permitiendo que se pueda continuar localizando y siguiendo un dispositivo.	

AirWatch
AirWatch es, desde febrero de 2014, de VMware, que planea usar AirWatch para completar su oferta de virtualización y gestión de aplicaciones SaaS. El producto que se ofrece con AirWatch tiene funcionalidad completa de EMM (más un extra de administración de PCs y MACs) aunque a veces los componentes de administración de contenido móvil y gestión de aplicaciones móviles carecen de estabilidad y facilidad de uso.
Se ofrece en formato local o SaaS.
Es una buena opción para organizaciones que traten con un amplio espectro de plataformas.

Puntos fuertes	Puntos débiles

[14] La implementación On_Premise de una solución consiste en la administración y mantenimiento por parte del departamento IT de la empresa de esta solución, instalando y ejecutando la aplicación en servidores (físicos o virtuales) de la propia empresa. Normalmente, el fabricante implementa la solución en las instalaciones del cliente y después es el cliente quien la administra.

[15] Modelo de distribución de un programa donde el soporte lógico y los datos se alojan en servidores de la compañía a la que contratamos el servicio. La administración de la aplicación en cuanto a configuración del sistema y de las opciones corren a cargo de la empresa que contrata el servicio y la empresa propietaria del sistema es la que se encarga de mantener los servidores, de actualizar la aplicación…

Ha demostrado implementaciones a gran escala.	Ha reportado varios errores y problemas en su aplicación Secure Content Locker[16] y en aplicaciones de correo.
Contiene una consola de administración con vídeos de aprendizaje, enlaces y un Wizard para ayudar a los administradores.	La última versión 7.1 está disponible solo para clientes en la nube. Si se requieren actualizaciones inmediatas del sistema solo la aplicación en la nube ofrece este servicio.
Soporta la última versión de iOS desde el primer día y fue una de las primeras en soportar tecnologías como Samsung Knox [17] y Apple Volume Purchase Program[18].	Se han detectado errores en instalaciones en local con el soporte y la estabilidad en el app wrapping [19] de AirWatch.

BlackBerry	
Solución usada por organizaciones que usan dispositivos BlackBerry.	
La versión actual del producto se puede adquirir mediante servicio local o SaaS y es la mejor solución para dispositivos BlackBerry 10.	
BlackBerry sigue perdiendo terreno en el espacio de los dispositivos móviles pese a que la falta de alternativas que ofrezcan capacidades similares de seguridad ha dado a la compañía un respiro.	
Su versión BES10 permite dispositivos BlackBerry, iOS y Android.	
Puntos fuertes	**Puntos débiles**
Opción para dispositivos BlackBerry, ofreciendo, incluso, la capacidad de auditoría y registro de los mensajes SMS.	Falta de soporte para algunas versiones de Android, Windows Phone, Windows 8 y Mac OS X. Windows 8 y Mac OS X son usados principalmente en tabletas digitales.
Ofrece QNX[20] y gestión de identidad y acceso (IAM [21]) para controlar el acceso a las aplicaciones Web como extra al resto de fabricantes.	El soporte para Android y iOS es menor en comparación con otros fabricantes.

[16] Solución empresarial para la sincronización y compartición de archivos protegiendo en un contenedor la información.

[17] Solución de Samsung para garantizar la seguridad y confidencialidad que las empresas buscan en los dispositivos móviles sin afectar la privacidad de los datos personales del usuario.

[18] Apple Volume Purchase Program, en castellano Programa de Compras por Volumen, es un programa de Apple que permite comprar apps del App Store y libros interactivos para el sector educativo.

[19] Permite a los desarrolladores agregar características de seguridad a las aplicaciones sin tener que escribir código adicional.

[20] Las Blackberrys con QNX pueden instalar y ejecutar aplicaciones Android.

[21] Identity Access Management: Permite la administración de identidades digitales, pudiendo otorgar o denegar acciones de usuarios remotos según su identidad en la red.

	La gestión de contenidos en la versión 10 está solo disponible para dispositivos BlackBerry. La compañía plantea ampliar el espectro de cobertura de la plataforma.

Citrix	
Una de sus soluciones, de nombre Workspace Suite, combina la virtualización de escritorios y EMM para ofrecer acceso a aplicaciones y contenido a cualquier dispositivo mediante una combinación de mecanismos físicos y virtuales.	
Su otra solución, XenMobile MDM, está disponible para su uso como opción local o a través de SaaS.	
Xen Mobile es compatible con iOS, Android, Windows Phone, BlackBerry y Windows 8. Citrix MDX Toolkit[22] es compatible con iOS y Android.	
Son una buena opción para las organizaciones que buscan una opción segura para trabajar con Windows, aplicaciones web y móviles, así como para aquellas organizaciones que usan tecnologías como XenApp, XenDesktop y NetScaler.	
Puntos fuertes	**Puntos débiles**
Los clientes valoran con buenas puntuaciones el soporte de Citrix y su asistencia in situ.	Tiene pocas implementaciones grandes (más de 10.000 usuarios) en comparación con otros fabricantes de EMM.
Su módulo Citrix Share File[23] es el más completo que hay entre todos los vendedores de EMM.	Su aplicación WorxMail [24] 1.0 está todavía en desarrollo y ha tenido algunos problemas. Citrix tiene previsto publicar las mejoras dentro de la nueva versión (9.0) de XenMobile.
	Las consolas de administración (MDM, AppController, NetScaler) están separadas haciendo que la administración sea más compleja y menos compacta.

Globo
Ofrece su servicio de soporte MDM a través de SaaS o en local para iOS, Android, Windows Phone y BlackBerry.

[22] Herramienta utilizada para preparar las aplicaciones iOS y Android para su despliegue con Citrix.

[23] Servicio de sincronización e intercambio seguro de archivos.

[24] Aplicación que ayuda a los usuarios a obtener/visualizar el contenido importante de forma más ágil y rápida.

Único entre el resto de competidores del análisis, Globo incluye MADP[25] como parte de la licencia de su solución EMM.	
Globo es una buena opción para aquellas empresas que busquen una solución única de MADP y EMM.	
Puntos fuertes	**Puntos débiles**
Es uno de los pocos proveedores que ofrece en su suite EMM una herramienta suplementaria de desarrollo de aplicaciones.	No proporciona un mecanismo para mostrar la licencia o acuerdo al usuario final antes de la inscripción al servicio del dispositivo. Puede suponer un problema para las empresas interesadas en obtener del usuario final un consentimiento explícito antes de que su dispositivo se añada al sistema EMM.
Soporte amplio para todas las plataformas móviles, incluyendo BlackBerry, lo que le hace ser una buena opción para entornos variados.	Su mobile application management no tiene respaldo para una larga lista de aplicaciones disponibles en los markets públicos.
Ofrece aplicaciones PIM [26] seguras, como correo electrónico, calendario, contactos y mensajería, además de una aplicación de gestión segura de contenidos. En otros "rivales" estos suplementos suponen un coste adicional.	Tiene un soporte MDM muy sólido, pero todavía lejos, en algunas otras áreas, de otros proveedores.

Good Techonology
Empresa ubicada en California conocida por su funcionalidad PIM de containerización a través de su solución Good for the Enterprise (GFE).
Su solución Good for the Enterprise se ha ampliado con la aplicación para gestión de móviles y la administración de contenido móvil, así como con la adquisición de BoxTone que fortalece las capacidades MDM y proporciona administración de servicio móvil que permite a los administradores controlar y gestionar el rendimiento del entorno móvil.
Good for the Enterprise es compatible con iOS y Android mientras que Good Dynamics (módulo de administración de aplicaciones móviles) soporta también Windows Phone.
Good for the Enterprise y Good Dynamics solo están disponibles como

[25] Mobile Application Development Platform: Plataforma de desarrollo de aplicaciones móviles que permite el diseño, desarrollo y pruebas de éstas desde un entorno único integrado.

[26] Calendario, contactos, tareas o notas.

arquitectura local pero Good ofrece sus aplicaciones de empresa y un MDM independiente como opción SaaS.	
Permite un estricto conjunto de normas de seguridad y una completa administración de las aplicaciones móviles.	
Puntos fuertes	**Puntos débiles**
Goods Secure PIM (email, calendario, contactos...) es la oferta más madura entre los fabricantes de EMM analizados que ofrecen aplicaciones PIM.	Su enfoque en la administración de aplicaciones móviles le coloca por detrás de otros vendedores EMM en soporte a MDM, sobretodo para Android y Windows Phone.
Los clientes valoran positivamente su soporte.	El soporte MDM para Windows 8 y Mac OS es más débil que el de otros proveedores líderes en EMM.
La aplicación Good Dynamics aporta una de las plataformas con las opciones de seguridad más completa para aplicaciones en comparación con el resto de fabricantes.	Puede resultar lento de implementar.

IBM	
IBM adquirió en Diciembre de 2013 Fiberlink y ha posicionado su aplicación MaaS360 como una importante solución dentro de las soluciones de movilidad empresarial.	
MaaS360 es compatible con iOS, Android, Windows Phone, Windows 7 y 8 y Mac OS X y su módulo de gestión de aplicación soporta iOS, Android y Windows Phone.	
Opción adecuada para empresas que buscan una solución SaaS y aquellos que ya disponen de otros productos IBM.	
Puntos fuertes	**Puntos débiles**
Puede soportar miles de instalaciones al día.	MaaS no elimina automáticamente los registros de los dispositivos inactivos. Para eliminar estos dispositivos de las vistas, reglas e informes los administradores deben configurar reglas.
Facilidad de uso a nivel de usuario final y administrador. Las instalaciones pueden ser fácilmente personalizadas para cubrir las necesidades de cada empresa. Contiene un autoayuda completa para los usuarios.	Los administradores pueden personalizar las alertas configurando roles y requisitos de cumplimiento. Sin embargo, la presentación de la consola de alertas no ayuda al administrador a priorizar tareas urgentes.

MaaS360 aporta administración de portátiles proporcionando soporte básico de MDM para dispositivos Windows 8.1 y Mac OS X.	

Landesk	
Los productos EMM de Landesk (Mobility Manager y Avalanche) nacen de la adquisición en 2012 de Wavelink.	
Los dos productos comparten el mismo código. Mobility Manager se integra con Landesk Management Suite[27] (LDMS), una herramienta de gestión sólida.	
Avalanche se ofrece como SaaS o como aplicación para su instalación local.	
Los dos productos EMM son compatibles con iOS, Android, BlackBerry, Windows Phone 8, Windows 7 y 8 y Mac OS X.	
Landesk ha fabricado Landesk Fuse que proporciona un portal para usuarios para obtener apps y contenido.	
Puntos fuertes	**Puntos débiles**
Mobility Manager tiene una herramienta de gestión con un potente RBAC[28] y soporte en diferentes idiomas.	Carece de gestión de certificados y políticas para iOS. Además, el soporte para APIs MDM para Android es limitado.
Mobility Manager es uno de los pocos productos que ofrece integración entre EMM y servicios de escritorio.	La gestión de contenidos móviles está limitado al contenido almacenado en el dispositivo y al contenido PUSH[29]. No proporciona acceso a ficheros compartidos ni sincronización.

MobileIron	
Trata de integrar/colaborar en su sistema con productos de otros fabricantes que están más desarrollados. Basa su estrategia en ser independiente de las aplicaciones y dispositivos que la organización use.	
Disponible de forma local o SaaS.	
Compatible con iOS, Android, Windows Phone, Windows 8 y Mac OS X. Su modulo de gestión de aplicación soporta iOS y Android.	
Puntos fuertes	**Puntos débiles**
El soporte al usuario está muy consolidado y recibe buenas críticas.	Su infraestructura dificulta la monitorización y configuración

27 Aplicación de administración que permite descubrir dispositivos en la red y guardar información sobre sus configuraciones, sistema operativo, velocidad de procesador…

28 Role-based Access control: Control de acceso basado en roles.

29 Tipo de comunicaciones sobre internet donde la petición de transacción tiene su origen en el servidor.

	respecto a otros fabricantes.
Sus aplicaciones 'server gateway', la de administración de aplicaciones móviles y sus aplicaciones para clientes han sido validadas por terceros como recomendables tanto en funcionalidad como en implementación.	Su soporte API para Android está más limitado que el de otros fabricantes.
Aporta monitorización en tiempo real de iOS, no habitual en el resto de fabricantes	La consola de administración de MobileIron está solo disponible en inglés, a diferencia de otros fabricantes que dan más cobertura de idiomas. La comunicación con los clientes y el reporte de incidencias sí está disponible en más idiomas.

SAP	
SAP Mobile Secure es una Suite de productos que incluye Afaria (MDM), SAP Mobile App Protection by Mocona (para la administración de aplicaciones móviles) y SAP Mobile Documents (para la administración de contenido móvil).	
Se ofrece como servicio local o SaaS.	
Afaria soporta iOS, Android y Windows Phone. SAP Mobile App Protection by Mocana soporta iOS y Android.	
Sus propuestas para EEM se integran perfectamente con otras plataformas de SAP por lo que es una opción apropiada para aquellas empresas que deseen integrar esta opción EEM con otras aplicaciones SAP ya instaladas.	
La estrategia de SAP pasa por esperar a ver la trayectoria que sigue el mercado y el resto de fabricantes, siguiéndolos a posteriori mostrando pocos factores diferenciadores sobre los principales fabricantes EMM.	
Puntos fuertes	**Puntos débiles**
SAP proporciona una arquitectura escalable, demostrada a través de varios clientes, permitiendo la expansión de los componentes a través de múltiples servidores.	Su historial de soporte a sistemas operativos móviles es más corto que el de sus competidores.
SAP tiene un largo número de socios a nivel mundial para ayudar en las ventas y la implementación de sus sistemas.	La capacidad de la aplicación MDM es incompleta, con debilidades en algunas áreas como la gestión de certificados y el soporte multiusuario para iOS y Android.
	El historial de SAP Mobile Secure muestra que tienen versiones inestables que requieren que los

	administradores implementen soluciones temporales y reinicien el sistema.

SOPHOS	
Su aplicación Sophos Mobile Control (SMC) soporta iOS, Android, Windows Phone y Blackberry.	
Es el único proveedor que tiene como componente de su aplicación un administrador de derechos digitales (digital rights management - DRM).	
SMC está disponible para instalación local.	
SMC suele verse en pequeñas y medianas empresas y raramente en empresas grandes.	
Es una buena opción para las empresas que deseen integrar EPP[30] y EMM en la misma consola.	
Puntos fuertes	**Puntos débiles**
Encriptado transparente que evita la fuga de datos del PC o dispositivo móvil que se integra con productos de otros proveedores de almacenamiento.	La capacidad para adaptarse a los cambios es más lenta que en otros proveedores de EMM.
Es uno de los dos vendedores de EPP incluidos en el estudio. Sus clientes puede aprovechar su relación con SOPHOS para reducir gastos combinando múltiples soluciones de SOPHOS.	Solo soporta certificados de confianza de Microsoft Certificate.
SMC se integra directamente con los gateways UTM [31] de Sophos y CheckPoint facilitando la habilitación del acceso remoto.	No proporciona funciones de seguridad para aplicaciones. Las empresas que deseen implementar aplicaciones deberán usar otro proveedor para esta función.

Soti
Su aplicación, MobiControl, se ofrece tanto como servicio SaaS o con instalación local.
MobiControl soporta iOS, Android, Windows Phone, Windows 8 y Mac OS X pese

[30] Endpoint Protection Platform: solución que aporta seguridad al dispositivo en un solo producto que tiene, entre otros, antivirus, anti programas espías, cortafuegos, control de aplicaciones…

[31] Unified Threat Management o Gestión Unificada de Amenazas. Se nombran así los dispositivos de red cortafuegos que engloban múltiples funcionalidades en la misma máquina, como por ejemplo: VPN, Antispam, Antivirus, Filtro de contenidos…

a que destaca, sobretodo, por el soporte a Android.	
Destaca por tener un administrador de configuración y control para Android con elevadas opciones de administración, configuración y control en comparación con otros fabricantes.	
Debido al buen soporte para Android es una opción recomendada para empresas donde la totalidad o la mayor parte de dispositivos móviles sean Android.	
Puntos fuertes	**Puntos débiles**
Buen soporte remoto, con control remoto total de dispositivos Android y para aplicaciones iOS con el SDK habilitado.	Soti relega en colaboradores suyos la mayoría de funciones de administración de aplicaciones como Secure PIM o el navegador seguro. Esto reduce en control de Soti sobre estos productos.
Tiene un gran número de clientes con un número de dispositivos Android elevado, por lo que tiene una amplia experiencia en funcionalidad y soporte de esta plataforma.	Corta trayectoria en cuanto a soporte a usuarios y administradores.
Su sistema de licencias es sencillo.	Proporciona un gran volumen de opciones y configuraciones para Android. No es así con iOS y Windows Phone donde las opciones son más limitadas.

Symantec	
Esta empresa con sede en California tiene su aplicación Mobile Management Suite (MMS) compuesta de Symantec App Center, Symantec Mobile Management y Symantec Mobile Security.	
MMS está disponible tanto en modo local como SaaS.	
La Suite es compatible con iOS, Android y Windows Phone.	
Symantec adquirió hace poco la aplicación Secure PIM de Nitrodesk que fortalecerá su oferta de EMM.	
Puntos fuertes	**Puntos débiles**
Su app wrapping permite a las aplicaciones ser actualizadas de forma dinámica sin tener que volver a tocar código.	Carece de algunas características básicas, como el soporte a Samsung Knox.
Integra fuertes medidas de seguridad para evitar la pérdida de datos (DLP[32]) y IAM[33].	Su precio se sitúa por encima de la media para soluciones similares.

[32] Data loss prevention

Es uno de los dos vendedores EPP[34] incluidos en el estudio de Gartner. Por lo tanto, los clientes EPP pueden aprovechar su relación con Symantec para el soporte y mejorar el precio de la oferta.	

Tangoe	
Esta empresa de Connecticut ofrece su producto EMM , de nombre MatrixMobile Enterprise Mobility Management, de forma independiente o como parte de su administrador de gastos de telecomunicaciones (TEM).	
MatrixMobile se ofrece para instalación local o como servicio SaaS.	
MatrixMobile soporta iOS, Android y BlackBerry (a través de BES). La compatibilidad con Windows Phone es limitada.	
Carece de algunas políticas de aplicación avanzadas.	
Buena opción para aquellas organizaciones que ya dispongan de TEM[35] y quieran ampliarlo con EMM.	
Puntos fuertes	**Puntos débiles**
Ofrece autoservicio de contratación, administración de activos y capacidad de activación	Muchos de los productos de Tangoe están pensados para ofrecer los mejores resultados cuando se integran en un sistema completo de MMS[36].
Su soporte 24x7 está muy bien valorado por sus clientes.	El soporte a Windows Phone es menor comparándolo con otros fabricantes.
	MatrixMobile EMM se apoya en terceros para completar su oferta EMM: Divide para PIM, Acronis para la administración de contenido móvil, SAP Afaria para soportar Knox. Esto implica que Tangoe no es el único que trabaja en la plataforma y esto puede provocar errores no detectados.

[33] Solución que se utiliza para autenticar un usuario y proporcionarle los derechos de acceso a los recursos adecuados.

[34] EndPoint Protection. Antivirus y cortafuegos administrado de forma centralizada pero que actúa en el dispositivo final.

[35] Telecom Expense Management.

36 Mobility managed services.

6 Conclusiones

Como hemos visto a lo largo del documento, el uso de los dispositivos móviles personales para llevar a cabo tareas laborales accediendo a recursos de la compañía desde ellos trae consigo una serie de ventajas:

- incremento en la productividad
- mayor satisfacción en el trabajador
- mejora en la atención al cliente
- ahorro en costes de adquisición de tecnología

y de desventajas:

- riesgos para la seguridad de la red corporativa
- aumento de las posibilidades de infección malware
- mayor consumo de los recursos de red
- necesidad de reforzar el departamento de soporte y de tecnologías de la información.

Esta nueva forma de relación trabajador-empresa implica riesgos para la información de la empresa y para los datos personales del trabajador. Este hecho obliga a centrar la atención en cualquier vulnerabilidad de los dispositivos móviles y los datos a los que acceden.

Los dispositivos móviles están expuestos a diferentes tipos de amenazas que pueden provocar la pérdida de datos o el robo de identidades. Para evitar y reducir al máximo estos riesgos de fugas de datos, las empresas deberán adoptar diferentes medidas de mitigación que ayuden a evitar fugas de datos que podrían incluso llevar al cierre de la empresa.

Para mantener una red de dispositivos móviles segura la empresa deberá actuar en las siguientes líneas:

Medidas de mitigación
Definición de políticas de uso y gestión
Uso de aplicaciones Mobile Device Management
Concienciación del usuario

Definición de políticas de uso y gestión

Para conseguir que los accesos a la red corporativa desde dispositivos móviles sea segura y que los datos corporativos estén a salvo es necesario definir unas políticas que ayuden a controlas los accesos a los datos y su uso. Estas políticas han de ser

claras y concisas y deberán ser aceptadas por escrito por aquellos que quieran hacer uso de sus dispositivos móviles en el entorno empresarial.

Ejemplos de políticas de uso y seguridad
Definición de qué equipos y aplicaciones pueden acceder a la red corporativa.
Definición de qué funciones están permitidas con los datos. Por ejemplo, se puede prohibir que un fichero recibido por correo sea descargado al dispositivo móvil o renviado a una cuenta de correo no corporativa.
Prohibición de *jailbreak o root*.
Habilitación del borrado remoto de los datos del dispositivo en caso de pérdida o robo.
Obligatoriedad de actualizar el sistema operativo y las aplicaciones a las nuevas versiones (en teoría, más seguras)

El incumplimiento de estas políticas por parte del trabajador puede acarrear problemas de seguridad a la empresa, por lo que ésta dentro de las políticas de la empresa podría incluirse la posibilidad de revocar al trabajador el derecho de uso del BYOD

Uso de aplicaciones Mobile Device Management o Enterprise Mobility Management

Estas aplicaciones son indispensables para controlar las conexiones a la red corporativa por parte de los dispositivos móviles, ayudando a aplicar y gestionar las políticas de seguridad tradicionales (firewalls, antivirus…) en su intento por lograr el máximo nivel de seguridad y gestión de los datos de la empresa. Las aplicaciones MDM o EMM se basan en el control de las aplicaciones y de sus funciones, en el control de los datos y en el comportamiento del usuario.

Permiten asegurar, monitorizar y gestionar dispositivos móviles de forma que se garantice la seguridad de la información y de la red.

Estas aplicaciones aportan diferentes ventajas al entorno profesional dotando de una base sólida a la empresa no solo en cuestión de seguridad:

Ventajas del uso de aplicaciones MDM
Permiten realizar un seguimiento de los dispositivos móviles, líneas, usuarios y datos: por ejemplo manteniendo una lista de contactos actualizada de forma centralizada para todos los dispositivos.
Permiten elaborar informes (por ejemplo: informe de consumo de datos) que permitan tomar mejores decisiones para el futuro de la

empresa.
Gestión de la información relacionada con el uso del dispositivo móvil.
Distribución y administración aplicaciones corporativas, tanto empresariales como de IT (seguridad).
Control de las aplicaciones que pueden ser utilizadas evitando que los usuarios ejecuten aplicaciones que no son productivas para las empresas.
Facilitan la administración de los dispositivos.

Las aplicaciones MDM o EMM permiten, a nivel de seguridad, securizar, monitorizar y gestionar diversas funciones de forma remota desde un servidor centralizado en el que se definen las políticas o actuaciones a realizar (instalación de un software, cambios de *password*, denegación de instalación de ciertos programas, activación de cifrado para la protección de datos, separación de datos personales y corporativos, prohibición de renvío de ciertos correos, seguridad en caso de robo o pérdida…).

Se pueden diferenciar cinco campos en los que se puede actuar desde una aplicación MDM en cuanto a la seguridad se refiere:

Campos gestionables desde un MDM	
Gestión de aplicaciones	Gestionando, implementando, instalando, bloqueando…. las aplicaciones móviles de los dispositivos.
Gestión de políticas	Controlando identidades, sincronizaciones, integración de cuentas…
Gestión de seguridad	Aplicando las políticas de seguridad, de autenticación y encriptación definidas, del bloqueo o borrado del dispositivo, de la detección de Jailbreak…
Gestión de inventario	Controlando el estado de los dispositivos y su ubicación.
Gestión de servicios de telecomunicaciones	Controlando consumos y usos de los servicios de telecomunicaciones.

La correcta elección, instalación y administración de una aplicación EMM será básica para lograr un alto índice de seguridad en el uso de los dispositivos móviles en el entorno laboral.

Medidas legales

Otra pieza clave dentro para llevar a cabo una correcta estrategia BYOD son las medidas legales. Dentro de éstas, trabajador y empresa deberán firmar un acuerdo

de consentimiento 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 regulará la confidencialidad y secreto y la regulación del uso de BYOD.

Concienciación del usuario

Para evitar ataques dirigidos al usuario del dispositivo móvil no hay mejor medida que aplicar medidas destinadas a concienciar y educar a los trabajadores para mejorar el nivel de ciberseguridad tanto en movilidad como en otros aspectos relevante en la empresa orientados a reducir l nivel de riesgo.

7 Anexos

7.1 Anexo I

¿Qué son los cuadrantes mágicos de Gartner?
Como ellos mismos definen, «*es la culminación de la investigación de un mercado específico, dotando al interesado en el informe de un amplio punto de vista de la posición relativa de los rivales en el mercado. Gartner, especialista en consultorías IT, afirma que aplicando criterios uniformes de evaluación y un tratamiento gráfico, el cuadrante ayuda rápidamente al interesado a ver como los proveedores de una tecnología están tratando la tecnología estudiada. Una vez realizado el estudio, se muestra en un cuadrante gráfico, ubicando cada empresa/producto/solución en el que corresponda según sus criterios.*»

Estos cuadrantes no han de ser cogidos por las empresas como el único punto para valorar que opción escoger para adoptar una tecnología u otra. Gartner recomienda a los interesados en estos productos seguir estas recomendaciones antes de decidirse por una u otra opción:

Recomendaciones de Gartner para escoger una tecnología	
1º	Señalar las necesidades de la empresa y luego elaborar una lista de proveedores.
2º	Considerar todos los posibles escenarios que se pueden tener en la empresa, tales como BYOD, y casos específicos de la organización.
3º	No elegir el proveedor simplemente basando la decisión en la posición de estos en el cuadrante mágico de Gartner.

Para ubicar las tecnologías analizadas en un cuadrante u otro Gartner se basa en dos criterios:

- En el eje x Gartner define el elemento ***completeness of visión*** (integridad de visión) que representa el conocimiento de la empresa sobre como se puede aprovechar el momento actual y futuro del mercado para generar valor. Para dar nota a este elemento Gartner evalúa las intenciones futuras de los proveedores sobre la orientación de su producto.
- En el eje y ***ability to execute*** se representa la habilidad de la empresa para ejecutar su visión de mercado, así como su capacidad para tener éxito en el mercado ganando cuota de mercado y lograr un crecimiento de los ingresos.

Mide la habilidad del fabricante de conocer las necesidades de los compradores de aplicaciones EMM.

El cuadrante se divide en 4 sectores, colocando, al final del estudio, a cada proveedor en un cuadrante. Para el caso que nos ocupa cada cuadrante significa lo siguiente:

Definición de los cuadrantes	
Leaders	Proveedores que puntúan alto en los dos criterios anteriores, con lo que están ejecutando bien su visión actual y están bien posicionados para el futuro. Estos proveedores llevan varios años de implementación probada en clientes, una cuota elevada de clientes y colaboraciones con otros proveedores. Tienen los productos más completos del mercado y están alineados con las tendencias del mercado MDM. Se considera que tienen una estrategia con una alta probabilidad de éxito.
Visionaries	Proveedores que tienen una alta capacidad en ciertos aspectos del mercado MDM. Abordan pequeñas parcelas del mercado de forma muy eficiente. No pueden tener el producto, rendimiento empresarial, capacidad ni integridad del producto como sí lo tienen los principales proveedores de estos productos.
Challengers	Proveedores que ejecutan de forma correcta en la actualidad o que dominan un segmento grande pero que no demuestran una correcta visión del futuro.
Niche Players	Proveedores que se centran en un segmento pequeño y que pecan de eficacia en el resto de aspectos. Normalmente son proveedores que trabajan en una idea más reducida en lugar de en la ejecución de una solución completa, normalmente por falta de recursos. Para un cliente esta puede ser una buena opción si no requiere más opciones que las que ofrece este proveedor.

Para la realización del informe se han tenido en cuenta diversos factores a la hora de seleccionar las empresas a analizar. Los distribuidores debían:

Requisitos Gartner para que una empresa MDM/EMM fuese analizada
Haber vendido 8 millones de dólares en EMM en 2013.

Tener 1500 clientes EMM.
Tener 500.000 licencias en entornos de clientes.
Tener cinco referencias del uso del producto en entornos de producción.
Tener soporte para al menos 3 sistemas operativos de móvil.
El producto debía ser capaz de gestionar las políticas y el control de datos compartidos por las aplicaciones móviles.
El producto debía proporcionar un contenedor en el dispositivo móvil para almacenar y administrar contenido.