Informe de Amenazas CCN-CERT IA-21/13

Riesgos y amenazas del *Bring Your Own Device* (BYOD)

30 de octubre de 2013

ÍNDICE

1. INTRODUCCIÓN

La movilidad y la necesidad o deseo de estar siempre conectado es una de las características que definen a nuestra sociedad actual. El desarrollo de las tecnologías inalámbricas y de los dispositivos y comunicaciones móviles ha posibilitado, y en buena medida fomentado, esta situación.

Gracias a esta movilidad, cada vez es mayor el número de empleados que utilizan la tecnología de la que son propietarios (hardware o software) para realizar tareas relacionadas con su trabajo, desde cualquier lugar, accediendo, por tanto, con distintas tecnologías (3G, Wi-Fi, etc.) al entorno, servicios y datos corporativos. Este fenómeno denominado *Bring your Own Device* (BYOD), en castellano "trae tu propio dispositivo", se ha convertido en una tendencia al alza, que, si bien produce beneficios para ambas partes (organización y trabajador), no está exenta de numerosos riesgos y amenazas para los sistemas de información corporativos, así como ciertos condicionantes legales que no pueden pasarse por alto en la Política de Seguridad de un organismo o empresa que decida, conscientemente, permitir la implantación de este concepto en el funcionamiento de su organización.

Dado que es probable que estemos ante un fenómeno imparable, del que ninguna organización pueda abstraerse, es preciso, por lo menos, conocer los riesgos, amenazas y vulnerabilidades existentes en estos entornos para poder desarrollar una **Política de Seguridad BYOD,** incluida en la Política de Seguridad General. Unas directrices que tengan en cuenta los **dispositivos**, las **formas de acceso** y **las aplicaciones** y que sean aplicables en todas las capas de la organización, incluidos, por supuesto los altos directivos (exceptuados en numerosas ocasiones, cuando en realidad son el blanco preferido de los ciberatacantes por manejar la información más importante y sensible de la organización).

Y aunque el concepto BYOD engloba a todos los dispositivos propiedad del empleado con los que se accede a la red corporativa (incluidos portátiles y ordenadores de sobremesa, por ejemplo), es preciso mantener una especial atención sobre los **dispositivos móviles de última generación** (tabletas, *smarthpones,* e-readers, etc.) que se han convertido en un blanco fácil para los ciberataques, tanto por su uso masivo, como por la ausencia de medidas de seguridad por parte de sus usuarios. De hecho, según, el último informe de Symantec (Norton 2013)[1], el incremento exponencial en su uso no está siendo acompañado de las medidas de seguridad que se requerirían (cerca del 50% de sus usuarios no realizan ninguna de las precauciones básicas como contraseñas, software de segurirdad o *back up* de archivos para sus dispositivos móviles). Los usuarios parecen olvidar que este tipo de dispositivos tiene como mínimo, las mismas capacidades que los ordenadores portátiles o de sobremesa, en donde las medidas de seguridad adoptadas son mayores.

Ante este reto que se presenta a las organizaciones, tanto públicas como privadas, se ofrece una serie de mejores prácticas de implantación, con el fin de evitar que el BYOD se convierta en un problema crítico en la organización.

[1] Symantec: 2013 Norton Report: go.symantec.com/norton-report-2013

2. ¿QUÉ ES BYOD?

En los últimos años, la tendencia a que los usuarios y empleados de una organización utilicen sus equipos personales para el acceso al entorno corporativo y la realización de sus tareas profesionales desde cualquier lugar se ha extendido de manera fulminante. Nos encontramos ante un baile de acrónimos del que, sin duda, el que ha conseguido una mayor aceptación es el de **BYOD** *(Bring Your Own Device)*, en castellano *Trae tu propio dispositivo*. Este es un concepto que define la posibilidad de que los empleados de una organización usen los dispositivos de los que son propietarios para desarrollar sus funciones profesionales, accediendo al entorno, servicios y datos corporativos.

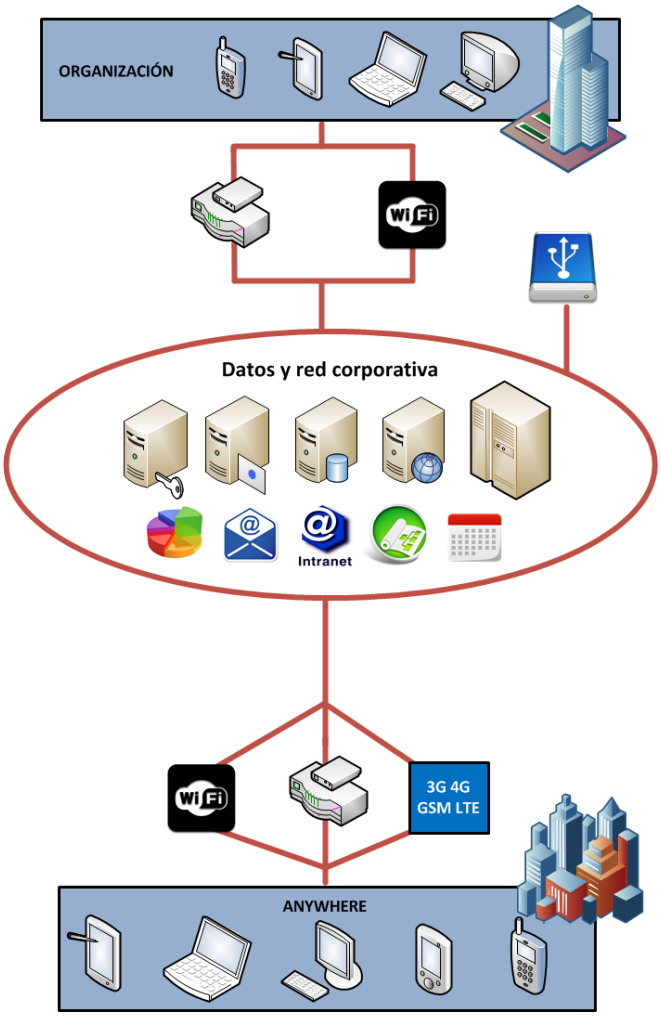

Figura 2-1. Esquema del BYOD

También se le conoce como **BYOT** (*Bring Your Own Technology*) un fenómeno mucho más amplio que incluye toda la tecnología y software propiedad de los empleados y utilizada por éstos para realizar tareas relacionadas con su trabajo,dentro o fuera de la empresa (navegador web, reproductor multimedia, antivirus, procesador de texto, aplicaciones, etc.).

El tercer término que está siendo adoptado es el denominado **BYOA** (*Bring Your Own App(lication)*) en donde los usuarios instalan apps de los mercados de aplicaciones públicos en sus dispositivo móviles personales o corporativos para incrementar su productividad, empleándolas para realizar tareas profesionales y manejar, por tanto, datos corporativos.

Por último, y quizá el más correcto y el que mejor refleja el riesgo para las organizaciones, es el de **CYOD** (*Connect Your Own Device*), ya que no existe riesgo de seguridad asociado hasta que el usuario conecta su dispositivo personal a la red (privadas o Internet, vía Wi-Fi o 3G, por ejemplo)o sistemas (por ejemplo, vía USB) de la organización para acceder a los servicios y datos corporativos[2].

[2] Guía CCN-STIC 457 "Herramientas de gestión de dispositivos móviles: MDM"

Sea cual fuere el término empleado, los modelos BYOD, como mínimo, permiten a los usuarios acceder a servicios, recursos o datos corporativos (tales como correo electrónico, servidores de archivos, bases de datos, aplicaciones…) desde sus *smarthpones* o teléfonos móviles avanzados e inteligentes, tablets, agendas electrónicas (PDA), lectores de libros electrónicos o *e-readers*, ordenadores portátiles, memorias USB e, incluso, ordenadores de sobremesa.

Estos dos últimos dispositivos no suelen estar incluidos estrictamente en la categorización de BYOD, sin embargo, son ampliamente utilizados para realizar tareas desde casa (teletrabajo) y para almacenar información corporativa. De hecho, según un estudio de ESET Latinoamérica[3] (Figura 2.2), el 83,3% de los empleados utiliza memorias USB de su propiedad para almacenar información del trabajo; un 82,2% portátiles y un 55% teléfonos inteligentes. El dato más preocupante es que cerca de la mitad de los encuestados no manejan la información corporativa de forma cifrada en su dispositivo personal, incluso el 15,6% dice no saber cómo se debe manejar dicha información.

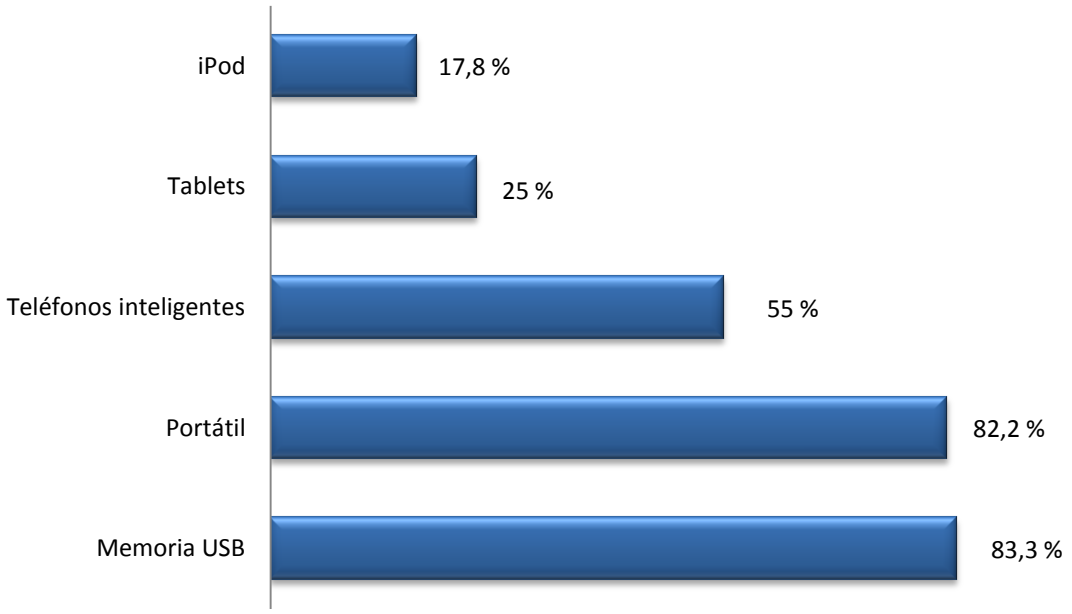

Figura 2-2.: Dispositivos personales más utilizados por los empleados en la empresa (Estudio de ESET)

2.1 Fenómeno en expansión

Centrándonos en el término que la industria ha adoptado de forma general (BYOD), aunque teniendo en cuenta que puede abarcar todos los anteriormente mencionados, conviene reseñar que la primera vez que que fue mencionado fue en un artículo de la Conferencia UBICOMP 2005 *(International Joint Conference on*

[3] "Retos de seguridad para las empresas a partir de BYOD" ESET Latinoamérica

Pervasive and Ubiquitous Computing)[4]. Su desarrollo, no obstante, se inició en 2009, en el seno de la compañía Intel que permitió y promovió esta política entre sus empleados.

Desde entonces y hasta la fecha, su evolución y aceptación ha ido en aumento en organizaciones de todos los tamaños y sectores (incluida la Administración Pública). Así, según el *Informe Norton 2013,* de Symantec, el 49% de los usuarios utilizan sus dispositivos personales para el trabajo (aunque el 36% manifiesta que su organización no cuenta con ninguna política específica de seguridad BYOD).

Por su parte, la consultora Gartner, señala que hoy en día el 36% de las empresas tienen una política BYOD y un 32% más tienen en mente instalarla en los próximos 12 meses. Esta misma consultora, considera que en 2016, el 80% de los empleados elegirá su propio equipamiento para trabajar[5].

Este fenómeno se ha visto favorecido por el desarrollo de los dispositivos móviles y de las tecnologías inalámbricas en los últimos años, que han incrementado sus capacidades, prestaciones y posibilidades, incluso superando a los ordenadores portátiles, al incluir elementos adicionales como *Bluetooth*, acelerómetros, GPS y/o cámaras de fotos y vídeo. De hecho, según un estudiio de IDC, el mercado de los dispositivos inteligentes conectados (PC, tabletas y smarthpones) alcanzó una cifra en 2012 de 916 millones de unidades en todo el mundo y alcanzará los 1.840 millones en 2016.

Las capacidades de estos dispositivos vienen determinadas por:

- **Hardware**: almacenamiento (disco duro o memoria interna y soporte para tarjetas externas), comunicaciones de voz y datos (infrarrojos, Bluetooth, Wi-Fi, GSM, GPRS, EDGE, UMTS, HSDPA…), localización (GPS), acelerómetro (para detectar la dirección, velocidad e intensidad de los movimientos del dispositivo), multimedia, interfaces de usuario avanzadas
- **Software:** sistema operativo (Windows Mobile, Symbian, RIM, Android, iPhone, WebOS, etc.) y aplicaciones.

[4] En.wikipedia.org/wiki/Bring_your_own_device

[5] Ken Dulaney and Paul DeBeasi, "Managing Employee-Owned Technology in the Enterprise," Gartner Group, October 2011.

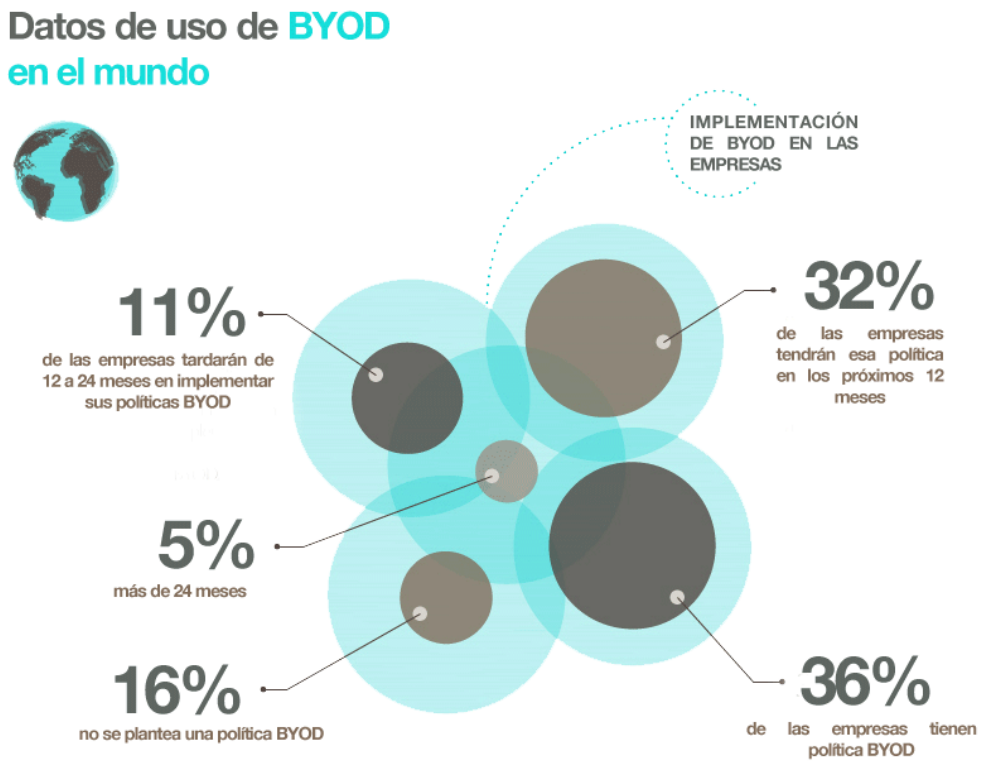

Figura 2.3 : Situación actual del BYOD[6] (IXOTYPE-Cisco Systems)

3. OPORTUNIDADES VS RIESGOS

El incremento constante del BYOD ha venido motivado no sólo por el desarrollo tecnológico conseguido, sino también por las ventajas y oportunidades que brindan tanto a las organizaciones, como para los usuarios. Sin embargo, todas ellas tienen un contrapunto que es preciso tener en cuenta a la hora de implantar una política BYOD (partiendo del hecho de que es muy probable que estemos ante una tendencia imparable que más pronto que tarde tendrá que estudiarse en cualquier tipo de organización). Entre ellas pueden señalarse las siguientes:

⇑ **Ahorro de costes** al no tener que adquirir la organización estos dispositivos (o financiarlos mediante *Leasing*), cargar con el software interno, comprar licencias corporativas, cubrir seguros de robos, hurtos, y otras eventualidades que pueden sufrir dichos dispositivos, asumir el deterioro de los equipos, o la obsolescencia tecnológica.

⇓ **Gastos adicionales:** un entorno BYOD conlleva una serie de gastos e inversiones adicionales de gestión, mantenimiento y soporte e integración en los entornos TIC de las organizaciones, que normalmente

6 IXOTYPE "BYOD en España" Infografía de fuentes: Cisco Systems, ZD NET, Gartner, VMwareel, Informe Ovum 2012, ComScore,CheckPoint http://www.ixotype.com/media/byod_infografia_ixotype..jpg

no es tenido en cuenta. Del mismo modo, la adopción de un modelo BYOD hace perder a la organización la capacidad de reducir costes mediante la compra masiva de hardware o software.

⇑ **Mejora de la productividad**, ligada a una mayor satisfacción de los empleados al utilizar dispositivos familiares para ellos y elegidos en función de sus gustos y afinidades.

⇓ **Distracción** por parte del empleado, dado las capacidades recreativas de todos estos dispositivos (aplicaciones multimedia, acceso a redes sociales, mensajería instantánea, etc.).

⇑ **Mejores condiciones de trabajo** fomentando la flexibilidad laboral y el teletrabajo, con la reducción de costes de desplazamiento y conciliación de la vida laboral que ello conlleva.

⇓ Incremento de posibilidades del **extravío y el hurto** de dispositivos, así como del uso de redes inseguras (redes públicas), que posibilita ciberataques de tipo *man-in-the-middle*[7]. El informe Norton 2013 señala que en 2012, un 27% de los adultos reconocía haber perdido su dispositivo móvil o haber sufrido un robo del mismo.

⇑ **Actualización constante:** Los dispositivos BYOD tienden a ser más novedosos y avanzados, por lo que la empresa se beneficia de las últimas características y capacidades. Los usuarios actualizan su hardware y software personal mucho más a menudo que las empresas, cuyos ciclos de actualización suelen ser más lentos.

⇓ **Complejidad añadida para el Departamento de Sistemas** que deberá gestionar los dispositivos y securizar en tiempo y forma las actualizaciones. La organización tiene que acomodar las dos facetas del dispositivo, personal y profesional, en el entorno TIC y de manera segura, así como definir y conjugar los requisitos y necesidades de ambos mundos.

⇑ **Empleados satisfechos** que pueden considerar un privilegio poder utilizar sus propios dispositivos y aplicaciones para trabajar en lugar de estar obligados a utilizar los que ha elegido el departamento de seguridad de la organización (dispositivos y aplicaciones menos vanguardistas, más económicos, más antiguos, utilizados por múltiples usuarios, etc). Estudios[8] revelan que el 74 % de las organizaciones ha experimentado una mejora en la productividad de los empleados, mientras que el 70 % ha mejorado los tiempos de respuesta a los clientes.

⇓ **Discriminación profesional** al crearse, involuntariamente, un trabajo desigual para los usuarios.

---

7 En criptografía, un ataque man-in-the-middle o JANUS es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar la voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante es capaz de observar e interceptar mensajes entre las dos víctimas

8 DELL: Global BYOD Survey Results http://www.dell.com/learn/us/en/uscorp1/secure/2013-01-22-dell-software-byod-survey

4. AMENAZAS Y VULNERABILIDADES DEL BYOD

Existen numerosas amenazas y vulnerabilidades asociadas a las políticas de BYOD que pueden poner en riesgo la seguridad, tanto del propio dispositivo, como de la información que gestiona y los sistemas a los que se accede. En este sentido, el último *Informe de Ciberamenazas y Tendencias* publicado por el **CCN-CERT**[9] señala el crecimiento constante de vulnerabilidades en dispositivos móviles, donde se descubren de manera tardía y tardan meses en resolverse. Esto hace posible que los atacantes dispongan de un tiempo más que suficiente para acceder a la información del dispositivo y, tras ello, a los sistemas corporativos a los que puedan estar conectados.

Conviene tener en cuenta que más de un tercio de las **vulnerabilidades** podría derivar potencialmente en una violación completa de los aspectos de seguridad de una organización: hacer que el sistema completo quede fuera de servicio (ataque a la disponibilidad), realizar alteraciones en los ficheros del sistema (ataque a la integridad), acceder a los ficheros del sistema (ataque a la confidencialidad) y suplantar la identidad del usuario del dispositivo (autenticación).

Un muestra del riesgo existente, lo encontramos en la cifra de código dañino identificado en la primera mitad de 2013[10] que alcanzó las 1.300 muestras diarias para móviles, detectándose unas 250.000 muestras solo para Android.

De hecho, recientes investigaciones muestran que casi el 75%[11] de las organizaciones estudiadas permiten el acceso a activos de información a través de dispositivos que no están sujetos a la administración de seguridad corporativa. Del mismo modo, muestran que, con frecuencia, la política de seguridad que se redacta y publica para tratar esta problemática es ignorada sistemáticamente por los empleados, cuya concienciación sobre los riesgos que se derivan de las fugas de datos es, todavía, baja. Estas mismas fuentes señalaron que más de la mitad de las organizaciones estudiadas han experimentado un aumento de los ataques de malware en relación con la explotación de aplicaciones o dispositivos al margen de los institucionales.

En una encuesta desarrollada por la empresa Fortinet[12], y realizada en más de quince países, entre ellos España, se encontró que cerca del 42% de los encuestados indicaron la pérdida de datos y la llegada de software malicioso a sus redes a consecuencia del BYOD.

9 CCN-CERT IA-09/13 Ciberamenazas 2012 y Tendencias 2013

10 FortiGuard Midyear Threat Report http://www.fortinet.com/resource_center/whitepapers/quarterly-threat-landscape-report-q213.html

11 Trend Micro (January 2012) 'Trend Micro Consumerization – The cause and effect of consumerization in the workplace': http://uk.trendmicro.com/imperia/md/content/uk/about/consumerization/consumerization_exec_summary-en.pdf

12 Fortinet® Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems (2012). http://www.fortinet.com/press_releases/120619.html

Asimismo, Fortinet señaló que "más de un tercio de los trabajadores, un 36%", admitió que había infringido o infringiría la prohibición de usar sus dispositivos personales con fines profesionales.

Por último, el Informe Norton 2013 remarca la escasa concienciación en materia de seguridad con respecto a los dispositivos móviles (muy inferior a otros equipos, tal y como refleja la Figura 4-1). Así cerca del 50% de los usuarios no realizan las precauciones básicas como contraseñas, software de seguridad o *back up* de archivos para sus dispositivos móviles. Sólo el 26% de los ususarios tiene medidas en este sentido.

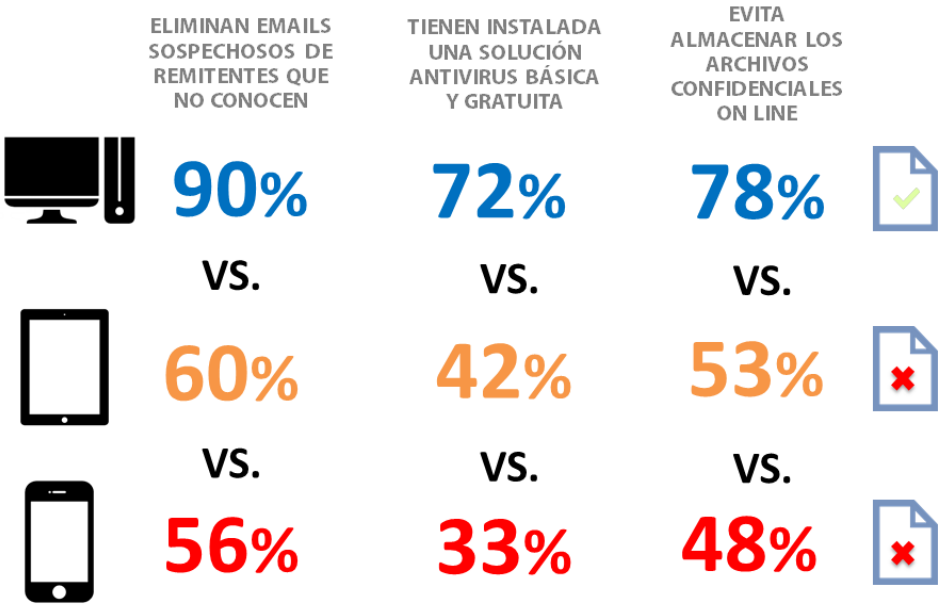

Figura 4-1. Comparativa de medidas de seguridad adoptadas según los distintos dispositivos (ordenador, Tablet o Smartphone). Informe Norton 2013

Por todo ello, antes de desplegar una solución BYOD, las organizaciones deben realizar un análisis de riesgos que identifique los recursos (activos) que resulten de interés, sus vulnerabilidades y amenazas y la probabilidad de materialización de éstas, determinándose seguidamente las medidas de seguridad a adoptar. Entre todos los riesgos conviene tener en cuenta los siguientes[13]:

4.1 Riesgos derivados de la movilidad

13 Para profundizar en estos riesgos y amenazas se pueden revisar las Guías CCN-STIC 450 (Seguridad en Dispositivos Móviles) y CCN-STIC-404: Control de soportes informáticos (para aquellos otros equipos como USB o portátiles que también pueden emplearse en una política BYOD.

Uno de los mayores problemas que plantea la securización de los dispositivos personales deriva, precisamente, de la posibilidad de que puedan usarse en ubicaciones muy diversas, tanto dentro de las instalaciones de la organización en cuestión (bajo cuyo perímetro de seguridad puede estar desplazándose permanentemente), como en localizaciones externas (domicilio de los usuarios, lugares públicos, hoteles, etc.), lo que facilita el acceso físico a los dispositivos (extravío, robo o descuido temporal) por parte de un intruso, tanto para el acceso a la información que allí se almacena, como para la instalación de software de espionaje encubierto (aunque este también puede llevarse a cabo a través de actualizaciones remotas). Este riesgo es muy importante dado que este tipo de dispositivos almacenan gran cantidad de información (credenciales de acceso a servicios web e Internet, credenciales de cuentas de correo electrónico, mensajes de correo y telefonía, información de llamadas de telefonía y VoIp, documentos privados y confidenciales, agenda de contactos, calendario con información de eventos y actividades, fotografías, vídeos, grabaciones de voz, lista de tareas, etc.).

Medidas de seguridad a adoptar
• **Nivel 1** Exigiendo autenticación antes de lograr el acceso al dispositivo y/o a los recursos corporativos accesibles a través de dicho dispositivo. Tales mecanismos de autenticación suelen estar basados en contraseñas simples (PIN) y, salvo excepciones, asumiendo que el dispositivo en cuestión tiene un único usuario. Otros métodos de autenticación más robusta, tales como los basados en dispositivos externos (tokens), autenticación de dispositivos basada en red y autenticación de dominios.
• **Nivel 2** No permitiendo el almacenamiento de información sensible en el dispositivo móvil. Si esto no es posible, será necesario proteger la información sensible almacenada –cifrándola, por ejemplo-, haciendo al tiempo imposible su extracción del dispositivo por personas no autorizadas.
• **Nivel 3** Proporcionando a los usuarios de dispositivos la formación y la concienciación necesarias para reducir los comportamientos poco seguros y su frecuencia.

4.2 Uso de dispositivos, aplicaciones y contenidos no-confiables

Los dispositivos propiedad de los usuarios presentan importantes deficiencias en materia de seguridad derivadas tanto de su propia estructura como de un uso inseguro. Tal es el caso, por ejemplo, de los procedimientos de *jailbreaking*[14] o *rooting*[15] que algunos usuarios llevan a cabo, introduciendo importantes elementos de riesgo.

14 El jailbreak es el proceso de eliminación de las restricciones impuestas por Apple en dispositivos que utilicen el sistema operativo iOS, mediante el uso de kernels modificados. Tales dispositivos incluyen los iPhone, iPod Touch, iPad y la Apple TV de segunda generación. El jailbreak permite a los usuarios acceder sin limitaciones al sistema operativo, permitiendo descargar aplicaciones y otros elementos que no estén disponibles a través de la App Store oficial.

En cuanto a las aplicaciones, una de las principales amenazas es la incapacidad de detectar qué software está instalado en los dispositivos personales que se conectan a su red. Máxime teniendo en cuenta que la mayoría de las aplicaciones que se ejecutan en *smarthpones* y tabletas se descargan de tiendas (oficiales y no oficiales) que pueden infectar nuestros dispositivos y por consiguiente a nuestra red corporativa.

Por último, en algunos casos, los dispositivos móviles pueden tener acceso a contenidos potencialmente peligrosos, que no son accesibles mediante otro tipo de equipamientos. Tal es el caso, por ejemplo, de los **códigos QR** (Quick Response Codes). Los códigos bidireccionales QR suelen contener direcciones URL a las que los dispositivos móviles acceden a través de sus cámaras. Es prácticamente imposible detectar si la URL de destino da acceso a una página web dañina, por lo que este tipo de contenidos deben ser tratados como potencialmente peligrosos, adoptando las medidas de seguridad oportunas. Lo mismo pasaría en ordenadores sobremesa o portátiles con el phishing[16] aunque en esta ocasión podemos y debemos revisar la URL de los enlaces y comprobar su legitimidad evitando acceder directamente.

Medidas de seguridad a adoptar
• **Nivel 1:** Forzar el tráfico de datos a través de pasarelas web seguras y utilizar servidores proxy HTTP, u otros dispositivos intermedios para verificar las URL de destino
• **Nivel 2:** Permitir la instalación únicamente de aplicaciones provenientes de "listas blancas" o posibilitar la ejecución de las mismas en contenedores seguros (*Sandbox*)
• **Nivel 3:** Verificar que las aplicaciones sólo tienen del dispositivo móvil los permisos estrictamente necesarios para su adecuado funcionamiento.
• **Nivel 4** Prohibir el uso de ciertos dispositivos móviles o la instalación de aplicaciones de terceras partes o el navegador (o restringir su uso a determinadas páginas)

15 El rooting en un proceso que permite a los usuarios de smartphones, tabletas y otros dispositivos que ejecutan el sistema operativo móvil Android de elevar el control de privilegios del sistema operativo. El rooting se realiza a menudo con el objetivo de superar las limitaciones que los operadores de comunicaciones o de hardware introducen en algunos dispositivos, lo que hace posible modificar o reemplazar las aplicaciones y ajustes del sistema, ejecutar aplicaciones especializadas que requieren permisos de administrador, o realizar otras operaciones de otro modo inaccesibles para un usuario de Android normal.

16 CCN-CERT 401 Glosario de términos. Los ataques de "phishing" usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros). Para alcanzar al mayor número posible de víctimas e incrementar as sus posibilidades de éxito, utilizan el correo basura ("spam") para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a lugares de Internet falsificados, páginas web, aparentemente oficiales, de bancos y empresas de tarjeta de crédito que terminan de convencer al usuario a que introduzca datos personales de su cuenta bancaria, como su número de cuenta, contraseña, número de seguridad social, etc.

4.3 Uso de redes inseguras

El acceso de los dispositivos personales a los servicios o a los datos corporativos puede llevarse a cabo usando redes públicas (por definición, no confiables) o redes privadas de la organización o infraestructuras de comunicación comunes. En el caso de redes públicas, las organizaciones no suelen disponer de mecanismos para controlar la seguridad del acceso de dispositivos móviles a tales redes públicas, acceso que puede tener lugar, generalmente, a través de mecanismos wi-fi o tecnologías de telefonía móvil. Por tanto, el uso de este tipo de redes posibilita ciberataques de tipo *man-in-the-middle* (véase nota 7), que podrían interceptar e incluso modificar los datos en tránsito.

Medidas a adoptar
• **Nivel 1:** Usar mecanismos de cifrado fuerte (tales como el uso de redes privadas virtuales VPN)[17].
• **Nivel 2:** Usar mecanismos de autenticación mutua que permitan a las partes intervinientes en la comunicación identificarse mutuamente antes de intercambiar ningún tipo de información.
• **Nivel 3:** Prohibir el uso de redes wi-fi inseguras, especialmente aquellas para las que se han publicado vulnerabilidades.
• **Nivel 4:** Desactivar aquellos interfaces de red del dispositivo que no vayan a usarse.

4.4 Interconexión con otros sistemas

Es muy frecuente que los dispositivos personales se interconecten con otros sistemas, a efectos de intercambio y almacenamiento de datos. Las interconexiones más usuales son aquellas que tienen lugar, a través de mecanismos inalámbricos o por cable, entre el dispositivo móvil y un ordenador de sobremesa o portátil, al objeto de sincronizar el contenido de ambos equipos. Ejemplos de estos riesgos se dan cuando se conecta un dispositivo móvil de titularidad del usuario a un ordenador de titularidad de la organización o cualquier dispositivo móvil a una estación de recarga (de baterías) no confiable.

En estos casos existe el riesgo de almacenamiento de datos en ubicaciones no confiables y fuera del control de la organización, intercambio no autorizado de datos entre dispositivos o transmisión de infecciones con código dañino, de un dispositivo a otro.

17 Sobre este particular, consúltese la Guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.

Medidas a adoptar
• **Nivel 1:** Especificar qué dispositivos personales pueden sincronizarse con cuáles otros dispositivos de la organización
• **Nivel 2:** Prevenir que los usuarios puedan acceder a servicios de back-up remoto

4.5 Uso de servicios de localización

La disponibilidad de GPS en la mayoría de los dispositivos móviles permite la creación y utilización de nuevos servicios basados en la localización física del usuariio en cualquier lugar del mundo. Estos servicios se han hecho muy populares y se usan con frecuencia en coordinación con otros, tales como: redes sociales, navegación, web browsers, etc.

Sin embargo, aquellos dispositivos móviles que mantienen activos los servicios de localización suponen un riesgo adicional, toda vez que posibilitan a los atacantes determinar la posición del usuario en función de la localización de su dispositivo móvil, lo que puede afectar gravemente no sólo a la seguridad de la organización sino también a las garantías de privacidad del propio usuario, facilitando la creación de mapas geográficos de los movimientos de los usuarios y, en algunos casos, el tipo de actividad que desarrollan.

Medidas a adoptar
• **Nivel 1:** Concienciar a los usuarios para que deshabiliten los servicios de localización dentro de áreas sensibles (de hecho salvo que no sea estrictametne necesario es recomendable desactivar este servicio)
• **Nivel 2:** Prohibir el uso de estos servicios en relación con determinadas aplicaciones (redes sociales, fotografías, etc.)

4.6 Aspectos legales

Existen numerosas implicaciones legales asociadas a los entornos BYOD que deben tenerse en cuenta desde el primer momento. Así, y entre otros, cabe considerar (especialmente si no se dispone de consentimineto del usuario por escrito):

- Monitorización de los dispositivos y su tráfico de red para detectar violaciones en la política de seguridad, borrado de datos o apps personales, acceso a datos almacenados en el dispositivo móvil o en servicios "en la nube" durante las auditorías o la investigación de un incidente de seguridad.

- Monitorización de los dispositivos fuera de las dependencias de la organización, como por ejemplo mediante la utilización de mecanismos de localización del dispositivo.
- Responsabiliad a la hora de compensar, reparar o sustituir un dispositivo robado, perdido o dañado.
- Acuerdos de confidencialidad y eliminación remota de información. Según ESET más de la mitad de los trabajadores almacenan la información laboral en su dispositivo personal y una quinta parte dice elimarla una vez terminado el trabajo. Para evitar que esta información almacenada en el dispositivo pueda ser utilizada de manera inapropiada por el usuario (divulgación a terceros) se deben redactar y firmar por parte de la organización y del empleado acuerdos de confidencialidad que proporcionen herramientas para actuar en el caso de que esa información fuera expuesta. Este caso tiene su nivel crítico cuando un empleado cesa su actividad, bien por propia voluntad o por parte de la organización. En este sentido, la organización debe tener el **derecho institucional a borrar remotamente** los datos del dispositivo. Este punto tiene que quedar correctamente reflejado en la Política de Seguridad BYOD.
- Implicaciones legales de la distribución o uso de software pirata o sin licencia, así como de aquellas otras licencias cuyas condiciones requieren su instalación en dispositivos propiedad de la organización.
- Tener contemplado qué hacer en caso de término de la relación contractual.
- Responsabilidad de los usuarios, entre ellas el mantenimiento de las medidas de seguridad exigidas en cada caso, pudiendo ser desactivado automáticamente de aquellos dispositivos que no cumplan las medidas.

Se recomienda por tanto consultar al departamento legal de la organización para analizar y profundizar estos aspectos.

Para completar este apartado de amenzas y riesgos, recogemos un cuadro de la Agencia Europea de la Seguridad de la Información, ENISA, en el que se informa de los riesgos de la consumerización (concepto muy ligado al BYOD y que define la extensión al mundo empresarial de tecnologías que ya se usan ampliamente en el mercado del consumidor final).

	RIESGOS
Riesgos relacionados con los costes	Aumento del riesgo de pérdida de valor de la marca de la empresa cuando los empleados hacen un uso incontrolado de los servicios / dispositivos de consumo
	El aumento de la variedad y complejidad de los dispositivos, sistemas y aplicaciones, dará lugar a un aumento de los costes.
	Es probable que más de un dispositivo se pierda, por lo tanto el aumento de los costes es mayor al tener que reponerlo
	Gasto adicional para asegurar que los requisitos de seguridad actúan para evitar el uso inadecuado de los dispositivos
Los riesgos legales y cuestiones reglamentarias	El gobierno corporativo y el control del cumplimiento a través de dispositivos propiedad de los empleados debe ser más débil
	Interoperación, modelos de uso y cambio de contexto de seguridad de una aplicación y sistemas harán más difícil controlar el cumplimiento legal y regulatorio.
	La falta de una clara distinción entre los datos personales y corporativos en los dispositivos propiedad de los empleados hará la detección electrónica más difícil y puede dar lugar a litigios con los empleados.
Los riesgos relacionados con la gestión de datos	Posible pérdida de datos corporativos como resultado del intercambio no autorizado de información en los dispositivos de los empleados y los servicios utilizados.
	Posible pérdida de datos corporativos, como resultado del acceso de los usuarios desconocidos y dispositivos no administrados por las redes empresariales.
	La pérdida potencial de datos corporativos como resultado de la dificultad de controlar la seguridad en las aplicaciones de los dispositivos móviles, especialmente si son propiedad de los empleados.
	Aumento del riesgo en los dispositivos móviles ya que se han convertido en el blanco de ataque para la adquisición de datos corporativos.

Figura 3.1. Riesgos de la consumerización identificados por ENISA18

18 "Consumerization of IT: Risk Mitigation Strategies". ENISA (2012-12-19). La llamada consumerización es una tendencia que está estrechamente ligada a BYOD. La consumerización significa que las TIC, cada vez más, se están desarrollando sobre la base de los requisitos de los propios consumidores y de sus dispositivos (CCN-CERT IA 09/13 Ciberamenazas 2012 y Tendencias 2013)

5. MEJORES PRÁCTICAS EN LA IMPLANTACIÓN DE UN SISTEMA BYOD

Tras conocer los riesgos y oportunidades que brinda una política BYOD en una organización, y con el fin de minimizar cualquier amenaza, es necesario desarrollar su implantación en torno a una estrategia previamente definida que se incluya en la Política de Seguridad de la organización y, por tanto, sea de obligado cumplimiento para todos sus miembros. Su implantación puede realizarse bajo tres perspectivas[19]:

a) **Virtualización**: Proporcionando acceso remoto a los sistemas de información corporativos, por lo que no habrá datos o ejecución de aplicaciones en el dispositivo personal.

b) **Aislamiento**: Haciendo que los datos o las aplicaciones corporativas se encuentren dentro de un contenedor seguro (*sandbox*), aislado de los datos y aplicaciones personales de su propietario.

c) **Coexistencia controlada**: Permitiendo en el dispositivo la convivencia de datos y aplicaciones corporativas con datos personales, contemplando las políticas de seguridad adecuadas que garanticen que los controles de seguridad se mantienen en todo momento.

Una vez decidido este punto, las medidas a adoptar podrían tener las siguientes fases:

5.1 Iniciación/análisis de riesgos

Comprende la identificación de las necesidades de la organización en relación con el uso de los dispositivos personales y las necesidades de los empleados. Partir del conocimiento de los activos de informació, saber cuáles son los datos más sensibles que requieren mayores niveles de protección, a qué información se puede acceder desde dispositivos personales, a qué información se puede acceder desde fuera de la red de la empresa y a cuál otra se debe restringir el acceso. Convendría tener en cuenta diversos aspectos como:

a) Capacidad y cobertura de las redes corporativas para permitir el acceso de dispositivos diferentes a los de la empresa.

b) Tipos de dispositivos personales y análisis de cuáles son los más adecuados pare el entorno de la organización.

c) Nivel de acceso de los distintos dispositivos a los recursos corporativos (determinados por su correspondiente análisis de riesgos, que deberá hacerse por cada tipo de dispositivo).

d) Gestión de roles, siendo el acceso a la información restringido de forma que garantice que solamente podrán acceder a la información aquellas personas que realmente lo necesiten.

e) **Política de Seguridad BYOD** que incluya los siguientes factores:

19 The White House: Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs http://www.whitehouse.gov/digitalgov/bring-your-own-device

a. Sensibilidad de la información manejada.
b. Cumplimiento de la Política de Seguridad de la Organización.
c. Coste asociados (directos e indirectos).
d. Ubicación del trabajo.
e. Limitaciones técnicas.
f. Conformidad con la normativa vigente y otras regulaciones de seguridad.
g. Seguridad jurídica en caso de pérdida, robo o finalización de la relación de trabajo del empleado, requiriendo el uso de contraseñas de acceso, bloqueo de dispositivos, cifrado de información, así como el **derecho institucional** a borrar remotamente los datos corporativos del equipo.
h. Responsabilidades de los usuarios, advirtiendo de la desactivación de aquellos dispositivos que no cumplan las medidas de seguridad hardware y software.
i. Actividades permitidas (descarga o no de datos, documentos, acceso a determinadas redes, uso de USB, etc.).
j. Dispositivos permitidos.
k. Servicio de soporte corporativo.
l. Asunción de costes y mantenimiento.

Pese a la importancia capital de contar con una Política de Seguridad BYOD, diversos estudios[20] señalan que aproximadamente el 60 por ciento de las organizaciones reconoce que no tienen una política especifica sobre cómo los empleados pueden usar sus propios dispositivos en el lugar de trabajo y, lo que es más preocupante, uno de cada cuatro reconoce que hacen **excepciones para el personal directivo**, precisamente aquel que puede acceder y almacenar la información más relevante para la organización y que suele ser el principal objetivo de los ciberataques dirigidos (ciberespionaje político o industrial).

20 Instituto Ponemon (Microsoft security chronicles - august 15, 2013)

a)

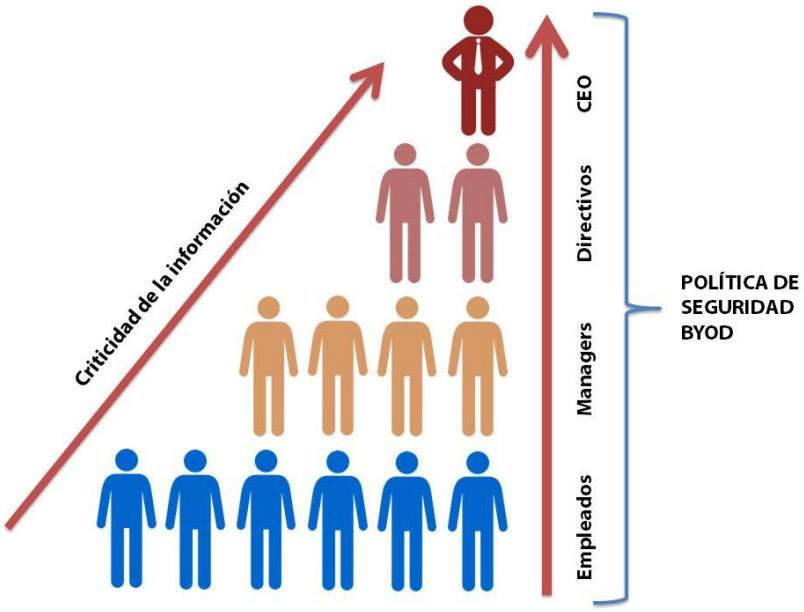

Figura 5-1. La Política de Seguridad BYOD de la organización debe implicar a todos los empleados

5.2 Desarrollo

A partir del análisis se deben establecer las medidas de control más adecuadas, que pueden ir desde dispositivos de carácter tecnológico (antivirus, DLP, VPN, Firewall, IDS, IPS, etc) hasta el establecimiento de políticas para la gestión de dispositivos que determinen cuáles pueden usarse y cuáles no. Además, se debería especificar las características técnicas de las soluciones que se requieren, incluyendo los métodos de autenticación exigibles y, en su caso, los mecanismos criptográficos usados para proteger las comunicaciones y los datos almacenados en los dispositivos.

En líneas generales convendría mantener las siguientes consideraciones de seguridad:

a) Arquitectura
b) Autenticación
c) Criptografía
d) Requerimientos de configuración y certificaciones
e) Aprovisionamiento de dispositivos

5.3 Implantación

Se configurará la tecnología (servidores y equipos) para alcanzar los objetivos y los requisitos de seguridad fijados con anterioridad. Comprenderá, entre otros, el análisis de los siguientes extremos:

a) Conectividad.
b) Protección de la información.
c) Autenticación.
d) Aplicacionese.
e) Gestión por parte de los administradores del sistema.
f) Loggin.
g) Rendimiento.
h) Seguridad de la implantación.
i) Configuración predeterminada.

5.4 Operación y Mantenimiento

Tareas que la organización debe desarrollar de forma continuada, para garantizar que la solución se mantiene en todo momento operativa y conforme con los niveles de seguridad exigidos.

Entre los procedimientos operativos y de mantenimiento más usuales se encuentran:

a) Verificación del estado de actualización y parcheado de los dispositivos.
b) Verificación de una adecuada sincronización entre los componentes de la infraestructura.
c) Configuración de control de accesos en función de los cambios y auditorías.
d) Monitorización de la red de dispositivos.
e) Mantenimiento de un inventario.
f) Formación y concienciación a los usuarios.
g) Verificación periódica de las políticas de seguridad.

5.5 Retirada

Tareas que deben acometerse cuando una solución de tecnología móvil o cualquiera de sus componentes se retira de la organización, incluyendo los requisitos legales de conservación de datos, limpieza de soportes y medios y retirada efectiva de equipamientos.

6. SOLUCIONES MDM (*MOBILE DEVICE MANAGEMENT*)

Una vez aprobado el uso del BYOD, las organizaciones pueden hacer uso de las soluciones tecnológicas que permitan la gestión de los dispositivos móviles a nivel corporativo. Una de estas soluciones se conoce como MDM, de sus siglas en inglés, *Mobile Device Management*. Este sistema permite gestionar de forma eficiente la diversidad y el despliegue masivo, dinámico y a gran escala de dispositivos móviles en una organización, con un enfoque principalmente orientado a incrementar su

seguridad, y mejorando colateralmente la productividad del usuario final. La posibilidad de gestionar diferentes tipos de dispositivos y marcas, facilita el uso de dispositivos propiedad de los usuarios como instrumentos de acceso a recursos corporativos.

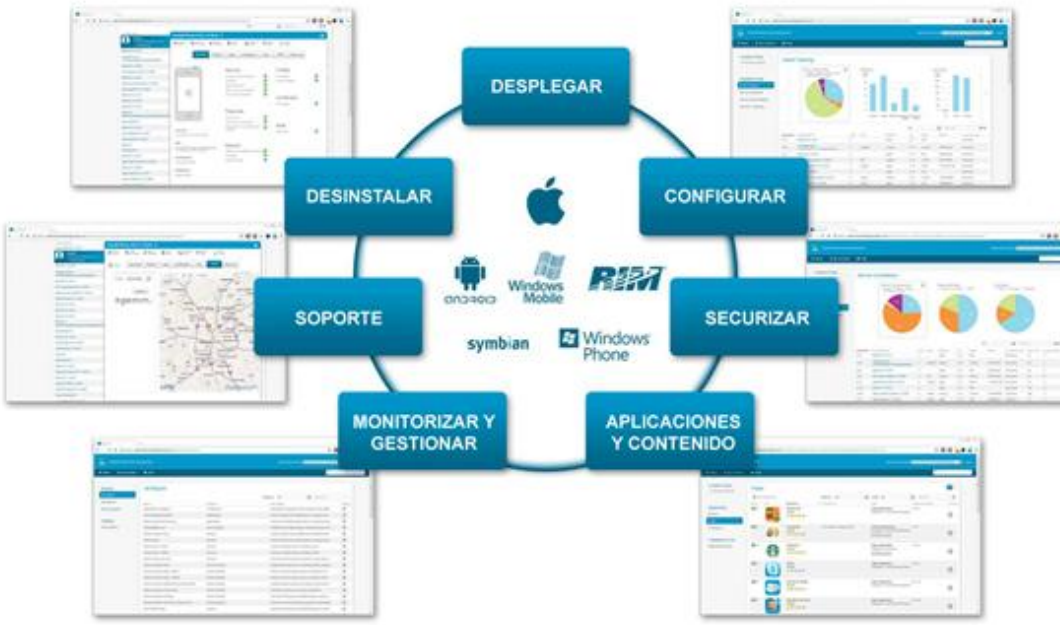

Figura 6-1. Las herramientas de gestión de dispositivos móviles MDM están orientadas a incrementar la seguridad

Cada uno de los fabricantes de las principales plataformas móviles proporciona sus propias soluciones de gestión empresarial de los dispositivos, centradas principalmente o únicamente en su plataforma móvil[21].

En general contemplan cuatro componentes:

a) servidor centralizado (que envía las órdenes de gestión a los dispositivos móviles).

b) software-cliente instalado en cada dispositivo móvil (que recibe y ejecuta tales órdenes).

c) base de datos centralizada (que contiene el estado de situación de cada uno de los dispositivos móviles del ámbito de la solución MDM).

d) modelo de comunicación entre el servidor centralizado y cada uno de los dispositivos móviles, denominado OTA (Over-the-air programming), capaz de configurar remotamente un dispositivo concreto, un conjunto determinado de ellos, o la totalidad del parque de dispositivos móviles de su ámbito de gestión, incluyendo actualizaciones de software y sistemas

[21] Véase Guía CCN-STIC 457. Pág. 22 Soluciones MDM en la Industria

operativos, bloqueo y borrado remoto de los dispositivos, análisis remoto, etc. En la actualidad, las soluciones MDM se ofrecen en base a la adquisición de licencias o mediante servicios cloud (Sofware as a Service).

Dentro de los tipos de soluciones MDM es importante diferenciar dos grandes grupos:

- Aquellas que se basan en la **gestión completa de la plataforma o dispositivo móvil** en base a las capacidades proporcionadas por cada uno de los fabricantes, y que se basan en la gestión de los datos, aplicaciones y servicios corporativos.
- **De tipo contenedor** (o container en inglés), una aproximación a la gestión de dispositivos móviles que considera la plataforma móvil como un entorno inseguro y que proporciona una app segura para llevar a cabo todas las actividades y tareas corporativas. En lugar de gestionar la plataforma móvil completa y todas sus apps, la gestión se centra en una única app, que es la que tiene acceso a los datos y servicios corporativos.

  Esta es la solución por la que se ha venido decantando la mayor parte de la industria ya que toda la gestión corporativa afecta únicamente a la app contenedora y es más sencilla su implantación (y eliminación) en los dispositivos móviles personales de los usuarios, y permite establecer una separación entre datos personales y corporativos.

CONCLUSIONES

Ante la consolidación de facto de un fenómeno como el BYOD (incluso aunque no haya un Política de Seguridad al respecto en la organización), resulta apremiante plantearse su implantación, partiendo de un análisis de riesgos pormenorizado que permita identificar los activos a proteger o evaluar, así como las ventajas y los riesgos que conlleva este tipo de entornos.

Figura 7-1. Recomendaciones de BT Business a la hora de implantar una política BYOD

La gestión de los dispositivos, el acceso a la información y a las diferentes tareas, las buenas prácticas, la racionalización de los recusos móviles, la seguridad de los datos y la administración de redes, todo esto son cuestiones que hay que contemplar, buscando siempre el equilibrio entre adaptabilidad y seguridad.

La mayor productividad y satisfacción de los empleados y la reducción de costes que puede llevar aparejado el BYOD, no puede hacer olvidar los riesgos en la seguridad y la privacidad de la información corporativa, la necesidad de soporte TI para una diversidad de dispositivos, aplicaciones y software y, sobre todo, el incremento del riesgo de sufrir ciberataques. Al fin y al cabo, con el BYOD las organizaciones multiplican las puertas de acceso y no siempre con las exigencias de seguridad adecuadas.

Será necesario, por tanto, desarrollar una **Política de Seguridad BYOD**, que tenga en cuanta y conecte las aplicaciones, recursos y usuarios, idependientemente del dispositivo y del lugar desde el que se acceda, con el máximo de garantías, fiabilidad y transparencia. Del mismo modo, se tendrá que proporcionar a los empleados acceso seguro, autenticación y gestión sencillas y consistentes políticas corporativas de movilidad. Todo ello acompañado de un adecuado **plan de divulgación y sensibilización** para que todos los niveles de la organización (incluidos los altos directivos) conozcan las restricciones de sus dispositivos y de acceso a la información.

Por último, se requerirá una mayor periodicidad de los análisis de riesgos y vulnerabilidades para determinar el estado de la organización ante esta tendencia, ya que la aparición de nuevos dispositivos o aplicaciones pueden afectar en gran medida la seguridad de las organizaciones.

ANEXO REFERENCIAS

[Ref – 1]	**CCN-STIC** Guía CCN-STIC-457: Herramientas de gestión de dispositivos móviles: MDM Agosto 2013
[Ref – 2]	**CCN-STIC** Guía CCN-STIC-450: Seguridad de dispositivos móviles Marzo 2013
[Ref – 3]	**CCN-STIC** Guía CCN-STIC-404: Control de soportes informáticos Diciembre 2006
[Ref – 4]	**CCN-STIC** Guía CCN-STIC-401: Glosario y abreviaturas Septiembre 2013
[Ref – 5]	**CCN-CERT** Abril 2013 CCN-CERT IA-09/13 Ciberamenazas 2012 y Tendencias 2013
[Ref – 6]	**ENISA** Consumeraitation of IT: Top Risk And Opportunities Septiembre 2012 http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/consumerization-of-it-top-risks-and-opportunities/at_download/fullReport
[Ref – 7]	**ESET** Retos de Seguridad para las empresas a partir del BYOD Octubre 2012 http://www.eset-la.com/pdf/prensa/informe/seguridad_en_byod.pdf
[Ref – 8]	**The White house** A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs. Agosto 2012 http://www.whitehouse.gov/digitalgov/bring-your-own-device
[Ref – 9]	**Magic Software** BYOD: An Opportunity for IT to Drive the New Age Enterprise Febrero 2012
[Ref – 10]	**IXOTYPE** "BYOD en España" Infografía de fuentes: Cisco Systems, ZD NET, Gartner, VMwareel, Informe Ovum 2012, ComScore,CheckPoint http://www.ixotype.com/media/byod_infografia_ixotype..jpg
[Ref – 11]	**Microsoft** Security Chronicles Agosto 2013
[Ref – 12]	**BT Business/Cisco** Is your business ready to embrace the BYOD revolution)

	2013
[Ref – 13]	**Symantec** 2013 Norton Report Octubre 2013 Go.symantec.com/norton-report-2013