SEGURIDAD Y POLÍTICAS DE USO PARA DISPOSITIVOS MÓVILES EN EMPRESAS DE TI

Daniel Campos Villalobos

ULACIT, San José, Costa Rica

Resumen

La presente investigación expone la percepción de empleados y gerentes del sector tecnológico de Costa Rica tienen sobre la seguridad y políticas de uso, las cuales ponen en práctica para controlar la interacción entre dispositivos móviles y datos corporativos. En este estudio se encontraron datos alarmantes, estas revelan que la mayoría de las empresas no cuenta con ningún control sobre la forma en la que sus colaboradores manejan los datos corporativos dentro de sus terminales móviles. Incluso quedó demostrado se está delegando a los empleados el decidir sobre cuales medidas de seguridad usar para proteger tanto su información personal así como la de sus compañías. Estas lamentables prácticas están poniendo en riesgo la información de las empresas porque las exponen directamente a cualquier amenaza cibernética.

Palabras clave: Dispositivos móviles, Seguridad, Políticas de uso, Malware, Tecnología de información.

Abstract

The present research exposes the perception of both employees and managers from Costa Rica's tech community about the security and usage policies used by their companies to control the interaction between mobile devices and the corporate data. In this study we found alarming data that revealed that the majority of the companies don't have any control of the way that their employees manage the enterprise data within their mobile terminals. It was even demonstrated that companies are delegating their employees with the security decisions to protect both personal and corporate information. These terrible practices are putting in risk the organization's data and it is exposing it directly to any cybernetic threat.

Keywords: Mobile Devices, Security, Use Policies, Malware, Information Technology.

Justificación

Más personas están adoptando algún dispositivo móvil como su principal sistema computacional. Estas cifras han crecido más rápido de lo estimado y están influyendo en como las empresas y departamentos de TI perciben el uso de estas tecnologías. Como resultado, la adopción de programas que permiten a los empleados de una empresa llevar sus propios dispositivos móviles para interactuar con los datos y sistemas corporativos va en aumento.

Consecuentemente, se están implementando políticas de uso y seguridad para tratar de controlar la utilización de dichos dispositivos dentro de las organizaciones. Desafortunadamente, muchas empresas han fallado en hacer cumplir dichas políticas, lo cual las deja en riesgo de comprometer sus datos y exponerse a cualquier amenaza cibernética. Esta investigación pretende encuestar a individuos dentro de empresas de TI para conocer sobre la adopción, ejecución, monitoreo, cumplimiento de políticas de seguridad y uso de dispositivos móviles dentro de sus organizaciones.

Marco de antecedentes

En los últimos años se ha observado un marcado incremento en el uso de terminales móviles a nivel mundial. Jones (2013) indica que según un estudio realizado por Gartner el envío de tabletas y teléfonos aumentará en más de un 70% entre el 2012 y el 2017 mientras que los envíos de computadoras de escritorio y laptops decaerán en un 20% durante ese mismo periodo. Estas cifras apuntan a que existe una gran cantidad de personas llevan consigo al menos un dispositivo inteligente (tableta o teléfono). Consecuentemente, se podría deducir quienes lo poseen lo llevan a su lugar de trabajo.

Samsung Mobile (2013), revela que aún existe un pequeño porcentaje de empresas que actualmente prohíben el uso de terminales móviles a sus empleados, aunque también se determinó que el 61% de las empresas encuestadas en dicho estudio cuentan con algún tipo de política, la cual le permite a sus empleados llevar sus propios dispositivos móviles a su trabajo para interactuar con aplicaciones e información de la empresa. Incluso otro dato revelador dentro de este es que el 77% de los encuestados concuerdan en que llevar dos teléfonos (uno de trabajo y otro personal), simplemente no tiene sentido. Por esta razón las empresas, simplemente, están permitiendo a estos utilicen sus dispositivos personales para interactuar con datos corporativos.

La flexibilidad brindada por este tipo de productos a las empresas ha hecho prolifere su adopción; lo anterior, permitiendo a los empleados usar sus propios teléfonos y tabletas dentro de su organización. Sin embargo, se debe tener en cuenta que cualquier dispositivo móvil, al estar la mayoría del tiempo en posesión del usuario "incrementa el riesgo de que se comprometa algún recurso de la empresa" (Abhishek & Misra, 2013, p. 97).

Sin importar si el dispositivo móvil fue proveído por la empresa, o traído por el empleado, se debe tener muy claro que si alguien llegara a tener acceso no autorizado a los datos almacenados en el terminal móvil se podría "revelar toda la información del usuario e incluso podría resultar en la pérdida de los datos del mismo" (Song, Shen, Zhang & Gu, 2014, p. 1247). Esto evidentemente no solo expone al usuario sino que también expone los datos e intereses comerciales de la compañía. Incluso existen muchas empresas, las cuales implementan políticas de uso para móviles; pero, "no siempre los responsables de TI están alineados con las prácticas afines a dichas políticas" (Samsung 2013, p. 3).

Es importante recalcar que una función primaria de TI es definir el grado de acceso y de seguridad otorgado a los usuarios cuando intentan hacer uso de recursos corporativos. Aunque lo anterior es una regla sagrada, en la práctica se convierte en una problemática. Esto al tratar de aplicarlo en el ámbito de los dispositivos móviles, pues en muchos casos TI no cuenta con los recursos necesarios. Aunado a esto la desinformación y poca experiencia de muchos de ellos se ve que controlar los dispositivos móviles se convierte en algo épico y quizá imposible.

Information Security Media Group (2014) en una entrevista hecha a JD Sherry de Trend Micro señala que "más individuos están teniendo problemas en el uso de plataformas móviles ya que no están utilizando precauciones de seguridad básica". Esto a su vez está provocando que un mayor número de estos usuarios se infecte al descargar contenido malicioso. Lo anterior, no es solo un gran problema para ellos sino también para las organizaciones, las cuales tienen políticas para que sus trabajadores usen sus propios dispositivos móviles.

Entre los principales retos que TI enfrenta a la hora de administrar y controlar el uso de dispositivos móviles podemos tomar en cuenta el cómo "lidiar con uso de terminales no homologados por la empresa así como el uso de aplicaciones, conexiones, contenido o servicios que no han sido aprobados por TI" (Abhishek & Misra, 2013, p. 97). De igual manera la incapacidad de TI, en cuanto a poder controlar la actualización de programas y sistemas operativos de los móviles, hace que los recursos corporativos sean fácilmente comprometidos gracias a vulnerabilidades dentro de aplicaciones de terceros.

En cuando a plataformas móviles popularmente utilizadas, actualmente Android es uno de los sistemas operativos que dominan el ámbito de las tecnologías móviles. Asimismo, es el más atacado por diversas amenazas. McAffee (2013) contabilizó un total de "36,699 muestras de malware en donde el 97% correspondían a software malicioso hecho exclusivamente para Android". Lo alarmante es que 95% de las muestras aparecieron en el transcurso de los 12 meses previos a la prueba.

F-Secure (2013) señala que Android, como tal, "ha tenido un bajo número de vulnerabilidades lo cual hace que este sistema operativo sea difícil de atacar". Sin embargo, dichos esfuerzos se desvanecen por la gran facilidad con la que han tenido los creadores de malware para engañar a los usuarios para instalar de manera voluntaria programas infectados en sus dispositivos. Debido a lo anterior, conceden los permisos necesarios para controlar a placer estos sistemas. Este tipo de timos expone directamente a los sistemas corporativos; pues, al permitir que una unidad móvil infectada acceda a la red empresarial, se le está garantizado la oportunidad para propagarse, o capturar información sensible de la organización.

Empresas como Apple han hecho grandes esfuerzos para minimizar estos ataques al introducir tecnológica para proteger a sus usuarios. Según Apple (2014), en su reporte sobre seguridad de IOS, "se ha incluido hardware dedicado para encriptación de datos y mecanismos como el "App Code Signing" que solo permite al sistema operativo a ejecutar aplicaciones que han sido digitalmente firmadas por Apple". Dicho tipo de tecnología previene que aplicaciones de terceros puedan descargar, o usar código malicioso. Este tipo de características son tomadas por las empresas como un extra a la hora de definir el perfil de los dispositivos permitidos dentro de sus políticas.

En conclusión, TI es quien debe ser responsable de la seguridad de los datos y sistemas corporativos, sin embargo, es evidente que la seguridad en los dispositivos móviles no es únicamente responsabilidad de esta, sino que gran parte recae en los usuarios. Los departamentos de informática, por su lado, deben garantizar las herramientas y educación para los usuarios y de esta manera manejar sus dispositivos responsablemente. Lo anterior, para beneficiar a las organizaciones y quien la emplea. Esto es, sin duda, una misión complicada, en donde la innovación de mecanismos, los cuales mezclen seguridad con buenas prácticas va a ser la llave.

Objetivo general

Identificar si la seguridad y políticas de uso de dispositivos móviles creadas por los departamentos de TI en empresas de tecnología se alinean con las prácticas reales de sus empleados.

Objetivos específicos

- Determinar cuáles medidas de seguridad son utilizadas por los usuarios de dispositivos móviles para proteger sus datos y los de su organización.
- Señalar qué políticas de uso se implementan en las empresas para el uso o manejo de dispositivos móviles.
- Conocer si las empresas imponen a sus empleados medidas de seguridad a la hora de manejar datos de la organización en sus dispositivos móviles.
- Listar cuáles soluciones o aplicaciones de seguridad y privacidad son mayormente utilizadas por las empresas investigadas.
- Analizar el valor a nivel de seguridad y privacidad que realmente aportan las aplicaciones más utilizadas por las empresas e individuos investigados.
- Investigar cuáles mecanismos usan las empresas para asegurar que sus políticas de uso y seguridad son respetadas por sus usuarios.

Marco metodológico

Esta investigación hace uso de la recolección y análisis de datos por medio de una encuesta. Al hacer uso de esta metodología cuantitativa, se podrán identificar patrones de interés sobre la seguridad y políticas de uso que aplican las empresas de tecnología para regular el uso de dispositivos móviles entre sus empleados y gerentes.

Sujetos y fuentes

Se tomaron como referencia, para esta investigación, varios datos y preguntas extraídas de una encuesta realizada en 2012 por IDG en nombre de Samsung; en la cual se analiza la adopción de políticas de "trae tu propio dispositivo" entre los empleados y gerentes de diferentes empresas estadounidenses. Adicionalmente se tomaron como referencia varios reportes de amenazas y del estado de Internet publicados en el presente año por la empresa de seguridad finlandesa F-Secure.

Población y muestra

La muestra que se generó consta de un total de 339 correos electrónicos de empleados y gerentes de diversos departamentos de TI y empresas de tecnología presentes en Costa Rica. Esta se construyó con base en una búsqueda de contactos obtenida por medio del sitio web de la Coalición Costarricense de

Iniciativas de Desarrollo (CINDE) y directamente en los portales web de múltiples empresas de tecnología. Como meta, se pretende completar al menos 50 encuestas las cuales respondan a las preguntas esta investigación.

Selección de la muestra

Para participar y calificar de dicha encuesta, los participantes deberán cumplir con los siguientes requisitos:

- Debe ser mayor de 18 años.
- Debe ser un empleado de tiempo completo.
- Debe contar con al menos un dispositivo móvil inteligente.

Instrumento de recolección de datos

El instrumento de recolección de datos será una encuesta electrónica aplicada por medio del sitio web http://www.surveymonkey.com.

Este sondeo se divide en diferentes grupos de preguntas las cuales tienen como objetivo:

- Ubicar al participante dentro del contexto de su empresa, años laborados y grupo de edad.
- Clasificar el tipo de terminal móvil utilizada por el participante.
- Identificar si la empresa subsidia, en algún grado, el costo del terminal móvil de sus empleados o el costo total o parcial de la factura telefónica, o de datos de los mismos.
- Determinar si la empresa del participante permite que sus empleados utilicen sus propios dispositivos móviles.
- Determinar si la empresa del participarte cuenta con políticas en cuanto al uso y manejo de dispositivos móviles.
- Identificar si la empresa tiene algún mecanismo de auditoría o comprobación de que los empleados efectivamente cumplan con las políticas de uso para los terminales móviles.
- Investigar si la empresa del participante da algún tipo de educación a los empleados sobre cómo utilizar adecuadamente su móvil a la hora de interactuar con los datos corporativos.

Análisis de resultados

La encuesta que se realizo en la presente investigación, se envió a 339 correos electrónicos de empleados y gerentes de departamentos de TI y empresas de tecnología presentes en Costa Rica. Del total solo 69 personas lo contestaron. De esta cantidad 65 completaron la encuesta correctamente, pero, cuatro fueron descalificados durante la ejecución de la misma por no cumplir con los requisitos solicitados.

Ahora bien, es importante destacar que el 42,65% de los encuestados está en un rango de edad de entre los 30 y 39 años, seguido por un 22.06%, el cual corresponde a participantes de 21 y 29 años. Adicionalmente, un 17.65% fue el tercer grupo más importante de 40 a 49 años. El resto de las personas quienes tomaron parte de la encuesta son mayores de 50 años. A nivel de género el 76.47%

corresponde a hombres y el 23.53% fueron mujeres. Además el 76.57% aseguró tener tres, o más años de laborar para sus empresas.

También se encontró que, del total de integrantes de la encuesta, un 46.88% se desempeña en puestos relacionados directamente con TI, programación y calidad, esto por un lado. Por el otro, el 28.13% corresponde a individuos en puestos de gerencia, líderes y dueños. El restante 25.01% correspondió a empleados ubicados en otros puestos no relacionados directamente con TI; pero, en departamentos dentro de las mismas empresas de tecnología y otros colaboradores externos.

En cuanto al uso de terminales móviles, los datos recolectados revelaron que la mayoría de los encuestados (71.4%) consideran a su teléfono celular como su principal dispositivo móvil. Adicional a este hay un 27%, el cual, además de su teléfono celular utiliza algún tipo de tableta y consideran a ambos esenciales. Tanto así que incluso el 29% de la muestra confirmó prefieren perder los datos de sus computadoras personales antes que perder los datos en sus dispositivos móviles. Este pequeño porcentaje indica hay personas quienes están empezando adoptar a sus terminales móviles como su dispositivo computacional primario.

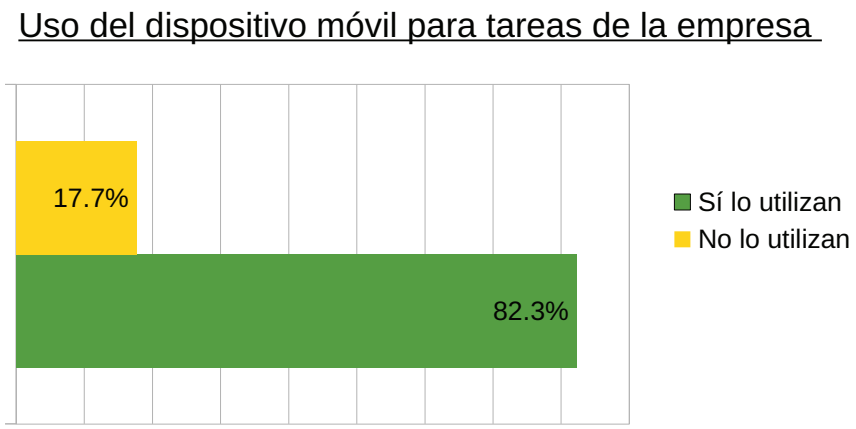


Figura 1. Participantes que afirmar usar su dispositivo móvil para realizar tareas de su empresa.

Como se muestra en la Figura 1, el sondeo reveló que la mayor parte de todos los encuestados (82.3%) afirma utilizar su dispositivo móvil principal para ejecutar tareas relacionadas a sus empresas. Incluso el 70.97% lo hace desde dispositivos móviles 100% personales; los cuales fueron adquiridos por sus propios medios y por convenios con sus empresas. Además, el 61.29% admitió que su empresa no cubre de forma parcial, o total, la cuenta telefónica ni de datos de sus teléfonos o tabletas. Finalmente, si se hacen algunos cálculos, con las cifras anteriormente citadas, se nota, entre los participantes quienes utilizan sus terminales para asuntos laborales, hay un 50.98% el cual adquirió por cuenta propia su dispositivo móvil y paga mensualmente el costo total de su cuenta telefónica o de datos.

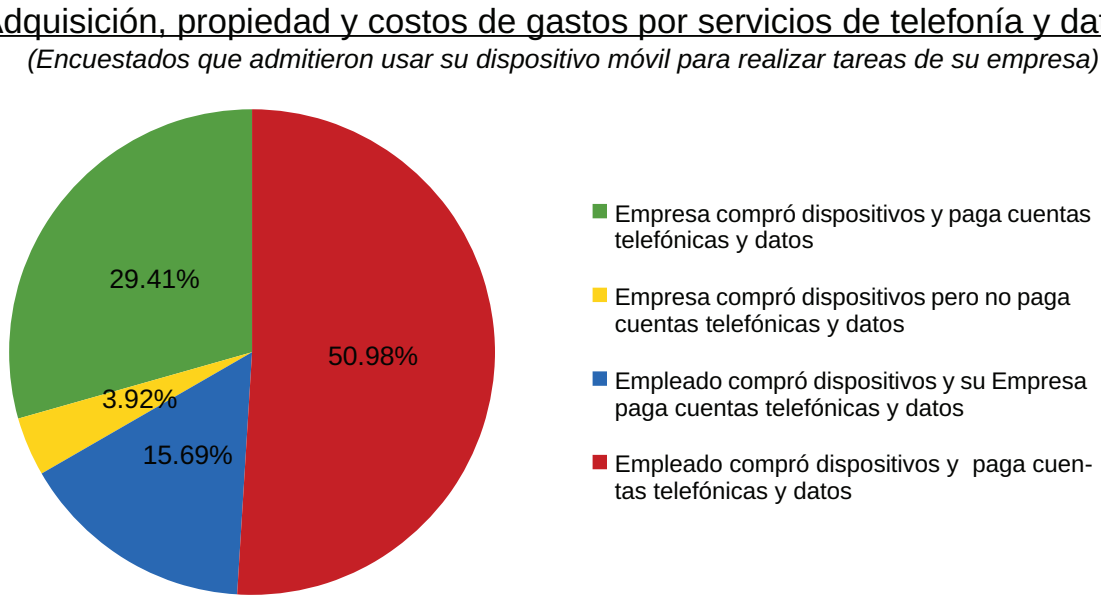


Figura 2. Comparación de como los empleados adquirieron sus dispositivos móviles y como financian el costo de los servicios por el uso de los mismos.

Los datos de la Figura 2 son muy relevantes, ya que la mayoría de estas empresas están permitiendo a sus empleados tener acceso desde sus terminales móviles a datos corporativos potencialmente confidenciales. El riesgo observado está en el 50.98% de los casos; lo anterior porque se trata de colaboradores quienes adquirieron su celular o tableta por cuenta propia; además, pagan sus propias facturas por servicios. Este detalle, de una u otra forma, faculta a este grupo a omitir controles y políticas de uso por parte de TI y automáticamente delega la seguridad de los datos corporativos al usuario.

Después de ver estos datos se cree que la solución está en que las empresas le den un celular o tableta dedicada a sus empleados. Pero, definitivamente, esto no es una medida efectiva, pues no garantiza la forma en la que un empleado pueda manipular o hacer uso de los datos corporativos. Inclusive llama la atención el hecho de que la mitad de los encuestados aseguró preferir usar un solo teléfono inteligente el cual puedan usar para el trabajo y uso personal.

En cuanto al uso que los participantes de la encuesta le dan a sus terminales, se puede destacar la utilización del correo corporativo (87.09%), los calendarios (77.41%) y otras aplicaciones empresariales (64.51%). Por lo tanto, definitivamente, la mayoría sí interactúa con información y datos de su empresa directamente desde su terminal móvil. Todo lo anterior pone en evidencia que las empresas necesitan mecanismos, los cuales ayuden a regular la forma en la cual sus trabajadores manipulan los datos corporativos desde sus dispositivos móviles personales.

Aunque, lo ideal sería que todas las empresas cuenten con mecanismos para gestionar el uso de información corporativa desde los dispositivos móviles de sus colaboradores, la realidad es otra (ver Figura 3). Por un lado, el 64.5% de los participantes asegura sus empresas no cuentan con ningún tipo de política, la cual regule como los empleados usan sus terminales dentro de sus instituciones. Por otro, hay que tomar en cuenta quizás muchas de esas empresas tengan algún tipo de reglamento sobre el uso de dispositivos móviles, pero, el hecho de que sus trabajadores ignoren, o no sepan, este reglamento es exactamente equivalente a no tenerlo del todo.

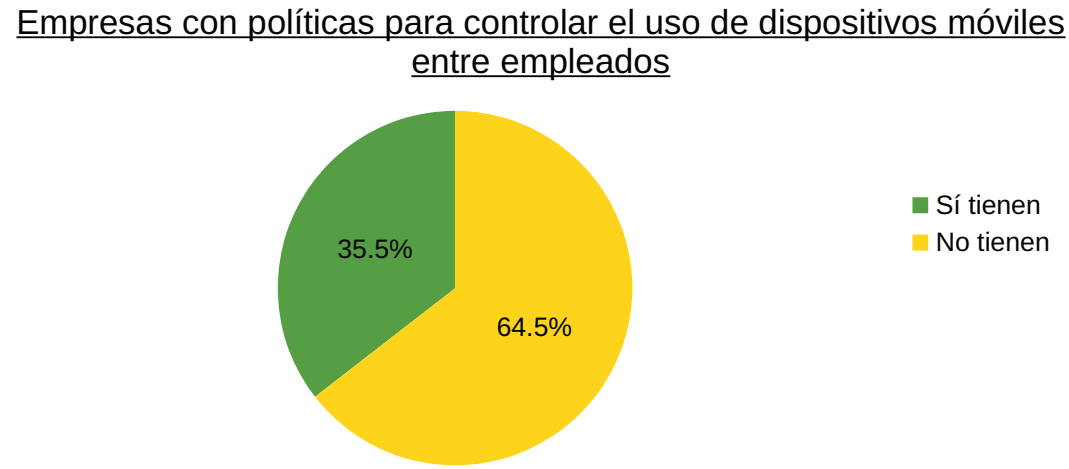


Figura 3. Percepción de los participantes sobre políticas utilizadas por sus empresas para regular el uso de dispositivos móviles entre empleados.

El 35.5% restante aseguró que sus empresas cuentan con dichas políticas. Este pequeño grupo mencionó diversas políticas de las cuales resaltamos los más relevantes siguiente:

1. Solo se permite el uso de dispositivos móviles proveídos por la empresa.
2. Uso restringido de los dispositivos móviles durante la jornada laboral.
3. Guardar dispositivos móviles personales en un casillero durante la jornada laboral y solo usar durante el almuerzo o recesos.
4. No utilizar los dispositivos móviles para enviar datos sensibles de la empresa.
5. Prohibido enviar mensajes de texto.
6. No conectar dispositivos móviles personales a la red empresarial.
7. Filtrado de contenido web por medio de la red empresarial.
8. Bloqueo de pantalla obligatorio para los dispositivos móviles.
9. Bloqueo de pantalla obligatorio para los dispositivos móviles haciendo uso de claves alfanuméricas.
10. Uso de antivirus es requerido.
11. No usar la red 3G para burlar los filtros de la red empresarial.

En resumen, solo una de las anteriores políticas (uso de antivirus) puede ser fácilmente verificada y gestionada por los departamentos de TI. Otra de las políticas listadas como el no conectar dispositivos móviles personales a la red empresarial quizá pueda implementarse y gestionarse por medio de esta. Pero, con un costo alto de tiempo y recursos. El resto se basan en el hecho de que los empleados van a acatar los reglamentos y ciegamente las instituciones y TI van a tener confianza en el juicio y las acciones de sus usuarios. Este hecho es alarmante, pues se expone la posibilidad de un gran número de empresas, las cuales no tienen control sobre los datos empresariales circulantes en los terminales móviles de sus empleados y están totalmente expuestas diversas amenazas cibernéticas.

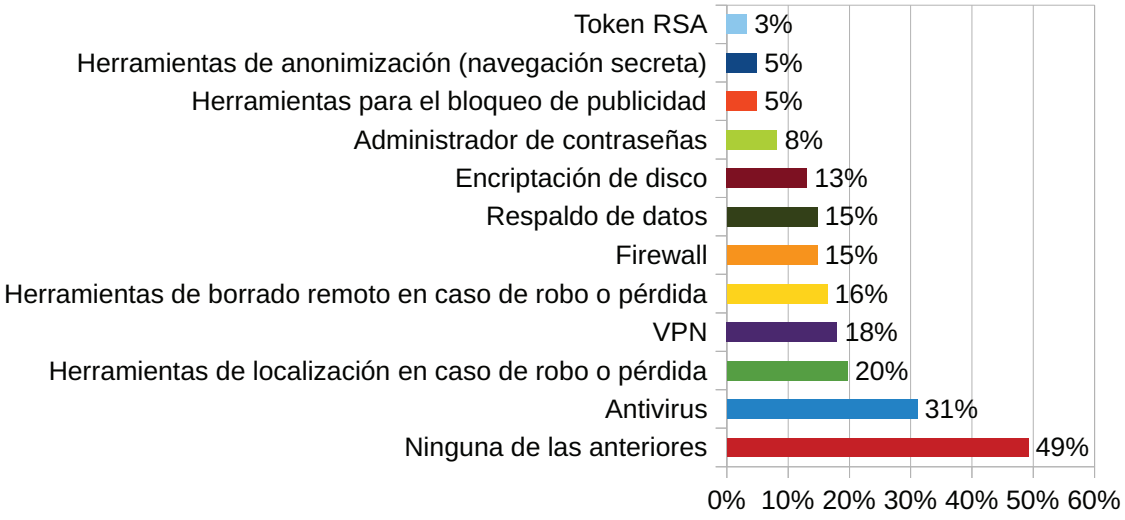


Figura 4. Aplicaciones de seguridad para dispositivos móviles exigidas por las empresas y departamentos de TI a sus empleados.

Por un lado, la Figura 4, nos revela otra alarmante realidad la cuál encaja con los datos sobre la no implementación de políticas de uso y seguridad por parte de las empresas. Como se puede apreciar un 49% de los encuestados corroboró que su empresa, o departamento de TI, no les exige a sus empleados utilizar herramientas de seguridad básicas para la protección de los datos e integridad de su terminal móvil.

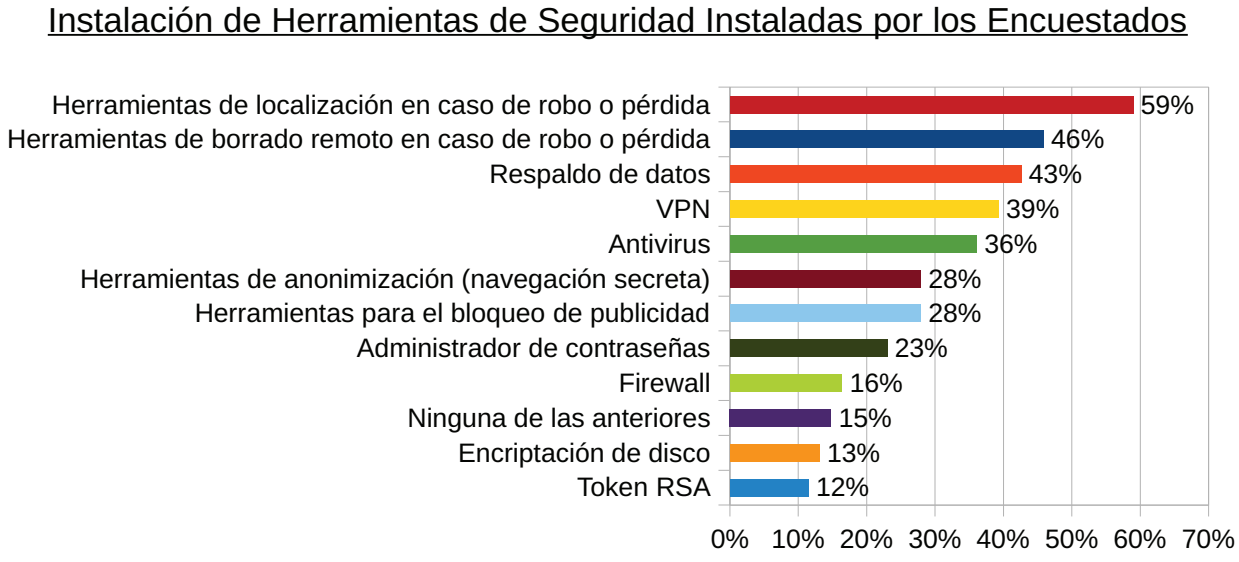


Figura 5. Aplicaciones de seguridad actualmente instaladas en los dispositivos de los encuestados.

Por otro lado, se debe rescatar el hecho que aunque las empresas o los departamentos de TI no lo exijan, hay un gran número de empleados quienes por su cuenta han instalado y utilizan herramientas de seguridad en sus teléfonos celulares y tabletas. Asimismo, en la Figura 4, podemos notar que el *top 5* de las herramientas de seguridad que más se utilizan son:

1. Herramientas para la localización en caso de que su unidad se pierda o sea robada.
2. Herramientas para borrado remoto en caso de que su unidad se pierda o sea robada.
3. Respaldo de datos.
4. VPN.
5. Antivirus.

Según Abhishek & Misra (2013), "El hecho de que un dispositivo este con el usuario todo el tiempo incrementa el riesgo de que se comprometa algún recurso de la empresa". Por lo tanto, al mirar las dos herramientas más utilizadas parece que a muchos usuarios les preocupa más el porvenir de sus datos, si su celular o tableta se extravían o son robados, que lo sucedido a su dispositivo al estar en su bolsillo. Por esta razón, si tanta importancia tiene el valor de los datos cuando se pierde el control físico del dispositivo por no usar alguna medida que realmente pueda ayudar, como por ejemplo la encriptación de los datos del dispositivo. Sin menospreciar el valor que las herramientas de localización y borrado remoto pueden dar es claro pueden ser burladas fácilmente. Aunque, este detalle es conocido se ve que desgraciadamente la encriptación de disco es una de las técnicas de seguridad menos usada por los encuestados y menos exigen sus compañías.

En la última posición del *top 5* está el antivirus, el cual no está mal como medida de seguridad; pero, tampoco es un secreto que progresivamente se ha vuelto ineficiente para protegernos de los peligros al que nos expone el Internet (Robb, 2014, p. 1).

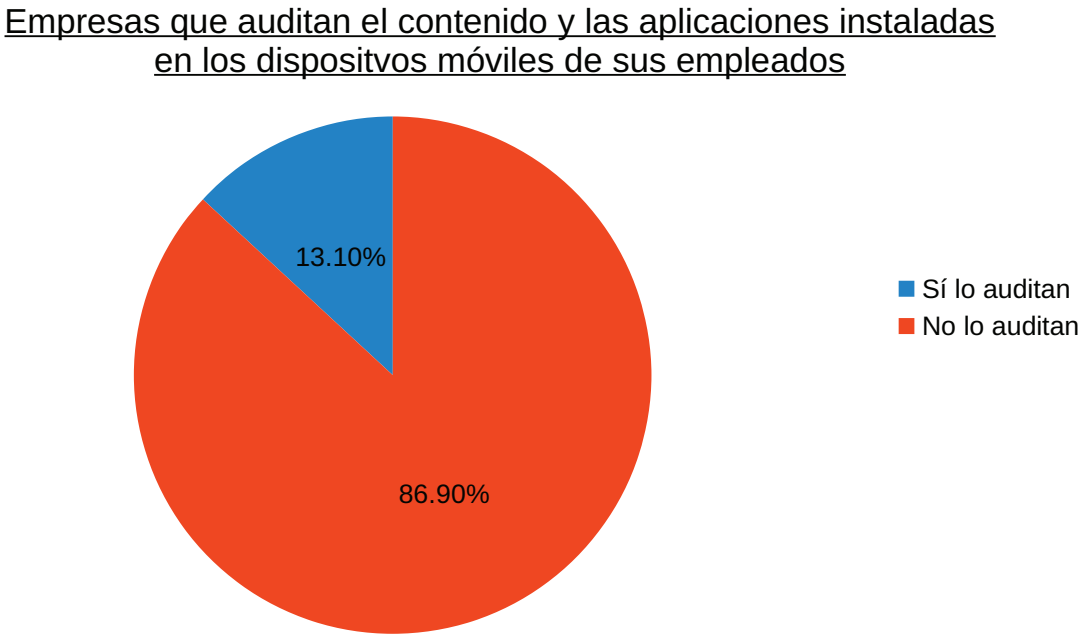


Figura 6. Empresas que auditan de alguna forma los dispositivos móviles de sus empleados.

Adicionalmente a lo mencionado sobre los datos de la Figura 5, hay un elemento del gráfico que llama la atención. Según la muestra hay un 15% que asegura no tener instalado ninguna herramienta de seguridad. Esto definitivamente es un dato para preocuparse, pues por ese pequeño porcentaje una empresa podría verse expuesta a ataques o comprometer datos confidenciales. Asimismo, los resultados son claros y se ha comprobado pocas empresas aplican medidas de seguridad o tienen políticas para gestionar el uso de las terminales móviles de sus usuarios.

Aunado a esto, se puede apreciar en la Figura 6, un 86.90% de los encuestados afirman que su empresa no audita de ninguna forma el contenido o las aplicaciones instaladas en las terminales móviles de sus empleados. Este confirma, simplemente, no hay control en este ámbito y las empresas, así como sus departamentos de TI basan su plan de seguridad móvil en la confianza y buenas prácticas de sus empleados. Lo anterior, está muy lejos de ser óptimo para garantizar la privacidad y confidencialidad de los datos corporativos.

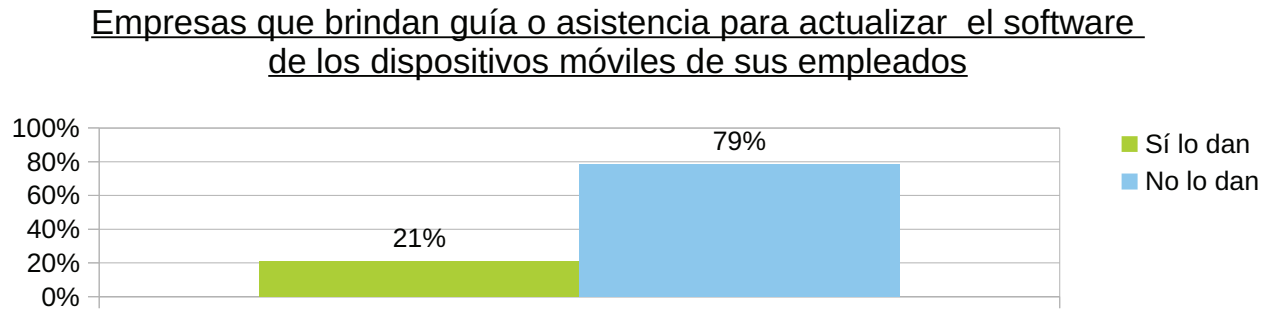


Figura 6. Empresas que asisten a sus empleados para que mantengan actualizados sus dispositivos.

También se debe aclarar que aunque una empresa cuente con políticas de uso adecuadas, e incluso herramientas, las cuales le permitan a TI gestionar y verificar su cumplimiento hay un detalle muy importante: las actualizaciones de software. Sin importar si TI instala el último antivirus en el terminal móvil; o si filtra la red para negar el acceso a sitios indebidos a los empleados, siempre habrá una posibilidad de que el móvil de alguno sea comprometido. Lo anterior, si no mantiene actualizadas sus aplicaciones y el sistema operativo del celular o tableta utilizado.

Sin importar el fabricante o sistema operativo de los dispositivos móviles, en general las actualizaciones de software de los mismos son gratuitas y continuas hasta el fin de vida del producto. Al tomar esto en cuenta, las empresas deberían adoptar a las actualizaciones de software como su primera línea de defensa en el ámbito de la seguridad móvil. Lo anterior, porque al hacerlo están cerrando vulnerabilidades y aplicando mejoras a este, así como al sistema operativo de las terminales de sus empleados sin tener que incurrir en gasto alguno.

Según la Figura 7, la encuesta recolectó datos los cuales indican como un 79% de los participantes no reciben guía o asistencia de sus empresas para mantener sus dispositivos corriendo con las últimas versiones de software. Aún así, existen usuarios responsables y preocupados por la seguridad y privacidad de sus datos personales, así como los de su empresa; los cuales aplican periódicamente las actualizaciones al software de sus dispositivos. Desgraciadamente, esta no es una práctica generalizada y hay muchos quienes por diversas razones simplemente no lo hacen, incluso apagan las actualizaciones automáticas para evitar sus aplicativos se actualicen del todo.

Finalmente, es casi seguro que todo grupo de TI conoce bien sobre la importancia de actualizar el

software de sus sistemas, y muy seguramente lo hace periódicamente. Entonces, si de antemano se sabe que la información confidencial de una institución va a estar almacenada en la terminal móvil de los empleados, ¿no es esto suficiente razón para que TI tome acción y evite delegar totalmente las tareas de seguridad a los usuarios?

En este caso, al mezclar dispositivos móviles, seguridad y políticas de uso, se encontrará que la responsabilidad es compartida. Lo anterior, porque, por un lado, las empresas deben comprometerse a proveer los recursos de seguridad necesarios a sus empleados así como también deben comprometerse a monitorear la utilización de dichos recursos; además de educar a sus empleados en su uso. Por el otro, los empleados y usuarios los cuales deben comprometerse a ser pro-activos en cuanto a la seguridad de sus datos personales y corporativos, cumpliendo a cabalidad con la seguridad y políticas de su empresa sobre el uso de dispositivos móviles.

Conclusiones

La adopción de dispositivos móviles entre la población está creciendo más rápido de lo que muchos estimaban. Actualmente, son más las empresas que están permitiendo a sus empleados interactuar con datos y sistemas corporativos desde sus dispositivos móviles. Desgraciadamente, estas y los departamentos de TI se han quedando atrás en la implementación políticas de uso y seguridad efectivas para controlar como estos acceden a los recursos corporativos desde sus terminales móviles.

Según la encuesta realizada durante la investigación, un 82.3% de los participantes aseguro usar su dispositivo móvil para realizar tareas relacionadas a sus empresas. De este porcentaje el 64.5% coincidió en que sus empresas no tienen ningún tipo de política, la cual regule como ellos usan sus terminales dentro de las instituciones. Estos resultados demuestran que las empresas se empeñan en delegar la seguridad de los dispositivos móviles a sus empleados y colaboradores. Lo anterior, pone la información de estas organizaciones y la de sus empleados a merced de cualquier amenaza cibernética.

En muchos casos las empresas han logrado generar un compromiso con sus empleados al asignarles u obsequiarles teléfonos inteligentes o tabletas. Incluso se ha logrado compromiso al pagar las cuentas de servicios telefónicos y de datos de ellos. Esto desgraciadamente no aplica a todos los casos y vemos que un 50.98% son quienes compraron los terminales y pagan los servicios propiamente. Esto deja a TI con rango de acción limitado; pues se vuelve muy complicado controlar lo que este porcentaje de empleados instala y ejecuta en sus teléfonos inteligentes o tabletas personales. Sin embargo, esto no exime a TI de su deber de monitorear y controlar cualquier abuso o exposición de los recursos corporativos el cual provenga de las terminales móviles de sus empleados.

Aunque los sistemas móviles de la actualidad cuentan con múltiples opciones para fortalecer su seguridad parece que no todos los usan. La encuesta realizada, mostró que un 15% de los participantes no usa ninguna herramienta de seguridad en sus dispositivos móviles, y un 49% asegura sus empresas, o departamentos de TI, no les exigen tener instalados ningún aplicativo de seguridad. Lo anterior, encaja con el 86.90%, el cual afirmó que sus empresas no auditan el contenido ni las aplicaciones instaladas en sus terminales. Es claro que TI no puede quedarse de brazos cruzados mientras existan empleados con acceso a datos corporativos desde terminales inseguras o comprometidas.

Desafortunadamente, el accionar de las empresas se ha quedado corto y vemos que un 79% de los encuestados aseguró: los departamentos de TI no dan ningún tipo de asesoramiento o ayuda en lo cual quizá sea una de las prácticas esenciales de seguridad: las actualizaciones de software. Aunque este dato es preocupante, se cree que con mayor apoyo de parte de TI las empresas podrían dar un primer paso y empezar a fomentar las buenas prácticas entre los empleados corporativos para ir creando poco a poco una cultura de seguridad dentro de las instituciones.

Quizá un segundo paso para mejorar toda esta situación está en que los departamentos de TI se

comprometan con sus empresas para revisar o crear políticas de uso, las cuales sean realizables y humanamente posibles de controlar y monitorear. Incluso a nivel de seguridad lo ideal es fortalecer y extender las actuales políticas de recursos como: Red, sistemas internos, etc, para de esta manera empezar a utilizar la encriptación en las comunicaciones de todos los servicios corporativos.

En definitiva, este no es un proceso rápido, fácil o barato. Y para ser realistas se debe admitir que pocas son las empresas las cuales tienen los recursos y la disposición para gastar en soluciones caras las cuales quizá no terminen siendo la solución. Por lo tanto, se cree que si las empresas dieran más apoyo a sus empleados y les inculcaran buenas prácticas de seguridad, además de permitir que TI se fortalezca en este ámbito, esto ayudaría a minimizar la gran cantidad de riesgos a quienes se exponen actualmente. Tener usuarios educados y comprometidos con la seguridad definitivamente es la ruta que se debe seguir.

Referencias

1. Abhishek, D., & Misra, A. (2013). Android Security: Attacks and Defenses. CRC Press. 96-105.

2. Apple. (February 2014). White Paper. IOS Security. Recuperado de http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf

3. F-Secure. (2014, February). How To - Whitepapers. Threat Report H2 2013. Recuperado de http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H2_2013.pdf

4. Information Security Media Group. (2014, June 25). Government info security news, training, education - GovInfoSecurity. BYOD: Bring Your Own Disaster? - GovInfoSecurity. Recuperado de http://www.govinfosecurity.com/interviews/byod-bring-your-own-disaster-i-2352

5. Jones, C. (2013, April 5). Gartner Survey Showing Declining PCs, Increasing Mobile Devices Through 2017. Forbes. Recuperado de http://www.forbes.com/sites/chuckjones/2013/04/05/gartner-survey-showing-declining-pcs-increasing-mobile-devices-through-2017/

6. McAfee. (2013, February 21). McAfee - Antivirus, Encryption, Firewall, Email Security, Web Security, Risk & Compliance. Mobile Malware Growth Continuing in 2013 | McAfee. Recuperado de http://www.mcafee.com/in/security-awareness/articles/mobile-malware-growth-continuing-2013.aspx

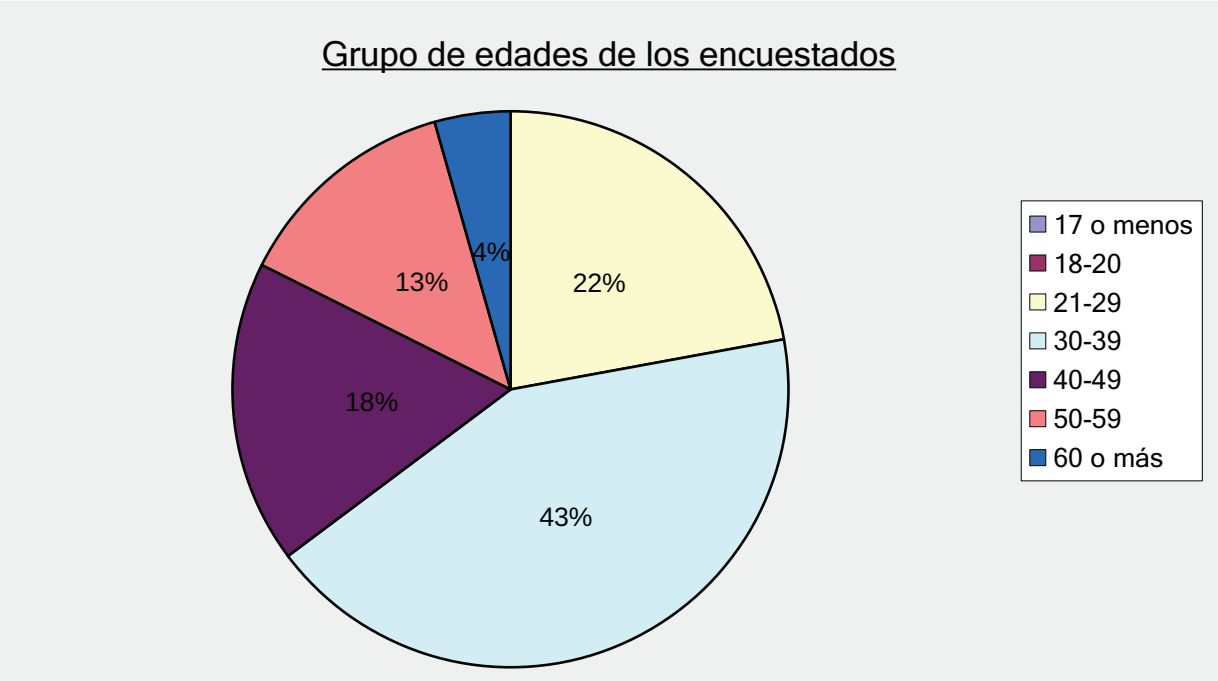
7. Robb, D. (2014, June 19). Is anti-virus software obsolete? Recuperado de http://techpageone.dell.com/technology/is-anti-virus-software-obsolete/#.U-gzC0iMqIg

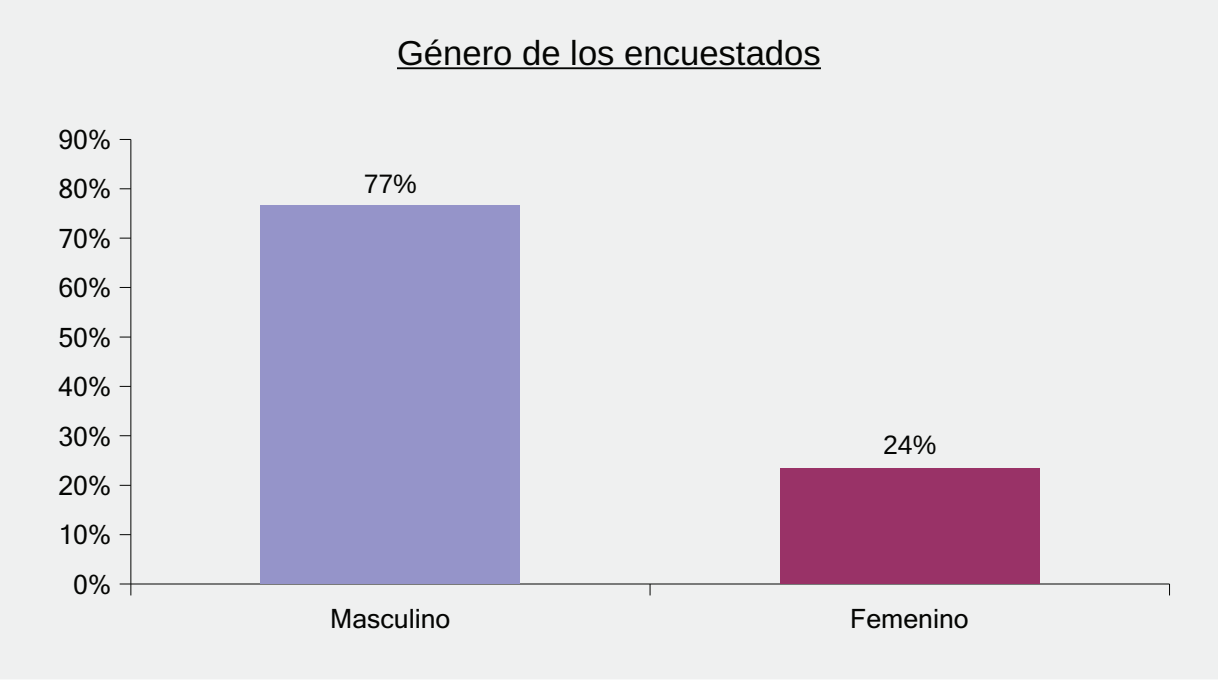
8. Samsung Mobile. (2013, January 8). Mobile Phones. Samsung Mobile BYOD Index: Comparing IT and End User Outlooks on Bring Your Own Device. Recuperado de http://www.samsung.com/us/pdf/byod/2013_BYOD_Index_20130103c.pdf

9. Song, H., Shen, Q., Zhang, X., & Gu, J. (2014, February 6). Research on Security Risk Assessment Model of Smart Mobile Terminals. Applied Mechanics & Materials, 1247.

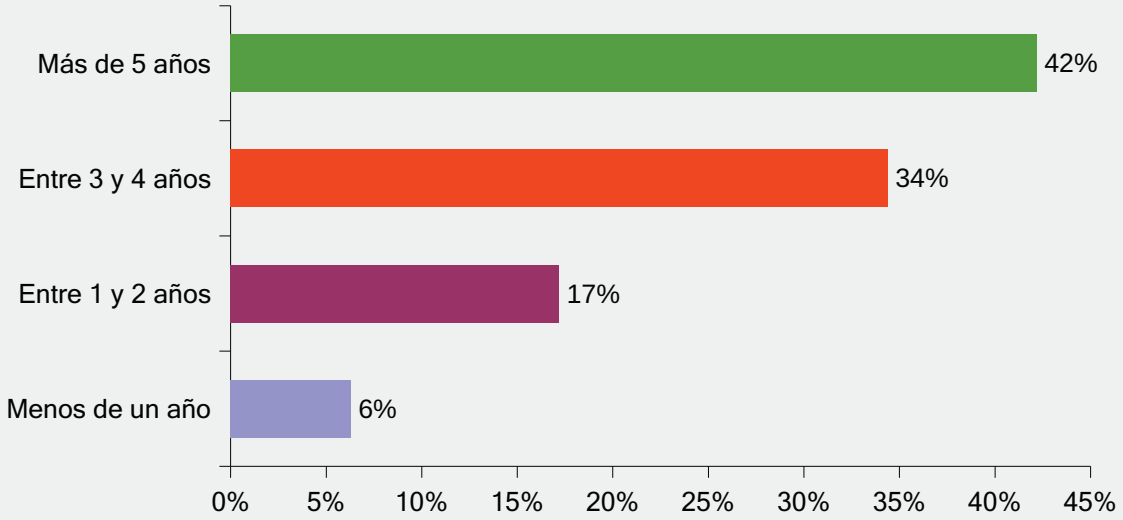
Anexos

Gráficos Adicionales de la Encuesta

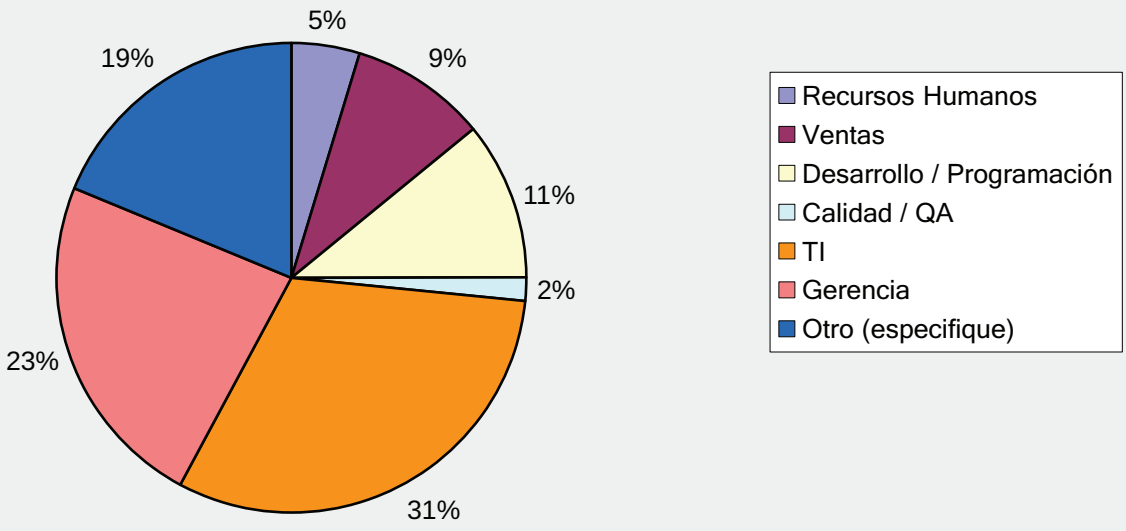




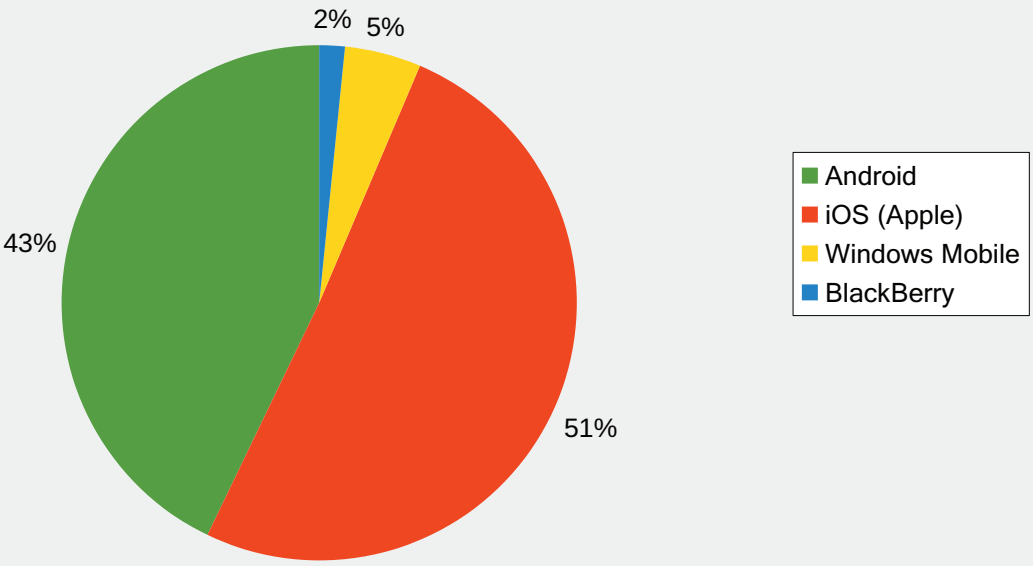
Años laborados por los encuestados para su empresa actual



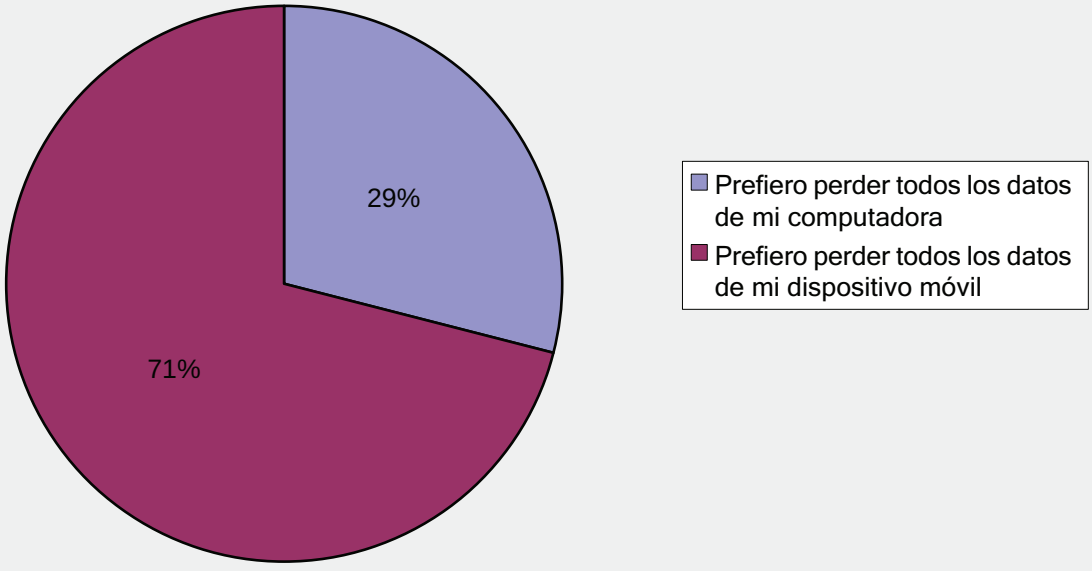
Departamento en el que se desempeñan los encuestados dentro de su empresa actual



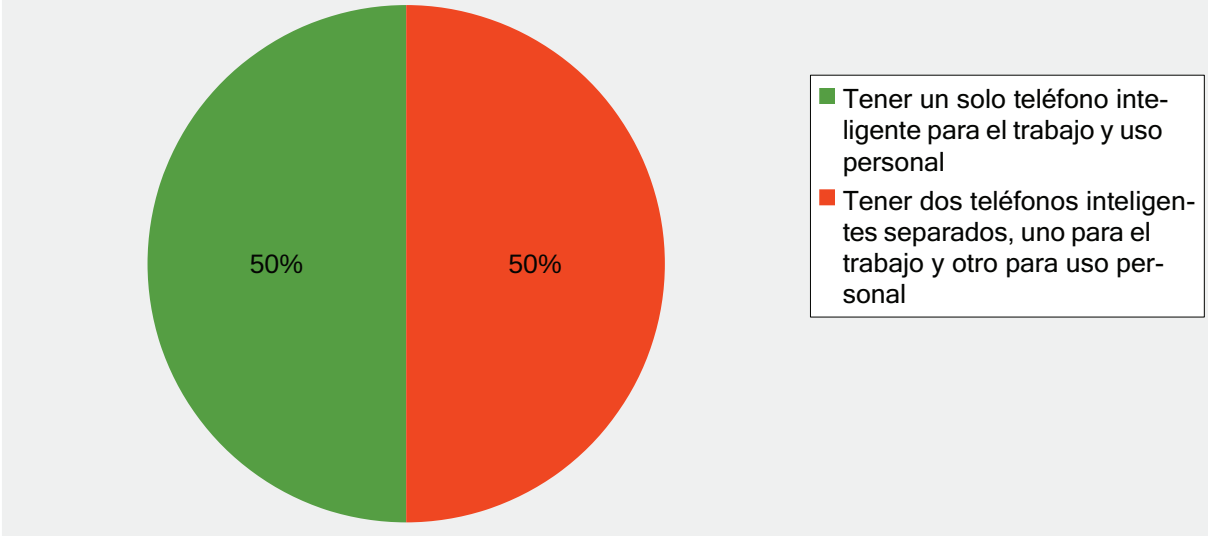
Sistema Operativo del principal dispositivo móvil de los encuestados



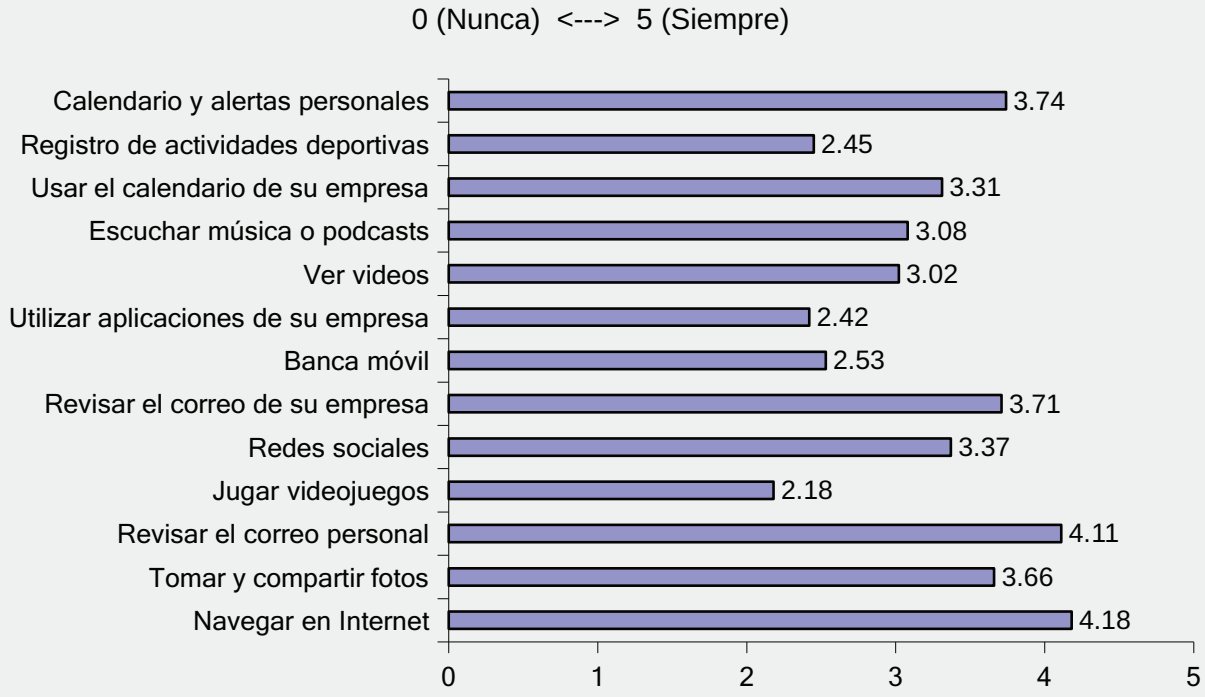
Opinión de los participantes sobre la pérdida de datos



Preferencia de los encuestados sobre el uso y número de dispositivos a utilizar para asuntos personales y de trabajo



Frecuencia de actividades ejecutadas por los participantes desde sus terminales móviles



Aplicaciones que los encuestado creen que aportan más seguridad a sus dispositivos