LOS RIESGOS DE LAS APPS EN EL ENTORNO CORPORATIVO

BARCELONA DIGITAL CENTRO TECNOLÓGICO

bdigital

TECNIO
Be tech. Be competitive

Depósito legal: [B. 28840-2013]

001

Cuando la información es lo que cuenta

> Creo que esa vieja distinción entre el mundo físico y el virtual va a desaparecer en los próximos años. A las personas les va a importar simplemente rodearse de objetos inteligentes, que hagan su vida más fácil, sin trazar la frontera entre lo físico y lo simulado. Y también va a desaparecer la diferencia entre el negocio y el usuario.
> **Todo va a formar parte de lo mismo.**[1]
>
> **Phil Libin**
> Creador de Evernote

Phil Libin, un joven emprendedor norteamericano creador de la popular aplicación Evernote, predice con esta afirmación pronunciada en septiembre del 2013 un nuevo escenario en la transformación de lo cotidiano a causa de la irrupción de las tecnologías digitales. Observamos cada día como las fronteras entre el mundo físico y el virtual van diluyéndose, que lo que nos ocurre en el mundo físico invade cada vez más las pantallas de nuestros ***smartphones***, y que a través de ellos podemos manejar un gran número de eventos que tienen su reflejo en el mundo material.

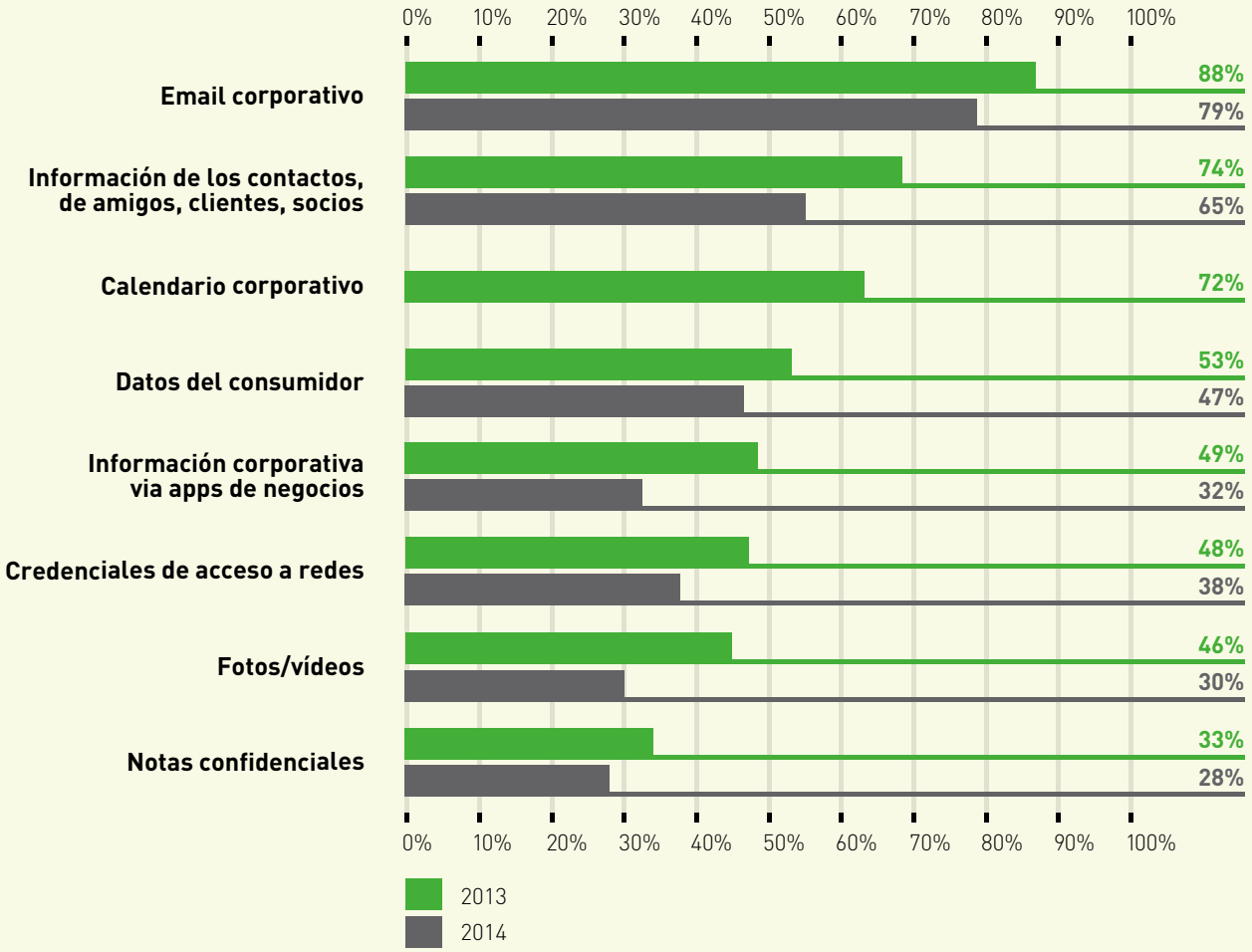
Debido a la accesibilidad por parte del gran público a este tipo de dispositivos (***consumerización***), a su inherente movilidad, y a su cada vez mayor potencia de cálculo, **los *smartphones* se han convertido en la principal puerta de acceso al mundo digital**[2]. Así, al alcance de nuestra mano y con la inmediatez del momento, es posible hacer una consulta en Facebook, revisar la bandeja de entrada de nuestro correo electrónico personal o de empresa, comprar entradas para un espectáculo o aceptar un contacto que nos llega a través de LinkedIn. La realidad digital en la que a menudo estamos sumergidos de forma inadvertida, converge en nuestro ***smartphone*** y difumina progresivamente la separación entre realidad y virtualidad y, por añadidura, la separación entre nuestra esfera personal y profesional.

Ciertamente, gracias a las 'apps' podemos acceder desde nuestro teléfono móvil a un gran número de servicios, muchos de ellos gratuitos y enormemente populares por su originalidad y utilidad. Sin embargo, aunque a los ojos del gran público las aplicaciones para móvil puedan parecer elementos inocuos desde el punto de vista de la seguridad, la realidad nos muestra que **la utilización de una aplicación en nuestro dispositivo móvil puede constituir un elemento de riesgo capaz de comprometer la seguridad de la información que genera y almacena**. Como usuarios es preciso tomar consciencia de estos peligros y adoptar las medidas que permitan mitigarlos. Esta recomendación adquiere, si cabe, una mayor trascendencia cuando se trata de dispositivos móviles corporativos, ya que se puede poner en riesgo información relevante.

En este sentido, noticias recientes como el 'Caso Snowden' [3] o diferentes programas de espionaje sacados a la luz [4], como PRISM [5], constatan la gran importancia de la información, el poder de quien la posee y al mismo tiempo la facilidad con la que esta información fluye gracias al enorme potencial tecnológico desarrollado al abrigo de nuestra Sociedad de la Información y el Conocimiento. Los modelos de negocio que sustentan el mundo de las 'apps' se basan frecuentemente en el aglutinamiento masivo de información personal, que habitualmente se venden a terceros con fines publicitarios y de marketing, hasta el punto que **muchas 'apps' declaran abiertamente la apropiación de la información de sus usuarios como mera consecuencia del uso de sus servicios**. Tal y como se muestra en el gráfico siguiente [6], la cantidad y variedad de información corporativa almacenada en un dispositivo móvil aumenta constantemente, hecho que adquiere una mayor trascendencia cuando se utiliza el mismo smartphone para usos personales y profesionales.

Información corporativa almacenada en dispositivos móviles

Fuente: Checkpoint



Así pues, y aunque muchos usuarios ya son conscientes de las amenazas de seguridad debido al uso de las 'apps' [7], **es necesario una mayor concienciación sobre los riesgos derivados de la descarga de aplicaciones en dispositivos móviles corporativos**. Este documento trata sobre la identificación de dichos riesgos y sus causas, así como de la forma de prevenirlos y mitigarlos a través de unas sencillas recomendaciones.

002

¿Te has preguntado alguna vez cómo se sustentan económicamente las 'apps'?

Hay centenares de miles de aplicaciones para las plataformas móviles más habituales (Android, iOS, Windows Phone 8, y Blackberry), un gran número de ellas gratuitas. Algunos desarrolladores tienen una motivación altruista y sólo buscan ofrecer un determinado servicio a la comunidad sin esperar necesariamente un retorno de la inversión realizada, aunque también es cierto que éste no es el comportamiento habitual y que estas 'apps' normalmente no figuran entre las más utilizadas por el público en general.

Así, tanto si son gratuitas como de pago, **las 'apps' necesitan de un modelo de negocio que sustente el coste incurrido en su diseño, construcción y mantenimiento**. Se podría pensar que las 'apps' de pago ya tienen este coste recompensado gracias a la venta por descargas, pero estos ingresos no soportan los costes de las actualizaciones y de las infraestructuras indispensables para su funcionamiento, y necesitan igualmente de un modelo de negocio que les permita mantener su evolución. Un modelo de negocio muy común consiste precisamente en, de una u otra forma, comerciar con la información que se puede obtener de un usuario a partir de su dispositivo móvil. Tanto es así que incluso hay desarrolladores que llevan esta práctica a un extremo y directamente diseñan y construyen sus 'apps' con la clara intención de engañar al usuario y sustraer información personal o corporativa.

Una posición habitual del usuario ante este hecho consiste en minusvalorar la trascendencia del fenómeno y la importancia de la información que genera y circula a través de las 'apps'. Muy al contrario, esta información tiene mucho valor para los propietarios de las 'apps', tanto, incluso que están dispuestos a costear servicios muy útiles con el fin de obtenerla. De nuestros hábitos, gustos, preferencias, y hasta de los detalles más insignificantes de comportamiento se desprende un perfil social de nuestra persona que nos describe detalladamente. Cuando esta caracterización se traslada a nuestra esfera profesional, incluye contactos, relaciones de trabajo, proyectos, pensamientos, y un sinfín de información que es fuente misma de la competitividad de nuestra empresa.

¿Cómo se sustentan económicamente las apps?

- → **Lista de contactos** (tanto personales como profesionales)
- → **Agenda**
- → **Identificador único del usuario** (UUID), del teléfono, y número telefónico
- → **Información de credenciales**
- → **Hábitos de uso** del dispositivo
- → **Geolocalización**
- → **Registro de llamadas y SMS**
- → **Historial** de navegación
- → **Correo electrónico**
- → **Información sensible** de la compañía (clientes, informes, fotos, vídeos, etc.)

Principales riesgos asociados a la descarga y uso de 'apps'

APROPIACIÓN INDEBIDA DE LA INFORMACIÓN

- → Falta de transparencia
- → Poca granularidad en la elección de la información a facilitar
- → Limitación de propósito
- → Falta de medidas de seguridad

ABUSO DEL DISPOSITIVO

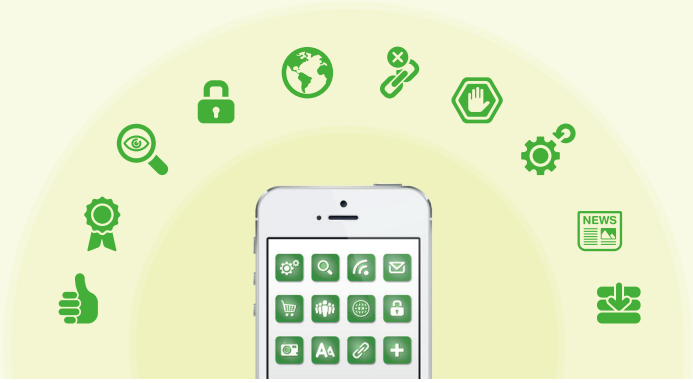
- → Espionaje
- → Secuestro del terminal
- → Agotamiento de recursos

INCUMPLIMIENTO LEGAL Y NORMATIVO

- → Acuerdo de Términos y Condiciones
- → Sistemas de Información Empresariales

Recomendaciones para minimizar los riesgos en el uso de 'apps' en dispositivos corporativos

- → **Seguir las reglas de seguridad establecidas por los responsables de Tecnologías** de la Información de la empresa, en cuanto a normas de seguridad en el uso del dispositivo móvil corporativo y, en particular, las normas respecto a las 'apps' cuya descarga no es recomendable o está prohibida.
- → **Usar siempre la tienda de aplicaciones oficial del dispositivo.**
- → **Revisar qué permisos solicitan las 'apps' al instalarse y que estos sean apropiados** para la función que va a desempeñar.
- → **Configurar los niveles de privacidad que la aplicación permite.**
- → **Revisar la configuración de geolocalización, y verificar si es necesario o no que esté** siempre activada.
- → **En aplicaciones de redes sociales no abrir enlaces que provengan de usuarios** desconocidos, especialmente cuando estos van en forma de enlaces cortos (*TinyURL*).
- → **No compartir contraseñas ni información sensible a través de 'apps'.**
- → **Mantener actualizado el Sistema Operativo.**
- → **Mantenerse informado de las últimas amenazas existentes.**
- → **Tener en cuenta que lo que se comparte por una red social podría quedar** permanentemente compartido.



003

Principales riesgos asociados a la descarga y uso de 'apps'

A continuación se exponen de manera clara y sencilla, los principales riesgos asociados a la descarga y uso de 'apps' en dispositivos móviles corporativos, consistentes en:

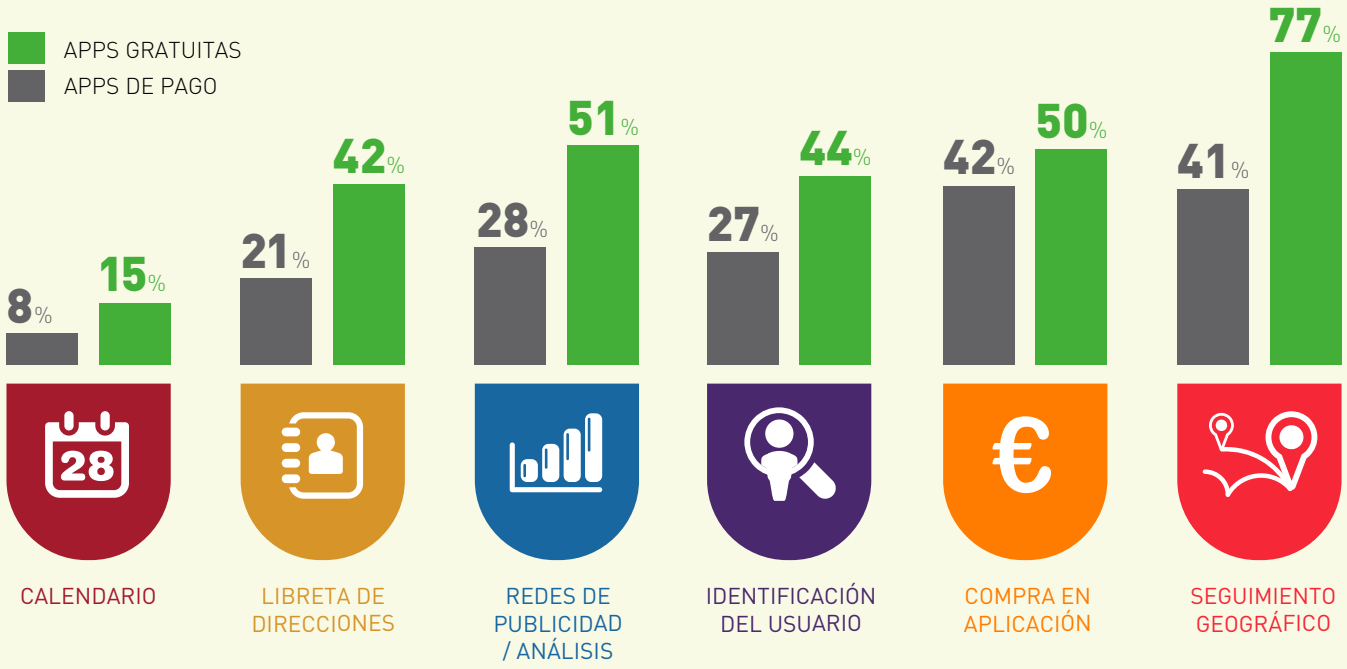
a) Apropiación indebida de la información
b) Abuso del dispositivo
c) Incumplimiento legal y normativo [8] [9].

A Apropiación indebida de la información

La información se ha convertido en una preciada mercancía en la Sociedad de la Información y el Conocimiento. Además de la información personal, cada vez es más frecuente el robo de información empresarial, muchas veces como consecuencia de una gestión poco cuidadosa tanto de los dispositivos móviles como de la información que se custodia en ellos.

Acceso a información sensible

Fuente: Appthority



La caída de las barreras existentes entre la esfera personal y la profesional hace que **cada vez que dejamos una huella en el mundo digital (un SMS, un correo electrónico, una fotografía, un tuit, etc.), además de actuar nuestra persona implícitamente actúa también nuestra relación con la corporación o corporaciones donde desempeñamos nuestro ejercicio laboral**. Es por ello que toda la información que vertemos a través de las 'apps' en el mundo digital, se convierte automáticamente en material valioso para terceros, tanto por lo que cada uno de nosotros es, como por lo que representa socialmente.

Debemos ser conscientes de la cantidad y la sensibilidad de la información que custodiamos en nuestros ***smartphones*** y del riesgo al que nos enfrentamos, puesto que no es únicamente la información que almacena, sino aquella que nuestro dispositivo es capaz de recoger, como nuestra geoposición. La figura anterior muestra cómo gran parte de las 'apps' más populares (agrupadas en 'apps' gratuitas y de pago), presentan comportamientos sospechosos respecto de la seguridad y la privacidad de los usuarios[10].

A continuación mostramos algunos de los **ejemplos de información más habitual que contiene un *smartphone***, así como las causas asociadas más importantes que dan pie a una apropiación indebida de los datos[11][12]:

- → **Lista de contactos** (tanto personales como profesionales)
- → **Agenda**
- → **Identificador único del usuario** (UUID), del teléfono, y número telefónico
- → **Información de credenciales**
- → **Hábitos de uso** del dispositivo
- → **Geolocalización**
- → **Registro de llamadas y SMS**
- → **Historial** de navegación
- → **Correo electrónico**
- → **Información sensible** de la compañía (clientes, informes, fotos, vídeos, etc.)

Falta de transparencia

Según datos recientes, únicamente el 61% de las 150 'apps' más descargadas tienen una política de privacidad clara donde se específica para qué y en qué condiciones va a ser utilizada nuestra información[13]. La inmensa mayoría de las 'apps' no informan ni de qué van a recoger ni de la finalidad de uso. Además, hay que ser conscientes de la existencia de algunas 'apps' que, de forma deliberada, utilizan el engaño y el comportamiento deshonesto para atacar el dispositivo móvil y sustraer información que va más allá de la contenida en el dispositivo, como credenciales de usuario, o números de tarjetas de crédito (utilizando, por ejemplo, técnicas de ***phishing***).

Las 'apps' que tienen una política de privacidad establecida presentan contratos de licencia enormemente extensos que raramente nadie lee pero que todo el mundo acepta, y que normalmente generan un entorno de actuación que beneficia claramente a los objetivos y fines del prestador de servicio, en detrimento de los derechos de privacidad del usuario.

> You grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License)
>
> **Facebook**

Poca granularidad en la elección de la información a facilitar

A excepción de algunos ejemplos loables, las opciones de privacidad de las 'apps' raramente ofrecen granularidad alguna sobre la información que realmente se quiere exponer al servicio. Los términos del contrato requieren habitualmente del uso de toda la información que se demanda en los permisos de instalación de la 'app', o bien que se decline el acuerdo de uso entre las partes. Frecuentemente, como hemos expuesto anteriormente, la 'app' no declara la información a la que va a acceder y con qué objetivos.

Limitación de propósito

¿Cómo es posible que una 'app' que provee una función de linterna nos pida acceso a nuestra agenda? Este es un claro ejemplo que ilustra el abuso que muchas 'apps' realizan de los permisos que requieren al instalarse. La información que una 'app' pueda requerir ha de ser proporcional a la funcionalidad que presta, aunque lamentablemente muchas aplicaciones no se ajustan a estos criterios.

Otros casos, quizás no tan evidentes, se basan en determinadas funcionalidades cruzadas que un servicio puede prestar a otro. Un ejemplo lo representan algunas redes sociales o plataformas de servicios, que prestan sus credenciales de autenticación para permitir que los usuarios se identifiquen en otros servicios o 'apps'. Al realizar esta operación, no únicamente se exponen credenciales en otro servicio sin conocer sus medidas de seguridad, sino que se da información a los primeros sobre los servicios que se están utilizando, las horas y tiempo de conexión, etc., consiguiendo así una mejor información de perfilado de los usuarios, con la que después podrán comercializar.

Falta de medidas de seguridad

Muchas aplicaciones ofrecen niveles de seguridad que garantizan que la información de los usuarios está a salvo, pero otras muchas son diseñadas y programadas por desarrolladores que o no son expertos en seguridad, o no tienen los medios necesarios para ofrecer unas medidas de seguridad aceptables. Exponer nuestra información - tanto personal como profesional - a estas 'apps' implica muy probablemente que ésta se pueda llegar a ver comprometida.

B Abuso del dispositivo

Diversas 'apps' intentan abusar del propio dispositivo móvil y de sus recursos (p. ej. cámara o micrófono), de las infraestructuras (conexión telefónica) o incluso del plan económico asociado a su uso. A continuación abordamos algunos de los casos de abuso de dispositivo más frecuentes.

Espionaje

Muchas 'apps' piden más permisos de los que realmente corresponden a la función que desempeñan. Se han dado casos donde 'apps' maliciosas han llegado a aprovechar estos privilegios para utilizar los componentes del smartphone con fines de espionaje. Pueden, por ejemplo, localizar el punto donde un usuario se encuentra en cada momento, identificarlo unívocamente y activar el micrófono o la cámara incorporada en su dispositivo, para así registrar lo que ocurre en cada momento. Es importante recordar también que la mayoría de los servicios que proporcionan las 'apps' pasan a través de ordenadores que no están bajo el control de la propia empresa, y que podrían ser atacados por terceros para sustraer información o interceptar las comunicaciones de los usuarios.

Muchas 'apps' piden más permisos de los que realmente corresponden a la función que desempeñan

Secuestro del terminal

Como hemos comentado anteriormente, las 'apps' pueden ser también construidas con motivaciones fraudulentas, y atacar directamente a nuestro terminal aprovechándose de sus vulnerabilidades, para apoderarse de él. Una vez queda bajo el control del atacante el dispositivo puede verse involucrado sin el conocimiento del usuario en actividades delictivas (p. ej. robo de información o ataque a otros sistemas informáticos) que pueden afectarlos a él mismo, a las infraestructuras de su empresa e incluso a terceros.

Agotamiento de recursos

Hay aplicaciones que buscan obtener réditos económicos agotando los recursos relacionados con el uso de los servicios de telefonía o las compras automáticas incrustadas dentro de las aplicaciones. Así, por ejemplo, existen aplicaciones que bajo la apariencia de dar una funcionalidad determinada, realizan llamadas a números de pago o envían SMS a servicios premium. Por otro lado, algunas aplicaciones incrustan compras semi-automáticas confusas para el usuario que se cargan a la cuenta de la plataforma o bien a la tarjeta de crédito previamente facilitada.

C Incumplimiento legal y normativo

Las Tecnologías de la Información y la Comunicación (TIC) se han incorporado de forma masiva a todos los ámbitos de nuestra vida, y especialmente al ámbito laboral, donde han sido claves para el aumento de la productividad y la innovación. Esta afirmación es especialmente cierta cuando nos referimos al uso de los dispositivos móviles corporativos, pues actualmente nos mantienen constantemente conectados al sistema nervioso de nuestra compañía, así como también a nuestras relaciones personales y hobbies, pues todo ello se halla dentro del mismo dispositivo.

Las normas de privacidad nacionales aplicadas en Europa provienen de la transposición de dos directivas europeas[13]:

- → **Directiva de Protección de Datos** (95/46/EC)
- → **Directiva ePrivacy (2002/58/EC, y revisada en 2009/136/EC)**

Estos documentos proporcionan el marco legal donde se establece como pilares básicos el consentimiento del usuario sobre la utilización de sus datos personales, las medidas de seguridad para su protección, y la proporcionalidad en el uso de estos datos respecto de la funcionalidad ofrecida por un sistema informático concreto. En España, las principales leyes aplicables son la Ley Orgánica de Protección de Datos (LOPD, 15/1999) y la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI, 34/2002).

Acuerdo de Términos y Condiciones

Habitualmente las condiciones de uso de una 'app' se encuentran en el Acuerdo de Términos y Condiciones (o Licencia de Uso) que se acepta a la hora de instalar la 'app', pero que muy pocos usuarios llegan a leer alguna vez. Estos Acuerdos, generalmente extensos, están diseñados para proporcionar un entorno favorable al prestador de servicio, con cláusulas que, muchas veces, al ser aceptadas[14]:

- **Lo convierten en propietario de la información que se deposita en su plataforma** (o 'app') o bien adquiere una licencia de uso libre de ámbito mundial no revocable, con la que pueden comerciar con la información sin que los usuarios puedan negarse ni cobrar por ello.
- **Lo exculpan de cualquier responsabilidad sobre las consecuencias de uso de su 'app',** limitando los supuestos de litigación permitidos y la jurisdicción aplicable.
- **Le permiten acceder a recursos del dispositivo móvil como la agenda personal,** las fotos, los vídeos, los sistemas de ficheros (p. ej. tarjeta SD), la cámara o el micrófono, entre otros, sin permitir la granularidad del permiso ni las condiciones en que se van a utilizar.
- **Le permiten cambiar las condiciones de licencia en cualquier momento; hecho que** implica usualmente la aceptación implícita de esos cambios por parte del usuario.

De esta forma, el conjunto de amplios derechos que una 'app' adquiere al instalarse le permiten acceder por entero a cada dispositivo móvil y obtener una gran cantidad de información, tanto la que se encuentra almacenada en él, como aquella que se puede obtener por el acceso a los diferentes componentes que lo conforman, como el GPS, el micrófono, o la cámara.

A pesar de ello, el usuario de las 'apps' normalmente tiene una falsa sensación de protección frente a temas de seguridad y privacidad, pensando a menudo que estas siguen los principios y recomendaciones de la legislación vigente y aplicable en estas cuestiones. Sin embargo, al amparo de una legislación diferente, concretamente la Patriot Act en EE.UU. y unas condiciones de uso aceptadas explícitamente por el usuario, podría permitir a los propietarios de las 'apps' almacenar una gran cantidad de información sobre cada uno de nosotros.

Sistemas de Información Empresariales

Adicionalmente, el uso de los sistemas de información cedidos por la empresa al empleado (p. ej. portátiles, móviles, etc.) está sujeto a la legalidad laboral vigente y a las normativas que la propia organización establece para la protección de la información y sus equipos. Se pueden diferenciar los siguientes aspectos claves [15]:

- **La utilización de los equipos por los trabajadores para fines no empresariales,** como podría ser el correo personal [16].
- **Las medidas que el empresario puede adoptar en el ejercicio de su derecho disciplinario.**
- **El poder de la Dirección y sus límites.**

No existiendo unas reglas absolutas al respecto, se establece que la relación entre el empleado y el empresario ha de seguir los principios de buena fe entre las partes y de control empresarial. El empresario puede controlar el uso que se da al equipamiento que pone en manos del empleado para el ejercicio de sus funciones, aunque para ello se tienen que mantener tres principios básicos: a) la idoneidad del control, b) la necesidad del mismo, y c) la proporcionalidad del control efectuado, garantizando en todo momento el derecho a la intimidad y al honor del empleado. Para despejar toda duda, es muy recomendable que el empresario comunique de forma efectiva a los trabajadores la normativa interna donde refleje los usos prohibidos y admitidos, así como la frecuencia y características de los controles que se podrían llegar a efectuar.

Principales riesgos asociados a la descarga y uso de 'apps'

A APROPIACIÓN INDEBIDA DE LA INFORMACIÓN

- → Falta de transparencia
- → Poca granularidad en la elección de la información a facilitar
- → Limitación de propósito
- → Falta de medidas de seguridad

B ABUSO DEL DISPOSITIVO

- → Espionaje
- → Secuestro del terminal
- → Agotamiento de recursos

C INCUMPLIMIENTO LEGAL Y NORMATIVO

- → Acuerdo de Términos y Condiciones
- → Sistemas de Información Empresariales

004

Algunos ejemplos

Un reciente estudio demuestra que 83 de las 100 'apps' más populares presentan algún tipo de comportamiento de riesgo en materia de seguridad[8]. A continuación analizamos cinco de estas aplicaciones móviles, que cuentan con un elevado nivel de popularidad y se encuentran en la gran mayoría de dispositivos móviles, ya sean de uso privado o corporativo. Nos centraremos, precisamente, en evaluar y tomar conciencia de los riesgos que su uso puede suponer en un entorno corporativo.

Whatsapp

Whatsapp es una de las aplicaciones más populares entre los usuarios de smartphone y ofrece unas características muy atractivas de comunicación basada en mensajes de texto. Las principales preocupaciones estriban en[17]:

- → **Acceso a toda la lista de contactos, que se copia en un servidor externo.**
- → **Todas las comunicaciones (texto, fotos, vídeos, etc.) pasan a través** de servidores totalmente ajenos a nuestra empresa.
- → **Las comunicaciones no son seguras, por lo que alguien podría interceptar el contenido** de los mensajes de texto si la comunicación se establece a través de redes inseguras (p. ej. redes Wi-Fi no seguras).
- → **Han salido a la luz ciertos problemas de privacidad del usuario relacionados con funciones** propias del servicio, como la última conexión y la notificación de lectura de los mensajes.
- → **Podría llegar a suplantarse una identidad conectándose con un número de teléfono falso.**

Como en cualquier medio de este estilo, es muy importante no compartir información sensible por este canal, tal como contraseñas, documentos internos, contactos, etc. Este tipo de información siempre debe comunicarse por otras vías más seguras destinadas a tal efecto[18].

Skype

Es una aplicación muy usada para audio y videoconferencia, que también soporta compartición de imágenes, videos y mensajería instantánea. Los principales aspectos a tener en cuenta son:

- → **Utiliza un sistema de cifrado propietario, por lo que nunca sabremos si estamos solos** en la conversación[19].
- → **Todas las comunicaciones pasan por servidores externos a la empresa.**
- → **Skype en su versión para smartphone accede a nuestra agenda de contactos.**

LinkedIn

Es una aplicación para el uso de la popular red social profesional del mismo nombre. Este es un claro ejemplo de la fusión de la esfera personal y profesional, ya que ponemos a disposición de nuestra labor profesional a toda nuestra red de contactos. Los principales aspectos a considerar son:

- → **Análisis de seguridad [20] han revelado casos de envío de elementos de información** privados como notas de calendario, mensajes, contactos, etc. sin el consentimiento del usuario.
- → **Los mensajes enviados a través de LinkedIn se almacenan en servidores externos.**
- → **Todo lo que se almacene como público en esa red, podría afectar a la imagen de la empresa.**
- → **Falsos usuarios intentan contactar con otros usuarios para obtener información privilegiada.**
- → **Los nuevos productos, como 'LinkedIn Intro' hacen pasar todo el correo por los servidores** de LinkedIn.

Facebook

Facebook implementa una red social con millones de usuarios distribuidos por todo el mundo, mayoritariamente para mantener contactos personales. Los principales aspectos relacionados con la privacidad y la seguridad son:

- → **Todos los contenidos subidos se convierten de forma automática en propiedad** de Facebook, incluso la geoposición del usuario que puede llegar a obtener la propia 'app'.
- → **Muchos usuarios utilizan el engaño a través de estas redes para llegar al propio** teléfono móvil, o incluso a la propia persona.
- → **La configuración por defecto comparte la información propia con todo el mundo,** así que es importante no compartir aquella que pueda potencialmente ser confidencial o sensible.
- → **Hay programas maliciosos (p. ej. algunos juegos) que se transmiten a través de esta red social.**

Twitter

Twitter es otro ejemplo de red social que permite publicar mensajes de longitud limitada, y que nos sirve para seguir la actividad de otros o que otros sigan la nuestra. Algunas de las consideraciones de seguridad a tener en cuenta son:

- → **Establecer el perfil de privacidad, puesto que muchas veces dejamos a Twitter acceder** a nuestra geolocalización, y esto se publica cuando hacemos un post de un mensaje.
- → **El intercambio de mensajes cortos con Tiny URL hace que no tengamos referencia** semántica de la web dónde nos dirigimos cuando pulsamos en un enlace de este tipo. Desconfiemos de mensajes (privados o no) de orígenes desconocidos.
- → **No fiarse de las cuentas no verificadas, pues no sabemos qué o quién puede estar detrás.**

005

Algunas recomendaciones útiles en el Mundo de las Apps

A continuación ofrecemos una serie de sencillos consejos con el objetivo de minimizar los riesgos al utilizar aplicaciones móviles en un dispositivo móvil corporativo:

- **Seguir las reglas de seguridad establecidas por los responsables de Tecnologías** de la Información de la empresa, en cuanto a normas de seguridad en el uso del dispositivo móvil corporativo y, en particular, las normas respecto a las 'apps' cuya descarga no es recomendable o está prohibida.
- **Usar siempre la tienda de aplicaciones oficial del dispositivo.**
- **Revisar qué permisos solicitan las 'apps' al instalarse y que estos sean apropiados** para la función que va a desempeñar.
- **Configurar los niveles de privacidad que la aplicación permite.**
- **Revisar la configuración de geolocalización, y verificar si es necesario o no que esté** siempre activada.
- **En aplicaciones de redes sociales no abrir enlaces que provengan de usuarios** desconocidos, especialmente cuando estos van en forma de enlaces cortos (***TinyURL***).
- **No compartir contraseñas ni información sensible a través de 'apps'.**
- **Mantener actualizado el Sistema Operativo.**
- **Mantenerse informado de las últimas amenazas existentes.**
- **Tener en cuenta que lo que se comparte por una red social queda** permanentemente compartido.

006

A corto plazo

Aun sabiendo la dificultad que supone aventurar lo que puede ocurrir en un futuro próximo respecto a los riesgos del uso de 'apps' en un entorno corporativo, las señales que hoy recibimos nos animan a dibujar la foto del mañana:

A **Las fronteras entre las esferas personales y profesionales van a seguir cayendo. El profesional** aportará a la empresa contactos, relaciones, imagen, etc. a modo de una compañía-unipersonal. Gestionará su vida digital a través de su dispositivo móvil (smartphone), muy probablemente de su propiedad, en base a su identificación y gustos.

B **Gestionará a partir de su *smartphone*, tanto su individualidad como las relaciones laborales con las** diferentes compañías con las que trabaje. Valorará en cada momento si la funcionalidad ofrecida por las 'apps' merece el tiempo destinado y la información que va a verter sobre esa plataforma, pero no dudará en utilizarla si la funcionalidad merece la pena. El ***smartphone*** se conectará a otros objetos del usuario para su colaboración, pero seguirá siendo el eje sobre el que pivote la conexión individual del usuario al mundo digital.

C **La falta de modelo alternativo de negocio para las 'apps' a corto plazo, hará que se mantenga en** algunos casos el modelo publicitario y la venta de información personal a terceros. Sin embargo, el paso del tiempo y la acomodación del usuario a la publicidad intrusiva, hará que el valor de los datos personales vaya decreciendo, aunque lentamente. La fiebre por las 'apps' también irá decreciendo lentamente ante las dificultades de monetización inmediatas para los desarrolladores, y la sensación de gratuidad que rodea al usuario.

D **Las autoridades reguladoras de protección de datos reaccionarán ante los desajustes actuales, muy** probablemente comandadas desde Europa. Obligarán a los productores de 'apps' a ajustar su marco de trabajo para evitar abusos, pudiendo incluso llegar a emitirse sanciones ejemplificadores en casos abusivos.

E **Debido a que el número de *smartphones* crecerá enormemente, el fraude y los delitos que actualmente** afectan a los ordenadores de escritorio migrarán a los dispositivos móviles.

007

Conclusión

En los últimos cinco años hemos asistido a una 'appificación' de nuestras vidas. La irrupción de los smartphones y su uso generalizado en la sociedad han hecho florecer la industria de las aplicaciones móviles que ofrecen servicios y entretenimiento y que permiten concentrar en un mismo terminal actividades de carácter personal y profesional.

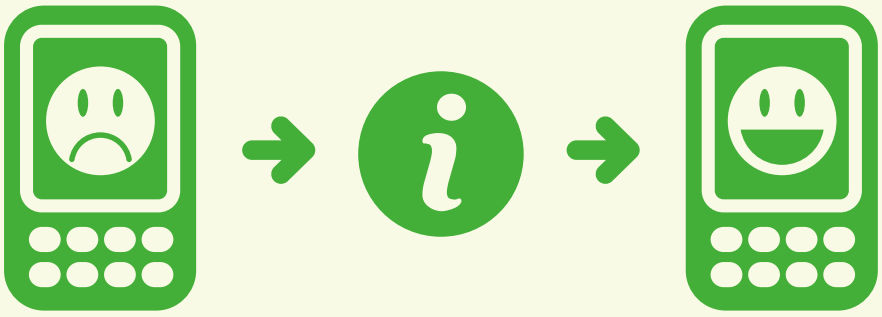
Precisamente esa conjunción de mundos ha hecho evidente los peligros de la utilización de 'apps' en un mundo corporativo donde la información, y concretamente la información de negocio, es un factor de competitividad esencial de las empresas. Los riesgos más importantes del uso de 'apps' en entornos móviles corporativos son

A **La apropiación indebida de información**

B **El secuestro del terminal**

C **El incumplimiento legal y normativo**

En nuestro desempeño profesional en la empresa somos depositarios de valiosos equipos informáticos y responsables del buen uso de la información corporativa a la que tenemos acceso. Ser conscientes de los riesgos que corremos al instalar determinadas 'apps' y sobre todo los mecanismos de mitigación más efectivos nos ayudará a sacar el máximo partido de nuestro smartphone en una sociedad donde la información es la fuente de la competitividad moderna.



008

Terminología

App
Aplicación móvil

Phishing
Ataque para robar credenciales basado en el engaño al usuario con una copia del sistema de información original, al que suplanta.

Consumerización
Proceso por el que dispositivos (generalmente teléfonos móviles) llegan al gran público debido a su asequibilidad en cuanto a precio y condiciones de uso.

PRISM
Programa de espionaje de la NSA (National Security Agency) estadounidense.

Smartphone
Teléfono móvil de altas prestaciones, capaz de ejecutar programas informáticos, establecer comunicaciones de datos, servicios de telefonía, etc.

UUID
Unique User IDentification:
Identificación unívoca de un usuario para un determinado sistema.

009

Referencias

[1] Ciberpaís, "**La distinción entre el mundo físico y virtual va a desaparecer**",
[Online] Disponible en:
http://tecnologia.elpais.com/tecnologia/2013/09/28/actualidad/1380330131_726588.html
Madrid (España), 28 de Septiembre de 2013.

[**2]** IAB Spain, "**V Oleada del Estudio Anual de Mobile Marketing**", IAB Research, [Online] Disponible en:
http://www.iabspain.net/mobile-marketing/
25 de Septiembre de 2013.

[3] Mazzeti M., Schmidt M. S., "**Ex-Worker at C.I.A. Says He Leaked Data on Surveillance**", The New York Times, [Online] Disponible en:
http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?_r=0
9 de Junio de 2013.

[4] RTVE, "**Traficantes de armas digitales**", La noche temática, [Online] Disponible en:
http://www.rtve.es/alacarta/videos/la-noche-tematica/
26 de Octubre de 2013.

[5] Gellman B., Soltani A., "**NSA collects millions of e-mail address books globally**", The Washington Post, [Online] Disponible en:
http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html,
15 de Octubre de 2013.

[6] Check Point, "**Checkpoint Mobile Security Survey Report 2013**", [Online] Disponible en:
https://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report2013.pdf
2013.

[7] EuropaPress, "**El 81% de los jóvenes conoce los riesgos de instalar 'apps' en el móvil**", [Online] Disponible en:
http://www.europapress.es/portaltic/sector/noticia-81-jovenes-conoce-riesgos-instalar-apps-movil-20131021120324.html
Madrid, 21 de Octubre de 2013.

[8] Appthority, "**App Reputation Report**", [Online] Disponible en:
https://www.appthority.com/resources/app-reputation-report
Summer 2013.

[9] Hogben, G., Dekker, M., "**Smartphones: Information security risks, opportunities and recommendations for users**", European Network and Information Security Agency (ENISA), [Online] Disponible en:
http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport
2010.

[10] Inteco, "**Guía para proteger y usar de forma segura su móvil**", [Online] Disponible en: http://www.inteco.es/guias/GuiaManual_movil
León (España), 2009.

[11] Wiewiórowski W. R., Kohnstamm, J., "**Warsaw declaration on the 'appification' of society**", 35th International Conference on Data Protection and Privacy Commissioners: a Compass in a Turbulent World, [Online] Disponible en:
http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/octubre/130924_Warsaw_declaration.pdf
Varsovia, 23 de Septiembre de 2013.

[12] Sheena L., "**FPF Mobile Apps Study**", FPF, [Online] Disponible en:
http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf
2012.

[13] Data Protection Working Party, "**Opinion 02/2013 on apps on smart devices**", Comisión Europea, [Online] Disponible en:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
Bruselas, 27 de Febrero de 2013.

[14] RTVE, "**Términos y condiciones de uso**", La noche temática, [Online] Disponible en:
http://www.rtve.es/alacarta/videos/la-noche-tematica/lnt-terminos-condiciones-uso-261013-2310/2101947/
26 de Octubre de 2013.

[15] Inteco, "**Utilización de las Tecnologías de la Información en el ámbito laboral**", Guías legales, [Online] Disponible en:
http://www.inteco.es/guias/guiaManual_utilizacion_tic_laboral
León, Diciembre de 2007.

[16] Autoritat de Protecció de Dades de Catalunya, "**Recomanació 1/2013 de l'Autoritat Catalana de Protecció de Dades**", [Online] Disponible en: http://www.apd.cat/ca/contingut.php?cat_id=146&cont_id=625, 2013.

[17] Bardia T., "**Cómo usar WhatsApp de forma segura**", El Periódico de Catalunya, [Online] Disponible en: http://www.elperiodico.com/es/noticias/tecnologia/usar-whatsapp-forma-segura-2037289 Barcelona, Agosto del 2012.

[18] Autoritat de Protecció de Dades de Catalunya, "**Dictamen en relació amb la consulta d'un Col·legi d'Advocats, en relació amb l'ús de les aplicacions "Whatsapp" i "Spotbros" en l'àmbit professional de les relacions entre advocat i client**", [Online] Disponible en: http://www.apd.cat/media/dictamen/ca_568.pdf Julio de 2013.

[19] Garfinkel S. L., "**VoIP and Skype Security**", [Online] Disponible en: http://www.cs.columbia.edu/~salman/skype/SkypeSecurity_1_5_garfinkel.pdf Universidad de Columbia, 2013

[20] CSA, "**Security Guidance for Critical Areas of Mobile Computing**", [Online] Disponible en: https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf 2013.

Este informe ha sido elaborado por
la División de I+D Seguridad de:

BARCELONA DIGITAL CENTRO TECNOLÓGICO

bdigital

TECNIO
Be tech. Be competitive

Más información **www.bdigital.org**