UNIVERSIDAD POLITÉCNICA DE VALENCIA

ESCUELA TÉCNICA SUPERIOR

DE INGENIEROS DE TELECOMUNICACIÓN

PROYECTO FIN DE CARRERA

Estudio sobre la implantación de las políticas de BYOD para el uso de dispositivos móviles personales en las comunicaciones de empresa

AUTOR: Olvido Nicolás Melero

TUTOR: D. Luis Castejón Martín

AÑO: 2014

Resumen del proyecto

Desde hace algunos años estamos viviendo un fenómeno poco habitual en el entorno tecnológico. La tecnología más avanzada ya no está en las empresas, sino que es propiedad de los empleados. En casa tenemos el último ordenador, el último móvil, la conexión de mayor ancho de banda, más gigas de almacenamiento, correo ilimitado, videoconferencia, etc. Pero en el trabajo, en muchos casos, tenemos la sensación de que volvemos al pasado en lo que a tecnología se refiere. Este fenómeno es lo que se ha llamado **"consumerización" de las TIC**. Según Gartner, la consumerización de la TI será la tendencia más significativa que afectará a las TIC durante los próximos diez años (1).

Poco a poco, esta corriente se ha ido trasladando a las empresas y organizaciones. Sus empleados quieren utilizar en su entorno laboral aquellas tecnologías (dispositivos, aplicaciones y servicios) que están usando en su entorno personal y con las que dicen poder ser más productivos. Esto ha dado lugar a diferentes tendencias en el entorno empresarial. La más importantes, el **BYOD ("*Bring Your Own Device*")** o "use su propio dispositivo", hace referencia al uso de dispositivos personales (smartphones, tabletas, portátiles, discos USB) en el trabajo.

El fenómeno BYOD, es cada vez más común en la mayoría de las geografías a nivel mundial. Para las organizaciones, es una puerta de entrada para potenciales mejoras en la satisfacción y compromiso de los empleados, incremento de la productividad y desarrollo de la innovación, habilitando nuevos negocios o innovando en los procesos de negocios existentes.

Sin embargo, no todo son ventajas. El BYOD también las expone a riesgos vinculados a la seguridad de los datos corporativos, y el control y gestión del programa supone un verdadero reto para los departamentos de TI. Otras implicaciones del BYOD, que pocas organizaciones llegan a plantearse, son las legales, de cumplimiento de normativas y de regulación, especialmente en lo referente a la privacidad. Por ello, la actitud de las empresas ante el BYOD varía mucho, yendo desde la prohibición total al fomento proactivo de este tipo de programas, pasando por el "dejar hacer".

Este documento pretende mostrar que el BYOD no es una moda pasajera. Es una tendencia estratégica en tecnología (19), y los departamentos de TI no pueden permitirse ignorarla. Se ofrece una visión global de las implicaciones del BYOD, haciendo hincapié en que un programa BYOD es más un proyecto de gestión del cambio que un proyecto de tecnología.

Así mismo, se pretende concienciar sobre los peligros de ignorar el BYOD. Se pone de manifiesto la necesidad de definir una Estrategia Global de Movilidad y BYOD que permita a los usuarios ser productivos, sin poner en peligro la información ni la infraestructura corporativa, y sin cruzar líneas legales. De esta forma los beneficios derivados de los programas de movilidad no se verán enturbiados con incidentes de seguridad que impacten negativamente en la organización (a nivel económico, legal o reputacional).

Palabras clave

BYOD, "*Bring Your Own Device*", BYOA, BYOT, Política, Movilidad, Dispositivo, Móvil, Smartphone, Tableta, MDM, EMM, Seguridad, Privacidad, Virtualización, Riesgos de la Información.

Índice de contenidos

Índice de ilustraciones

Glosario

A	
Actitud *"always-on"*, *20*	Actitud de estar conectado a Internet permanentemente.
Actitud hacia el riesgo, *53*	*Risk apetite* en inglés. En gestión de riesgos, es el nivel de riesgo que una organización está preparada para aceptar.
Activos, *53*	El objetivo de la protección en un análisis de seguridad.
Adware, *34*	Un programa de clase adware es cualquier programa que automáticamente muestra publicidad web al usuario durante su instalación o durante su uso para generar lucro a sus autores.
Antiphishing, protección, *57*	Protección frente a técnicas de *phishing* o suplantación de identidad, tipo de abuso informático que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información sobre tarjetas de crédito u otra información bancaria).
API, *Application Programming Interface*, *65*	Interfaz de programación de aplicaciones. Es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.
Apk, fichero o extensión, *65*	Un archivo con extensión .apk (Application PacKage File) es un paquete para el sistema operativo Android. Este formato es una variante del formato JAR de Java y se usa para distribuir e instalar componentes empaquetados para la plataforma Android para smartphones y tabletas.
App, *42*	Aplicación específica para dispositivo móvil.
App Store, *42*	(Application store). Portal online a través del cual programas software están disponibles para su adquisición y descarga. Los principales fabricantes de sistemas operativos móviles, como Apple, Google, BlackBerry y Microsoft, disponen de su propio app store, aunque también hay app stores de terceros, como el Amazon Appstore para Android o Cydia para dispositivos Apple iOS liberados. Un concepto relacionado es el de app store corporativo, un portal controlado por el área de TI que pone a disposición de los usuarios aplicaciones concretas de negocio que han sido previamente aprobadas.
App wrapping, *67*	Proceso de agregar una capa de gestión a una app móvil sin realizar ningún cambio a la app subyacente. El app wrapping permite establecer determinados elementos de una política sobre una app o grupos de apps
Ataque de fuerza bruta, *58*	En criptografía, se denomina a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.
Autenticación, *56*	Técnica que utiliza un sistema o red para verificar la identidad de alguien que pide acceso.
Autenticación multifactor, *56*	Forma de autenticación que implica dos o más tipos de factores de autenticación, normalmente una combinación de algo que el usuario sabe, algo que el usuario tiene y algo que el usuario es.
B	
BYOA ("*Bring Your Own App*"), *12*	"Use su propia aplicación", tendencia de los usuarios a usar también en el trabajo aplicaciones móviles de consumo que usan habitualmente en su ámbito personal.
BYOC ("*Bring Your Own Cloud*"), *12*	"Use su propia nube", tendencia en la que los empleados acceden a servicios cloud de consumo (como Dropbox, SkyDrive, etc.) a través de la red corporativa.

BYOC (“*Bring Your Own Computer*”), 12	"Trae tu propio ordenador", política empresarial donde los empleados llevan sus propios ordenadores a su lugar de trabajo para tener acceso a recursos de la empresa.
BYOD (“*Bring Your Own Device*”), *12*	"Trae tu propio dispositivo", política empresarial donde los empleados llevan sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa.
BYOL (“*Bring Your Own Laptop*”), *12*	"Trae tu propio portátil", política empresarial donde los empleados llevan sus propios portátiles a su lugar de trabajo para tener acceso a recursos de la empresa.
BYON (“*Bring Your Own Network*”), *12*	“Use su propia red”, hace referencia a la habilidad de los usuarios de crear o acceder a redes alternativas cuando las opciones disponibles no son satisfactorias para sus propósitos.
BYOPC (“*Bring Your Own PC*”), *12*	"Trae tu propio ordenador", política empresarial donde los empleados llevan sus propios ordenadores a su lugar de trabajo para tener acceso a recursos de la empresa.
BYOT (“*Bring Your Own Technology*”), *12*	"Trae tu propia tecnología", expresa un fenómeno mucho más amplio que el BYOD ya que no sólo cubre al equipo sino que también cubre al software y los servicios.
C	
Cloud computing, *11*	La computación en la nube, o también llamada servicios en la nube, informática en la nube, nube de cómputo o nube de conceptos, es un paradigma que permite ofrecer servicios de computación a través de Internet.
COBIT, *11*	Marco de referencia para el desarrollo, implementación, monitorización y mejora de la gobernanza y prácticas de gestión de la tecnología de la información, publicado por el IT Governance Institute y la Information Systems Audit and Control Association (ISACA).
COBIT 5 for Information Security, *62*	Marco de referencia publicado por el IT Governance Institute y la Information Systems Audit and Control Association (ISACA) a fin de proporcionar una guía práctica en la seguridad de la empresa, en todos sus niveles prácticos
Confidencialidad, *53*	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso (ISO 17799).
Consumerización de las TIC, *11*	Tendencia creciente en la cual las nuevas tecnologías de la información surgen primero en el mercado del consumidor y luego se propagan hacia las organizaciones comerciales y gubernamentales.
COPE (*Corporate-Owned, Personally-Enabled*), *77*	Modelo a través del cual una organización proporciona dispositivos móviles a sus empleados y permite que los use como si fueran personales.
Crimeware, *34*	Tipo de software que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos en línea. El crimeware (que debe ser diferenciado del spyware, adware) ha sido diseñado, mediante técnicas de ingeniería social u otras técnicas genéricas de fraude en línea, con el fin de conseguir el robo de identidades para acceder a los datos de usuario de las cuentas en línea, con el objetivo de obtener fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo.
CYOD (Choose Your Own Device), *77*	Modelo que limita el tipo de hardware que los empleados pueden usar. Puede ser proporcionado por la empresa o propiedad del empleado, o una mezcla de ambos.
D	
DaaS , *Desktop as a Service*, *45*	Servicio cloud en la que el back-end de una infraestructura de escritorio virtual (VDI) está alojada en un proveedor de servicios cloud.

Dirección MAC del dispositivo, *59*	En las redes de computadoras, la dirección MAC (siglas en inglés de *Media Access Control*, "control de acceso al medio"), o dirección física, es un identificador de 48 bits que corresponde de forma única a un dispositivo de red.
Dispositivo MiFi, *12*	MiFi o WiFi móvil es un router móvil (3G o posterior) que actúa como hotspot WiFi móvil. MiFi hace referencia a 'Mi Wi-Fi'. MiFi se puede conectar a un teléfono móvil o módem USB 3G (o posterior). MiFi trabaja a una distancia de hasta 10 m y proporciona internet o acceso a red a cualquier dispositivo habilitado para WiFi.
DLP, *Data Loss Prevention*, *6*	Prevención de Fuga de Datos. Término de seguridad informática que se refiere a los sistemas que identifican, supervisan y protegen los datos en uso, los datos en movimiento y los datos estáticos a través de inspecciones de contenido, análisis del contexto de seguridad de la transacción y con un marco de gestión centralizada. Los sistemas DLP están diseñados para detectar y prevenir el uso no autorizado y la transmisión de información confidencial.
Dropbox, *12*	Servicio de alojamiento de archivos multiplataforma en la nube, operado por la compañía Dropbox.
E	
EAP-TLS (*Extensible Authentication Protocol Transport Layer Security*), *59*	Estándar abierto del Internet Engineering Task Force (IETF) que utiliza el protocolo *Transport Layer Security* (TLS). Es el protocolo original y standard de autenticación en redes LAN wireless y está ampliamente soportado entre fabricantes wireless.
EMM, *Enterprise Mobility Management*, *64*	Sistema global de gestión de la movilidad corporativa que implica una combinación de funcionalidades de gestión de dispositivos, de aplicaciones y de la información.
F	
Fingerprinting, *59*	Técnica que utilizan algunos productos DLP (Data Loss Prevention) para "marcar" datos. La técnica implica el uso de criptografía para generar hashes para elementos de información sensible.
Firewalls, de red y host-based, *57*	Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Es un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Hay dos tipos principales: firewalls de red (protegen el perímetro de una red) y firewalls host-based (o firewalls personales, protegen un dispositivo individual independientemente de la red a la que esté conectado).
H	
Hack, *34*	Modificación de un programa o máquina para un uso beneficioso o perjudicial.
Hash, *59*	También, funciones de resumen. Algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).
Hotspot, *12*	Zona de acceso inalámbrico a internet
I	
ITIL (*Information Technology Infrastructure Library*), *62*	La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL, es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

ITSM (*IT Service Management*), *62*	La gestión de servicios de tecnologías de la información es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final. ITSM propone cambiar el paradigma de gestión de TI, por una colección de componentes enfocados en servicios de extremo a extremo usando distintos marcos de trabajo con las "mejores prácticas", como por ejemplo la *Information Technology Infraestructure Library* (ITIL) o el eSCM (*Enabled Service Capability Model*).
L	
Lista blanca de aplicaciones, *67*	También lista de aprobación o *whitelist* en inglés. Lista o registro de entidades que, por una razón u otra, pueden obtener algún privilegio particular, servicio, movilidad, acceso o reconocimiento. Por el contrario la lista negra o *blacklisting* es la compilación que identifica a quienes serán denegados, no reconocidos u obstaculizados.
Lista negra de aplicaciones, *67*	También *blacklisting* en inglés. Lista o registro que identifica a quienes, por una razón u otra, serán denegados, no reconocidos u obstaculizados en la obtención de acceso a algún privilegio, servicio, movilidad, o reconocimiento.
M	
Malware, *34*	(Del inglés *malicious software*). También *badware*, código maligno, software malicioso o software malintencionado. Tipo de software que tiene como objetivo infiltrarse o dañar un dispositivo o sistema de información sin el consentimiento de su propietario. El término malware es utilizado para referirse a una variedad de software hostil, intrusivo o molesto. Incluye virus, gusanos, troyanos, la mayor parte de los rootkits, *scareware*, *spyware*, *adware* intrusivo, *crimeware* y otros softwares maliciosos e indeseables. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos. Malware no es lo mismo que software defectuoso; este último contiene bugs peligrosos, pero no de forma intencionada.
MAM (*Mobile Application Management*), *64*	Herramienta utilizada para la instalación, actualización, eliminación, auditoria y monitorización de programas software en smartphones y tabletas de forma remota.
MIM (*Mobile Information Management*), *64*	Sistema independiente del dispositivo para la gestión de la información en dispositivos móviles.
MDM (*Mobile Device Management*), *22*	Tipo de herramienta software que permite asegurar, monitorizar y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios. La mayoría de las MDM permiten hacer instalación de aplicaciones, localización y rastreo de equipos, sincronización de archivos, reportes de datos y acceso a dispositivos, entre otras funcionalidades, todo esto de manera remota y centralizada.
Movilidad Empresarial o Movilidad Corporativa, *18*	Libertad para comunicarse a cualquier hora y en cualquier lugar. Este es el principal concepto de movilidad. Dentro de una empresa, este concepto va más allá: es la oportunidad de generar nuevos negocios y estar en contacto con los clientes y partners en todo momento.
N	
NAC, *Network Access Control, 39*	Control de acceso a la red, también llamado control de admisión a la red. Método de reforzar la seguridad de una red propietaria restringiendo la disponibilidad de los recursos de red a dispositivos de acceso que cumplen con una política de seguridad definida.
P	
PAN, *Personal Area Network, 12*	Red de área personal para la comunicación entre distintos dispositivos (tanto ordenadores, puntos de acceso a internet, teléfonos móviles, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal.

PEAP (*Protected Extensible Authentication Protocol*), *59*	Version del protocolo de autenticación EAP usado en redes wireless y conexiones punto-a-punto. PEAP está diseñado para proporcionar una autenticación más segura en redes WLAN 802.11 que soportan control de acceso a puertos 802.1X.
Perfil de riesgo, 52	Análisis cuantitativo de los tipos de amenazas a las que se enfrenta una organización, un activo, un proyecto o un individuo.
Phablet, 14	Tabléfono o tabletófono son alternativas en español del término *Phablet* (del inglés: contracción de *phone* y *tablet*) o fableta, denominaciones informales utilizadas para designar dispositivos electrónicos móviles o portátiles, con pantallas táctiles entre 5 y 7 pulgadas aproximadamente, que combinan las funcionalidades y capacidades de un teléfono inteligente con una tableta.
Plugin, *65*	(Complemento). Aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la API. También se conoce como plug-in, add-on (añadido), conector o extensión.
Política BYOD, *40*	Una política BYOD es un conjunto de reglas que, aunque son específicas para cada organización, a nivel más básico, gobiernan el nivel de soporte del departamento de TI a los dispositivos propiedad del empleado, definen qué dispositivos están aceptados, si la empresa subvenciona de algún modo el dispositivo o los gastos asociados al mismo, cómo deben proteger los dispositivos los usuarios. La política BYOD forma parte de la política de Movilidad Empresarial definida en la organización, junto las políticas de Uso Aceptado.
R	
Red ad-hoc inalámbrica, *12*	Tipo de red inalámbrica descentralizada. La red es ad-hoc porque no depende de una infraestructura pre-existente, como routers (en redes cableadas) o de puntos de accesos en redes inalámbricas administradas. En lugar de ello, cada nodo participa en el encaminamiento mediante el reenvío de datos hacia otros nodos, de modo que la determinación de estos nodos hacia la información se hace dinámicamente sobre la base de conectividad de la red.
Resiliencia del negocio, *53*	Empresas resilientes son aquellas capaces de absorber cambios y rupturas, tanto internos como externos, sin que por ello se vea afectada su rentabilidad y que incluso desarrollan una flexibilidad tal que, a través de procesos de rápida adaptación, logran obtener beneficios extras, sean éstos pecuniarios o intangibles, derivados de circunstancias adversas y/o imprevistas.
Rootkit, *34*	Programa que permite un acceso de privilegio continuo a un dispositivo pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones. La detección del rootkit es dificultosa pues es capaz de corromper al programa que debería detectarlo.
S	
SaaS, *Software as a Service, 49*	Software como Servicio. Modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación, a los que se accede con un navegador web desde un cliente, a través de Internet.
Sandboxing, 65	En seguridad informática, el aislamiento de procesos es un mecanismo para ejecutar programas con seguridad y de manera separada. A menudo se utiliza para ejecutar código nuevo, o software de dudosa confiabilidad proveniente de terceros. Ese aislamiento permite controlar de cerca los recursos proporcionados a los programas "cliente" a ejecutarse, tales como espacio temporal en discos y memoria. Habitualmente se restringen las capacidades de acceso a redes, la habilidad de inspeccionar la máquina anfitrión y dispositivos de entrada entre otros.
Scareware, 34	El scareware (del inglés scare, «miedo» y software) abarca varias clases de software para estafar con cargas maliciosas, o con limitados o ningún beneficio, que son vendidos a los consumidores vía ciertas prácticas no éticas de comercialización.

SDK, *Software Development Kit, 65*	Kit de desarrollo de software. Conjunto de herramientas de desarrollo de software que le permite al programador crear aplicaciones para un sistema concreto.
SkyDrive, *12*	SkyDrive (oficialmente Microsoft SkyDrive) es un servicio de alojamiento de archivos en la nube que también permite a los usuarios cargar, crear, editar y compartir documentos de Microsoft Office directamente dentro de un navegador web. Incluye versiones de Microsoft Word, Excel, PowerPoint, y OneNote, y proporciona funcionalidades para que los usuarios puedan colaborar en los documentos almacenados en SkyDrive.
SLA, *Service Level Agreement, 62*	Acuerdo de nivel de servicio (ANS). Contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.
Smartphone, *11*	Teléfono inteligente. Teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar datos y realizar actividades semejantes a una minicomputadora y conectividad que un teléfono móvil convencional.
Spyware, 34	Programa espía. Software que recopila información de un ordenador o dispositivo móvil y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del dispositivo. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono. A diferencia de los virus, el spyware no se intenta replicar en otros ordenadores, por lo que funciona como un parásito.
SSL *(Secure Sockets Layer)*, protocolo 60	Protocolo que proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.
T	
Tendencias estratégicas en tecnología, *35*	En este proyecto se ha adoptado la definición de Gartner, que considera una tecnología estratégica, aquella que potencialmente puede tener un impacto significativo en la empresa durante los próximos tres años. Entre los factores que representan un impacto significativo están la posibilidad de generar disrupción en el área de TI o en el negocio, la necesidad de una inversión económica considerable o los riesgos asociados a la adopción tardía de la tecnología.
Token criptográfico, *59*	Un token de seguridad (también token de autenticación o token criptográfico) es un dispositivo electrónico o elemento software, que almacena información criptográfica y permite realizar funciones criptográficas.
TLS *(Transport Layer Security)*, protocol, *60*	Protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet.
V	
Virtualización del desktop, *40*	La virtualización de escritorio es un término que describe el proceso de separación entre el escritorio, que engloba los datos y programas que utilizan los usuarios para trabajar, y la máquina física. El escritorio "virtualizado" es almacenado remotamente en un servidor central en lugar de en el disco duro del ordenador personal. Esto significa que cuando los usuarios trabajan en su escritorio desde su ordenador personal, todos sus programas, aplicaciones, procesos y datos se almacenan y ejecutan centralmente, permitiendo a los usuarios acceder remotamente a sus escritorios desde cualquier dispositivo capaz de conectarse remotamente al escritorio, como un portátil, smartphone o cliente ligero.
VPC, *Virtual Private Cloud*	Nube privada virtual. Es la división lógica de la red pública de un proveedor de servicio para soportar cloud computing privado en un entorno de cloud público. Al

	igual que una VPN, proporciona transferencia segura de datos entre una organización y un proveedor de cloud pública, asegurando que los datos de cada cliente permanecen aislados unos de otros, tanto durante la transferencia como en la red del proveedor.
VPN, *Virtual Private Network, 3*	Red privada virtual. Tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.
Vulnerabilidad, *34*	Cualquier circunstancia o evento que puede repercutir de manera negativa sobre un activo mediante el acceso no autorizado, la destrucción, la divulgación, la modificación de los datos y/o la denegación de servicio.
W	
Wearable technology, *42*	Computadoras Corporales. Dispositivos electrónicos en miniatura que son usados por el portador debajo, junto o por encima de la ropa.
Wi-Fi Protected Access 2 (WPA2), protocolo, *58*	Sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA. WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.
WIDPS (*Wireless Intrusion Detection and Prevention Systems*), *58*	Sistema de sensores que monitorizan las comunicaciones de red wireless a su alcance y las analiza buscando señales de ataques, violaciones de políticas u otros problemas.
Wired Equivalent Privacy (WEP), *59*	Sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits o de 128 bits. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada. A partir de 2001, analistas criptográficos identificaron varias debilidades serias. Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos.

(2) (3)

Módulo 1: Análisis de la Tendencia *Bring Your Own Device* (BYOD)

1. Contexto

Consumerización de las TIC

Desde hace algunos años estamos viviendo un fenómeno poco habitual en el entorno tecnológico. La tecnología más avanzada ya no está en las empresas, sino que es propiedad de los empleados. En casa tenemos el último ordenador, el último móvil, la conexión de mayor ancho de banda, más gigas de almacenamiento, correo ilimitado, videoconferencia, mensajería instantánea, etc. Pero cuando llegamos a la oficina, en muchos casos, tenemos la sensación de que damos un paso atrás y volvemos al pasado en lo que a tecnología se refiere. Este fenómeno es lo que se ha llamado **"consumerización" de las TIC**. Según Gartner, la consumerización de las TIC será la tendencia más significativa que afectará a las Tecnologías de la Información y Comunicación (TIC) durante los próximos diez años (1).

Según algunos autores (4), la consumerización es resultado del rápido desarrollo de cuatro tecnologías:

- la introducción de los smartphones,
- el desarrollo de Internet como la plataforma ideal de distribución de medios multimedia gracias a YouTube,
- el cloud computing, que nos permite acceder desde cualquier lugar y cualquier dispositivo a cualquier servicio, recurso, o dato que haya en la red,
- las redes sociales. El gran impacto de Facebook, Twitter, etc. ha hecho que la red haya pasado de ser un sitio donde leer a convertirse en un lugar donde expresarse y compartir.

Poco a poco, esta corriente se ha ido trasladando a las empresas y organizaciones. Los empleados quieren utilizar en su entorno laboral aquellas tecnologías (dispositivos, servicios y aplicaciones) que están usando en su entorno personal y con las que dicen poder ser más productivos.

BYO ¿Use su propio qué?

La consumerización de las TIC ha dado lugar a diferentes tendencias en el entorno empresarial que están estrechamente relacionadas entre sí, y que normalmente son conocidas por sus siglas en inglés. Aunque la más conocida es el BYOD, éste antes o después acaba introduciendo a las demás a la empresa (5):

- BYOD ("*Bring Your Own Device*"): "use su propio dispositivo", hace referencia al uso de dispositivos personales (smartphones, tabletas, portátiles, discos USB) en el trabajo. Generalmente la denominación BYOD se usa para referirse sobre todo a tabletas y smartphones, y cuando se habla de portátiles se emplea la denominación BYOPC ("*Bring Your Own PC*"), BYOC ("*Bring Your Own Computer*") o BYOL ("*Bring Your Own Laptop*"). En este proyecto se usará la denominación BYOD para referirse sólo a smartphones y tabletas.
- BYOA ("*Bring Your Own App*"): "use su propia aplicación", es la tendencia de los usuarios a usar también en el trabajo aplicaciones móviles de consumo que usan habitualmente en su ámbito personal.
- BYOC ("*Bring Your Own Cloud*"): "use su propia nube", similar a la anterior pero referida a los servicios cloud (Dropbox, SkyDrive, etc.). Los usuarios acceden a estos servicios y aplicaciones a través de la red corporativa, y almacenan información corporativa, que puede ser sensible, en estos servicios cloud de consumo, que normalmente no ofrecen las mismas

medidas de seguridad que los servicios orientados a uso empresarial. Esto puede originar fugas de información y, en cualquier caso, aunque no se produzca ningún incidente de seguridad, la empresa deja de tener el control de dónde están replicados y almacenados los datos sensibles, lo que puede llevar al incumplimiento de normativas de privacidad.

- BYON ("*Bring Your Own Network*"): "use su propia red", hace referencia a la habilidad de los usuarios de crear o acceder a redes alternativas cuando las opciones disponibles no son satisfactorias para sus propósitos. En la empresa, se refiere en concreto a la capacidad de los usuarios de crear redes de área personal (PANs, *Personal Area Networks*) o redes ad-hoc como alternativa a la red corporativa. Los usuarios crean puntos de acceso wireless (hotspots) usando su dispositivo móvil como modem para dar acceso a Internet a otros dispositivos a los que se conectan vía Bluetooth o cable USB. Los empleados pueden crear también hotspots utilizando dispositivos MiFi (dispositivos portátiles de banda ancha que permiten compartir conexión 3G o 4G a múltiples usuarios o dispositivos. En algunas organizaciones los empleados utilizan el BYON para acceder a redes sociales, webs de comercio electrónico, juego online, etc. que los administradores de la red corporativa han bloqueado. Los problemas surgen porque, una vez que se ha creado la red ad-hoc (sin ningún tipo de seguridad ni monitorización) los empleados usan esa misma conexión para acceder a aplicaciones corporativas. Esto puede causar fuga de información sensible o entrada de malware a la red corporativa.
- BYOT ("*Bring Your Own Technology*"): "use su propia tecnología", podemos decir que incluiría a todos los anteriores.

La revolución de la movilidad

Se considera que el momento en el que el fenómeno BYOD apareció fue con la llegada del iPhone de Apple en 2007. Supuso toda una revolución en el ámbito de la tecnología de consumo. Los altos ejecutivos, condenados desde hacía años a terminales serios y funcionales como la BlackBerry, se encontraban con un dispositivo ligero, táctil y divertido, y quisieron llevárselo a la oficina.

Desde esos momentos, la revolución de la movilidad no ha parado. Hemos observado la proliferación de smartphones y tabletas con funcionalidades avanzadas en el entorno personal de los trabajadores. Según un estudio de ABI Research (6), a finales de 2013 habrá 1,4 miles de millones de smartphones en el mundo. Teniendo en cuenta que la población mundial es de unos 7 mil millones, eso quiere decir que habrá un smartphone por cada 5 personas en el mundo.

Esta democratización de la tecnología móvil, ha ido alimentando el fenómeno BYOD y extendiéndolo a todos los niveles en la empresa.

Como podemos ver en la Figura 1, a día de hoy los PCs son ya una parte muy pequeña de los dispositivos conectados a Internet, los smartphones y tabletas representan un 60%.

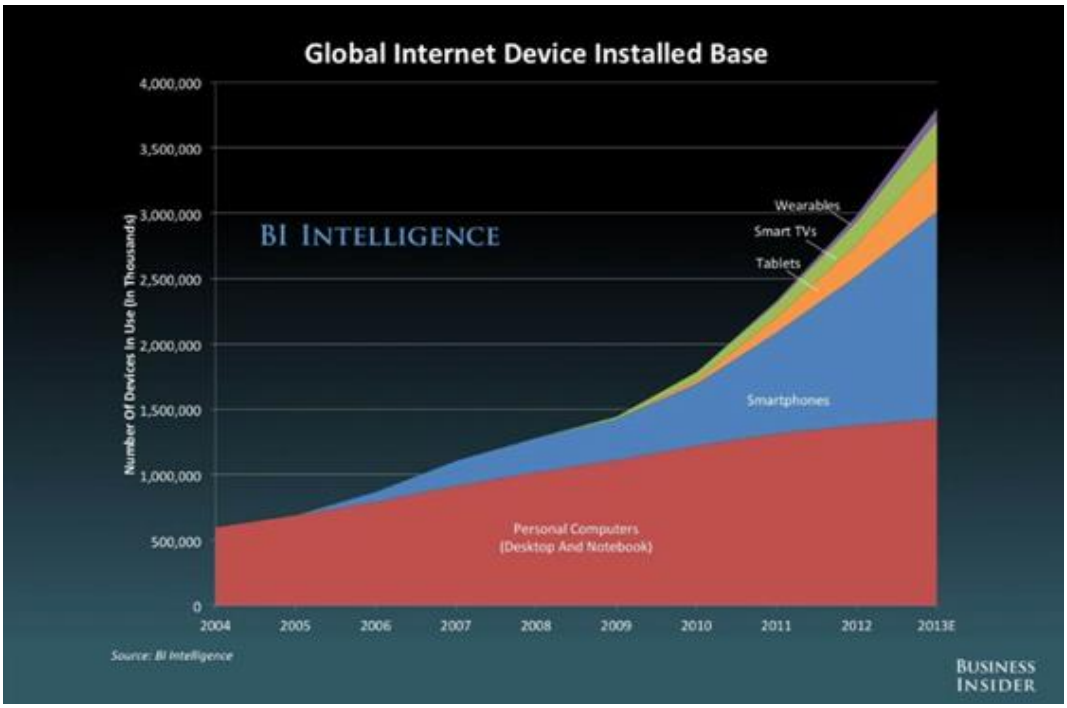


Figura 1. A día de hoy un 60% de los dispositivos online son smartphones o tabletas (7).

Según IDC (8), en el 2017 el 87% de los dispositivos conectados a Internet serán smartphones y tabletas. Las tendencias de las ventas de dispositivos avalan esta predicción como podemos ver en la Figura 2 y Figura 3, donde vemos también que las tabletas poco a poco están canibalizando los PCs.

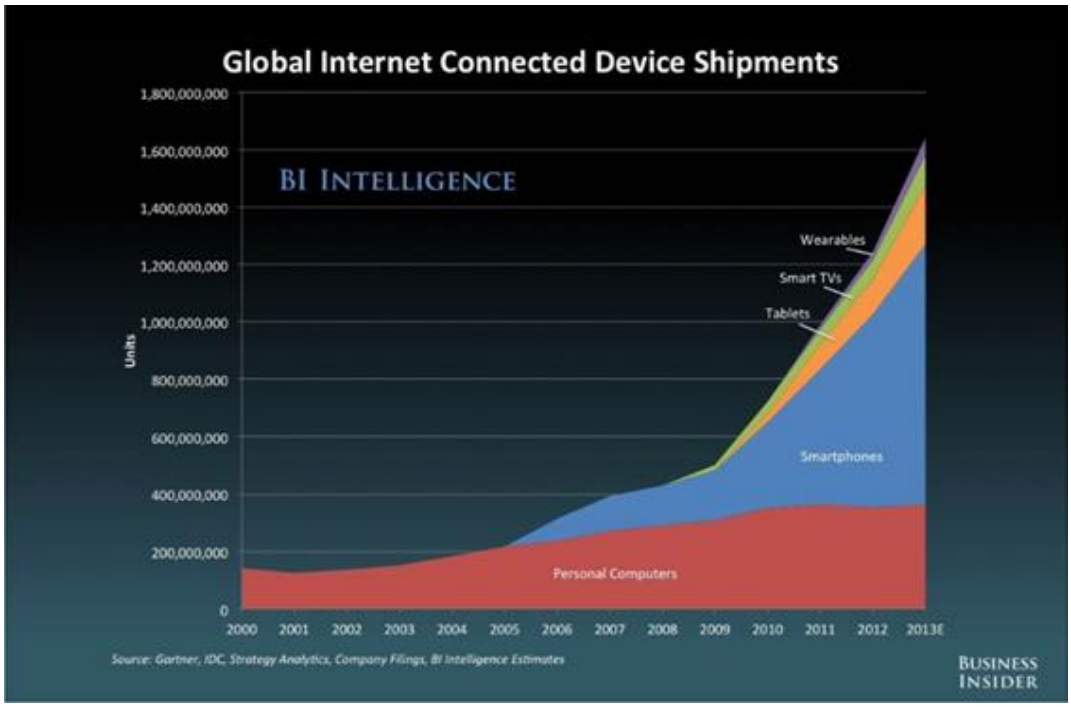


Figura 2. Comparación de volumen de ventas de los dispositivos conectados a Internet (7).

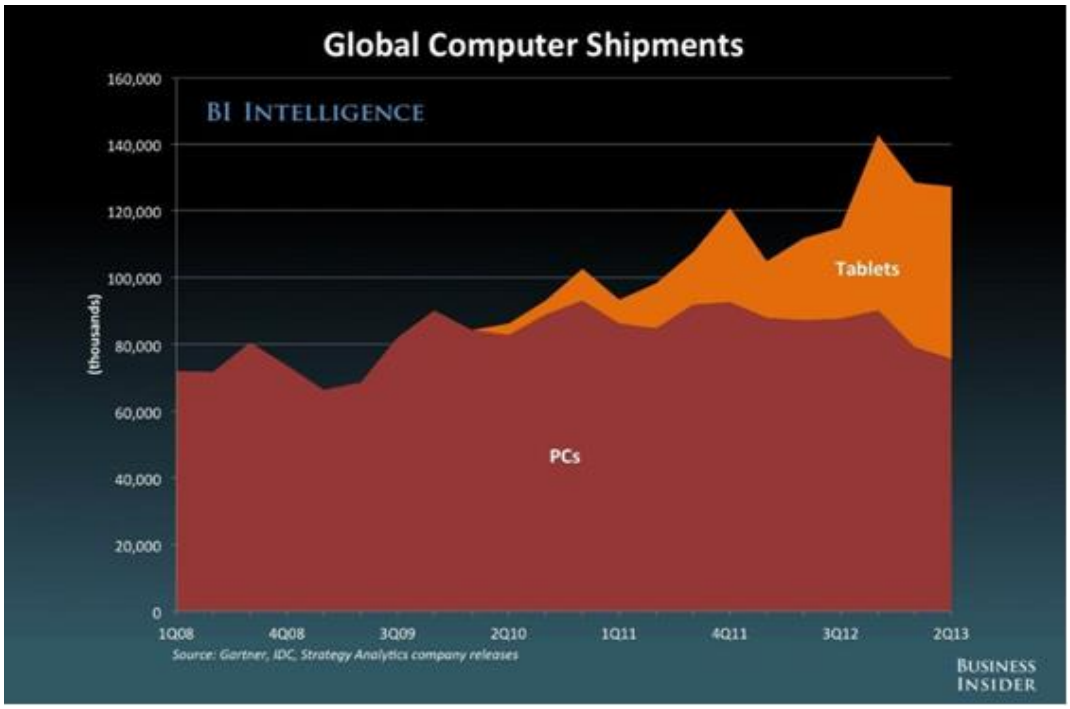


Figura 3. Las tabletas están canibalizando los PCs (7).

En mercados emergentes, donde el número de dispositivos por persona no es tan elevado como en los mercados maduros, el crecimiento espectacular lo están teniendo las "*phablets*", que combinan en un solo dispositivo las ventajas del smartphone y la tableta.

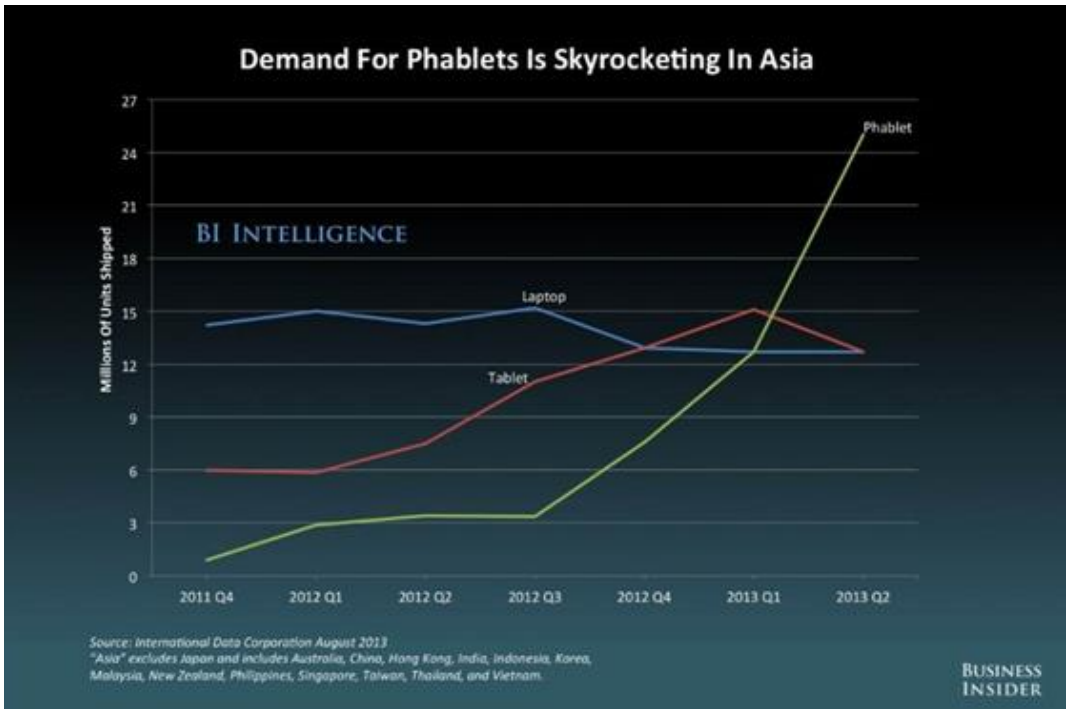


Figura 4. Crecimiento de las "Phablets" (7).

La transición tecnológica que estamos viviendo está cambiando totalmente las reglas del juego. La forma en que vivimos, aprendemos, jugamos y, sobre todo, trabajamos se está transformando. Todas las dimensiones de nuestra vida laboral están llamadas a cambiar: con quién trabajamos y cuándo, dónde, cómo y por qué lo hacemos; todos estos aspectos se verán afectados. Ahora nuestra vida y nuestro trabajo son móviles.

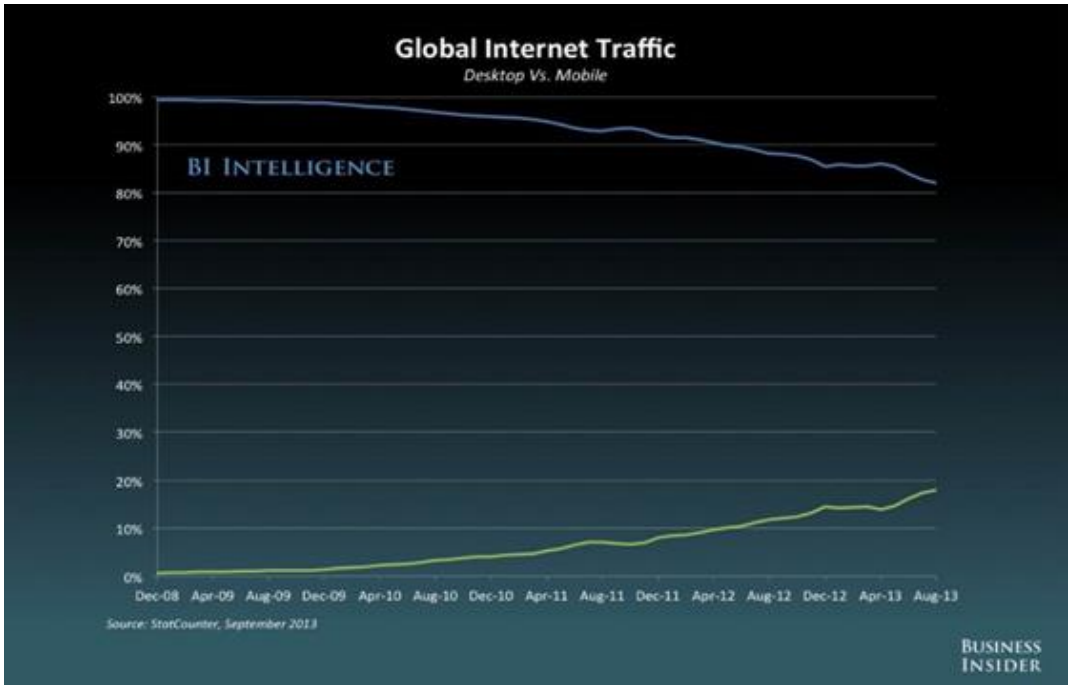


Figura 5. Ahora una quinta parte del tráfico de Internet proviene de dispositivos móviles (7)

El fenómeno *Bring Your Own Device* (BYOD)

La tendencia *Bring Your Own Device* es cada vez es más popular en el mundo empresarial. La adopción varía mucho según geografía como se puede ver con más detalle en la sección 2 (“Situación actual del BYOD a nivel mundial”). Está ocurriendo en compañías de todos los tamaños aunque está más extendido en empresas de medio y gran tamaño (de entre $500 y $5.000 millones de facturación, con 2.500- 5.000 empleados, según Gartner (9)). El BYOD también permite a empresas más pequeñas entrar en el mundo de la movilidad sin tener que hacer grandes inversiones en servicios y dispositivos. Es fácil entender el porqué. A primera vista, un dispositivo comprado por un empleado es un dispositivo que la organización no tiene que comprar, mantener y soportar.

La forma en que las empresas han recibido este tipo de programas también varía mucho. Por ejemplo, en Estados Unidos las empresas daban un apoyo económico al empleado para que pudiera comprar el dispositivo con el que se sintiera más cómodo y, por tanto, fuera más productivo. En España las empresas también dejaron que sus trabajadores utilizaran sus propios dispositivos, aunque en la mayoría de las ocasiones se han saltado el paso de poner dinero sobre la mesa.

Antes de nada, veamos qué tipos de programas BYOD podríamos considerar en función del tipo de tecnología que apoya y del modelo económico que utiliza.

Tipos de programa BYOD por tecnología

Como se ha comentado anteriormente, en función de los dispositivos que se usen hay cuatro tipos de programas BYOD más habituales:

- Tabletas. Según datos de la consultora Gartner (10), una media del 47% de empresas ofrece soporte a tabletas en sus programas BYOD, aunque sólo un 16% lo subvenciona de alguna forma. En la Figura 6 podemos ver la penetración de estos programas por industria (datos a nivel mundial).
- Smartphones. Lo ofrecen una media del 34% de las empresas y más de la mitad lo subvencionan de alguna forma. En la Figura 7 podemos ver el desglose por industria.
- PCs. Solo un 14% de las empresas tienen programas que permiten el uso de un PC secundario para uso ocasional y menos de un 2% lo subvenciona.
- "Bring any Technology". Los programas que dan algún tipo de subvención, dieta o reembolso para el uso de cualquier tecnología que elija el usuario o el departamento son los más raros y representan menos del 0,5% de las empresas.

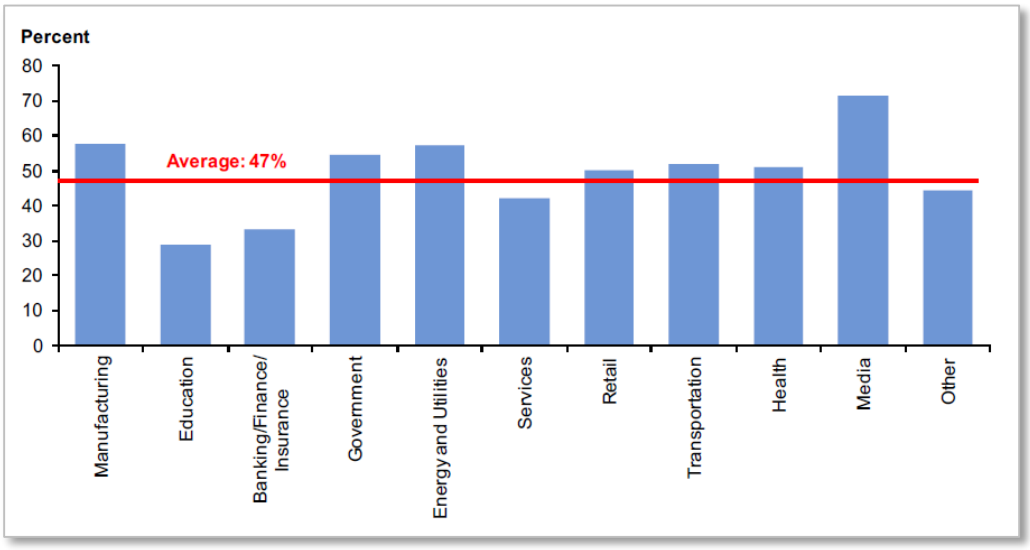


Figura 6. Adopción de tabletas en programas BYOD por industria a nivel internacional. Abril 2013 (10).

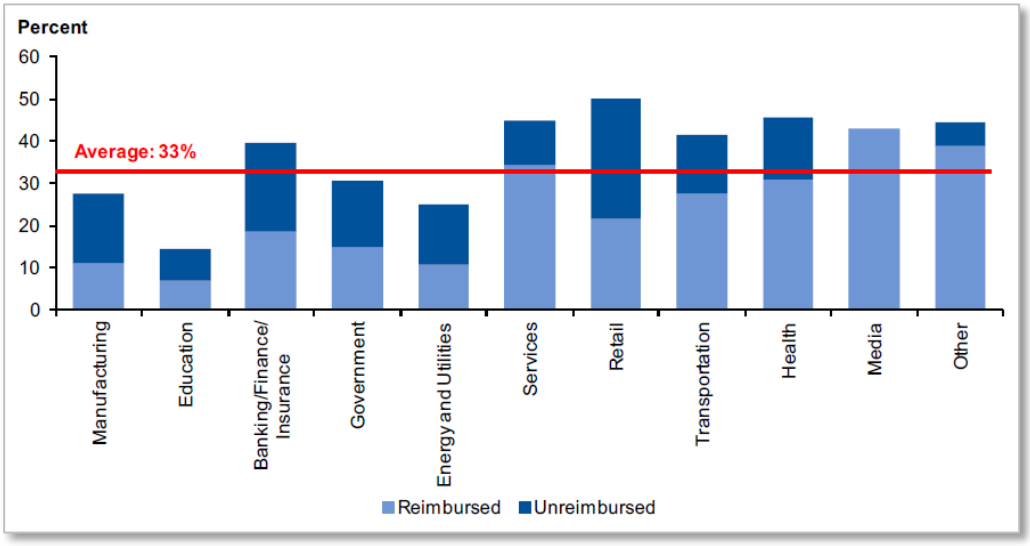


Figura 7. Adopción de smartphones en programas BYOD a nivel internacional segmentado por sector. Abril 2013 (10).

Tipos de programa BYOD por modelo económico

Según el apoyo económico que recibe los programas BYOD por parte de la empresa podemos encontrar 3 modelos básicos:

- Modelos Responsabilidad del Empleado. En estos modelos, la empresa trasfiere toda la responsabilidad del dispositivo al usuario. La empresa subvenciona el uso profesional del dispositivo mediante subvenciones, reembolsos o incrementos en el salario.
- Modelos Responsabilidad Híbrida. Hay varios enfoques según se comparta la responsabilidad en la propiedad, pago y/o soporte. El modelo más común permite que un dispositivo proporcionado por la empresa se utilice para aplicaciones personales. Otro modelo híbrido combina el dispositivo personal del empleado con un contrato corporativo con el operador. O una variación de este último, es el caso en que el empleado tiene un precio especial dentro de un acuerdo corporativo con un operador en el que la empresa puede pagar una parte proporcional correspondiente al uso profesional.
- Modelos Dispositivo Secundario. En estos modelos el dispositivo personal se utiliza como un complemento no subvencionado para un dispositivo proporcionado por la empresa (por ejemplo para acceder al correo a través de la web).

2. Situación actual del BYOD a nivel mundial

A la hora de definir un programa BYOD es muy importante tener presente en qué país está situada la organización donde se vaya a implantar. En el caso de las multinacionales, deberá contemplar las particularidades de los diferentes países y las políticas deberán adaptarse según las diferentes necesidades. El uso de una política única para todas las geografías puede conducir al fracaso del programa.

La firma Ovum ha realizado un interesante estudio (11) sobre el estado y percepción de la tendencia BYOD a nivel mundial, recogiendo respuestas de cerca de 4.000 trabajadores de organizaciones de más de 50 empleados, en 17 países. Este estudio reveló divergencias entre las actitudes de los empleados en mercados maduros y en mercados en desarrollo con gran crecimiento. Estos diferentes comportamientos y actitudes no sólo definirán diferentes patrones de Movilidad Empresarial en ambos tipos de mercados, sino que también dictarán los mercados que más van a beneficiarse de la revolución BYOD.

Las principales conclusiones del estudio son:

- Los empleados en mercados emergentes están muy positivamente dispuestos a tener un acceso constante a las aplicaciones y datos corporativos, desde donde sea e incluso fuera de los horarios de trabajo. También están más dispuestos que sus colegas en mercado maduros a utilizar un único dispositivo para uso personal y profesional. Dichas actitudes muestran un mayor nivel de comodidad con la dilución de las fronteras entre trabajo y vida personal. En los mercados maduros prevalece la actitud de mantener una cómoda vida privada.
- Estas actitudes, junto al elevado número de jóvenes que se unen al mercado laboral y un índice de penetración de dispositivos inteligentes en continuo crecimiento, hace que en los mercados emergentes el BYOD tenga alto potencial de crecimiento.
- Desde el punto de vista empresarial, el BYOD está tan extendido que es extremadamente importante que las empresas lo gestionen para evitar problemas se seguridad, que pueden tener notables consecuencias económicas, legales y reputacionales.
- Los responsables de la definición de programas BYOD deberían considerar cómo las actitudes de sus usuarios pueden ser una barrera o un impulso para el éxito del programa, y adoptar políticas, modelos de gestión y medidas control que puedan mitigarlas o reforzarlas para su beneficio.

A continuación se precisan los hallazgos del estudio con más detalle.

Hallazgos del estudio “BYOD: an emerging market trend in more ways than one” de Ovum

Para determinar la penetración del BYOD, se preguntó a los empleados si usaban su propio dispositivo (smartphone o tableta) en el trabajo (para actividades que implicasen acceder a datos corporativos), Ovum halló que un 57,1% participaban en algún tipo de BYOD. En la Figura 8 puede verse información más detallada por mercado que muestra una tendencia clara a un mayor uso de dispositivos propios en mercados emergentes (74,9%) que en mercados maduros (44,4%).

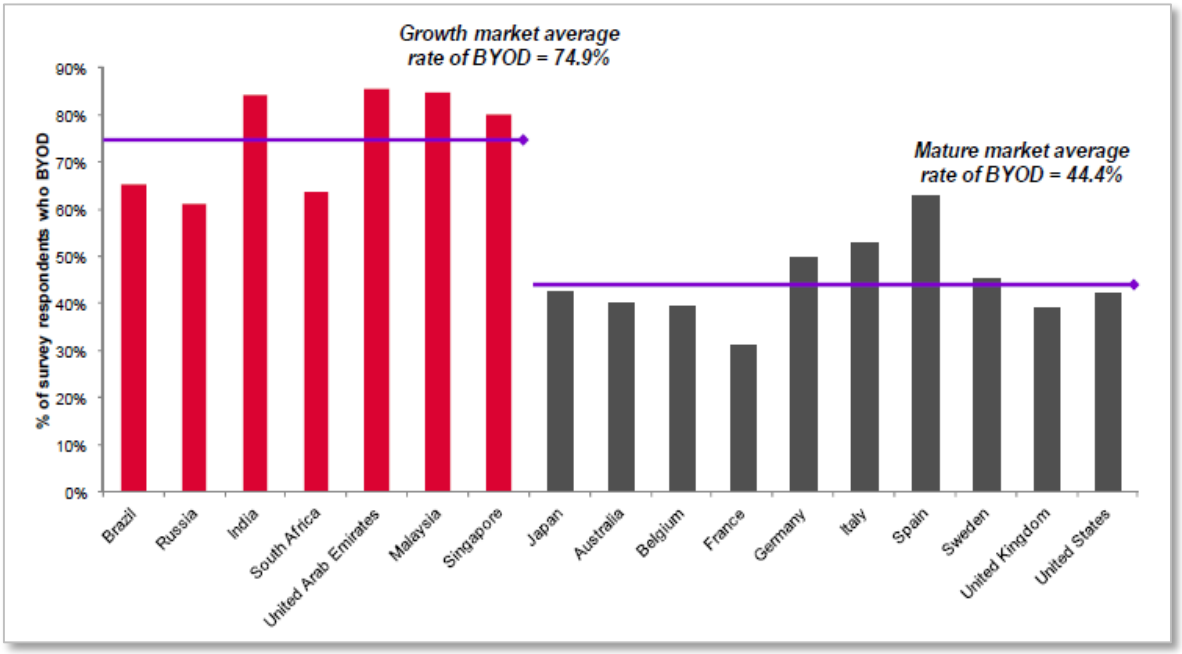


Figura 8. Diferencia de penetración del BYOD en mercados maduros vs. mercados emergentes (11).

Separación entre vida personal y profesional

La mayor preferencia por el BYOD en mercados emergentes es sintomática de un par de factores importantes:

- hay mucha menor presencia de programas de movilidad corporativa que proporcionen smartphones y tabletas a los empleados, lo que hace que quien siente que necesita usar un dispositivo móvil para ayudarle en su trabajo acabe usando el suyo propio;
- los empleados en estos mercados muestran un mayor nivel de comodidad con la dilución de las fronteras entre trabajo y vida personal. Tienen una actitud más flexible hacia el horario laboral y no les importa usar sus dispositivos para hacer su trabajo donde sea necesario.

En los mercados maduros, en general, los empleados están más "acomodados". Están más acostumbrados a que los dispositivos los proporcionen las empresas, y son más celosos de la separación entre vida personal y laboral.

Cabe destacar aquí el caso de España, donde un 62,8% de los empleados utilizan sus dispositivos, muy por encima de la media de los mercados maduros. En el estudio lo achacan a las dificultades económicas que atraviesa el país, que harían que los empleados estuviesen dispuestos a usar cualquier medio para sacar adelante su trabajo.

En mercados maduros como Francia, donde la penetración es la más baja (30,9%), los empleados han demostrado comportamientos arraigados que piden una clara separación entre el tiempo personal y el laboral. Así mismo, muestran una clara actitud de protección de su privacidad deseando mantener sus actividades personales fuera del conocimiento de cualquier tipo de autoridad, ya sea el estado o su empresa.

En Europa la privacidad es una cuestión importante. Sin embargo en otros países, como Estados Unidos, es algo secundario. En países como Brasil o Rusia donde todavía hay censura o ha dejado de

haberla hace poco, la actitud predominante es que las autoridades siempre pueden ver lo que haces, por lo que no importa demasiado de quien sea el dispositivo que usan para temas personales o profesionales.

Flexibilidad y actitud "always-on"

Respecto a la actitud hacia estar siempre conectado, en la Figura 9 podemos comprobar que la respuesta a la pregunta "la posibilidad de acceder al correo corporativo y otras aplicaciones de negocio fuera del horario laboral oficial me permite hacer mejor mi trabajo" está más consensuada en todas las geografías encuestadas, aunque de nuevo en los mercados emergentes la tendencia es que perciben más que estar siempre conectados a los datos corporativos es un facilitador, 79% vs. 53,5% en mercados maduros. En los mercados maduros, Italia y España son los que más de acuerdo están con los mercados emergentes.

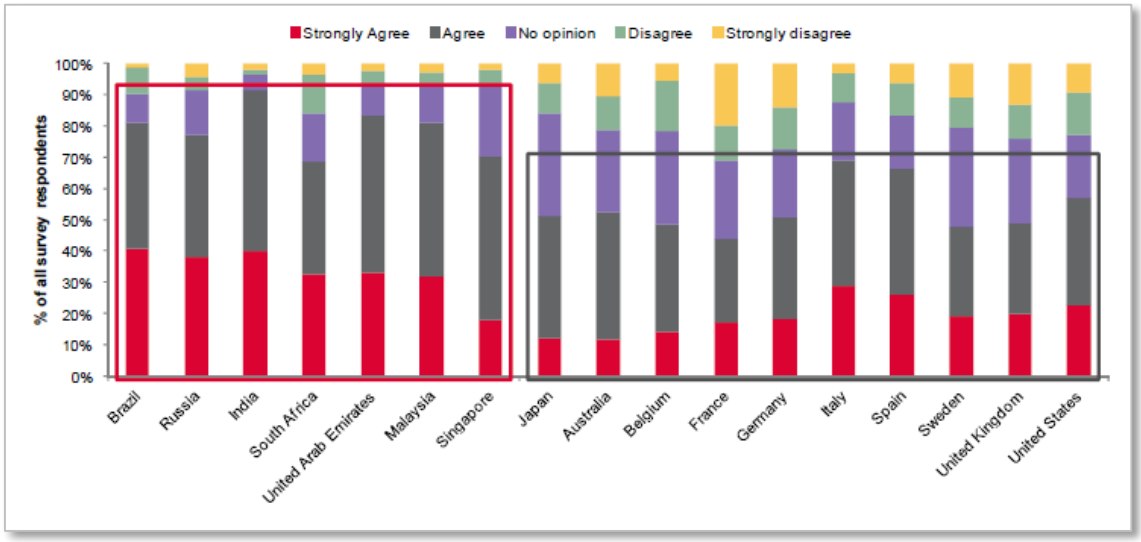


Figura 9. "La posibilidad de acceder al correo corporativo y otras aplicaciones de negocio fuera del horario laboral oficial me permite hacer mejor mi trabajo" (11).

Sin embargo, que algo se perciba como un facilitador del trabajo no implica que guste hacerlo. Por tanto también se les preguntó si les gustaba la flexibilidad de poder acceder a datos corporativos fuera del horario laboral oficial. De nuevo los mercados emergentes son mucho más receptivos a este "*always-on*" (78,6% vs. 55,1% en mercados maduros) como podemos ver en la Figura 10. Estas actitudes coinciden con los datos de mayor presencia de BYOD.

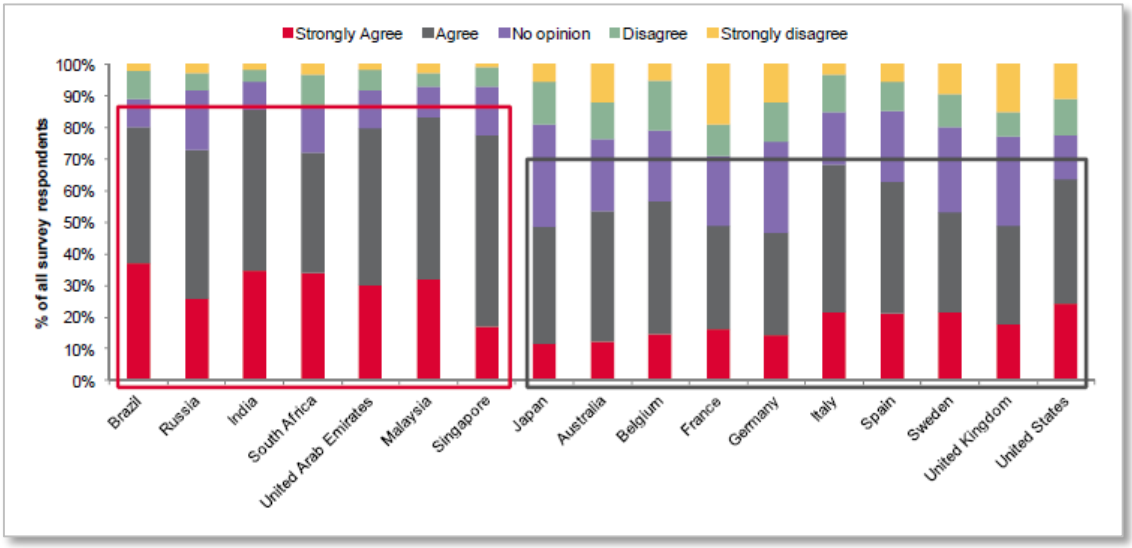


Figura 10. "Me gusta la flexibilidad de poder acceder al correo corporativo y otras aplicaciones de negocio fuera del horario laboral oficial" (11).

Uso de un único dispositivo

Aparte del requerimiento de acceso continuo a datos y aplicaciones corporativas, otro driver distintivo del comportamiento BYOD es el deseo de usar un solo dispositivo para uso personal y profesional. Aquí también vemos divergencias en las respuestas de mercados emergentes, donde un 59,1% quieren un solo dispositivo vs. un 37,7% en mercados maduros, como podemos observar en la Figura 11. De nuevo, estas respuestas coinciden con los datos de mayor presencia de BYOD.

Esto puede ser debido a que para muchas personas en los mercados emergentes los smartphones pueden ser el primer y único ordenador que poseen, muchos se han saltado la generación PC, por lo tanto usarlo en todas las facetas de su vida parece algo obvio. Hay poca tradición de programas de movilidad corporativa y por tanto no hay comportamiento a modificar.

En los mercados maduros, los usuarios ya tienen comportamientos aprendidos a lo largo de 15 años de uso de dispositivos móviles. Para la "Generación BlackBerry", móvil significa teléfono BlackBerry proporcionado por la empresa. Las empresas adoptaron ampliamente este tipo de dispositivos para tener una separación clara entre aplicaciones profesionales y profesionales porque era la única forma de estar conectado con el trabajo en todo momento. Ha sido con el despliegue de la consumerización y la aparición de dispositivos de consumo potentes y económicamente asequibles, cuando ha surgido el planteamiento de trabajar en un dispositivo personal.

Por tanto en los mercados maduros existían comportamientos previos en el ámbito de la movilidad, y las actitudes hacia el uso de un único dispositivo a nivel personal y profesional varían. Probablemente aquellos que han estado usando diferentes dispositivos quieran seguir haciéndolo, mientras que quienes han crecido con dispositivos móviles personales potentes es más probable que quieran usar un único dispositivo a todas horas del día.

Esta tendencia se acentúa en los colectivos más jóvenes en mercados emergentes. Para las empresas será cada vez más importante encontrar formas de conectar con este colectivo laboral que desea flexibilidad y movilidad.

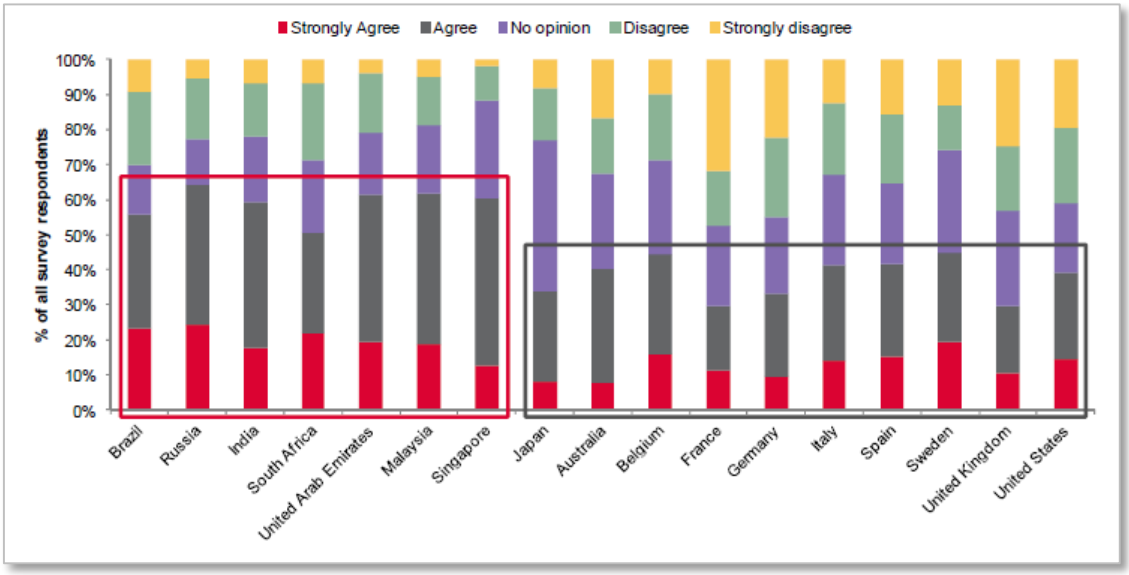


Figura 11. "Me gustaría usar un solo teléfono para uso personal y profesional" (11).

Los departamentos de TI deben tener en cuenta estos comportamientos

A medida que el BYOD se extiende globalmente impulsado por el crecimiento de la penetración de smartphones, es aconsejable tener en cuenta las diferencias en las actitudes en los diferentes mercados a la hora de definir las políticas y sistemas de gestión y control del BYOD. TI debería buscar un nivel de gestión adecuado que no degrade la experiencia de usuario para aquellos empleados que están preparados para trabajar de forma flexible.

Por ejemplo, los sistemas MDM (*Mobile Device Management*) permiten un alto nivel de control sobre las actividades del dispositivo, pero en mercados maduros pueden considerarse demasiado intrusivos. En esos entornos puede ser más adecuada una gestión a nivel de datos de aplicaciones, utilizando soluciones que compartimenten claramente los datos y aplicaciones personales y las profesionales.

En cualquier caso, lo fundamental es tener una política que gobierne el BYOD y que los empleados la suscriban. Como podemos ver en la Figura 12, la falta de gestión del BYOD es un problema en todas las geografías encuestadas, situando la media de usuarios que han firmado una política de BYOD en sólo un 12%.

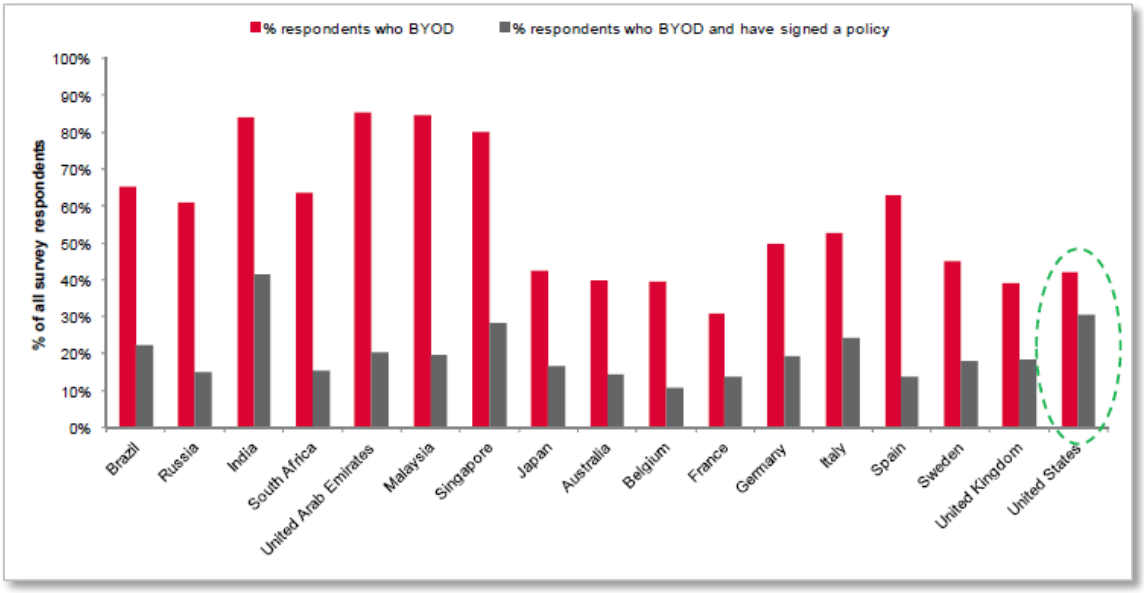


Figura 12. La falta de gestión del BYOD es un problema en todas las geografías (11).

Actitud de los departamentos de TI hacia el BYOD

Para establecer cuál era la actitud de los departamentos de TI hacia el fenómeno BYOD, Ovum preguntó a los empleados que usaban su móvil personal sobre la opinión de su departamento de TI acerca del uso del correo corporativo en dispositivos personales. Las opciones eran: "No sabe nada" (podemos considerarlo ignorancia pasiva); "Ignora que está sucediendo" (ignorancia activa, o política "prefiero no saber"); "Lo fomenta" o "Lo desaconseja". De nuevo, como podemos ver en la Figura 13, hay una tendencia general a impulsar este tipo de programas en mercados emergentes más que en los mercados maduros. En general, hay un 17,7% de usuarios que dicen que sus departamentos de TI no saben nada mientras que un 28,4% dicen que lo están ignorando activamente.

Hay excepciones, por supuesto, como por ejemplo Rusia donde la actitud prevalente es de ignorancia activa. O Gran Bretaña, Australia y Estados Unidos, donde los departamentos de TI están acogiendo este nuevo comportamiento de los usuarios. Sin duda, Estados Unidos muestra el índice de fomento del BYOD más elevado que ningún otro país en todas las geografías encuestadas. Aunque estos países no muestran un alto índice de penetración del BYOD, los departamentos de TI se están preparando para el próximo paso en el desarrollo de una estrategia de movilidad corporativa. La siguiente tarea será establecer las estrategias de gestión que mejor encajen con las exigencias culturales de sus empleados, los requerimientos regulatorios de su industria y de la legislación en materia laboral y de privacidad especifica de su país.

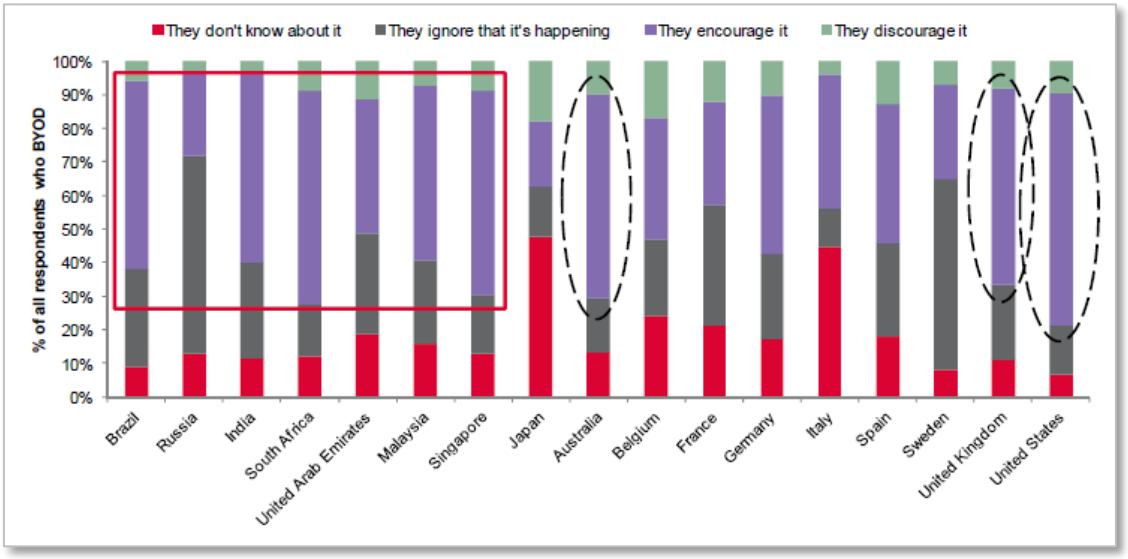


Figura 13. Actitud de los departamentos de TI hacia el BYOD (11).

3. Nuevo papel de los departamentos de TIC

Como hemos visto, los empleados quieren utilizar en su entorno laboral aquellas tecnologías (dispositivos, servicios y aplicaciones) que están usando en su entorno personal. Esto hace que las organizaciones se enfrentan a la disyuntiva de si deben permitir o no la incorporación de estas nuevas tecnologías que aumentan la productividad de los empleados, pueden ser un estímulo para la innovación en la organización, pero que también pueden suponer un riesgo. Y, por su parte, los departamentos de TI deben salvaguardar el acceso a la información corporativa, velando por la integridad y seguridad de los datos, y su necesidad de minimizar los riesgos.

El entorno de trabajo se está redefiniendo hacia un nuevo modelo cuyas características podemos ver en la Figura 14.

Antes: Vinculado al escritorio	Ahora: En cualquier lugar
Basado en PC	Priman los dispositivos de mano
Liderado por el área de TI	Liderado por los empleados o clientes
Dispositivos proporcionados por la empresa	Dispositivos propiedad del empleado
Conectividad limitada	Conectividad ubicua
Red cerrada	Red abierta
Voz móvil	Vídeo móvil
Trabajadores individuales	Trabajadores colaborativos
Productividad personal	Productividad de los procesos de negocio

Figura 14. El entorno de trabajo ha cambiado (12).

Esta situación ha supuesto un importante cambio en el papel y la percepción de las áreas de TI en las organizaciones. Recordemos como eran las cosas en el 2003, cuando apareció la BlackBerry 6210, la

primera que podemos considerar antecesor de los modernos smartphones (13). En una escena muy simplificada, los responsables de TI eran los que solían decir a los directivos "Mira este dispositivo, puedes leer tu correo electrónico en cualquier sitio", y la respuesta que normalmente recibían era "No, no quiero usar eso, no me gusta, no sé si quiero estar tan conectado". En aquella época, generalmente era el área de TI la que innovaba y los usuarios los que se resistían. TI tenía que pelear duro para que se aceptase y se usase la nueva tecnología, y al final los usuarios acaban encantados con ella. La percepción que tenían los usuarios del área de TI es que eran "los buenos" y los innovadores, estaban ahí para ayudarles y que pudieran hacer hace mejor su trabajo.

Ahora el reto es que son los usuarios los innovadores, TI está tratando de seguirles el ritmo. La percepción ha cambiado notablemente, ahora el área de TI es quien les ponen freno e impedimentos para que no puedan hacer su trabajo todo lo bien que podrían gracias a los nuevos dispositivos, servicios online y aplicaciones que ellos ya utilizan en su vida personal.

Sin embargo, las áreas de TI tienen la oportunidad de convertirse en habilitadores de esa innovación. La suya ya no es una labor sólo de operaciones (que los sistemas y procesos sigan funcionando), sino de permitir la transformación del negocio dando ese poder a los empleados, pero a la vez mitigando el riesgo para la organización y no solo controlándolo.

4. Beneficios y riesgos del BYOD

Beneficios y ventajas

Tanto analistas como fabricantes y organizaciones coinciden en que los programas BYOD pueden ser beneficiosos para las organizaciones. Según informes de Cisco (14) (15), los principales beneficios que el BYOD puede aportar a una organización son una mayor productividad (los usuarios trabajan más cómodos, contentos y a menudo más rápido con sus propios dispositivos), la mejora de la satisfacción de los empleados (pueden trabajar de forma más flexible) y la potencial reducción de costes vinculados a programas de movilidad (hay ahorros en hardware, licencias de software, telecomunicaciones y mantenimiento de dispositivos).

En la Figura 15 podemos comparar los ahorros por usuario móvil en diferentes geografías con implementaciones de programas BYOD básicas e integrales. En general, parece que cuanto más se usa BYOD, más se entiende su potencial. Y lo usuarios incluso pueden ver más allá de implementaciones pobres de BYOD (como en Alemania) hacia los beneficios de un enfoque más integrado.

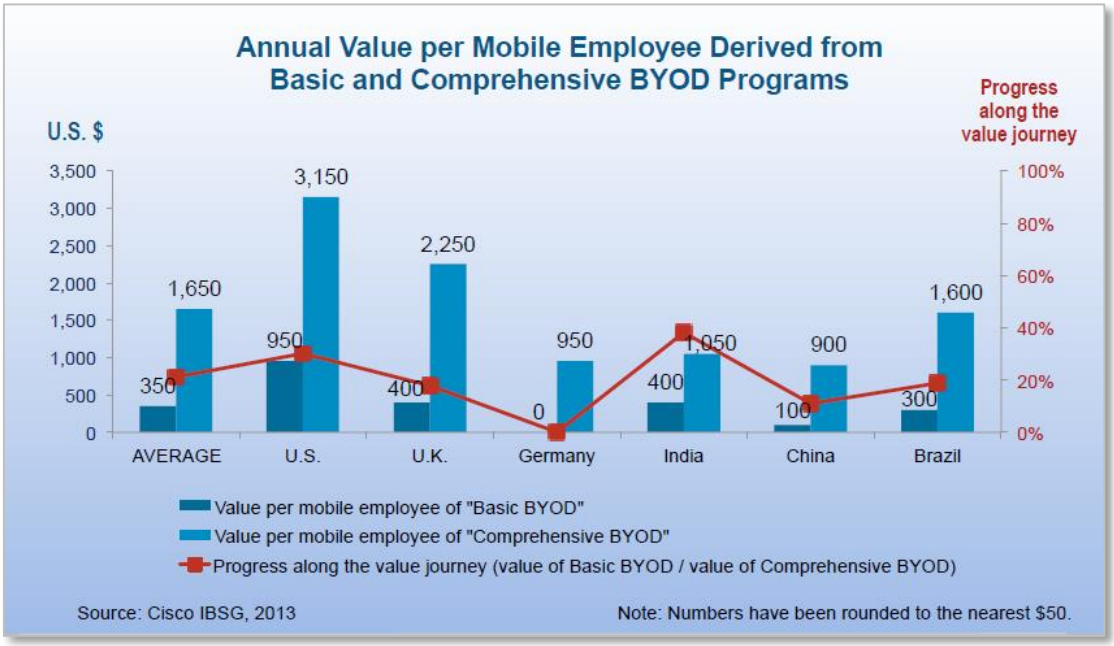


Figura 15. Ahorro en costes en la implementaciones básicas e integrales de programas BYOD (14).

El mejor acceso a la información corporativa al poder acceder en cualquier momento y lugar, puede contribuir a la mejora en la toma de decisiones. Y también existe un potencial beneficio transformativo del BYOD como habilitador de la innovación impulsada por los empleados. Al permitir que los empleados decidan la forma, el momento y las herramientas con las cuales se lleva a cabo el trabajo, las empresas pueden mejorar modelos de trabajo existen o desarrollar nuevos modelos de trabajo o de negocio.

Riesgos e inconvenientes

El uso de los dispositivos personales normalmente va acompañado del uso de aplicaciones y servicios en la nube personales y esto puede suponer costes potenciales para las organizaciones. Uno de ellos es el mayor ancho de banda que requieren muchas de ellas. Algunas de las aplicaciones más populares que utilizan los empleados incluyen elementos multimedia, entre ellas las redes sociales y la transmisión de servicios multimedia. La combinación de más dispositivos en la red y las aplicaciones multimedia no aprobadas pueden crear cuellos de botella en la red, a menos que los departamentos de TI sean muy celosos acerca de su administración de la red y su planificación de recursos.

Otra área que requiere administración activa es el uso creciente de herramientas de colaboración no aprobadas. Los empleados usan cada vez más servicios de mensajería instantánea, administración de archivos, videoconferencia móvil y colaboración en la nube para complementar o incluso reemplazar a las aplicaciones de colaboración corporativas. Aunque puede ser beneficioso para los empleados usar las herramientas de colaboración de su preferencia, especialmente si las ofrecidas son limitadas o inadecuadas, existe un potencial para la autogeneración de "islas" de colaboración que excluyan a otras personas de forma inadvertida. Es vital que las empresas garanticen que las herramientas de colaboración no aprobadas se integren a la mensajería instantánea corporativa, los directorios corporativos, el software social corporativo y las herramientas de colaboración de video para evitar la creación de estas "islas".

El peor riesgo para la organización: la seguridad de la información corporativa

Definitivamente, el BYOD se lo está poniendo difícil al departamento de TI. Según una encuesta a

profesionales de TI (16), de entre las compañías que permiten el uso de dispositivos personales en sus redes, una aplastante mayoría del 93% indica que cuando los empleados usan su propio smartphone, tableta u otro dispositivo para trabajar con información vinculada a la empresa, esto les genera problemas.

El principal reto al que se enfrentan las áreas de TI al adoptar programas BYOD es, según el 67% de los participantes en la encuesta, la seguridad de la información corporativa (Figura 16). La información de una organización está tan segura como lo esté el más débil de sus elementos, y ahora los dispositivos personales se han convertido en el eslabón más débil de la cadena.

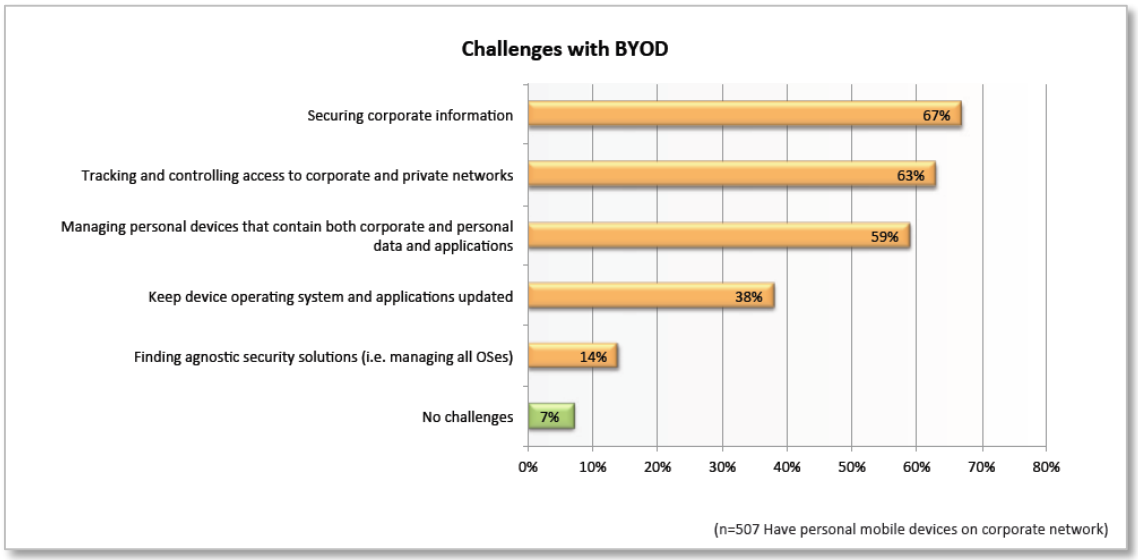


Figura 16. Principales retos que los responsables de TI encuentran en el BYOD (16).

No es de extrañar que la seguridad sea una preocupación. Según muestra otra reciente encuesta (17), la concienciación entre los usuarios sobre la necesidad de tomar precauciones de seguridad en los dispositivos móviles es muy baja: el 52% de los participantes llevaba encima regularmente un dispositivo móvil con información sensible del trabajo y el 61% de los que usan su dispositivo para trabajar no usan una contraseña de protección. Teniendo en cuenta que, además, el 27% afirmaba haber perdido hasta tres dispositivos de empresa, es comprensible la preocupación de los responsables de TI por proteger la información corporativa.

Cuando se accede información corporativa desde dispositivos personales, el riesgo de fuga de datos es especialmente acentuado, y no solo por la pérdida de dispositivos que ni siquiera usan contraseña. Los virus y otro malware, la fuga de datos entre aplicaciones móviles y las intrusiones en la red corporativa son otras de las amenazas que traen los dispositivos móviles personales.

Según un informe (18), el 100% de las 100 principales apps de pago Android y el 56% de las Apple iOS han sido hackeadas. Las aplicaciones gratuitas no están fuera de peligro, el 73% de las Android y el 53% de las iOS han sido hackeadas. Las aplicaciones pueden haber sido manipuladas para incluir malware (virus, gusanos, troyanos, rootkits, *scareware*, *spyware*, *adware* intrusivo, *crimeware*, etc.) y otros softwares, o para, a través de ingeniería inversa o decompilación, analizar el código y preparar ataques dirigidos a la lógica o datos de negocio.

Según el Informe de Amenazas de Seguridad de Internet elaborado por Symantec (19), el 32% del malware móvil tiene como objetivo el robo de información.

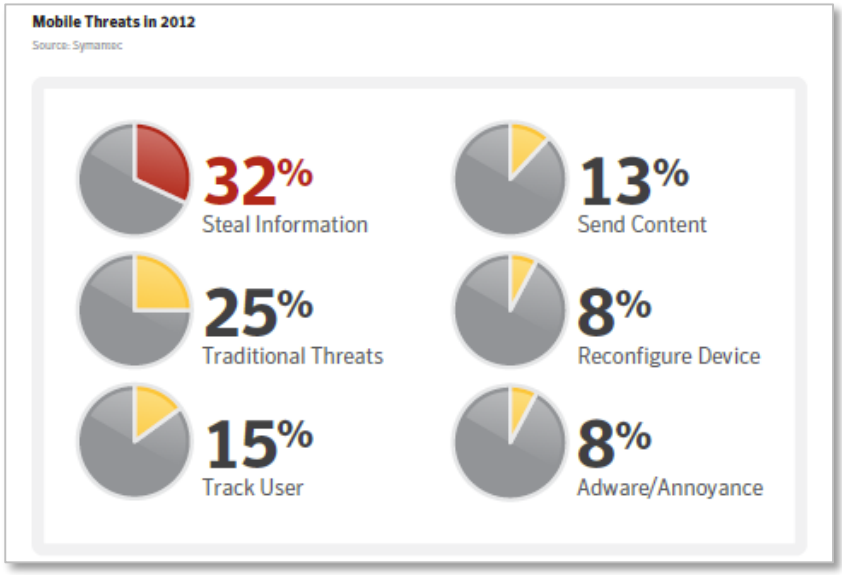


Figura 17. Actividades realizadas por el malware de móviles (19)

El sistema operativo de los dispositivos elegidos por los usuarios de los programas BYOD impactará mucho en la seguridad. Según el mismo informe de Symantec, en 2012 el 93% de las vulnerabilidades publicadas eran de la plataforma iOS. Sin embargo, Android domina el entorno del malware con un 97% de las nuevas amenazas en el mismo año.

Otros riesgos que no suelen pensarse

Sin embargo, hay otros riesgos que pocas empresas llegan a plantearse, pero que también acarrean los programas BYOD. Son los legales, de cumplimiento de normativas y de regulación, especialmente en lo referente a la privacidad. La línea divisoria entre gestionar un dispositivo de un usuario e invadir su privacidad personal es muy difusa. Además, si los usuarios descargan datos personales de clientes en los dispositivos, la organización deja de tener control sobre donde están los datos que tiene obligación de proteger y las copias que se han podido hacer.

Desde el punto de vista legal no todos los aspectos de la consumerización están cubiertos. Hay muchos asuntos legales vinculados a BYOD que aún no tienen resolución. Esto deja en manos del área de TI la tarea de definir una estrategia global de BYOD que permita a los usuarios ser productivos sin cruzar líneas legales, alejando a la empresa de las zonas grises de vacíos legales.

¿Los riesgos entonces superan los beneficios?

Las empresas pueden beneficiarse plenamente del BYOD y la consumerización si aplican una estrategia que reduzca los riesgos de seguridad y privacidad, así como la complejidad de la gestión. Esta estrategia ayudará al equipo de TI a través de una infraestructura de soluciones y un programa BYOD que permitirá al equipo de TI:

- La gestión unificada de las políticas: una única plataforma de gestión de políticas que proteja datos, aplicaciones y sistemas, y que reconozca el perfil de usuario. Asimismo debería identificar y gestionar todos los dispositivos móviles que acceden a la red corporativa.
- Proporcionar acceso seguro a la red y servicios corporativos, en función del perfil de usuario y dispositivo usado, y manteniendo la capacidad de red necesaria.

- Proteger los datos independientemente de su ubicación con una seguridad capaz de identificar el contexto.
- Facilitar la transmisión segura de datos entre los dispositivos y la infraestructura de red o cloud.

5. ¿Pueden los departamentos de TI esperar a que pase esta moda?

La respuesta es muy sencilla, no.

En primer lugar, el BYOD está demostrando ser mucho más que una moda pasajera. Las estrategias BYOD son el cambio más radical en la cultura de los ordenadores cliente en las empresas en décadas. La consultora Gartner, autora de sus populares informes de predicciones sobre tecnología, considera la gestión y la diversidad de los dispositivos móviles una de las **10 tendencias estratégicas en tecnología para 2014** (20). Gartner considera una tecnología estratégica, aquella que potencialmente puede tener un impacto significativo en la empresa durante los próximos tres años. Entre los factores que representan un impacto significativo están la posibilidad de generar disrupción en el área de TI o en el negocio, la necesidad de una inversión económica considerable o los riesgos asociados a la adopción tardía de la tecnología.

Gartner estima que una consecuencia inesperada del BYOD es que el volumen de trabajadores móviles se duplicará, o incluso triplicará, para el 2018. En este contexto, el área de TI seguirá desempeñando un papel fundamental, y será crítico disponer de políticas que cubran los dispositivos propiedad de los empleados, y que equilibren la flexibilidad necesaria con los requerimientos de seguridad, confidencialidad y privacidad.

Es mucho mejor abordar la situación antes de que se convierta en un problema inabordable con un volumen de usuarios inmanejable.

Tendencias de futuro

También según Gartner (9), este movimiento va a crecer. Para el 2017 la mitad de las empresas requerirán que sus empleados utilicen sus propios dispositivos para el trabajo, y en el 2020 el BYOD será parte del 85% de las empresas. Según sus previsiones, que podemos ver en la Figura 18, las empresas que ofrecerán sólo dispositivos corporativos a los empleados para trabajar serán pronto la excepción.

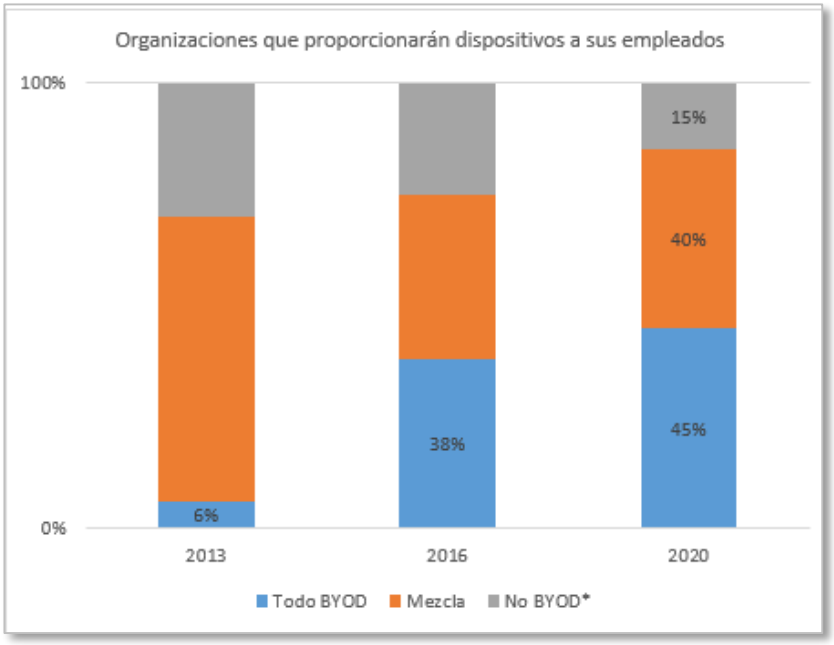


Figura 18. Previsión de organizaciones que proporcionarán dispositivos a los empleados en los próximos años (10)

Pero además el BYOD no vendrá solo, será la era de la Nube Personal (20). A nivel personal cada vez usaremos más las "nubes móviles personales". Nuestro enfoque cambiará hacia los servicios, en vez de hacia el dispositivo que usamos para acceder a esos servicios. Esto nos ayudará a afrontar los tres factores limitantes de la movilidad: vida de la batería, memoria y procesador. Los responsables de TI corporativos deben tener esta tendencia en cuenta a la hora de plantear las políticas y medidas de seguridad de los programas BYOD.

Otras tendencias que afectarán a quien se esté planteando un programa BYOD o ya lo tenga implantado son (21):

- Los smartphones y las tabletas se harán cada vez más inteligentes, incorporarán nuevas funcionalidades y mejorará su capacidad de procesamiento, almacenamiento y ancho de banda. El smartphone ya es y seguirá siendo nuestro ordenador principal. Las empresas deben tener en cuenta que veremos la web, y sus servicios, a través de nuestro móvil.
- Crecerá la virtualización del almacenamiento, escritorio, aplicaciones y networking al mejorar la seguridad de la virtualización. También crecerá la virtualización de la capacidad de procesamiento, que permitirá a los dispositivos móviles acceder a los recursos de procesamiento de supercomputadores y aplicarlos a procesos como compras o logística, por ejemplo.
- La gestión de la Identidad Digital será cada vez más importante para organizaciones e individuos. Nuevo software permitirá a los usuarios gestionar mejor sus múltiples identidades en redes personales y corporativas.
- La "tecnología que se viste" (*wearable technology*) estará cada vez más presente. Las principales marcas tecnológicas lanzarán relojes inteligentes, gafas inteligentes y mucho más, creando nuevos problemas y nuevas oportunidades para organizaciones de cualquier tamaño. Si en los últimos años el *Bring Your Own Device* (BYOD) cogió por sorpresa a las áreas de TI, ahora tienen la oportunidad de preparase para una nueva tendencia y empezar a pensar como convertirla en una ventaja competitiva: el *Wear Your Own Device* (WYOD) empezará a despuntar a partir del 2014.

- Las Apps móviles también para procesos de negocio como compras, cadena de suministro, ventas, mantenimiento, etc. crecerán rápidamente. Cada vez habrá más interés en App Stores Empresariales que permitirán a las empresas dar acceso a los usuarios a información personalizada. La nueva generación de tecnologías biométricas integradas en nuestros smartphones, jugarán un papel relevante en la gestión de la identidad y la seguridad. Veremos alternativas biométricas, como reconocimiento facial, dactilar, de voz en función de los requerimientos de seguridad necesitados.

Módulo 2: Definición e Implementación de un Programa de Dispositivos Móviles BYOD

6. Consideraciones para implementar un programa BYOD.

Cómo hemos visto hasta ahora un programa de movilidad empresarial basado en BYOD puede mejorar la productividad, estimular la satisfacción de los empleados y ser un germen para la innovación, al tiempo que puede permitir a la empresa ahorrar tiempo y dinero.

Sin embargo, si una organización implementa el programa BYOD de una forma no adecuada puede perder el control sobre su infraestructura y, lo que es más importante, sus datos, con las consecuencias económicas, legales y reputacionales que esto puede acarrear.

La implantación de un programa BYOD es compleja, tiene múltiples fases e implica a muchas áreas diferentes de la empresa. Por este motivo es fundamental planificarla cuidadosamente y abordarla de una forma sistemática y estructurada. Estas pautas pueden ser de utilidad a la hora de decidir cómo abordar la iniciativa (22) (23) (24) (25) (26).

a. Establecer un punto de partida: Evaluar la situación real de uso del BYOD (autorizado o no) en la organización

El primer paso es analizar la situación actual de la empresa desde un punto de vista realista. Si hasta ahora se sabía que los usuarios utilizaban sus dispositivos, aplicaciones o incluso redes, pero se hacía la vista gorda, este es el momento de reconocerlo. Hablando con los usuarios con una actitud no sancionadora se puede aflorar la situación real de la organización en cuanto al uso de tecnología no corporativa.

Hay que tener en cuenta también los dispositivos secundarios, PCs y otros dispositivos que los empleados pueden utilizar en casa para trabajar ocasionalmente.

b. Determinar la necesidad de un programa BYOD

Es conveniente analizar cómo trabajan los usuarios en los PCs corporativos para evaluar si podrán mantener esa productividad en sus dispositivos personales. En algunos casos, los usuarios serán mucho más productivos usando sus dispositivos personales, pero, en otros casos, puede que no tenga sentido debido al estilo de trabajo de los empleados, la cultura corporativa u otras razones.

Entender los diferentes segmentos de usuarios que hay en la organización y sus necesidades

Por ejemplo se puede realizar un análisis básico de segmentación en la empresa como muestra la Figura 19. Se han considerado las necesidades de movilidad y de aplicaciones móviles de diferentes roles de empleados, frente al nivel de soporte que podrían necesitar. Implantar un programa BYOD puede ser fácil con usuarios que necesitan poco soporte de TI, que probablemente puedan buscar el soporte ellos mismos en comunidades, pero puede ser muy complejo con usuarios con altas necesidades de movilidad y que también necesitan un elevado nivel de soporte (como pueden ser los directivos).

En un siguiente nivel de segmentación, se podría analizar el tipo de aplicaciones, servicios y datos que necesita acceder cada grupo de usuarios y el nivel de riesgo que se le podría asociar a cada uno en base a la medida acordada (por ejemplo pérdida económica, impacto en reputación, etc.).

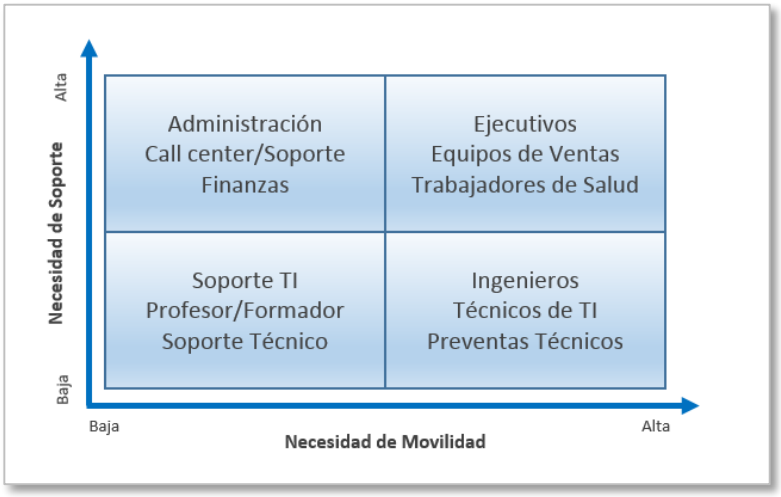


Figura 19. Segmentos de usuarios y necesidades (26).

Preguntar a los propios empleados permitirá tener una idea más exacta de la **amplitud de la demanda real del BYOD**. Es de esperar que no todos los empleados sean partidarios de pasar de herramientas corporativas a dispositivos personales. Tener clara la demanda nos ayudará a definir las prioridades en el programa y su evolución futura.

También es conveniente determinar aquellos **escenarios en los que el BYOD no será en absoluto aplicable** (por ejemplo, entornos de alta seguridad o sometidos a estrictos requerimientos normativos, áreas donde los usuarios tienen escasa alfabetización digital o donde hay resistencia o falta de interés en el BYOD).

c. ¿Está la organización preparada para sostener un programa BYOD?

Deberemos valorar si la empresa está preparada para soportar dispositivos propiedad de los empleados. Algunas preguntas a plantear son:

- ¿Tiene la organización los recursos necesarios para soportar un programa BYOD que implique múltiples tipos de plataformas y que afecte a todas las áreas de la empresa?
- ¿Están las infraestructuras preparadas para este tipo de accesos?
- ¿La empresa tiene implementado algún sistema de control de acceso a la red (NAC)?
- ¿Dispone de sistemas de gestión de dispositivos MDM?
- ¿El área de TI cuenta con los recursos y habilidades adecuadas para gestionar el programa y dar soporte a los usuarios?
- ¿A qué datos tienen que acceder los usuarios BYOD (correo, calendarios, aplicaciones corporativas, datos de clientes, información confidencial, información con propiedad Intelectual, etc.)? ¿Estos datos disponen de suficientes controles de seguridad?
- ¿Las políticas implementadas actualmente cubren todos los posibles casos de uso y las diferentes plataformas BYOD?

d. Decidir la estrategia de adopción de BYOD a seguir

Una vez que conocemos cuál es nuestro punto de partida, debemos definir qué esperamos del programa BYOD. Como ya se comentado, estos programas pueden ser más que un mero método de ahorro de costes y la organización puede planteárselo como una forma potencial de reinventar la naturaleza del trabajo en sí mismo.

Según un estudio de Forrester Consulting para Trend Micro (27), el principal objetivo que lleva a las implementar programas BYOD es la mejora de la productividad de los empleados, seguido muy de cerca por la posibilidad de proporcionar acceso a los recursos corporativos a los empleados que trabajan fuera de la oficina (Figura 20).

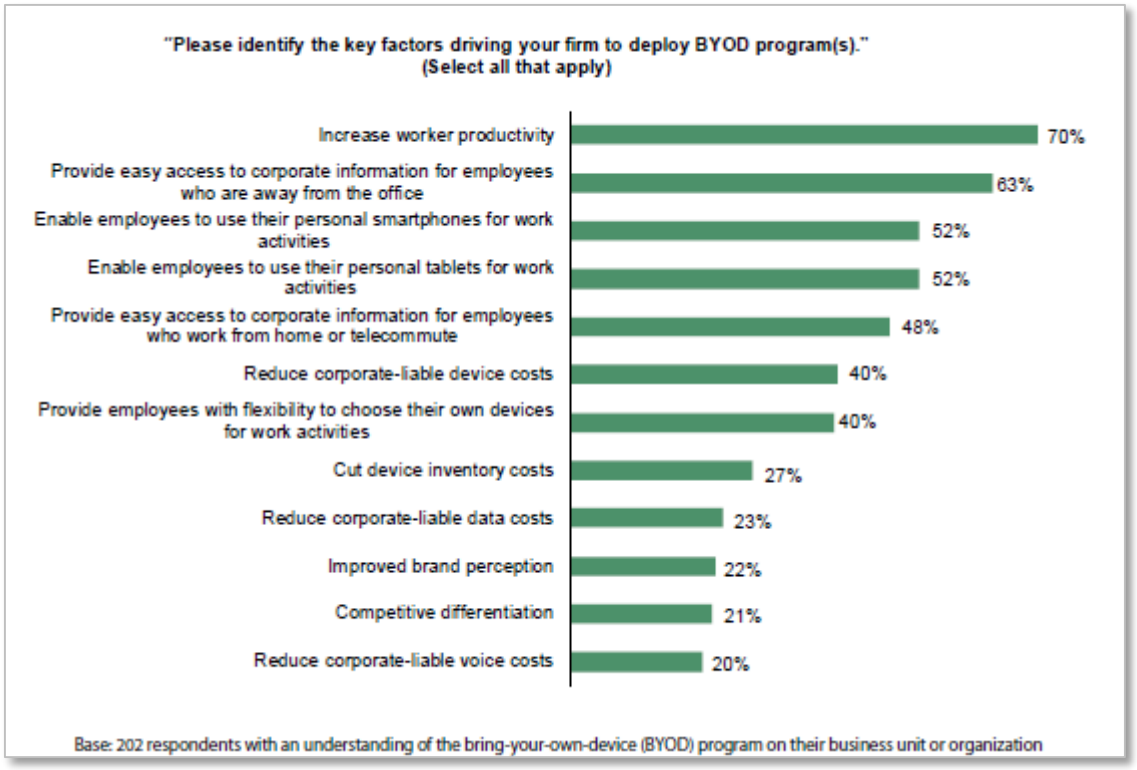


Figura 20. Principales factores que llevan a las empresas a implementar un programa BYOD (27).

Pero para obtener el máximo valor, se debe adoptar un enfoque estratégico hacia la adopción del BYOD. Si el equipo directivo (incluyendo el área de TI) es consciente de los beneficios que el BYOD les ofrece para la productividad de los empleados, el BYOD se convierte en un asunto empresarial más allá de la organización de TI que requiere el apoyo de la dirección. **El BYOD es un proyecto de gestión del cambio, no un proyecto de tecnología**. Como todo proceso de cambio necesitará un sponsor que, idealmente pertenecerá al área de negocio y estará en una posición que le permita influenciar o dirigir a los empleados que participen en el programa.

Como ejemplo, en la Figura 21 podemos ver los cuatro escenarios de adopción que define Cisco (26). En el caso más limitado, que aplicaría en organizaciones de sectores muy regulados, puede ser necesario adoptar una estrategia de BYOD muy restrictiva para proteger los datos sensibles. Los dispositivos deben ser estrechamente controlados y gestionados por TI y no se autorizaría el uso de dispositivos personales. En el extremo contrario, las organizaciones se plantearían una adopción integral y proactiva donde se priorizarían los entornos móviles (estrategia "*mobile first*"), y que

incluiría el desarrollo de nuevos servicios y aplicaciones corporativas especialmente orientados a este modelo de movilidad empresarial buscando obtener una ventaja competitiva.

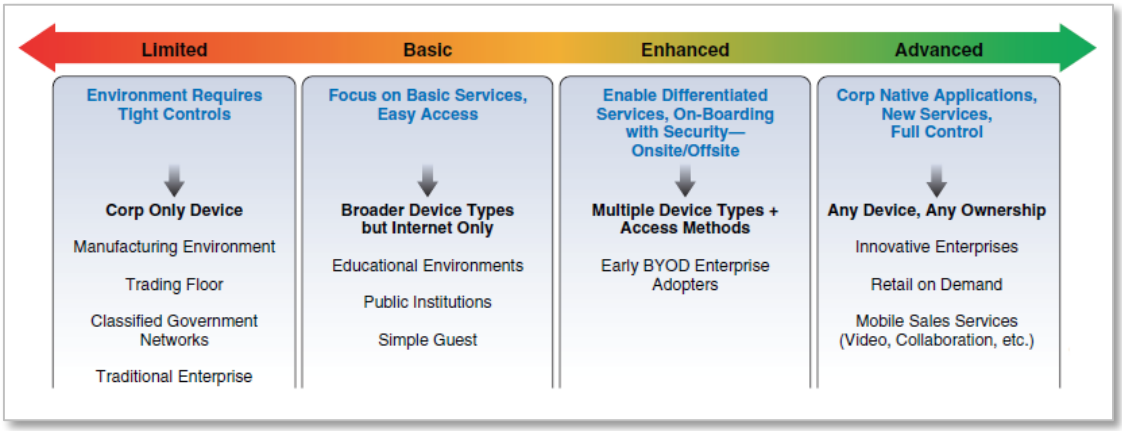


Figura 21. Estrategias de adopción del BYOD (26).

En cualquier caso, **es fundamental definir una estrategia BYOD en la organización**, incluso aunque nuestra estrategia sea no autorizarlo y permitir sólo la conexión de dispositivos de empresa a los recursos corporativos.

Una vez decidida la estrategia de adopción, hay que tener en cuenta que los programas BYOD no son un todo o nada. En función de las necesidades de la empresa, las expectativas definidas para el programa, la situación de partida en cuanto a disponibilidad de recursos y el nivel real de adopción actual, se pueden plantear diferentes fases que se pueden testear a través de diferentes pilotos.

La estrategia BYOD no es algo inamovible, de hecho deberemos revisarla periódicamente para adaptarla a la evolución de la organización, nuestras necesidades y objetivos, así como a la evolución de la tecnología. Por ejemplo, partiendo de una posición totalmente reactiva de dar soporte a las necesidades de los usuarios actuales en una única plataforma (smartphone) y con acceso limitado a recursos corporativos, se podría ir ampliando el programa para cubrir otros dispositivos (tabletas), ampliar los recursos corporativos a los que se puede acceder, extenderlo a otras áreas de la empresa, optimizar aplicaciones corporativas para su uso en entornos móviles, o diseñar iniciativas para promocionar activamente el BYOD.

e. Considerar la virtualización móvil

La virtualización del desktop permite proporcionar imágenes del escritorio corporativo en los dispositivos personales, asegurando que los usuarios no verán un cambio radical cuando el programa BYOD entre en funcionamiento. Un beneficio adicional es que el área de IT puede gestionar las imágenes del escritorio directamente desde una interfaz y despreocuparse por el hardware del dispositivo.

f. No olvidar la estrategia de aplicaciones

Aunque los empleados vayan a utilizar sus propios dispositivos aún necesitan acceder a las aplicaciones corporativas. La arquitectura de aplicaciones es un apartado fundamental de la gestión

del desktop. Implica no solo controlar como poner las aplicaciones a disposición de los usuarios sino también como monitorizar y gestionar la configuración de las aplicaciones de forma centralizada.

La Figura 22 muestra los pros y contras de tres posibles arquitecturas de aplicaciones: nativa, basada en navegador web y virtual.

Es importante decidir qué arquitectura de aplicaciones se adoptará. Muchas organizaciones adoptan un enfoque híbrido, usando el modo nativo para las aplicaciones de negocio estándar y el modo virtual para aplicaciones con requerimientos más estrictos de confidencialidad o privacidad de datos.

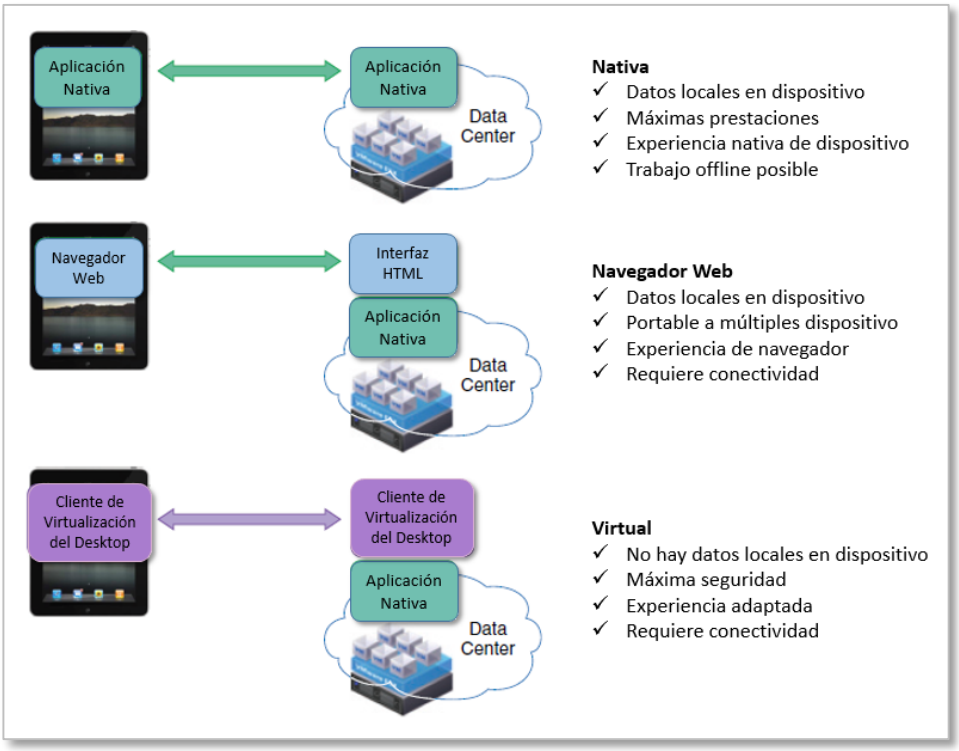


Figura 22. Aplicaciones en modo Nativo, Navegador y Virtual (26).

g. Extender la colaboración a los dispositivos BYOD

Los usuarios no se conectan a la red sólo para acceder a datos sino también para colaborar y comunicarse entre ellos. Al igual que en otros entornos de trabajo, los usuarios con dispositivos BYOD desean acceder a los servicios de voz, video y comunicaciones de la organización.

Los enfoques individuales, como confiar en las comunicaciones basadas en la red de telefonía del smartphone, pueden servir hasta cierto punto. Para ser realmente efectivos, es esencial tener un enfoque integral que permita que los usuarios sean fácilmente contactables dentro del directorio y los sistemas de comunicación de la organización.

Un programa BYOD integral debe plantearse extender la suite completa de aplicaciones de colaboración de la organización a los dispositivos BYOD, incluidos los servicios integrados de voz, video, mensajería instantánea, conferencia, compartición de aplicaciones y tele presencia. Un programa BYOD no debe pensar sólo en los usuarios que tienen dispositivos BYOD sino también en aquellos que tienen que colaborar con ellos.

h. Planificar la seguridad y gestión del BYOD

Aunque se utilicen dispositivos personales, los administradores de TI aún tienen que controlar y gestionar el acceso a la infraestructura y datos corporativos. Al igual que hacen en el caso de los dispositivos propiedad de la organización, los administradores deberán crear grupos de seguridad y políticas estrictas además de monitorizar la seguridad general.

A la hora de decidir qué solución o conjunto de soluciones de gestión y seguridad implementar debemos tener claro:

- La lista de dispositivos y sistemas operativos que incluirá el programa BYOD y cuáles de ellos son estratégicos.
- La lista de funcionalidades críticas, funcionalidades necesarias y funcionalidades deseables de la solución de gestión de la movilidad en función de los requerimientos de la organización y sus perfiles de riesgo.
- Nuestros requerimientos o limitaciones económicas (nos servirá para decidir por ejemplo, si necesitamos ir a un servicio de pago por uso en la nube o un producto con coste fijo anual).

i. Conseguir el apoyo de los usuarios

Hay que tener en consideración que es posible que no todos los usuarios sean partidarios del BYOD. Habrá empleados que querrán mantener una clara separación entre su vida personal y laboral, por ejemplo. Uno de los puntos importantes a planificar en el programa BYOD es la concienciación y formación de los usuarios, así como el hacerles manifiesto que el departamento de TI puede ayudarles a disfrutar de una mejor experiencia de trabajo con sus dispositivos personales.

Con un testeo progresivo del programa, las organizaciones pueden ganarse el apoyo de los usuarios y conseguir que sean más abiertos a la idea de usar sus dispositivos personales para el trabajo.

j. Desarrollar políticas BYOD

Implementar un programa BYOD no quiere decir que los empleados vayan a poder utilizar cualquier dispositivo. Para que el programa se implemente con éxito los administradores deben definir con antelación que dispositivos estarán soportados en los diferentes perfiles de trabajo.

Por ejemplo, se puede acceder a un escritorio virtual completo en un teléfono Android, pero probablemente no sea práctico debido al reducido tamaño de la pantalla. Pero ese mismo escritorio en un iPad puede ser factible para algunos usuarios. Es necesario definir claramente las necesidades de los usuarios y seleccionar aquellos dispositivos que encajen con ellas.

El área de TI también debe desarrollar, implementar y hacer cumplir una política BYOD que gobierne el acceso de los usuarios a la infraestructura y datos corporativos desde sus dispositivos.

¿Qué sucederá cuando un empleado no cumpla una política? ¿Y cuando deje la compañía? ¿Cómo se actuará en el caso de robo o pérdida del dispositivo? ¿El BYOD puede afectar al cumplimiento de alguna normativa o legislación?

Hay que asegurarse de que las políticas cubren todos los escenarios y áreas que se verán impactadas por el BYOD. Las políticas no afectan sólo a los usuarios, también a los directivos que tendrán que

fomentar su cumplimiento, al área de TI que tendrá que establecer sistemas para implementarlas, y al área de soporte de TI que deberá conocer los niveles de soporte que tendrá que proporcionar.

Igualmente importante será la comunicación y formación en estas políticas a todos los implicados, por lo que el área de Recursos Humanos también debe estar involucrada. Para evitar responsabilidades legales, es necesario notificar a los empleados por escrito la política que detalle como tratará la organización los datos y comunicaciones corporativas y personales.

k. Considerar los planes de despliegue

Los programas BYOD no son un todo o nada. En función de las necesidades de la empresa, las expectativas definidas para el programa, la situación de partida en cuanto a disponibilidad de recursos y el nivel real de adopción actual, se pueden plantear diferentes fases que se pueden testear a través de diferentes pilotos.

Conocer los niveles de implantación actual, así como la demanda actual y la esperada a futuro para cada plataforma, nos ayudará a priorizar y planificar el despliegue del programa.

l. Valorar periódicamente las políticas BYOD y el nivel de preparación de la organización

El BYOD crece muy rápidamente, así como la variedad de tecnologías de consumo que son aplicables a la empresa. Por ello será necesario re-evaluar periódicamente las políticas de BYOD implantadas así como el nivel de preparación de la organización para soportar los dispositivos, aplicaciones y servicios utilizados, sin dejar de mantener el nivel de seguridad y privacidad deseado.

m. Estimación del ROI del programa BYOD

Cuando llegamos a la parte económica del BYOD, hay que hacer los números con cuidado. El BYOD puede reducir los costes de los programas de movilidad, pero también puede elevarlos.

Como hemos visto en el apartado "*Beneficios y ventajas*" de la sección 4, según informes de Cisco, la implantación de un programa BYOD integral puede suponer considerables ahorros para la organización. Sin embargo otros expertos insisten en que hay que analizar con cuidado todas las variables de nuestro programa (28).

Para comprender el retorno de inversión real, debemos estudiar estos seis elementos del programa BYOD y cómo afectan a los costes y beneficios en la situación concreta de la organización.

- Coste del dispositivo. El coste de un dispositivo corporativo variará en función de que esté subvencionado por el operador o no. Las organizaciones grandes además pueden negociar descuentos por grandes volúmenes de compra o conseguir dispositivos de backup de forma gratuita. El ahorro comparado con un dispositivo propiedad del empleado deja de ser significativo. Según Nucleus Research (28), el coste del dispositivo representa menos del 10% del coste total anual de las iniciativas de movilidad corporativa.
- Costes de datos y voz. El coste del plan de datos y voz puede ser hasta 10 veces mayor que el coste del dispositivo. Si la organización va a subvencionar a los empleados estos costes, debe analizar cuidadosamente el importe a reembolsar, especialmente si hay costes de roaming

internacional involucrados. Hay que tener en cuenta además los costes asociados al propio proceso de gestión del reembolso.

- Costes de soporte técnico. Dependiendo del nivel de soporte necesario, así como el nivel de conocimientos necesarios para ofrecer ese soporte, los costes pueden variar mucho. Es importante delimitar claramente el soporte a ofrecer así como buscar alternativas de auto-soporte basadas en comunidades y wikis (ver sección 7.5 más adelante).
- Costes de desarrollo de aplicaciones móviles. Un programa de movilidad está incompleto sin aplicaciones móviles. La inversión necesaria para desarrollar nuevas aplicaciones corporativas para las plataformas móviles, o adaptar las ya existentes puede ser una inversión considerable. Sin embargo, esta inversión puede traer consigo mejoras en la productividad de los empleados y eficiencias en procesos.
- Software de gestión de la movilidad. Será necesario implementar una solución de gestión de la movilidad (que incluya funcionalidades de gestión de datos y aplicaciones móviles, y de seguridad), así como formar adecuadamente al área técnica y a los usuarios.
- Productividad conseguida específicamente a través de los dispositivos móviles personales. Aunque la productividad se considera el beneficio principal del BYOD, es complicado calcular un número concreto. Para medir el beneficio en la productividad derivado del BYOD, la organización debería calcular primero la productividad conseguida con un dispositivo personal comparada con la conseguida con un dispositivo de empresa. Por ejemplo, Intel recientemente estimó un ahorro de tiempo de 57 minutos al día de sus 23.500 usuarios BYOD. Según una encuesta de Cisco (14), los empleados BYOD ahorraban hasta 81 minutos a la semana.

  El cálculo es difícil y dependerá de la situación concreta de la organización. Si el BYOD es la única alternativa a no tener un programa de movilidad, la perspectiva será diferente.

7. Implementación de un programa BYOD

Una vez definidos los puntos tratados en el apartado anterior, podemos afrontar la implantación del programa BYOD.

Sabemos de dónde partimos, dónde queremos llegar y los objetivos de negocio asociados a este "viaje", hemos definido grupos de usuarios según sus patrones de uso, requerimientos y perfil de riesgo. Destacaremos a continuación algunos de los puntos críticos para la implementación con éxito del programa BYOD.

7.1. Definición de la política BYOD dentro de la política de movilidad corporativa

Qué es una política BYOD

Una política BYOD es un conjunto de reglas que gobiernan los aspectos relacionados con el uso de dispositivos personales para acceder y utilizar recursos de la organización.

Una política es algo específico para cada organización puesto que debe basarse en los requerimientos de la organización, su perfil de riesgo y su situación, pero en esta sección describiremos los aspectos generales que debe cubrir.

Si en la organización ya existe una política de movilidad corporativa, deberá revisarse para incorporar la política BYOD. Así mismo, deberemos revisar otra políticas que también se verán afectadas (negocio, seguridad, acceso a recursos, regulatorias y legales, RRHH, etc.).

A la hora de definir la política, es conveniente tener en mente que lo que impulsa los programas de movilidad corporativa es la necesidad de proporcionar acceso seguro y transparente (es decir, con la mejor experiencia de usuario) a los recursos corporativos en cualquier momento, en cualquier lugar y desde cualquier dispositivo. Las iniciativas de movilidad deben contribuir a facilitar la continuidad del negocio, mejorar la colaboración, simplificar el teletrabajo y mejorar la satisfacción de los empleados.

La política BYOD debe revisarse periódicamente (cada 6-12 meses) para asegurar que se adapta en todo momento a la organización y sus necesidades de negocio. También va a ser necesario estar al corriente de los cambios tecnológicos que la afectan (nuevas funcionalidades o nuevos dispositivos, aplicaciones y servicios de consumo; innovaciones y tendencias en los sistemas de gestión MDM, EMM; nuevas amenazas de seguridad, medidas de protección y mitigación, etc.).

La política debe ser clara, concisa, realista, sostenible y adaptada a los usuarios que la van a utilizar. Una política que pretende influenciar el comportamiento de los empleados no puede estar escrita en un oscuro lenguaje técnico ni alejarse de la cultura y estilo de la organización.

Aunque en un principio la elaboración de la política pueda parecer una tarea abrumadora, hay que tener en cuenta que **la peor política es la ausencia de política**. Cuando los empleados saben qué se espera de ellos, cuáles son los comportamientos aceptables y las consecuencias del incumplimiento, es menos probable que rompan las reglas y, en caso de hacerlo, los planes de contingencia definidos con anterioridad en las políticas permitirán actuar con rapidez y minimizar el impacto negativo.

Cualquier persona que participe en el programa BYOD debe firmar explícitamente sus condiciones de uso.

Pero **las políticas por sí mismas no son suficientes** para evitar las consecuencias del incumplimiento de las normas, ya sea por error, accidente o decisión voluntaria del usuario. Necesitaremos herramientas que nos ayuden a hacer cumplir las políticas, como pueden ser los sistemas de gestión de dispositivos móviles (*Mobile Device Management*, MDM), sistemas de gestión de aplicaciones móviles, etc.

Quien debe participar en la definición de una política BYOD

Como hemos visto hasta ahora, un programa BYOD afecta a muchas áreas de la organización más allá del área de TI. A la hora de crear la política es importante contar con la participación de todas. Muchas organizaciones carecerán de la estructura organizativa necesaria para crear estas políticas y deberán crearla ex profeso para asegurar la gobernanza necesaria para implementar con éxito el programa.

Estas son las áreas que deberían participar en la definición de la política. Según el tamaño de la organización, algunos de estos roles coincidirán en una única persona:

- Representantes de las áreas de negocio y de los usuarios
- Recursos humanos
- Área legal y de regulación
- Área de TI:
  - Seguridad
  - Red
  - Mensajería y comunicaciones unificadas
  - Operaciones de servidor
  - Administración de servicios de TI
  - Desarrollo y mantenimiento de aplicaciones
  - Soporte al usuario

Análisis y gestión del riesgo de la información y la actitud de la organización hacia el riesgo

La seguridad de la información debe ir de la mano de los riesgos de la información. Esto permitirá alinear el área de TI con los objetivos de negocio de la organización.

La tecnología avanza a velocidades vertiginosas, y las amenazas también. Es necesario establecer un marco de referencia adecuado para entender y gestionar estos nuevos riesgos para la organización que están en continua evolución (29). Por ello, se recomienda seguir una estrategia estructurada de gestión del riesgo para afrontar los riesgos de forma sistemática.

En primer lugar, tenemos que diferenciar entre riesgo y seguridad. Podemos ver el riesgo de la información como una parte de la gestión de riesgos corporativos, y la seguridad como el habilitador. El riesgo definiría dónde vamos y la seguridad determinaría el cómo (30). En la Figura 23 podemos ver la relación entre gestión del riesgo y seguridad, así como las principales funciones de cada una.

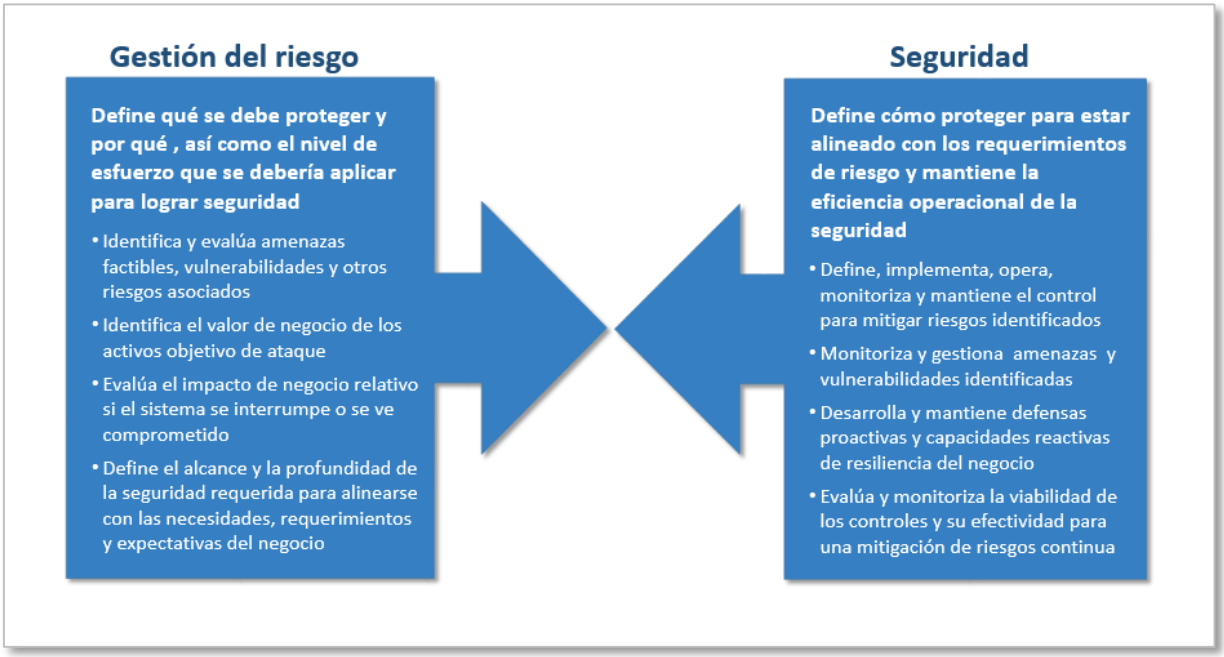


Figura 23. Gestión del riesgo vs. seguridad (31).

Primero, debemos entender la actitud hacia el riesgo de la organización, es decir, el nivel de riesgo que la organización está preparada para aceptar. Examinar a fondo lo que más le importa y por qué.

La actitud hacia el riesgo no es fácil de concretar, cada organización puede tolerar niveles de riesgo diferentes. Sin embargo, es importante que la organización establezca una definición común de sus riesgos y que se prepare en función de la probabilidad y el impacto de las amenazas conocidas. La organización debería definir el máximo nivel de tolerancia al riesgo en cada área de riesgo antes de determinar acciones.

La actitud hacia el riesgo a veces se expresa a través de una "declaración de actitud hacia el riesgo", un documento que sirve de guía a la organización en las labores de gestión de riesgos. Esta declaración debería basarse en las perspectivas y preocupaciones de todas las áreas implicadas, así como en las prioridades y estrategias corporativas actuales.

A continuación, debemos detallar los perfiles de riesgo de la información en la organización que, entre otros, implicará contemplar aspectos como (31):

- decidir y acordar lo que se considera un riesgo aceptable;
- la identificación de todos los activos físicos y lógicos de la organización, manteniendo un inventario preciso de activos, incluyendo aquellos que se acceden o almacenan en dispositivos móviles, (lo que no se conoce no se puede proteger);
- la clasificación de los activos (información pública y confidencial, por ejemplo), para identificar los objetivos y requerimientos de las medidas de control. No todos los recursos tendrán que protegerse de la misma forma ni necesitan accederse o almacenarse en dispositivos móviles;
- definir los incidentes que son significativos (por ejemplo si un incidente implica la pérdida de algunos datos puede no ser significativo para la organización, por lo que el coste de proteger los datos no debería superar el valor de los datos);
- qué se considera una pérdida aceptable;

- priorización de los riesgos;
- análisis realista de amenazas y vulnerabilidades alineadas con el negocio (incluyendo impacto en el negocio y probabilidad de ocurrir);
- el impacto material en el negocio, que puede variar en cada organización, considerando el impacto económico, en la reputación o en el cumplimiento de legislación y normativas;
- el impacto en la cadena de suministro o en el ecosistema de partners y colaboradores;

Para elaborar el perfil de riesgo de la organización en el programa BYOD es necesario conocer muy bien el negocio de la organización, así como el entorno legal y regulatorio en el que se mueve. Por ello, estos perfiles de riesgo deben estar vinculados al análisis y actividades corporativas de gestión de riesgos, y el área de TI deberá trabajar estrechamente con esas áreas.

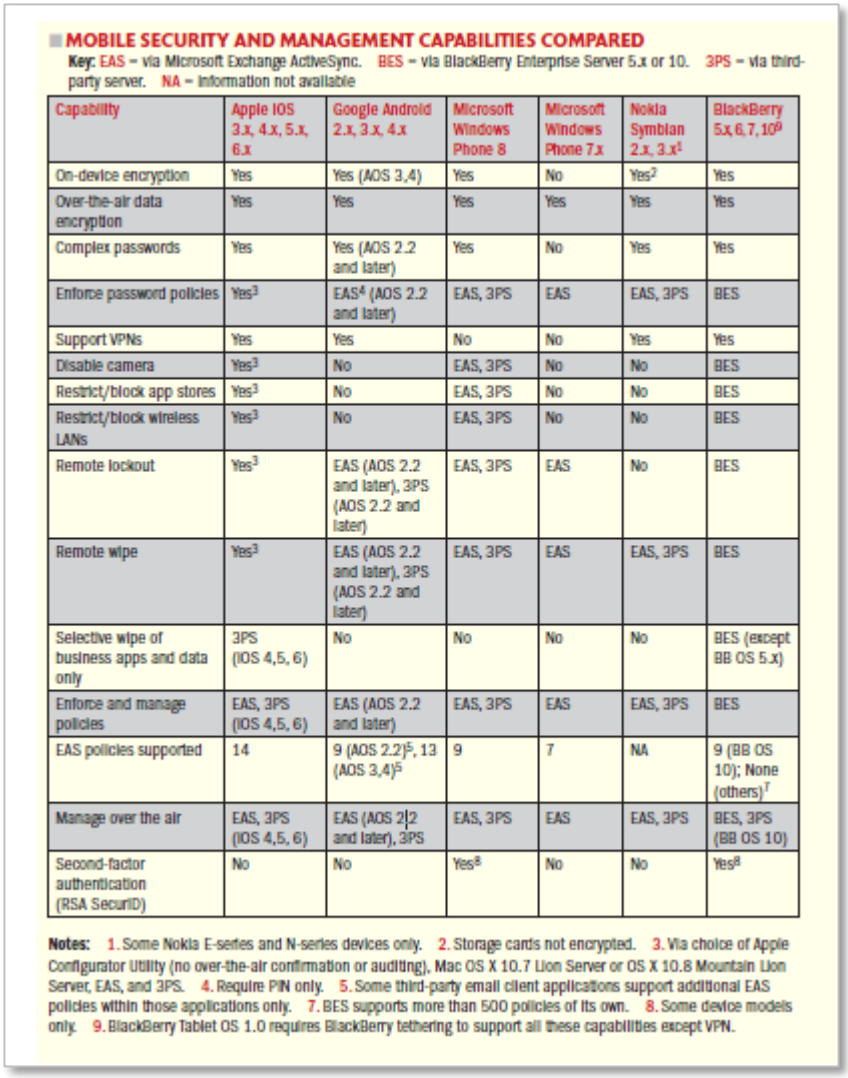
Una vez elaborados los perfiles de riesgo de la información, tanto el área de negocio como el área legal deberían firmarlos. Estos perfiles definirán las medidas a tomar para reducir la probabilidad de riesgos (medidas preventivas), y las acciones a emprender en caso de producirse un incidente (planes de contingencia). Definiremos los requerimientos a nivel tecnología y sistemas de control a implantar en el programa, en base a un enfoque que evalúe las amenazas y alinee las defensas a los riesgos.

Detalle de plataformas, sistemas operativos y dispositivos aceptados en los diferentes grupos de usuarios/roles definidos

Es necesario dejar claro a los usuarios si dentro del programa BYOD se aceptarán todo tipo de plataformas, sistemas operativos y dispositivos, o si, por el contrario, el área de TI sólo dará acceso y soporte a determinados dispositivos. Esta información hay que definirla para cada grupo de usuarios identificado.

El área de TI puede **determinar la lista de dispositivos, sistemas operativos y versiones admitidos** en función de las necesidades de seguridad, control, aplicaciones y soporte de la organización, puesto que las funcionalidades admitidas van a variar mucho según sistema operativo y dispositivo utilizado.

A modo ilustrativo, la Figura 24 muestra una comparativa de funcionalidades de gestión soportadas en diferentes versiones de sistemas operativos móviles. Si la organización va a implementar una solución MDM/EMM, debemos asegurarnos de que los dispositivos aprobados están soportados por el sistema de gestión.



MOBILE SECURITY AND MANAGEMENT CAPABILITIES COMPARED

Key: EAS = via Microsoft Exchange ActiveSync. BES = via BlackBerry Enterprise Server 5.x or 10. 3PS = via third-party server. NA = information not available

Capability	Apple iOS 3.x, 4.x, 5.x, 6.x	Google Android 2.x, 3.x, 4.x	Microsoft Windows Phone 8	Microsoft Windows Phone 7.x	Nokia Symbian 2.x, 3.x[1]	BlackBerry 5.x, 6, 7, 10[9]
On-device encryption	Yes	Yes (AOS 3,4)	Yes	No	Yes[2]	Yes
Over-the-air data encryption	Yes	Yes	Yes	Yes	Yes	Yes
Complex passwords	Yes	Yes (AOS 2.2 and later)	Yes	No	Yes	Yes
Enforce password policies	Yes[3]	EAS[4] (AOS 2.2 and later)	EAS, 3PS	EAS	EAS, 3PS	BES
Support VPNs	Yes	Yes	No	No	Yes	Yes
Disable camera	Yes[3]	No	EAS, 3PS	No	No	BES
Restrict/block app stores	Yes[3]	No	EAS, 3PS	No	No	BES
Restrict/block wireless LANs	Yes[3]	No	EAS, 3PS	No	No	BES
Remote lockout	Yes[3]	EAS (AOS 2.2 and later), 3PS (AOS 2.2 and later)	EAS, 3PS	EAS	No	BES
Remote wipe	Yes[3]	EAS (AOS 2.2 and later), 3PS (AOS 2.2 and later)	EAS, 3PS	EAS	EAS, 3PS	BES
Selective wipe of business apps and data only	3PS (iOS 4,5, 6)	No	No	No	No	BES (except BB OS 5.x)
Enforce and manage policies	EAS, 3PS (iOS 4,5, 6)	EAS (AOS 2.2 and later)	EAS, 3PS	EAS	EAS, 3PS	BES
EAS policies supported	14	9 (AOS 2.2)[5], 13 (AOS 3,4)[5]	9	7	NA	9 (BB OS 10); None (others)[7]
Manage over the air	EAS, 3PS (iOS 4,5, 6)	EAS (AOS 2.2 and later), 3PS	EAS, 3PS	EAS	EAS, 3PS	BES, 3PS (BB OS 10)
Second-factor authentication (RSA SecurID)	No	No	Yes[8]	No	No	Yes[8]

Notes: 1. Some Nokia E-series and N-series devices only. 2. Storage cards not encrypted. 3. Via choice of Apple Configurator Utility (no over-the-air confirmation or auditing), Mac OS X 10.7 Lion Server or OS X 10.8 Mountain Lion Server, EAS, and 3PS. 4. Require PIN only. 5. Some third-party email client applications support additional EAS policies within those applications only. 7. BES supports more than 500 policies of its own. 8. Some device models only. 9. BlackBerry Tablet OS 1.0 requires BlackBerry tethering to support all these capabilities except VPN.

Figura 24. Comparativa de opciones de gestión en diferentes versiones de sistemas operativos móviles (32).

También será necesario definir las condiciones y plazos de actualización de los dispositivos, así como la obligatoriedad de la actualización. Es posible que el área de TI quiera estudiar si nuevas versiones de los sistemas operativos móviles son compatibles con las aplicaciones corporativas instaladas en los dispositivos o con el sistema MDM antes de permitir que los usuarios actualicen sus dispositivos. Del mismo modo, es posible que se descubra una vulnerabilidad de seguridad que se corrige con una actualización y que el área de TI requiera que los usuarios actualicen de inmediato sus dispositivos. Igualmente será necesario especificar en la política las consecuencias de no seguir la pautas establecidas por el área de TI (por ejemplo, no disponer de soporte técnico si no se usa un hardware de dispositivo que cumpla los mínimos requerimientos, interrupción del acceso a la red si no se cumplen las condiciones de seguridad, etc.).

Estas especificaciones deben revisarse periódicamente por el área de TI.

Controles de seguridad y gestión

En la parte más técnica de la política deberemos especificar cuestiones como los requerimientos para el acceso a la red, las configuraciones de seguridad recomendadas y obligatorias, los controles de seguridad y gestión que se aplicarán sobre el dispositivo y los datos, (incluyendo el posible reseteo o

borrado del dispositivo), la monitorización y auditorías que se efectuará sobre el dispositivo, las aplicaciones permitidas y no permitidas, las posibles restricciones en el acceso a datos corporativos, etc.

Aspectos relacionados con el área de RRHH, como contenido y remuneraciones

Un capítulo importante a abordar a la hora de desarrollar la política BYOD es la definición de **Usos Aceptables** dentro del programa. Aunque el dispositivo sea propiedad del empleado, la visualización de contenido inapropiado en el mismo puede ser contrario a las políticas de la organización. Será conveniente por tanto definir qué se considera un uso apropiado del dispositivo en el entorno de trabajo, así como definir qué se considera entorno de trabajo.

Otro tema que también es importante definir claramente son las **responsabilidades y derechos** de los participantes. Si, por ejemplo, el usuario tiene que comprometerse a reponer el dispositivo en un determinado plazo o a cumplir unas determinadas normas de seguridad, tiene que entender y aceptar explícitamente esas responsabilidades. Del mismo modo, si la organización se compromete a dar determinado nivel de soporte técnico o si va a realizar algún tipo de **aporte económico** al empleado como parte del programa, es necesario definir claramente las condiciones (quién es elegible, condiciones de participación, cantidades, forma y periodo de pago, tributación aplicable, etc.).

El área de Recursos Humanos también debería crear un **programa de formación y comunicación** de los detalles del programa a los usuarios. Si ahora parte de la responsabilidad de protección de la información de la organización va a recaer en los usuarios, es necesario concienciarles sobre la importancia de esta protección así como dotarles de herramientas y conocimientos sobre cómo hacerlo.

Así mismo, trabajando con el área legal y de regulación, también deben establecerse mecanismos para asegurar que los empleados participantes en el programa conocen las **condiciones de privacidad y posibles implicaciones legales** que puedan derivar del programa, y que estos reconocen la aceptación de la política según requiera la legislación local aplicable.

Consideraciones legales y sobre privacidad al planificar una política BYOD

El hecho de que los empleados accedan a recursos corporativos desde dispositivos que están fuera de control del departamento de TI puede plantear diversas cuestiones legales. Los recursos corporativos incluyen ficheros con información sensible, así como el acceso a redes, aplicaciones y servidores. La integridad de estos recursos es primordial para el día a día de las operaciones de TI.

Desde el punto de vista legal no todos los aspectos de la consumerización están cubiertos aun, hay muchos asuntos legales vinculados a BYOD que aún no tienen resolución. Esto deja en manos del área de TI la tarea de definir una estrategia global de BYOD que permita a los usuarios ser productivos sin cruzar líneas legales.

Las políticas y acuerdos de uso son herramientas básicas para establecer un entendimiento mutuo entre la dirección, el área de TI y los usuarios, sobre las reglas a seguir y sobre cómo hacer que se cumplan.

Algunos puntos a considerar son:

- **Uso personal versus uso laboral**. Puede incurrirse en horas extras y otras consideraciones reflejadas en leyes, normativas y convenios que regulen horarios y salarios. Por ejemplo, si los empleados que trabajan por horas usan su teléfono fuera de horas de trabajo, podrían considerarse horas extra que la empresa tendría que pagar, dependiendo de las tareas específicas que realizasen.
- **Privacidad.** La organización debería evaluar cómo usa las tecnologías de seguimiento y control, así como la forma en que acceden a la información personal de los usuarios almacenada en los dispositivos, porque pueden surgir problemas de invasión de la privacidad de los empleados. Las leyes de privacidad en lo que respecta a BYOD todavía son imprecisas, por eso la línea divisoria entre gestionar un dispositivo de un usuario e invadir su privacidad personal es muy difusa. Además, si los usuarios descargan datos personales de clientes en los dispositivos, la organización deja de tener control sobre donde están los datos que tiene obligación de proteger y de las copias que se han podido hacer.
- **Responsabilidad**. Hay muchas consideraciones a este respecto. Por ejemplo, si el empleado usa el dispositivo mientras conduce, la empresa podría pasar a ser parte en un proceso legal si un empleado que está usando el teléfono con fines laborales tiene un accidente. O, si la empresa descubre algún comportamiento ilegal en el uso del dispositivo del empleado (por ejemplo, imágenes pederastas), ¿debería denunciarlo?

Otro punto que las políticas BYOD deben contemplar es cómo gestionarán los empleados la información en un dispositivo de su propiedad durante un caso legal. Puesto que el dispositivo es propiedad del empleado, cuando la empresa se enfrenta a un incidente legal (o el propio trabajador es objeto de una investigación), puede ser difícil obtener acceso al dispositivo. Si es necesaria la recopilación y preservación de datos la incapacidad de acceder y poseer un dispositivo físico puede ser extremadamente perjudicial. Por ejemplo, si una organización no es capaz de conservar los datos que pueden constituir evidencia en litigio, podría enfrentarse a sanciones judiciales. Esto también puede causar problemas a los propios individuos que probablemente (al menos temporalmente) no puedan utilizar su dispositivo personal mientras dure la investigación. Además, la captura de datos e imágenes del dispositivo personal implica posibles problemas de privacidad.

Por otro lado, es necesario considerar cómo las herramientas tradicionales que mantienen seguros los activos corporativos pueden tener consecuencias problemáticas cuando se aplican a datos personales. Servicios como el de monitorización de acceso a sitios web o la monitorización de las comunicaciones, son normalmente aceptados cuando se usa un dispositivo de la organización, así como controles habituales como la encriptación o el borrado de datos. Pero ¿deberían aplicarse esas mismas medidas en un dispositivo personal cuando el empleado está fuera de horario laboral? ¿Y qué sucede cuando los datos incluyen información personal? Por ejemplo, si se pretende utilizar servicios de geolocalización para ayudar a encontrar dispositivos perdidos, los empleados deben ser notificados con anterioridad. De igual forma, si se van a monitorizar las comunicaciones de los empleados, deben estudiarse las posibles implicaciones de hacerlo.

Expertos en el área legal de tecnología (33) sugieren que para mitigar las trabas legales del BYOD es recomendable establecer políticas que se centren en los datos en vez de en los dispositivos. Las soluciones tecnológicas que permiten establecer contenedores separados para los datos personales y los corporativos son especialmente útiles. También se debería limitar el alcance del BYOD o establecer políticas específicas para aquellos usuarios que necesitan acceder a información muy sensible o que viajan mucho. El Information Commissioner Office (ICO), el organismo público encargado de la protección de los datos personales en el Reino Unido, ha publicado una útil guía (34)

para la protección de datos personales en entornos BYOD. La guía puede descargarse de forma gratuita en su página web:
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod.

Si las organizaciones tratan de imponer políticas demasiado rígidas o no realistas, los empleados no las aceptarán o, lo que es peor, buscarán formar de esquivarlas siempre que puedan. Todas las partes involucradas – recursos humanos, legal, regulación, TI, finanzas, departamentos de operaciones y empleados – deberían consultarse para la elaboración de las mismas. Y, en cualquier caso, deberían prevalecer el sentido común y un correcto asesoramiento especializado en aspectos legales del BYOD.

¿Por qué es importante la privacidad en los proyectos BYOD?

En primer lugar, los empleados odian la seguridad invasiva. Los controles estándar de seguridad que las organizaciones utilizan para proteger los activos corporativos pueden tener consecuencias imprevistas cuando se aplican (sin ninguna modificación) a un dispositivo personal de un empleado. Estas medidas potencialmente invasivas influyen negativamente en el apoyo de los empleados a los proyectos BYOD, minando una de las razones por las que las organizaciones se deciden a adoptar este tipo de iniciativas. Una encuesta reciente (35) refleja los siguientes datos:

- el 82% de los usuarios consideran una invasión de su privacidad que se pueda hacer seguimiento de su teléfono
- el 76% no daría a sus organizaciones acceso para ver las aplicaciones instaladas en su dispositivo personal
- el 75% no permitiría a su organización instalar una app que le permitiera localizarlo a cambio de acceder a recursos corporativos
- el 82% están preocupados o muy preocupados por el hecho de que sus empresas hagan seguimiento de su actividad en Internet durante su tiempo personal
- al 86% les preocupa que sus datos personales (fotos, correo, música, etc.) puedan ser borrado sin su autorización

Por otro lado, la regulación en materia de privacidad es cada vez más restrictiva, especialmente en algunos países, por lo que el incumplimiento de las medidas de protección de la privacidad de los empleados puede significar importantes sanciones para la organización. Ese es el caso de la Comunidad Europea, donde la Comisión Europea en su nueva propuesta de Reglamento Europeo contempla sanciones que pueden llegar hasta el millón de euros o, si se trata de una empresa, hasta el 2% de su volumen de negocios anual a nivel mundial (36).

El consentimiento informado es fundamental

Hay algunos aspectos claves en torno a la privacidad que conviene abordar desde un principio. El primero es el **consentimiento informado** de la forma en que la organización va a acceder a un dispositivo propiedad de un empleado. Es fundamental asegurarse de que cuando se vaya a acceder a cualquier información en dispositivos propiedad de empleados, se hace con el conocimiento y consentimiento del empleado. Idealmente, una política BYOD debe hacer que estas notificaciones sean obligatorias y sin ambigüedad.

Por otro lado, deben pensarse las acciones disciplinarias que se tomarán si se descubriera alguna infracción. ¿Qué sucedería si la organización descubre un conflicto de intereses? ¿Qué sucedería si el empleado accede a contenidos ilegales o piratas? ¿Bajo qué circunstancias la organización debería informar a las fuerzas de seguridad?

Colaboración del área de TI con al área Legal, de Regulación y de Recursos Humanos

Las políticas BYOD pueden llevar en algunas ocasiones a las organizaciones a un territorio legal desconocido. Hay consideraciones éticas, de cumplimiento de normativas y regulación, y potencialmente legales en la monitorización de comunicaciones personales y en el acceso/modificación de datos personales. Por ello, como se ha comentado con anterioridad, es necesario involucrar a un equipo operativo mucho más amplio del habitual cuando se toman decisiones vinculadas con las TI, que incluya al área Legal, de Regulación y de Recursos Humanos para la planificación de la política BYOD.

Soporte al usuario

El soporte al usuario es un elemento crítico del programa. Si no se define adecuadamente puede ser una fuente de insatisfacción para los usuarios y de costes no previstos para la organización. Es conveniente precisar qué pueden esperar los usuarios y a partir de qué punto es responsabilidad suya gestionar el soporte.

Se puede delimitar un tipo y nivel de soporte para cada grupo de usuarios dentro del programa: por ejemplo, usuarios para los que es menos crítico el uso de herramientas móviles se puede ofrecer opciones de auto-ayuda online a través de wikis y fórums, y para el equipo directivo se puede definir un nivel de soporte Premium.

Ejemplo de política BYOD

Una política BYOD es específica de cada organización, pero leer las que otras organizaciones están usando puede ayudar a dar los primeros pasos para definir la nuestra.

En el Anexo 1 se incluye como referencia un sencillo ejemplo de plantilla de política publicada por el fabricante de soluciones MDM, Good Technology. El documento puede descargarse de Internet en formato PDF en la web del fabricante: http://www.welcometogood.com/byod/byod_policy_wp.pdf.

7.2. Definición del equipo de trabajo

A la hora de definir quién debe participar en la implantación del programa BYOD, debemos recordar que más que un proyecto de TI, el BYOD es un proceso de gestión del cambio que impactará en toda la empresa.

Al igual vimos en la definición de la política BYOD (ver sección 7.1), va a ser necesaria la colaboración de diferentes áreas de la empresa durante todo el proceso de implantación. Podemos crear un equipo de trabajo con representantes de las áreas que participaron en la definición de la política, sin olvidarnos de contar con los usuarios, pues su feedback será esencial durante todo el proceso.

7.3. Definición de la estrategia de seguridad en base a los riesgos definidos en la organización

La seguridad es la primera causa de preocupación en los programas BYOD. Para poder disfrutar plenamente de los beneficios que nos puede ofrecer debemos definir cuidadosamente una estrategia de seguridad que nos permita mitigar sus riesgos.

Es recomendable definir una estrategia inteligente que se adapte a los riesgos identificados en nuestra organización y a su actitud hacia el riesgo, convirtiendo los riesgos encontrados a controles de seguridad a implementar (ver apartado " *Análisis y gestión del riesgo de la información y la actitud de la organización hacia el riesgo"*). No podemos proteger todo de la misma manera, ni podemos proteger todos los activos. Los perfiles de riesgo definirán los requerimientos a nivel tecnología y sistemas de control a implantar en el programa, en base a un enfoque que evalúe las amenazas y alinee las defensas a los riesgos.

Figura 25. Seguridad inteligente alineando las defensas a los riesgos (37).

En cualquier caso, debemos implementar una estrategia que nos permita descubrir las posibles incidencias y reaccionar ante ellas con rapidez. Según datos de Verizon (37), los atacantes actúan muy rápido, el 84% de las intrusiones ocurren en minutos, pero las organizaciones atacadas no. El 66% de las brechas permanecen sin ser descubiertas durante meses, y muchas veces ni siquiera es la propia organización quien las descubre (en el 69% de los casos la brecha es descubierta por terceros).

La solución que mejor se encaja en una organización concreta es única, puesto que se adapta a los requerimientos, tecnología y entornos específicos de esa organización.

Rompiendo con conceptos de seguridad móvil tradicionales, un enfoque integrado considera la seguridad BYOD en tres niveles (38):

- Seguridad en el dispositivo
- Protección de los datos y el tráfico
- Protección de la red

Seguridad en el dispositivo

Proteger un dispositivo móvil puede ser una tarea sorprendentemente difícil, especialmente en programas BYOD. Las herramientas y controles de seguridad que son habituales en entornos corporativos de PCs y desktops controlados por el área de TI, no suelen estar disponibles para estos dispositivos de forma nativa. Por el contrario, requieren que los dueños de los dispositivos instalen

herramientas específicas y modifiquen las opciones de seguridad de los sistemas operativos y aplicaciones. Este proceso es complejo para los usuarios y no es realista esperar que lo realicen ellos solos sin la intervención de TI.

Otro factor que añade complejidad es la proliferación de modelos y versiones de dispositivos, cada uno con diferentes características de seguridad y potenciales vulnerabilidades.

Las herramientas que utilizan las áreas de TI para la gestión de la seguridad a nivel de dispositivo son:

- Enterprise Mobility Management (EMM)

  EMM es un término general que hace referencia a soluciones que implican todo lo relacionado con la gestión de dispositivos móviles y componentes relacionados (como redes wireless). Las soluciones EMM van más allá de la seguridad de la información, incluyendo gestión de aplicaciones móviles, gestión de inventario y gestión de costes, aunque la seguridad es una parte importante.

  Estas soluciones se estudian más a fondo en la sección 7.4 más adelante.

- Software Mobile Device Management (MDM)

  En los últimos años los programas MDM se han convertido en la solución más popular para la gestión de dispositivos móviles. Al igual que los EMM, sus funcionalidades van más allá de la seguridad. Además, conforme la tecnología MDM está madurando, los fabricantes están ampliado mucho el ámbito de sus funcionalidades. En la sección 7.4 se analizan en más detalle, pero aquí queremos destacar sus principales funcionalidades en el área de la seguridad, que pueden agruparse en tres categorías:

  - Configuración remota de la seguridad. Permite al área de TI la imposición de políticas de seguridad en los dispositivos a través de Internet, y la monitorización continua del cumplimiento de dichas políticas por el dispositivo. Esto permite establecer mecanismos automáticos para restringir o impedir el acceso a los recursos corporativos a dispositivos potencialmente inseguros.

    Hay muchas configuraciones de seguridad aplicables a BYOD, entre otras:

    - Restricción del acceso al hardware, que impediría por ejemplo copiar información localmente
    - Restricción del acceso al software, que impediría el uso de información corporativa en dispositivos con aplicaciones no aprobadas previamente
    - Encriptado de datos corporativos almacenados en el dispositivo, para evitar que sean accesibles a aplicaciones no autorizadas
    - Exigencia de autenticación, como por ejemplo autenticación multifactor, para poder acceder a datos y aplicaciones corporativas
    - Restricción de aplicaciones
  - Borrado o bloqueo remoto. Permitiría bloquear o borrar un dispositivo perdido o robado.
  - Gestión de aplicaciones móviles. Algunas de sus principales características incluyen:
    - *Sandboxing* de apps, que aísla la aplicación en un determinado contexto
    - Distribución de apps, que permitiría gestionar la instalación de determinadas apps corporativas en función de perfiles de seguridad definidos por IT, o la desinstalación

remota de aplicaciones (por ejemplo si el usuario cambia de puesto o deja la organización)

- Distribución de actualizaciones de apps, específicamente distribución de parches y nuevas versiones de aplicaciones y sistemas operativos de los dispositivos
- *Blacklisting*, que permite elaborar listas de aplicaciones no autorizadas en los dispositivos

- Controles de seguridad adicionales

  Hay muchos otros controles de seguridad relacionados con la seguridad en el dispositivo, entre otros:

  - Firewalls host-based. Tradicionalmente los smartphones y tabletas no implementaban firewalls personales puesto que confiaban en los firewalls de red (como los de la red móvil) para evitar el acceso no autorizado. Puesto que ahora los dispositivos se conectan frecuentemente a redes WiFi tiene sentido implementar niveles adicionales de seguridad. Este tipo de soluciones son bastante novedosas por lo que la oferta en el mercado puede no ser muy amplia.
  - Software antivirus o antimalware. Como en el caso anterior, son soluciones relativamente nuevas. Es importante testear cómo interactúan con dispositivo específicos puesto que pueden degradar su rendimiento.
  - Seguridad para webs móviles. Muchos navegadores incluyen controles de seguridad que pueden contribuir a mantener la seguridad del dispositivo, como por ejemplo la protección antiphishing.

Protección de los datos y el tráfico

Debemos extender la seguridad más allá del dispositivo para incluir los datos cuando están almacenados en el dispositivo, cuando se transmiten por las redes y cuando se usan, tanto dentro como fuera del control de la organización. Proteger los datos en cada uno de esos estados no es una tarea trivial, requiere controles de seguridad específicos.

- Encriptación del almacenamiento de datos

  Las tecnologías de encriptación protegen la confidencialidad de los datos alterándoles mediante el uso de un algoritmo criptográfico y una clave de encriptación secreta. Hay tecnologías que usan una misma clave para encriptar y desencriptar, y otras utilizan dos claves diferentes (una pública y otra privada). Es importante tener en cuenta que, dada la cantidad de herramientas gratuitas disponibles para romper la encriptación, una encriptación débil no aporta demasiada seguridad.

  La mayoría de dispositivos BYOD no implementa por defecto encriptación segura de los datos almacenados y transmitidos, aunque muchos de esos dispositivos si la soportan de forma nativa. Sólo es necesario configurarla.

  - Claves criptográficas. En importante tener en cuenta que, aunque se elijan claves seguras para la encriptación, estas pueden volverse débiles con el tiempo (por ejemplo, porque los atacantes descubran vulnerabilidades en el algoritmo de encriptación). Además, los avances en el hardware hacen que claves que hace 10 años no eran descifrables, ahora pueden serlo

fácilmente mediante ataques de fuerza bruta. Por ello es fundamental sustituir las claves periódicamente.

- Encriptación de almacenamiento. Aunque tienen una base común, las tecnologías de cifrado de almacenamiento y de tráfico son diferentes. El cifrado de almacenamiento se centra en proteger datos en reposo. La Figura 26 muestra los tres tipos principales de encriptación de almacenamiento.

Tipo de cifrado	Como funciona	Escenarios de uso
Cifrado de disco	Esta tecnología encripta todos los datos en un medio. Partes individuales de información se descifran cuando es necesario.	Este enfoque es adecuado en dispositivos especialmente susceptibles de robo o pérdida.
Cifrado de fichero	Esta tecnología encripta ficheros individuales en un dispositivo. Al descifrar un fichero el resto permanece cifrado.	Este enfoque es adecuado en dispositivos que almacenan información con diferentes niveles de sensibilidad.
Cifrado de disco virtual	Esta tecnología es un híbrido del cifrado de disco y de fichero. Crea un contenedor virtual encriptado que aloja todos los ficheros sensibles.	Este enfoque es adecuado en despliegues corporativos masivos que utilizan tecnología MDM.

Figura 26. Tecnologías de cifrado de almacenamiento (38).

- Utilización de múltiples tecnologías de encriptación de almacenamiento. Es posible utilizar diferentes tecnologías de cifrado de forma simultánea. Por ejemplo, un usuario puede utilizar cifrado de disco para conseguir una protección básica del dispositivo y cifrado de disco virtual (a través del MDM) para añadir seguridad a los datos corporativos.
- Almacenamiento cloud personal. Cada vez es más habitual que los usuarios utilicen servicios cloud de almacenamiento (tipo Dropbox, SkyDrive, etc.). Este almacenamiento supone un riesgo para la organización puesto que los datos corporativos podrían acabar en un servicio del que el área de TI no tiene conocimiento, perdiendo así el control de los datos corporativos y de su seguridad. Algunas soluciones MDM permiten restringir la copia de datos corporativos a este tipo de servicios en los dispositivos BYOD mientras que permiten que el usuario si pueda almacenar sus datos personales.

▪ Encriptación del tráfico

Las tecnologías de encriptación de transmisión de datos más usadas son:

- Encriptación del tráfico a nivel de red. Normalmente se implementa como una red privada virtual (VPN). Para el caso de dispositivos que se conectan a una red corporativa, dichas VPNs suelen utilizar arquitecturas host-to-gateway. El dispositivo establece su propia conexión con un gateway VPN centralizado y se autentica con el gateway en nombre del usuario. El gateway es el punto de cifrado-descifrado para todas las conexiones VPN y proporciona túneles de cifrado seguros por los que circula el tráfico de red.

  En el dispositivo un cliente VPN (que normalmente ya incorpora el sistema operativo), permite la conexión con el gateway.

  La cuestión que normalmente plantea la solución VPN es qué tráfico debe enviarse por el túnel encriptado, puesto que enviar todo el tráfico generado en el dispositivo puede consumir demasiado ancho de banda y ralentizar la conexión. Además pueden surgir cuestiones relativas a la privacidad de los datos personales del usuario puesto que el tráfico VPN está monitorizado.

- Encriptación del tráfico a nivel de aplicación. Este cifrado puede utilizarse cuando el tráfico a proteger está relacionado con aplicaciones concretas. El ejemplo más común son las aplicaciones web que usan el protocolo *Hypertext Transfer Protocol* para comunicarse. El HTTP puede protegerse con el protocolo SSL (*Secure Sockets Layer*) o el TLS (*Transport Layer Security*), generando lo que se conoce como HTTP Seguro (HTTPS).

  El HTTPS es una solución ideal cuando hay que proteger sólo tráfico web, evitando la complejidad de implementar una VPN y mantener los clientes VPN en los dispositivos.

- Autenticación multifactor

  La autenticación multifactor implica dos o más tipos de factores de autenticación (normalmente, una combinación de algo que el usuario sabe, algo que tiene y algo que es). Un ejemplo de autenticación multifactor es el uso de un token criptográfico (hardware o software). Un atacante debería robar el token y conseguir el PIN para poder autenticarse y lograr el acceso.

  En programas BYOD, se pueden utilizar factores de autenticación "algo que tienes" virtuales (es decir, software), combinados con certificados digitales u otras formas de identificadores digitales almacenados en el dispositivo. Este modelo es más cómodo para los usuarios pero supone un mayor riesgo para la organización puesto que, si se roba el dispositivo, se roba con él un factor de autenticación. Además es necesario que el dispositivo del usuario esté protegido con un factor de autenticación (PIN o contraseña). El PIN autentica al usuario ante el dispositivo y la autenticación multifactor autentica al usuario ante la organización.

- Software de Prevención de Fuga de Datos (DLP)

  Los programas DLP (*Data Loss Prevention*) son una tecnología emergente estratégica para proteger la información sensible de la organización frente a fugas. Analizan el contenido de los datos identificando características que lo identifican como sensibles (por ejemplo, número de DNI o tarjeta de crédito).

  Los programas DLP pueden monitorizar tres tipos de información sensible: información almacenada, información transmitida e información manipulada por acciones en el propio dispositivo (como copiar y pegar). La organización puede disponer de software DLP instalado en los servidores y redes, pero la solución DLP está incompleta a menos que también tenga software DLP en los dispositivos BYOD. De esta forma se puede identificar información corporativa sensible en los dispositivos, monitorizar su uso o transmisión e impedir las acciones inapropiadas (como copiar información sensible de un documento y pegarla en otro no protegido, o enviarlo a un correo externo a la organización).

  El software DLP puede identificar los datos sensibles de diferentes formas, las técnicas más habituales suelen ser las que se describen a continuación. Normalmente los DLPs utilizan una combinación de ellas.

  - Identificación de patrones. El DLP busca palabras clave, como "DNI", o patrones de caracteres, como "XX-XXX-XXX-Y" donde X es un numero e Y una letra.
  - Fingerprinting. Esta técnica implica el uso de criptografía para generar hashes para elementos de información sensible. Si se encuentra un hash igual en algún otro sitio indica que se ha realizado una copia de información sensible.
  - Análisis estadístico. Este enfoque utiliza técnicas estadísticas avanzadas para analizar las características de los documentos que contienen información sensible. Documentos con características similares se investigan como posible duplicación de datos.

- Entrega segura de aplicaciones

  Puesto que la gestión de la información sensible que hay en los dispositivos implica tantos controles de seguridad, muchas organizaciones tratan de reducir la información sensible en ellos. Una opción es la utilización de técnicas de entrega segura de aplicaciones, que permite que la aplicación (y sus datos) resida en un datacenter centralizado en vez de alojarse en el dispositivo. Sólo existe transmisión de la imagen de la aplicación y los datos, lo que minimiza la exposición de información sensible.

  El principal inconveniente que tienen estas técnicas es que implica modificar la arquitectura de las aplicaciones, lo cual no siempre es posible en aplicaciones comerciales. Con el incremento vertiginoso de la movilidad en los entornos corporativos, cada vez son más los fabricantes que ofrecen sus productos con interfaces de cliente basados en web.

Arquitectura blindada: Protección de la red

Hasta ahora hemos hablado de la seguridad en los dispositivos permitidos en el programa BYOD, y de la seguridad de los datos que esos dispositivos acceden y usan, ya sean transmitidos o estén almacenados localmente. Hay otra dimensión en la estrategia de seguridad BYOD, salvaguardar cualquier red de la organización que transporte trafico BYOD. Si esas redes nos son seguras, los atacantes podrían "pinchar" la red.

Otro componente defensivo es la monitorización continua de la red de forma que se pueda reaccionar rápidamente si se realiza un ataque o hay violación de alguna política. La violación de las políticas puede ocurrir de forma accidental (por ejemplo, si un usuario se confunde de red al intentar conectarse) o de forma intencionada (por ejemplo, si un usuario no permite la instalación de una actualización de seguridad en su dispositivo e intenta conectarse a la red corporativa).

Una solución proactiva requiere una combinación de protección de las redes y monitorización continua de la actividad en esas redes, de forma que los responsables de TI puedan hacer un seguimiento de cerca del uso del BYOD.

- Arquitecturas wireless seguras

  Uno de los riesgos del BYOD proviene de la conexión a las redes internas de la organización de dispositivos personales de los empleados. Esto puede comprometer esas redes (y los ordenadores e información que hay en ellas) al exponerlas a un dispositivo personal infectado o inseguro.

  Generalmente es recomendable crear segmentos de red separados para el acceso únicamente de dispositivos BYOD. Al tener redes segregadas se puede separar el trafico BYOD del resto de tráfico en las infraestructuras de la organización. Además, una red segregada se puede proteger y monitorizar completamente de forma más sencilla que una red que contiene tráfico mixto de dispositivos personales y corporativos.

  La topología se puede estructurar de forma que los dispositivos en la red BYOD puedan contactar cualquier host externo pero solo determinados servidores internos, como los servidores de correo. Además se pueden configurar políticas de red que prohíban que usuarios BYOD contacten directamente hosts internos u otros dispositivos de la red local, lo que impediría que un dispositivo comprometido atacase a otros dispositivos o servidores internos

  Normalmente la red segregada BYOD será una red wireless, que debe residir fuera del perímetro de la red de la organización y de los firewalls corporativos. Esta red debería proporcionar sólo

un acceso básico a los recursos de la organización (al igual que si los usuarios BYOD estuviesen conectados a una red externa conectada a Internet).

Si la organización proporciona además acceso temporal a visitantes, debería tener una red wireless independiente para este propósito, de forma que no se mezcle el trafico invitado con el trafico BYOD ni con el tráfico de dispositivos corporativos.

Otras consideraciones de seguridad especiales para establecer redes wireless BYOD son:

- Seguridad de los puntos de acceso wireless. Las redes wireless son especialmente sensibles a ser "pinchadas". Con antenas especiales un atacante podría interceptar las señales a una distancia considerable. Incluso un dispositivo móvil corrupto podría configurarse para interceptar las comunicaciones wireless. Para proteger la red, deberían usarse protocolos de encriptación wireless seguros como el WPA2 (*Wi-Fi Protected Access 2*), y evitar el uso de protocolos que se saben poco seguros como el WPA (*Wi-Fi Protected Access*) o el antiguo WEP (*Wired Equivalent Privacy*).

  Los puntos de acceso wireless deberían configurarse para permitir sólo comunicaciones con protocolos seguros, deshabilitando la posibilidad de usar otros protocolos si un dispositivo o punto de acceso en la red no los soporta.

  Otro tema a considerar sobre los puntos de acceso wireless es su seguridad física. Si se encuentran situados en lugares fácilmente accesibles podrían sufrir ataques físicos (por ejemplo, podrían ser reseteados para que vuelvan a la configuración de fábrica que elimina las configuraciones específicas de seguridad).
- Autenticación del dispositivo. En algunas circunstancias puede ser aconsejable implementar autenticación de los dispositivos. La autenticación que se basa en la dirección MAC del dispositivo no es una opción segura. Actualmente existen alternativas como el uso del protocolo PEAP (*Protected Extensible Authentication Protocol*), o el EAP-TLS (*Extensible Authentication Protocol Transport Layer Security*) que requiere un certificado en el dispositivo para acceder a la red. Nuevos estándares como el EAP-TLSv2 (*Extensible Authentication Protocol Transport Layer Security version 2*), permitirá autenticación 2-factor en redes 802.1x.
- Sistemas WIDP (*Wireless Intrusion Detection and Prevention*). Los sensores de los sistemas de detección y prevención de intrusiones monitorizan todas las comunicaciones de la red wireless dentro de su rango y las analizan en busca de ataques wireless, violaciones de políticas wireless y otros problemas. Otra función importante es la detección de redes wireless no autorizadas. Una técnica utilizada por los atacantes es introducir un punto de acceso falso con la esperanza de que los usuarios se conecten a él. Los sistemas WIDP permiten detectarlos y alertar a los administradores de la red.

▪ Soluciones de Control de Acceso a la Red (NAC)

Una solución NAC (*Network Access Control)* regula el acceso de los dispositivos a la red de la organización. El NAC examina las características de seguridad del dispositivo cada vez que intenta conectarse a la red BYOD. Si las características de seguridad cumplen las políticas de seguridad, al dispositivo se le permite el acceso a la red wireless y a los recursos autorizados. Por el contrario, si el dispositivo no cumple las políticas de seguridad corporativas se le niega el acceso, o se desvía a una red de "remediación" para que pueda aplicar las acciones correctivas necesarias.

Hay muchas características de seguridad del dispositivo móvil que la solución NAC puede revisar, como:

- Configuración de las opciones de seguridad
- Parches y actualizaciones del sistema operativo y aplicaciones
- Software antivirus
- Firewall host-based (firewall personal)

Hay soluciones MDM que implementan funcionalidades NAC, lo que permite implementar programas BYOD con una protección de acceso más potente y con opciones de control más granulares.

- Monitorización continua

  Finalmente, es importante implementar también una monitorización continua del proceso de auditoría de la seguridad de la red o los dispositivos, de forma que se pueda reaccionar rápidamente si se realiza un ataque, hay violación de alguna política, o algún otro problema.

  La monitorización permite la detección temprana de incidencias y evita que una incidencia de seguridad se extienda inadvertidamente en el tiempo. En el contexto del BYOD, la monitorización de la actividad en la red generada por dispositivos personales va a permitir detectar si hay alguna actividad maliciosa o incluso inapropiada (como descarga de contenido pirata o pornográfico) y detener esos comportamientos.

7.4. Implementación de la gestión y control del programa BYOD

Integración en los modelos de Gobernanza y Gestión de los Servicios TI (ITSM)

La introducción de un programa BYOD puede enturbiar los procesos de Gobernanza y Gestión de Servicios TI establecidos en la organización. El planteamiento del programa BYOD de una forma estructurada y sistemática contribuirá a su éxito, por lo que los responsables de TI deberían integrar estos procesos dentro de los modelos de Gobernanza o Gestión de Servicios TI (ITSM) basados en estándares y marcos de referencia (39) (40).

Además de las cuestiones ya planteadas sobre la gestión de riesgos, hay otros aspectos del BYOD que impactan en otros procesos centrales del ITSM como gestión de incidentes, cambio, soporte y acuerdos de nivel de servicios (SLAs, *Service Level Agreements*).

No hay que olvidar que el BYOD no son sólo dispositivos, sino también aplicaciones, procesos y la experiencia global que tienen los usuarios. Aquí es donde puede ayudar, por ejemplo, el marco de referencia para la gestión de servicios ITIL o el marco de referencia para la gobernanza de TI, COBIT. Se podría pensar que ITIL y la Gestión de Servicios sólo se puede aplicar a plataformas estáticas pero, independientemente del tipo de plataforma, al final todo se reduce a la gestión de riesgos.

El BYOD añade un nivel de complejidad a los temas que las buenas prácticas tratan de gestionar, por ejemplo, ajustar un estándar corporativo para disminuir los costes de utilización y mejorar la seguridad, disminuyendo la vulnerabilidad y riesgo para el negocio. Afectará a todos los pasos del

ciclo de vida del marco ITIL, como la estrategia del servicio, el diseño del servicio, y la transición u operación del servicio.

Deberemos incluir el "BYOD como servicio" como parte del catálogo de servicios Por ejemplo, la estrategia del servicio debe considerar el escenario de adopción de BYOD en la organización (ver la sección 6 para más información); en el apartado de soporte, se deben definir de forma clara los SLAs de las cosas a las que se da soporte en un dispositivo propiedad del usuario y a las que no; a la hora de planificar la capacidad de los sistemas se tienen que tener en cuenta la infraestructura necesaria para gestionar los dispositivos personales, etc.

En definitiva, cada uno de los procesos y políticas ITSM deben ser modificados o ampliados, pero el uso de un buen marco de referencia como ITIL puede acomodar la gestión del BYOD.

En el área más específica de la seguridad de la información se puede utilizar otros marcos de referencia como:

- *'COBIT 5 for Information Security'* de ISACA, que proporciona pautas para implementar medidas para la seguridad de la información en el marco de referencia para la gobernanza y prácticas de gestión de la tecnología de la información, COBIT 5.
- ISO 27000x. El standard internacional para las prácticas de seguridad de la información. Utiliza un enfoque basado en riesgos para priorizar el énfasis en la seguridad y contiene estrategias prácticas de control de datos.

Selección de la opción de gestión de la movilidad adecuada: ¿MDM? ¿MAM? ¿MIM? ¿EMM?

Los responsables de TI tienen un amplio abanico de opciones en lo referente a sistemas de gestión de la movilidad empresarial. Es un verdadero quebradero de cabeza identificar las mejores herramientas y técnicas, así como las funcionalidades necesarias para operar, controlar y securizar los programas implantados.

Podemos identificar tres enfoques o componentes principales:

- gestión de dispositivos móviles (MDM, *Mobile Device Management*)
- gestión de aplicaciones móviles (MAM, *Mobile Application Management*)
- gestión de información móvil (MIM, *Mobile Information Management*)

Estos tres componentes los podemos encontrar en el mercado como productos o servicios independientes, o como suites que engloban los tres enfoques, denominadas EMM (*Enterprise Mobility Management*), y que representan un modo más efectivo de gestionar la movilidad aunque también puede ser más caro y complejo.

Debemos tener en cuenta que, aunque el sistema de gestión es un componente muy importante del programa BYOD, independientemente del tipo de solución y tecnología que elijamos, aún tendremos que ocuparnos de definir la estrategia, crear políticas y hacerlas cumplir, así como informar y formar a los usuarios.

Veamos la filosofía y principales características de cada uno de estos enfoques (41) (42) (43) (44) (45) (46) (47) (48).

MDM, Mobile Device Management

El MDM se centra en la gestión del dispositivo. Permite registrar, configurar, controlar, encriptar, monitorizar, y bloquear es dispositivo, así como forzar políticas (como escaneo de virus, requerir el uso de una contraseña o de la red privada virtual, etc.). En resumen, el MDM otorga un control total del dispositivo al área de TI.

Su principal inconveniente es que actúa sobre todo el dispositivo. Por ejemplo, en el caso de que el dispositivo se pierda o robe, TI puede borrarlo remotamente, eliminando con ello todos los datos y aplicaciones personales que el propietario tuviera.

En la época en que los dispositivos eran proporcionados por la empresa, las soluciones MDM tenían una gran aceptación. En programas BYOD donde el usuario es propietario del dispositivo y de la información personal que contiene, estos sistemas se consideran demasiado intrusivos.

Puesto que las características que gestionan los MDM son muy específicas del hardware y sistema operativo del dispositivo, a la hora de elegir un MDM tenemos que asegurarnos que tiene soporte multiplataforma y que soporta al menos una mayoría de los dispositivos y sistemas operativos incluidos en nuestro programa BYOD. Es común que los MDM actuales soporten Apple iOS 4 o superior, Google Android 2.3 o superior, y Windows Phone 6 y 7, sin embargo no es tan habitual que soporten BlackBerry OS o Windows Phone 8/RT aunque está mejorando, mientras que Symbian y WebOS están perdiendo popularidad.

MAM, Mobile Application Management

El MAM gestiona lo que está permitido o no dentro del dispositivo a nivel de aplicaciones. Es decir, gestiona las aplicaciones a las que queremos dar o restringir el acceso al usuario, a través de sistemas de listas blancas y listas negras de aplicaciones (*whitelisting* y *blacklisting*).

El MAM está relacionado con instalar, mantener, securizar, auditar y controlar el acceso al software desde smartphones y tabletas, ya sean propiedad del empleado o de la organización. Permite, por ejemplo, que TI encripte, bloquee o elimine aplicaciones corporativas específicas en lugar de todo el dispositivo. De esta forma el usuario mantiene el control de los aspectos personales del dispositivo.

Las dos formas más comunes de implementar MAM es por medio de app stores corporativos y de *app wrapping* (o utilizando una combinación de ambos):

- El *app wrapping* es el proceso de agregar una capa de gestión a una app móvil sin realizar ningún cambio a la app subyacente. El *app wrapping* permite establecer determinados elementos de una política sobre una app o grupos de apps (como por ejemplo, si es necesaria la autenticación de los usuarios para acceder a una app específica, o si los datos asociados con la app se pueden almacenar en el dispositivo, o si se permitirán determinadas APIs como copiar y pegar o compartir ficheros).
- Un app store corporativo es un portal web controlado por el área de TI a través del cual los usuarios pueden acceder, descargar e instalar aplicaciones concretas que han sido previamente aprobadas. Al hacer el despliegue de software corporativo a través de estos portales, el área de TI puede gestionar las licencias de las aplicaciones móviles, de escritorio, basadas en la nube y en la web, así como mantener determinado nivel de control sobre la seguridad.

Diferentes proveedores, como Symantec, VMware y Citrix Systems, ofrecen productos que permiten crear app stores corporativos.

Uno de los problemas del enfoque MAM es que los usuarios quieren descargarse aplicaciones de los app stores de los fabricantes de dispositivos (Apple App Store, Google Play, etc.). La forma en que estos app stores están estructurados hace imposible que los fabricantes de soluciones MAM puedan situarse entre el store y el usuario. Algunos buscan alternativas como publicar su propia versión "segura" de estas aplicaciones (correo, calendario, etc.), pero la experiencia de usuario no es la misma. ¿Y qué ocurre cuando se necesita una aplicación que el fabricante MAM no proporciona? Algunos fabricantes disponen de SDKs y APIs para que otros fabricantes puedan conectar sus aplicaciones de seguridad, pero requiere que esos fabricantes inviertan en desarrollar plugins para MAM.

En el caso del *app wrapping* el problema surge cuando el área de TI quiere proteger una app genérica iOS o Android app, necesitan los ficheros originales de la app. Si por ejemplo quisieran hacer *wrapping* de la app Microsoft Outlook para Android para ofrecérsela a sus usuarios corporativos, tendrían que convencer a Microsoft de que le enviasen el fichero .apk original.

El MAM tampoco parece la solución perfecta.

MIM, Mobile Information Management

La idea que prevalece detrás del MIM es que proteger la información es la clave para operar con éxito en entornos móviles. MIM utiliza el *sandboxing* o creación de compartimentos seguros alrededor de los datos sensibles, manteniéndolos encriptados y permitiendo el acceso o la transmisión sólo a aplicaciones validadas.

EMM, Mobile Application Management

Las soluciones EMM incorporan una combinación de funcionalidades incluidas en los tres enfoques anteriores. Además de la gestión del propio dispositivo, gestionan las aplicaciones que corren en el dispositivo, las conexiones de red con la organización, y los datos que se generan, acceden o comparten.

Muchos fabricantes tradicionales de soluciones MDM están ampliando rápidamente sus productos y servicios para ofrecer funcionalidades EMM.

Fabricantes de soluciones MDM y EMM

Las editoriales ZDNET y TechRepublic han realizado un ranking de fabricantes de soluciones MDM/EMM, que podemos ver en la Figura 27, basado en los 5 informes del año 2012 de los analistas Aragon Research, Forrester Research, Gartner, Info-Tech, y The Radicati Group (43).

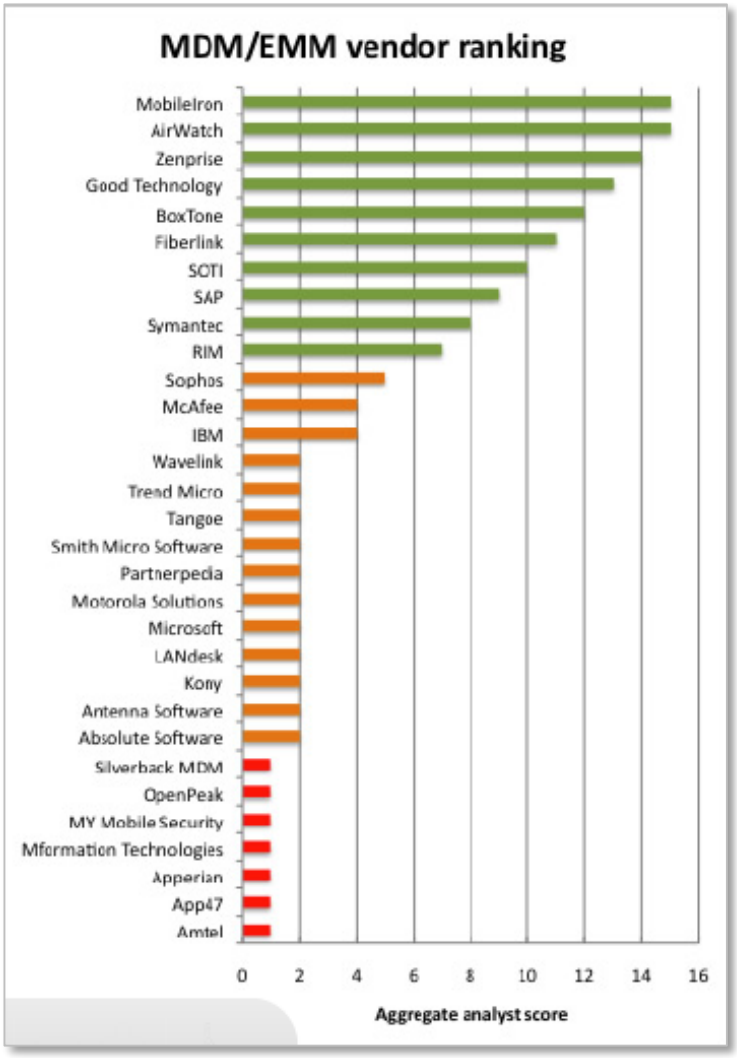


Figura 27. Ranking de proveedores de soluciones MDM/EMM. 2013 (43).

Los diez primeros fabricantes (barras verdes) incluyen una mezcla de especialistas puros en MDM y empresas como Good Technology, SAP, Symantec y RIM, con ofertas más amplias. Algunos —como AirWatch, MobileIron, SOTI, y Zenprise— ofrecen tanto soluciones on-premise como soluciones basadas en la nube (SaaS), mientras otros — BoxTone y Good Technology— solo ofrecen soluciones on-premise. El único entre estos fabricantes MDM que ha optado por ofrecer sólo soluciones basadas en la nube es Fiberlink, con su suite MaaS36.

En total, los cinco informes de los analistas cubrían 31 fabricantes, por lo que esta no es una lista exhaustiva. ZDNet ha elaborado un práctico directorio de fabricantes de soluciones MDM divididos por región geográfica. A continuación se detallan las direcciones donde se puede acceder a la información del directorio.

- En EMEA (49): http://www.zdnet.com/directory-mobile-device-management-vendors-in-emea-7000009879/
- En EEUU (50): http://www.zdnet.com/directory-mobile-device-management-vendors-in-the-us-7000010695/
- En Asia (51): http://www.zdnet.com/directory-mobile-device-management-vendors-in-asia-7000010549/

La Figura 28 muestra otra clasificación de fabricantes, realizada por la revista ComputerWorld, en función de las necesidades de gestión móvil y seguridad que cubren.

DLP Móvil (Prevención de Pérdida de Datos)		Gestión de Dispositivos Móviles	Gestión de Aplicaciones Móviles			
Monitorización de Tráfico	Almacenamiento Online Gestionado		Distribución de Aplicaciones	Desarrollo Seguro y Gestión de Apps	Gestión del Contenido de las Apps	Contenedores Seguros de Apps
InterGuard Software Symantec	Accellion Box Citrix Zenprise Dropbox YouSendIt	AirWatch BlackBerry BoxTone Centrify Fiberlink Good Technology Intel McAfee Microsoft MobileIron SAP Sybase Symantec Tangoe Wyse Trellia Zenprise	Apperian App47 Apple Good Technology MobileIron Odyssey Software (Symantec) SAP Sybase Partnerpedia Zenprise	AppCentral Good Technology MobileIron SAP Sybase Veracode Verivo	AppCentral Good Technology MobileIron Mocana Symantec Nukona	Antenna Software Cellrox Enterproid Fixmo NitroDesk Open Kernel Labs

Figura 28. Principales fabricantes en función de necesidades de gestión móvil (32).

Cómo decidir qué solución necesito

Para resumir en pocas palabras los puntos anteriores, la diferencia entre MDM, MAM y MIM es que el MDM se centra en gestionar dispositivos mientras que el MAM gestiona apps, y el MIM aporta un nivel más bajo de granularidad gestionando solo datos. En EMM incluye funcionalidades de los tres.

Además de la especialización en movilidad y modelo de servicio (On-premise/cloud), otros factores a considerar a la hora de elegir un fabricante MDM/EMM incluyen: si soportan aplicaciones móviles (apps) y gestión de contenidos, cómo se gestiona la separación de datos personales y corporativos, y si la solución se integra con los sistemas de gestión de infraestructura TI existentes en la organización.

A la hora de decidir qué solución o conjunto de soluciones implementar debemos tener claro:

- La lista de dispositivos y sistemas operativos que incluirá el programa BYOD y cuáles de ellos son estratégicos.
- La lista de funcionalidades críticas, funcionalidades necesarias y funcionalidades deseables de la solución de gestión en función de los requerimientos de la organización.
- Nuestros requerimientos o limitaciones económicas (nos servirá para decidir por ejemplo, si necesitamos ir a un servicio de pago por uso en la nube o un producto con coste fijo anual).
- Antes de adquirir la solución definitiva, es conveniente probar varias. Muchos fabricantes ofrecen versiones de evaluación de sus productos o servicios.

Estas tablas de funcionalidades básicas y avanzadas de sistemas MDM/EMM pueden ayudar a elaborar la lista de funcionalidades que deseamos incorporar. Podemos ver que algunos de los controles de seguridad discutidos en la sección 7.3 se incluyen como funcionalidades del MDM/EMM.

Funcionalidad	Descripción	Tareas	Características
Gestión de Inventario	Establecer y mantener una base de datos de dispositivos registrados y de sus propiedades.	• Registro de dispositivos • Seguimiento de activos • Retirada del servicio	• Auto- registro • Integración en el directorio • Política de Uso Aceptable • Detalles del activo • Historial de cambios • Borrado remoto • Backup / restauración
Gestión de Políticas de Dispositivo	Establecer/consultar los atributos y restricciones del dispositivo para validar e implementar políticas definidas por TI.	• Definir políticas • Provisionar dispositivos • Mantener políticas • Implementar políticas	• Criterios de aceptación • Políticas de grupo / localización • Actualización de políticas • Comprobación de cumplimiento de normativas • Acciones para forzar políticas
Gestión de la Seguridad	Proteger y gestionar la integridad de los dispositivos registrados.	• Configurar controles • Forzar controles • Chequear la integridad • Detectar dispositivos comprometidos	• PIN / Contraseña • Desconexión por inactividad • Fallo de login • Cifrado de datos • Restricciones de dispositivo • WiFi, VPN, Email seguros • Detección de dispositivos liberados (jailbreak) • Listas negras
Monitorización e Informes	Proporcionar visibilidad en tiempo real e históricos de dispositivos registrados y sus actividades.	• Estado en tiempo real • Notificación de alertas • Registro de eventos • Localización de dispositivos	• Dashboard configurable • Registro de peticiones • Mapeo / seguimiento GPS • Informes personalizables • Vistas detalladas y resumidas

Figura 29. Funcionalidades básicas MDM/EMM (47).

Funcionalidad	Descripción	Tareas	Características
Gestión del Servicio	Monitorización y control del uso del servicio de redes para gestionar los gastos resultantes.	• Definir presupuestos • Configurar conexiones • Monitorizar el uso • Forzar límites	• Limites de texto/tiempo de llamada • Datos 3G/4G • Restricciones de roaming • Analíticas de uso • Informes de gastos
Gestión de Aplicaciones	Instalar, actualizar y eliminar aplicaciones móviles públicas y corporativas.	• Crear librerías de aplicaciones • Establecer políticas de aplicaciones • Recomendar aplicaciones • Instalar/Actualizar aplicaciones • Monitorizar el uso • Deshabilitar/Desinstalar	• App store corporativo • Gestión de licencias • Actualizaciones transparentes • Listas blancas • Application wrapping
Gestión de Documentos	Descargar, actualizar y eliminar documentos corporativos, usando contenedores encriptados.	• Crear librerías de documentos • Establecer políticas de documentos • Recomendar documentos • Descargar /Actualizar • Monitorizar el uso • Deshabilitar/Eliminar	• Sincronización de ficheros/Backup • Integración con SharePoint • Compartición de ficheros • Acceso offline • Restricciones de seguridad
Gestión de Contenedores	Administrar mecanismos para separar datos y aplicaciones corporativos y personales.	• Habilitar contenedores • Configurar políticas • Monitorizar el uso • Borrar contenedor	• Cifrado seguro • Prevención de fuga de datos • Doble perfil • Borrado selectivo

Figura 30. Funcionalidades Avanzadas MDM/EMM (47).

La virtualización móvil puede ser una alternativa

La tecnología de virtualización ha sido un gran éxito en los entornos de data center y servidor. En el entorno móvil, sin embargo, algunos analistas coinciden (52) en que hasta que esta tecnología no sea independiente del tipo de dispositivo, y el mercado de fabricantes esté más definido, no la ven como alternativa al EMM.

La idea es que el área de TI puede crear un espacio virtual seguro y gestionado en el dispositivo, donde se desarrollarían las actividades vinculadas con la organización, al igual que ocurre en el desktop del PC corporativo.

La principal ventaja que aporta esta tecnología es que permite tener configurados dos perfiles de características muy diferentes (perfil de uso personal y perfil de uso profesional) en un mismo dispositivo hardware. Esta dualidad permitiría que si la organización quiere imponer una política de seguridad, ésta podría convivir perfectamente con lo que haya en el perfil personal. Los activos corporativos están protegidos y los usuarios hacen lo que quieran en su perfil personal.

Algunas soluciones disponibles son (43):

- Horizon Mobile de VMware, disponible para dispositivos Android e iOS, permite proporcionar y administrar espacios de trabajo virtuales para los usuarios
- Citrix XenDesktop y VMware View proporcionan escritorio, aplicaciones Web o SaaS a diversos dispositivos.
- Nivio, proporciona acceso a escritorios Windows, aplicaciones, almacenamiento y un interfaz de administración en cualquier dispositivo que soporte HTML5.
- Cloud Desktop de Mikogo es similar al anterior
- Desktone, es uno de los principales fabricantes en el mercado DaaS (*desktop-as-a-service*).

7.5. Definición del soporte a usuarios

El soporte al usuario es un elemento crítico del programa. Si no se define adecuadamente puede ser una fuente de insatisfacción para los usuarios y de costes no previstos para la organización. Es conveniente precisar qué pueden esperar los usuarios y a partir de qué punto es responsabilidad suya gestionar el soporte.

Deberemos definir qué tipo de soporte se va a prestar a los usuarios y en qué modo se hará. No todos los perfiles de usuarios identificados en el programa (ver apartado "*Determinar la necesidad de un programa BYOD*" en la sección 6) necesitarán las mismas opciones. Si la empresa tiene implantado un sistema de Gobernanza de TI o de Gestión de Servicios TI, los procesos de soporte BYOD deberán integrase dentro del marco global (ver apartado "*Integración en los modelos de Gobernanza y Gestión de los Servicios TI (ITSM)*" en la sección 7.4).

Podemos definir dos niveles de soporte. Un nivel básico, que cubra configuraciones básicas y soporte del dispositivo, y un nivel más avanzado, que cubra las aplicaciones móviles, problemas de red y otros problemas avanzados). Es recomendable invertir en la elaboración de buenas prácticas, configuraciones recomendadas, documentación de procedimientos sencilla, consejos, etc. que puedan compartirse en un repositorio o intranet, así como crear wikis colaborativos donde los propios usuarios puedan ayudarse entre sí. Crear programas de "recompensa" para premiar a los usuarios más

participativos, puede ser una forma económica de descargar al área de TI del primer nivel de soporte básico al usuario. De esta forma pueden reservarse esos recursos para ofrecer un soporte más personalizado a los grupos de usuarios que lo puedan requerir (directivos, puestos críticos, etc.)

En cualquier caso, hay que tener en cuenta que la variedad de dispositivos, plataformas y sistemas operativos impacta mucho en los recursos necesarios para ofrecer soporte. Los usuarios tienen dispositivos de múltiples fabricantes y además los sistemas operativos móviles están muy fragmentados (a modo ilustrativo, la Figura 31 muestra gráficamente la fragmentación del sistema operativo Android), y esto puede ser una pesadilla para el área de soporte. Las diferentes plataformas y sistemas operativos tienen características muy diferentes entre sí, incluso entre diferentes versiones del mismo sistema operativo y el equipo de soporte deberá tener una formación adecuada en todos aquellos incluidos en el programa.

Es importante delimitar claramente qué dispositivos, sistemas operativos y versiones van a estar soportados dentro del programa para evitar que los costes derivados del incremento de recursos para el soporte a usuarios, o la insatisfacción de los usuarios por sentirse "abandonados" a su suerte, ensombrezcan el éxito del programa.

Figura 31. Fragmentación del sistema operativo Android (7).

7.6. Implementación de un programa de información y formación de usuarios

La comunicación es una pieza fundamental del programa BYOD. De nada sirve establecer las mejores políticas, herramientas de seguridad y gestión, así como programas de soporte, si los usuarios no son conscientes de ello.

Colaborando con las áreas adecuadas, como Recursos Humanos, es necesario establecer un marco de comunicación y formación para los usuarios **antes del lanzamiento del programa**.

Los usuarios deben conocer qué pretenden las políticas BYOD y de seguridad establecidas, los usos aceptados, por qué es importante el cumplimiento de las políticas y qué herramientas va a utilizar el área de TI para implementarlas. Además deben recibir formación sobre las medidas de seguridad que deben implementar en sus dispositivos y el porqué de ello (por ejemplo, de nada sirve que la organización implemente el más seguro de los sistemas de autenticación, si los usuarios dejan sus credenciales al descubierto). Según un informe de Verizon (37), las organizaciones fallan en las medidas de seguridad más básicas, generalmente vinculadas a usuarios (el 76% de las intrusiones de red explotaron credenciales débiles o robadas).

Los usuarios deben conocer también las consecuencias del incumplimiento de las políticas.

Una vez conocidos los detalles del programa, los usuarios que deseen participar en el deberán firmar explícitamente la aceptación de la política.

Se puede trabajar con Recursos Humanos para que este proceso de formación y aceptación de política se incorpore en el plan de acogida para nuevos empleados, y se una al código de conducta y otros documentos corporativos cuya firma los empleados renuevan periódicamente.

7.7. Dimensionamiento de las infraestructuras y planes de actualización

La infraestructura de la organización está dimensionada para soportar un determinado número de dispositivos y una determinada carga de tráfico. Hay que tener en cuenta que con el programa BYOD, tanto el número de dispositivos conectados a nuestra red wireless como el tráfico que habrá en ella crecerá notablemente, impactando en todo el ecosistema TI.

Según un informe de Cisco (53), hoy lo usuarios utilizan una media de 2,8 dispositivos pero en 2016 se espera que esa media crezca un 18%, es decir los usuarios utilizarán una media de 3,3 dispositivos. Será necesario incrementar el número de puntos de acceso a nuestra red wireless para evitar cuellos de botella.

También habrá un mayor consumo de ancho de banda y de direcciones IP. El servidor DHCP puede quedarse sin direcciones IP y será necesario reconfigurarlo para acomodar la nueva demanda.

Será necesario analizar tanto el diseño (ver "*Arquitectura blindada: Protección de la red*" de la sección 7.3) como la capacidad de nuestras redes para adaptarse al programa. Tendremos que analizar los puntos de acceso necesarios (y su impacto en el número de switches y conexiones al backbone). Si es necesario, plantearse actualizar infraestructuras 802.11a/b/g a 802.11n (o incluso 802.11ac cuando se ratifique como estándar) para mejorar el ancho de banda y la cobertura.

También pueden tomarse medidas para preservar el ancho de banda como limitar el uso de determinadas aplicaciones personales de comunicaciones o video, pero si no existen aplicaciones corporativas que ofrezcan funcionalidades similares puede no ser conveniente.

7.8. Definición de un piloto

Un programa BYOD es un proyecto muy complejo. Es recomendable empezar definiendo un piloto sencillo, con un grupo limitado de usuarios y pocos dispositivos soportados para, a partir de esa primera experiencia, ir ampliando el proyecto.

En este punto es importante recordar que un programa BYOD no es un proyecto de tecnología, sino un proyecto de gestión del cambio en la empresa y hay que tener esto en cuanta a la hora de definir el piloto. Un factor crítico será, por ejemplo, la inclusión de los usuarios finales en el piloto, y el análisis y aceptación del feedback que aporten. También será importante la inclusión hábil del equipo directivo puesto que su apoyo será fundamental para la implantación del programa con éxito.

Como se ha comentado anteriormente, antes del arranque del piloto es recomendable que todos los empleados estén informados sobre el proyecto y que los participantes en el piloto hayan recibido la formación adecuada.

7.9. Evaluación y seguimiento

El programa BYOD es un proyecto vivo, por lo que deberemos revisar periódicamente la validez de las políticas definidas para asegurarnos que se siguen adaptando a los objetivos y requerimientos de la organización, así como a los avances de la tecnología.

Así mismo, debemos evaluar y monitorizar el programa implementado para asegurarnos que el programa funciona según esperábamos y que los requerimientos de negocio y de seguridad se están cumpliendo.

A la hora de definir las métricas a utilizar, además de tener en cuenta el feedback de los usuarios y de las áreas implicadas, debemos identificar aquellas métricas que estén alineadas con los objetivos definidos para el programa. Si, por ejemplo, el objetivo era mejorar la eficiencia del área de ventas, una de las cosas a medir será el incremento en las ventas; si el objetivo era la reducción de costes de TI buscaremos métricas vinculadas a esos costes. Para evaluar la eficiencia del programa, deberíamos incluir también métricas relacionadas con los costes del programa, su impacto en la infraestructura, la satisfacción de los usuarios y los beneficios de negocio logrados.

Según un estudio de Forrester Consulting para Trend Micro (27) sobre la medida del valor de la consumerización, entre el 38% y el 60% de las empresas que han implementado programas BYOD miden su impacto en los costes (ya sea directamente o como parte de los procesos generales de negocio), como podemos ver en la Figura 33. Algunas empresas también miden el impacto del programa en otro tipo de aspectos (Figura 32): el 59% mide el impacto en la facturación, el 50% en costes de plantilla vinculada a programas de comunicaciones, el 40% en costes de personal de soporte, y el 32% en costes del personal de red.

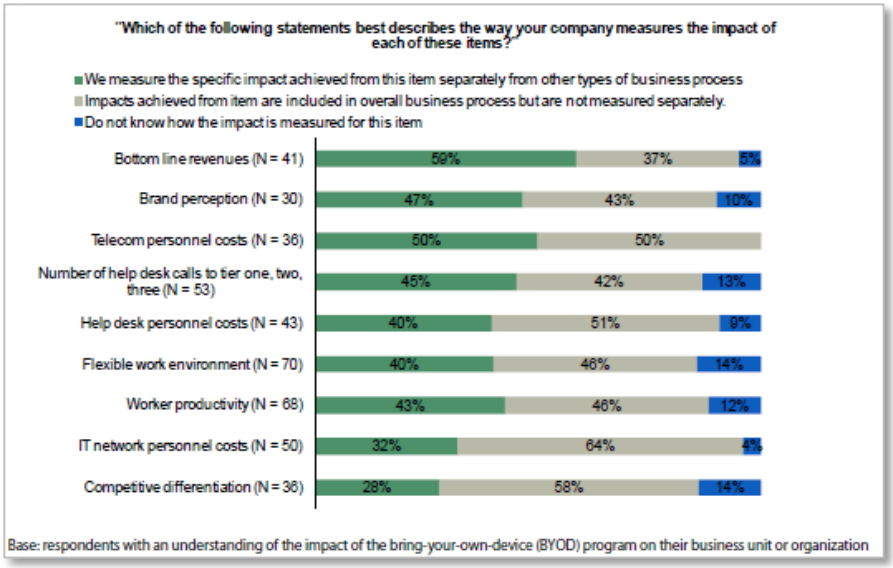


Figura 32. Medida del impacto del programa BYOD en diferentes áreas (27).

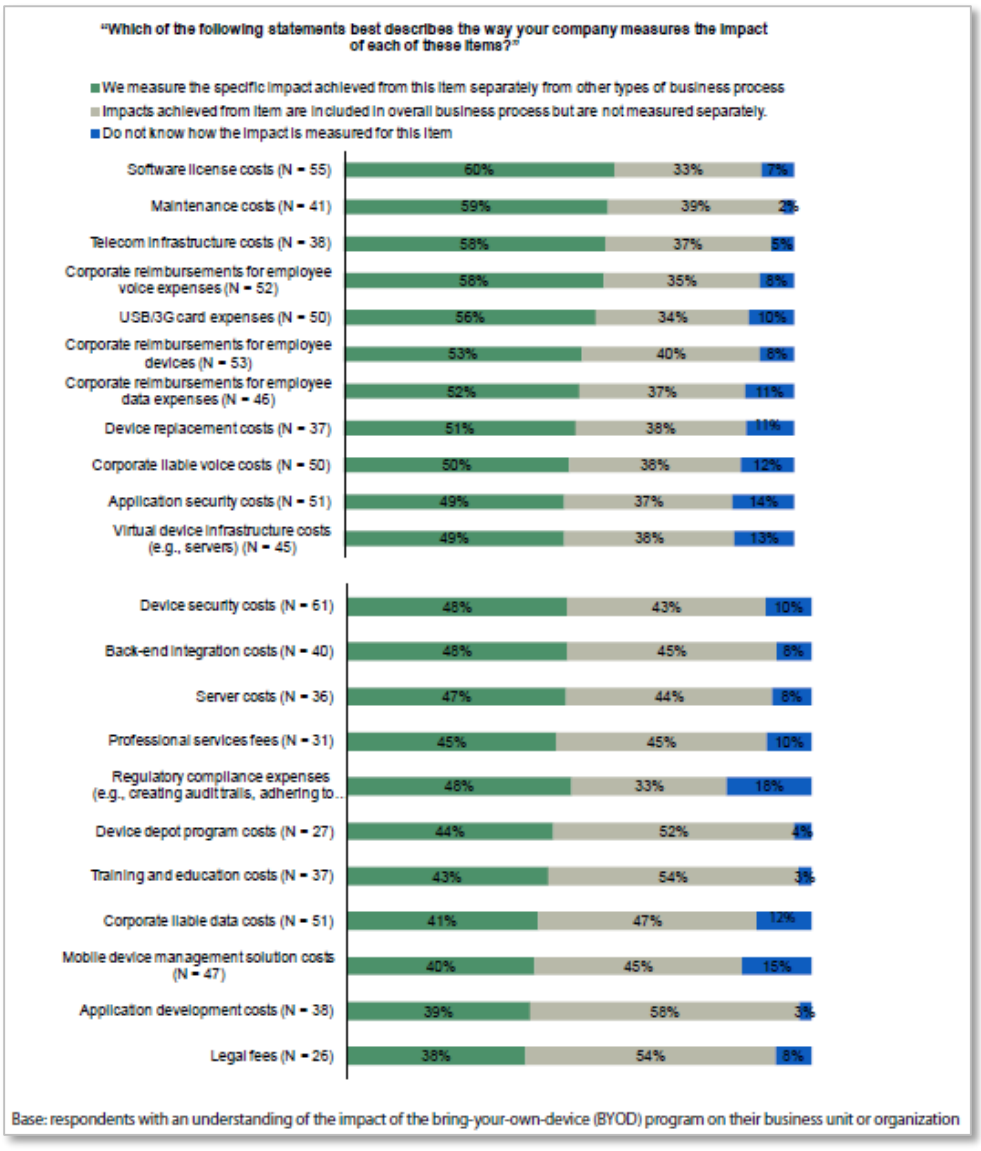


Figura 33. Las empresas miden el impacto de los programas BYOD implementados sobre diferentes gastos (27).

Módulo 3: Conclusiones

8. Recomendaciones

La consumerización de las TIC es una tendencia estratégica en tecnología que está teniendo un fuerte impacto en las organizaciones. Una de sus consecuencias es el fenómeno BYOD (*Bring Your Own Device*), que abre las puertas a otras corrientes como el *Bring Your Own Application* o el *Bring Your Own Cloud*.

Hemos visto que estos fenómenos tienen sus ventajas e inconvenientes. Pueden decidir acogerlos o prohibirlos, pero **en ningún caso las organizaciones pueden permitirse ignorar el BYOD**, puesto que las implicaciones para la seguridad de la información corporativa son demasiado importantes, y pueden derivar en incidentes con un impacto negativo para la organización (a nivel económico, legal o reputacional).

Hoy día **la Movilidad es algo inevitable en las organizaciones, pero el BYOD sí lo es**. En los últimos años la movilidad ha pasado de ser una ventaja competitiva a ser un requerimiento necesario para cualquier organización. Sin embargo, el BYOD es sólo un modelo de implementación de la movilidad. Existen otras opciones. Las organizaciones deberían evaluar que modelos encajan mejor dadas sus circunstancias concretas y, en cualquier caso, tomar una decisión respecto al BYOD. Puede optarse, por ejemplo, por modelos híbridos que combinen dispositivos corporativos y dispositivos personales en función del perfil del usuario. O puede optarse por modelos como el CYOD (*Choose Your Own Device*), en los que las opciones de dispositivos y aplicaciones están mucho más limitadas que en el BYOD y el dispositivo puede pertenecer a la empresa o al empleado, o por modelos COPE (*Corporate-owned, Personally-Enabled*), en los que el dispositivo pertenece a la empresa pero el empleado puede usarlo como personal.

Para obtener el máximo beneficio del BYOD las organizaciones deberían **afrontarlo desde un enfoque estratégico**, definiendo unas metas globales y resultados deseados de la implementación del programa BYOD, identificando cómo impactará el programa BYOD en las diversas unidades de negocio, así como los procesos de negocio que deben ser modificados, y definiendo un marco temporal para alcanzar los beneficios acordados del programa BYOD.

Las organizaciones deben aplicar una estrategia que reduzca los riesgos de seguridad y privacidad, así como la complejidad de la gestión. Deben **establecer las estrategias de gestión** que mejor encajen con las exigencias culturales de sus empleados, los requerimientos regulatorios de su industria y de la legislación en materia laboral y de privacidad específica de su país. Esta estrategia ayudará al equipo de TI a través de una infraestructura de soluciones y un programa BYOD que permitirá al equipo de TI:

- La gestión unificada de las políticas: una única plataforma de gestión de políticas que proteja datos, aplicaciones y sistemas, y que reconozca el perfil de usuario. Asimismo debería identificar y gestionar todos los dispositivos móviles que acceden a la red corporativa.
- Proporcionar acceso seguro a la red y servicios corporativos, en función del perfil de usuario y dispositivo usado, y manteniendo la capacidad de red necesaria.

- Proteger los datos independientemente de su ubicación con una seguridad capaz de identificar el contexto.
- Facilitar la transmisión segura de datos entre los dispositivos y la infraestructura de red o cloud.

A la hora de definir un programa BYOD es recomendable tener en cuenta estas consideraciones:

- **Un programa BYOD es más un proyecto de gestión del cambio que un proyecto de tecnología**. Afecta a muchas áreas de la organización más allá del área de TI y será necesario involucrarlas a todas a la hora de definir e implementar el programa.
- Cuando llegamos a la parte económica del BYOD, hay que hacer los números con cuidado. **El BYOD puede reducir los costes de los programas de movilidad, pero también puede elevarlos**. Para comprender el retorno de inversión real, se debe estudiar todos los elementos del programa BYOD y cómo afectan a los costes y beneficios en la situación concreta de la organización.
- El primer paso es **analizar la situación actual de la empresa** desde un punto de vista realista. Habrá que determinar el punto de partida (qué dispositivos personales y cómo se están utilizando) y cuál es la demanda real del BYOD, así como determinar hasta qué punto los recursos de la empresa están preparados para soportar un programa BYOD.
- Es conveniente determinar aquellos **escenarios en los que el BYOD no será en absoluto aplicable.**
- Debe desarrollarse e implementarse una **política BYOD** que gobierne el acceso de los usuarios a la infraestructura y datos corporativos desde sus dispositivos, antes de que ocurran los problemas, no después. Una vez que se ha creado una política hay que asegurarse de que los empleados la conocen. Así mismo hay que darle a los empleados la política cuanto antes, aunque no esté completa. Una política incompleta es mejor que ninguna política.
- La política deben ser clara, concisa, **realista, sostenible y adaptada a los usuarios que las van a utilizar** (deben contemplar diferentes Casos de Uso). Una política que pretende influenciar el comportamiento de los empleados no puede estar escrita en un oscuro lenguaje técnico ni alejarse de la cultura y estilo de la organización. Aunque en un principio la elaboración de la política pueda parecer una tarea abrumadora, hay que tener en cuenta que **la peor política es la ausencia de política**.
- La política BYOD debe incluir una **definición de Usos Aceptables** que detalle qué se considera un uso apropiado del dispositivo en el entorno de trabajo, así como definir qué se considera entorno de trabajo. Así mismo, debe **precisar las responsabilidades y derechos de los participantes**.
- **Los principales riesgos del BYOD están vinculados a la seguridad y la privacidad. Es recomendable establecer políticas de seguridad que se centren en los datos en vez de en los dispositivos**. Es recomendable definir diferentes perfiles de usuario y permitir el acceso únicamente a aquellos recursos que se vayan a utilizar. Las soluciones tecnológicas que permiten establecer contenedores separados para los datos personales y los corporativos son especialmente útiles. Este enfoque también ayuda a mitigar las implicaciones legales y de privacidad del BYOD.
- **Delimitar claramente los dispositivos, sistemas operativos y versiones que están soportados en el programa**.

- **Las políticas por sí mismas no son suficientes, necesitaremos herramientas** que nos ayuden a implementarlas, como pueden ser los sistemas de gestión de dispositivos móviles (*Mobile Device Management*, MDM), sistemas de gestión de aplicaciones móviles, etc.
- Se debe crear un programa de **formación y comunicación a los usuarios antes de iniciar el despliegue del programa**. Si ahora parte de la responsabilidad de protección de la información de la organización va a recaer en los usuarios, es necesario enseñar a los empleados cómo proteger sus dispositivos y cómo reconocer los signos de que su dispositivo ha sido comprometido. Es importante concienciarlos sobre la importancia de mantener el software, la plataforma y los programas de seguridad continuamente actualizados, así como de la necesidad de comunicar inmediatamente al área de IT el robo o pérdida de cualquier dispositivo que tenga acceso a datos corporativos para que se tomen las medidas de seguridad pertinentes.
- Deben establecerse mecanismos para asegurar que los empleados participantes en el programa conocen las condiciones de privacidad y posibles implicaciones legales que pueden derivar del programa, y que éstos hayan dado su **consentimiento informado** a la política de forma explícita según requiera la legislación local aplicable.
- El **soporte al usuario** es un elemento crítico del programa. Si no se define adecuadamente puede ser una fuente de insatisfacción para los usuarios y de costes no previstos para la organización. Es conveniente precisar qué pueden esperar los usuarios y a partir de qué punto es responsabilidad suya gestionar el soporte.
- No hay que olvidar la **planificación de la capacidad de la infraestructura necesaria** para acomodar el programa BYOD.
- Hay que **ofrecer opciones para aquellos usuarios que no quieran unirse al programa BYOD**. Una vez que el usuario se dé cuenta de lo vulnerable que es su dispositivo, es posible que no quiera unirse o quiera abandonar el programa BYOD. La organización debería dar a los usuarios la opción de usar dispositivos de empresa. Es necesario tomar precauciones de seguridad cuando un dispositivo de uso privado deja el programa BYOD (porque el empleado deje la empresa o pase a usar dispositivo de empresa), como cambiar la tarjeta SIM o los passwords encriptados.
- Un programa BYOD es un proyecto muy complejo. **Es recomendable empezar definiendo un piloto sencillo**, con un grupo limitado de usuarios y pocos dispositivos soportados para, a partir de esa primera experiencia, ir ampliando el proyecto.
- La estrategia BYOD no es algo inamovible, de hecho deberemos **revisar la estrategia y políticas periódicamente** para adaptarla a la evolución de la organización, nuestras necesidades y objetivos, así como a la evolución de la tecnología.

Bibliografía

1. Trend Micro. BYOD: consumerización de la TI. [En línea] 2013. http://www.trendmicro.es/grandes-empresas/consumerizacion/.

2. TechTarget. WhatIs.com. *WhatIs.com.* [En línea] 2013. http://whatis.techtarget.com/.

3. *Wikipedia.* [En línea] http://es.wikipedia.org/wiki/Wikipedia:Portada.

4. Zamora, Javier. Colaborador científico del IESE. [entrev.] IESE Insight. *TIC, de la consumerización a la customización.* 16 de Mayo de 2011.

5. SearchCIO. Planning for the future of mobility: A BYOD guide for enterprise CIOs. *SearchCIO.* [En línea] 2013. http://searchcio.techtarget.com/essentialguide/Planning-for-the-future-of-mobility-A-BYOD-guide-for-enterprise-CIOs#guideCategory3.

6. Business Insider Intelligence. There Will Soon Be One Smartphone For Every Five People In The World. *Business Insider* . [En línea] 7 de febrero de 2013. http://www.businessinsider.com/15-billion-smartphones-in-the-world-22013-2.

7. Business Insider (Henry Blodget). The Future of Digital. [En línea] 12 de noviembre de 2013. http://www.businessinsider.com/the-future-of-digital-2013-2013-11?op=1.

8. IDC. *Tablet Shipments Forecast to Top Total PC Shipments in the Fourth Quarter of 2013 and Annually by 2015.* septiembre 2013.

9. Gartner. Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes. *www.gartner.com.* [En línea] 1 de mayo de 2013. http://www.gartner.com/newsroom/id/2466615.

10. Gartner (David A. Willis). *Bring Your Own Device: The Facts and The Future.* Gartner. s.l. : Gartner, abril 2013. Research.

11. Ovum. *BYOD: an emerging market trend in more ways than one. N= 3796.* s.l. : Logicalis, Q4 2012.

12. Cisco. *Six Essential Steps for Unleashing the Power of Enterprise Mobility.* 2013.

13. CBC News. 5 major moments in cellphone history. *CBC News - Technology & Science.* [En línea] 3 de abril de 2013. http://www.cbc.ca/news/technology/5-major-moments-in-cellphone-history-1.1407352.

14. Cisco. *The Financial Impact of BYOD. A Model of BYOD's Benefits to Global Companies.* 2013.

15. Bradley, Joseph, y otros. BYOD: A Global Perspective. Harnessing Employee-Led Innovation. *Cisco.com.* [En línea] 2013. https://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf.

16. Dimensional Research. *The impact of mobile devices on Information Security: a survey of IT Professionals.* s.l. : Check Point, junio 2013.

17. Trend Micro. *2013 Mobile Security Report.* 2013.

18. Arxan. *State of Security in the App Economy 2013.* s.l. : Arxan, 2013.

19. Symantec. *2013 Internet Security Threat Report, Volume 18.* s.l. : Symantec, 2013.

20. Gartner. Gartner Identifies the Top 10 Strategic Technology Trends for 2014. *Gartner.com.* [En línea] 8 de octubre de 2013. http://www.gartner.com/newsroom/id/2603623.

21. Burrus, Daniel. 25 Game-Changing Trends That Will Create Disruption & Opportunity. *Burrus.com.* [En línea] 16 de diciembre de 2013. http://www.burrus.com/2013/12/game-changing-it-trends-a-five-year-outlook-part-i/.

22. Kleyman, Bill. How to make a BYOD program work. *SearchConsumerization.* [En línea] noviembre de 2011. http://searchconsumerization.techtarget.com/tip/How-to-make-a-BYOD-program-work.

23. Gartner (Michael Disabato). *Implementing a Bring Your Own Device (BYOD) Program.* Gartner. s.l. : Gartner, Enero 2013.

24. Stuart, Anne. Six steps for launching an effective BYOD program. *SearchCloudApplications.com.* [En línea] August de 2013. http://searchcloudapplications.techtarget.com/tip/Six-steps-for-launching-an-effective-BYOD-program.

25. Gartner (Andy Rowsell-Jones; Nick Jones). *Checklist for Determining Enterprise Readinessto Support Employee-Owned Devices.* Gartner. s.l. : Gartner, Junio 2012. Research.

26. Anderson, Neil. Cisco Bring Your Own Device - Device freedom without compromising the IT Network. *Cisco.com.* [En línea] agosto de 2013. http://www.cisco.com/web/ANZ/midsize/images/byodwp.pdf.

27. Forrester Consulting. *Key Strategies To Capture And Measure The Value Of Consumerization Of IT.* s.l. : Trend Micro, mayo 2012.

28. Nucleus Research. *Understanding the hard ROI of BYOD.* June 2013.

29. Pironti, John. The Changing Role of Security Professionals. *InfoSecurity Magazine.* [En línea] 15 de enero de 2013. http://www.infosecurity-magazine.com/view/30212/the-changing-role-of-security-professionals/.

30. Jackson Higgins, Kelly. Embrace Your Inner Risk Adviser. *Security Dark Reading.* [En línea] 8 de octubre de 2013. http://www.darkreading.com/vulnerability/embrace-your-inner-risk-adviser/240162419.

31. Pironti, John P. *Balancing the Corporate Risks and Rewards of Mobile Devices.* 2013.

32. InfoWorld. *Mobile and BYOD. Deep Dive.* s.l. : InfoWorld, 2013 febrero.

33. Mathias, Craig J. Potential BYOD legal issues you may not have thought of. *SearchConsumerization.com.* [En línea] noviembre de 2013. http://searchconsumerization.techtarget.com/tip/Potential-BYOD-legal-issues-you-may-not-have-thought-of?asrc=EM_ERU_25178032&utm_medium=EM&utm_source=ERU&utm_campaign=20131128_ERU%20Transmission%20for%2011/28/2013%20(UserUniverse:%20586604)_myka-reports@t.

34. Information Commissioner Office (ICO). Bring your own device (BYOD). *www.ico.org.uk.* [En línea] 2013. http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod.

35. Harris Interactive. BYOD Beware! *www.maas360.com.* [En línea] septiembre de 2012. http://www.maas360.com/maasters/blog/security-information/byod-beware-infographic/?A=PR.

36. Long, William. EU Data Protection Regulation: fines up to €100m proposed. *ComputerWeekly.com.* [En línea] 4 de diciembre de 2013. http://www.computerweekly.com/opinion/EU-Data-Protection-Regulation-fines-up-to-100m-proposed?asrc=EM_ERU_25272177&utm_medium=EM&utm_source=ERU&utm_campaign=20131203_ERU%20Transmission%20for%2012/03/2013%20(UserUniverse:%20583481)_myka-reports@techtarget..

37. Verizon. *Verizon Data Breach Investigations Report - Smarter Security: can your business keep up?* s.l. : Verizon, 2013.

38. CDW. *Securing BYOD.* s.l. : CDW, marzo 2013.

39. Tucci, Linda. BYOD and ITIL: Amicable relationship or irreconcilable differences? *SearchCIO-Midmarket.com.* [En línea] 20 de abril de 2011. http://searchcio-midmarket.techtarget.com/news/2240034916/ITIL-and-BYOD-Amicable-relationship-or-irreconcilable-differences.

40. Norsa, Gerard. BYOD and ITSM: What you need to know. *ITWorld.com.* [En línea] 6 de mayo de 2013. http://www.itworld.com/355177/byod-and-itsm-what-you-need-know.

41. Phifer, Lisa. *Technical Guide on Mobile Device Management.* s.l. : TechTarget - Security Media group, March 2013.

42. Madden, Brian. What is MDM, MAM, and MIM? (And what's the difference?). *BrianMadden.com.* [En línea] 29 de mayo de 2012. http://www.brianmadden.com/blogs/brianmadden/archive/2012/05/29/what-is-mdm-mam-and-mim-and-what-s-the-difference.aspx.

43. TechRepublic - ZDNet. The Executive's Guide to BYOD and the Consumerization of IT. *ZDNet.com.* [En línea] 2013. http://b2b.cbsimg.net/downloads/Gilbert/exec_guide_byod_consumerization_it.pdf.

44. TechTarget. MAM. *WhatIs.com.* [En línea] TechTarget, 2013. http://whatis.techtarget.com/definition/mobile-application-manager-MAM?track=NL-1823&ad=889978.

45. Steel, Colin. Management technologies to ensure mobile data security and compliance. *SearchConsumerization.com.* [En línea] 26 de noviembre de 2013. http://searchconsumerization.techtarget.com/feature/Management-technologies-to-ensure-mobile-data-security-and-compliance.

46. TechTarget. e-Guide Mobile Device Management: going beyond basics. *SearchConsumerization.com.* [En línea] agosto de 2013.

47. Phifer, Lisa. Evaluating mobile device management products. *SearchConsumerization.com.* [En línea] abril de 2013. http://searchconsumerization.techtarget.com/ebook/Choosing-and-managing-mobile-devices/Evaluating-mobile-device-management-products.

48. Steele, Colin. Mobile device management vs. mobile application management. *SearchConsumerization.com.* [En línea] 12 de agosto de 2013. http://searchconsumerization.techtarget.com/feature/Mobile-device-management-vs-mobile-application-management?.

49. McLellan, Charles. Directory: Mobile Device Management vendors in EMEA. *ZDNet.com.* [En línea] 4 de febrero de 2013. http://www.zdnet.com/directory-mobile-device-management-vendors-in-emea-7000009879/.

50. Gray, Patrick. Directory: Mobile Device Management vendors in the US. *ZDNet.com.* [En línea] 4 de febrero de 2013. http://www.zdnet.com/directory-mobile-device-management-vendors-in-the-us-7000010695/.

51. Yap, Jamie. Directory: Mobile Device Management vendors in Asia. *ZDNet.com.* [En línea] 4 de febrero de 2013. http://www.zdnet.com/directory-mobile-device-management-vendors-in-asia-7000010549/.

52. Tucci, Linda. Is mobile device virtualization the answer to BYOD? *SearchCIO.* [En línea] 17 de julio de 2012. http://searchcio.techtarget.com/news/2240159786/Is-mobile-device-virtualization-the-answer-to-BYOD.

53. Higbie, Carrie. Designing a network to withstand BYOD. *Modern Infraestructure.* [En línea] octubre de 2013. http://searchdatacenter.techtarget.com/ezine/Modern-Infrastructure/Can-Microsofts-Azure-platform-lift-the-companys-cloud-hopes.

54. GoodTtechnology. Bring Your Own Device - Individual Liable User Policy Considerations. *www.welcometogood.com.* [En línea] 2012. http://www.welcometogood.com/byod/byod_policy_wp.pdf.

55. Ashford, Warwick. Many enterprises not getting value of consumerisation, says IDC. *ComputerWeekly.com.* [En línea] 27 de November de 2013. http://www.computerweekly.com/news/2240210048/Many-enterprises-not-getting-value-of-consumerisation-says-IDC.

56. Mathias, Craig. Mobility management: Beyond MDM and BYOD. *SearchCIO.* [En línea] September de 2013.

57. Beadon, Kevin. One step ahead - the importance of staying in control of your organisation's BYOD policy. *ComputerWeekly.com.* [En línea] September de 2013. http://www.computerweekly.com/opinion/One-step-ahead-the-importance-of-staying-in-control-of-your-organisations-BYOD-policy.

58. SearchConsumerization.com. Put it on paper: A guide to mobile device policy creation - Essential guide. *SearchConsumerization.com.* [En línea] 2013. http://searchconsumerization.techtarget.com/essentialguide/Put-it-on-paper-A-guide-to-mobile-device-policy-creation.

59. Information Commissioner’s Office (ICO) . Bring Your Own Device (BYOD) - Guide. *www.ico.org.uk.* [En línea] octubre de 2013. http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod.

60. Gartner (Carsten Casper). "Privacy by Design" Can Save Costs and Reduce Total Cost of Ownership. *Gartner.com.* [En línea] octubre de 2013. http://www.gartner.com/newsroom/id/2610515.

61. McGillicuddy, Shamus. BYOD challenges that lurk beyond network security. *SearchNetworking.com.* [En línea] enero de 2013. http://searchnetworking.techtarget.com/feature/BYOD-challenges-that-lurk-beyond-network-security.

62. Mathias, Craig J. Enterprise mobility management options: MDM, MAM and MIM. *SearchConsumerization.com.* [En línea] 17 de septiembre de 2012. http://searchconsumerization.techtarget.com/tip/Enterprise-mobility-management-options-MDM-MAM-and-MIM.

Anexo 1: Ejemplo de plantilla para la elaboración de una política BYOD del fabricante Good Technology

Bring Your Own Device - Individual Liable User Policy Considerations (54)

Introduction

As more companies embrace the broad usage of individual liable mobile devices for access to corporate applications and data, Good Technology is often asked for guidance on the establishment of an associated individual liable usage policy. This policy document is intended to provide guidance on questions that companies should ask themselves when establishing their own policies and related considerations.

Policy Document Objectives & Legal Disclaimer

Only your combined Information Technology (IT), Human Resource (HR), Finance, and Legal functions—working closely with your executive team and business unit managers—can determine the exact corporate liable and/or individual liable policy that best fits your company, meets its financial goals and objectives, and takes into account security, legal, regulatory, tax, or other requirements and considerations that may uniquely apply to your Company and its operations.

Accordingly, the objective of document is not to define an actual individual liable user policy. The questions and policy considerations outlined herein are just that, and must not be construed either individually or collectively as: (i) an actual or complete policy; (ii) either necessary or sufficient to meet the fiduciary, legal, regulatory, or other requirements that may apply to a particular company or policy; or (iii) legal or finance advice.

Good Technology disclaims any and all liability for the use of this document and/or the considerations outlined herein, either in whole or in part, in the definition and/or application of specific policies by any company.

Eligibility Considerations

Questions to Ask

- Are all employees eligible for mobile access to company data and applications?
- Will you restrict access, even within the individual liable population, based on role, title, manager approval, geography, or other organizational considerations?
- Will you restrict access for individually liable users to particular company applications or data? If so, which apps and data?
- Will you support any individual liable device, or, for example, only devices explicitly certified by Your EMM solution vendor for use with your EMM solution?

Policy Considerations

- Policy should clearly address:
  - All eligibility requirements
  - Any device support limitations
  - Employee risks and responsibilities
  - Any applications or data access limitations

- Any processes for obtaining approval

Reimbursement Considerations

Questions to Ask

- Are individual liable users ever entitled to reimbursement?
- If so, for which services and under what conditions (e.g., voice usage, data usage, Wi-Fi hotspot usage, roaming usage, business vs. personal usage, manager approval, etc.)?
- Are any services not eligible for reimbursement (e.g., SMS/MMS, ringtone downloads, 90X calls, any service not explicitly identified as eligible for reimbursement)?
- Are there any caps on reimbursement (e.g., in the form of fixed monthly stipends or maximum-expense backlimits, irrespective of charges incurred)?
- Are individual liable users ever eligible for full or partial reimbursement of device acquisition or replacement costs?

Policy Considerations

- Policy should clearly address conditions for reimbursement and eligibility of devices, i.e.: Reimbursement of device purchase and/or replacement costs (e.g., no reimbursement, full, partial up to a limit, frequency of reimbursement, etc.)
  - Any reimbursement limitations (e.g., services, max amounts, etc.)
  - Any monthly stipend amounts and related eligibility
  - Maximum reimbursement amounts
- Policy should encourage users to consider voice plans, unlimited data plans, roaming plans, etc. that do not exceed monthly stipend and/or maximum reimbursement amounts. However, policy should clearly state that, should the user choose a plan which exceeds these costs, the company does not assume any financial responsibility, except as otherwise consistent with policy.
  - For example: if stipend amount or reimbursement max is $100/month and user chooses an unlimited voice/data plan with international roaming option at $300/month, policy should clearly state that the company is not liable for the cost difference.

Security Considerations

Questions to Ask

- What is your policy and process for handling a lost or stolen device?
- What is your policy and process for handling the decommissioning of a device (e.g., if user switches to new device, change in user's role/title deems them no longer eligible for access, user leaves or is terminated by company, etc.)?
- Will your company wipe the entire device, corporate data and apps only, or both?
- Will you allow user to initiate wipe action(s) themselves (e.g., through self-service portal)?
- Will your company set and enforce use of a whole device password?
- Will your company ever wipe the whole device?

- Will your company only set and enforce password on the Good client?
- Will your company only wipe data explicitly managed by the Good client?
- Will your company require limits on the use of cameras, browsers, Bluetooth, or other applications and services?
- Will you require users to acquire and install anti-malware as a condition for access to corporate data and apps? Will you provide such anti-malware? Will you require particular vendors or versions?
- What is your policy and process for a user device that has been infected with malware?

Policy Considerations

- Policy should expressly prohibit: (i) device "jailbreaking," "rooting," or the equivalent; and (ii) making any other modifications to device hardware and/or OS software beyond routine installation of updates as directly provided by the applicable device maker or mobile operator. Performing such actions or making such unauthorized modifications is essentially an "inside attack" on device, application, and data security, and should be treated very seriously.
- Policy should be clear on process and timing requirements for reporting lost or stolen devices, changing to a new device, and actions to be taken when an employee leaves the company.
- Policy should be clear on whether or not you will require use of whole device password and associated requirements for frequency of change, minimum strength, etc.
- Policy should be clear on whether or not you will wipe whole device and conditions under which you would do so (e.g., lost or stolen device, change to new device, move to new role, departure from company, etc.).
- Policy should clearly state that you always reserve the right to wipe either company data and applications and/ or the whole device if deemed necessary in your sole discretion to secure company data or applications.
- Policy should be clear that wiping company data and applications may impact other applications and data (e.g., including but not limited to native Address Book data).
- Policy should disclaim any liability for loss of personal applications or data, whether directly or indirectly resulting from the usage of company apps or data, and/or the wiping of such apps or data, or the whole device.
- User should be encouraged to minimize the risk of losing personal applications and/or data.
- Policy should be clear on any restrictions on the usage of cameras, browsers, Bluetooth, or other applications and services. The ability to enforce such restrictions may be dependent on device capabilities, which in turn may become an eligibility consideration).
- Policy should be clear on any requirements for the use of anti-malware (including specific vendors or versions as applicable) and process and timing requirements for reporting any suspected instances of malware infection.

Acceptable Use Considerations

Questions to Ask

- What is your policy regarding use of device by users other than corporate end-user?
- Will you provide intranet access to individual liable users?

- Will you require individually liable device users to conform to acceptable use guidelines on all Internet usage, even if not enabled through corporate infrastructure and/or for personal reasons (e.g., as a condition of receiving stipend, reimbursement, or access to company apps or data)?

Policy Considerations

- Policy should be clear on whether device enabled for corporate apps and data access may be used or loaned to other users (e.g., if a EMM client has a separate password and the whole device password is not used, it may be acceptable for company end-user to allow someone else to temporarily use the device, as use of device does not require company end-user to first "unlock" the EMM client that enables access to corporate data or apps).
- If you provide intranet access (e.g., through a EMM solution or mobile VPN client), policy should be clear that company's acceptable use guidelines for desktop/laptop browser usage will apply to any usage of intranet and/or internet access that is enabled through the use of a EMM solution or other mobile VPN infrastructure.
- Most companies will not apply acceptable use policies to usage not enabled through corporate infrastructure—if your company chooses to do so (e.g. as condition of receiving stipend or reimbursement), then policy should be clear on this.

End-User Support

Questions to Ask

- Will you provide any end-user support for individual liable users?
- If so, for what applications, services, or scenarios (e.g., lost or stolen device)?

Policy Considerations

- Policy should be clear on what support, if any, will be provided and: (i) explicitly for which applications, services, and scenarios; (ii) any "self-service" actions that must first be taken before requesting support; and (iii) process and/or tools for requesting support (e.g., submitting trouble ticket vs. calling).
- Many companies will opt for individual liable support policy that is expressly limited to the EMM client and applications and require that users first attempt to resolve routine issues via "self-service" mechanisms (e.g., always contacting carrier for billing issues, contacting carrier first if not able to connect, resetting own password via self-service portal).

Policy Violations

Questions to Ask

- What should happen if user violates policy?
- Should different violations be treated differently (e.g., eligibility vs. security vs. acceptable use)?

Policy Considerations

- Policy should be clear on consequences of policy violation and any differences from one policy or policy type to the next.

Unauthorized Access or Use of Cellular Telephone Service

On receipt of a monthly bill, enterprise users should immediately check the call detail record section of the bill for any indication of unauthorized calls. Discovery of any such calls should be immediately reported to:

- The carrier providing the service
- The security department

Additional Info: Smartphone Policies & Security

The use of a Smartphone in connection with (Company Name) business is a privilege granted to employees through approval of their management. (Company Name) reserves the right to revoke these privileges in the event that users do not abide by the policies and procedures set forth below.

The following policies are aimed to protect the integrity of (Company Name) data and ensure it remains safe and secure under (Company Name) control. Please note that there may be limited exceptions to these policies owing to device limitations between vendors.

(Define corporate policies here. Note: These are only examples and will vary per enterprise.)

- Your device will lock your account after 10 failed login attempts.
- Your device or EMM application will lock every 30 minutes requiring reentry of your password.
- Your device will include password rotation every 90 days.
- The password must be a minimum of six characters.
- The password must contain at least one letter or number (except on devices that cannot accept alphanumeric passwords).
- The password must not be one of your previous four passwords.
- Your device will be remote wiped if: (i) you lose the device; (ii) you terminate employment with (Company Name); (iii) IT detects a data or policy breach or virus; or (iv) if you incorrectly type your password 10 consecutive times.
- Your iPhone, iPad or Android w/ EMM client device may allow for only the remote wipe of (Company Name) data. This means your personal data is still vulnerable, and thus it is recommended you also set a device password and take additional security precautions.
- In addition to the above security settings, all users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, "jailbreaking" your iPhone.

Personal Smartphone: A personal Smartphone can be connected to the (Company Name) infrastructure, but the user is personally liable for the device and carrier service costs. Users of personal Smartphones are not eligible for expense reimbursement for hardware or carrier services. Users of personal Smartphones must agree to all terms and conditions in this policy to be allowed access to those (Company Name) services.

Employees that purchase a device on their own that is not in line with our standard approved device lists may not be allowed to have their devices added to the servers. It is highly recommended that the employee refer to the Smartphone support website to review the devices that are being supported by IT. Users of personal Smartphones are not permitted to connect to (Company Name) infrastructure

without documented consent from (Company Name) IT. Furthermore, (Company Name) and (Company Name) IT reserve the right to disable or disconnect some or all services without prior notification.

Release of Liability and Disclaimer to Users of Personal Smartphones Users. (Company Name) hereby acknowledge that the use of a personal Smartphone in connection with (Company Name) business carries specific risks for which you, as the user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.

(Company Name) hereby disclaims liability for the loss of any such data and/or for service interruptions. (Company Name) expressly reserves the right to wipe the Good application (or similar applications) at any time as deemed necessary for purposes of protecting or maintaining the (Company Name) service.

Furthermore, depending on the applicable data plan, the software may increase applicable rates. You are responsible for confirming any impact on rates as a result of the use of: (Company Name) - supplied applications as you will not be reimbursed by (Company Name). Finally, (Company Name) reserves the right, at its own discretion, to remove any (Company Name) - supplied applications from your Smartphone as a result of an actual or deemed violation of the (Company Name) Smartphone Policy.

Employee Declaration

I, [employee name], have read and understand the above *XX Policy*, and consent to adhere to the rules outlined therein.

_____ _____

Employee Signature Date

_____ _____

Manager Signature Date

_____ _____

IT Administrator Signature Date