Cuaderno Activa
Revista científica de la Facultad de Ingeniería

Vulnerabilidad en dispositivos móviles con sistema operativo Android.

Vulnerability in Mobile Devices with Android Operating System.

Jorge Iván Escobar Martínez*
Luis Carlos Quinto Rojas**

Tipo de artículo: Reflexión.

Recibido: 9 de Enero, 2015
Aceptado: 24 de Abril, 2015

Resumen
El sistema operativo (S.O.) Android en dispositivos móviles es uno de los más usados en el mercado con un porcentaje del 48.96%. La vulnerabilidad, también entendida como fallos de seguridad, está relacionada con todo aquello que altera o provoca pérdida de información mediante amenazas en un sistema. Los incidentes de seguridad en dispositivos con S.O. Android se han incrementado de manera alarmante debido a la preferencia de sus usuarios, esto los hace más vulnerables de ser atacados. Se presenta un alto riesgo de vulnerabilidad en la violación de información confidencial de las personas que administran estos dispositivos. De acuerdo con esto, en este artículo se pretende reflexionar acerca de los aspectos más relevantes en dicho problema de seguridad que afecta a las terminales con S.O. Android, y se describen las amenazas más frecuentes que se presentan. Además, se dan posibles recomendaciones para lograr minimizar los riesgos de seguridad que se presentan en estas terminales.

Palabras clave: Sistema operativo Android, dispositivos móviles, seguridad.

Abstract
The Android Operating System (OS) for mobile devices is one of the most used in the market with a share of 48.96 %. Vulnerability is also understood as security flaws associated with anything that alters or causes loss of information through system threats. Security incidents on devices with Android OS have increased alarmingly due to the preference of its users. This makes them more vulnerable to being attacked. People who manage these devices present a high risk of vulnerability for violation of confidential information. In this paper, we intend to reflect on the most relevant aspects of this security issue, which is affecting terminals with Android OS, and describe the most frequent threats that occur. In addition, we give recommendations to minimize security risks that occur in these terminals.

Keywords: Android Operating System, mobile devices, security.

* Ingeniero Informático. Especialización en Seguridad de la Información. Tecnológico de Antioquia- Institución Universitaria. jescobar_2000@yahoo.com

** Ingeniero de Sistemas. Especialización en Seguridad de la Información. Tecnológico de Antioquia- Institución Universitaria. quintorojas@gmail.com

Introducción

La revolución tecnológica ha permitido que los dispositivos móviles inteligentes de última generación sean cada vez más sofisticados, convirtiéndose en verdaderos computadores. Estos dispositivos no solo se han transformado para realizar una simple llamada, sino también para otros propósitos como descargar archivos, enviar SMS, juegos interactivos, interactuar en redes sociales, realizar compras en línea, disponer información de geolocalización, ingresar a páginas web, entre otros. Estos dispositivos proporcionan conexiones de redes activas, permitiendo desplazarse a cualquier lugar del mundo y disponer de la información inmediatamente. Lo cierto es que estas características de alta disponibilidad en la red de Internet se deben considerar un factor de enormes problemas de seguridad por sus innumerables vulnerabilidades, por eso la importancia de generar políticas y mecanismos de seguridad para estos dispositivos móviles que permitan mitigar los riesgos.

El objetivo del artículo es realizar una reflexión acerca de los problemas de seguridad más comunes en equipos móviles con sistema operativo Android, ya que es uno de los más utilizados en el mundo y como tal, es el blanco predilecto de los ciberdelincuentes para robar información. El artículo introduce conceptos básicos de seguridad, S.O. Android, antecedentes y estadísticas o cifras de códigos maliciosos, usabilidades del S.O., detecciones de malware y una serie de vulnerabilidades o reconocidos fallos de seguridad más comunes, continuando con una serie de recomendaciones finales de cuáles son las posibles soluciones o prevenciones que se deben tener ante estos problemas de seguridad.

Marco conceptual

Seguridad

El término seguridad puede ser definido como "característica que indica que un sistema está libre de todo peligro, daño o riesgo" (Mifsud, 2012). Sobre seguridad en las tecnologías de la información y la comunicación (TIC) existen dos conceptos: seguridad informática y seguridad de la información; aunque son términos parecidos, existen grandes diferencias entre ellas.

a) Empleando una definición más formal, se toma la de iso/iec 27001, la cual manifiesta que la seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. (Mifsud, 2012).

b) La seguridad de la información se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a las organizaciones asegurar la confidencialidad, integridad y disponibilidad de su sistema de información (Mifsud, 2012), y aplica no solamente para organizaciones, también para personas que disponen de información que pueda ser vulnerada.

Vulnerabilidad

Se entiende por vulnerabilidad o fallo de seguridad todo aquello que provoca que los sistemas informáticos funcionen de manera diferente a lo programado, afectando la seguridad y pudiendo llegar a provocar la pérdida y/o robo de información sensible. (Crespo y Ramos, 2012).

Los fallos de seguridad más empleados para realizar intrusiones e infectar sistemas, están basados en software, habiendo también otro tipo de vulnerabilidades que se centran en el ámbito físico. Las intrusiones y vulnerabilidades de seguridad se pueden dar debido a fallas en software y en hardware, sin embargo, son las más comunes las intrusiones por fallos en el software.

Dispositivos móviles

Un dispositivo móvil se define como un aparato o dispositivo pequeño que cuenta con capacidades de procesamiento, conexión permanente o intermitente a una red, memoria limitada, diseños específicos para una función principal y versatilidad para el desarrollo de otras funciones. Tanto su posesión como su operación se asocia al uso individual de una persona, quien puede configurarlo a su necesidad y a su gusto. (González, 2012).

Debido a la importancia que han alcanzado los dispositivos móviles en la sociedad (Amazing Colombia, s.f.), la movilidad, conectividad, funcionalidad, procesamiento y operatividad se convierten en las principales características funcionales de las cuales disponen estos equipos.

El documento sobre seguridad en dispositivos móviles (Sallis y Caracciolo, s.f.), afirma que "hoy en día los dispositivos móviles van ocupando ese lugar tan privilegiado. En la pelea por ocuparlo, los actores principales del mercado se enfocan en "la experiencia del usuario" trabajando en los temas de seguridad de manera reactiva", para lo cual se centran en la problemática de la seguridad física, seguridad en los sistemas operativos, seguridad en las aplicaciones, seguridad en el almacenamiento de datos y seguridad en el control de accesos.

Sistema operativo Android

Frank (et al.,2014) declara que Android es una plataforma basada en Linux y distribuida para sistemas móviles con código abierto gratuito y que no requiere pago de licencias; el usuario tiene un fácil acceso a este sistema operativo, gracias a su interfaz gráfica, práctica y didáctica. Se trata de un sistema operativo basado en el kernel de Linux, diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes o tabletas. En comparación con muchas otras plataformas, Android permite a los usuarios administrar las funciones de seguridad en sus teléfonos o tabletas, desde un navegador hasta la más simple de las simples aplicaciones desarrolladas y que están disponibles en el Mercado.

Android Experto (2013) refiere que Android se ha convertido en el sistema operativo preferido de usuarios y fabricantes, gracias a su flexibilidad y performance, y por la gran cantidad de aplicaciones que se ofrecen para él en las distintas tiendas de aplicaciones.

La fragmentación del producto (S.O. Android), es decir, su tendencia a ramificarse en muchas versiones y modificaciones diferentes, es una de sus características más relevantes, ya que al existir en el mercado tantos teléfonos inteligentes y tabletas con resoluciones de pantalla, procesadores y características disímiles, desarrollar aplicaciones que se adapten y ejecuten en cada modificación de este S.O. para móviles es una tarea difícil y que rara vez se cumple.

Las versiones de Android reciben en inglés el nombre de diferentes postres En cada versión el postre elegido empieza por una letra distinta, conforme a un orden alfabético: Figura 1.

- Apple Pie: tarta de manzana.
- Banana Bread: pan de plátano.
- Cupcake: panqué.
- Donut: rosquilla.
- Éclair: pastel francés.
- Froyo (abreviatura de «frozen yogurt»): yogur helado.
- Gingerbread: pan de jengibre.
- Honeycomb: panal de miel.
- Ice Cream Sandwich: emparedado de helado.
- Jelly Bean: gominola.
- KitKat: Marca registrada de una tableta de chocolate con leche.

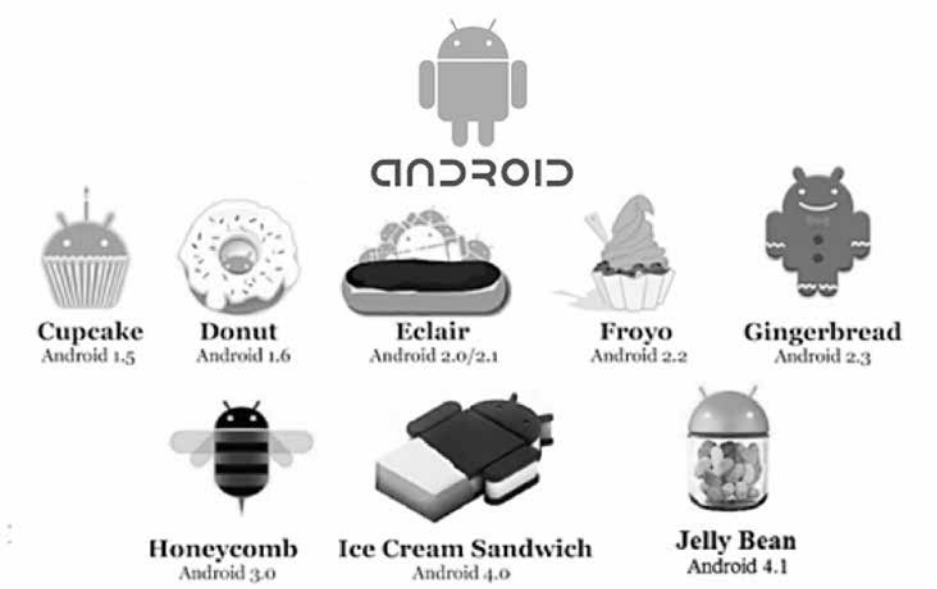

Figura 1. Versiones de Android.
Fuente: Android Experto (2013).

Reflexión

El equipo de investigación de ESET Latinoamérica manifiesta que el sistema operativo Android de Google se convirtió en el más utilizado en los equipos móviles como Smartphone y Tablets del mundo, en este sentido, la tendencia imperante en el mercado que ocupa Android apunta a un uso cada vez mayor de este sistema, lo que permite explicar el aumento y consolidación de diversas vulnerabilidades o amenazas informáticas que afectan a dicha plataforma. Según los datos estadísticos de Statcounter, en el periodo del tercer trimestre del 2014 el S.O. Android fue el más usado en el mundo con el 48.96% del mercado, seguido de iOS 33.58%. Figura 2.

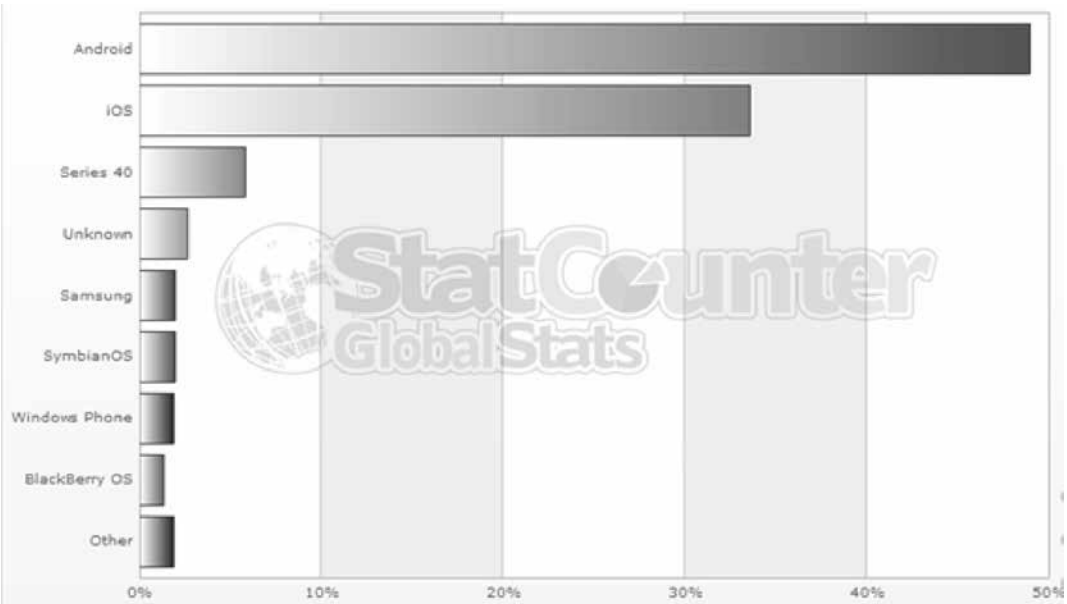

Figura 2. Mercado que ocupa Android en el mundo.
Fuente: Equipo de Investigación de ESET Latinoamérica (2014).

El resultado en Colombia, en el tercer trimestre del 2014, según los datos estadísticos de Statcounter, Android tenía el 62.87% del mercado, seguido de iOS con el 23.09%. Figura 3.

Figura 3. Datos estadísticos de S.O. en Colombia.
Fuente: Equipo de Investigación de ESET Latinoamérica (2014).

Para minimizar los riesgos de seguridad en estos dispositivos móviles, es importante implementar soluciones adecuadas y fortalecer el nivel de seguridad en el uso de estas tecnologías en el acceso físico, en los sistemas operativos, en la configuración y personalización del móvil, en el software y aplicaciones, y en la conectividad. En la investigación (Tendencias 2014: El desafío de la privacidad en Internet, 2014) la empresa de seguridad ESET Latinoamérica consultó a los usuarios acerca de la necesidad de contar con una solución de seguridad en los Smartphone, y 9 de cada 10 usuarios expresó que es importante contar con una solución de seguridad en su teléfono móvil. Sin embargo, más del 80% no protege su información con una herramienta de seguridad; sólo el 20% dijo contar con protección ante los códigos maliciosos o el robo del dispositivo.

El crecimiento de códigos maliciosos para Android continúa aumentando a un ritmo vertiginoso. La primera cifra que permite corroborar este punto tiene relación con la cantidad de detecciones únicas. Si se comparan las detecciones ocurridas en 2012 y 2013, es posible establecer que se incrementaron un 63% en el ámbito mundial. Cabe destacar que en este aspecto se contempló todo el año 2012 y una parte de 2013 (desde el 1 de enero hasta el 22 de octubre). Aun así, el crecimiento es considerable.

Los países que registran el mayor crecimiento en el número de detecciones de malware para Android son Irán, China y Rusia. Por otro lado, si se consideran los cinco países de América Latina que registraron el mayor incremento porcentual de detecciones, comparando 2012 y 2013, se destacan Perú (150%), Ecuador (142%), Bolivia (114%), Paraguay (94%) y México (90%). Figura 4.

Si se comparan las cifras de este año con las expresadas en el documento Tendencias 2013,

Perú y Ecuador continúan liderando este ranking. Debajo quedan Colombia (63%), Chile (17%) y Argentina (20%), dando paso a Bolivia, Paraguay y México. (Equipo de Investigación de ESET Latinoamérica, 2014)

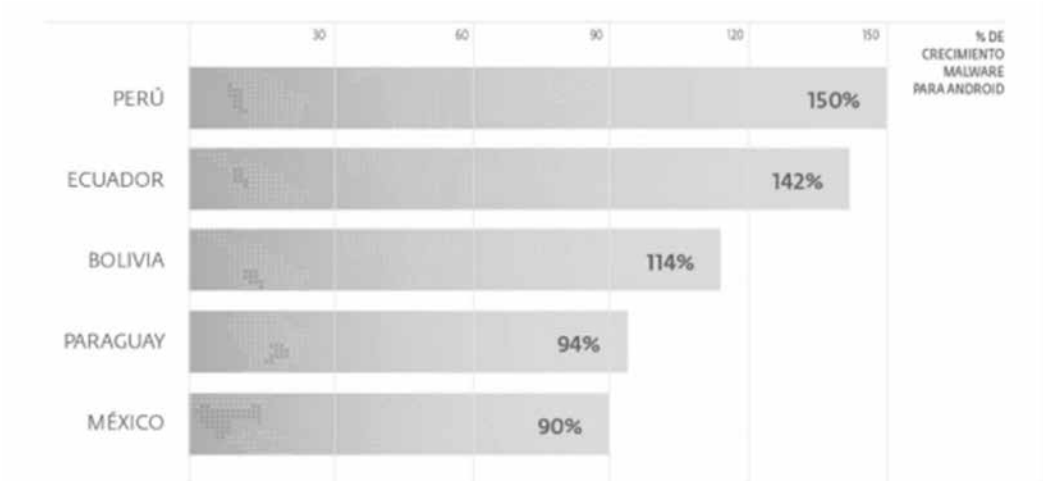

Figura 4. Crecimiento de Malware en A.L.
Fuente: Equipo de Investigación de ESET Latinoamérica (2014).

¿Qué sistema tiene menos virus o apps dañinas?

El 60% del malware móvil ataca a Android. Al ser el sistema más usado es también el blanco favorito de los piratas informáticos. Los virus atacan Android no desde Google Play, que es muy seguro, sino a través de black markets (tiendas piratas). No se conocen virus para iOS y Windows Phone.

Virus como Android Defender, una app falsa que secuestraba móviles, no se han visto ni en iOS ni en Windows Phone por un motivo muy simple: solo Android permite instalar apps fuera de Play Store. Para este último abundan las apps engañosas, programas en apariencia oficiales o legítimos que contienen virus o spam. (Ferri, 2014)

Vulnerabilidades

Los dispositivos móviles se han convertido en una herramienta básica en la vida cotidiana, debido a su popularidad "enfrentan una serie de amenazas que aprovechan las numerosas vulnerabilidades que comúnmente se encuentran en tales dispositivos. Estas vulnerabilidades pueden ser el resultado de controles técnicos inadecuados, pero también puede ser consecuencia de las malas prácticas de seguridad de los consumidores" (Pc Word, 2009).

A continuación se describe varias vulnerabilidades conocidas y que son las más comunes en las plataformas móviles.

Los dispositivos móviles no tienen contraseñas habilitadas.

Muchos de los usuarios, al adquirir estos dispositivos móviles, no registran el acceso con contraseñas para poder salvaguardar los datos almacenados. Muchos dispositivos tienen la capacidad técnica para soportar contraseñas, números de identificación personal (PIN) o patrones de clave en la pantalla para la autenticación. Algunos dispositivos móviles también incluyen un lector biométrico para escanear una huella dactilar como autenticación. (Pc Word, 2009).

Las transmisiones inalámbricas no siempre están encriptadas.

Las redes públicas o gratis de Wi-Fi, no sólo están abiertas a los usuarios, sino también a ataques de piratas informáticos que intentan robar datos confidenciales.

La información generada por un dispositivo móvil no suelen estar cifrada durante su transmisión. Muchas aplicaciones no encriptan los datos que transmiten y reciben a través de la red, lo que facilita que puedan ser interceptados. Por ejemplo, si una aplicación está transmitiendo datos a través de una red WiFi sin encriptar y utilizando HTTP (en lugar de HTTP seguro), los datos pueden ser fácilmente interceptados. Cuando una transmisión inalámbrica no está cifrada, los datos pueden ser interceptados fácilmente. (Pc Word, 2009).

Los dispositivos móviles pueden contener malware.

Malware son programas informáticos maliciosos con el fin de robar información privada (como datos personales o bancarios) o bien instalar programas y correr procesos sin tu consentimiento.

Los usuarios pueden descargar aplicaciones que contienen malware. Los consumidores descargan estos programas sin saberlo, ya que pueden estar disfrazados como un juego, parche de seguridad, utilidad o aplicación. Es difícil que los usuarios noten la diferencia entre una aplicación legítima y una que contenga un software malicioso. Cuando una transmisión inalámbrica no está cifrada, los datos pueden ser fácilmente interceptados por intrusos que pueden obtener acceso no autorizado a información sensible. (Pc Word, 2009).

Los dispositivos móviles a menudo no utilizan software de seguridad.

Al adquirir un dispositivo móvil, las empresas distribuidoras no instalan un software para protegerse de aplicaciones como virus, troyanos, spyware y spam; además los usuarios, por desconocimiento del funcionamiento del móvil, no saben instalar dicho software, por ende no conocen la importancia de tener un aplicativo de seguridad.

Los canales de comunicación pueden estar mal asegurados.

Uno de los problemas más comunes de seguridad es dejar abiertos los canales de comunicación. El Bluetooth, o en el modo 'descubrimiento' (que permite que el dispositivo sea visto por otros dispositivos compatibles con Bluetooth para que se puedan hacer conexiones), podría permitir que un atacante instale malware a través de esa conexión, o active subrepticiamente un micrófono o una cámara para espiar al usuario. (Pc Word, 2009).

Otro problema común es el uso de redes públicas o puntos de Internet inalámbrico Wi-Fi, lo que podría permitir que un atacante se conecte al dispositivo y vea la información sensible.

Descargar nuevas aplicaciones solamente a través de los canales oficiales de los fabricantes.

El software malicioso no es un problema exclusivo de los ordenadores, también afecta a los Smartphone y Tablets, por tanto, necesitan la misma protección que se utiliza en cualquier PC. Al instalar aplicaciones de cualquier otra fuente, como páginas web u otras tiendas de aplicaciones, estamos corriendo el riesgo de instalar aplicaciones maliciosas.

La mayor parte de los virus se "cuelan" en los dispositivos móviles a través de descargas de aplicaciones desde sitios poco fiables.

Para minimizar los riesgos de seguridad en los dispositivos móviles que usan Android, se recomienda usar Play Store -el canal oficial- para descargar aplicaciones. (Gestión, 2014)

El dispositivo móvil y las aplicaciones actualizadas.

Uno de los problemas principales de seguridad en los dispositivos móviles es tener desactualizadas suss apps. Un inconveniente (Cooney, 2012) de los parches de seguridad para las aplicaciones de terceros es que no siempre se desarrollan y se publican en el momento oportuno. Además, las aplicaciones móviles de terceros, incluyendo los navegadores web, no siempre notifican a los consumidores cuando hay actualizaciones disponibles. A diferencia de los navegadores web tradicionales, los navegadores móviles rara vez obtienen actualizaciones. El uso de software obsoleto aumenta el riesgo de que un atacante pueda explotar vulnerabilidades asociadas con estos dispositivos.

Protección ante el robo o la pérdida de un terminal móvil.

Los dispositivos móviles como los Smartphone y las Tablets correen un riesgo diario de robo o extravío; la solución ante estos escenario no es dejar de usarlos, sino salvar la información contenida para que la pérdida del equipo no sea traumática.

Un dispositivo móvil puede contener información muy valiosa: datos de tarjetas de crédito, números de cuentas bancarias, contraseñas, datos de contacto, fotos, videos, correos electrónicos y una larga lista de información privada. Una información muy atractiva para cualquier ciberdelincuente. (Pc Word, 2009).

Los dispositivos móviles a menudo no utilizan firewall de seguridad.

Los dispositivos móviles como los Smartphone y las Tablets corren un riesgo al momento de conectarse a una red WI-FI desconocida, donde automáticamente empieza a descargar o actualizar las apps instalados, dando la posibilidad de que se instale un software malicioso o malintencionado y pueda dañar o robar la información.

Recomendaciones

Los dispositivos móviles como los Smartphone y Tablets se han convertido en unas de las principales entradas a Internet, y por ende, permiten realizar intercambios de información a través de el correo electrónico o perfiles en Twitter, Facebook o Instagram; también facilitan transacciones bancarias y el manejo de agendas de contactos. El dispositivo como tal está expuesto a un robo, entre otras circunstancias, por lo tanto, existe una serie de consejos y buenas prácticas que los usuarios no aplican en el día a día y que pueden ser relevantes ante una posible eventualidad de este tipo y que propicie que la información allí contenida pueda caer en manos de terceros.
La seguridad en este ámbito debe verse como una inversión, pues el tiempo y los recursos dedicados a seguir buenas prácticas de seguridad adquirirán su importancia en el momento en que el dispositivo se ha víctima de robo de la información o del equipo en sí.

Habilitar contraseñas.

Al momento de adquirir un dispositivo móvil tipo tableta o smartphone, es recomendable configurarlo para que solicite una contraseña o clave PIN. Adicional a esto, debe enmascararse dicha clave para que otras personas no puedan visualizarla, con lo cual se impedirán los accesos no autorizados. De igual forma, se recomienda configurar el dispositivo para que bloquee automáticamente el acceso tras un determinado período de tiempo sin interacción alguna. (McAfee, 2012).

Archivos encriptados.

Otra alternativa muy útil es cifrar los archivos relevantes. El cifrado impide que el atacante tenga acceso a la información y a las imágenes de los dispositivos o servicios de copia de seguridad en línea, además, se puede activar la herramienta de doble autenticación: un código enviado a un dispositivo seleccionado o al teléfono inteligente como un

mensaje SMS. Esto impide que un tercero tenga acceso a las cuentas personales; los smartphones intentan conectarse a las redes Wi-Fi cercanas siempre que sea posible (al menos que se configure el equipo para que no lo haga). Para un atacante, todos los datos son valiosos. (Gestión, 2014).

Software de seguridad.

Para prevenir problemas de seguridad, en el mercado existen varias opciones de antivirus y según cada necesidad, las licencias pueden obtenerse en forma gratuita o pagando una suscripción. Algunos de los antivirus más conocidos son kaspersky, mcafee, avg, norton antivirus, eset nod32, Avast!, panda, avira antivirus, entre otros.

Asegurar canal de comunicación.

La solución propuesta para minimizar los posibles ataques mediante los dispositivos de comunicación Bluetooth, consiste en tener desactivado o deshabilitado estos canales cuando no se esté haciendo uso del mismo. También es de gran utilidad contar con una contraseña al momento de activar este servicio. En cuanto a la redes Wi-Fi, se deben utilizar únicamente aquellas que sean de reconocida confianza.

Descarga software de canales oficiales.

Otra medida preventiva muy útil para disminuir los riesgos de seguridad en dispositivos móviles que usan Android Play Store, es acudir siempre al canal oficial para descargar aplicaciones. (Pc Word, 2009). Algunos consejos útiles relacionados son:

- Comprar en tiendas de aplicaciones de confianza. Antes de descargar una aplicación, es mejor informarse sobre ella y sobre su editor. Si se es usuario de Android, hay que evitar instalar aplicaciones no comercializadas desactivando la opción ““Fuentes desconocidas” en el menú de Configuración - Aplicaciones.
- Comprobar los comentarios y las calificaciones de otros usuarios para asegurarse que la aplicación no representa ningún peligro.
- Leer la política de privacidad de la aplicación (si la tiene), con el fin de conocer la información a la que tiene acceso y si va a compartir sus datos con terceros. Por ejemplo, si una aplicación de juegos solicita acceder a su libreta de direcciones, debe preguntarse por qué necesita acceder a esta información. Si tiene la más mínima duda, no descargue la aplicación (McAfee, 2012).

Las aplicaciones actualizadas.

Mantener actualizado, al día, el dispositivo móvil con la última versión disponible del software, baja significativamente las posibilidades de sufrir una vulneración en seguridad.. No hace falta un gran esfuerzo para esto, simplemente dejar marcada la casilla “Actualización automática del software”, en el apartado “Acerca del dispositivo” que podremos encontrar en “Ajustes”. En muchos casos serán necesarias actualizaciones manuales de software, lo que implica una constante gestión en parches de seguridad (Fabriciano, 2014).

Proteger el dispositivo de un robo.

Para prevenir problemas en caso de pérdida o robo del dispositivo, es importante seguir algunas recomendaciones:

- Proteger el dispositivo mediante un PIN, un patrón de desbloqueo o una contraseña. Esto dificultará el acceso a la información y permitirá incluso llevar a cabo algunas acciones antes de que el delincuente acceda a información personal.
- Instalar alguna aplicación de control remoto en los dispositivos. Los principales fabricantes de móviles o grandes empresas como Google disponen de sus propias aplicaciones.
- Realizar copias de seguridad de la información almacenada en el dispositivo para casos de robo o pérdida.

Utilizar un firewall de seguridad.

Otra buena medida es instalar un firewall en el dispositivo móvil; esta aplicación monitorea todas las comunicaciones entrantes y salientes en función de un conjunto de reglas preestablecidas para prevenir las intrusiones no deseadas. (ESET, 2014).

Crear copias de seguridad de datos.

Se trata de una operación relativamente fácil de llevar a cabo, y muchos smartphones y tablets tienen la capacidad de generar copias de seguridad de forma inalámbrica, con el fin de que se pueda restaurar rápidamente esta información en caso de pérdida o eliminación accidental de los datos. Además, si se pierde el dispositivo, también se podrá recuperar la información. (McAfee, 2012).

Evitar "piratear" el dispositivo móvil.

Al "piratear" o modificar de manera informal un dispositivo móvil para eliminar restricciones impuestas por un proveedor, se puede debilitar de manera importante su seguridad al abrir brechas que pueden no detectarse de forma inmediata, dado que se menguan los mecanismos de seguridad originales incorporados en el dispositivo. Igualmente, se hace necesario comprar estos dispositivos en lugares autorizados por las entidades que regulan las telecomunicaciones (McAfee, 2012).

Cierre debido de sesiones en páginas web de banca electrónica y compras online.

- El cierre de sesión debe hacerse en las páginas, en lugar de cerrar el navegador. Si no se hace de esa manera, en caso de pérdida o robo del celular o de la tableta, un delincuente podría reiniciar esa sesión. Nunca se deben utilizar nombres de usuario y contraseñas permanentes en el navegador móvil o en sus aplicaciones, en prevención de lo anteriormente expuesto (McAfee, 2012).
- Se debe evitar la realización de operaciones bancarias y compras online a través de conexiones Wi-Fi públicas. Es mejor reservar dichas transacciones para cuando se esté conectado a una red debidamente protegida. (McAfee, 2012).
- Se recomienda comprobar siempre que el URL del sitio al que se ingresa para esta clase de transacciones es el correcto. Hay que verificar que la dirección web es correcta antes de iniciar una sesión o enviar información confidencial. Lo mejor es descargar la aplicación oficial del banco, para que tener siempre la seguridad de que se accede al sitio web correcto. (McAfee, 2012).

Conclusiones

La tendencia en equipos móviles con S.O. Android apunta a que ésta siga siendo la plataforma más utilizada para dispositivos móviles en el mercado. Su popularidad y difusión han hecho que esta plataforma sufra las más diversas amenazas y vulnerabilidades informáticas, siendo el blanco favorito de los cibercriminales. En este artículo se da un breve repaso a los problemas de seguridad en dispositivos móviles, enumerando los posibles inconvenientes más comunes, sucedidos cuando los usuarios no protegen sus equipos y la información contenida en ellos con herramientas de seguridad. En este texto se describe la importancia de considerar o aplicar buenas prácticas de seguridad que pueden ser decisivas al momento de que el dispositivo sea víctima de un ataque o robo, ya sea del equipo o de la información.

La seguridad informática debe ser considerada como una inversión; se trata de tiempo y esfuerzo bien invertidos, ya que previene riesgos y mitiga los efectos nocivos que acarrea ser víctima de cibercriminales.

Los ciberdelincuentes seguirán castigando a las presas más débiles, es decir, aquellas que no toman una serie de medidas de seguridad básicas que deberían ser de dominio común y que son explicadas en este artículo.

Referencias

Mifsud, E. (2012). Introducción a la seguridad informática - Seguridad de la información/ Seguridad informática. Recuperado de: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1.

Crespo M. A, y Ramos, R. E. (2012). Estudio del impacto financiero de las vulnerabilidades de las páginas Web de los bancos en Ecuador. Tesis obtención de título. Universidad Politécnica Salesiana. Guayaquil.

González, G. (2012). Software de desarrollo para aplicaciones móviles. Veracruz. Universidad Veracruzana. Recuperado de: http://cdigital.uv.mx/bitstream/123456789/32061/1/gonzalezmelgarejogrecia.pdf

Amazing Colombia. (s. f). Seguridad de la Información en Dispositivos Móviles. Recuperado de: http://www.amazing.com.co/blog/seguridad-de-la-informacion-en-dispositivos-moviles/

Sallis. E. & Caracciolo, C. (s.f.). Mobile Device Security, La era Post PC. Recuperado de: http://www.8dot8.org/2011/deck/8dot8_pres_ES_CC.pdf

Frank, D., Lipachoque, A., Huarcayaquilla, E. y Facundo,C.(2014).SistemaOperativoAndroid. Recuperado de: http://www.monografias.co/trabajos101/sistemaoperativoandroid/sistemaoperativoandroid.shtml.

Android Experto. (2013). Todo lo que tienes que saber sobre las versiones de Android. Recuperado de: http://www.androidexperto.com/aprender-android/versiones-android/.

Pc Word. (2009). 10 problemas de seguridad móvil y cómo enfrentarlos. Recuperado de: http://www.pcworld.com.mx/Articulos/25567.htm

Equipo de Investigación de ESET Latinoamérica. (2014). Tendencias 2014: El desafío de la privacidad en Internet. Recuperado de: http://www.esetla.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf, octubre 2014.

Cooney, M. (2012). 10 problemas de seguridad móvil y cómo enfrentarlos. Recuperado de: http://www.computerworldmexico.mx/Articulos/25567.htm.

Ferri, F. (2014) ¿Cuál es más seguro, Android, iOS o Windows Phone?. Recuperado de: http://articulos.softonic.com/comparativa-seguridad-android-ios-windows-phone.

Gestión. (2014). Aprenda a proteger su privacidad en línea en siete pasos. Recuperado de: http://gestion.pe/tendencias/aprenda-proteger-su-privacidad-linea-siete-pasos-2107953.

McAfee. (2012). 10 consejos prácticos para mejorar la seguridad de los dispositivos móviles. Recuperado de: http://images.mcafee.com/es-mx/advicecenter/pdf/MobileeGuide_Jan2012.pdf

Fabriciano. (2014). Tres medidas de seguridad para tu Android que no puedes despreciar. Recuperado de: http://www.batiburrillo.net/tres-medidas-de-seguridad-para-tu-android-que-no-puedes-despreciar/.

ESET. (2014). ESET Mobile Security. Recuperado de: http://www.eset-la.com/hogar/mobile-security-antivirus.

"El conocimiento es poder. La información es libertadora. La educación es la premisa del progreso, en toda sociedad, en toda familia".

Kofi Annan.

Cymbidium / Autor: Diego Alonso Rivera Vergara