Riesgos de seguridad de la información en el uso de dispositivos móviles para aplicaciones empresariales

Felipe Silgado, *felipe.silgado@co.pwc.com*

Gerente de Consultoría en Seguridad de la Información

Manager ITE/TRS

+57 (1) 668 49 99 Ext. 204/115/113

PricewaterhouseCoopers

Con el uso creciente de los dispositivos móviles en las organizaciones para soportar su operación y mantenerse en contacto con sus clientes, se hace crítico evaluar los riesgos y las contramedidas que garanticen el almacenamiento y la seguridad de la información, transmitida desde y hacia estos dispositivos.

El rápido crecimiento y la amplia adopción para el uso empresarial de los dispositivos móviles (teléfonos inteligentes –smartphones- y tabletas –tablets-), ha sobrepasado todas las expectativas. Las personas que tienen un smartphone o tablet hoy navegan más de la mitad del tiempo desde ese dispositivo móvil y no desde su computador de escritorio o equipo portátil como ocurría hace unos años.

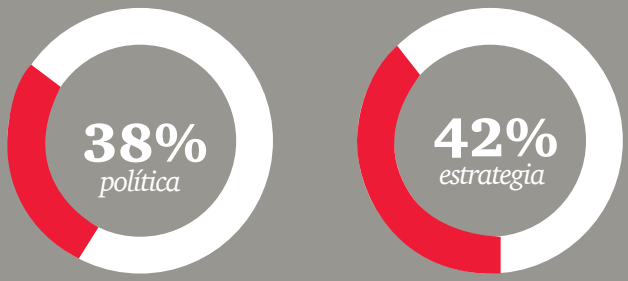
El acelerado crecimiento y la tendencia de las organizaciones a nivel mundial de contar por lo menos con una aplicación móvil o un sitio Web para móviles, convierte en un factor crítico la seguridad de la información transmitida desde y hacia estos dispositivos.

El uso de las aplicaciones móviles puede ser diverso dependiendo del objetivo que persiga la organización, algunos ejemplos son los siguientes:

Tipo de uso	Empresarial Empleados	Empresarial Clientes	No empresarial *(Social o entretenimiento)*
Consultar información	Directorios, Lista de clientes y datos de contacto Lista de precios	Portafolios de productos y servicios, Directorio oficinas	Rutas de autobús, Mapas, Noticias Datos del clima
Descargar información al dispositivoinformación	Información de clientes y sus productos	Directorio de oficinas, Información de servicios adquiridos, Datos de personalización del servicio, Pasabordos y tiquetes, Exámenes de salud	Mapas, Noticias, Datos del clima Música, Videos, Imágenes
Procesar y/o enviar información	Cotizaciones, Órdenes de pedido, Facturas y pagos, Inventarios, Aplicaciones core de negocio	Cambios de planes, Personalización de sus servicios, Pagos Cotizaciones, Solicitud de servicios, Datos de Salud del usuario	Redes sociales, Discos duros virtuales, Compras, Traductores

Riesgos de seguridad de la información asociados al uso de aplicaciones móviles

Al tener tantas posibilidades de consultar, enviar, almacenar, procesar y compartir información mediante dispositivos móviles, ¿cuáles son los nuevos riesgos a los cuales se enfrenta una organización?



Según la encuesta global de seguridad de la información de PwC 2014, el 38% de empresas tienen una política de seguridad que cubra los aspectos relacionados con seguridad para dispositivos móviles y el 42% indica tener una estrategia de seguridad para dispositivos móviles.

El análisis de riesgos de seguridad de la información para las aplicaciones móviles es crucial para identificar los niveles de exposición actuales de la información que es consultada, enviada, almacenada, procesada o compartida a través de estos dispositivos. En general, el riesgo se mide como la multiplicación entre el impacto y la probabilidad de ocurrencia *(Riesgo = Impacto *Probabilidad)*, el impacto se refiere a la(s) consecuencia(s) luego de materializado el riesgo, y la probabilidad se refiere a si podría o no suceder el riesgo y con qué frecuencia.

La organización puede partir de un portafolio de riesgos estándar para validar cuales riesgos corresponden a la aplicación móvil específica de la compañía y cuáles no. Por ejemplo, puede basarse en los riesgos técnicos definidos en el OWASP Mobile Security Project (Open Web Application Security Project, https://www.owasp.org/index.php/OWASP_Mobile_Security_Project), y luego realizar una definición del impacto que tendrían en la información o en el negocio.

A continuación se muestra el portafolio de riesgos técnicos de OWASP Mobile Security Project e igualmente una lista de impactos en la información y el negocio ejemplo, adaptables a las aplicaciones móviles en general. Estos portafolios no pretenden abarcar todos los posibles riesgos a que está expuesta una aplicación móvil, sino únicamente ilustrar algunos aspectos críticos que deben ser tenidos en cuenta al momento de desarrollar una aplicación móvil.

Riesgos técnicos definidos por el OWASP Mobile Security Project:

A continuación se muestran los diez riesgos más importantes para las aplicaciones móviles definidos por el OWASP Mobile Security Project (https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks):

1. Weak Server Side Controls *(Debilidad en los controles del lado del servidor de la aplicación)*
2. Insecure Data Storage *(Almacenamiento de datos inseguro)*
3. Insufficient Transport Layer Protection *(Protección insuficiente en la capa de transporte)*
4. Unintended Data Leakage *(Fuga de datos involuntaria)*
5. Poor Authorization and Authentication *(Autenticación y autorización pobres)*
6. Broken Cryptography *(Criptografía rota)*
7. Client Side Injection *(Inyección del lado del cliente)*
8. Security Decisions Via Untrusted Inputs *(Decisiones de seguridad vía entradas no confiables)*
9. Improper Session Handling *(Manejo de sesiones inapropiado)*
10. Lack of Binary Protections *(Falta de protección de los binarios)*

1. *Weak Server Side Controls* *(Debilidad en los controles del lado del servidor de la aplicación)*

La aplicación servidor a la cual se conecta el dispositivo móvil remotamente, no posee controles suficientes de seguridad por lo cual la aplicación cliente podría enviar datos que el servidor no sepa procesar y por ende crear una condición de vulnerabilidad que puede permitir ejecutar código del lado del servidor, inyectar código o realizar acciones arbitrarias tendientes a afectar los datos contenidos en el servidor.

2. *Insecure Data Storage* *(Almacenamiento de datos inseguro)*

La aplicación cliente no almacena los datos de manera segura (corresponde solo en los casos en que la aplicación móvil almacena datos en el dispositivo), por lo cual si alguien pierde el dispositivo, los datos podrían verse comprometidos (fuga de información), o en caso que se guarden datos sensibles de la aplicación, que el usuario no debiera conocer o alterar, es viable que el usuario los pueda llegar a acceder o modificar sin autorización y sin que la aplicación servidor pueda identificar estas alteraciones.

3. *Insufficient Transport Layer Protection* *(Protección insuficiente en la capa de transporte)*

Al momento en que la aplicación cliente en el dispositivo se conecta al servidor para transmitir información, esta conexión no se realiza de manera segura, por lo cual los datos en tránsito se encuentran en riesgo de ser interceptados, lo que deja los datos expuestos a fuga de información o modificación no autorizada de la misma.

4. *Unintended Data Leakage*
(Fuga de datos involuntaria)

La aplicación en el dispositivo puede fugarse debido a las actualizaciones del sistema operativo, de los frameworks de software, o incluso del hardware (cuando es posible). Estas actualizaciones ponen en riesgo o cambian el comportamiento de la aplicación.

5. *Poor Authorization and Authentication*
(Autenticación y autorización pobres)

La aplicación no provee los niveles adecuados y necesarios de autorización y autenticación, por lo cual un usuario podría saltarse la autenticación de la aplicación logrando acceso no autorizado y suplantación de identidad, o modificar los niveles de autorización logrando, por ejemplo, escalamiento de privilegios o acceso no autorizado a información de la aplicación.

6. *Broken Cryptography*
(Criptografía rota)

La aplicación no realiza un cifrado adecuado a la información almacenada o transmitida (desde o hacia el dispositivo) por lo cual se puede lograr acceso no autorizado a información de la aplicación.

7. *Client Side Injection*
(Inyección del lado del cliente)

La aplicación cliente en el dispositivo móvil, no posee controles suficientes de seguridad para la entrada o envío de datos al servidor, por lo cual desde la aplicación cliente se podrían enviar datos que el servidor no procese adecuadamente y permita realizar acciones sobre los datos contenidos en el servidor.

8. *Security Decisions Via Untrusted Inputs*
(Fuga de datos involuntaria)

La aplicación podría recibir datos de entrada de varias fuentes (diferentes a la aplicación cliente), los cuales si no son validados previamente para ser procesados por la aplicación, podrían poner en riesgo la seguridad de la información de la aplicación.

9. *Improper Session Handling*
(Manejo de sesiones inapropiado)

La aplicación no provee los niveles adecuados y necesarios, por lo cual uan sesión de usario válida podría ser interceptada y los datos transmitidos estarían en riesgo. Igualmente, un usuario no autorizado podríaa clonar una sesión válida de usuario, saltando con esto los controles de autenticación y autorización. Aspectos como manejo de timeout, uso de cookies de aplicación e insegura creación y manejo de tokens/llaves de sesión podrían permitir acceso no autorizado a los datos y suplantación de identidad.

10. *Lack of Binary Protections*
(Autenticación y autorización pobres)

Cuando una persona no autorizada realiza cambios a los binarios de la aplicación y modifica el comportamiento de esta, por ejemplo, para variar los datos enviados al servidor, para transmitirlos a un servidor alterno no autorizado, realizar cualquier tipo de modificación a la información, modificar la presentación de la aplicación e incluso llegar a permitir la fuga de la información.

Impactos en la información y en el negocio

Los impactos en la información y en el negocio que pueden traer los riesgos asociados a aplicaciones móviles son diversos, a continuación se muestran algunos ejemplos ilustrativos de cómo una organización se podría ver afectada

Fuga de información (de negocio o personal)

Uno de los impactos que más puede afectar a una organización es la fuga de información. Por una parte, porque puede ser información de know-how de negocio o confidencial sobre los clientes, que implicaría un incumplimiento en la protección de datos, o por otra parte, porque puede ser información personal o privada que está protegida por leyes como la ley de protección de datos (ley 1581 de 2012), lo que puede implicarle a la organización desde una multa hasta el cierre de actividades.

Fraude

A través de los accesos no autorizados y problemas asociados al manejo de datos de entrada de la aplicación, tanto del lado del cliente como del servidor, un atacante podría realizar un fraude (si es viable a través de la aplicación móvil) poniendo en riesgo la reputación de la organización y generando problemas con los clientes hasta llevar a la pérdida de estos, cuando el fraude afecta a los clientes de la organización directamente.

Modificación de información no autorizada

La modificación de información puede llevar a diversos impactos: puede afectarse el servicio de un cliente, llevar a un fraude a través de la aplicación, puede implicar la alteración de datos personales protegidos por leyes como la ley de protección de datos (ley 1581 de 2012), la ley de Habeas Data (ley 1266 de 2008), la ley de la protección de la información y de los datos (ley 1273 de 2009) o el decreto nacional 1377 de 2013 (reglamenta parcialmente la Ley 1581 de 2012) , o incluso la pérdida de datos vitales de la organización.

Robo de información (de negocio o personal)

Otro impacto que puede afectar a una organización es el robo de información, puede ser de información confidencial de negocio e incluso de información financiera como por ejemplo datos de tarjetas de crédito o débito, o información con datos personales protegidos por leyes como la ley de protección de datos (ley 1581 de 2012), la ley de Habeas Data (ley 1266 de 2008), la ley de la protección de la información y de los datos (ley 1273 de 2009) o el decreto nacional 1377 de 2013 (reglamenta parcialmente la Ley 1581 de 2012) lo que puede implicarle a la organización desde una multa hasta el cierre de actividades.

Pérdida de información (de negocio o personal)

El impacto de pérdida de información puede afectar directamente la operación del negocio, dado que por ejemplo podría no saberse qué cliente tiene servicios, qué tipo de servicios, perderse información de facturación o incluso cuando el servicio de la organización es el resguardo de la información podría no solo afectar a ésta sino a los clientes del servicio, con lo cual el impacto podría ser mayor por el incumplimiento de contratos y niveles de servicio.

Acceso no autorizadoinformación (de negocio o personal)

El acceso no autorizado puede permitir que un individuo realice cualquier cosa con la información de una aplicación, desde consultarla, hasta alterarla e incluso borrarla, lo que puede impactar a la organización y a sus clientes, poniendo en riesgo la imagen de la organización, el cumplimiento regulatorio y el de los contratos establecidos.

Impactos en la información y en el negocio

Ingeniería social

La ingeniería social permite que un individuo persuada a su víctima a dar información confidencial o privada, utilizando técnicas de llamadas telefónicas, correos electrónicos, entre otros mecanismos, obteniendo información de las aplicaciones (información no protegida en los dispositivos o que no esté asegurada en su transporte entre el dispositivo y el servidor), de tal manera que una persona suplante a alguien de la organización y con la información obtenida persuada bien sea telefónicamente o por correo al usuario víctima para obtener acceso a la aplicación y a otra información.

Incumplimiento regulatorio

Las aplicaciones que manejan información con datos personales protegidos por leyes como la ley de protección de datos (ley 1581 de 2012), la ley de Habeas Data (ley 1266 de 2008), la ley de la protección de la información y de los datos (ley 1273 de 2009) o el decreto nacional 1377 de 2013 (reglamenta parcialmente la Ley 1581 de 2012), deben ser especialmente aseguradas para evitar que la información puede ser divulgada sin autorización o alterada, para evitar desde una multa hasta el cierre de actividades de la organización.

Incumplimiento de contratos y SLAs

Los contratos de servicios con clientes pueden contener acuerdos de niveles de servicio (SLA – Service Level Agreements) los cuales pueden implicar a la organización multas o pérdidas de contratos en caso que la información manejada por la aplicación móvil sea divulgada, perdida o alterada sin autorización.

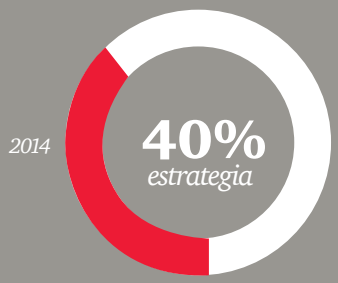
Con este panorama de riesgos e impactos, ¿qué acciones debe realizar la organización para que sus aplicaciones móviles estén seguras?

Recomendaciones para mitigar los riesgos asociados al uso de aplicaciones móviles

El primer aspecto a tener en cuenta es que la organización defina una política de seguridad para aplicaciones móviles y una estrategia de seguridad para el manejo de aplicaciones móviles, con esto habrá dado el primer paso y tendrá al menos un gobierno de seguridad definido que apalanque los esquemas requeridos de seguridad en las aplicaciones móviles.

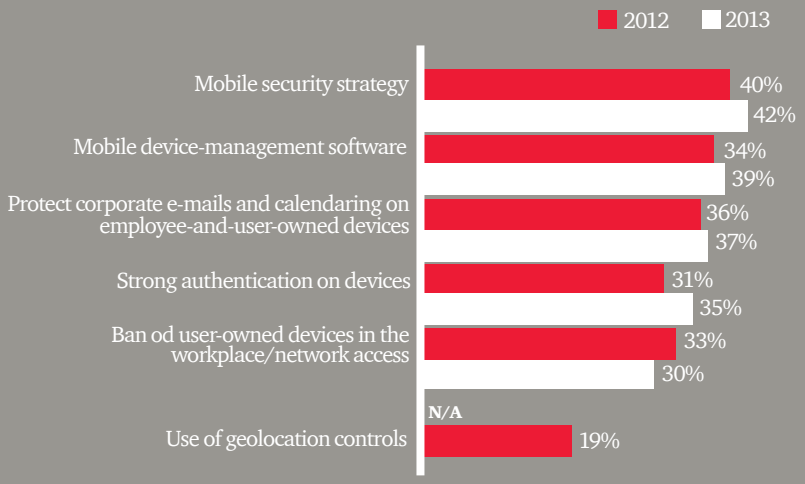
Seguido de esto, se recomienda establecer un marco de seguridad para aplicaciones móviles (framework de seguridad para aplicaciones móviles) que cubra cuatro frentes principales:

- Aspectos del desarrollo
- Aspectos de la arquitectura
- Manejo de la seguridad
- Aspectos de la infraestructura



Según la encuesta global de seguridad de la información de PwC 2014, solo el 40% de empresas tienen una estrategia de seguridad que cubra los aspectos relacionados con seguridad para dispositivos móviles.

Según la encuesta global de seguridad de la información de PwC 2014, solo el 40% de empresas tienen una estrategia de seguridad que cubra los aspectos relacionados con seguridad para dispositivos móviles.



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Aspectos del desarrollo

En este aspecto se deben tener en cuenta los siguientes puntos:

- Almacenamiento de datos, tanto del lado del cliente como del servidor: Utilizar algoritmos de cifrado fuerte, o en caso que resulte costoso no almacenar datos del lado del cliente. No almacenar datos en memorias externas SD o micro SD que permita conectar el dispositivo.
- Autenticación: Utilizar sistemas de autenticación fuerte (sistemas de token, sistemas de autenticación por dos canales, o utilizando SQRL -Secure QR Login-).
- Autorización: Utilizar mecanismos de definición de roles y perfiles.
- Manejo de sesiones: Manejo de llaves de sesión con mecanismos de validación dinámica de sesiones y cambios de llaves de sesión en cada intercambio de información. Revalidación de sesiones activas cada cierto tiempo, terminación de sesiones huérfanas, y control de múltiples sesiones de un mismo usuario desde diferentes dispositivos, incluso se puede desarrollar una funcionalidad para que el usuario registre su dispositivo para que luego otros dispositivos no autorizados no puedan conectarse a la aplicación.
- Registro de eventos y auditoría: Registro en la base de datos del servidor, de todos los eventos de seguridad ocurridos en la aplicación.
- Manejo de la memoria: Manejo de memoria de la aplicación para evitar overflows o intercepción de datos que se almacenen en texto claro en la memoria del dispositivo. Limpiar la memoria al finalizar sesión o cuando hayan terminaciones anormales de las sesiones.
- Navegador: Cuando se utilice el navegador del dispositivo para acceder a la aplicación, no permitir el uso de navegadores viejos u obsoletos.
- Realizar la ofuscación del código fuente y ocultar aquellas clases o propiedades que son sensibles para la operación de la aplicación.
- Realizar la ofuscación y ocultar las propiedades de configuración sobre el dispositivo.
- Validar las necesidades de propiedad intelectual del código fuente, teniendo presente que esta aplicación tendrá que ser cargada en los Marketplace de los proveedores del sistema operativo.

Aspectos de la arquitectura

En este aspecto se deben tener en cuenta los siguientes puntos:

- Seguridad: Módulos independientes de manejo de la seguridad, arquitectura de DMZ y MZ para los diferentes componentes de la arquitectura de la aplicación.
- Capacidad de mantener: Un buen diseño de la aplicación y capacidad de mantenimiento evitará que más adelante al tratar de corregir algún problema o adicionar nuevas funcionalidades, la aplicación pueda quedar vulnerable o se alteren módulos de control de la seguridad.
- Escalabilidad: Capacidad para el crecimiento de dispositivos conectados y cantidad de información intercambiada entre el dispositivo y el servidor, soporte de nuevas marcas de dispositivos y sistemas operativos.
- Disponibilidad: Capacidad de respuesta al servicio y resiliencia.
- Conectividad y disponibilidad: Se debe tener en cuenta el tipo de red de datos celular a utilizar (2G, 3G, 4G, etc.) con el dispositivo móvil (debido a necesidades de velocidad o estabilidad en la conexión), si se requiere o no el uso de funcionalidades como Vertical Handover (o también llamado Vertical Handoff, para soportar cambios en la conectividad del dispositivo por ejemplo cuando deja de tenerse conectividad por la red WIFI que haga el cambio a la red celular de datos y viceversa sin perder conexión a la aplicación), diseño de mecanismos de failover y recuperación de conectividad cuando hay fallos en la comunicación, entre otros aspectos.

Manejo de la seguridad

En este aspecto se deben tener en cuenta los siguientes puntos:

- Políticas de privacidad: Clasificar la información de la aplicación y poder almacenar en contenedores o espacios diferentes los datos confidenciales y los datos personales o privados, cumpliendo con la legislación vigente.

- Valoración de riesgos: Valorar los riesgos específicos asociados al tipo de aplicación y de información a manejar, para definir contramedidas específicas para la organización. Definir escenarios de riesgo que ayuden a encontrar contramedidas de seguridad, por ejemplo que pasa si el dispositivo se pierde y alguien no autorizado trata de utilizar la aplicación o acceder la información del dispositivo? Qué pasa si conecto el dispositivo por USB a un computador? Qué pasa si el usuario sufre un daño en su dispositivo?

- Pruebas de seguridad: Dentro de las pruebas a efectuar es recomendable definir escenarios de cómo se utilizará la aplicación (desde un Smartphone o Tablet) y los eventos que puedan ocurrir al dispositivo (robo, daño, actualización del sistema operativo, degradado del sistema operativo, sistema operativo con Jailbreak para eliminar las limitaciones y bloqueos, etc.).
  Los aspectos mínimos a contemplar en las pruebas son los siguientes:

- Revisión de código fuente: Es importante que durante el desarrollo de la aplicación, se realice una revisión de código fuente en cuanto a aspectos de seguridad, de tal forma que se garantice que la aplicación no tenga vulnerabilidades, backdoors (puertas traseras) y otras debilidades de seguridad que permitan a un atacante acceder a la aplicación y su información. Se recomienda revisar, al menos, los siguientes aspectos:

- ***Definición de escenarios de prueba***
  Escenarios de configuración del dispositivo
  Escenarios de tipos diferentes de dispositivo
  Escenarios de conexión a la aplicación
  (datos celular, Bluetooth o WIFI, uso de proxy)

- ***Identificación de información de la aplicación***
  Dirección IP
  Puertos TCP/UDP
  Dirección URL y dirección DNS del servidor
  Verificación de certificados y conexión

- ***Pruebas al servidor***
  Capturar requerimientos de conexión y datos hacia el servidor
  Utilizar conexión proxy de prueba y análisis de tráfico
  Escanear el servidor con herramientas de detección de vulnerabilidades (por ejemplo Nessus, Acunetix, Rapid7, etc.) y explotar las vulnerabilidades identificadas
  Manipulación de información de los campos sobre los métodos que viajan hacia el servidor
  Reutilización de información de la sesión

- ***Pruebas al dispositivo que tiene la aplicación***
  Hacer ingeniería reversa de la aplicación e identificar información clave como contraseñas quemadas, direcciones IP, rutinas de la seguridad de la aplicación, etc.
  Identificación de información sensible sobre paquetes de instalación
  Identificación de Información sobre las respuestas del servidor
  Renegociación sobre la conexión SSL
  Leer la información almacenada en la aplicación y sistema de archivos del dispositivo
  Utilizar emuladores y simuladores de sistema operativo y dispositivos móviles
  Probar aspectos específicos del sistema operativo y dispositivo utilizado acorde con el escenario definido
  Hacer pruebas con actualización o degradado del sistema operativo, e incluso realizando Jailbreak.

- Variables de entrada de datos y la forma en cómo la aplicación las utiliza.
- Detección de problemas asociados a la comunicación entre el dispositivo y el servidor como por ejemplo direcciones IP o puertos TCP quemados en el código.
- Detección de fallas que lleven a inyección de código.
- Detección de backdoors y código sospechoso.
- Detección de contraseñas y llaves quemadas en el código.
- Detección de algoritmos débiles (por ejemplo de cifrado).
- Detección de definiciones de almacenamiento de datos.
- Detección de problemas específicos de la plataforma (iOS, Blackberry,
- Android, Symbian, Windows Mobile, etc.)

Aspectos de la infraestructura

En este aspecto se deben tener en cuenta los siguientes puntos:

- Acceso a recursos de red y conectividad: Asegurar que la conexión se realice vía VPN o SSL con certificados digitales válidos, cifrando la sesión y el transporte de datos entre el dispositivo y el servidor.
- Comportamiento de la aplicación: Desarrollar capacidades de detección de amenazas, utilizar cookies seguras, utilizar redirecciones seguras.
- Firewalls: Configurar firewall de aplicación del lado del servidor para evitar que se generen ataques al servidor desde los dispositivos.
- Anti-malware: Asegurar que los dispositivos utilicen software anti-malware para garantizar que a través de la aplicación no ingrese malware a la red de la organización.
- Sistemas MDM (Mobile Device Management): Utilizando este tipo de herramientas su organización puede garantizar que los dispositivos móviles que se conectan a las aplicaciones están configurados adecuadamente a nivel de seguridad, que los usuarios no tiene aplicaciones potencialmente peligrosas, que la conexión puede realizarse de manera segura a la aplicación, que el dispositivo tiene la versión correcta de la aplicación, entre otros aspectos de seguridad.
- Aprovisionamiento de la aplicación y entrega: La organización debe asegurarse que la estrategia de implementación de la aplicación en los dispositivos móviles sea segura y adecuada, si se va a utilizar un Marketplace se recomienda informar a los usuarios cual es el nombre completo de la aplicación y el nombre del desarrollador de ésta o fabricante que aparece en el Marketplace para que el usuario no baje la aplicación errónea o una aplicación falsa. Si se va a utilizar un link vía código QR o vía correo electrónico, asegúrese que no vaya a ser el usuario víctima de un phishing (correo electrónico con un link falso) o QRishing (código QR falso).

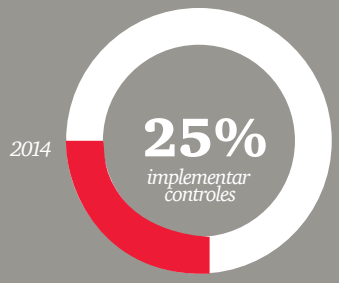
Una vez aplicado este framework de seguridad para aplicaciones móviles, se espera que las organizaciones puedan tener una base de seguridad al momento de desarrollar aplicaciones móviles tanto para su uso interno como para servicios a clientes.

Recomendaciones finales

El uso creciente de los dispositivos móviles es imparable, hoy día superan en cantidad a los computadores de escritorio y portátiles, por lo cual la seguridad de los dispositivos móviles se vuelve un aspecto fundamental en las estrategias de tecnología y negocio de las organizaciones. El ambiente de amenazas que existen hoy hace necesario que las organizaciones adopten e implementen estrategias de seguridad para mitigar los problemas y riesgos que se derivan del uso de estos dispositivos para fines empresariales.

Los aspectos enunciados a lo largo de este documento son solo algunos de los puntos a tener en cuenta que sirven para cualquier organización como una base general de control.

Sin embargo, su personalización y ampliación dependerá de lo que la empresa requiera a nivel de la aplicación y cómo espera que ésta sea utilizada por los usuarios, por lo cual se recomienda que cada organización inicie con la definición de su estrategia de seguridad de dispositivos móviles y, a partir de esto, personalice este framework según sus necesidades.



Según la encuesta global de seguridad de la información de PwC 2014, se espera que en este año un 25% de las empresas dediquen sus esfuerzos de seguridad a implementar controles en sus dispositivos móviles tales como: cifrado de smartphones, definición de estrategia para empleados para el uno de dispositivos personales en la empresa y la implementación de herramientas MDM.

PwC ayuda a las organizaciones y personas a crear el valor que están buscando. Somos una red de firmas presente en 157 países, con más de 184.000 personas comprometidas a entregar calidad en los servicios de Auditoría, Impuestos y Consultoría. Cuéntanos lo que te importa y encuentra más información visitando nuestra web: www.pwc.com.