



Movilidad Corporativa 2008: el reto de la gestión

Alberto Bellé y Jaime García Cantero

Patrocinado por:

SYBASE®



1 CONTEXTO ACTUAL DE MOVILIDAD

1.1 Proliferación de móviles

En todo tipo de organizaciones se está asistiendo a una proliferación de los dispositivos móviles, ya sean éstos para un uso total o parcialmente empresarial. Ahora bien, en muchos casos, las empresas no tienen control directo de los dispositivos móviles utilizados por sus empleados, y ello por varios factores:

- Hay distintos tipos de políticas que favorecen la adquisición de dispositivos móviles. Algunas empresas compran dispositivos móviles para sus empleados, y otras tienen un programa oficial de devolución de los gastos mensuales de móvil.
- Las necesidades de los trabajadores móviles cada vez son más complejas. Cuando las empresas no pueden cubrir esas necesidades (por ejemplo, porque los terminales no son los adecuados), puede que los empleados opten por comprar un dispositivo por su cuenta.

Según estimaciones de IDC, los móviles adquiridos por las empresas representan la minoría de los dispositivos móviles convergentes empleados con fines empresariales, y esta tendencia seguirá sin cambios hasta 2011. Las compras particulares representan en promedio un 60% de los dispositivos móviles convergentes. Este tipo de compras se pueden dividir en dos categorías:

- Usuarios orientados al consumo que pueden hacerse con un dispositivo móvil convergente de empresa.
-
- Usuarios individuales empresariales móviles, quienes comprenden aquellos usuarios que utilizan algún tipo de activo empresarial (por ejemplo, e-mail, aplicación CRM, directorio empresarial, etc.), sin la participación o el apoyo de un departamento informático (IT).

1.2 Personalización

Además de la proliferación de móviles, lo que preocupa a los departamentos de IT es la personalización del dispositivo. Por personalización entendemos un conjunto de comportamientos que pueden tener los usuarios, por ejemplo, almacenar fotos personales y música en un dispositivo que también usan para el trabajo.

La personalización va a incrementarse debido a dos factores:

- El creciente interés de los compradores individuales por los dispositivos móviles convergentes.

- Los avances en la tecnología móvil: puede que los usuarios no quieran realizar todas las tareas que realizarían en un ordenador de sobremesa. No obstante, por su propia naturaleza, el dispositivo móvil es un objeto mucho más personal que un ordenador de sobremesa o un ordenador portátil, lo que origina distintos comportamientos y riesgos y modos de uso.

1.3 Consecuencias

La proliferación de dispositivos móviles, si se produce de manera descontrolada, y la personalización plantean diversas dificultades a los departamentos de IT:

- La gestión de dispositivos móviles que tal vez ni siquiera puedan ser identificados por su solución MDM/de seguridad.
- El incremento del número de sistemas operativos que debe gestionar (por ejemplo, Linux y Mac), lo que aumenta la complejidad.
- Seguridad:
 - Los empleados llevarán dispositivos móviles convergentes a todos lados, con lo cual aumentarán las posibilidades de perderlos y, al tiempo, de perder información empresarial confidencial.
 - Nuevos tipos de dispositivos y aplicaciones.
 - Los teléfonos duales pueden causar preocupación por el mantenimiento de conversaciones VoIP móviles en redes WiFi no seguras.
 - El WiFi por radio es otro punto de acceso al dispositivo al igual que el Bluetooth.
 - Nuevas aplicaciones móviles de voz como por ejemplo las extensiones móviles PBX también pueden ser motivo de preocupación.

Aunque las empresas han ido adoptando paulatinamente soluciones de gestión de dispositivos móviles y de seguridad móvil, IDC estima que la adopción generalizada tan sólo es cuestión de tiempo. Pronto, las empresas más avezadas empezarán a tomar iniciativas para evitar los riesgos.

1.4 El futuro: La computación ubicua

La proliferación de dispositivos no se circunscribe a dispositivos móviles o teléfonos inteligentes, también llamados *Smartphones*. En 2011, se habrán multiplicado por cinco el número de dispositivos distintos de PCs conectados a redes, nos estamos refiriendo, por ejemplo, a teléfonos móviles aptos para Internet, dispositivos de juegos y entretenimiento “en línea”, automóviles, sistemas de automatización y controladores industriales, sin contar con los sensores y las etiquetas RFID.

Se registrarán dos tendencias paralelas: los dispositivos convergerán (teléfonos móviles con más funciones) y, por otro lado, se diferenciarán (dispositivos para un único uso, como los lectores RFID).

La adición de millones de dispositivos a la red hará necesaria la existencia de más sistemas empresariales para su instalación y gestión. Otra consecuencia será que el tráfico predominante pasará del centro de la red a la periferia, procediendo del exterior hacia el interior, lo que afectará a las arquitecturas de las comunicaciones y de la computación.

2 LA GESTIÓN INTEGRAL DE DISPOSITIVOS MÓVILES

Dado que la proliferación de dispositivos móviles ya se ha producido, resulta crucial tener controlada esta multitud de dispositivos de forma segura y estructurada. La clave es:

- Establecer una política sobre dispositivos móviles a nivel empresarial, definiendo los perfiles de usuario y sus necesidades, y los recursos disponibles de IT.
- Aplicar la política de gestión de dispositivos móviles.

2.1 Política de movilidad

Una política de movilidad es un conjunto de procedimientos, dentro de un marco regulador, que sirve de pauta en cuanto al uso de las soluciones móviles de que dispone la organización. La política abarca los dispositivos, las aplicaciones, los recursos, así como los instrumentos de seguridad y de gestión.

Esto ha exigido que, en primer lugar, se planificaran las necesidades de la organización en relación con la tecnología y los recursos IT disponibles y, luego, se definiera una política clara y coherente sobre el uso de ordenadores portátiles.

Los principales pasos para establecer una política de dispositivos móviles son los siguientes:

1. Segmentar los trabajadores móviles en perfiles.
2. Definir las necesidades empresariales y tecnológicas de cada perfil.
3. Aplicar la política de movilidad en la organización: publicarla, implantarla y analizarla periódicamente.

En este documento, se analizan los dos primeros pasos. En todo caso, nos parece que el uso de instrumentos de gestión de movilidad contribuye en gran medida al cumplimiento de la política de movilidad.

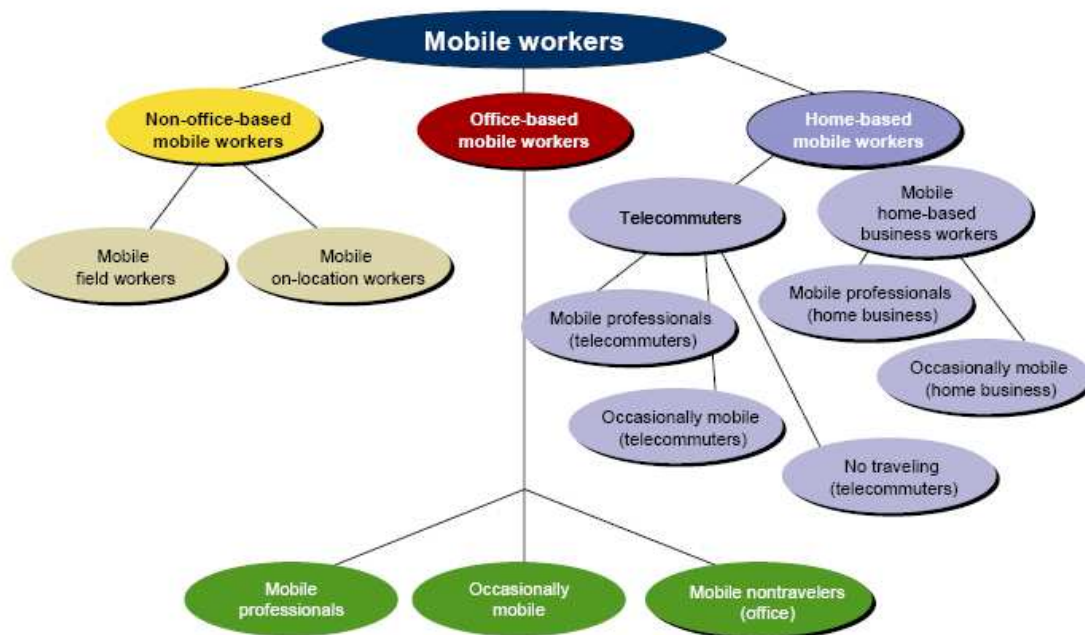
2.1.1 Segmentar los trabajadores móviles en perfiles

El porcentaje de trabajadores móviles ha ido incrementándose constantemente en los últimos años. Se trata de una tendencia que, según IDC, continuará. Se seguirá registrando un crecimiento a medida que el número de trabajadores especializados se acerque al mundo de la movilidad, sobre todo porque las tecnologías inalámbricas emergentes facilitan aún más las posibilidades de que estos trabajadores trabajen fuera de la oficina.

Los trabajadores móviles tienen cargos y responsabilidades diversas. Los departamentos de IT tienen que determinar las funciones y misiones más corrientes dentro de la organización. Una vez definidas, se deberían denominar y describir. No es necesario hacerlo desde cero, hay varias definiciones de perfiles de trabajadores móviles ya disponibles.

IDC define los segmentos prioritarios de trabajadores móviles del modo siguiente (véase la Figura 1):

FIGURA 1: JERARQUÍA DE LA POBLACIÓN DE TRABAJADORES MÓVILES



- Profesionales móviles: los profesionales móviles son aquellos empleados que están fuera de su lugar de trabajo principal un 20% o más de su tiempo. Por lo general, estos empleados son ejecutivos que viajan, consultores,

representantes de ventas, agentes de seguro, representantes farmacéuticos y otros, por ejemplo, los profesionales del sector sanitario. A los profesionales móviles se les considera viajeros cuando están en tránsito, de un sitio a otro, y visitantes cuando llegan.

- Profesionales ocasionalmente móviles: estos trabajadores móviles son aquellos que pueden participar en algunas actividades móviles fuera de su lugar de trabajo principal pero que no encajan en la categoría de profesionales móviles que están fuera de sus oficinas al menos el 20% de su tiempo. Estos empleados pueden ser móviles tan sólo unas cuantas veces al año, o menos del 20% de sus jornadas laborales mensuales.
- Teletrabajador: los teletrabajadores son empleados que trabajan en sus casas durante el horario comercial normal. El mínimo que un teletrabajador trabaja en su casa es tres días o más al mes, y puede que algunos ni siquiera trabajen en oficinas tradicionales. Estos trabajadores suelen haber suscrito un acuerdo informal con su empleador y su supervisor, o bien el acuerdo de trabajo pueden estar más formalizado y figurar en una política y contrato por escrito.
- Autónomos con oficina en casa: en este grupo de trabajadores móviles cabe incluir a todos aquellos que trabajan por cuenta propia. Este grupo consta de profesionales móviles y profesionales ocasionalmente móviles.

2.1.2. Definir las necesidades de cada perfil

Cada perfil tiene distintas necesidades tecnológicas, de ahí la necesidad de disponer de múltiples dispositivos y aplicaciones. Los departamentos de IT tendrán que sopesar estas necesidades con la consecución de un cierto nivel de simplicidad a fin de facilitar su gestión. En particular, tendrán que decidir el número de dispositivos y aplicaciones distintas que se aceptarán.

A fin de determinar estas necesidades, IDC propone evaluar cuatro factores:

- Grado de movilidad: determinar la cantidad de tiempo que un empleado pasa fuera de su entorno de trabajo principal en dos aspectos:
 - Proporción de tiempo pasado fuera,
 - Distancia del lugar de trabajo (por ejemplo, moverse dentro del recinto empresarial, viajar dentro de límites metropolitanos, o viajar entre varias ciudades, o internacionalmente).
- Acceso a la información en tiempo real, o acceso asíncrono. La necesidad de acceso a la información en tiempo real para realizar la función laboral. Deberían evaluarse en términos de coste, batería, consumo de ancho de banda y recursos del servidor utilizados las implicaciones en IT que suponen los empleadores permanentemente en línea.
- Las aplicaciones a las que se precisa acceder: correo electrónico empresarial, aplicaciones *backoffice*, o aplicaciones específicas del puesto.
- La confidencialidad de la información a la que se accede/o que se almacena y las incidencias en la seguridad. La cantidad de información confidencial

almacenada en el dispositivo y el riesgo asociado de robo o pérdida del dispositivo, así como las repercusiones regulatorias o de cumplimiento.

2.2 Soluciones de gestión de dispositivos móviles

Poner en marcha una solución de gestión de dispositivos móviles es el paso lógico tras la aplicación de una política generalizada sobre dispositivos móviles.

Hay varios factores que están llevando a la adopción de estos instrumentos.

2.2.1 La estandarización de los sistemas operativos móviles es un desafío

Las empresas cada vez tendrán más dificultades para intentar estandarizar en un único sistema operativo móvil. Los empleados cada vez más quieren elegir su dispositivo móvil y usarlo para su trabajo. Los dispositivos móviles convergentes solían ser un símbolo de estatus en los ejecutivos de alto nivel pero, hoy en día, hay múltiples modelos destinados tanto al mercado empresarial como al mercado de consumo, y muchos de estos móviles se utilizan para ambos propósitos.

Aunque un dispositivo móvil pueda estar destinado al mercado empresarial y otro al de consumo, si llevan el mismo sistema operativo, en él se pueden emplear, en su mayoría, las mismas aplicaciones. Las empresas pueden optar por tener una política de mutismo (ni preguntes ni lo cuentes), y arriesgar la integridad de la red, o bien ser realistas sobre la situación y decidir utilizar sistemas operativos múltiples.

2.2.2 Diferentes necesidades funcionales de la gestión de los dispositivos móviles por tipo de dispositivo

Existen diversas funcionalidades necesarias en un producto de gestión de dispositivos móviles, dependiendo de los tipos de dispositivos móviles que se estén usando en la empresa.

En el pasado, los productos de gestión de dispositivos móviles solían estar orientados hacia dispositivos reforzados y/o incuistrados que se usaban para un objetivo industrial vertical específico, y que se conectaban a través de una red inalámbrica no móvil. En estos casos, lo más importante era que las aplicaciones se mantuvieran actualizadas y en funcionamiento.

A medida que las funcionalidades de los dispositivos móviles convergentes se incrementan, cada vez hay más conciencia de que estos dispositivos tienen que ser gestionados del mismo modo que cualquier otro dispositivo cliente. Además, los dispositivos móviles convergentes de hoy en día pueden almacenar información empresarial confidencial y, por tanto, su gestión es crucial.

2.2.3 Estructura corporativa

En muchos sectores, la necesidad de cumplir con las normativas corporativas será el factor clave para adoptar una gestión de dispositivos móviles. De hecho, el mantenimiento de registros de conformidad podría alentar iniciativas en otros ámbitos, a medida que las empresas modifican su conducta. Por ejemplo, tendrá una incidencia positiva en el gasto en software de infraestructura que contribuya a archivar, proteger y recuperar datos. Las inversiones en temas de conformidad parecen justificarse gracias a las eficiencias obtenidas en las operaciones empresariales.

2.2.4 Aplicaciones móviles

Las aplicaciones móviles emergentes, por ejemplo, las extensiones de PBX móviles, contribuirán a incentivar el interés en la gestión de dispositivos móviles en los años venideros.

2.3 Demanda de soluciones MDM

2.3.1 Características de una solución MDM

A un nivel general, hay diversos elementos que el mercado está pidiendo o que pedirá en el futuro:

- Compatibilidad con la infraestructura de IT cliente existente,
- Sencillez de soporte y mantenimiento,
- Perspectiva pormenorizada para garantizar que:
 - Los dispositivos que se puedan necesitar en el futuro también tengan cabida,
 - Las necesidades y aplicaciones pueden variar, y se pueden adoptar los cambios oportunos.
- Políticas y características necesarias para cumplir con las necesidades de conformidad y seguridad.
- Arquitectura adecuada de la solución: por ejemplo, si una empresa dispone de muchos usuarios diseminados por el mundo, una funcionalidad como la instalación con tecnología OTA resulta imprescindible,
- Equilibrio apropiado entre facilidad de uso y seguridad,
- Exhaustividad e inclusión de una serie de funciones avanzadas que cubran las necesidades específicas de los perfiles móviles.

2.3.2 Proveedores de MDM: Matriz de liderazgo de IDC

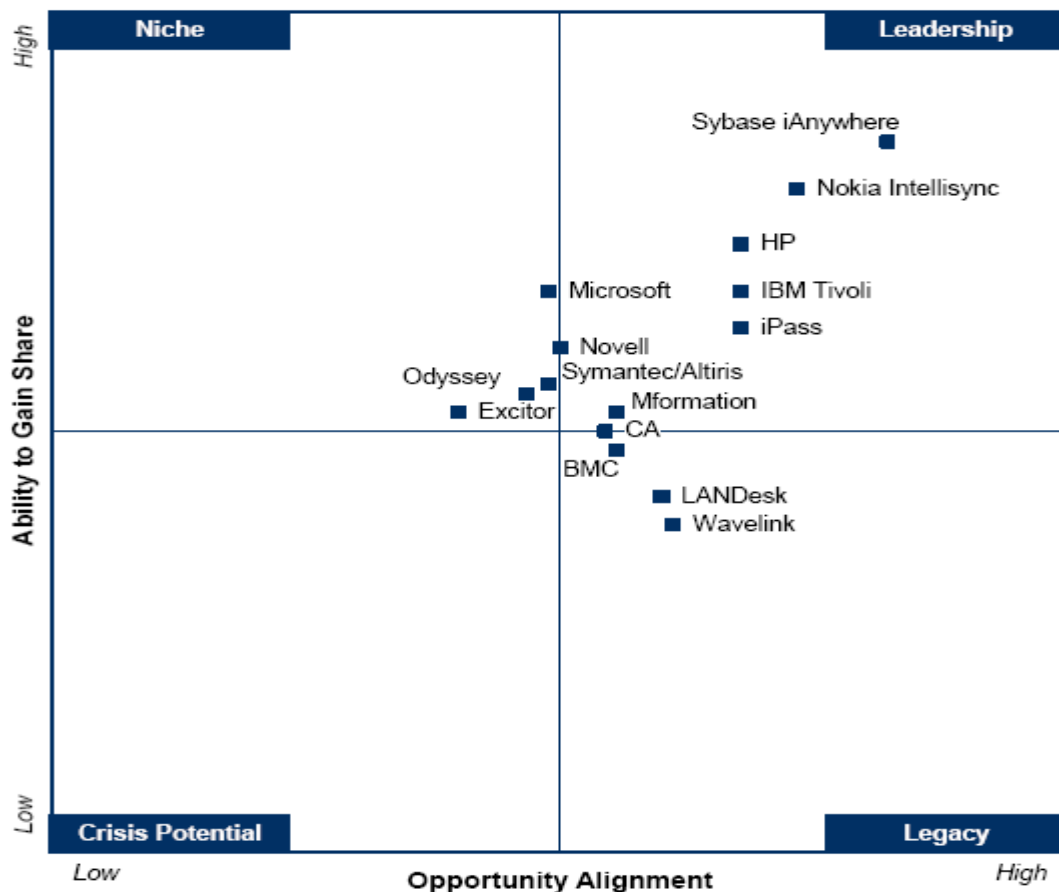
La matriz de liderazgo de IDC ofrece una comparación cualitativa de los proveedores dentro del mercado empresarial de gestión de dispositivos móviles. Es una representación ilustrada de la posición de cada proveedor dentro del mercado, basándose en dos factores: la capacidad del proveedor para obtener cuota de mercado y su adecuación con las oportunidades futuras de mercado.

En el eje de abscisas se mide la adecuación del proveedor con las oportunidades o su capacidad de influir en tendencias esenciales en el mercado a lo largo del periodo de previsión, así como el potencial de crecimiento del proveedor y su capacidad para convertirse en un actor clave en el mercado.

El eje de coordenadas representa la capacidad del vendedor a la hora de obtener cuota de mercado, basándose en cuestiones como los canales y la fortaleza en finanzas, la percepción de la clientela, y sus socios.

A continuación figura la matriz de IDC para gestión de dispositivos móviles:

FIGURA 2: MATRIZ DE LIDERAZGO DE IDC: MERCADO EMPRESARIAL DE GESTIÓN DE DISPOSITIVOS MÓVILES



3. SEGURIDAD

La seguridad cada vez es más importante. Esta tendencia queda ejemplificada en el hecho de que la mayoría de los productos de gestión de dispositivos móviles incluyen ahora sistemas remotos de bloqueo/borrado de los dispositivos, como elemento de verificación de la funcionalidad.

En realidad, cada vez resulta más difícil diferenciar claramente entre los mercados de seguridad móvil y de gestión de dispositivos móviles ya que la seguridad móvil es una pieza clave de la gestión de los dispositivos de seguridad.

Hay varios factores que están haciendo de la seguridad un aspecto cada vez más relevante:

- El elevado nivel de crecimiento previsto del mercado de dispositivos móviles convergentes está incrementando la necesidad de garantizar la seguridad y gestión de estos dispositivos.
- El aumento de dispositivos para consumidores profesionales (*prosumers*) ha generado una mayor preocupación por la seguridad debido a que los empleados quieren usar sus dispositivos personales tanto para el trabajo como para su uso personal.
- La seguridad es una cuestión fundamental en todos los sectores, no sólo los blancos más obvios. Los empleados de cualquier sector pueden perder los dispositivos móviles con información empresarial confidencial.
- Al contrario de lo que pueda parecer, el software cada vez es más vulnerable. Los piratas informáticos y similares siguen encontrando maneras de dar mal uso al software de otros. Inicialmente, esto lo hacían explotando una vulnerabilidad, pero ahora están encontrando maneras de piratear software sin vulnerabilidades.

Hay dos aspectos que condicionarán el mercado de seguridad de los dispositivos:

3.1 Protección y control de la información

El filtrado de datos de gran confidencialidad a través de dispositivos móviles y ordenadores portátiles sigue haciendo de la protección y control de la información (IPC) una prioridad fundamental para la seguridad móvil. El acceso a información confidencial se ha convertido en la mayor amenaza para la seguridad de las redes empresariales (Informe de Seguridad de IDC, 2007). Por primera vez en los ocho años que IDC lleva elaborando su informe de seguridad anual, los troyanos, virus y otros tipos de códigos maliciosos han sido destronados como aspectos esenciales de las amenazas a la seguridad empresarial.

La protección y el control de información para dispositivos móviles y ordenadores portátiles abarcan tecnologías de prevención de la pérdida de datos y de encriptado

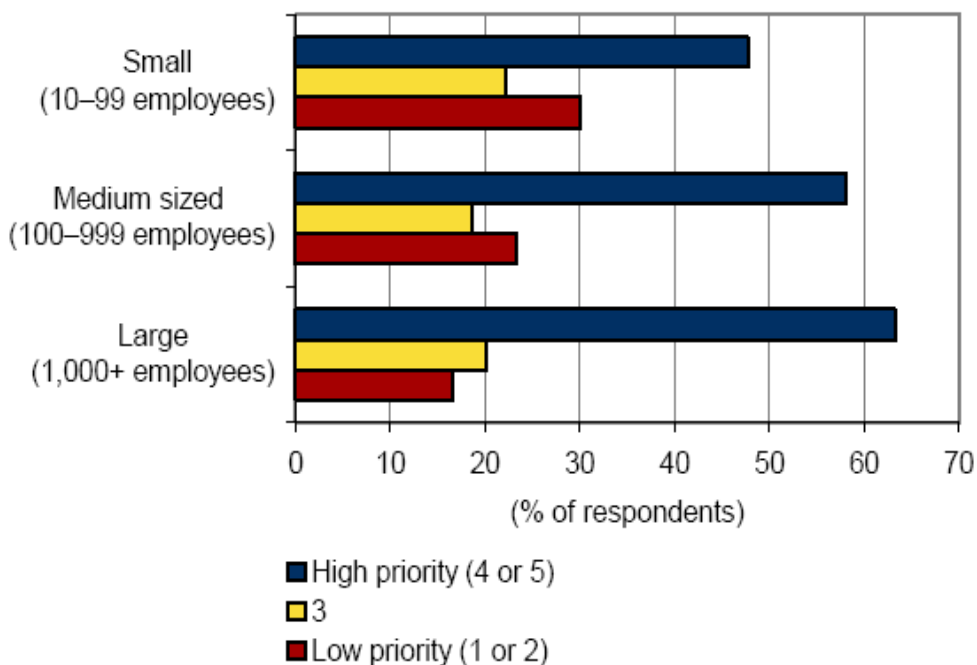
de ficheros y discos. La proliferación de dispositivos móviles que permiten a los empleados sacar información confidencial de los límites de la propia empresa dificulta sobremanera el control de la información. De hecho, un 63% de las grandes empresas consideran una prioridad básica la securización de los dispositivos móviles para evitar fugas de datos y violaciones de conformidad, como se refleja en el gráfico de más abajo.

IDC también ha descubierto que:

- Un 50% de las empresas que han sufrido una fuga de datos sostuvieron que ésta se debió a un ordenador portátil perdido o robado. Además, otro 33% indicó que había sido a causa de un dispositivo móvil perdido o robado (PDA, Smartphone, etc.).
- Un 40% de las empresas usan en la actualidad soluciones de protección y control de la información (IPC) para dispositivos móviles y otro 39% están evaluando soluciones IPC para proteger la información almacenada (también denominada “datos en reposo”) en los próximos 12 meses.
- Cada vez son más las denuncias presentadas por robos de ordenadores portátiles y dispositivos móviles. IDE estima que el coste de los dispositivos en sí (ordenadores portátiles, dispositivos móviles, etc.) es insignificante, en comparación con el coste de los datos almacenados en el dispositivo.

FIGURA 3: IMPORTANCIA DE “SECURIZAR” DISPOSITIVOS MÓVILES

Importance of Securing Mobile Devices to Prevent Data Leaks and Compliance Violations by Company Size



3.2 *Malware* a través de móviles

En el mundo móvil, al igual que en el mundo alámbrico, los motivos y la intención de los piratas informáticos y los creadores de virus han pasado a ser el fraude y las ganancias financieras. El robo de información es el objetivo. Se está desarrollando software malintencionado, o *malware*, y software espía, o *spyware*, a través de móviles para ofrecerles a los piratas informáticos, o a cualquier persona dispuesta a pagar, el acceso a información confidencial almacenada en dispositivos móviles. Además, como la realización de transacciones financieras a través de dispositivos móviles aumenta, los creadores de virus dirigirán su atención al mundo móvil.

Pese a la mayor complejidad del *malware* vía móviles en 2007, el grado de amenaza sigue siendo bastante escaso. Varias fuentes del sector calculan que el número de virus móviles existentes a fines de 2007 se elevará a aproximadamente 400, lo que no tiene ni punto de comparación con el número de virus para PCs.

Con todo, IDC estima que atacantes más experimentados, con frecuencia pertenecientes al crimen organizado, recurrirán cada vez más al *malware* y *spyware* para móviles a fin de obtener números de tarjetas de crédito, información de cuentas bancarias y otros datos confidenciales.

A medida que los dispositivos móviles adquieran más funcionalidades, el *malware* por móvil hará lo propio. Los dispositivos móviles pronto rivalizarán con los PCs en cuanto a potencia computacional y capacidad de almacenamiento. IDC opina que la motivación crematística supondrá un incremento en el número, la complejidad, la frecuencia y la dureza de los ataques dirigidos contra dispositivos móviles en los dos próximos años.

Pese a la adopción de políticas de seguridad, los usuarios finales tienen la responsabilidad de garantizar el mantenimiento de las políticas de seguridad, una vez que éstas han sido adoptadas. Es tarea de la empresa cerciorarse de ofrecerles formación sobre esas políticas y asegurarse de que entienden la importancia que revisten.

4. MIDDLEWARE

Una solución *middleware* para móviles es una plataforma de software que incluye un software servidor y/o cliente que amplía el alcance de las aplicaciones existentes por IP u otras aplicaciones críticas para una misión (por ejemplo, *groupware*, mensajería, gestión de relaciones con los clientes, automatización de la fuerza de ventas, planificación de recursos de empresa, anfitriones, u otras aplicaciones), o bien ofrece la posibilidad de concebir nuevas aplicaciones para usuarios móviles aprovechando diversos dispositivos inalámbricos, en particular, ordenadores portátiles, dispositivos *handhelds*, teléfonos móviles y otros dispositivos móviles convergentes.

El *middleware* para móviles puede comprender la plataforma, las aplicaciones *front-end* y las herramientas de desarrollo en un solo producto. El software *middleware* para móviles también puede ofrecerse como un servicio alojado en un servidor.

La tendencia general, según ha averiguado IDC, es que las empresas cada vez muestren más interés por disponer de una plataforma de movilidad. Es probable que no deseen tener un proveedor de correo electrónico móvil, otro para gestión y seguridad de los dispositivos y otro más para las aplicaciones móviles de voz.

Cuando se opta por una solución *middleware*, la demanda va a favorecer las soluciones neutras en cuanto a red, y a arquitectura *back-end*. También preferirá una solución integrada que ofrezca una clara estrategia para aplicaciones móviles, más allá del correo electrónico. En resumen, el mercado favorecerá una solución capaz de movilizar cualquier aplicación y cualquier servidor hacia cualquier dispositivo.

Además, las empresas buscan una plataforma ampliable que crezca a medida que un número mayor de aplicaciones empresariales pasen a ser móviles. Un aspecto crítico en la selección de la plataforma *middleware* es la capacidad de la misma de sincronizar datos desde/a los dispositivos móviles con bases de datos centrales, buses de mensajes, web services, etc ... de una forma transparente que incluya la resolución de conflictos y la gestión de interrupciones en la conexión a la red.

A continuación figura la matriz de liderazgo de IDC.

FIGURA 4: MATRIZ DE LIDERAZGO DE IDC SOBRE EL MERCADO DE MIDDLEWARE PARA MÓVILES



5. CONCLUSIONES:

- Las empresas tienen que actuar de manera proactiva e implantar una estrategia de movilidad para toda la compañía en vez de intentar arreglar problemas de movilidad según van surgiendo. Deben aplicar una política de movilidad generalizada.
- Los departamentos de IT tendrán que regular los recursos que asignan a cada categoría de perfil de usuario para sacar el máximo partido a los recursos IT

disponibles. Todo acceso innecesario a aplicaciones en tiempo real tiene repercusiones en el ancho de banda, el coste y el uso de servidores.

- Cada vez resulta más difícil estandarizarse en un solo tipo de dispositivo y, por ende, las empresas tendrán que abarcar varios SO móviles.
- Las empresas que instalan cualquier aplicación móvil, incluido el correo electrónico, tienen que tratar los dispositivos móviles convergentes como cualquier otro dispositivo que se conecte a la red y puede almacenar información confidencial de la compañía.
- Las cuestiones de seguridad cada vez son más importantes: si se pierde o roba un dispositivo las funcionalidades de borrado y bloqueo son fundamentales en cualquier solución de gestión de dispositivos móviles. No obstante, disponer de una funcionalidad de copias de seguridad y recuperación reviste idéntica importancia para mantener la productividad de los trabajadores móviles. La demanda de estas funcionalidades va a ser cada vez mayor.
- Los mercados de gestión de dispositivos móviles (MDM) y de seguridad móvil cada vez convergen más.
- La demanda empresarial está favoreciendo la aparición de una solución middleware que pueda movilizar cualquier aplicación o cualquier servidor hacia cualquier dispositivo.