ANÁLISIS DE RIESGO DE SEGURIDAD EN LOS DISPOSITIVOS MÓVILES PERSONALES CON SISTEMA OPERATIVO ANDROID

OSCAR ENRIQUE MENA ASPRILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDÓ-CHOCÓ
2021

ANÁLISIS DE RIESG DE SEGURIDAD EN LOS DISPOSITIVOS MÓVILES PERSONALES CON SISTEMA OPERATIVO ANDROID

OSCAR ENRIQUE MENA ASPRILLA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

YENNY STELLA NUÑEZ ALVAREZ
Asesora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDÓ-CHOCÓ
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico éste trabajo a mi hijo, que con su carisma y comprensión me acompañó en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones de madre, también lo dedico a mi mamá que con su apoyo, consagración y paciencia disminuyo mis tareas en el hogar permitiéndome una entrega más tranquila en el estudio y trabajo.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

pág.

GLOSARIO

ANDROID: Es el sistema operativo que utilizan algunos dispositivos móviles para poder funcionar.

APLICACIONES: Es una herramienta informática diseñada para realizar operaciones o funciones específicas en un dispositivo tecnológico.

ARQUITECTURA: Es la estructura, o la forma como están estructurados y relacionados el hardware, software, redes y datos.

LINUX: Sistema operativo de código abierto para computadoras, servidores, mainframes, dispositivos móviles y dispositivos embebidos.

OWAP: Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro**.**

SISTEMA OPERATIVO: Son una seria de programas o software que dirige todos los servicios o aplicaciones que se utilizan en un dispositivo tecnológico.

VERSIÓN: Es un número o nombre que se asigna a un programa informático para mencionar su nivel de desarrollo y su actualización.

VULNERABILIDAD: Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma

RESUMEN

El objetivo de la presente monografía es realizar un análisis de seguridad informática a los dispositivos móviles con sistema operativo Android, permitiendo describir los pasos y las metodologías que se deben llevar a cabo para realizar dicho análisis. También se busca identificar y conocer los principales riesgos a los que se exponen los mencionados dispositivos, teniendo en cuenta que estos por su alta tecnología se ven expuestos a ataques cibernéticos y a muchas vulnerabilidades.

Esto genera mucha preocupación a los usuarios que, si bien se ven atraídos por las funcionalidades que estos tienen, no son conscientes de los ataques y vulnerabilidades a los que se expone la información contenida en dichos dispositivos, debido a que no todos tienen conocimientos en sistemas.

Se realiza un recorrido corto por la historia de los dispositivos móviles para después exponer el concepto de seguridad de la información a nivel de celulares y por último se citan algunas normas internacionales que permiten adaptar políticas de seguridad de la información en dispositivos móviles.

Palabras Claves: Dispositivos, seguridad, vulnerabilidades, Android, sistema operativo, escaneo.

ABSTRACT

The objective of this monograph is to carry out an analysis of computer security for mobile devices with Android operating system, specify the steps and methodologies that must be carried out to carry out said analysis. It also seeks to identify the main risks to which mobile devices with an Android operating system are exposed, taking into account that these are affected by cyberattacks and many vulnerabilities due to their high technology.

This generates a lot of concern to users that if they are well attracted by the functionalities they have, they are not problems with the attacks and vulnerabilities to which the information contained in said devices are exposed, because not everyone has knowledge of systems.

A short tour of the history of mobile devices is made after exposing the concept of information security on mobile devices, and finally, some international standards that allow adapting information security policies on mobile devices are cited.

Keywords: Devices, security, vulnerabilities, Android, operating system, scan.

INTRODUCCIÓN

Los dispositivos móviles tipo Smartphone se han vuelto indispensables para las tareas diarias de las personas, hasta el límite que un usuario tiende a tener varios dispositivos, siempre los llevan consigo para todos lados, ya que poseen características y funcionalidades que los hacen valiosos, debido a esto se encuentran expuestos a riesgos, amenazas y vulnerabilidades que permiten el acceso indebido de los ciberdelincuentes a todas sus aplicaciones, quienes se aprovechan de los datos personales de los usuarios para acceder a su privacidad, robar cuentas bancarias y llenarlos de malware.

Lo que se busca con esta monografía es realizar un análisis de la seguridad de estos dispositivos móviles con sistema operativo Android, se trataran temáticas como su arquitectura, las evoluciones de mejoras implementadas a través del tiempo, las vulnerabilidades a que se ven expuestos, del mismo modo dar a conocer algunas recomendaciones y la guía de buenas prácticas que se pueden llevar a cabo para disminuir o evitar dichos riesgos, y los diferentes ataques a los que se encuentran expuestos estos dispositivos móviles.

En sus inicios la seguridad de la plataforma Andriod, estuvo muy expuesto siendo uno de los sistemas menos seguros, a través del tiempo Google ha estado desarrollando actualizaciones de seguridad con base a las amenazas existentes, logrando convertirlo actualmente en unos de los sistemas operativos más usados en dispositivos móviles, aunque aún se encuentran vulnerabilidades y fallos. Entre las vulnerabilidades reportadas por la CVE, las afectaciones o ataques que han sufrido estos dispositivos podemos encontrar el Framework y el Kernel, se efectúan mediante la ejecución de código remoto, elevación de privilegios, mediante las cuales se pueden dar el acceso no autorizado y la divulgación de información, además de diversas vulnerabilidades críticas en los componentes de código cerrado de Qualcomm.

En la escala de versiones del sistema Android, estos han evolucionado según los hallazgos y necesidades de los usuarios mejorando su interfaz de software (imagen, sonido, usabilidad, adaptabilidad etc.) además de la conectividad, permitiendo de forma eficiente integración entre los dispositivo y las personas.

La mayoría de las exposiciones que se encuentran en los dispositivos móviles con sistema Android, son ocasionadas por las aplicaciones libres que son instaladas y sobre todo las de fuentes no seguras, que son descargadas por fuera de la Play Store de Google, es indispensable que los usuarios tengan una claridad de la explosión información sensible que generan al instalar aplicaciones, como accesos a navegadores, galería, mensajes, llamadas, ubicación etc. Ya que la mayoría de las aplicaciones cuando se instalan solicitan una seria de permisos y entre ellos se

encuentran los antes mencionados y es donde se ven expuestos y vulnerables a cualquier tipo de ataque informático o de uso no autorizado. Es por ello que esta monografía encontraras una serie de herramientas, métodos que ayudaran a realizar un analisis de seguridad a tus dispositivos si en algún momento imagina si se encuentra vulnerable.

Los dispositivos móviles con sistema operativo Android, han evolucionado en cuanto al uso entre los usuarios, por el número de dispositivos móviles que tienen a Android como sistema operativo, la demanda que generan en el entorno, usabilidad y adaptabilidad, pero se debe tener en cuenta que una falla en dicho sistema afectaría a un gran número de usuarios de distintas formas, como la información privilegiada almacena, por ello es un sistema que es blanco de ataques todo el tiempo por los cibercriminales afectando también la plataforma digital Google Play, por la cual los usuarios descargan aplicaciones falsas reposadas en este directorio.[1]

[1] ROMANO, Agustín y LUNA, Carlos. Descripción y análisis del modelo de seguridad de Android. [En línea]. UR. FI – INCO, 2013. Reportes Técnicos 13-08. [Consultado: 14 de abril de 2022 [Fecha consulta: 21 de abril 2022].]. Disponible en: https://www.colibri.udelar.edu.uy/jspui/handle/20.500.12008/3475

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los dispositivos móviles tipo Smartphone en la actualidad son usados por casi el 100% de la población mundial, ya que con el tiempo han desarrollado nuevas funcionalidades como juegos, correo electrónico, redes sociales, mensajería instantánea, video llamadas, almacenar datos, entre otras, estos tienen sistemas operativos que también han evolucionado con el tiempo como lo son android, iOS, Windows Phone o BlackBerry OS etc.[2]

Los sistemas operativos Android en los cuales se centra esta monografía, iniciaron a desarrollarse por Andy Rubin, Rich Miner, Chris White y Nick Sears en el año 2003, después fueron comprados por Google en 2005, con el fin de desarrollar su propio sistema operativo móvil, en la actualidad Google se ha mantenido activo con estos sistemas operativos ya que se actualiza con frecuencia y ha establecido relaciones con muchos fabricantes de dispositivos.

El sistema operativo Andriod durante el transcurso de los avances tecnológicos ha estado presentado diversos ataques, en el informe de amenazas móviles de F-Secure para el primer trimestre del año 2014, fueron creadas 277 nuevas familias y variantes de malware, de las cuales 275 fueron dirigidas a la plataforma de Google, se denota que más del 99% de estas amenazas iban dirigidas a usuarios con sistemas Android[3].

En el informe presentado por Jose Pagliery, de CCN en español para el año 2016 los dispositivos Andoid fueron afectados por aplicaciones ilegales, debido al ataque que sufrió Google afectando numerosos servicios y posteriormente prologándose a los dispositivos móviles, este malware también instaló un software de publicidad engañosa que rastrea a los usuarios, los hackers pudieron robar los autenticadores digitales (tokens) y así lograr el acceso a los servicios de Google [4]

Según los investigadores de Check Point**,** en el año 2017 ha mediado del mes de mayo, con la aparición del **virus Judy**, siendo posiblemente el ataque más grande

[2] SHRAİM, Khitam y CROMPTON, Helen. “Perceptions of Using Smart Mobile Devices in Higher Education Teaching: A Case Study from Palestine". Contemporary Educational Technology 6. 2015. P. 301-318

[3] BESTYGAME. Android es el objetivo de ataques masivos. [en línea]. [consultado: 8 de diciembre de 2021]. Disponible en: https://bestygame.com/es/android-es-el-objetivo-de-ataques-masivos/

[4] PAGLIERY, Jose. Greenwich. 1, Diciembre 2016. Más de un millón de celulares Android fueron infectados por hackers. [en linea]. [Consultado: 8 de diciembre de 2021]. Disponible en: https://cnnespanol.cnn.com/2016/12/01/mas-de-un-millon-de-celulares-android-fueron-infectados-por-hackers/

sufrido por este sistema operativo, afectando de forma masiva un promedio de 8,5 y 36 millones de Smartphones y Tablet, el malware utiliza dispositivos infectados para generar grandes cantidades de clics fraudulentos en anuncios, este fue desarrollado por unos hackers coreanos extendiendo una cantidad 41 aplicaciones de juegos en Google Play alcanzando 4,5 millones y 18,5 millones de descargas[5].

Con la masiva utilización de los dispositivos móviles y auge de crecimiento de la cobertura móvil e utilización de los servicios de comunicación son más propensos a diversos ataques, por ellos es importante realizar un análisis de los riesgos a los que estos se encuentran y las medidas de correctivas que deben tener los usuarios que utilizan estos dispositivos móviles.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son los principales riesgos de vulnerabilidad a que se ven expuestos los dispositivos móviles con sistemas operativos Android y como se pueden evitar o corregir estos riesgos?

[5] CHEKPOINT. Judy Malware: posiblemente la campaña de malware más grande encontrada en Google Play. [En línea]. [Consultado: 8 de diciembre de 2021]. Disponible en: https://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/

2 JUSTIFICACIÓN

Los dispositivos móviles tipo Smartphone en la actualidad son muy utilizados por la mayoría de las personas, posee características similares a la de un sistema operativo, por lo cual son vulnerables a los virus o a los ataques al mismo sistema operativo tal como sucede con un computador normal, estos permiten guardar y manejar todo tipo de información desde cualquier sitio donde se encuentre, permitiendo el manejo de cuentas bancarias, transacciones en línea, soporte de correos electrónicos, GPS que son servicios de geolocalización, pantalla táctil, mensajes de texto, números de contactos, fotos, documentos etc.[6] Estos a su vez permiten llamada de voz, utilizan conexiones wifi para navegar por internet, bluetooth para transferir información, , tienen tecnologías 3G-4G por medio de las cuales pueden navegar en la red a una alta velocidad y además, conectarse por wifi a través del plan de datos de su operador de telefonía celular, pueden instalar muchas aplicaciones de acuerdo a sus gustos y necesidades, así como una serie de distintos beneficios, lo que los usuarios de este tipo de dispositivos móviles desconocen es que la información y los datos privados que guardan en ellos están expuestos a muchos riesgos y vulnerabilidades, estos no tienen conocimiento de los ataques de los que pueden ser víctimas sus dispositivos móviles, como malware, troyanos, gusanos, programas de dudosa proveniencia etc. Por medio de los cuales los ciberdelincuentes pueden atacar la disponibilidad e integridad de la información, servicios y recursos que se encuentran almacenados en estos dispositivos y obteniendo muchos beneficios económicos productos del ataque.[7] [8]

Los usuarios ignoran que se pueden llevar a cabo medidas de seguridad para proteger su dispositivo móvil y así aminorar el impacto de los ataques que dejan grandes consecuencias este y en la integridad, seguridad y privacidad de la persona, ya que la información que se maneja en estos dispositivos está disponible, por esta razón se hace muy importante conocer los riesgos a que están expuestos los dispositivos móviles tipo Smartphone.

De acuerdo con el informe del periódico el tiempo en 2017, “el sistema operativo más utilizado en dispositivos móviles es el Android, ya que el 37,93 por ciento de los usuarios navega desde un dispositivo móvil con Android, que es propiedad de

[6] APONTE GOMEZ, Sanly y DAVILA RAMIREZ, Carlos. Sistemas operativos móviles: funcionalidades, efectividad y aplicaciones útiles en Colombia. [En línea]. Universidad EAN, 2011. [Consultado: 12 de abril de 2022]. Disponible en: https://repository.ean.edu.co/bitstream/handle/10882/761/AponteSanly2011.pdf?sequence=1

[7] BETANCUR JARAMILLO, Oscar y ERASO HANRRYR, Sonia Elizabeth. Seguridad en dispositivos móviles Android. [en línea] Trabajo de grado. Universidad Nacional a Distancia, 2015. [consultado: 28 de noviembre de 2020]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/3614/59836994.pdf?sequence=1&isAllowed=y

[8] BAZ ALONSO, Arturo et al. Dispositivos móviles. [En línea]. EPSIG Ing. Telecomunicación Universidad de Oviedo, 2011, vol. 12. [Consultado: 7 de diciembre de 2021]. Disponible en: http://isa.uniovi.es/docencia/SIGC/pdf/telefonia_movil.pdf

Google”[9], lo que lo convierte en el más utilizado del mundo y también lo vuelve más atractivo para los ciberdelincuentes, esto se ve reflejado en el artículo publicado por Christian Collado, quien dice que “Android fue el sistema operativo más vulnerable de todo el año pasado, superando a plataformas como Windows 10, Ubuntu o Debían, ya que durante todo el 2019 tuvo 414 brechas o fallos de seguridad”[10]

Este último informe muestra cómo han aumentado gradualmente los riesgos y amenazas que tienen los dispositivos móviles con sistema operativo Android, de la misma manera las vulnerabilidades a las que están expuestas las aplicaciones que se descargan en estos sistemas operativos.

Debido a lo anterior en esta monografía se busca formular y analizar los riesgos de seguridad y las vulnerabilidades a los que se ven expuestos estos dispositivos, lo que permitirá que las personas que los utilizan conozcan acerca de estos ataques y vulnerabilidades que pueden sufrir sus celulares y también para que los desarrolladores fomenten y orienten acerca de las buenas prácticas que pueden tener para salvaguardar la información contenida en estos dispositivos Android.

[9] Redacción Tecnosfera el TIEMPO. Bogotá D.C. 03, abril 2017. Android destrona a Windows como el sistema operativo más usado en red. [en línea]. [consultado: 23 de septiembre de 2019]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/android-destrona-a-windows-como-el-sistema-operativo-mas-usado-en-red-74448

[10] COLLADO, Christian. Andro4all. Android fue el sistema operativo más vulnerable de 2019 duplicando a otros como Windows 7 o Ubuntu. [en línea]. [consultado: 30 de noviembre de 2019]. Disponible en: https://andro4all.com/noticias/android/android-sistema-operativo-mas-vulnerable-2019

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar los riesgos de seguridad en los dispositivos móviles personales con sistema operativo Android a partir de su arquitectura de seguridad y la guía de pruebas de seguridad móvil de Owasp.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los ataques y vulnerabilidades que pueden exponer los dispositivos móviles desde la arquitectura de funcionamiento y operatividad de Android.

- Examinar las diferentes metodologías y estándares relacionados con el escaneo, análisis de vulnerabilidades y detección de fallos aplicados a dispositivos móviles con sistema operativo Android.

- Establecer las fases de la metodología para el análisis de vulnerabilidades y detección de fallos de Android a través de los procesos, técnicas y herramientas utilizadas para las pruebas de seguridad de aplicaciones móviles basada en Owasp.

- Crear una guía de buenas prácticas que se puedan implementar para evitar riesgos de seguridad en los dispositivos móviles con sistema operativo Android.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Los dispositivos móviles fueron evolucionando de tal forma que sus funcionalidades fueron mejorando, desapareció el teclado normal siendo reemplazado por el táctil, las cámaras fueron evolucionando y con ello aparece la grabación de pequeños videos, pero la evolución más grande fue el diseño de sistemas operativos con los que se posibilita descargar aplicaciones, aumentar y mejorar las funcionalidades de estos, los sistemas operativos más comunes son Windows phone, iOS, symbian, BlackBerry, Android entre otros, este último ha cobrado una gran importancia en los últimos años, el cual en la actualidad tiene más usuarios en todo el mundo en sus diferentes versiones.

Los sistemas operativos de Android, desde su aparición hasta la actualidad han tenido varias versiones; la primera, fue la versión de prueba que de acuerdo con la página electrónica Uxxermag, fue bautizado con el nombre Android 0.5 Milestone, con interfaz para terminales de pantallas pequeñas solamente, adaptadas a apps como Google Maps, y algunas herramientas básicas del teléfono. Con el pasar del tiempo fueron saliendo nuevas versiones con mejores funcionalidades y ventajas, la última versión de Android conocida es la número 12 que fue lanzada en el transcurso de los meses de agosto y septiembre de 2021.

4.2 MARCO CONCEPTUAL

Estos dispositivos con sistema Android por sus diferentes funcionalidades y por la información que guardan deben contar con un sistema de seguridad eficiente que permita resguardar la información. Se entiende por seguridad al conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información integradas con la aplicación de políticas de seguridad basadas en el estándar ISO 17799 | 22 en un sistema informático para intentar reducir las amenazas que puedan afectar al mismo.

Se pueden identificar cuatro principios claves de seguridad de la información, los cuales son:

- La confidencialidad es la propiedad que asegura que solo los que están autorizados tendrán acceso a la información. Esta propiedad también se conoce como privacidad.

- La integridad consiste en que el sistema no debe modificar ni corromper la información que almacene o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información.

- La autenticación es la propiedad que hace referencia a la identificación. Es el punto de unión entre la información y su emisor.

- El no repudio es la propiedad que asegura que ninguna parte pueda negar ningún compromiso o acción realizados anteriormente.

Se debe llevar a cabo un trabajo bien estructurado y organizado para cumplir con los principios de seguridad informática, lo cual permite determinar políticas que forman parte del cumplimiento de los objetivos, para lo cual se han creado distintas normas que establecen estándares que regulan la seguridad en la información.

Dentro de esas normas tenemos la ISO/IEC/17799 (ISO 17799 - Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información), que brinda algunas recomendaciones para gestionar de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

Otra norma que podemos citar es la Norma ISO 27001, la cual ofrece un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). Igualmente se encuentra (ISO, 2006), esta norma es certificable mientras y caso de poca seguridad y economía, se tiene la ISO 17799 que no es una norma certificable. Para el presente proyecto se ha tomado como referente principal la norma ISO 17799, teniendo en cuenta que los objetivos de control y los controles enumerados en la norma ISO 27001 se han obtenido directamente de los ISO/IEC 17799 y están alineados con ellos En este análisis se busca empalmar estas normas con el uso y aplicación de políticas que permitan controlar los dispositivos móviles para resguardar la información de las organizaciones empresariales donde se utilizan los dispositivos móviles personales para su manejo.

4.3 MARCO HISTÓRICO

Haciendo un recorrido por la historia de estas nuevas tecnologías, se puede evidenciar que, con la aparición del internet en el mundo, fueron apareciendo las nuevas tecnologías de comunicación y con ellos los dispositivos móviles, que se han vuelto uno de los mejores inventos de la actualidad, se puede encontrar que el primer dispositivo móvil desarrollado fue el invento de Newton, el cual fue comercializado por Apple, se vendió durante los años 1993 y 1998. En su tiempo fue un dispositivo revolucionario porque implementaba un sistema de reconocimiento de escritura y que podía sincronizarse con un ordenador de sobremesa (de Apple, claro está).

Seguidamente, pero antes del dispositivo de Newton existieron distintos dispositivos portátiles como fueron las calculadoras programables, que tenían capacidades gráficas, funcionales desde 1984, con una pantalla de una sola línea, con 32 caracteres de 5x7 puntos, teclado QWERTY y teclado numérico, 4 KB de RAM. Ya para el año 2000, apareció la PocketPC que tenía como sistema operativo el Windows CE 3.0, que sigue vigente hasta la actualidad, debido a que tiene una forma muy sencilla de manejo.

Actualmente, los PocketPC y las Palm tienen pantallas de resolución VGA, en prácticamente todos los casos incorporan protocolos de comunicaciones inalámbricos, como Bluetooth o Wifi, o unidades de GPS. No se podría dejar a un lado el teléfono móvil que marco la revolución de la tecnología, la primera generación 1G de dispositivos móviles, los celulares en el año de 1977 en Chicago, los que iniciaron a funcionar bien en 1978, que llego a tener un aproximado de 300 clientes. Luego, en Japón en 1979 se creó una red de celulares lanzada por NIT, que cubría toda el área de Tokio, tenía 23 estaciones base a las que se comunicaban, con el tiempo esta red se expandió convirtiéndose en la primera red 1G nacional. La señal de estos dispositivos se basaba en sistemas de transmisión FM, permitiendo llevar la voz, aunque todo el sistema de control fuera digital. Este no tenía seguridad y su velocidad era muy baja y poco precisa. Desde ese entonces los dispositivos celulares se convirtieron en una demanda mundial y han ido evolucionando y avanzando, incluyéndoles nuevas funciones y características, una de estas considerada como una revolución para la época, la comunicación por medio de llamadas de voz, como un entorno de comunicación distante, novedoso y además practico.

Por otro lado, en 1980 la compañía Psion fue creada lanzando diferentes teléfonos celulares como el Psion Organiser o el Psion Series 5mx, en 1998 se unieron las compañías Psion, Nokia, Ericsson y Motorola para crear Symbian Ltd. (Una empresa dedicada a desarrollo de Software). Ésta empresa creo el Symbian OS (Un sistema operativo diseñado especialmente para operar en dispositivos móviles).

La segunda generación 2G de los teléfonos celulares marca el paso de la telefonía análoga a la telefonía digital, permitiendo la mejora del manejo de las llamadas, mediante la introducción de una serie de protocolos, se integraron otros servicios adicionales al de voz, como lo fue la creación de los SMS (Short Message Service). En 1992 se envió el primer SMS por Brit Neil Papworth, el cual se envió desde una computadora hasta un orbitel 901 Handset. Pero solo hasta 1999 se pudo enviar mensajes de texto entre diferentes redes y operadores. Luego se fueron incorporando nuevas mejoras tecnológicas a los teléfonos móviles a lo que se le llamo la generación 2.5G, ya que utilizaban el GPRS y EDGE en redes 2G con tasas de transferencias de datos superiores a los teléfonos 2G, pero inferiores a la 3G.

Igualmente, Con la aparición de la generación 3G se busca aumentar la capacidad de transmisión de datos para ofrecer un mejor servicio como la conexión a internet desde el teléfono celular, apareciendo nuevas funcionalidades idénticas a las de televisión, descarga de archivos y video conferencias. En este caso, el sistema operativo Android Inc. fue fundado en 2003 por Andy Rubín, Rich Miner, Nick Sears y Chris White con el objetivo de desarrollar dispositivos móviles que están al corriente de la ubicación y preferencias del usuario.

De lo anterior, en el año 2005 el sistema operativo Android es comprado por el buscador Google, pero solo hasta el 2007 hicieron el anuncio oficial del sistema operativo Android, entre las principales ventajas se encuentra la notificación desplegable, en la que se puede tener toda la información en tiempo real y a la vista, la integración con el correo de Gmail y lo mejor fue su propia tienda de aplicaciones Android que en la actualidad se conoce como Google Play.

4.4 ANTECEDENTES O ESTADO ACTUAL

En la actualidad se cuenta con la generación 4G que ofrece al usuario de telefonía celular un ancho mayor de banda que permite la recepción de televisión de alta definición, descarga de aplicaciones en tiempo real, video llamadas, video conferencias y una serie de funciones que no se alcanzan a explorar, la velocidad con que se trabaja permite realizar tareas en menos tiempo.

Desde el 2007 hasta la actualidad, han salido varias actualizaciones de los sistemas operativos Android, mejorando siempre la anterior, haciéndolo cada vez más atractivo para los consumidores. También han surgido otros dispositivos móviles como las tablets que cumplen la misma funcionalidad del teléfono celular, con la diferencia que no incluyen la función de teléfono, su pantalla es más grande y tiene una muy buena calidad de imagen.

Sin embargo, en la actualidad los smartphone o teléfonos inteligentes con sistemas operativos Android cuentan con muchas características importantes, como permitir la instalación de programas y aplicaciones, tienen una cámara con numerosos megapíxeles, con cámara delantera y trasera para realizar selfie, cuentan con GPS, soporte de correo electrónico, redes sociales, permiten la instalación de programas de terceros, tienen pantalla táctil, agenda digital, acceso a datos de internet a través de la 4G y la red wifi, en fin, un sinnúmero de funcionalidades, que permiten considerar este dispositivo como un miniordenador de bolsillo.

4.5 MARCO LEGAL

Revisando el marco legal acerca de la seguridad de los dispositivos móviles y de la información que allí se guarda se encontró lo siguiente: Constitución Política de

Colombia Artículo 15. Reconoce como el derecho a la intimidad personal, familiar y el Habeas Data en el que su artículo 20 expresa lo siguiente:

Se garantiza la libertad de expresión y de Información Ley 527 de 1999. “Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”

Ley 1266 de 2008. “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países”

Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

5 ATAQUES Y VULNERABILIDADES DISPOSITIVOS MÓVILES

5.1 Arquitectura del sistema

La arquitectura de funcionamiento de los dispositivos móviles está compuesta por diferentes módulos o capas, el sistema se basa en el sistemas Linux heredando varios elementos de seguridad como la protección basada en sandboxing en la cual cada aplicación tiende a ejecutarse por separado mediante un identificador único (UID), "se aísla la aplicación de otras aplicaciones para asegurarse de que sólo puede acceder a sus propios recursos previstos. Por ejemplo, la aplicación A no puede leer los archivos que pertenecen a la aplicación B y viceversa. Una aplicación Android puede hacer uso de varios recursos del sistema. Sin embargo, la mayoría de ellos están prohibidos sin el permiso adecuado"[11].

Las aplicaciones de Andriod tienen una distribución en formato APK, las cuales están compuestas por un formato de empatado que integra lo necesario de una aplicación "recursos, imágenes, manifiesto, XML etc." La clase de java compilado en un formato de bytecode que se conoce como DEX el cual es independiente de la arquitectura del procesador, el uso de estos dispositivos cada vez para las organizaciones va en aumento, donde las organizaciones van implementado políticas para el uso y acceso a las redes corporativas con tecnología personal.

Sin embargo, el aumento en el uso viene acompañado de una explosión de malware móvil (código malicioso diseñado para atacar smartphones y tablets). Según el estudio realizado por los investigadores de la universidad de **Cambridge** averiguaron que el 87% de los smartphones Android están expuestos a al menos una vulnerabilidad crítica. Por otra parte, el estudio realizado por **Zimperium Labs** a principios de este año, confirma que el 95% de los dispositivos Android se pueden piratear mediante la aplicación de un simple mensaje de texto.[12]

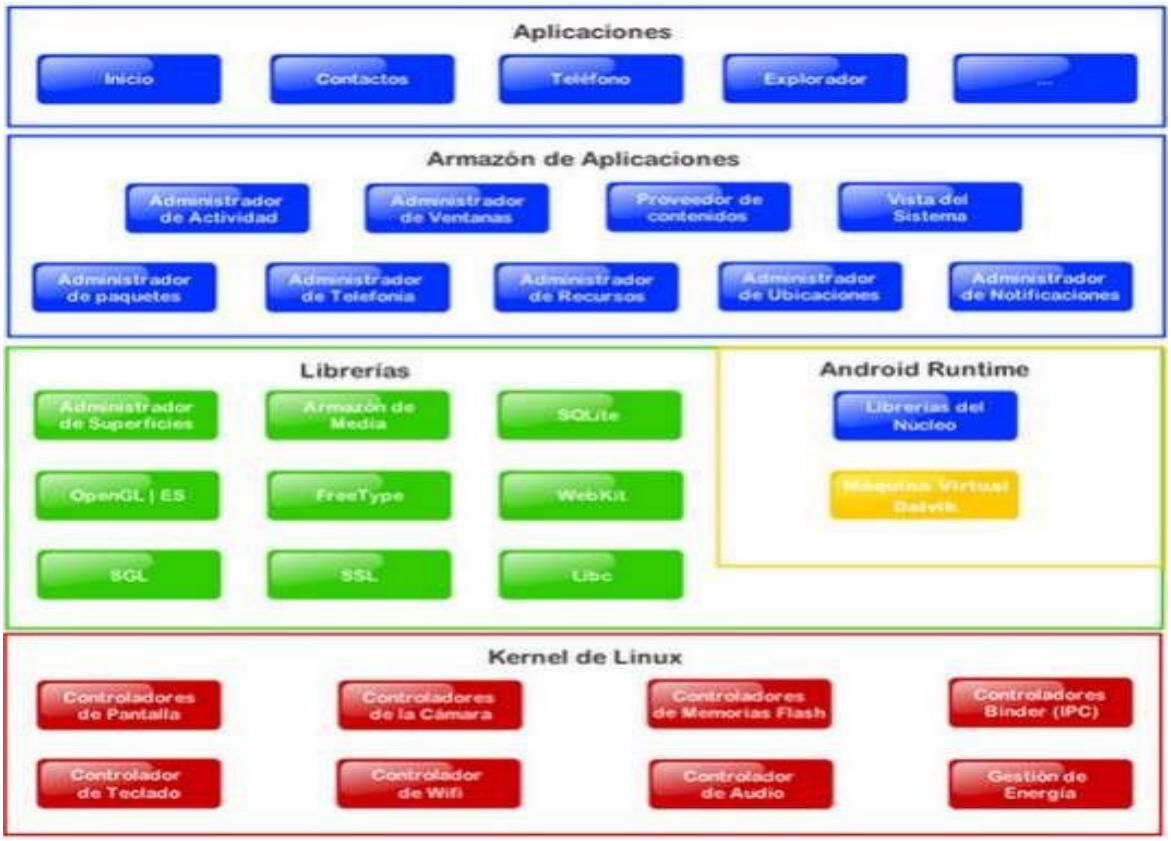
Es fundamental que tengan instalados antivirus, antimalware etc. Ya que también son susceptibles, la mayor amenaza con la que cuentas los dispositivos con sistemas operativo Android es la instalación de aplicaciones maliciosas, las cuales pueden dañar el dispositivo y lograr hacer algo no autorizado con los datos

[11] VELIZ, Pacheco. *et al*. Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones. [en línea]. Trabajo de grado Licenciatura en Sistemas. Universidad nacional de la plata. Facultad de informática. p.139. La plata, 2016. [en línea]. [consultado: 24 de noviembre de 2019] Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/58591/Documento_completo.%20y%20Piazza%20Orlando,%20C.%20Estudio%20y%20an%C3%A1lisis%20de%20seguridad%20en%20dispositivos%20m%C3%B3viles.pdf-PDFA.pdf?sequence=4&isAllowed=y

[12] KASPERSKY. [sitio web]. Kapersky.es. Amenazas a la seguridad móvil para Android. [En línea]. [Consultado 17 de septiembre 2020]. Disponible en: https://www.kaspersky.es/resource-center/threats/mobile

almacenados en el mismo, entre los diversos malware más utilizados por los hackers, a los cuales se encuentran expuestos los dispositivos móviles se encuentran ingeniería social, phishing y otros.

Figura 1: Arquitectura Android



Fuente: Universidad Carlos III de Madrid. Programación en dispositivos móviles portables. Arquitectura Android. [En línea]. [Consultado 10 de abril de 2022]. Disponible en: https://sites.google.com/site/swcuc3m/home/android/generalidades/2-2-arquitectura-deandroid

5.2 Versiones del Sistema Android

La plataforma Andriod inicio en desde los años 2005, cuando Google se hizo con sus derechos al adquirirlo, su primer versión salió para el año 2008, de la cual se acordó con los fabricantes de los Smartphone, y de esto surgió el primer dispositivo móvil para este sistema.

A continuación se describen las versiones del sistema Android.

Cuadro 1. Versiones Del Sistema Android.

Versión & Nombre	Fecha	Característica
1.0 Apple Pie	Septiembre de 2008	En esta de tipo comercial, la cual fue para dispositivos HTC Dream, contando con especificaciones como pantalla táctil, funcionalidad de navegabilidad y conectividad.
1.5 Cupcake	Abril de 2009	En esta versión del sistema conto con características notables como la del teclado virtual y mejoras de la interfaz.
1.6 Donut	Septiembre de 2009	Se añadieron mejoras a la hora de realizar búsqueda rápida en cuanto a su contenido, como la información interna, contactos, mensajes y demás aplicaciones mejorando notablemente su rendimiento.
2.0 Eclair	Octubre de 2009	En esta versión del sistema para el año 2010 en una actualización logro un exitoso avance con el Nexus One, ya que dio inicio a la serie de teléfonos de google. Además de incorporarse Google Maps.
2.2 Froyo	Mayo de 2010	Se logró la ampliación de los paneles de inicio, cambiando de 3 a 5, asimismo los accesos directos, aplicándose avances en la resolución de videos y capacidad de memoria. Además se añadió un logro importante en cuanto a la seguridad disponiendo las opciones de establecer contraseñas y/o pin en la pantalla desbloqueo en los teléfonos.
2.3 Gingerbread	Diciembre de 2010	Para esta versión Google se apoyó en Samsung logrando el lanzamiento con el dispositivo Nexus S. siendo muy llamativa por la forma curva de su pantalla, se mejoró también el rendimiento de la batería, y el panel de notificación agregando alertas de las aplicaciones que más consumían recursos.
3.0 Honeycomb	Febrero de 2011	Versión exclusivamente para Tablets, siendo diseñada para dispositivos con pantallas de gran tamaño, logrando cambiar la interfaz su primer dispositivo fue el Motorola Xoom.

4.0 Ice Cream Sandwich	Octubre de 2011	Esta versión tanto para Tablet y Smartphones, a través del Samsung Galaxy Nexus se realizó el lanzamiento. Se incorporaron mejoras en cuanto al bloqueo de pantalla como el desbloque facial y el analisis de flujo de datos, permitiendo saber que aplicaciones consumen más datos.
4.1 Jelly Bean	Julio de 2012	Se logró mejorar la funcionalidad y la interfaz de usuario, la Tablet Nexus fue el primer dispositivo en utilizar esta actualización.
4.3 Jelly Bean (Michel)	Julio de 2013	En esta versión se logró el lanzamiento de la segunda generación de los Nexus 5, contando con características se destacadas como la conectividad 4G LTE y avance en la seguridad.
4.4 KitKat	Noviembre de 2013	Se lanzó con los dispositivos Nexus de google y LG, trjajo consigo la implementación de impresión vía inalámbrica - WIFI, y mejoras en el rendimiento del sistema.
5.0 Lollipop	Noviembre de 2014	Implemento nuevas características principalmente en el diseño, con la gama de colores e imágenes de ayuda de borde a borde, además destacándose la iluminación, las sombras de tipo realista, siendo más fácil y amigable el uso de los dispositivos.
6.0 Marshmallow	Octubre de 2015	Con esta actualización se introducen ciertas funcionalidades que consolidan a Android como un sistema sólido, principiante la función la cual permite que al cambiar de dispositivo o restaurarlo de fábrica conserva las aplicaciones y datos descargados anteriormente.
7.0 Nougat	Agosto de 2016	Versión que fue lanzada con los dispositivos Nexus 6, 5X, 6P, Nexus Player, Pixel C y Android One, además se mejoró la usabilidad de la batería, tanto el sistema como aplicaciones son más alígeras.
8.0 Oreo	Agosto de 2017	En cuanto a la versión anterior esta adelantó la mejora en cuanto las notificaciones, implementándose texto inteligente auto relleno del texto.
9.0 Pie	Agosto de 2018	Posee sistema de navegación por deslizamiento, función de batería adaptativa, que da prioridad a la aplicación que se usan con más frecuencia.

10 Android Q	Marzo de 2019	Se mejoró la seguridad y privacidad en cuento a la gestión de los usuarios, permitiendo un control en los permisos sobre las aplicaciones, como el de ubicación o el acceso al portapapeles del sistema.
11.0 Developer	Febrero de 2020	Se aplicó avances para los desarrolladores, mediante la cual pueden optimizar las aplicaciones, y aplicando evolución por ejemplo el 5G, móviles plegables, las pantallas curvas. También se enfatizó en: las personas, el control y la privacidad, aplicando un menú de apagado totalmente renovado, el cual hospeda controles de los dispositivos digitales que hacen son parte de nuestro hogar.
12.0	18 de febrero de 2021	Es la versión actual, se implementaron mejoras en la privacidad, seguridad y estabilidad de la cámara, nuevas APIs para desarrolladores, del mismo modo se aplicó el rediseño prácticamente de casi toda la totalidad de la interfaz de usuario del sistema, con un nuevo lenguaje visual, Material You, el cual otorga un control al usuario en cuanto la apariencia de la interfaz.

Fuente: MANRIQUE LOZADA, Cristhian Jose. Análisis de la seguridad de smartphone con sistema android. [En línea]. Trabajo de grado. Universidad Nacional a Distancia, 2019. [Consultado: 16 de abril de 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/

5.3 Vulnerabilidades en Sistemas Operativos Android

Después de una exhaustiva búsqueda se logró establecer que los principales riesgos y vulnerabilidades a que están expuestos los móviles con sistema operativo Android.

- Framework (CVE-2019-1986, CVE-2019-1987, CVE-2019-1988): Vulnerabilidades que permite a los atacantes ejecutar código remoto de manera privilegiada a través de una imagen manipulada con formato PNG. Librerías (CVE-2017-17760): Ejecución remota de código en calidad de proceso no privilegiado por medio de un archivo malicioso.

- Kernel (CVE-2018-10879, CVE-2019-1999, CVE-2019-2000, CVE-2019-2001): “Ejecución remota de código que permite a una aplicación maliciosa ejecutar código en calidad de proceso privilegiado (EoP)”[13].

[13] SOFISTY CIBERSECURITY

- Bootloader (CVE-2020-0069): “Mediante la cual permite conseguir privilegios de sistema sin necesidad de desbloquear el gestor de arranque del dispositivo, la falencia se halla en el módulo que se encarga de la gestión de los comandos del procesador y permitiendo sobre escribir algunos procesos del kernel elevando privilegios. Además, desactiva el módulo ‘SELinux’, encargado de proporcionar mecanismos de seguridad al núcleo del sistema”.[14]

- (CVE-2020-0032): En las versiones 8, 8.1, 9 y 10 de Android permite la ejecución de código arbitrario.

- (CVE-2020-0033 - CVE-2020-0034): Vulnerabilidades consideradas de alta prioridad, ya que permiten la elevación de privilegios y revelan información sensible.

- Múltiples vulnerabilidades en Framework que podrían permitir el aumento de privilegios (CVE-2020-0074, CVE-2020-0388, CVE-2020-0391, CVE-2020-0401)

  - Múltiples vulnerabilidades en Framework que podrían permitir la divulgación de información (CVE -2020-0382, CVE-2020-0389, CVE-2020-0390, CVE-2020-0395, CVE-2020-0397, CVE-2020-0399)

  - Una vulnerabilidad en Media Framework que podría permitir el aumento de privilegios (CVE -2020-0392)

  - Varias vulnerabilidades en Media Framework que podrían permitir la divulgación de información (CVE-2020-0245, CVE-2020-0381, CVE-2020-0383, CVE-2020-0384, CVE-2020-0385, CVE- 2020-0393)

- Varias vulnerabilidades en el sistema que podrían permitir el aumento de privilegios (CVE-2020-0386, CVE-2020-0394)

  - Una vulnerabilidad en el sistema que podría permitir la ejecución remota de código (CVE-2020-0380)

  - Múltiples vulnerabilidades en el sistema que podrían permitir la divulgación de información (CVE-2020-0396, CVE-2020-0379)

  - Múltiples vulnerabilidades en el kernel que podrían permitir el aumento de privilegios (CVE-2020-0402, CVE-2020-0404)

[14] SALIDO, Francisco. Android soluciona varias vulnerabilidades críticas Una al Día. [En línea]. [Consultado: 20 de octubre de 2021]. Disponible en: https://unaaldia.hispasec.com/2020/03/android-soluciona-varias-vulnerabilidades-criticas.html

- Una vulnerabilidad en el kernel que podría permitir la divulgación de información (CVE-2020-0407)

- Varias vulnerabilidades en las actualizaciones del sistema Google Play que afectan a los componentes de Project Mainline (CVE-2020-0245, CVE-2020-0383)

- Varias vulnerabilidades de alta gravedad en los componentes de MediaTek que afectan al controlador de sonido de Android TV, mdla y ATF (CVE-2020-0123, CVE-2020-0229, CVE-2020-0278, CVE-2020-0342)

- Varias vulnerabilidades de alta gravedad en los componentes del kernel de Qualcomm (CVE-2019-10527, CVE-2019-14117, CVE-2020-3613, CVE-2020-3656, CVE-2020-11124)

- Varias vulnerabilidades de gravedad crítica en Qualcomm de código cerrado componentes (CVE-2019-10628, CVE-2019-10629, CVE-2019-13994, CVE-2020-3621, CVE-2020-3634)

- Varias vulnerabilidades de alta gravedad en los componentes de código cerrado de Qualcomm (CVE-2019-10596, CVE-2019-13992, CVE-2019-13995, CVE-2019-14074, CVE-2020-3617, CVE-2020-3620, CVE-2020-3622, CVE-2020-3629, CVE-2020-3671, CVE- 2020-11129, CVE-2020-11133, CVE-2020-11135)[15]

Con el avanece tecnológico se ha observado a través del tiempo como se ha vulnerado la seguridad de los dispositivos móviles, es sumamente importante que los usuarios tengan claro los diferentes métodos o técnicas que emplean o utilizan los ciber-delincuentes para sabotear o robar la información confidencial que se almacenan en estos dispositivos.

5.4 Ataques A Dispositivos Con Sistemas Operativos Andriod

A continuación, se muestran los ataques que más han afectado estos dispositivos desde la aparición de los sistemas operativos Android.

Malware bancario: Acorde con la revista digital Dark Reading, “el malware móvil basado en la banca ha aumentado progresivamente, porque los ciberdelincuentes buscan comprometer a los usuarios que prefieren llevar a cabo todos sus negocios desde sus dispositivos móviles”[16]. Para este tipo de infiltraciones en los dispositivos

[15] DOXNET. Multiple Vulnerabilities Discovered in Google Android OS. [en línea]. [Consultado 22 de octubre de 2021]. Disponible en: https://www.doxnet.com/article.cfm?ArticleNumber=62
[16] DARKREADING

móviles, los más utilizados son los troyanos ya que estos son los que se implementan para recoger información sobre inicios de sesión y contraseñas bancarias, que después se envían a un servidor que controla la información.

Malware LOAPI: Fue publicado por Kapersky, denominado Loapi (potencialmente vinculado a otro malware denominado Podec), malware móvil que implementa una compleja arquitectura modular para llevar a cabo múltiples actividades ilícitas, el cual contiene unos módulos de minando para las criptomonedas y realiza la distribución de anuncio, ejecuta ataques DDos, generación de tráfico web, subscripción del usuario víctima a servicios de pago, etc.[17]

Ransomware móvil: Este bloquea los datos importantes del usuario, como documentos, fotos y vídeos por medio de cifrado de la información, después extorsionan al dueño del dispositivo para que le pague rescate al creador del malware, de no hacerlo a tiempo, eliminan todos los archivos o se bloquean para que el usuario no pueda acceder más a ellos. International Data Group (IDG), "reveló que el 74 % de las empresas informaron de una brecha de seguridad en 2015, con el ransomware como una de las amenazas más frecuentes".

Spyware móvil: Este supervisa la actividad y registra la ubicación, luego roba información crítica, como las contraseñas de correos electrónicos y de los sitios de compras electrónicas. El spyware pasa desapercibido en el sistema, solo se muestra cuando el rendimiento del dispositivo disminuye o hasta que se realice un análisis antimalware en el celular con sistema operativo Android.

Troyanos de SMS: Los ciberdelincuentes aprovechan los troyanos de SMS para sembrar el caos financiero mediante el envío de mensajes SMS a números con tarificación especial de todo el mundo, lo que aumenta las facturas telefónicas de los usuarios. En 2015, algunos usuarios de Android se infectaron con un troyano bancario que podía interceptar los mensajes de texto que incluían información financiera y, a continuación, enviaba una copia del mensaje de texto a través del correo electrónico, lo que proporcionaba a los cibercriminales toda la información que necesitaban para infiltrarse en las cuentas financieras.

Gusanos: Malware que es considerado entre los más peligrosos, tiende a que una vez se encuentra instalado o alojado en el dispositivo, este se reproduce afectando todos los archivos, estos suelen aparecer por correo electrónico, en las aplicaciones no oficiales, sitio web sin certificación y por mensajes de texto.

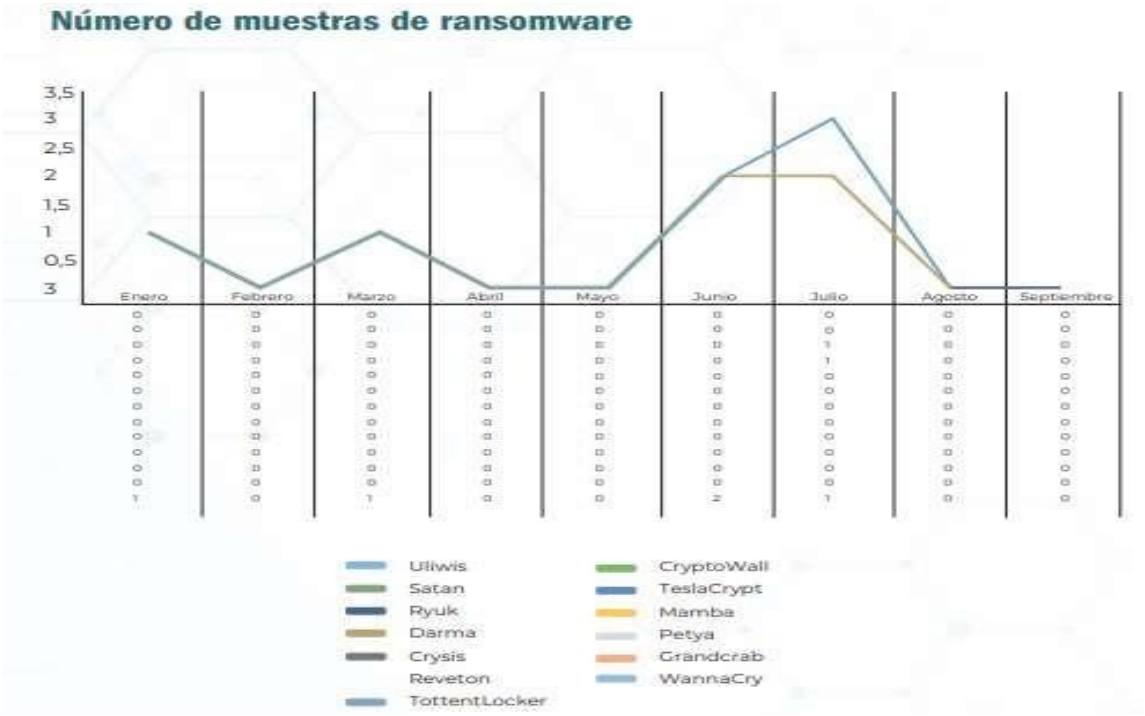
Adware móvil: Su funcionamiento es de las incomodas ventanas emergentes que aparecen en las aplicaciones, las cuales realizan una recopilación de datos y

[17] CCN-CERT. Informe Anual 2018 Dispositivos y comunicaciones móviles. [En línea]. [Consultado: 3 de septiembre de 2021]. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html

generan descargas cada vez que un usuario la clic a unas de estas, según ZDNet, “algunos de ellos han creado código de publicidad maliciosa que puede infectar y acceder a la raíz del dispositivo para forzarlo a descargar determinados tipos de adware y permitir a los atacantes robar información personal”.[18]

Según el informe de tendencias de ciber crimen en Colombia 2019-2020, En los últimos meses el RANSOMWARE “SAMSAM” había cobrado relevancia en Colombia, porque permite al atacante el robo de contraseñas para el acceso remoto a los dispositivos a través del acceso a credenciales RDP (Remote Desktop Protocol) y de ese modo secuestrar la información de las compañías víctimas.

Figura 2: Numero de muestras de ransomware

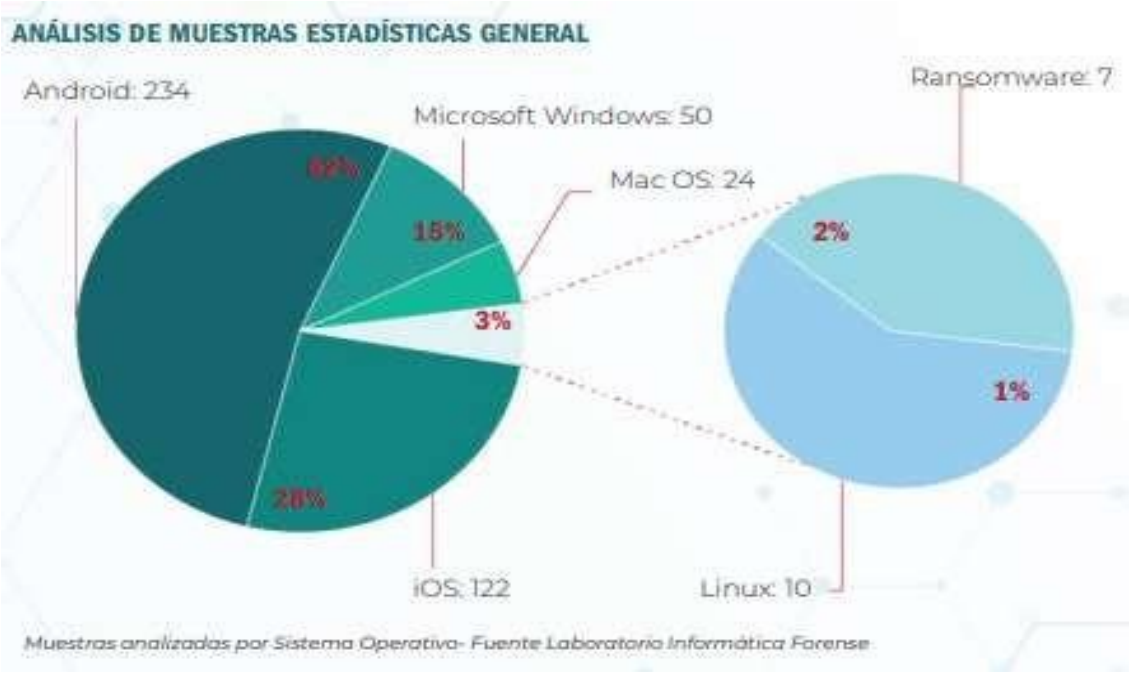


Fuente: LOPEZ CEBALLOS, Adriana et al. Informe de tendencias cibercrimen en Colombia (2019-2020). Bogotá D. C. Ccit.org.co. 2019-2020. [en línea]. [Consultado: 25 de octubre de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Durante ese año analizaron un total de 447 muestras, de las cuales 33 han sido identificadas como código malicioso (Malware), correspondientes a: Virus, Troyanos, Backdoors, Rootkit, RAT, Dropper y Ransomware.

[18] OSBORNE, Charlie. [Sitio web]. Mobile malware evolves: Adware now breaks and roots your phone. [En línea]. [Consultado: 18 de octubre de 2021]. Disponible en: https://www.zdnet.com/article/mobile-malware-evolves-adware-now-breaks-and-roots-your-phone/

Figura 3: Análisis de muestras estadísticas general



Fuente: LOPEZ CEBALLOS, Adriana *et al.* Informe de tendencias cibercrimen en Colombia (2019-2020). Bogotá D. C. Ccit.org.co. 2019-2020. [en línea]. [Consultado: 25 de octubre de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Acorde con la gráfica anterior "durante los meses de Septiembre y Octubre se analizaron diversas muestras de Malware para Sistemas Operativos Android (.APKs), identificando un común denominador frente a los permisos cargados en memoria (android.permission.WRITE_EXTERNAL_STORAGE) el cual consiente que se realice la modificación de la información almacenada en los dispositivos externos conectados (MicroSD), exhibiendo la información del usuario e incrementado los índices de compromisos".[19]

Para el presente estudio se analizaron un total de 234 muestras bajo la extensión APK. Pertenecientes a Sistemas Operativos Android, hallando muestras positivas para Malware, de las cuales un 89% llegan a ser Cryptominer y el otro 11% Adware. Teniendo como técnica la propagación de anuncios publicitarios fraudulentos a través de las redes sociales obteniendo la atracción de usuario para que posteriormente realice la acción deseada y de esa forma poder infectar el dispositivo.

[19] LOPEZ CEBALLOS, Adriana et al. Informe de tendencias cibercrimen en Colombia (2019-2020). Bogotá D. C. Ccit.org.co. 2019-2020. [en línea]. [Consultado: 25 de octubre de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Según el reporte realizado por Guisto Denise de Wilivesecurity durante el primer semestre de 2019, que para mitad de año de 2018, se publicaron 16 fallas de seguridad en los dispositivos Android, en la cual la CVE alcanzo los 611 reportes de fallos publicados; Sin embargo, el 68% de los fallos publicados en 2019 fueron de criticidad alta y el 29% de ellos permitía la ejecución de código malicioso. Esto resulta una desmejora considerable respecto a años anteriores, donde el porcentaje de fallos graves era más bajo. Por ello, es importante que los usuarios instalen a tiempo los parches de seguridad para evitar verse afectados por serias vulnerabilidades como las parcheadas el pasado julio por Google.

Figura 4: Vulnerabilidades críticas en Android

Gráfico 1. Vulnerabilidades de criticidad alta en Android a lo largo de los años

Fuente: GUISTO, Denise. Wilivesecurity. Análisis de la seguridad en dispositivos móviles durante el primer semestre de 2019. [En línea]. [Consultado: 25 de octubre de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2019/09/03/analisis-seguridad-dispositivos-moviles-primer-semestre-2019

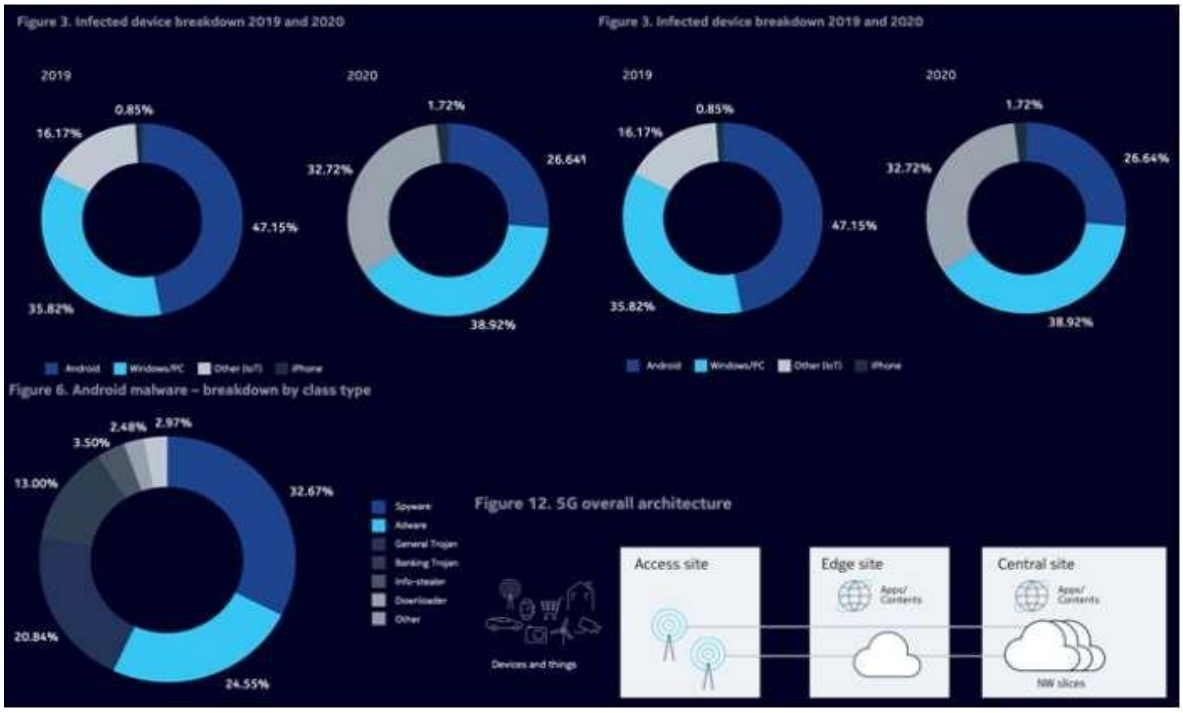
Para el primer semestre del año 2019, las detecciones de malware para Android se concentraron mundialmente en Rusia (16%), Irán (15%) y Ucrania (8%), El primer país latinoamericano en aparecer dentro del ranking internacional es México (3%) en el sexto puesto, seguido por Perú (2%) en el décimo lugar. Realizando un filtro de los países de Latinoamérica que tuvieron mayores detenciones se situaron México (26%), Perú (16%) y Brasil (12%).

Figura 5: Países de Latinoamérica con mayores detenciones de malware en Android.

Fuente: GUISTO, Denise. Wilivesecurity. Análisis de la seguridad en dispositivos móviles durante el primer semestre de 2019. [En línea]. [Cosultado:25 de octubre de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2019/09/03/analisis-seguridad-dispositivos-moviles-primer-semestre-2019

En la vigencia del año 2020, según el informe presentado por CCN- CERT IA, destaca la distribución de malware en redes móviles, con el entorno a la COVID-19 utilizando variantes como CoViper o COVIDLock disfrazadas como Apps legitimas las cuales proporcionaban información de la evolución de la pandemia, durante ese periodo Android fue la plataforma con más vulnerabilidades obteniendo un 27% de las víctimas.

Figura 6: Comparación de ataques de malware en Android y otras plataformas.



Fuente: CN-CERT. Informe Anual 2020. Dispositivos y comunicaciones móviles. [En línea]. [Consultado: en 23 de octubre de 2021]. Disponible en: https://derechodelared.com/wp-content/uploads/2021/08/CCN-CERT-IA-18-21-Informe-Anual-2020.-Dispositivos-Moviles-1.pdf

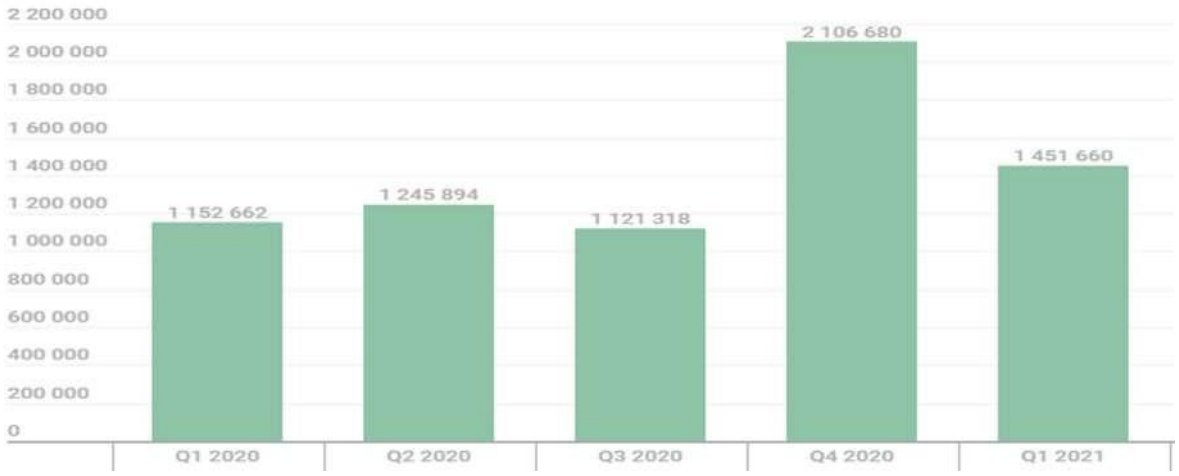
El informe presentado por Kaspersky sobre la "evolución del malware en 2020, destaca numerosas variantes para distribuir la app como si fuera realmente otras legítimas asociadas que dicen ofrecer información relacionada a la COVID-19, en la cual los cibercriminales difunden malware móvil, como (troyanos de acceso remoto móvil, marcadores telefónicos, troyanos bancarios, ransomware móvil y uso de ingeniería social etc)" [20].

Según Chebyshev, en el estudio realizado por Kaspersky Security Network para el primer trimestre del año 2021 se detectaron aproximadamente 1.451.660 paquetes de instalación maliciosas, de estos 25.314 pertenecían a troyanos bancarios móviles y 3.596 resultaron ser troyanos ransomware móviles, en la cual el (61.43%) de las amenazas detectadas son del tipo de Adware (aplicaciones publicitarias)[21]

[20] KASPERSKY. [sitio web]. Boletin de seguridad kaspersky 2020. [En línea]. [Consultado: 25 de octubre de 2021] Disponible en: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_sp.pdf

[21] CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

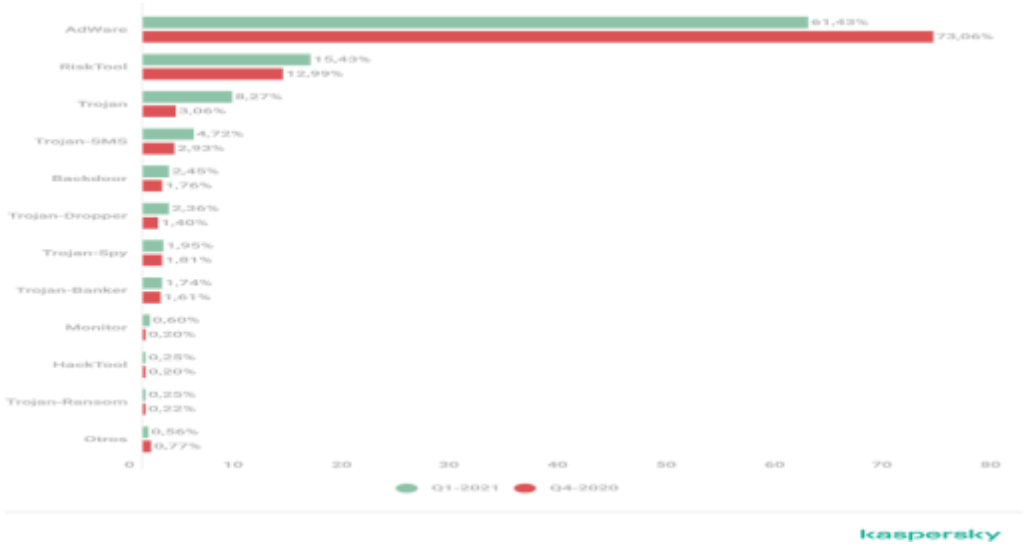
Figura 7: Paquetes de instalación maliciosas



Fuente: CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

En cuanto a la distribución de tipos de programas móviles detectados durante el primer trimestre de 2020 y 2021, se puede observar las variantes en cada uno del malware móvil que a los usuarios siendo el adware el más utilizado por cibercriminales durante estos periodos.

Figura 8: Distribución de tipos de programas móviles



Fuente: CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de

octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

Entre todas las amenazas detectadas en el primer trimestre de 2021, la gran mayoría son de aplicaciones de adware, alcanzando el 61,43%, de los cuales los más pertenecen a la familia AdWare.AndroidOS.Ewind (65,17% de todas las amenazas descubiertas de este tipo), AdWare.AndroidOS.HiddenAd (17,82%) y AdWare.AndroidOS.FakeAdBlocker (11,07%).

En cuanto a las aplicaciones potencialmente no deseadas de RiskTool, obtuvieron el segundo lugar (15,43%), y su cuota aumentó en 2 p.p. En un promedio 9 de cada 10 aplicaciones de esta clase detectadas pertenecían a la familia SMSreg.

Cuadro 2: Top 20 de los programas maliciosos para los dispositivos móviles.

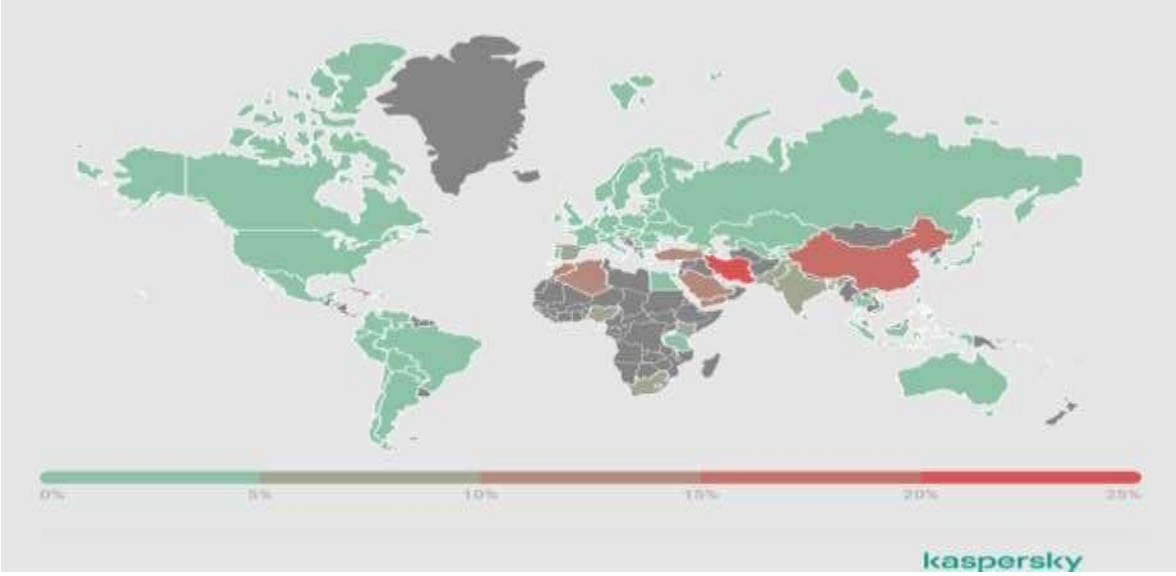
Cantidad	Veredicto	%*
1	DangerousObject.Multi.Generic	32,10
2	Trojan.AndroidOS.Boogr.gsh	12,24
3	Trojan-SMS.AndroidOS.Agent.ado	6,43
4	DangerousObject.AndroidOS.GenericML	4,98
5	Trojan-Dropper.AndroidOS.Hqwar.cf	4,13
6	Trojan.AndroidOS.Agent.vz	3,50
7	Trojan-Downloader.AndroidOS.Necro.d	3,48
8	Trojan.AndroidOS.Triada.el	2,91
9	Trojan-Downloader.AndroidOS.Helper.a	2,79
10	Trojan.AndroidOS.Whatreg.b	2,32
11	Trojan-Downloader.AndroidOS.Gapac.c	2,27
12	Trojan.AndroidOS.Triada.ef	2,26
13	Trojan.AndroidOS.MobOk.ad	2,24
14	Trojan.AndroidOS.LockScreen.ar	2,17
15	Trojan-Downloader.AndroidOS.Agent.ic	2,17
16	Trojan-SMS.AndroidOS.Agent.acv	2,16
17	Trojan-Banker.AndroidOS.Agent.eq	1,98
18	Trojan.AndroidOS.Hiddad.fw	1,91
19	Exploit.AndroidOS.Lotoor.be	1,68
20	Trojan-Dropper.AndroidOS.Hqwar.di	1,65

Fuente: CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

Entre las acciones más conocidas de estos malware se encuentran las desactualizaciones de los antivirus en línea que no cuentan con datos para detección de programas maliciosos, descargas exploits, generación de anuncios

intrusivos en la pantalla del dispositivo, suscripción a servicios de pagos sin consentimiento, dan control absoluto a los atacantes de las cuentas bancarias como los SMS la gran mayoría fueron detectado en Rusia.

Figura 9: Grafica de amenazas móviles a nivel mundial



Fuente: CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

Entre los países más atacados se encuentran Irán con un 25,80%, seguido China con el 16,39 y en tercer lugar Arabia Saudita con 13,99.

Cuadro 3: Top 10 de pises atacados por malware móvil.

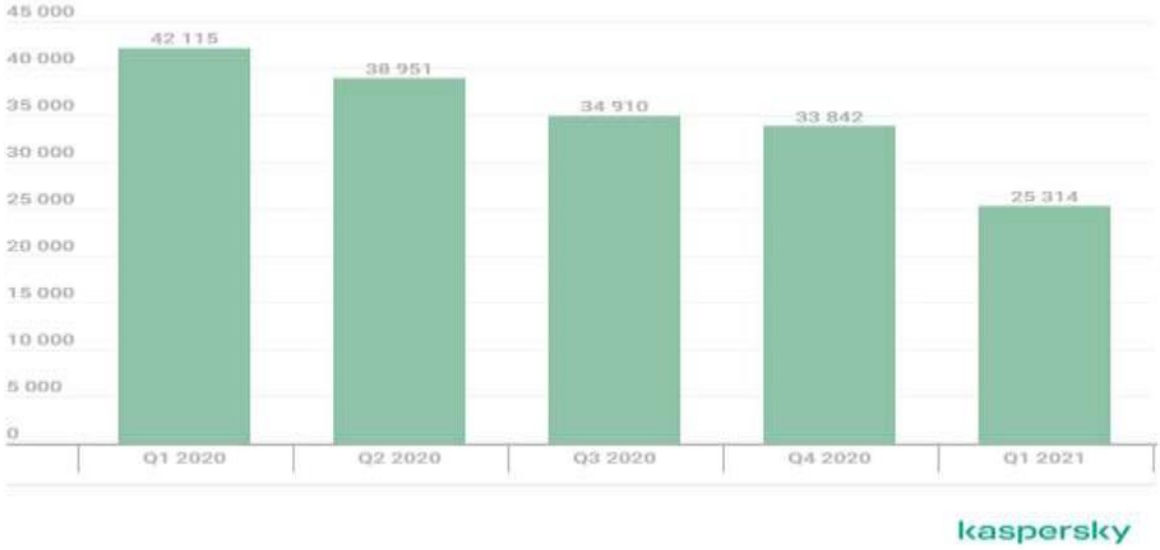
Cantidad	País*	%**
1	Irán	25,80
2	China	16,39
3	Arabia Saudita	13,99
4	Argelia	13,22
5	Marruecos	10,62
6	Turquía	10,43
7	Yemen	10,05
8	Nigeria	9,82
9	India	8,08
10	Kenia	8,02

Fuente: CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de

octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/
En el primer trimestre hubo 25.314 paquetes de instaladores de troyanos bancarios móviles, en cuanto al cuarto trimestre del año 2020 hubo un descenso de 8.528.

Entre los malware bancario más detectados estan Trojan-Banker.AndroidOS.Agent (57,51% del total de troyanos bancarios detectados), Trojan-Banker.AndroidOS.Wroba (7,98%) y Trojan-Banker.AndroidOS.Gustuff (7,64%).

Figura 10: Troyanos bancarios móviles.



Fuente: CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

Cuadro 4: Tipos de troyanos bancarios móviles.

Cantidad	Veredicto	%*
1	Trojan-Banker.AndroidOS.Agent.eq	22,06
2	Trojan-Banker.AndroidOS.Anubis.t	11,01
3	Trojan-Banker.AndroidOS.Svpeng.q	9,67
4	Trojan-Banker.AndroidOS.Asacub.ce	5,62
5	Trojan-Banker.AndroidOS.Asacub.snt	5,03
6	Trojan-Banker.AndroidOS.Anubis.n	4,66
7	Trojan-Banker.AndroidOS.Asacub.bv	3,66
8	Trojan-Banker.AndroidOS.Agent.ep	3,56
9	Trojan-Banker.AndroidOS.Hqwar.t	3,43
10	Trojan-Banker.AndroidOS.Agent.cf	2,52

Fuente: CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de

octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

En cuanto a los troyanos bancarios móviles entre los países más atacados se encuentran Japón con un 1,59%, con el con Trojan-Banker.AndroidOS.Agent.ep. Seguido Turquía 0,67 con el malware con Trojan-Banker.AndroidOS.Agent.ep y tercer lugar 0,40 con el siendo Trojan-Banker.AndroidOS.Agent.eq.

Cuadro 5: Países más atacados por troyanos bancario

1	Japón	1,59
2	Turquía	0,67
3	Alemania	0,40
4	España	0,31
5	Francia	0,31
6	Australia	0,28
7	Noruega	0,22
8	Corea del Sur	0,19
9	Italia	0,16
10	Finlandia	0,12

Fuente: CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

6 METODOLOGIAS Y ESTANDARES DE ESCANEO, ANALISIS DE VULNERABILIDADES Y DETECCION DE FALLOS APLICADOS A DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID.

Cuando hablamos de metodología nos referimos a la evaluación que se les puede hacer a los dispositivos móviles en este caso con sistema operativo Android, con el fin de detectar algunos errores o fallos en el sistema los cuales se muestran en un informe detallado.

Existen algunas metodologías que se han desarrollado para realizar el escaneo y análisis de riesgos de vulnerabilidades de los dispositivos móviles personales con sistema operativo Android, las cuales son muy eficientes para prevenir amenazas y protegerlos frente a ellas. debido al incremento y frecuencia de las diversas técnicas y ataques a la que se encuentra expuesto el sistema operativo Android y las secuelas que se dan de estos.

El sistema operativo Android cuenta con una gran cantidad de aplicaciones móviles disponibles, debido a esto, tiende a presentar muchas vulnerabilidades. No

obstante, cuenta con muy buenos estándares de seguridad ante las posibles amenazas; pese a que, quienes desarrollan las aplicaciones cuentan con las opciones de realizar un sometimiento o no la app a regulaciones y permisos para asegurar la información, controles que diversas veces no se emplean. Todo esto tiende a dejar como resultado las problemáticas más comunes, como dificultades en la transmisión de los datos e inconvenientes en la privacidad y almacenamiento de estos.[22]

A nivel mundial encontramos pruebas de intrusión y algunos estándares relacionados con el escaneo y análisis de vulnerabilidades, dentro de los cuales tenemos inicialmente las metodologías para la gestión de riesgos de privacidad CNIL, la cual se basa en el tratamiento de la información personal encontrada en los dispositivos móviles de los usuarios, la cual tiene como objetivos:

Tener una visión de los riesgos que son resultados del tratamiento de la información personal de los usuarios.

Saber la forma de determinar las medidas de seguridad, las cuales son necesarias para tomar todas las medidas que sean útiles para la naturaleza de la información de los usuarios y los riesgos de su procesamiento, con el fin de preservar la seguridad de los datos y evitar que estos sean alterados, dañados o que sean accedidos por personas no autorizadas.

Existen varios tipos de metodologías para llevar a cabo la evaluación de seguridad en los dispositivos con sistemas operativos Android.

6.1 Open Android Security Assessment Methodology -OASAM

Por otro lado encontramos la metodología OPEN ANDROID SECURITY ASSESSMENT METHODOLOGY -OASAM, que significa metodología abierta de evaluación de seguridad de Android, debido a que el sistema operativa Android es muy extenso, las aplicaciones tienden hacer las que más se desarrollen para este, por ello es que fundo el proyecto OASAM el cual procura convertirse en una taxonomía completa y sólida de vulnerabilidades con framework de respaldo y soporte.

Esta metodología tiene como objetivo principal realizar un análisis de vulnerabilidades y de seguridad a las aplicaciones de los dispositivos móviles Android, esta metodología sirve de apoyo no solo a los desarrolladores de

[22] TORO SANCHEZ, Cristian, *et al.* Guía para validar el nivel de seguridad de los permisos y uso de recursos de una aplicación móvil bajo plataformas Android. [En línea] Proyecto de grado. Universidad Católica de Colombia. Bogotá D.C. 2015. [Consultado: 29 de octubre de 2021]. Disponible en https://repository.ucatolica.edu.co/bitstream/10983/2778/1/Proyecto%20Gu%C3%ADa%20Validaci%C3%B3n%20Seguridad%20App%20M%C3%B3vil%20APA.pdf

aplicaciones, sino también a los encargados de buscar vulnerabilidades en las mismas.

Cuenta con una cantidad de controles de seguridad para las aplicaciones Android, las cuales están estructuradas por categorías donde cada una se corresponde a un ámbito de evaluación.[23]

OASAM-INFO: Recolección de información: Recolección de información y definición de superficie de ataque, en la cual se realizan muchas pruebas de vulnerabilidad en la cual se define el parámetro del ataque, aplicándose controles como “información general, lista de componentes, permisos de componentes, permisos de componentes e intenciones de lanzamiento de componentes”

OASAM-CONF: Gestión de la configuración y el despliegue: Evaluación de la configuración y el despliegue, en la cual se definen varios errores en la configuración o en la opción de despliegue de las aplicaciones, tiene controles como: “depuración sin restricciones, uso de bibliotecas no actualizado, archivos predeterminados y de respaldo, metadatos sobre los archivos, endurecimiento de WebView insuficiente, permisos de archivo incorrectos, permisos incorrectos del proveedor de contenido, permisos incorrectos del proveedor de contenido, permisos de actividades indebidas, permisos de servicios inadecuados Permisos de receptores de transmisión inadecuados, permisos de base de datos incorrectos y permisos de preferencias compartidas incorrectos”

OASAM-AUTH: Autenticación: Fase en la cual se evalúa la autenticación, las funcionalidades en cuanto al uso de logins mediante la aplicación, evaluando las debilidades con la aplicación. Se aplican controles como “Usuarios y contraseñas predeterminados, Política de contraseñas débiles y Funcionalidad de recordar credenciales”.

OASAM-CRYPT: Criptografía: Se realiza la evaluación del uso de la criptografía, se prueban funcionalidades relacionadas con el uso de criptografías en las aplicaciones y pueden ocurrir en él envió o almacenamiento de los datos, también cuenta con controles para lograr ese objetivo “credenciales codificadas, almacenamiento de datos inseguro, uso inseguro del protocolo de transporte y la fijación de certificados.”

OASAM-LEAK: Information Fuga: Fase en la cual se realiza la verificación de la información que se filtra en los medios. Donde la información sensible podría estar relacionada con el usuario o con el propio teléfono.

[23] MEDIANERO, Daniel. OASAM [En línea]. [Consultado: 30 de octubre de 2021] Disponible en: https://github.com/b66l/OASAM

OASAM-DV: Validación de datos: Evaluación de la gestión de entrada de usuarios, cuando el usuario administra de forma inadecuado sus datos es susceptible a vectores de ataque, debido a que podría permitir a un atacante alterar el flujo de datos de la aplicación, inyectando código y afectando de manera grave la aplicación y los datos almacenados en ella. Cuenta con controles como: Inyección de código HTML, Desbordamiento de búfer, Inyección de comandos en bases de datos, Inyección de ruta en el acceso a archivos, Comprobación de parámetros nulos, Inyección de registros y Control del proceso de inyección a través de datos de intención.

OASAM-IS: Intent Spoofing: Evaluación de gestión de recepción de intenciones, donde la víctima es utilizada por el atacante enviando datos inesperados aprovechándose de las funcionalidades, Intención de suplantación de identidad en componentes de difusión, lanzamiento arbitrario de actividades, lanzamiento arbitrario de servicios y debilidades relacionadas con el uso inseguro de Pending Intents.

OASAM-UIR: Recibo de intención no autorizado: Se realiza la evaluación de resolución de intención, en el momento que una aplicación envíe un Intent implícito, no hay garantía que este no sea captado por una aplicación maliciosa, debido que las aplicaciones maliciosas podrían registrar un Intent Filter capaz de pasar la resolución (acción, datos y categoría), a no ser que este Intent cuente con un conjunto, este cuenta con controles como: “Robo de transmisiones, secuestro de actividades, secuestro de servicios e intenciones especiales de debilidad.

Lógica empresarial OASAM-BL: Evaluación de la lógica empresarial de la aplicación, en la cual se incluyen las vulnerabilidades con componentes más centrados en el diseño que en codificación.

6.2 OWASP

Metodología de OWASP o Proyecto Abierto de Seguridad de Aplicaciones Web, por sus siglas en inglés, es una organización sin ánimo de lucro que surge a partir del año 2001, con la finalidad de realizar aportes para mejorar las capacidades de seguridad del software, asimismo mostrar lo muy importante la ralentización en los criterios de seguridad en las aplicaciones brindando información adecuada.

El proyecto OWASP organiza sus acciones mediante un enfoque colaborativo donde cualquier profesional de la seguridad informática podría realizar aportes de sus conocimientos, con su acción de la promoción de los contenidos e ideas al público, con la finalidad de preservar y garantizarla seguridad.

OWASP cuenta herramientas y estándares de seguridad en aplicaciones,

- Libros, aplicaciones y desarrollo de códigos fuentes seguro,
- revisiones de seguridad en código fuente, videos y presentaciones
- Hojas de trucos en varios temas comunes.
- Controles de seguridad estándar y bibliotecas.
- Capítulos locales en todo el mundo.
- Investigaciones de vanguardia.
- Numerosas conferencias alrededor del mundo.
- Listas de correo.

Cada una de las anteriores herramientas de OWASP son totalmente gratuitas, documentos, videos, presentaciones y capítulos son gratuitos y abiertos a cualquier interesado en mejorar la seguridad en aplicaciones.

Además cuenta con unas fases de seguridad, un top 10 de aplicaciones de seguridad con la cual se da a conocer las vulnerabilidades más frecuentes, que son recolectadas de las informaciones que generan o reportan muchas organizaciones como medidas de seguridad, mediante la información que se logra obtener se conoce el modo operando y cuáles son las medidas, acciones y/o recomendaciones se deben llevar cabo para reducir estos riesgos.

6.3 OSSTMM

OSSTMM (Open Source Security Testing Methodology Manual) esta metodología permite realizar pruebas exaustivas de seguridad, donde por medio de una auditoria realiza una precisa medición de la seguridad a nivel operacional, evitando suposiciones y evidencia anecdótica. Está diseñada para ser consistentes y repetible como metodologia.

La gestión del riesgo cuantitativo puede ser hecha desde el reporte con los hallazgos de la auditoría OSSTMM, proporcionando un resultado mejorado debido a resultados más precisos libres de error, “sin embargo se podría encontrar la gestión de confianza propuesta aquí superior a la gestión del riesgo. OSSTMM incluye información para planificar el proyecto, cuantificar resultados, y las reglas del contrato para realizar auditorías de seguridad”[24].
Este manual es un complemento para el desarrollo y correcta aplicación de las normas NIST, ISO 27001-27002 e ITIL entre otras, que lo convierten en uno de los manuales más completos en lo que respecta a la aplicación de pruebas de

[24] QUEZADA CABALLERO, Eduardo Alonso. Introducción a OSSTMM (Open Source Security Testing Methodology Manual. [En línea]. [Consultado: 30 de octubre de 2021]. Disponible en: http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual

seguridad e información en las instituciones y la nueva implementación de su versión número 3, conocida como OSSTMM 3.[25]

6.4 ISSAF

ISSAF, de OISSG (Open Information System Security Group). Es uno de los frameworks más importante dentro del ámbito de metodología de testeo. Realiza un análisis detallado de todos los posibles aspectos que afectan al testeo de seguridad.

La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar "Criterios de Evaluación", cada uno de los cuales ha sido escrito y revisado por expertos en cada una de las áreas de aplicación. Estos criterios de evaluación a su vez se componen de los siguientes ítems[26]:

- Una descripción del criterio de evaluación.
- Puntos y objetivos para cubrir.
- Los prerrequisitos para conducir la evaluación.
- El proceso mismo de evaluación.
- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.
- Referencias y Documentación Externa.

Del mismo modo encontramos algunos métodos de escaneo de vulnerabilidades como lo son:

App-Ray: este método puede detectar amenazas antes que se echen a perder los datos y al mismo tiempo impide instalar aplicaciones maliciosas. "El desarrollo acelerado y la entrega rápida a menudo dan como resultado posibles fallas y vulnerabilidades en las aplicaciones, el escáner ayuda a identificar y corregir las amenazas y vulnerabilidades en las aplicaciones descargadas en el dispositivo móvil.

[25] El flujo de este manual OSSTMM comienza con determinar la situación objetivo, esta situación está determinada por la cultura, reglas, normas, regulaciones, legislación y políticas definidas en esta. La metodología propone un modelo jerárquico de Canales, Módulos y Tareas, donde los vectores son simplemente las líneas de análisis que apuntan a cada uno de los canales. Los módulos son áreas específicas de cada canal, pudiendo encontrar actividades que se encuentran en la frontera entre dos canales.

[26] JUNTA DE ANDALUCIA. [Sitio web]. Marco De Desarrollo De La Junta De Andalucia. [Consultado 14 de octubre de 2021]. Disponible en: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.1/contenido-recurso-216.html

La metodología emplea diversas técnicas de análisis, de forma dinámica como estática; para el análisis estático se utiliza cuando hay problemas de codificación como “el cifrado, fuga de los datos, y técnicas anti-depuración”.

De igual forma para el análisis dinámico se utiliza para las pruebas instrumentales y no modificadas, acceso a archivos de comunicación, etc. Una vez que se ejecute el análisis se logra observar todos los detalles técnicos permitiendo la descarga de los archivos necesarios.[27]

Codified Security: este método de escaneo detecta y soluciona muy rápido los problemas de seguridad utilizando Codificación. Solamente se carga el código de la aplicación y se usa el escáner para probarlo, lo que da como resultado un informe detallado que muestra todos los riesgos de seguridad del dispositivo móvil, además actúa en modo autoservicio simplemente con lograr cargar los archivos en la plataforma lográndose integrar con los ciclos de entrega sin problemas alguno creando parámetros para los motores estáticos estableciendo niveles de cumplimiento.

Después del análisis de seguridad realiza una descripción clara de los riesgos o hallazgos asociados a la aplicación en móvil en análisis, para posteriormente dar una serie de pautas o acciones aplicables que ayuden a prevenir las vulnerabilidades.

Codified admite cargas de IPA y APK. Facilita las pruebas de bibliotecas estáticas, dinámicas y de terceros y se complementa con las aplicaciones como Phonegap, Xamarin y Hockey, siendo compatibles con aplicaciones Java, Swift y Objective-C.

Mobile Security Framework: Se utiliza en dispositivos móviles Android para realizar el análisis de malware, pruebas de penetración, evaluación de seguridad entre otros, los cuales se pueden ejecutar de forma estática y dinámica.

[27] KUMAR, Chandan. 11 Escáner de aplicaciones móviles para encontrar vulnerabilidades de seguridad. [En línea]. [Consultado en 21 de octubre de 2021]. Disponible en: https://geekflare.com/es/mobile-app-security-scanner/

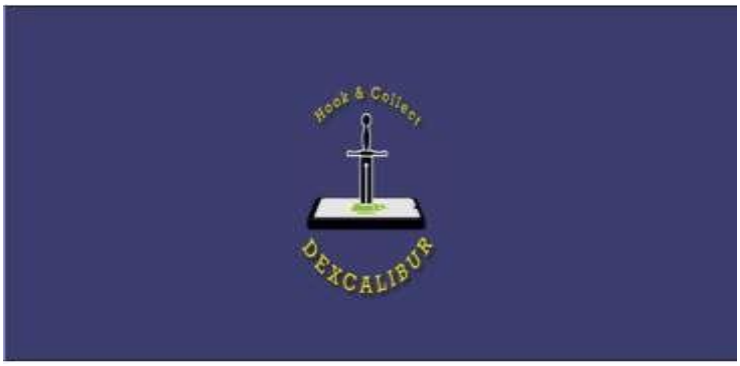
Figura 11. Interfax de Mobile Security Framework

Fuente: KUMAR, Chandan. 11 Escáner de aplicaciones móviles para encontrar vulnerabilidades de seguridad. [En línea]. Geekflare. [Consultado en 21 de octubre de 2021]. Disponible en: https://geekflare.com/es/mobile-app-security-scanner/

Este método de escaneo proporciona API REST para poder integrar su canalización DevSecOps o CI / CD sin problemas. Por otro lado, admite binarios de aplicaciones móviles como IPA, APK y APPX, y códigos fuente comprimidos. También puede ejecutar evaluación de seguridad en tiempo de ejecución con su analizador dinámico instrumentado.

Dexcalibur: este es un escáner de Android de ingeniería inversa que se centra en la automatización de la instrumentación. Su propósito es enderezar la función ejecutada, donde también puede representar las funciones que se pueden ejecutar según la profundidad del valor de configuración.

Figura 12: Escaner Dexcalibur



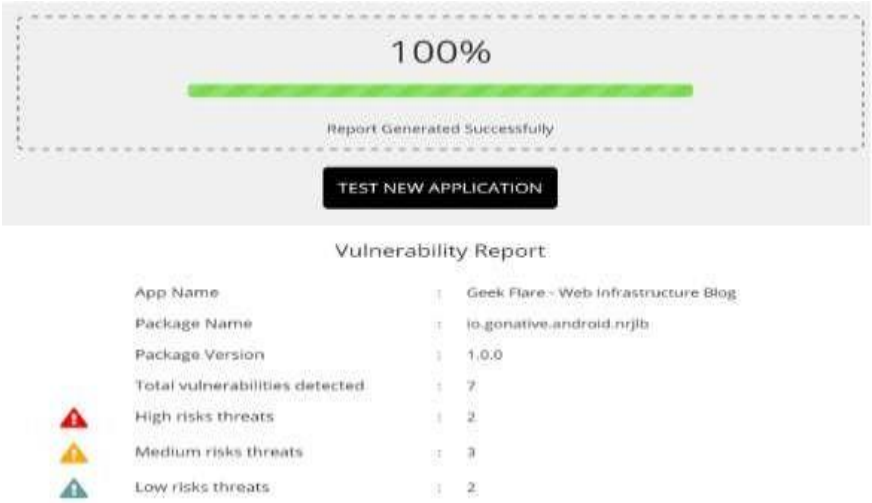
Fuente: KUMAR, Chandan. 11 Escáner de aplicaciones móviles para encontrar vulnerabilidades de seguridad. [En línea]. [Consultado: 21 de octubre de 2021]. Disponible en: https://geekflare.com/es/mobile-app-security-scanner/

Entre los objetivos de este escáner esta realizar procesos automatizados como:

Procesar datos que recopila un gancho, como un archivo dex, un cargador de clases, un método invocado, etc. Descompilar códigos de bytes interceptados, escribir códigos de gancho y realizar la administración de mensajes de gancho.

Quixxi Security: Herramienta de seguridad de extremo a extremo inteligente e integrado. En la cual los desarrolladores pueden proteger y monitorear cualquier aplicación móvil en minutos, proporcionando protección de aplicaciones sin código contra piratas informáticos que buscan la clonación, manipulación, inyección de códigos maliciosos.

Figura 13: Herramienta Quixxi Security



Fuente: KUMAR, Chandan. 11 Escáner de aplicaciones móviles para encontrar vulnerabilidades de seguridad. [En línea]. [Consultado: 21 de octubre de 2021]. Disponible en: https://geekflare.com/es/mobile-app-security-scanner/

El análisis puede tardar unos minutos y, una vez hecho, obtendrá una descripción general del informe de vulnerabilidad. Además cuenta con tres momentos importantes para el logro de los objetivos:

Escáner: para identificación de vulnerabilidades y protección de los dispositivos, mediante una prueba de vulnerabilidad automatizada, cuenta con una evaluación manuela avanzada y está inspirado en OWPAS.

Blindaje: Etapa de Supervisión, administración y mejora en las aplicaciones móviles en la conexión con los usuarios “Adapte su seguridad, Protección de ingeniería inversa, Detección de manipulación, Protección en tiempo de ejecución.

Supervisa: Acelera el desarrollo de sus aplicaciones móviles o comercializa su código: Licencia, analítica y el diagnóstico.

7 FASES DE LA METODOLOGÍA PARA EL ANÁLISIS DE VULNERABILIDADES Y DETECCIÓN DE FALLOS DE ANDROID

Las metodologías para el análisis de vulnerabilidades y detección de fallos en los dispositivos móviles con sistema Android, están enfocadas en proteger la información personal que en estos reposa, tratando de evitar un posible ataque. Del mismo modo la metodología en sí, debe ser un proceso repetitivo debido a que las tecnologías nunca dejan de evolucionar y con su avance aparecen nuevos riesgos.

Surge con la finalidad de garantizar la seguridad de aplicaciones web, pero debido a su experiencia en el mercado de la seguridad, se notó efectivo que por el aumento de las aplicaciones móviles era indispensable crear una guía orientada específicamente para el enfoque de este tipo de aplicaciones.

Es así, como de acuerdo con las técnicas y herramientas utilizadas para las pruebas de seguridad de aplicaciones móviles basadas en Owasp, se establecen las fases de recopilación de información, prueba de gestión de la configuración, prueba de la lógica de negocio, prueba de autenticación, prueba de autorización, prueba de gestión de sesiones, prueba de validación de datos, prueba de denegación de servicios, prueba de servicios web y prueba de Ajax.

7.1 Fases de análisis de vulnerabilidades OWASP

Como ya se había mencionado anteriormente OWASP o Proyecto Abierto de Seguridad de Aplicaciones Web, por sus siglas en inglés, es una organización sin ánimo de lucro que surge a partir del año 2001, con la finalidad de realizar aportes para mejorar las capacidades de seguridad del software, asimismo mostrar lo muy importante la ralentización en los criterios de seguridad en las aplicaciones brindando información adecuada.

Es así, como de acuerdo con las técnicas y herramientas utilizadas para las pruebas de seguridad de aplicaciones móviles basadas en owasp, se establecen las fases de recopilación de información.

Fases de recopilación de información. Dentro de estas fases tenemos las siguientes:

Pruebas de gestión de la configuración: Los análisis sobre la infraestructura o la topología de la arquitectura revelan datos importantes sobre una aplicación Web.

Con estas pruebas se pueden obtener datos importantes como por ejemplo el código fuente, los métodos HTTP permitidos, funcionalidades administrativas, métodos de autenticación y configuraciones de la infraestructura.

Algunas de las pruebas de gestión de configuración son:

- Pruebas de SSL/TLS

Las pruebas SSL/TLS consisten en realizar el aseguramiento del cifrado en los protocolos, permitiendo de esta forma una comunicación segura entre un cliente y servidor como lo es en el caso del protocolo http el cual es asegurado cuando se incorpora SSL o TSL, el cual dará como resultado un protocolo https para el correcto cifrado de los datos, además permite la identificación de los servidores.

Es importante que se realice la comprobación de los certificados utilizados en uso, verificando la robustez de las páginas web previendo que sean susceptibles ataques, cabe resaltar que existen diferentes herramientas que se pueden utilizar para verificar que tan seguros son los servicios.

- Pruebas del receptor de escucha de la BD

Consiste en recibir solicitud o petición de conexiones remotas a las BD de los clientes, cuando el dominio logra ser comprometido tiende afectar con él la disponibilidad, ya que actúa como un enlace de conexión remoto a la BD Oracle, mediante la cual recibe, procesa las solicitudes y las gestiona.

Entre los ataques más destacados se encuentran:

Se aplica la detección del receptor mediante un ataque Dos, además le aplican en la configuración una contraseña con la cual evitan que se pueda acceder el control del receptor, para posteriormente secuestrar la BD.

También se aplican la escritura en los registros de trazado y registro a cualquier archivo accesible al proceso propietario de tnslnr (generalmente Oracle) - Posible revelación de información.

Lograr información minuciosa de los receptores, BD y las configuraciones de las aplicaciones.

- Pruebas de gestión de configuración de la infraestructura

En la aplicación de los servidores o servicios tiende hacer muy importante la configuración de su infraestructura, ya que por medio de esta se preservará la seguridad de las aplicaciones web, es importante que se realicen análisis de la gestión adecuada de la configuración aplicada en la infraestructura del servidor, lo más importante es llevar a cabo una revisión de la configuración con detalle y de problemas conocidos de seguridad.

Además que a menudo se apliquen pruebas de los errores o fallas conocidos, revisando y asegurando los servicios, siendo vital para escudriñar las

vulnerabilidades ya que una simple amenaza podría minar la seguridad de la totalidad de la infraestructura, reduciendo los riesgos y/o amenazas.

Por ejemplo, una vulnerabilidad de un servidor que permitiese a un atacante remoto exponer el código fuente de la propia aplicación (una vulnerabilidad que ha aparecido en varias ocasiones, tanto en servidores web como de aplicación) podría comprometer la aplicación, ya que usuarios anónimos podrían usar la información expuesta en el código fuente basándose en ella para realizar ataques contra la aplicación o sus usuarios.[28]

Ante las vulnerabilidades y/o amenazas a las que se encuentra expuestas las infraestructuras es importante que se apliquen los siguientes pasos.

Se deben determinar los elementos que conforman la infraestructura, para esta forma entender su interacción y si afectan o no a la seguridad.

Realizar un análisis detallado de cada uno de los elementos que conforman la infraestructura validando que estos no contengan vulnerabilidades conocidas.

Las herramientas administrativas que se utilizan para el mantenimiento de cada uno de los componentes deben ser revisadas evitando fallos en ellas.

Si, en algún caso llegase a existir sistemas de “autenticación” es importante que se revisen para constatar que sirve a las necesidades de la aplicación, además que no puedan ser manipulados y que deniegue el acceso a usuarios externos.

Para cada uno de los puertos definidos para la utilización de la aplicación, deberán tenerse bajo el control de cambios.

- Pruebas de gestión de configuración de la aplicación

Es importante que se realice la adecuada configuración de cada uno de los componentes que interactúan o hacen parte de la aplicación, evitando que hayan errores que comprometan la seguridad.

Tiende hacer difícil la validación y prueba de la configuración a la hora de crear y mantener una arquitectura de este tipo, por la integración de las aplicaciones y estas cuentan con diversas configuraciones genéricas que posiblemente no se encuentren adecuadas a las tareas que se realizarían en el sistema específico a integrar. Sin embargo durante la instalación típica de servidores web y de Aplicaciones estos incluyen diversas funcionalidades (como ejemplos de aplicación,

[28] OWASP. Guía de pruebas de OWASP 2008. Ver 3.0. [en línea]. [Consultado 30 de octubre de 2021]. Disponible en: https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

documentación y páginas de prueba), aquello que no es esencial para la aplicación debería ser eliminado antes de la implementación, evitando las explotaciones después de su instalación.

Entre las medidas más recomendadas encontramos:

Se debe habilitar los módulos de servidor (extensiones ISAPI en el caso de IIS) que sean indispensables para las aplicaciones, para de esta forma reducir los ataques por la reducción del tamaño y complejidad.

Manipular los errores de servidor, se tendrá que tener en cuenta del aseguramiento específico que no sea devuelto algún tipo de error a usuario final en la ejecución de la aplicación, puesto que esto conllevaría a un ataque inminente por parte de especialista en el área.

Asegurarse que la ejecución de los privilegios sean mínimos de tal forma de prevenir errores en el software del servidor y que este a su vez comprometa el sistema por completo.

- Gestión de extensiones de archivo

Son implementadas con la finalidad de determinar cuáles serían las adecuadas para gestionar y responder las peticiones en el servicio web, bien sea por tecnologías / lenguajes o plugins. Dependiente del tipo de archivo a los que se intenten acezar, el uso de las extensiones de archivos estándar proporcionan información de beneficiosa a quien realiza las pruebas de intrusión, sobre qué tipo de tecnologías son utilizadas en una aplicación web, de esta forma ayudando a comprobar los escenario de ataque que se pueden utilizar sobre las tecnologías específicas.

- Archivos antiguos, copias de seguridad y sin referencias

Durante la creación de los servicios o aplicaciones web tienden a quedar archivos que no son gestionados y sin referencia u olvidados con los cuales se podrían obtener información sensible de la infraestructura o credenciales. Generalmente se encuentran datos que no tienen nada que ver con la aplicación, son creados de la edición de los archivos de la aplicación encuentran archivos en versiones viejas modificados, renombrados o en su defecto copias de seguridad manuales o archivos comprimidos, convirtiéndose en una fuente de vulnerabilidad activa debido a que es particular que se olviden archivos de este tipo siendo una amenaza para las aplicaciones.[29]

Los archivos sin referencia pueden dejar información delicada que con llevaría a un ataque, en cuanto los archivos viejos y los backup se podrían encontrar debilidades

[29] Ibíd., p. 109-115.

que fueron corregidos en versiones más recientes, y los archivos de los registros almacenan toda la información de los usuarios en la utilización de la aplicación.

- Interfaces de administración de la infraestructura y de la aplicación

Proceso en el cual se le permite a un usuario a través de la interface obtener unos privilegios accediendo a diversas funcionalidades mediante las cuales puede generar cambios en la aplicación, además se tiende a evaluar cómo estas funcionalidades logran ser acezadas por un usuario sin privilegios ni autorización.

En las aplicaciones que requieren de la interface de administrador para que posteriormente este pueda habilitar a un usuario con privilegios el cual pueda realizar la provisión de cuentas de usuario, diseño del sitio y disposición, manipulación de los datos y cambios a la configuración.

- Métodos HTTP y XST

Sirven como modelos para la realización de acciones en los servidores web, además de ayudar a los desarrolladores en la implementación y probar sus aplicaciones web, el modelo HTTP cuando no se encuentra bien configurado el servidor puede ser nefasto si este se encuentra mal configurado.

La segunda fase es la de prueba de gestión de la configuración, donde se realizan los análisis sobre la infraestructura o la topología de la arquitectura, pueden revelar importantes datos acerca de una aplicación que se encuentra instalada en el dispositivo móvil tipo Android.

Las pruebas que se pueden realizar en la gestión de configuración pueden ser: Pruebas de SSL/TLS, Pruebas del receptor de escucha de la BD, Pruebas de gestión de configuración de la infraestructura, Pruebas de gestión de configuración de la aplicación, Gestión de extensiones de archivo, Archivos antiguos, copias de seguridad y sin referencias, Interfaces de administración de la infraestructura y de la aplicación, Métodos HTTP y XST entre otros.[30]

Seguidamente, en la fase número tres tenemos la comprobación del sistema de autenticación, donde la autenticación depende de algunos factores, en este caso, es el proceso de intentar verificar la identidad digital del remitente de un mensaje, en este proceso de comprobación intervienen la transmisión de credenciales a través de un canal cifrado, enumeración de usuarios, pruebas de diccionario sobre cuentas de Usuario o cuentas predeterminadas, pruebas de fuerza bruta, Saltarse

[30] SALAZAR, Edgar. Pruebas de Seguridad en aplicaciones web según OWASP. [en línea]. [Consultado: 20 de octubre de 2021]. Disponible en: https://owasp.org/www-pdf-archive/OWASP_SUSCERTE.pdf

el sistema de autenticación, “Comprobar Sistemas de recordatorio/restauración de contraseñas vulnerables, pruebas de gestión del caché de navegación y de salida de sesión, pruebas de CAPTCHA, Múltiples factores de autenticación, probar por situaciones adversas”.[31]

Ante ello, la fase cuarta es la gestión de sesiones, que cubre todos los controles que se realizan sobre las aplicaciones del dispositivo, desde la autenticación hasta la salida de la aplicación.

Seguidamente, la prueba de autorización como quinta fase es la que permite el acceso a los recursos a los que se tiene permiso únicamente con autorización, esta significa entender la forma como funciona el proceso de autorización y como utilizar dicha información para saltarse el sistema de autorización. “La sexta fase es la prueba de lógica de negocios, que consiste en comprobar por fallas en la lógica de negocio en una aplicación para Android, se requiere pensar en modos no convencionales”.[32]

La séptima fase es la prueba de validación de datos, donde la debilidad más común en la seguridad de aplicaciones para dispositivos móviles es la falta de una validación adecuada de las entradas procedentes del cliente o del entorno de la aplicación, la cual conduce a casi Todas las principales vulnerabilidades en aplicaciones, como inyecciones sobre el intérprete, ataques locale/Unicode, sobre el sistema de archivos y desbordamientos de búfer.[33]

Por esto, la fase octava es la prueba de denegación de servicio, donde existe un tipo de ataque muy común llamado denegación de servicios (Dos), el cual es del tipo empleado en una red para hacer inalcanzable a la comunicación a un servidor por parte de otros usuarios válidos. El concepto fundamental de un ataque DOS de red es un usuario malicioso inundando con suficiente tráfico una máquina objetivo para conseguir hacerla incapaz de sostener el volumen de peticiones que recibe. Cuando el usuario malicioso emplea un gran número de máquinas para inundar de tráfico una sola máquina objetivo, se conoce generalmente como ataque denegación de servicios distribuidos (DDOS).[34]

Igualmente, la prueba de servicios web y SOA (Arquitectura Orientada a Servicios), es la fase novena, siendo aplicaciones en expansión que están permitiendo que los negocios operen entre sí y crezcan más rápido. Las vulnerabilidades en servicios web son similares a otras vulnerabilidades como la inyección SQL, revelación de información, etc. Pero también tienen vulnerabilidades de XML[35]

[31] Ibíd., p. 12.
[32] Ibíd., p. 14-15.

[33] Ibíd., p. 16.
[34] Ibíd., p. 17.
[35] Ibíd., p. 18.

Por último, la décima fase que es la prueba AJAX, donde se pueden conseguir grandes beneficios en la experiencia de uso por parte de los usuarios de las aplicaciones, pero desde el punto de vista de la seguridad. Las aplicaciones AJAX tienen una superficie de ataque mayor que las aplicaciones web convencionales, a veces son desarrolladas centrándose más en qué se puede hacer que en qué se debería hacer.[36]

7.2 Procesos, Técnicas Y/O Herramientas Owasp Para Pruebas De Seguridad

Owasp cuenta con unas guías de seguridad para móvil en la cual se abordan todos los procesos, técnicas y/o herramientas que se utilizan durante las pruebas de seguridad en los dispositivos móviles, permitiendo obtener resultados consistentes y completos que ayudan a mejorar la seguridad, entre estos tenemos:

7.2.1 Guía de prueba de seguridad móvil MSTG:

Manual completo para pruebas de seguridad de aplicaciones móviles e ingeniería inversa para probadores de seguridad móvil de iOS y Android, está integrado por:

- Partes internas de la plataforma móvil
- Pruebas de seguridad en el ciclo de vida del desarrollo de aplicaciones móviles
- Pruebas de seguridad básicas estáticas y dinámicas
- Ingeniería inversa y manipulación de aplicaciones móviles
- Evaluación de las protecciones de software
- Casos de prueba detallados que se corresponden con los requisitos de MASVS.[37]

7.2.2 Masvs:

Es el estándar de seguridad y verificación de aplicaciones móviles, el cual puede ser utilizado por los arquitectos o quienes desarrollan softwares móviles y deseen que estos sean muy seguros, para probar la seguridad y confirmar la integridad y coherencia de los resultados obtenidos de las pruebas realizadas.

Por esto el MASVS Establece unos requisitos de seguridad básicos para las aplicaciones móviles:

SDLC: para establecer los requisitos de seguridad que deben seguir los arquitectos y desarrolladores de soluciones;

---

[36] Ibíd., p. 19.
[37] OWASP. OWASP Mobile Security Testing Guide. [En línea]. [Consultado: 28 de octubre de 2021]. Disponible en: https://owasp.org/www-project-mobile-security-testing-guide/

En pruebas de penetración de aplicaciones móviles: para garantizar la integridad y coherencia en las pruebas de penetración de aplicaciones móviles.

En adquisiciones: como una vara de medir para la seguridad de las aplicaciones móviles, por ejemplo, en forma de cuestionario para proveedores.[38]

7.2.3 Owasp Zap:

Escáner de seguridad web de código abierto, que busca hacer uso de este como una aplicación de seguridad y herramienta profesional para las pruebas de penetración. Es una herramienta multiplataforma, la cual se encuentra escrita en JAVA, además tiene disponibilidades en los sistemas operativos como Windows, Linux y Ubuntu. [39]

Owasp zap funciona mediante la creación de un servidor proxy, haciendo que el tráfico del sitio web pase a través del servidor. Además cuenta con escáneres automáticos en ZAP que ayudan en la interceptación de vulnerabilidades, utiliza la IP de los equipos para el análisis de vulnerabilidades.

Cuenta con unas características importantes como:

Tiene las pruebas de seguridad de código abierto más popular en el mundo.

Se mantiene activo por los voluntarios internacionales los cuales brindan un apoyo en su desarrollo y actualizaciones, su instalación es muy fácil y es disponible en 20 lenguajes diferentes.
También es una gran herramienta para las pruebas de seguridad manuales.

[38]OWASP. OWASP/owasp-masvs. The Mobile Application Security Verification Standard (MASVS) is a standard for mobile app security. [En línea]. [Consultado: 13 de octubre de 2021]. Disponible en: https://github.com/OWASP/owasp-masvs

[39] OWASPZAP. Wikipedia, la enciclopedia libre. [en línea]. [Consultado: 13 de octubre de 2021]. Disponible en: https://es.wikipedia.org/wiki/OWASP_ZAP

Figura 14: Interfax del escáner de seguridad Owasp Zap

Fuente: OWASP Zed Attack Proxy. Getting Started Guide. [En línea]. zaproxy.org/. [Consultado: 14 de abril de 2022]. Disponible en: https://www.zaproxy.org/pdf/ZAPGettingStartedGuide-2.11.pdf

7.2.4 Immuniweb® Mobilesuite

Herramienta que inmersa el top 10 de Owasp Mobile, cuenta con la integración única de aplicación móvil y sus pruebas d backend de forma consolidada, por su uso equipado con SLA de cero falsos positivos y garantía de la devolución del dinero si se encontrase un falso positivo tiene paquetes flexibles de pagos.

Esta herramienta cuenta con unas características principales que sirven para:

- Pruebas de aplicaciones móviles y backend.
- SLA cero falso positivo.
- Cumplimiento de PCI DSS y GDPR.
- Puntuaciones CVE, CWE y CVSSv3.
- Pautas de remediación procesables.
- Integración de herramientas SDLC y CI / CD.
- Parcheo virtual con un clic a través de WAF.
- Acceso 24/7 a analistas de seguridad.

A su vez ofrece en línea un escáner móvil gratuito para la detección de problemas de privacidad, verificación de los permisos en las aplicaciones, ejecución DAST / SAST y las pruebas OWASP Mobile Top 10 para los desarrolladores y pymes.

7.2.5 Mobile Security Framework (MOBSF)

Herramienta de prueba de seguridad automatizada en sistemas operativos Android, iOS y Windows. Mediante la cual se realiza el análisis estático y dinámico de pruebas de seguridad de aplicaciones móviles.

Por el avance tecnológico de la mayoría de las aplicaciones suelen utilizar los servicios web en la cual se pueden tener huecos de seguridad. MobSF trata problemas relacionados con la seguridad de los servicios web.

Esta herramienta cuenta con unas características principales que sirven para:

- Es una herramienta de código abierto para pruebas de seguridad de aplicaciones móviles.
- El entorno de prueba de aplicaciones móviles se puede configurar fácilmente con MobSF.
- MobSF está alojado en un entorno local, por lo que los datos confidenciales nunca interactúan con la nube.
- Análisis de seguridad más rápido para aplicaciones móviles en las tres plataformas (Android, iOS, Windows).
- MobSF admite código fuente binario y comprimido.
- Es compatible con las pruebas de seguridad de API web mediante API Fuzzer.
- Los desarrolladores pueden identificar vulnerabilidades de seguridad durante la fase de desarrollo.

8 GUÍA DE BUENAS PRÁCTICAS

Con la utilización e implementación de las buenas prácticas los usuarios lograran reducir los diversos ataques y/o amenazas que se enunciaron anteriormente, además es muy importante que se apliquen las recomendaciones para un uso seguro de los dispositivos móviles. Por el avance tecnológico que va en aumento día a día donde los dispositivos son utilizados frecuentemente en organizaciones, oficinas e instituciones para realizar labores propias, donde la seguridad de la información prima siendo un factor importante en lo corporativo y personal.

Seguidamente, es fundamental que se le aplique una buena configuración al sistema operativo, ya que este es el encargado de realizar las ejecución y administración de aplicaciones y recursos del sistema, para fortalecer la seguridad. Las actualizaciones del sistema. Cada vez que el fabricante realicé el lanzamiento de una versión nueva del sistema operativo, es importante actualizarlo ya que estas cuentan con parches de seguridad con los cuales se reducen las vulnerabilidades encontradas.[40]

Figura 15: Actualización de Sistema operativo

Fuente: Propia del autor

[40] WELIVESECURITY. Consejos para mitigar el impacto de amenazas en dispositivos móviles. [en línea]. [consultado: 26 de noviembre de 2021]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf

Lo anterior permite aplicar la actualización constante de las aplicaciones e instalar antivirus o antimalware desde la tienda oficial “Play Store” y no descargar e instalar aplicación de fuentes no confiable, previniendo la instalación de un software no deseado. Analizar todas las Apps que no utilice, verificar las que no sean parte del sistema y eliminarlas, previniendo que estén ejecutándose en segundo plano y sean accedidas por un software dañino.

Figura 16: Actualización de Sistema operativo

Fuente: Propia del autor

Figura 17: verificación de las aplicaciones no utilizadas

Fuente: Propia del autor

Adicionalmente como se enuncio anteriormente en las técnicas y/o herramientas para detección vulnerabilidades, intrusiones o puertos abiertos que exponga la seguridad en los dispositivos como los son mobile security framework, masvs, mobilesuite etc. En fundamental aplicar herramientas de testing como **Nmap**, para realizar un análisis del tráfico de la red. En el caso de la herramienta **Zanti**, con diversas técnicas para validad ataques como hombre en el medio, intercepción del tráfico en la red analizando todos los dispositivos conectados arrojándolos las IP y la MAC.

A continuación se listas las herramientas forenses gratuitas genéricas:

- AFLogical OSE - Open source Android Forensics app and framework: se debe instalar en la terminal de Android, para posteriormente extraer información de tarjeta SD (registro de llamadas, listado de contactos y de aplicaciones instaladas, mensajes de texto y multimedia).

- Open Source Android Forensics: es utilizado mediante máquinas virtuales permitiendo realizar análisis estático y dinámico.

- LIME- Linux Memory Extractor: ayuda a obtener la información de los sistemas basados en Linux y se puede ejecutar remotamente.

En cuanto a las gratuitas específicas se tienen:

- Android Data Extractor Lite (ADEL): Desarrollado por Python cuenta con la ventaja de obtener un flujograma forense de las BD de los dispositivos móviles.

- Skype Xtractor: Cuenta con el soporte para Linux, permite ver la información de los ficheros mian.db de Skype como chats, llamadas etc.

Para las herramientas de pago se encuentran:

- Cellebrite Touch: Es muy reconocida y cuenta con una gama de beneficios como el trabajo de más de 6.300 terminales distintos y es uy fácil su utilización.

- Oxygen Forensic Suite: Mediante la cual se logra obtener información de más de 10.000 dispositivos móviles, además de la importación de Backups e imágenes.[41]

[41] MARTÍNEZ, Asier. Incibe. Herramientas para realizar análisis forenses a dispositivos móviles. 2016. [en línea]. [consultado: 8 de diciembre de 2021] Disponible en: https://www.incibe-cert.es/blog/herramientas-forense-moviles

En el dispositivo móvil de debe comprobar que este desactivado la instalación de aplicaciones desconocidas y programas automáticamente, además realizar un análisis en el administrador de permisos verificando que Apps necesitan acceder a la información del dispositivo y cuáles no.

Figura 18: verificacion del estado para la instalacion de aplicaciones desconocidas.

Fuente: propia del autor

Figura 19: administrador de permisos

Fuente: propia del autor

Para elevar la seguridad es fundamental que a la hora de utilizar un antivirus utilicen de los más valorados en el mercado, por s eficiencia y consolidación en la detección de amenazas como en el caso de Kaspersky, AVG, Norton 360 y Bitdefender Total Security etc. Ya que todos aplican protección de datos en tiempo real, gestores de contraseña, cifrado de archivos y controles online entre otros. Además de activar todos los componentes sugeridos en el aplicativo.

También es indispensable que utilicen gestores de contraseñas, que ayuden en el guardado seguro y generaciones robustas de claves, entre las App más importantes encontramos Lastpass, Dashlane, Norton AppLock etc.

Realizar copias de seguridad permanentemente y habilitar el guardado fuera de línea, como contramedida en caso de daño en el dispositivo móvil. Implementar contraseñas en las diferentes Apps que contengan información privilegiada. No utilizar contraseñas como nombres o fechas, aplicar patrones seguros en la pantalla de bloqueo del dispositivo.

Figura 20: habilitado de copias de seguridad

Fuente: propia del autor

Figura 21: Contraseñas seguras

Fuente: propia del autor

Tener deshabilitada las conexiones inalámbricas como Bluetooth, Wi-Fi si en el momento no son necesarias, para evitar que haya una conexión con dispositivos inseguros evitando la propagación de un malware informático.

Figura 22: Deshabilitado Bluetooth, Wi-Fi

Fuente: propia del autor

No se recomienda abrir link, ni descargar archivos que lleguen por SMS, correo electrónico o de remitentes desconocido o extraño.

Realizar la navegación en páginas que tangan el protocolo https, no utilizar hipervínculos desconocidos o extraños.

Figura 23: Navegación segura

Fuente: propia del autor

Desarrollo de aplicaciones con la utilización de códigos seguros para evitar el robo de la información. Se debe cerrar sesión de usuario cada vez que se vaya a dejar de utilizar el servicio, además de no guardar contraseñas en los navegadores, cada una de las anteriores son acciones de buenas prácticas para neutralizar los diversos ataques. Cuando vaya a instalar aplicaciones en su dispositivo Android es necesario considerar su procedencia y los permisos que requieren. Es de gran importancia utilizar repositorios oficiales y confiables para las descargas. Por lo anterior, no acceder a enlaces desconocidos, aunque sean compartidos por un contacto, ya que pueden haber sido productos de alguna aplicación maliciosa que infectó al contacto. Se recomienda desactivar la ubicación GPS para las fotografías, ya que en ocasiones, como durante vacaciones, se suelen compartir fotos directamente desde el dispositivo móvil y en ellas se podrían encontrar las coordenadas exactas de la foto.

Figura 24: GPS desactivado

Fuente: propia del autor

9 CONCLUSIONES

En conclusión, el presente trabajo se analizó los riesgos de seguridad en los dispositivos móviles personales con sistema operativo Android, a partir de su arquitectura de seguridad y la guía de pruebas de seguridad móvil de Owasp, por medio de la búsqueda bibliográfica se pudo afirmar que los sistemas operativos Android, permanecen en constante actualización de sus versiones, permitiendo que los usuarios puedan obtener mejoras en cuanto a la seguridad y usabilidad.

Se realizó un analisis exhaustivo pudiendo comprender e identificar los módulos que integran la arquitectura el sistema operativo basado en Linux, en cuanto al funcionamiento de forma separada prebendó la seguridad cada vez que se ejecuta una aplicación, las cuales tienden a efectuarse por separado, brindado los recursos asignados para cada una de las capaz y de esta forma cada vez que sufra de un ataque estas no se encuentran todas expuestas a la vez, del mismo modo cada una de las aplicaciones que se ejecutan deben ser en formato APK las cuales se basan en lenguaje Java, además de las múltiples vulnerabilidades y ataques de “malware, Ransomware, Spyware, Troyanos, Gusanos, código malicioso etc. Que realizan una elevación de privilegios, secuestro y robo de información una vez efectuados, a su vez se comprende las recomendaciones según la CVE para limitar el alcance de estos ataques.

Se logra analizar que el sistema operativo Android tiene vulnerabilidades como cualquier sistema y que a lo largo del tiempo con cada versión y parches de actualizaciones nuevas que lanza su desarrollador “Google” busca corregir y prevenir las falencias y/o vulnerabilidades encontradas en las versiones anteriores de la plataforma.

Se logró analizar las metodologías y estándares de seguridad como (OASAM, OWASP, OSSTMM, ISSAF etc.), que cuentan con una capa o niveles de procesos y pueden ejecutarse a la hora de validar que tan seguro se encuentra el dispositivo en cuanto a las vulnerabilidades y detención de fallos, y de esta forma saber cuáles son las amenazas que afectan de manera constante la seguridad y privacidad de los mismos, para posteriormente implementar acciones correctivas según los hallazgos, cabe resaltar que por la falta de conocimiento y/o precaución por parte de los usuarios a la hora de descargar e instalar aplicaciones, navegar en la Web etc. Tienden a conllevarlos hacer unas victimas fijas de ataques cibernéticos.

En cuanto a la detección de fallos y vulnerabilidades según las fases de la metodología Owasp, se realizó el correcto análisis de cuán importante es la aplicabilidad de cada una las fases que cuenta esta metodología a la hora de efectuar una recopilación, analisis de información en cuanto a la seguridad, mediante pruebas que ayudarían a validar la estructura, funcionalidades, componentes de códigos fuentes, la navegabilidad segura mediantes los protocolos

de seguridad, buscando mejorar las falencias encontradas en el sistema para de esta forma aplicar las mejoras correctivas pertinentes.

Se realizó la creación de una guía de buenas prácticas que se puedan implementar para evitar riesgos de seguridad en los dispositivos móviles con sistema operativo Android, mediante la cual se detallan las recomendaciones que se deben aplicar para minimizar las diversas amenazas y/o vulnerabilidades a las que están expuestos los usuarios que utilizan dispositivos móviles con sistemas operativo Android.

Finalmente, por sus características y funcionalidades estos dispositivos móviles se encuentran en constante peligro, ya que existen piratas que están a la vanguardia y aprovechan cualquier oportunidad para realizar robos cibernéticos, donde utilizan múltiples mecanismos para lograr vulnerar la seguridad de los dispositivos, y de esta forma lograr su cometido, bien sea secuestrando y/o robando la información importante. Por otro lado conocemos de casos en donde hay personas que han perdido la vida por un dispositivo de estos, lo que nos muestra que por su costo y funcionalidades son atractivos para los ladrones.

10 RECOMENDACIONES

Tener en cuenta las políticas de seguridad al momento de explorar los sistemas operativos Android, para que el usuario final sea consciente de las medidas preventivas que deben tener en cuenta para guardar la información Indagar sobre las vulnerabilidades de los sistemas operativos Android ante la descarga de aplicaciones de terceros.

Realizar actualizaciones constantes a los dispositivos móviles con sistema operativo Android para disminuir los riesgos de seguridad a partir de su arquitectura de seguridad y la guía de pruebas de seguridad móvil de Owasp

Establecer políticas de seguridad para el manejo de los dispositivos móviles con sistema operativo Android, que el usuario pueda acceder y aplicar, donde este encuentre las medidas preventivas para manejar su información teniendo en cuenta los principios de seguridad.

BIBLIOGRAFÍA

1. ABAD, Mónica. SOLANO, Las nuevas tecnologías en la familia y la educación: retos y riesgos de una realidad inevitable. Fundación Univ. San Pablo, 2013.

2. ALBARRACIN, Juan Carlos. PARRA CAMARGO, Leidy Maribel. Y CAMAGO Vega, Juan Jose. SEGURIDAD EN DISPOSITIVOS MÓVILES CON SISTEMAS OPERATIVOS ANDROID Y IOS. Tecnología, Investigación y Academia. 2013. Disponible http://revistas.udistrital.edu.co/ojs/index.php/tia/article/view/4312

3. APONTE GOMEZ, Sanly y DAVILA RAMIREZ, Carlos. Sistemas operativos móviles: funcionalidades, efectividad y aplicaciones útiles en Colombia. [En línea]. Universidad EAN, 2011. [Consultado: 12 de abril de 2022]. Disponible en: https://repository.ean.edu.co/bitstream/handle/10882/761/AponteSanly2011.pdf?sequence=1

4. BAZ ALONSO, Arturo et al. Dispositivos móviles. [En línea]. EPSIG Ing. Telecomunicación Universidad de Oviedo, 2011, vol. 12. [Consultado: 7 de diciembre de 2021]. Disponible en: http://isa.uniovi.es/docencia/SIGC/pdf/telefonia_movil.pdf

5. BESTYGAME. Android es el objetivo de ataques masivos. [en línea]. [consultado: 8 de diciembre de 2021]. Disponible en: https://bestygame.com/es/android-es-el-objetivo-de-ataques-masivos/

6. BETANCUR JARAMILLO, Oscar y ERASO HANRRYR, Sonia Elizabeth. Seguridad en dispositivos móviles Android. [en línea]. Trabajo de grado. Universidad Nacional a Distancia, 2015. [consultado: 28 de noviembre de 2020]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/3614/59836994.pdf?sequence=1&isAllowed=y

7. CANDELA, Santiago. GARCÍA, Carmelo Rubén. QUESADA, Alexis. SANTANA, Francisco José. y SANTOS, José Miguel. Fundamentos de sistemas operativos: teoría y ejercicios resueltos. Editorial Paraninfo, 2007.

8. CIBERSEGURIDAD. Ataques Informáticos seguridad informática, redes y programación. [en línea]. [consultado: 17 de septiembre de 2020]. disponible en: https://www.cyberseguridad.net/index.php/ataques-informaticos

9. CHEKPOINT. Judy Malware: posiblemente la campaña de malware más grande encontrada en Google Play. [En línea]. [Consultado: 8 de diciembre de 2021]. Disponible en: https://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/

10. COLOMBIA.CONGRESO DE LA REPÚBLICA. Constitución política de Colombia. 1991. Gaceta Constitucional No. 116 de 20 de julio de 1991.p.150.

11. COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 DE 2008. Diario Oficial No. 47.219 de 31 de diciembre de 2008.

12. COLOMBIA.CONGRESO DE LA REPÚBLICA. Ley 1273 De 2009. (enero 5). Diario Oficial No. 47.223 de 5 de enero de 2009. Congreso De La República.p.4.

13. COLLADO, Christian. Andro4all. Android fue el sistema operativo más vulnerable de 2019 duplicando a otros como Windows 7 o Ubuntu. [en línea]. [consultado: 30 de noviembre de 2019]. Disponible en: https://andro4all.com/noticias/android/android-sistema-operativo-mas-vulnerable-2019

14. CCN-CERT. Informe Anual 2018 Dispositivos y comunicaciones móviles. [En línea]. [Consultado: 3 de septiembre de 2021]. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html

15. CHEBYSHEV, Victor. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [En línea]. [Consultado 19 de octubre de 2021]. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

16. CN-CERT. Informe Anual 2020. Dispositivos y comunicaciones móviles. [En línea]. [Consultado: en 23 de octubre de 2021]. Disponible en: https://derechodelared.com/wp-content/uploads/2021/08/CCN-CERT-IA-18-21-Informe-Anual-2020.-Dispositivos-Moviles-1.pdf

17. DOXNET. Multiple Vulnerabilities Discovered in Google Android OS. [en línea]. [Consultado 22 de octubre de 2021]. Disponible en: https://www.doxnet.com/article.cfm?ArticleNumber=62

18. EL TIEMPO. Bogotá D.C. 03, abril 2017. Android destrona a Windows como el sistema operativo más usado en red. [en línea]. [consultado: 23 de septiembre de 2019]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/android-destrona-a-windows-como-el-sistema-operativo-mas-usado-en-red-74448

19. ESET. Guía de seguridad para Usuarios de Smartphones, 2017. [En línea]. [Consultado: 28 de noviembre de 2020]. Disponible en: https://www.welivesecurity.com/wpcontent/uploads/2014/01/documento_guia_de_seguridad_para_usuarios_de_smar tphone_baj.pdf

20. FENRECK. Historia y evolución de los dispositivos móviles.2016 [en línea]. [Consultado: 28 de octubre de 2020]. Disponible en: https://fenreck.wordpress.com/2016/05/16/historia-y-evolucion-de-los-dispositivos-moviles/

21. GARCIA, Alfonso; HURTADO, Cervigón y RAMOS ALEGRE, Maria del Pilar. Seguridad informática. [En línea].Madrid (España) Edic.1.2011. [consultado: 26 de septiembre de 2020]. Disponible en https://books.google.com.mx/books/about/SEGURIDAD_INFORMATICA_ED_11_Paraninfo.html?id=c8kni5g2Yv8C

22. GUISTO, Denise. Wilivesecurity. Análisis de la seguridad en dispositivos móviles durante el primer semestre de 2019. [En línea]. [Consultado: 25 de octubre de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2019/09/03/analisis-seguridad-dispositivos-moviles-primer-semestre-2019

23. JUNTA DE ANDALUCIA. [Sitio web]. Marco De Desarrollo De La Junta De Andalucia. [Consultado 14 de octubre de 2021]. Disponible en: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.1/contenido-recurso-216.html

24. KASPERSKY. [sitio web]. Kapersky.es. Amenazas a la seguridad móvil para Android. [En línea]. [Consultado 17 de septiembre 2020]. Disponible en: https://www.kaspersky.es/resource-center/threats/mobile

25. KASPERSKY. [sitio web]. Boletin de seguridad kaspersky 2020. [En línea]. [Consultado: 25 de octubre de 2021] Disponible en: https://go.kaspersky.com/rs/802-IJN-40/images/KSB_statistics_2020_sp.pdf

26. KUMAR, Chandan. 11 Escáner de aplicaciones móviles para encontrar vulnerabilidades de seguridad. [En línea]. [Consultado en 21 de octubre de 2021]. Disponible en: https://geekflare.com/es/mobile-app-security-scanner/

27. LOPEZ CEBALLOS, Adriana *et al*. Informe de tendencias cibercrimen en Colombia (2019-2020). Bogotá D. C. Ccit.org.co. 2019-2020. [en línea]. [Consultado: 25 de octubre de 2021]. Disponible en:

https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

28. NORMAS ISO NORMA TÉCNICA NTC-ISO/IEC 27001. Bogotá, Colombia: ICONTEC [en línea]. [consultado: 22 de noviembre de 2019]. Disponible en: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf.

29. MANRIQUE LOZADA, Cristhian Jose. Análisis de la seguridad de smartphone con sistema android. [En línea]. Trabajo de grado. Universidad Nacional a Distancia, 2019. [Consultado: 16 de abril de 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/31570

30. MEDIANERO, Daniel. OASAM [En línea]. [Consultado: 30 de octubre de 2021] Disponible en: https://github.com/b66l/OASAM

31. MUÑOZ Caceres, Yamir Asmirio. Estado del arte vulnerabilidades de seguridad en sistemas operativos móviles Andrioid y IOS. [En línea]. Trabajo de grado. Universidad Nacional a Distancia, 2019. [Consultado: 13 de abril de 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/25396/%20%09yamunozca.pdf?sequence=1&isAllowed=y

32. MURILLO ARGUDO, Alejandro Julio. Estudio de la afectación a la privacidad de los usuarios que utilizan aplicaciones Android desarrolladas para instituciones públicas del ecuador. 2019. p. 165.

33. OSBORNE, Charlie. [Sitio web]. Mobile malware evolves: Adware now breaks and roots your phone. [En línea]. [Consultado: 18 de octubre de 2021]. Disponible en: https://www.zdnet.com/article/mobile-malware-evolves-adware-now-breaks-and-roots-your-phone/

34. OWASP. Guía de pruebas de OWASP 2008. Ver 3.0. [en línea]. [Consultado 30 de octubre de 2021]. Disponible en: https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

35. OWASP. OWASP Mobile Security Testing Guide. [en línea]. [consultado: 28 de octubre de 2021]. Disponible en: https://owasp.org/www-project-mobile-security-testing-guide/

36. OWASP. OWASP/owasp-masvs. The Mobile Application Security Verification Standard (MASVS) is a standard for mobile app security. [En línea]. [Consultado: 13 de octubre de 2021]. Disponible en: https://github.com/OWASP/owasp-masvs

37. OWASP´s Zed Attack Proxy. Getting Started Guide. [En línea]. zaproxy.org/. [Consultado: 14 de abril de 2022]. Disponible en: https://www.zaproxy.org/pdf/ZAPGettingStartedGuide-2.11.pdf

38. PAGLIERY, Jose. Greenwich. 1, Diciembre 2016. Más de un millón de celulares Android fueron infectados por hackers. [en linea]. [Consultado: 8 de diciembre de 2021]. Disponible en: https://cnnespanol.cnn.com/2016/12/01/mas-de-un-millon-de-celulares-android-fueron-infectados-por-hackers/

39. GAVIRIA PULGARÍN, Hermes Duvier y CARMONA Jhon Fernando. Metodología de testing de seguridad para aplicaciones móviles android, en el campo de la salud. 2018. p.183

40. QUEZADA CABALLERO, Eduardo Alonso. Introducción a OSSTMM (Open Source Security Testing Methodology Manual. [En línea]. [Consultado: 30 de octubre de 2021]. Disponible en: http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual

41. ROMANO, Agustín y LUNA, Carlos. Descripción y análisis del modelo de seguridad de Android. [En línea]. UR. FI – INCO, 2013. [Consultado: 14 de abril de 2022]. Disponible en: https://www.colibri.udelar.edu.uy/jspui/handle/20.500.12008/3475

42. SALAZAR, Edgar. Pruebas de Seguridad en aplicaciones web según OWASP. [en línea]. [Consultado: 20 de octubre de 2021]. Disponible en: https://owasp.org/www-pdf-archive/OWASP_SUSCERTE.pdf

43. SALIDO, Francisco. Android soluciona varias vulnerabilidades críticas Una al Día. [En línea]. [Consultado: 20 de octubre de 2021]. Disponible en: https://unaaldia.hispasec.com/2020/03/android-soluciona-varias-vulnerabilidades-criticas.html

44. SOFTWARE DE COMUNICACIONES. 2.2. Arquitectura Android. [En línea]. (Recuperado: 1 de septiembre de 2021.) Disponible en: https://sites.google.com/site/swcuc3m/home/android/generalidades/2-2-arquitectura-de-android

45. TARDÁGUILA, César. Dispositivos móviles y multimedia. Mosaic [en línea], julio 2006, no. 49. ISSN: 1696-3296.DOI: [Consultado: 30 de octubre de 2021]. Disponible en: https://doi.org/10.7238/m.n49.0619.

46. TECNOLOGIAMOVIL. Arquitectura de Android. [En línea]. [Consultado: 8 de diciembre de 2021]. Disponible en: https://tecnologiamovil128806266.wordpress.com/equipos/

47. TORO SANCHEZ, Cristian, et al. Guía para validar el nivel de seguridad de los permisos y uso de recursos de una aplicación móvil bajo plataformas Android. [En línea] Proyecto de grado. Universidad Católica de Colombia. Bogotá D.C. 2015. [Consultado: 29 de octubre de 2021]. Disponible en https://repository.ucatolica.edu.co/bitstream/10983/2778/1/Proyecto%20Gu%C3%ADa%20Validaci%C3%B3n%20Seguridad%20App%20M%C3%B3vil%20APA.pdf

48. Universidad Carlos III de Madrid. Programación en dispositivos móviles portables. Arquitectura Android. [En línea]. [Consultado 10 de abril de 2022]. Disponible en: https://sites.google.com/site/swcuc3m/home/android/generalidades/2-2-arquitectura-deandroid

49. UXXERMAG. Todas las versiones de Android y sus características. [En línea]. [consultado: 26 de octubre de 2020]. Disponible en: https://uxxermag.com/todas- lasversiones-de-android-y-sus-caracteristicas/

50. VELIZ, Pacheco. *et al.* Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones. [en línea]. Trabajo de grado Licenciatura en Sistemas. Universidad nacional de la plata. Facultad de informática. p.139. La plata, 2016. [en línea]. [consultado: 24 de noviembre de 2019] Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/58591/Documento_completo.%20y%20Piazza%20Orlando,%20C.%20Estudio%20y%20an%C3%A1lisis%20de%20seguridad%20en%20dispositivos%20m%C3%B3viles.pdf-PDFA.pdf?sequence=4&isAllowed=y

51. VILLA, Luis Alfonso; PONCE, Victor Hugo y SANTANA. Infraestructura de comunicaciones cliente-servidor para aplicaciones móviles. [En línea]. Instituto Politécnico Nacional. Centro de Investigación en Computación. [consultado: 17 de julio de 2021]. Disponible en: http://www.repositoriodigital.ipn.mx//handle/123456789/6095

52. WELIVESECURITY. Byod - Retos de la seguridad. [en línea] [consultado: 20 de septiembre de 2020]. Disponible en: http://www.welivesecurity.com/wpcontent/uploads/2014/01/documento_guia_byod_W.pdf

53. WELIVESECURITY. Consejos para mitigar el impacto de amenazas en dispositivos móviles. [en línea]. [consultado: 26 de noviembre de 2021].

Disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf

54. XATAKANDROID. Historia y evolución de Android: cómo un sistema operativo para cámaras digitales acabó conquistando los móviles. [en línea]. [consultado: 30 de noviembre de 2021]. Disponible en https://www.xatakandroid.com/sistema-operativo/historia-y-evolucion-de-android-como-un-sistema-operativo-para-camaras-digitales-acabo-conquistando-los-moviles

55. SHRAİM, Khitam y CROMPTON, Helen. “Perceptions of Using Smart Mobile Devices in Higher Education Teaching: A Case Study from Palestine". Contemporary Educational Technology 6. 2015. P. 301-318

56. MORILLO Pozo, Julian. [En linea]. Introducción a los dispositivos móviles. España, Universidad de Oberta de Catalunya. [Consultado: 9 de abril de 2022]. Disponible en: https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_(Modulo_2).pdf

ANEXOS

Plantilla RAE

Fecha de Realización:	Noviembre 20 de 2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Infraestructura tecnología y Seguridad en Redes
Título:	Análisis De Riesgo De Seguridad En Los Dispositivos Móviles Personales Con Sistema Operativo Android
Autor(es):	Oscar Enrique Mena Asprilla
Palabras Claves:	Dispositivos, seguridad, teletrabajo, Android, Vulnerabilidad.
Descripción:	El objetivo de la presente monografía es realizar un análisis de seguridad informática a los dispositivos móviles con sistema operativo Android, permitiendo describir los pasos y las metodologías que se deben llevar a cabo para realizar dicho análisis. También se busca identificar y conocer los principales riesgos a los que se exponen los mencionados dispositivos, teniendo en cuenta que estos por su alta tecnología se ven expuestos a ataques cibernéticos y a muchas vulnerabilidades. Esto genera mucha preocupación a los usuarios que si bien se ven atraídos por las funcionalidades que estos tienen, no son conscientes de los ataques y vulnerabilidades a los que se expone la información contenida en dichos dispositivos, debido a que no todos tienen conocimientos en sistemas. Se realiza un recorrido corto por la historia de los dispositivos móviles para después exponer el concepto de seguridad de la información a nivel de celulares y por último se citan algunas normas internacionales que permiten adaptar políticas de seguridad de la información en dispositivos móviles.

Fuentes bibliográficas destacadas:

1. GUISTO, Denise. [3 de septiembre de 2019]. Wilivesecurity. Análisis de la seguridad en dispositivos móviles durante el primer semestre de 2019. Disponible en: https://www.welivesecurity.com/la-

es/2019/09/03/analisis-seguridad-dispositivos-moviles-primer-semestre-2019/

2. 23.SALAZAR, Edgar. OWASP Venezuela Chapter Leader. Pruebas de Seguridad en aplicaciones web según OWASP. Disponible en: https://owasp.org/www-pdf-archive/OWASP_SUSCERTE.pdf

3. 26.VELIZ, Pacheco. EXEQUIEL, Sebastián. PIAZZA, Orlando. DAMIAN Carlos. Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones. 139. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/58591/Documento_completo.%20y%20Piazza%20Orlando,%20C.%20Estudio%20y%20an%C3%A1lisis%20de%20seguridad%20en%20dispositivos%20m%C3%B3viles.pdf-PDFA.pdf?sequence=4&isAllowed=y

4. FENRECK, A. Historia y evolucion de los dispositivos móviles. Disponible en: https://fenreck.wordpress.com/2016/05/16/historia-y-evolucion-de-osdispositivos-moviles/

5. CHEBYSHEV, Victor. Securelist.lat. Evolución de las amenazas informáticas en el primer trimestre de 2021 Estadísticas de amenazas móviles. [sitio web]. Securelist.lat, 2021. Disponible en: https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

Contenido del documento:	Introducción 1. Definición Del Problema 1.1 Antecedentes Del Problema 1.2 Formulación Del Problema 2 Justificación 3 Objetivos 3.1 Objetivos General 3.2 Objetivos Específicos 4 Marco Referencial 4.1 Marco Teórico 4.2 Marco Conceptual 4.3 Arco Histórico 4.4 Antecedentes O Estado Actual 4.5 Marco Legal 5 Ataques Y Vulnerabilidades Dispositivos Móviles 5.1 Arquitectura Del Sistema 5.2 Vulnerabilidades En Sistemas Operativos Android

	5.3 Ataques A Dispositivos Con Sistemas Operativos Andriod 6 Metodologias Y Estandares De Escaneo, Analisis De Vulnerabilidades Y Deteccion De Fallos Aplicados A Dispositivos Móviles Con Sistema Operativo Android. 6.1 Open Android Security Assessment Methodology -Oasam 6.2 Owasp 6.3 Osstmm 6.4 Issaf 7 Fases De La Metodología Para El Análisis De Vulnerabilidades Y Detección De Fallos De Android 7.1 Fases De Análisis De Vulnerabilidades Owasp 7.2 Procesos, Tecnicas Y/O Herramientas Owasp Para Pruebas De Seguridad 7.2.1 Guía De Prueba De Seguridad Móvil Mstg: 7.2.2 Masvs: 7.2.3 Owasp Zap: 8 Guía De Buenas Prácticas 9 Conclusiones 10 Recomendaciones Bibliografía Anexos
Marco Metodológico:	N/A
Conceptos adquiridos :	Sistema Android, Seguridad, Vulnerabilidades, Metodologías, Owasp, Herramientas, Ataques, Buenas Practicas
Conclusiones:	En conclusión, el presente trabajo se analizó los riesgos de seguridad en los dispositivos móviles personales con sistema operativo Android, a partir de su arquitectura de seguridad y la guía de pruebas de seguridad móvil de Owasp, por medio de la búsqueda bibliográfica se pudo afirmar que los sistemas operativos Android, permanecen en constante actualización de sus versiones, permitiendo que los usuarios puedan obtener mejoras en cuanto a la seguridad y usabilidad.

	Se realizó un analisis exhaustivo pudiendo comprender e identificar los módulos que integran la arquitectura el sistema operativo basado en Linux, en cuanto al funcionamiento de forma separada prebendó la seguridad cada vez que se ejecuta una aplicación, las cuales tienden a efectuarse por separado, brindado los recursos asignados para cada una de las capaz y de esta forma cada vez que sufra de un ataque estas no se encuentran todas expuestas a la vez, del mismo modo cada una de las aplicaciones que se ejecutan deben ser en formato APK las cuales se basan en lenguaje Java, además de las múltiples vulnerabilidades y ataques de “malware, Ransomware, Spyware, Troyanos, Gusanos, código malicioso etc. Que realizan una elevación de privilegios, secuestro y robo de información una vez efectuados, a su vez se comprende las recomendaciones según la CVE para limitar el alcance de estos ataques. Se logra analizar que el sistema operativo Android tiene vulnerabilidades como cualquier sistema y que a lo largo del tiempo con cada versión y parches de actualizaciones nuevas que lanza su desarrollador “Google” busca corregir y prevenir las falencias y/o vulnerabilidades encontradas en las versiones anteriores de la plataforma. Se logró analizar las metodologías y estándares de seguridad como (OASAM, OWASP, OSSTMM, ISSAF etc.), que cuentan con una capa o niveles de procesos y pueden ejecutarse a la hora de validar que tan seguro se encuentra el dispositivo en cuanto a las vulnerabilidades y detención de fallos, y de esta forma saber cuáles son las amenazas que afectan de manera constante la seguridad y privacidad de los mismos, para posteriormente implementar acciones correctivas según los hallazgos, cabe resaltar que por la falta de conocimiento y/o precaución por parte de los usuarios a la hora de descargar e instalar aplicaciones, navegar en la

	Web etc. Tienden a conllevarlos hacer unas victimas fijas de ataques cibernéticos. En cuanto a la detección de fallos y vulnerabilidades según las fases de la metodología Owasp, se realizó el correcto análisis de cuán importante es la aplicabilidad de cada una las fases que cuenta esta metodología a la hora de efectuar una recopilación, analisis de información en cuanto a la seguridad, mediante pruebas que ayudarían a validar la estructura, funcionalidades, componentes de códigos fuentes, la navegabilidad segura mediantes los protocolos de seguridad, buscando mejorar las falencias encontradas en el sistema para de esta forma aplicar las mejoras correctivas pertinentes. Se realizó la creación de una guía de buenas prácticas que se puedan implementar para evitar riesgos de seguridad en los dispositivos móviles con sistema operativo Android, mediante la cual se detallan las recomendaciones que se deben aplicar para minimizar las diversas amenazas y/o vulnerabilidades a las que están expuestos los usuarios que utilizan dispositivos móviles con sistemas operativo Android. Finalmente, por sus características y funcionalidades estos dispositivos móviles se encuentran en constante peligro, ya que existen piratas que están a la vanguardia y aprovechan cualquier oportunidad para realizar robos cibernéticos, donde utilizan múltiples mecanismos para lograr vulnerar la seguridad de los dispositivos, y de esta forma lograr su cometido, bien sea secuestrando y/o robando la información importante. Por otro lado conocemos de casos en donde hay personas que han perdido la vida por un dispositivo de estos, lo que nos muestra que por su costo y funcionalidades son atractivos para los ladrones.