Deloitte.

La Seguridad del Dispositivo Móvil

Traiga su Propio Dispositivo

Andrés Casas, Director

15 de Marzo de 2012

Definiendo Dispositivos Móviles

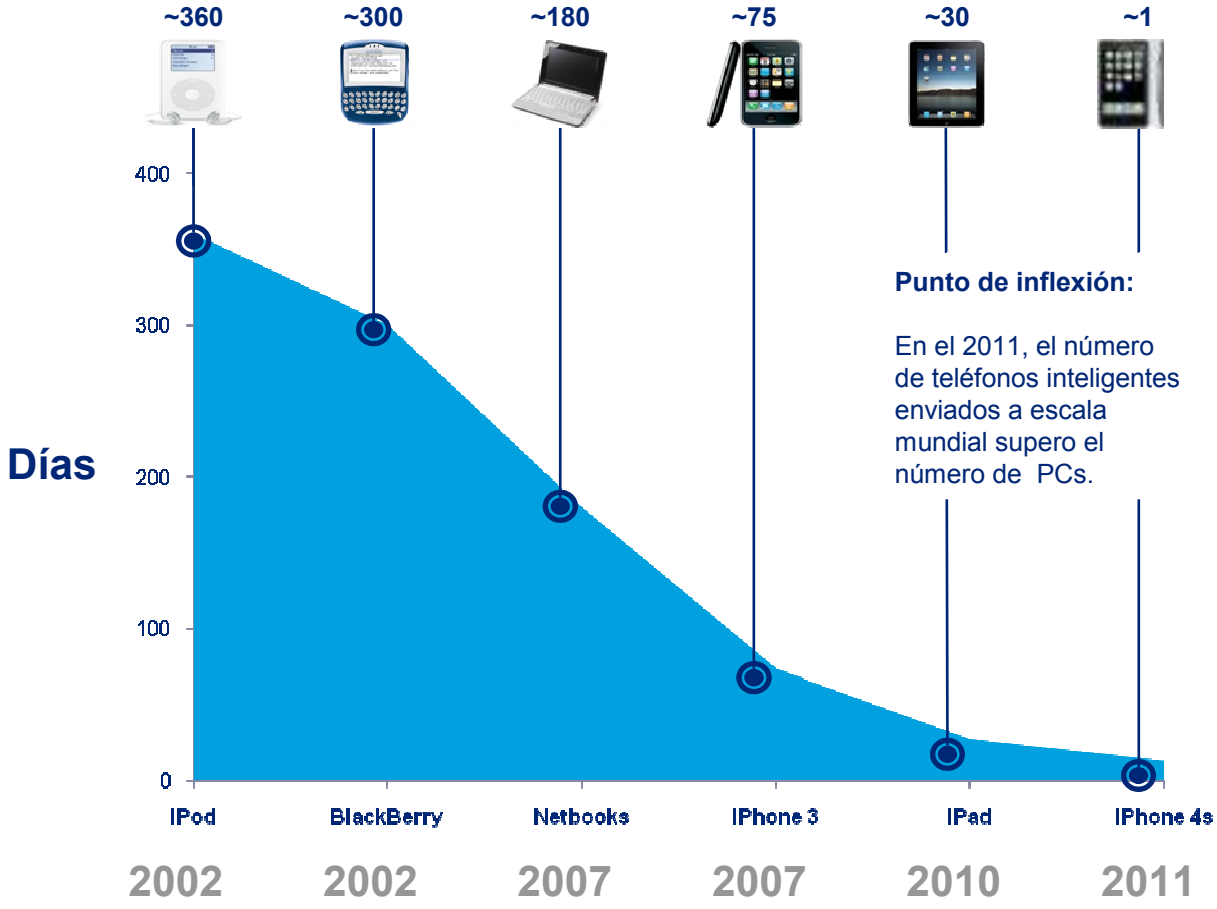
© 2012 Deloitte

La movilidad y la conectividad persisten - han cruzado el punto de inflexión

La inversión continúa, el hardware/software de la innovación se traducirá en los dispositivos móviles y sistemas operativos cada vez más potentes, alimentando cada vez más la demanda de los consumidores.

Conductores de adopción de tecnología

Número de días para llegar a 1 millón de unidades vendidas



© 2012 Deloitte

Tendencias del Dispositivo Móvil

- Los empleados se distribuyen y requieren apoyo a la movilidad
- La demanda para apoyar los dispositivos personales (Trae tu propio dispositivo/ Consumo).
- Presión para crear aplicaciones móviles y adopción de "socialmente conectados" aplicaciones.
- El uso de aplicaciones sin saber qué riesgos se introducen.
- Aplicaciones inseguras.
- Aumente productividad y reduzca costos:
  - All Nippon Airways - 6000 iPads, 400 millones yen (3.89 millones de euros) ahorros anuales.
  - El Senado del parlamento Holandés sustituye los documentos parlamentarios impresos con el iPad.

La administración de dispositivos móviles y la seguridad son importantes desafíos.

© 2012 Deloitte

Aplicaciones empresariales extendidas a dispositivos móviles

Nuevas oportunidades para la habilitación de ventas, atención al cliente y la interacción con socios, la productividad del empleado, aceleración de procesos de negocio y acceso instantáneo a los análisis de información.

© 2012 Deloitte

Tendencias tecnológicas móviles previstas

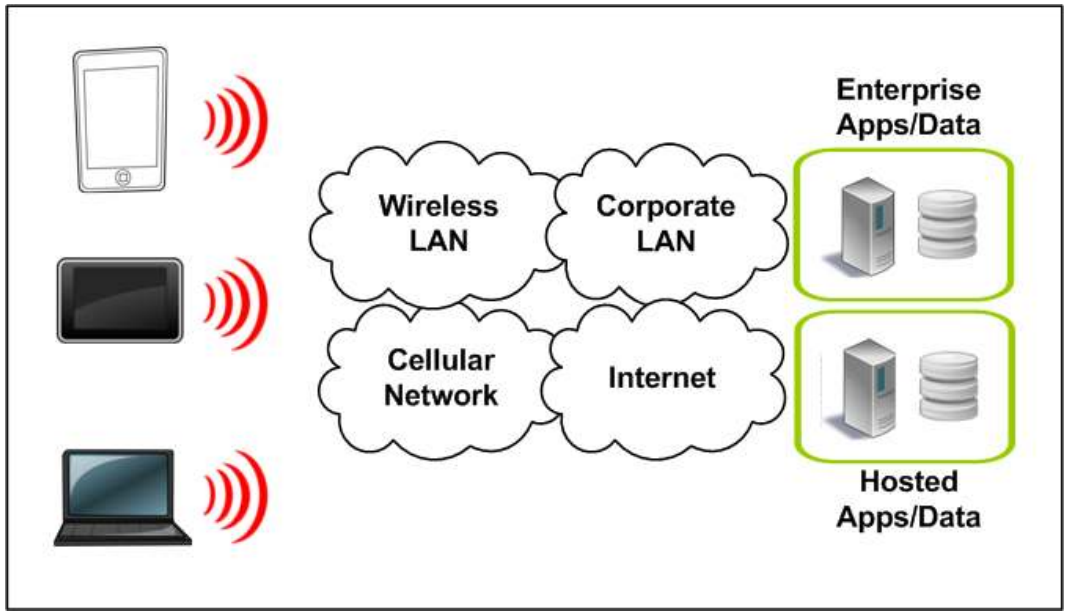
Dispositivos Móviles	• Mejoras de rendimiento de hardware y la consolidación de chipset es probable que continúe, lo que viene a dar: - Más potente, más delgado, más ligero y aparatos de energía eficientes, con un rendimiento similar al escritorio. - Soporte para aplicaciones de negocios más poderosas, consumo de aplicaciones y juegos. •Las teclcos que puedan seguir apoyando a varios proveedores de teléfonos para beneficiarse de la competencia entre proveedores. • Las telcos que puedan seguir ofreciendo los dispositivos con diferentes estilos y precios para atraer a diferentes segmentos del mercado.
Hardware privativo	• GPS es probable que sea estándar, permitiendo el uso generalizado de aplicaciones de localización. • La Cámara es probable que sea estándar, permite en tiempo real compartir fotos, videoconferencia, proyección de imágenes, escaneo de código de barras y la superposición de realidad aumentada. • Near Field Communications (NFC) es probable que sea estándar permitiendo el **pago de móvil** generalizado. • Los sensores son propensos a ser cada vez más presentes en los dispositivos, creando nuevas oportunidades de recolección de datos.
Tecnología Inalámbrica	• Las telcos son propensas a seguir invirtiendo en el espectro, las torres y la tecnología inalámbrica, lo que lleva a una mayor cobertura de alta velocidad, las conexiones más confiables y mayor velocidad de conexión. • Los dispositivos móviles están dispuestos a apoyar múltiples tecnologías inalámbricas y la transición transparente a través de interiores, exteriores, zonas urbanas, suburbanas y rurales. • Incorporado Wi-Fi permite la cobertura en interiores.
Sistemas de funcionamiento móvil	• Los ciclos de liberación rápida, es probable que continúen acorde a la lucha de los proveedores por la cuota de mercado mediante la innovación. • Adiciones continuas de características mejoran la experiencia del usuario. • Las telcos no están motivados para empujar actualizaciones del sistema operativo, prefieren actualizar contrato con dispositivo y volver a comprometerse, durante 24 meses. • La consolidación de sistema operativo es probable que sea limitado, debido al deseo de soporte para la competencia. • Reconocimiento de voz, realidad aumentada, los servicios basados en localización convirtiendo rápidamente en la corriente principal.

Los dispositivos móviles pueden llegar a ser más poderosos y ricos en sensores.
El hardware y el entorno de sistema operativo móvil es probable que permanezcan heterogéneo y volátil.

La Nube Móvil

Cuando se combina con la computación en nube, los usuarios pueden alternar entre los computadores desktop, computadores portátiles, tablets y smartphones a lo largo del día.

- Movilidad entre dispositivos cuando se accede a la misma aplicación en el transcurso del día.
- Movilidad entre redes inalámbricas cuando se accede a la misma aplicación en el transcurso del día
- Moverse entre los servidores de aplicaciones y servidores externos desde el mismo dispositivo a través de cualquier red inalámbrica.



Los dispositivos móviles pueden llegar a ser más poderosos y ricos en sensores. El hardware y el entorno de sistema operativo móvil es probable que permanezcan heterogénea y volátil.

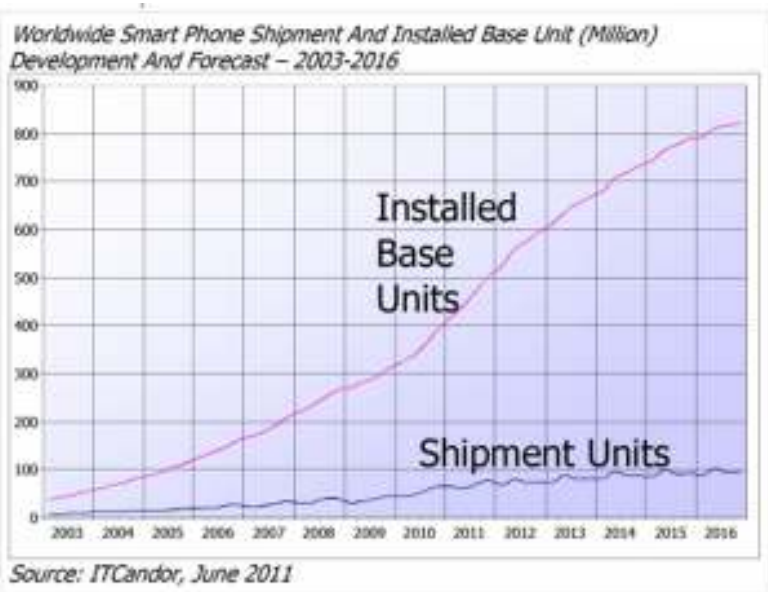
© 2012 Deloitte

© 2012 Deloitte

Dispostivos Móviles: Un desafío de la seguridad

Figure 1 The Top Five Priorities For Forrester's Security & Risk Council

Source: Forrester Research, Inc.



© 2012 Deloitte

La seguridad móvil en los titulares

Android bug lets attackers install malware without warning

Google patch cycle puts users at risk

By **Dan Goodin in San Francisco** · **Get more from this author**

Posted in Malware, 20th September 2011 19:40 GMT

OFFICE HARDWARE Jun 11, 2010 6:00 pm

iPad 3G Leak Flaw More Common than You Think

By Tony Bradley, PCWorld

AT&T is taking some well-deserved heat for a Web security flaw resulting in the exposure of more than 114,000 iPad 3G owners' e-

Complete PCWorld Coverage

Dropbox Security Breach- Protect your network and users from Mobile Security Risks!

June 22nd, 2011

Hacked: Scarlett Johansson & Mila Kunis Mobile Phones

Written on September 16, 2011 by Chilton Tippin in Mobile, Privacy and Security

99.7% of Android smartphones can leak data?

Edwin Kee 05/17/2011 07:22 PDT

SpyEye hacking kit adds Android infection to bag of tricks

Intercepts text messages bank use as secondary authentication for account access

By Gregg Keizer

September 13, 2011 01:47 PM ET Add a comment Like 29 +1 10

New Hack Turns Smartphones Into Covert Spying System

The Huffington Post | Amy Lee | First Posted: 01/19/11 09:39 AM | Updated: 01/19/11 09:39 AM

News

Report: Smartphone malware rises by 273 per cent in 2011

POSTED BY ROBERT LEEDHAM ON THE 13TH SEPTEMBER 2011

Smartphone virus attacks soar

Smartphones including the iPhone and Google Android devices are under increasing threat from computer virus writers aiming to steal money and personal data from users.

By Christopher Williams, Technology Correspondent

12:45PM GMT 08 Feb 2011

Former Cybersecurity Czar Says Smartphones Create Security Problems

By Ellen Messmer

Mon, September 19, 2011

iPhone keeps record of everywhere you go

Privacy fears raised as researchers reveal file on iPhone that stores location coordinates and timestamps of owner's movements

Charles Arthur

guardian.co.uk, Wednesday 20 April 2011 14.06 BST

Article history

© 2012 Deloitte

Necesidad de un gobierno de dispositivos móviles

En los últimos años hemos sido testigos de:

- Rápida introducción de dispositivos móviles
- Aumento en el panorama de riesgos
- Inseguridad tecnológica
- Presión de usuarios vrs presión del negocio/TI adoptando nuevas tecnologías
- Trae tu propio dispositivo/Consumo
- Popularidad entre los usuarios técnicos y no técnicos
- Mezcla de empresa y agendas personales
- Erupción de iniciativas y proyectos de dispositivos móviles
- Enlace a los medios sociales y soluciones en la nube

Quién posee la estrategia de dispositivo móvil y el modelo de gobierno?

© 2012 Deloitte

Trae tu propio dispositivo

Los empleados quieren cada vez más utilizar su dispositivo móvil favorito para su uso personal y empresarial. Se desea almacenar los datos personales e instalar los juegos en Internet en los dispositivos, también se utilizan para acceder a aplicaciones y datos empresariales.

Si los empleados compran su propio dispositivo y el plan, esto puede reducir los costos de Telecomunicaciones, sin embargo, crea varios retos de negocio y riesgos de seguridad.

BYO Base Lógica

- Perspectiva del usuario:
  - Deseo de un dispositivo y un número, no dos.
  - Deseo de un propio proceso de selección a la hora de escoger un dispositivo móvil.
  - Deseo de las últimas actualizaciones (trabajadores jóvenes)
  - Tienda local ofrece una mejor selección que el departamento de TI.
- Perspectiva de la compañía:
  - Aumento de la productividad del personal debido a un mejor estado de ánimo y hardware.
  - Potencial para reducir el hardware, el servicio mensual, el aprovisionamiento y los costos del soporte.
- Perspectiva del departamento de TI
- Potencial para reducir la carga de trabajo del personal como los usuarios se mueven fuera de los dispositivos, provisto por el empleador y los dispositivo.

BYO Retos

- Seguridad
  - Datos de la empresa, confidencialidad, integridad y disponibilidad.
  - Responsabilidad de los datos personales.
  - Definiendo y reforzando el perímetro de seguridad
- Solicitud de grietas
  - Impacto del entorno de dispositivos heterogéneos en del desarrollo de aplicaciones y necesidades de apoyo.
- Soporte
  - Certificación de equipos, aprovisionamiento y administración.
- Costo
  - Posible pérdida de descuentos por volumen a nivel corporativo, debido a la compra personal.

Las empresas deben alinear las expectativas de los usuarios, Las capacidades de TI y la política de seguridad. La falta de acción puede aumentar el riesgo de seguridad y como los dispositivos móviles continúan administrados para conectarse a la red de la empresa.

Mobile Device Security Challenges

Área	Retos	Retos adicionales – trae tu dispositivo
Gobierno/Política	Política, Uso aceptable, Monitoreo, Incumplimiento.	Aplicación de la política, Monitoreo.
Aplicaciones Móviles	Aplicaciones no autorizadas, Fuga de datos, Vulnerabilidades en las aplicaciones, Autenticación débil.	Aplicaciones que causan fuga de datos corporativos.
Sistemas operativos móviles.	Desbloqueo, distribución de aplicaciones, almacenamiento en la nube.	Almacenamiento de datos.
Dispositivo móvil	Robo de dispositivos,autenticación débil, virus, uso inapropiado	Limpieza remota Acceso controlado (niños) Ejecución de líneas de base de seguridad.
Red Inalámbrica	Escuchas no autorizadas	
Red Core	Escuchas no autorizadas, acceso no autorizado.	
Administración	Rápido cambio de la tecnología, falta de experiencia, ciclo de vida de la administración.	Desmantelamiento de los dispositivos con los datos corporativos
Operaciones	Integración de TI en el soporte a procesos, Proporcionar diagnósticos.	Soporte
Legal/Regulatorio	Privacidad, Auditoría	Refuerzo de políticas, auditoria.

© 2012 Deloitte

© 2012 Deloitte

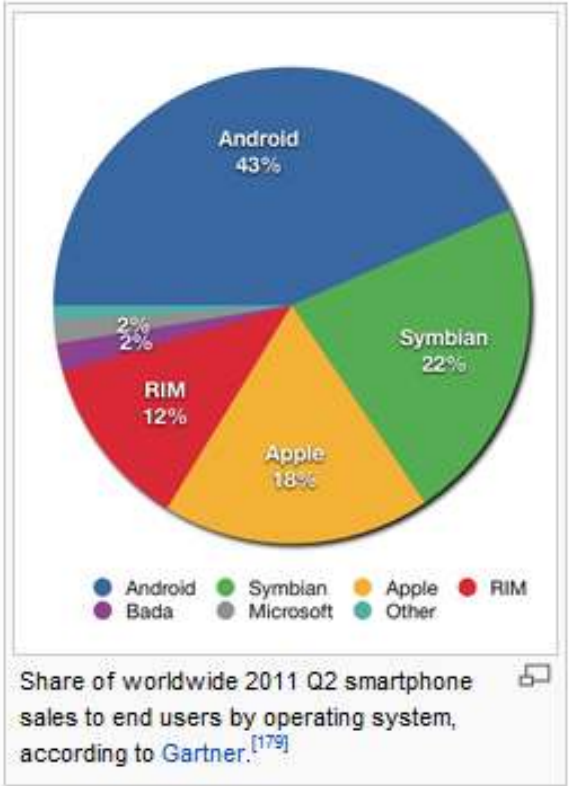
Los riesgos de seguridad en disposiivos móviles

El alto nivel de riesgos en la seguridad de dispositivos móviles no son diferentes de los tradicionales riesgos de seguridad de TI. El verdadero desafío es que los dispositivos móviles introduce nuevas vulnerabilidades y vectores de ataque para las áreas de riesgo tradicionales.

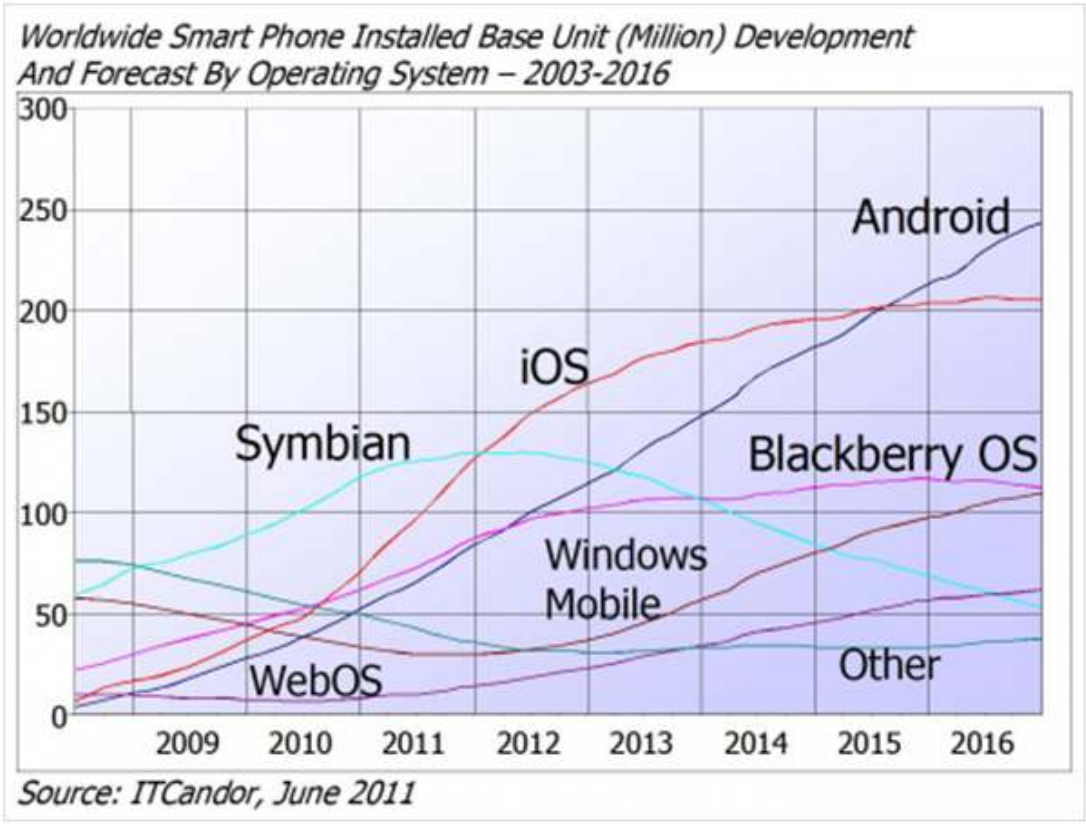
Topic	Risks
Gobierno	• No existe un marco de gobierno claro. • Falta de comprensión de riesgos.
Seguridad de la información	• Ineficacia de los controles de acceso a dispositivos de móviles y socios. • Prevención de ataques maliciosos. • Inefectividad en los procesos de control de virus/actualizaciones en seguridad. • La falta de procesos de supervisión para responder a las amenazas actuales
Privacidad/Protección de datos	• Acceso no autorizado a datos personales. • Cumplimiento de leyes transfronterizas, almacenamiento en alta mar. • Fuga de datos.
Administración en la continuidad del negocio.	• Incapacidad para recuperar datos. • Disponilbilidad de recursos críticos.
Gestón del cambio	• Cambio en el control de procesos. • Pruebas antes de la implementación. • Acceso al ambiente de producción.

© 2012 Deloitte

Sistemas operativos en móviles



Share of worldwide 2011 Q2 smartphone sales to end users by operating system, according to Gartner.[179]



© 2012 Deloitte

Características de seguridad en un sistema operativo

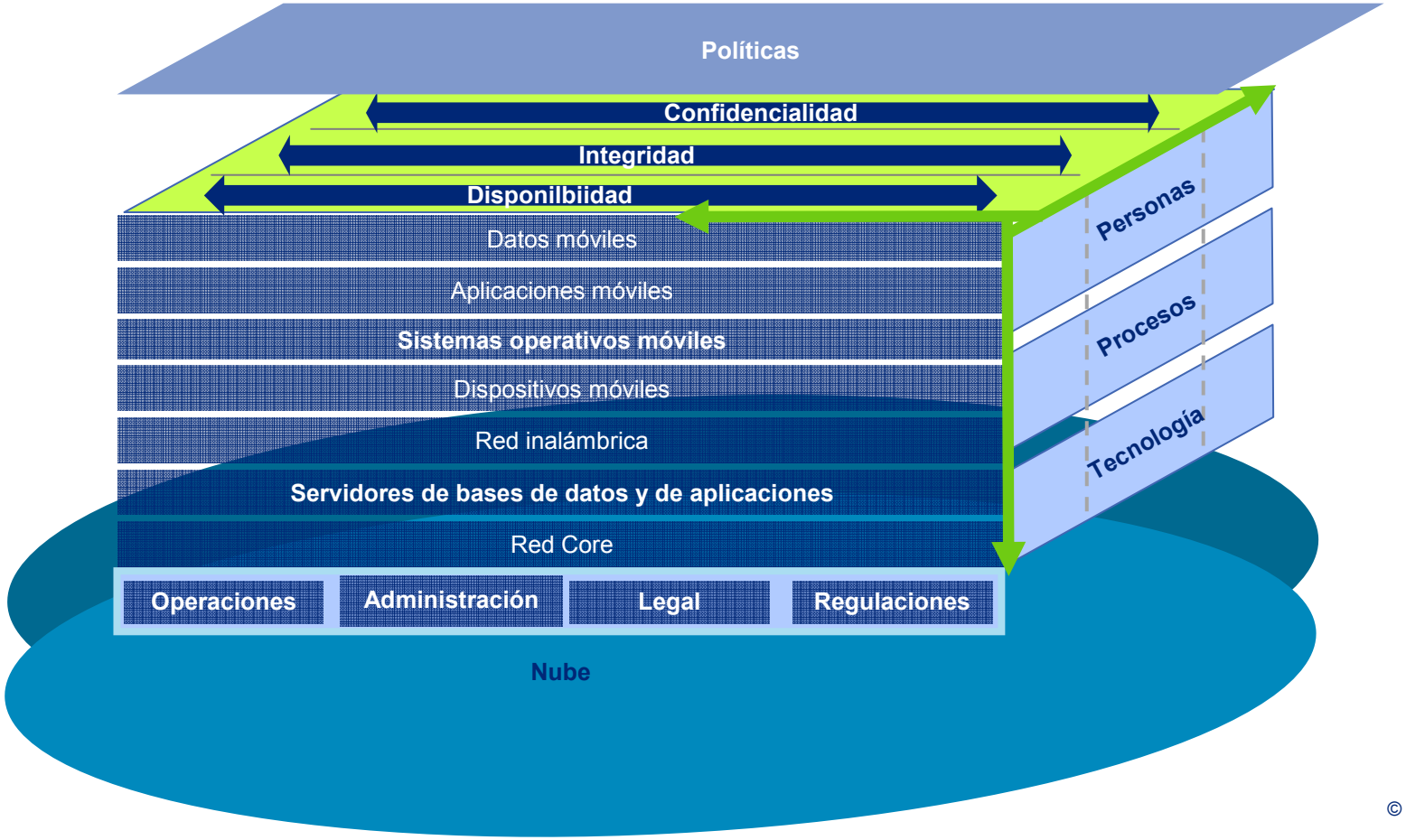
	iOS	Android	Windows Phone 7	BlackBerry
Bloqueo de Pantalla	Contraseña	Contraseña, Acceso facial.	Contraseña	Contraseña
Encriptación	Total en el dispositivo	Total en el dispositivo (3.0, 4.0)	No en el dispositivo.	Total en el dispositivo
Aplicación para proceso de aprobación	Estricto	Menos estricto	Estricto	Estricto
Aplicación de aislamiento.	Niveles de ejecución de privilegios.	Máquina virtual	Niveles de ejecución de privilegios	Máquina virtual.
Permisos	iOS se encarga	El usuario acepta antes de instalar	Algunos coinciden con el usuario	Algunos coinciden con el usuario
Virus	Algunos	Muchos	No muchos aún.	Algunos

© 2012 Deloitte

© 2012 Deloitte

Movilidad y marco de seguridad

- Los riesgos de seguridad móvil incluyen la pérdida o robo del dispositivo, la pérdida de datos, el compromiso de datos, robo de credenciales, los virus, acceso a la red no autorizado y los ataques directos de los dispositivos y servidores de aplicaciones expuestas.
- Para proteger su organización, debe extender su política de seguridad de la empresa, la estrategia de seguridad y los objetivos básicos de la seguridad (confidencialidad, integridad, disponibilidad) para cada capa de la pila de la movilidad. Las soluciones móviles de seguridad tienen la tecnología, procesos, y el componente de recursos humanos.



© 2012 Deloitte

Administrando los riesgos de dispositivos móviles

Topic	Strategies
Gobierno/Política	Uso apropiado de políticas de seguridad
Aplicaciones móviles	Virtualización
Sistemas operativos móvles	Segmentación, diversidad de dispositivos, jailbreak
Dispositivos móviles	Contraseña, bloqueo automático
Red Inalámbrica	Encripción, separador de redes inalámbricas
Red Core	Encripción, certificados de administración, Firewalls, DMZ
Administración	Administración de dispositivos móviles(MDM)
Operaciones	Integridad en el soporte a móviles.
Legar/Regulatorio	Auditoría

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." – Bruce Schneier

© 2012 Deloitte

Riegos en la gestión de su propio dispositivo

1. Minimizar la cantidad de datos almacenados en el dispositivo.
2. Utilice la virtualización.
3. Establezca políticas y un acuerdo final de aceptación por parte del usuario:
   - Uso apropiado.
   - Entrega
   - Limpieza de políticas y riesgos.
   - Monitoreo y respaldo de datos.
   - Requerimientos mínimos en configuración.
   - Requerimientos mínimos en seguridad.

4. Mantener los dispositivos no autorizados fuera de la red (herramientas de monitoreo de red)
5. Continúa y efectiva educación en la conciencia de los usuarios.

© 2012 Deloitte

Administración de dispositivos móviles

- Administración de dispositivos móviles proporciona un completo soporte del ciclo de vida para los dispositivos móviles, aplicaciones móviles y tiendas asociadas de datos para ayudar a asegurar:
  - Las aplicaciones, parches, agentes de seguridad. Están debidamente provisionados.
  - Los datos se copian automáticamente y protegidos en todo momento.
  - Los dispositivos están configurados correctamente y protegido de amenazas.
  - TI pueda corregir los problemas, limpie los datos y desactive dispositivos.
- Esto requiere que los sistemas utilicen procesos definidos y recursos especializados en múltiples áreas:

Aprovisionamiento

- Solicitud de aplicaciones móviles
- Mapa de usuario y dispositivo a un grupo de usuarios y aplicaciones móviles
- Aprovisionamiento de servicio inalámbrico.
- Aprovisionamiento de control de accesos a la red.
- Imagen del dispositivo móvil.
- Distribución de aplicaciones
- Dispositivo de aislamiento de aplicaciones de usuario/datos de apllicaciones empresariales o de datos.

Gestión de la configuración

- El seguimiento de activos físicos y de contabilidad
- Licencia de software / aplicaciones de descarga de contabilidad y gestión
- Reperación, reemplazo de hardware y garantias
- Copia de seguridad de datos de usuario final.
- Gestión de configuración de dispositivos.

Seguridad

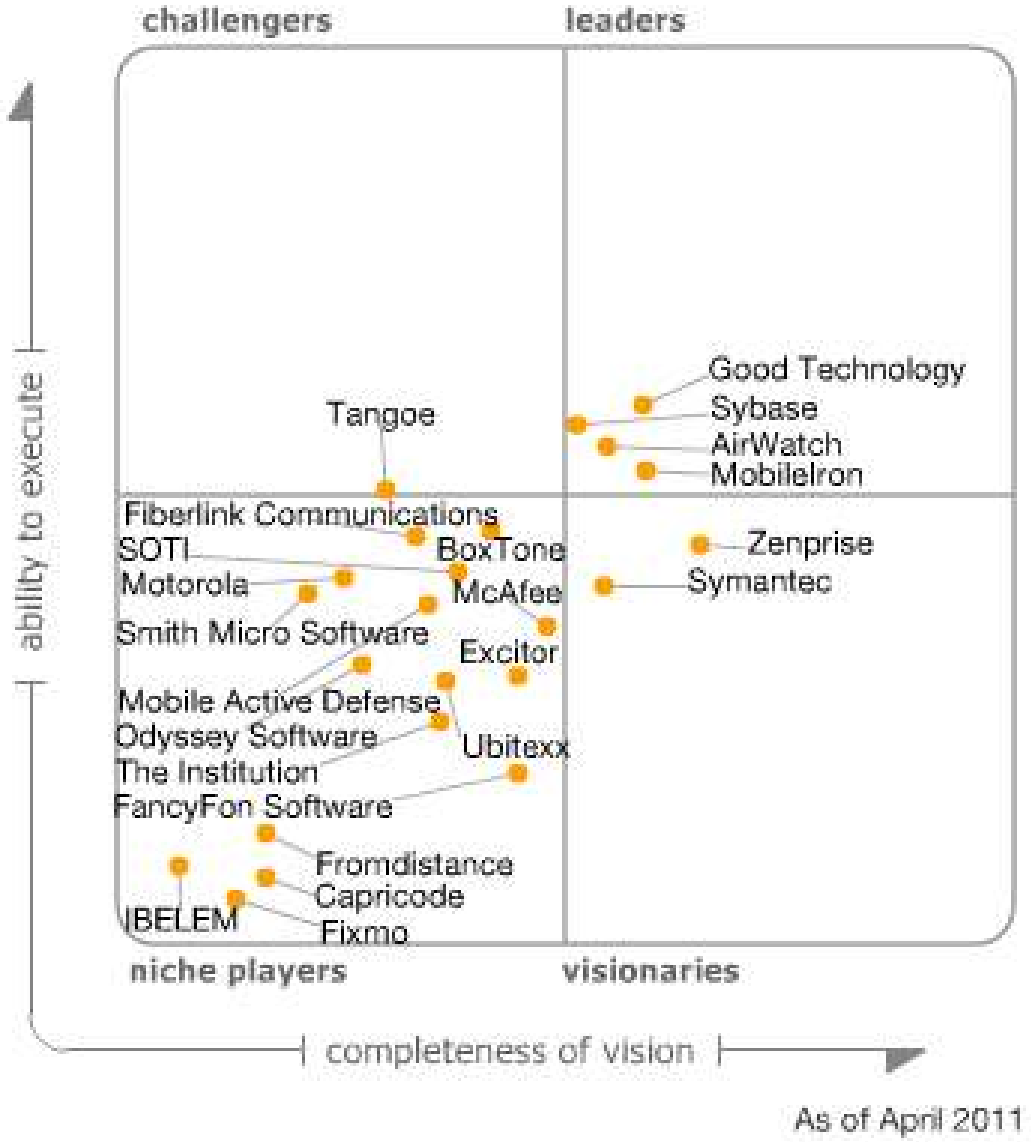
- Dispositivo y aplicación móvil.
- Almacenamiento de datos de cifrado y encriptación de extremo a extremo
- Filtrado de contenidos y de protección contra malware
- Monitoreo de eventos de seguridad, registro y respuesta
- Datos de la protección de fugas y control de almacenamiento extraíble

Soporte de usuario

- Reseteo de contraseña
- Soluciónde problemas a distancia
- Dispositivo, aplicaciones y restauración de datos.
- Resolución de incidencias y la base de datos de conocimiento de soporte
- Análisis de tendencias
- Formación teórico sobre los dispositivos y aplicaciones

© 2012 Deloitte

Cuadrante Mágico de Gartner para soluciones de MDM



© 2012 Deloitte

Como empezar: Definir los principios de seguridad de los dispositivos móviles

La gestión del cambio rápido y sin tomar decisiones fundamentales sobre los principios más importantes (y, posteriormente, la formalización de los mismos) puede dar lugar a confusión, incompleta o mal diseñado soluciones de apoyo, los retos, las lagunas de control, riesgos de seguridad y el riesgo empresarial.

El mínimo de recomendaciones para la seguridad de los dispositivos móviles a nivel empresarial, incluye las siguientes áreas:

1. **Gobierno de dispositivos móviles.**

2. **Políticas de uso aceptable.**
- Uso personal.
- Dispositivos de propiedad personal.

3. **Seguridad**
- Ajustes de sistemas operativos móviles.
- Dispositivo móvil, aplicaciones, autenticación de la red.
- Acceso controlado a la red.
- Conexiones inalámbricas.
- Normas de seguridad para aplicaciones móviles.

4. **Integración en control interno de TI.**
- Administración de dispositivos móviles.
- Protección de datos y respaldos.
- Distribución de software.
- Acceso a internet.
- Respuesta a incidentes.

© 2012 Deloitte

Arranque su estrategia de movilidad empresarial

Estrategia de Negocio	Establecer un equipo de liderazgo de movilidad. Identificar y priorizar las aplicaciones móviles para cada unidad de negocio. Crear un plan de trabajo ~ 24 meses de movilidad. Esto se convierte en un destino concreto para el equipo de TI.
Aplicaciones móviles	Desarrollar un marco de diseño para guiar las decisiones de diseño de aplicaciones. Definir casos de uso, los dispositivos de destino, los requisitos funcionales, estructuras alámbricas y la prueba de los conceptos de los mejores ~ 10 aplicaciones.
Arquitectura empresarial	Identificar los datos y servicios de aplicaciones que necesitan los dispositivos móviles. Desarrollar interfaces estándar de servicio que escala y son seguras. Desarrollar una arquitectura de nube en el exterior (por ejemplo, el cliente delgado o sincronización) que permite la itinerancia sin fisuras entre el smartphone, tablet y ordenador portátil en el transcurso del día.
Infraestructura	Decidir sobre un modelo de empuje y de atracción para las aplicaciones móviles. Implementar una tienda de aplicaciones o método de distribución alternativa. Entender el papel de middleware móvil y evaluar las opciones de la arquitectura.
Redes inalámbricas	Entender las expectativas de sus aplicaciones inalámbricas móviles. Asegúrese de que tiene una autenticación segura y fiable, de conectividad inalámbrica.
Seguridad	Llevar a cabo revisiones de seguridad en todo el proceso de desarrollo de aplicaciones móviles. Evaluar los riesgos de seguridad para cada aplicación móvil y cada capa de la pila de la movilidad y mitigar como sea necesario.
Administración de dispositivos	Desarrollar las normas de adquisiciones de dispositivos móviles, seguridad y administración. Definir los requisitos de protección de dispositivos móviles y de gestión de datos y soluciones. Desarrollar un proceso ágil para los nuevos dispositivos.
Traiga su propio (BYOD, por sus siglas en inglés)	Implementar el control de acceso a la red para evitar que los dispositivos no autorizados accedan a la red. Desarrollar una política alrededor de los dispositivos BYOD. Definir los requisitos mínimos de seguridad y controles de gestión. Implementar sistemas y procesos que proporcionan un control adecuado. Comunicar a los usuarios.
Gobierno	Desarrollar un marco de aplicación de lanzamiento móvil que se refiere a la entrega de los sistemas de ciclo de vida completo: requisitos, diseño, pruebas, formación de usuarios, documentación de usuario, ayudar a disposición de escritorio. , etc.

© 2012 Deloitte

Los vendedores van al mercado con nuevas soluciones de dispositivos móviles para satisfacer las necesidades de la empresa de gestión remota

Sybase iAnywhere Mobile Office

- Con seguridad se extiende la funcionalidad de las aplicaciones empresariales de correo electrónico y leve ambiente de pruebas
- Soporta iOS, Android, Windows Mobile, BlackBerry y Symbian

Citrix Receiver for Mobile Devices

- Permite el acceso de escritorio virtual a varias plataformas móviles
- Los datos de la empresa no abandonan el perímetro, pero una conexión de datos se requiere

CheckPoint Mobile Access Blade

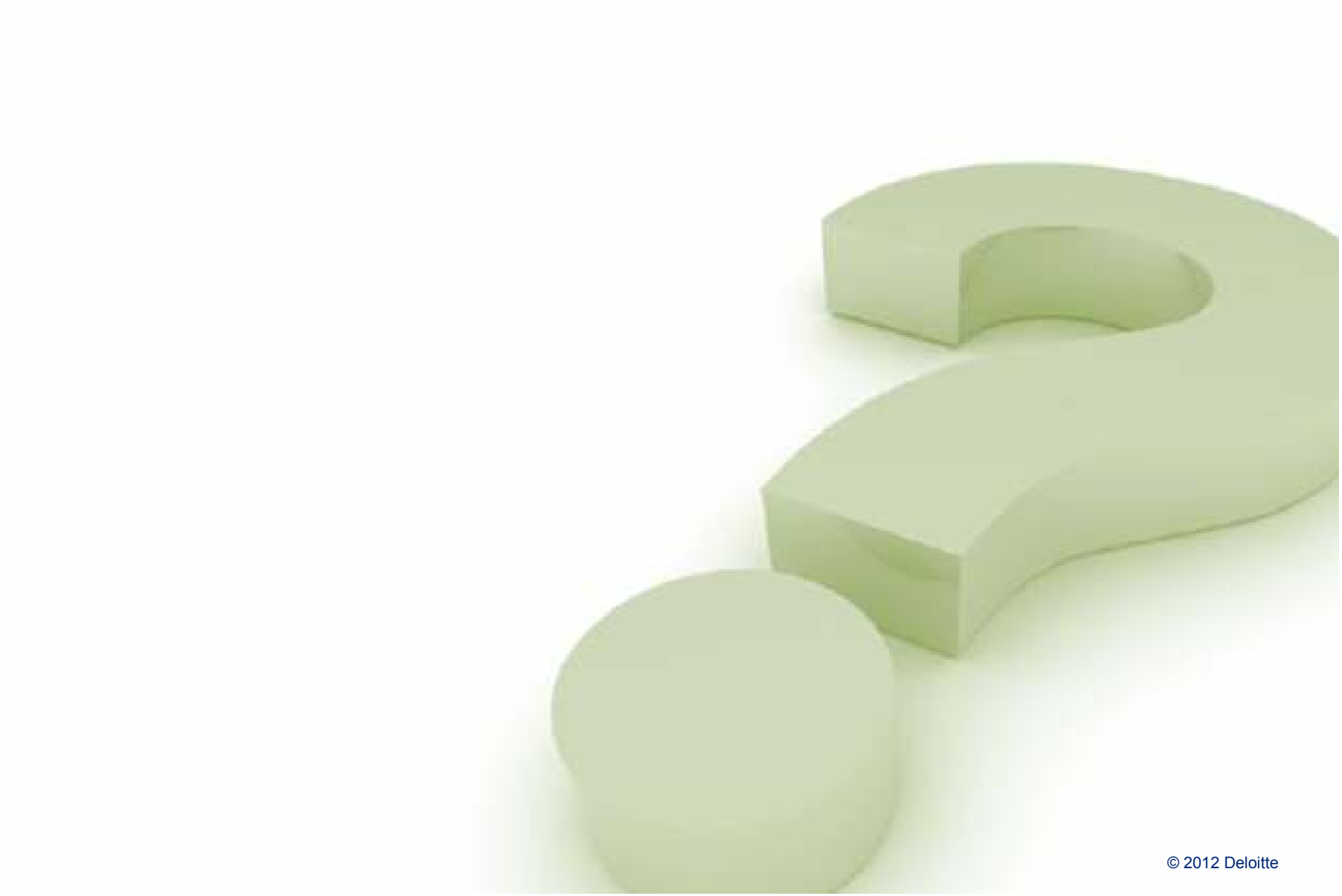
- Combina servidor de lado la provisión de datos móvil, conectividad VPN y dispositivos basados en cajas de arena
- Soporta iOS y Android de forma nativa, así como a través de acceso web

Good for Enterprise

- Ayuda a las empresas desplegar y gestionar los iPhones o iPads de manera similar a BlackBerry Enterprise Server

© 2012 Deloitte

Preguntas y Respuestas?



© 2012 Deloitte

Contacto

Andrés Casas - Director

Gestión de Riesgos (Deloitte)
Privacidad y Seguridad

ancasas@deloitte.com

Tel: +506 22465103

© 2012 Deloitte


Deloitte.