PROJECT, DESIGN AND MANAGEMENT

ISSN: 2683-1597

Cómo citar este artículo:

Cassinda Qussanga, F. (2019). Caracterização de sistemas operacionais móveis celulares: Android, Symbian, iphone e Windows phone. *Project, Design and Management, 1*(2), 75-88. doi: 10.29314/pdm.v1i2.200

CARACTERIZAÇÃO DE SISTEMAS OPERACIONAIS MÓVEIS CELULARES: ANDROID, SYMBIAN, IPHONE E WINDOWS PHONE

Fernando Cassinda Quissanga
Escola Superior Aberta do Brasil (Brasil), Universidad Europea del Atlántico (España)
fernandoquissanga@hotmail.com · https://orcid.org/0000-0003-4468-7206

Resumo: O presente tema refere-se à caracterização dos sistemas operacionais móveis celulares: Android, Symbian, *iPhone*, *Windows Phone*. Apresentar qual dos sistemas operacionais móveis celulares, é mais seguro e o mais susceptível aos vírus informáticos, a metodologia de forma qualitativa baseada pelo referencial bibliográfico, os dados coletados em livros, manuais técnicos, informações de fabricantes e em sites da internet; à análise dos dados é documental, feita em tabelas. Entretanto, conclui-se que nem todo tipo de vírus informáticos infectam os telefones celulares, depende do núcleo (kernel) do sistema operacional. Foi possível saber que o Symbian é o sistema operacional mais propenso a contaminação de vírus informáticos, este sistema operacional é feito de uma linguagem de programação C++ proveniente da linguagem C uma das mais populares e possui muitos desenvolvedores. O Android é um sistema operacional para dispositivos móveis, não tão seguro, baseado no núcleo (*kernel*) do *Linux*, sendo um *software* livre permite maior número de desenvolvedores da tecnologia. O *Windows phone* é o menos susceptível a pragas virtuais. E a *Microsoft* investiu bastante no seu sistema de segurança, restringiu o acesso ao *app store* para impedir que o usuário baixe programas fora do mercado, visto que a cada dia são colocados inúmeros aplicativos. A tecnologia *bluetooth* representa maior forma de transmissão de vírus informáticos.

Palavras-chave: Telefone Móvel Celular. Vírus informáticos. Sistemas Operacionais.

CHARACTERIZATION OF CELLULAR MOBILE OPERATING SYSTEMS: ANDROID, SYMBIAN, IPHONE AND WINDOWS PHONE

Abstract: The present theme refers to the characterization of cellular mobile operating systems: Android, Symbian, iPhone, Windows Phone. To present which of the cellular mobile operating systems, is the most secure and the most susceptible to computer viruses, the qualitative methodology based on the bibliographic

reference, data collected in books, technical manuals, manufacturer information and on internet sites; to the analysis of the documentary data, done in tables. However, it is concluded that not all types of computer viruses infect cell phones, it depends on the kernel of the operating system. It was possible to know that Symbian is the operating system most prone to contamination of computer viruses, this operating system is made of a C ++ programming language coming from the C language one of the most popular and has many developers. Android is a mobile operating system, not so secure, based on the kernel of Linux, being free software allows more number of developers of the technology. Windows phone is the least susceptible to virtual pests. And Microsoft has invested heavily in their security system, restricted access to the app store to prevent the user from downloading programs out of the market, since every day are placed numerous applications. Bluetooth technology represents a major form of virus transmission.

Keywords: Cellular Phone, Computer viruses, Operational systems.

CARACTERIZACIÓN DE SISTEMAS OPERACIONALES MÓVILES CELULAR: ANDROID, SYMBIAN, IPHONE Y WINDOWS PHONE

Resumen: El presente tema se refiere a la caracterización de los sistemas operativos móviles móviles: Android, Symbian, iPhone, Windows Phone. En el caso de los sistemas operativos móviles, es más seguro y más susceptible a los virus informáticos, la metodología de forma cualitativa basada en el referencial bibliográfico, los datos recogidos en libros, manuales técnicos, informaciones de fabricante y en sitios de Internet; al análisis de los datos documentales, hecha en tablas. Sin embargo, se concluye que no todo tipo de virus informáticos infectan los teléfonos celulares, depende del núcleo (núcleo) del sistema operativo. Es posible saber que Symbian es el sistema operativo más propenso a la contaminación de los virus informáticos, este sistema operativo está hecho de un lenguaje de programación C ++ proveniente del lenguaje C una de las más populares y posee muchos desarrolladores. Android es un sistema operativo para dispositivos móviles, no tan seguro, basado en el núcleo (Linux) de Linux, siendo un software libre permite mayor número de desarrolladores de la tecnología. Windows Phone es el menos susceptible a las plagas virtuales. Y Microsoft ha invertido bastante en su sistema de seguridad, ha restringido el acceso al app store para impedir que el usuario descargue programas fuera del mercado, ya que cada día se plantean numerosas aplicaciones. La tecnología bluetooth representa una mayor forma de transmisión de virus.

Palabras clave: Teléfono móvil. Virus informáticos. Sistemas operacionales.

Introducción

Se entiende una cantidad considerable de teléfonos móviles, sin embargo, estos dispositivos actualmente permiten la comunicación, mensajes multimedia, transferencias bancarias, consulta de servicios meteorológicos, servicios de ubicación geográfica, sistema de posicionamiento global (GPS) , impresión de documentos, otros servicios de convergencia de tecnología, calculadora, libreta de contactos, galerías, intercambio de datos, internet (*hotspot* portátil) y puede transmitir la señal de internet a 10 o más dispositivos de transferencia de información bluetooth. Tienen memorias, procesadores y un sistema operativo incorporado, lo que permite un mayor flujo, manejo e intercambio de información entre los usuarios. Sin embargo, propaga la inseguridad, sobre todo, la pérdida y el robo de información ha sido la mayor preocupación. Cabe destacar que el cibercrimen ha aumentado, sin embargo, el teléfono móvil se ha vuelto muy vulnerable a los ataques de virus informáticos.

Según Giménez (2011) afirma: “Lo primero que hay que saber es que una solución de seguridad móvil es completamente diferente de una solución de seguridad para desktop

o *notebook*. Por ejemplo, según Symantec, hay más de 286 millones de malware informático, hay alrededor de 1000 para dispositivos móviles [...]". Teniendo en cuenta esta cita, podemos ver que los sistemas operativos móviles son diferentes entre sí en términos de su solidez y vulnerabilidad, sin embargo, los virus de un sistema operativo Android no atacan el iOS de forma inversa, debido a su núcleo (*kernel*), es decir, depende del código fuente y su lenguaje de programación.

Objetivo general: caracterizar cuál de los sistemas operativos celulares móviles es el más seguro y el más susceptible a los virus informáticos.

La investigación es cualitativa basada en la referencia bibliográfica, que permitió evaluar el material de interés de estudio del tema referido como soporte del artículo científico. En las técnicas e instrumentos de investigación se aplicaron un (1) cuestionario y ocho (8) entrevistas. Sin embargo, podemos analizar la definición de Chaer, Diniz y Ribeiro. (1987, p. 15). 260 apud Gil, 1999, p.128): "como la técnica de investigación compuesta de un número mayor o menor de preguntas presentadas por escrito a las personas, con el objetivo de conocer opiniones, creencias, sentimientos, intereses, expectativas, situaciones experiencias, etc." A través de las entrevistas fue posible identificar diferencias entre los sistemas operativos móviles mencionados.

En cuanto a los datos recopilados, es posible observar un número limitado de publicaciones sobre trabajos en virus informáticos en telefonía celular móvil. Sin embargo, la investigación se realizó en libros, manuales técnicos, artículos científicos, información del fabricante y en sitios web. "El análisis documental, como un proceso intrínseco a la Organización de la Información en el campo de la Ciencia de la Información, establece parámetros descriptivos teórico-metodológicos que explican los procedimientos de elaboración analítica que conducen a la identificación de los conceptos del documento". (Nascimento, 2009)

Virus informáticos en teléfonos celulares

Hablar sobre virus en la sociedad actual nos trae a la mente los virus biológicos que se traducen como veneno, toxina o agentes infecciosos. Sin embargo, en este capítulo, mencionaremos sobre los virus informáticos en los teléfonos móviles, que podemos definir como *software* malicioso hecho por lenguaje informático. La programación que infecta el sistema operativo y los hosts en el programa y se replica en otras ubicaciones del sistema, corrompe e impide el inicio normal del funcionamiento del *software* o programa.

> Los *Crackers* (criminosos virtuales) son muy ágiles en el lenguaje de programación, tienen conocimiento de redes de computadoras, telecomunicaciones e ingeniería de software, a veces sin educación. Crean virus para tomar dividendos, monitorean todas las vías posibles, se descomponen contraseñas y detectan fallas de seguridad en diversas áreas, empresas, bancos y otros (Quissanga, 2015, p. 10).

Hay relatos que afirman que algunos virus no se hicieron intencionalmente, sin embargo, para probar el sistema de seguridad como un medio para conocer mejor el comportamiento de los virus, otros para estudiar en laboratorios que permiten una mayor interacción de los estudiantes, otro aspecto que podemos decir que algunos virus fueron creados por programadores aficionados y *hackers* por diversión, sin conocer los riesgos y medir las consecuencias. Estos virus no son tan conocidos, pero han causado muchas dificultades, además de dañar los sistemas operativos. También existen virus específicos para el robo de información, ya que los teléfonos móviles se utilizan para realizar muchas

operaciones, sea bancarias, transferencias de aplicaciones o envíos.,correos electrónicos, mensajes... Es específico para llamar, con internet permite interactuar en redes sociales, grabaciones, es decir, todo lo que llamamos convergencia tecnológica. Sin embargo, esta característica de convergencia tecnológica, sobre todo cuando se conecta a Internet, permite la transmisión de virus informáticos a dispositivos móviles celulares, por lo que debemos proteger el sistema operativo mediante antivirus, *antimalware* y *antispyware*. Según Trif y Vişoiu (2011, p.119) afirman que: "Los nuevos logros en tecnologías móviles han allanado el camino para nuevas aplicaciones diseñadas para ejecutarse en dispositivos móviles. Al principio, los dispositivos móviles ofrecían una funcionalidad muy limitada debido a la poca memoria, la potencia informática y la interacción difícil".

Sin embargo, el robo por teléfono móvil ha sido de manera silenciosa, ya que el usuario no tiene idea de que su dispositivo es vulnerable al delito cibernético, siendo espiado. Sus credenciales son capturadas por delincuentes cibernéticos, sus correos electrónicos son monitoreados, sus datos bancarios están en peligro. Los piratas informáticos tienen muchas motivaciones para crear virus y llevar a cabo cualquier delito cibernético.

Sin embargo, vale la pena mencionar el comportamiento o la motivación que impulsa a los programadores de computadoras a crear virus, aunque la verdadera motivación es destruir los sistemas operativos.

Sin embargo, los virus tienen dos aspectos:

- El programador crea virus para destruir o corromper aplicaciones móviles de teléfonos móviles;
- Enviar mensajes para robar datos del usuario.

> A menudo, el usuario permite que los medios de propagación aumenten sustancialmente debido a la falta de precaución y al poco conocimiento de las formas en que se transmiten los virus, por lo que cualquier fabricante, desarrollador o bufete de abogados debe promover las conferencias, debates, foros y seminarios sobre las causas, formas de propagación, daños y prevención de virus informáticos […] (Quissanga, 2015, p. 10).

Los virus en los teléfonos móviles se originaron en 2004, lo que podemos considerar muy reciente en comparación con los virus informáticos a fines de la década de 1980. Sin embargo, podemos observar a F-Secure Company sobre el informe del descubrimiento del primer virus en la telefonía móvil celular.

Según Martinelli, (2008, p. 94):

> En el año 2004, el primer virus móvil fue descubierto por la compañía de seguridad F-Secure, llamándose Cabir.A. Cabir.A es en realidad un worm que se propaga solo en teléfonos celulares que usan tecnología de transmisión inalámbrica *Bluetooth*, que afecta a dispositivos basados en el sistema operativo Symbian, mejor conocido como la plataforma Series 60.

Pero la plaga no se extiende a todos los dispositivos, por lo que vemos algunas restricciones para tener virus específicos para cada sistema operativo. La tecnología *Bluetooth* es una de las tecnologías de transmisión de red inalámbrica que permite el intercambio de información entre dispositivos, teniendo una característica muy peculiar de efectuar un bajo consumo de energía. El virus Cabir.A se originó a partir de esta tecnología al enviar mensajes infectados al dispositivo móvil. Sin embargo, se considera como la primera forma de propagar el virus en el teléfono móvil. Por lo general, esta

tecnología permite una transferencia de información muy simple de punto a punto. En su mayor parte, los dispositivos móviles han estado desprovistos de cualquier antivirus que evite que los virus informáticos infecten el sistema operativo y, a su vez, lo dañen o roben información, por lo que los teléfonos móviles deben tener protección porque la principal ruta de transmisión del virus en los teléfonos celulares móviles ha sido *bluetooth* e internet.

Describir los posibles tipos de virus informáticos en la telefonía móvil celular.

Después de abordar el origen de los virus, es apropiado mencionar los tipos de virus en los teléfonos móviles.

Sin embargo, los virus informáticos están más extendidos en cómo propagarse y actuar sobre sus presas, además de tener muchos desarrolladores, por lo que hay muchos tipos de virus, que no es el caso con los virus de teléfonos móviles. Su descubrimiento muy reciente, que ha limitado la investigación y el desarrollo, así como la introducción de virus en el mercado y el acceso muy reciente a sus dispositivos que de alguna manera los desarrollaron.

Los virus silenciosos son comunes hoy en día. Los crackers los usan para espiar y eliminar cualquier vulnerabilidad del dispositivo móvil, como imágenes, videos, información comprometedora o confidencial, códigos bancarios para realizar transferencias múltiples. Debemos tener cuidado con la información que ponemos en nuestros dispositivos móviles cuando no tenemos antivirus, *antimalware* y *antispyware*.

Los virus celulares no son tan populares como los virus informáticos, sino también la evolución de varias generaciones de teléfonos móviles. Sin embargo, los teléfonos móviles de la marca Nokia y Siemens que utilizaron el sistema operativo Symbian, como la clasificación del sistema eran tecnología de tarea única, de usuario único, pero rudimentaria en comparación con los dispositivos móviles multitarea y multiusuarios actuales. Sin embargo, no permitieron grandes volúmenes de datos o información, vídeos, imágenes, contactos y SMS, MMS, correos electrónicos, es decir, una convergencia tecnológica, una interfaz gráfica como la presentada por los dispositivos móviles actuales.

Tabla 1. Virus informáticos en teléfonos celulares

N°.	Nombre del virus/*Worm*/Año *(Actualizado)*	Sistemas Operativo
1.	Cabir A (Junio de 2004)	Symbian
2.	Caballo de Troya (marzo de 2017)	Symbian, *Windows*, Android y Mac OS X
3.	CommWarrior (Octubre de 2018)	Symbian y Android
4.	Crossover (Marzo de 2011)	*Windows Mobile*
5.	Doomboot (Julio de 2019)	Symbian
6.	Liberty (Septiembre de 2007)	*Palm* OS
7.	RedBrowser (Septiembre de 2017)	J2ME
8.	FlexiSpy (Junio de 2019)	Symbian y Android
9.	Skuller (Junio de 2004)	Symbian
10.	Gingermaster (Abril de 2011)	Android
11.	Ikee (Noviembre de 2009)	*iPhone* OS (IOS)
12.	DroidKungFu (Junio de 2011)	Android
13.	Zitmo (Abril de 2018)	Symbian, Android, *Windows Mobile* y *Blackberry*
14.	YiSpecter (Abril de 2018)	*iPhone* OS (IOS)

Nota: Fuente: Elaboración propia (2018).

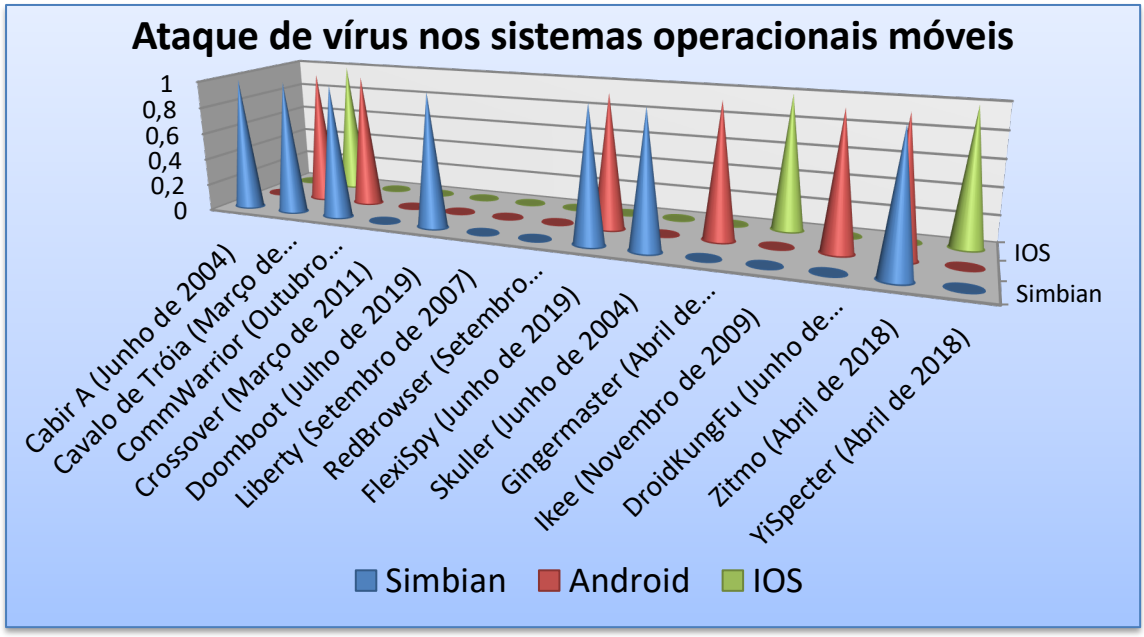

Figura 1. Ataque de virus en sistemas operativos celulares

Nota: Fuente: Elaboración propia (2019).

Según la Figura 1., se puede observar que el sistema operativo Symbian representa el 50% de los 14 virus, ya que tiene 7 tipos de virus que infectan el sistema operativo. En segundo lugar, podemos ver el sistema operativo Android con una representación de 6 virus y, por último, el IOS con 3 variedades de virus.

El sistema operativo Mac OS X está infectado por el caballo de Troya, sin embargo, el Mac no es invencible, observamos que una de las características del caballo de Troya, su capacidad de transmisión de cliente y servidor, a veces puede presentarse oculto en un archivo y cuando el cliente lo ejecuta, el sistema envía instrucciones al servidor.

El caballo de Troya de los virus que infectan los teléfonos móviles, como se muestra en la Tabla 1, es el tipo de virus que ataca la mayor cantidad de sistemas operativos, como su nombre lo indica, y conocemos mejor el comportamiento del caballo, ya que posee una característica de transmisión muy rápida, tiene una capacidad oculta en el sistema, ataca silenciosamente sin darse cuenta, en las descargas son sus favoritos, sin embargo, al descargar un determinado programa se mata, al instalar el *software* confiable también instala el virus y destruye lentamente el sistema de arranque del sistema operativo. Estos virus tienen dos formas de propagación: uno se esconde secretamente en su presa y otro necesita la ayuda de un ciberdelincuente para contaminar a la presa.

Pero la inversión realizada para contener estos virus aún no es satisfactoria; Se necesita invertir mucho más en seguridad de la información. No hay uniformidad en el derecho penal para el cibercrimen o el ciberterrorismo, que aumenta sustancialmente todos los días. Deberíamos tener una ley universal para castigar a los delincuentes o las leyes cercanas porque el crimen puede ser transversal con una computadora remota en Rusia y cometer crimen en Angola, ya que su descubrimiento no es fácil, una vez que debe haber una política universal para poder criminalizar a los ciberdelincuentes. Los crímenes de este tipo involucran mucha tecnología para descubrir al criminal.

Sin embargo, es apropiado abordar los diferentes sistemas operativos, presentar su robustez y su fragilidad y cuál es el más susceptible a las plagas virtuales y cuál presenta mayor seguridad para estas plagas virtuales.

Sistemas operativos móviles

Windows Phone 7

Windows Phone es un sistema operativo móvil evolucionado de *Windows Mobile*. El *MS-Windows Mobile* se distribuye en teléfonos móviles de las principales compañías del mundo; la única excepción es Nokia, que utiliza Symbian en sus teléfonos. Según Tumejormovil (2019): "Los sistemas operativos *Windows Phone*, actualmente *Windows 10 Mobile*, son propiedad de Microsoft y están diseñados para ofrecer el mejor rendimiento posible para *smartphones* y *tablets*. Se cerró al código y su núcleo es *Windows NT*".

Sin embargo, *Windows Phone* es uno de los últimos sistemas operativos móviles diseñados por Microsoft. Construido por un proyecto de gran magnitud desde el punto de vista de la seguridad de la información, los teléfonos de este sistema tienen muchas limitaciones de descargas en el *Marketplace*, lo que no permite incluso ser vulnerable a varias plagas virtuales.

Observamos en el artículo de Sandeep, Chollie y Bandi (2012, p. 1575), que afirman:

> La aplicación de teléfono del *Windows* está diseñada desde cero con seguridad de alta prioridad. *Windows* ha agregado características de seguridad y ha facilitado la creación de seguridad adicional para las aplicaciones de

> *Windows Phone*. El modelo de seguridad de *Windows Phone* es la base para proteger la confidencialidad, integridad y disponibilidad de datos y comunicaciones.

Sin embargo, el sistema operativo *Windows Phone* tiene gráficos muy simples pero su lenguaje de programación no es muy conocido, por lo que evita que los *hackers* desarrollen *softwares* maliciosos para dispositivos móviles.

Figura 2. Teléfono móvil del Sistema Operativo Windows Phone 8.1

Nota: Fuente: Buld (2014).

Según la Tabla 1, se declara que la peste virtual que generalmente ataca a *Windows Mobile* es *Crossover*, un tipo de virus conceptual. El virus elimina el directorio "Mis documentos" y se replica cada vez que se reinicia el teléfono.

Es de considerarse que *Windows Mobile* es vulnerable a ser fácilmente infectado por el muy destructivo virus *Crossover*. Sin embargo, con la plataforma de *Windows Phone* presenta mayor resistencia al virus, según Altermann (2013):

> Los teléfonos con *Windows Phone* son uno de los dispositivos más seguros hasta el momento. Debido a que no ejecutan ningún archivo que no esté vinculado al *Marketplace*, todavía no se han descubierto virus desarrollados por la plataforma. El hecho de que sea un sistema con poca representación de ventas también contribuye al hecho de que no muchas personas están preocupadas por la creación de virus para dicha plataforma. Pero eso no significa que no deba mantener la misma atención que tendría con cualquier otra plataforma.

Sin embargo, se puede decir que *Windows Phone* es más robusto que otros sistemas operativos, como lo señalan Sandeep, Cholli y Bandi (2012, p. 1575) afirman que: "*Windows Phone 7* es un sistema operativo que encadena una gran cantidad de métodos de cifrado que cuentan *AES, SHA1* y *SHAA256*. *Windows Phone 7* tiene el modelo de seguridad, la base para proteger la confidencialidad, integridad, accesibilidad de datos e interacciones".

La criptografía también se llama escritura codificada, lo que le permite escribir mensajes en código y descifrar o cifrar cierta información. Son las mejores formas de autenticación, clave primaria, clave pública, base de datos, datos bancarios, tienen éxito

gracias a las técnicas fundamentales de criptografía. Hoy se sabe que, para una seguridad eficiente, se utiliza la criptografía, ya que permite una mayor seguridad, al variar los diversos códigos de acceso, no permitiendo que los ciberdelincuentes descubran la contraseña. Por ejemplo, las nuestras tarjetas de crédito, contraseñas para proteger las redes de routers, para que haya protección, se utiliza la técnica de cifrado. Según Quissanga (2015, p.14) "*Microsoft* ha invertido mucho en la seguridad de *Windows Phone 7*. Por lo tanto, restringió el acceso a la tienda de aplicaciones para evitar que los usuarios descarguen programas del mercado, ya que muchas aplicaciones se colocan todos los días". Dado este tema, *Windows Phone* está muy a salvo de ataques informáticos. Así como la cantidad de programadores de virus de virus de computadora móvil para este sistema operativo representa menos, como *Microsoft*, otras compañías deberían optar por este sistema de seguridad.

Android 4.3.2

Android es un sistema operativo móvil no tan seguro basado en el kernel de Linux y su código abierto permite que más desarrolladores de tecnología lo hagan muy vulnerable a los ataques informáticos. Según Munhoz (2017) "Un nuevo virus para Android ha surgido ahora y puede ser la perdición para muchas personas, ya que el *software* malicioso se descarga automáticamente, incluidas las aplicaciones y los juegos pagos".

Sin embargo, se puede ver en la Tabla 1, el sistema es infectado por 6 tipos de virus. Según Tumejormovil (2019): "De hecho, según estudios de 2017, el 67.1% de los teléfonos móviles en todo el mundo tienen Android y, específicamente en España, el 90%, por lo que se demuestra que es un buen sistema operativo y que podría ser silenciosamente el mejor en el mercado ". El sistema operativo Android también es vulnerable a los ataques de plagas virtuales, en las estadísticas es posible observar la mayor cantidad de representaciones telefónicas en el mercado, por lo que son susceptibles de robo de *hackers* y *crackers* presentando debilidades. La capacidad del usuario para usar software fuera de la tienda permite que el *software* malicioso infecte el dispositivo móvil celular, la facilidad de transferir programas y aplicaciones, la conexión a Internet sin protección del sistema permite la contaminación del dispositivo móvil celular.

Según Lima, es posible observar (2013):

> Entre los cinco principales sistemas operativos disponibles en el mercado (Android, iOS, *Windows Phone, Blackberry OS*, Symbian), *Windows Phone* 8 puede considerarse uno de los más seguros entre ellos. Si bien Android 1 de cada 10 aplicaciones contiene contenido malicioso, los virus para Windows Phone solo aparecen en rumores".

Sin embargo, Lima dice que todavía se rumorea que los virus informáticos para *Windows Phone* se deben a que el sistema de seguridad no es vulnerable, mientras que Android es susceptible a los ataques cibernéticos, su tienda de aplicaciones contiene muchos programas sospechosos que permiten la contaminación de dispositivos móviles, la tecnología de dispositivos Android existe en las definiciones, aplicaciones y luego encontramos que la opción de habilitar fuentes desconocidas permite la instalación de software o aplicaciones fuera del mercado.

iPhone 3.1.2

El *iPhone* es un dispositivo móvil de *Apple*, lanzado el 29 de junio de 2007, fue uno de los principales eventos en la historia de la telefonía móvil. Miles de personas serían las

primeras en comprar en las tiendas de *Apple* antes de su lanzamiento. Probablemente se vendieron tres millones y medio de *iPhones* en los Estados Unidos de América en los primeros seis meses de su lanzamiento. Según Tumejormovil (2019): "El IOS, anteriormente llamado iPhone OS, es el segundo sistema operativo con más *smartphones* en el mundo. A diferencia de Android, su código está cerrado directamente y está fabricado por el *kernel* operativo de *Apple*, MAC OS, [...]".

También podemos hacer referencia a la seguridad del sistema operativo Mac OS X que está infectado por un caballo de Troya, hoy ya no es realidad que Mac no esté infectado por plagas virtuales, notamos que una de las características del caballo de Troya es su capacidad rápida, que puede presentarse como un cliente y al mismo tiempo como un servidor, a menudo se oculta en un archivo y, a medida que el cliente ejecuta, el sistema envía instrucciones al servidor. Según Power (2018): "El primer worm escrito en C por ikee para *iPhone*. Este worm explota el hecho de que la mayoría de los usuarios de *iPhone*/*iPod touch* con *jailbreak* instalan SSH y también se olvidan de cambiar la contraseña de root/móvil (que es "alpino" por patrón)".

Sin embargo, permite autenticar al usuario sin darse cuenta; el usuario a veces ingresa sus credenciales o contraseña sin saber que las instrucciones no son auténticas, una vez que esta característica del virus lo hace tan peligroso y eficiente.

El sistema operativo de *Apple* no es invencible, también es susceptible a los virus. La rede social *Reddit*, según Souza (2014) "[...] descubrió un nuevo malware llamado Unflod Baby Panda, el virus afecta a todos los dispositivos con jailbreak y es programado para robar ID de *Apple* de dispositivos infectados enviando estas credenciales a sus creadores". Es de destacar que los virus que afectan al iPhone no son bien conocidos, al igual que algunas publicaciones afirman que es menos propenso a los ataques a la tecnología del sistema operativo Android porque es menos representativo en el mercado. En cuanto a la seguridad, tenemos pruebas claras de que Internet es una de las formas más rápidas de transmitir virus informáticos. Hay algunas medidas paliativas para evitar que los virus infecten ciertos dispositivos móviles celulares, pero decir que cierto sistema operativo es inmune a los ataques informáticos, estaríamos equivocados, todos los días surgen nuevos virus informáticos justo cuando se desarrolla la tecnología a medida que evoluciona el cibercrimen. La política era la siguiente: restringir su tienda de aplicaciones para evitar que otras fuentes no autorizadas accedan, evitando la posible transmisión de cualquier *malware*.

Según Lima (2013):

> También sabemos que esta relación virus/sistema operativo es directamente proporcional a su popularidad y al número de usuarios activos. Por lo tanto, cuanto más popular sea *Windows Phone*, más probable es que surjan más virus y *malwares*, pero no necesariamente aumentarán sus vulnerabilidades.

Sin embargo, es imposible decir que estamos totalmente seguros cuando estamos conectados a Internet, es decir, cuanto más pensamos que estamos seguros, nos sorprende una tecnología que puede alterar nuestro sistema de seguridad en 90° o 100°.

Sin embargo, aún se aborda la vulnerabilidad del sistema operativo iPhone como se puede ver según Pandya y Stamp (2010, p. 84):

> Por supuesto, el *iPhone* es un dispositivo vulnerable con múltiples agujeros de seguridad. La filosofía de seguridad del *iPhone* en sí tiene un defecto importante. El enfoque de Apple para hacer del *iPhone* un dispositivo seguro era reducir la "intensidad de ataque del dispositivo" o la "exposición del

> dispositivo a vulnerabilidades". *Apple* solo permitió el acceso de escritura a un área de *sandbox* en el sistema de archivos y la instalación no permitida de aplicaciones de terceros.

Las compañías móviles tienen que invertir mucho en seguridad de la información para que los usuarios de sus dispositivos sean más creíbles, porque hoy en día el teléfono se ha vuelto bastante relevante en nuestra vida cotidiana, depositamos una gran cantidad de información que debe protegerse.

> En caso de que Apple se sienta excluida, en 2015 llegó el primer malware iOS para dispositivos sin *jailbroken*. Básicamente, YiSpecter creó una puerta trasera en dispositivos comprometidos que permitió a los invasores instalar y desinstalar aplicaciones, descargar archivos y mostrar anuncios, entre otras cosas. (Power, 2018).

Apple tiene una filosofía en sus dispositivos móviles que impide la transferencia de información a través de *bluetooth*, lo que podemos decir que esta medida impidió un poco la transmisión de virus informáticos a otros dispositivos, la transmisión a través de *bluetooth* es la más grande de todas las otras formas estudiadas.

Sin embargo, cuando comenzamos a diseñar o desarrollar un prototipo, un dispositivo móvil, siempre pensamos cómo será desde el punto de seguridad, y nunca imaginamos que esta tecnología o sistema podría resistir varios ataques cibernéticos, como *Apple*, sorprendentemente los *hackers* ya estaban preparados para ennegrecer el sistema de seguridad y llevar la inseguridad a los consumidores.

Symbian^3

Las empresas que utilizan este sistema son: Nokia, Sony Ericsson, Panasonic, Siemens y Samsung. Symbian es muy susceptible a un ataque de virus, considerado el más popular y destructivo de la historia, el famoso caballo de Troya, al igual al *worm* originó la plaga virtual cabir.A, el primer virus móvil. Según Martinelli, (2008, p. 88) afirma: “Cabir fue escrito en el lenguaje C ++, originalmente para infectar los sistemas móviles basados en la serie Symbian 60. El virus utilizó exclusivamente la tecnología Bluetooth para propagarse entre los teléfonos celulares". El lenguaje de programación C es el más popular, dice Olhar Digital(2013), “El lenguaje C continuo como el más utilizado en el mundo según un nuevo informe de Tiobe Software. Al conquistar el 18.15% de los programadores, C extendió su ventaja sobre Java, una opción del 16.5% de los profesionales ". El lenguaje C ++ integra la mayor parte, permitiendo que más desarrolladores creen virus informáticos para infectar el sistema operativo Symbian. Sin embargo, si hay más desarrolladores, también es posible tener más creadores amadores de lenguajes informáticas, de lo contrario, porque hay una gran representación de teléfonos en el mercado, que también se traducen en más presas virtuales. En la actualidad, este sistema operativo está en baja expresión, ya que el mercado internacional es el más buscado por los dos grandes gigantes de la tecnología móvil, *Apple* y Samsung, que representan los sistemas operativos iOS y Android. Siendo entre ellos los más seguros.

Resultados y Discusión

Los sistemas operativos tienen sus propios gráficos, su estructura está diseñada de acuerdo con su desarrollador sin desalentar ningún estándar universal, cada sistema tiene

su propio prototipo, y estas características pueden hacerlos fuertes o débiles a los ataques informáticos, por ejemplo, el sistema operativo. Symbin presenta una característica similar, ya que de acuerdo con el análisis encontrado, podemos observar que los sistemas se crean con un lenguaje de programación muy conocido y más fácil de desarrollar, estos sistemas permitieron una mayor programación de virus informáticos en el mercado. La facilidad de instalación de *software* o aplicaciones fuera de la tienda de dispositivos móviles, que principalmente transporta virus informáticos, causa una vulnerabilidad y daña los sistemas de arranque del dispositivo.

Sin embargo, a diferencia del sistema operativo *Windows Phone*, tiene una realidad diferente, son sistemas con una estructura robusta, tiene una protección que no permite que las instalaciones fuera de la tienda instalen *softwares* maliciosos, sin embargo, esta característica lo hace muy seguro porque no permite la transmisión de virus fácilmente, de lo contrario no permite a los desarrolladores programar virus debido a la ignorancia de su lenguaje de programación ya que la contaminación solo ocurre cuando es el mismo código fuente o núcleo (*kernel)*. El sistema operativo *Windows Phone 7* hace un uso intensivo de los métodos de protección criptográfica del sistema. Esta característica evita numerosos ataques informáticos en el sistema operativo.

Los virus del sistema operativo no son tan conocidos, pero no podemos afirmar que no son atacados, sino que también son vulnerables al virus Ikee. El IPhone no es tan vulnerable como los sistemas operativos Symbian y Android. Sin embargo, mencionar que el sistema operativo *iPhone* de *Apple* tiene una característica que evita que los programas o algunos dispositivos afecten el sistema, porque se sabe que en los teléfonos móviles la tecnología *bluetooth* es la forma más rápida de transmitir virus informáticos y *Apple* ha restringido la transferencia de aplicaciones de esta tecnología a otros dispositivos. Su lenguaje de programación no tiene muchos desarrolladores. Estas características lo hacen menos susceptible a las plagas informáticas.

Conclusión

Al aprender más sobre los sistemas operativos móviles, se puede concluir que: las infecciones de virus informáticos en los teléfonos celulares móviles tienen que ver con el sistema operativo, su núcleo (*kernel)*, la tecnología del teléfono y el lenguaje de programación. declara Martinelli (2008, p. 32) “Cada sistema operativo tiene un núcleo llamado de *kernel* que delimita sus funciones. Es una de las razones por las que un virus de teléfono celular no se propaga fácilmente a otros dispositivos debido a las diferentes versiones y estructura interna de los diversos sistemas operativos móviles".

Se sabe que Symbian es el sistema operativo más propenso a la contaminación por virus informáticos, ya que este sistema operativo está hecho de un lenguaje de programación C ++ que proviene del lenguaje C, uno de los más populares y que tiene muchos desarrolladores.

Android es un sistema operativo móvil no tan seguro basado en el *kernel* de Linux, y el código abierto permite un número más grande de desarrolladores de la tecnología.

Finalmente concluimos que entre los sistemas operativos de teléfonos móviles como Android, *iPhone*, Symbian y *Windows Phone,* este último es el más seguro desde el punto de vista de seguridad de ataque virtual porque se sabe que *Microsoft* ha invertido muchísimo en su sistema de seguridad, restringiendo el acceso a la tienda de aplicaciones para evitar que los usuarios descarguen programas del mercado, ya que cada día se colocan muchas aplicaciones maliciosas y no solo.

Referencias

Altermann, D. (2013). Como remover vírus do celular: Como remover vírus do Windows Phone? *Tech tudo.* Retrieved from http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2012/08/como-remover-virus-do-celular.html.

Buld (2014). *Microsoft Officially Intros Windows Phone 8.1, Details Cortana.* Retrieved from https://news.softpedia.com/news/BUILD-2014-Microsoft-Intros-Windows-Phone-8-1-Details-Cortana-435504.shtml.

Chaer, G. Diniz, R. R. P. Ribeiro, E. A. (2011). A técnica do questionário na pesquisa educacional: O questionário em questões de cunho empírico. Evidência, Araxá, v. 7, n. 7, p. 251-266, Retrieved from http://www.educadores.diaadia.pr.gov.br/arquivos/File/maio2013/sociologia_artigos/pesqusia_social.pdf.

Gimenez, R. (2011). *5 Antivírus para celular e por que você precisa deles.* Retrieved from https://danresa.wordpress.com/page/14/?app-download=nokia.

Lima, A. (2013). *A segurança da informação no seu Windows Phone 8, Windows Phone Brasil.* Retrieved from http://windowsphonebrasil.com.br/a-seguranca-da-informacao-no-seu-windows-phone-8/.

Lima, A. (2013). *A segurança da informação no seu Windows Phone 8, Windows Phone Brasil.* Retrieved from http://windowsphonebrasil.com.br/a-seguranca-da-informacao-no-seu-windows-phone-8/.

Martinelli, H. (2008). *Vírus de celular: Estudo e classificação para um protótipo de defesa: Telefonia celular e vírus*. Porto Alegre: Uniritter.Retrieved from : http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k8/TCC%202%20final(Horst).pdf.

Martinelli, H. (2008). *Vírus de celular: Estudo e classificação para um protótipo de defesa: ANEXO B: Código do vírus Cabir.* Porto Alegre: Uniritter, Retrieved from http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k8/TCC%202%20final(Horst).pdf.

Munhoz, V. (2017) *Skyfin: o malware de Android capaz downloads e compras ilegalmente.* Tecmundo. Retrieved from. https://www.tecmundo.com.br/malware/113680-skyfin-malware-android-capaz-fazer-downloads-compras-ilegalmente.htm.

Nascimento, L. M. B. do. (2009) Análise documental e análise diplomática: perspectivas de interlocução de procedimentos. Resumo. Retrieved from: http://marilia.unesp.br/Home/PosGraduacao/CienciadaInformacao/Dissertacoes/nascimento_lmb_do_mar.pdf.

Olhar Digital. (2013). *C se mantém como a linguagem de programação mais popular***.** Retrieved from https://olhardigital.com.br/pro/noticia/c-se-mantem-como-a-linguagem-de-programacao-mais-popular/38882.

Pandya, V. R. & Mark, S. (2010). *iPhone Security Analysis: Security Analysis. Journal of Information Security*. Retrieved from: https://file.scirp.org/pdf/JIS20100200003_25782595.pdf.

Power. J. P. (2018). Maliciosamente móvel: uma breve história do malware móvel: Ikee. Retrieved from. https://medium.com/threat-intel/mobile-malware-infosec-history-70f3fcaa61c8.

Power. J. P. (2018). Maliciosamente móvel: uma breve história do malware móvel: YiSpecter. Retrieved from. https://medium.com/threat-intel/mobile-malware-infosec-history-70f3fcaa61c8.

Quissanga, F. C. (2015). Caracterização de vírus informáticos em telefonia móvel celular: Os Crackers .(Trabalho de conclusão do curso) Escola Superior Aberta do Brasil -ESAB - Vitoria: Espírito Santo-Brasil. Retrieved from https://campusonline.esab.edu.br/campusonline/modulos/campus/index.cfm.

Quissanga, F. C. (2015). Caracterização de vírus informáticos em telefonia móvel celular: Propagação e infeção. (Trabalho de conclusão do curso) Escola Superior Aberta do Brasil -ESAB - Vitoria - Espírito Santo. Retrieved from https://campusonline.esab.edu.br/campusonline/modulos/campus/index.cfm.

Quissanga, F, C. (2015). Caracterização de vírus informáticos em telefonia móvel celular: Windows Phone 7. Escola Superior Aberta do Brasil - Vitoria - Espírito Santo. Retrieved from https://campusonline.esab.edu.br/campusonline/modulos/campus/index.cfm.

Sandeep, B. V, Cholli, N. G, & Bandi, S. (2012). Securing Applications in Windows Phone: Introduction. *International Journal of Electronics and Computer Science Engineering-IJECSE, 1*(3), 1574. doi: 10.1.1.259.7340&rep=rep1&type=pdf.

Sandeep, B. V; Cholli, N. G; & Bandi, S. (2012). Securing Applications in Windows Phone: Windows Phone security. *International Journal of Electronics and Computer Science Engineering-IJECSE, 1*(3) 1575. doi: 10.1.1.259.7340&rep=rep1&type=pdf.

Souza, R. de. (2014) *Novo malware para iOS é descoberto por usuário do Reddit: Batizado como UnflodBaby Panda, vírus é de origem chinesa e afeta qualquer dispositivo que tenha sofrido processo de jailbreak.* Tecmundo. Retrieved from http://www.tecmundo.com.br/ios/53792-novo-malware-para-ios-e-descoberto-por-usuario-do-reddit.htm.

Tumejormovil (2019). Comparação Dos Sistemas Operacionais Móveis Mais Utilizados (Android, IOS, Windows Phone): Sistema operacional Android. Retrieved from: https://tumejormovil.com/sistemas-operativos/.

Tumejormovil (2019). Comparação Dos Sistemas Operacionais Móveis Mais Utilizados (Android, IOS, Windows Phone): Sistema operacional IOS. Retrieved from: https://tumejormovil.com/sistemas-operativos/.

Tumejormovil (2019). Comparação Dos Sistemas Operacionais Móveis Mais Utilizados (Android, IOS, Windows Phone): Sistema operacional Windows Phone. Retrieved from: https://tumejormovil.com/sistemas-operativos/.

Trif, S., & Vişoiu, A. (2011). Business Intelligence Mobile applications**.** *Informatica Economică*, *15*(2), 119. Retrieved from http://revistaie.ase.ro/content/58/11%20-%20Trif,%20Visoiu.pdf.

Fecha de envío: 18/03/2019
Fecha de revisión: 18/11/2019
Fecha de aceptación: 02/12/2019