SEGURIDAD EN DISPOSITIVOS MOVILES CON SISTEMA OPERATIVO ANDROID VERSION LOLLIPOP

LIDA JAZMIN CARDENAS GARZON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA (ECBTI)
PROYECTO DE SEGURIDAD INFORMATICA II
SEGURIDAD INFORMATICA
BOGOTA D.C.
2020

SEGURIDAD EN DISPOSITIVOS MOVILES CON SISTEMA OPERATIVO ANDROID VERSION LOLLIPOP

LIDA JAZMIN CARDENAS GARZON

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

Directora:
Msc. Katerine Marceles Villalba

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA (ECBTI)
PROYECTO DE SEGURIDAD INFORMATICA II
SEGURIDAD INFORMATICA
BOGOTA D.C.
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 01 de octubre de 2020

DEDICATORIA

Con amor dedico éste trabajo a mi hija, 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 mas 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.

TABLA DE CONTENIDO

pág.

LISTA DE FIGURAS

ANEXOS

pág.

GLOSARIO

AMENAZA: Posibilidad de generar o producir un daño.

ANTIVIRUS: Software creado con la intención de proteger de los daños que pueda ocasionar un virus.

ATAQUE: Acción orientada a causar perjuicios.

CIBERDELINCUENTE: Delincuente informático.

CRYPTOLOCKER: Descarga de un virus que se realiza al abrir un enlace o archivo adjunto situado en el correo electrónico.

CRYPTOWALL: Virus que se descarga al ingresar a sitios web maliciosos o aceptando actualizaciones falsas de sistema o aplicaciones.

DISPOSITIVO MOVIL: Aparato de tamaño apto para ser portado, con capacidades como conexión a una red.

HACKER: Persona discreta con altas capacidades de aprendizaje y absorción de información cuyo objetivo es obtener información.

IPC: Inter Process Communication es decir Comunicación entre procesos.

KERNEL: Médula de un sistema operativo.

MALWARE: Software escrito específicamente para dañar e infectar el sistema host.

PC: Computadora Personal.

PHISHING: Envío de correos electrónicos fraudulentos en los cuales son usados nombres de empresas, personas, anuncios falsos entre otros.

RANSOMWARE: Programa maligno que codifica información almacenada en los dispositivos electrónicos.

RIESGO: Posibilidad de estar en peligro.

SKIMMING: Hurto a través de exploración y escaneo de una información específica.

SMARTPHONE: Teléfono inteligente.

SMISHING: Práctica de adquirir información confidencial mediante mensajes de texto enviados a los usuarios de telefonía móvil.

SO: Sistema Operativo.

SOFTWARE: Programa o parte lógica que permite el funcionamiento de un hardware o dispositivo.

SPOOFING: Suplantación.

TRASHING: Rastrear y buscar información como contraseñas o directorios.

VIRUS: Software creado con la intención de ocasionar daños en un dispositivo o la información contenida en él.

VULNERABILIDAD: Falencia o posibilidad de permitir el acceso a algo indeseado.

WEB SPOOFING: Sitio web falso al que un usuario de la red es redireccionado para que éste entre y sean monitoreadas sus acciones.

RESUMEN

Esta monografía tiene como propósito llevar a cabo un estudio documental relacionado con el tema correspondiente a seguridad en dispositivos móviles que utilizan sistema operativo Android Lollipop y su evolución hasta el sistema operativo Android versión 10, en ese sentido se busca investigar e identificar los ataques, riesgos y vulnerabilidades a los que se encuentran expuestos dichos dispositivos con el sistema operativo mencionado y que se pueden presentar con la descarga de aplicaciones o actualizaciones; así mismo se pretende analizar la información, con el fin de evaluarlo y orientarlo al análisis del impacto que generan dichas inseguridades, como también dar a conocer la información para la mitigación de la inseguridad tanto de los dispositivos como de la información almacenada en estos.

Con el constante cambio y avances de las tecnologías y teniendo en cuenta que en la actualidad las labores cotidianas, tanto personales como laborales se prestan para ser realizadas a través de aparatos compatibles con las mejoras tecnológicas, los cuales se convierten en un objetivo de ataque dependiendo de la intención del hacker informático, lo que permite asumir la valides de indagar sobre la información que los usuarios alojan en los medios electrónicos usados por ellos y la pertinente seguridad que le otorgan a la misma.

Teniendo en cuenta lo anterior se llega al objetivo de consolidar la información, dando a conocer el análisis realizado a lo relacionado con esta versión de Android para dichos aparatos y así brindar una investigación adecuada para fomentar y animar a poner en práctica un correcto manejo de controles para la seguridad tanto del hardware como del software de dichos terminales y la información contenida en ellos.

En conclusión, con esta investigación se busca conocer el nivel de seguridad de los dispositivos móviles que utilizan el sistema operativo mencionado.

PALABRAS CLAVE: Sistema Operativo, Ataques, Riesgos, vulnerabilidades.

ABSTRACT

The purpose of this monograph is to carry out a documentary study related to the topic of security in mobile devices that use the Android Lollipop operating system and its evolution up to the Android operating system version 10, in that sense it seeks to investigate and identify attacks, risks and vulnerabilities to which said devices are exposed with the aforementioned operating system and that may occur with the download of applications or updates; Likewise, it is intended to analyze the information, in order to evaluate it and orient it to the analysis of the impact generated by said insecurities, as well as to publicize the information to mitigate the insecurity of both the devices and the information stored in them.

With the constant change and advances in technologies and taking into account that today daily tasks, both personal and work, lend themselves to be carried out through devices compatible with technological improvements, which become a target of attack depending on of the intention of the computer hacker, which allows to assume the validity of inquiring about the information that users host in the electronic media used by them and the pertinent security that they grant to it.

Taking into account the above, the objective of consolidating the information is reached, making known the analysis carried out regarding this version of Android for said devices and thus providing adequate research to encourage and encourage the implementation of a correct handling of controls for the security of both the hardware and the software of said terminals and the information contained in them.

In conclusion, this research seeks to know the level of security of mobile devices that use the mentioned operating system.

KEY WORDS: Operating System, Attacks, Risks, vulnerabilities.

INTRODUCCION

En un artículo publicado el 17 de marzo de 2017 por el tiempo, en su sección de economía y negocios titulado “En el país hay más hogares con celular que con acueducto”[1], indica que en Colombia aproximadamente el 96,5 % de hogares cuenta como mínimo con un celular en casa. Estos aparatos también llamados dispositivos móviles son usados a nivel mundial y así como en los PC se utiliza un sistema operativo, en los dispositivos móviles también, para éstos el sistema operativo más usado es Android.

Estos dispositivos son usados para tareas cotidianas tanto personales como laborales, se han vuelto necesarios y son utilizados por personas de diferentes rangos de edad en todo el mundo.

Teniendo en cuenta que en ellos se maneja todo tipo de información, se vuelven foco de numerosas amenazas, fallas, riesgos y vulnerabilidades, aprovechando que los usuarios no tienen el conocimiento o la experticia para reconocer si están en riesgo o no, ó simplemente no se percatan de las amenazas que los rodean, esto evidencia la necesidad de profundizar en dichos ataques, consolidando la información recopilada y dándola a conocer, para que los usuarios finales tengan mayor conocimiento y por ende busquen la manera de implementar mayores controles de seguridad, mitigando y contrarrestando dichos riesgos y así logrando de alguna manera poner un alto a los ciberdelincuentes.

Estos riesgos conllevan a un impacto económico por la pérdida de datos o información privada y relevante para el individuo, así como un impacto social pues afecta directamente a los usuarios, por ello con este documento se pretende contribuir al conocimiento, comprensión y discernimiento de esta situación, verificando los riesgos y vulnerabilidades a los que se encuentra expuesto el sistema operativo Android Lollipop.

[1] ECONOMIA Y NEGOCIOS, En el país hay más hogares con celular que con acueducto. [En línea]. Bogotá: El tiempo.com. 2018., Disponible en: http://www.ventics.com/estadisticas-uso-android-paises/

1. DEFINICION DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Sistema Operativo en adelante denominado S.O., es un software que permite el funcionamiento de las máquinas que requieren de éste para su funcionamiento, en una gran cantidad de dispositivos móviles el S.O. más utilizado es Android, él permite almacenamiento, edición y reproducción de diversos datos e información, además de realizar y ejecutar numerosas tareas, debido a que la información es uno de los activos más importantes de una compañía o persona, por no decir que el activo prácticamente invaluable en tema monetario, pues es con lo que toda compañía o individuo realiza sus actividades, labores, procesos y mejoras. Todo sujeto debe ser consiente que si les llegasen a modificar, eliminar o secuestrar dicho activo, estarían corriendo un riesgo bastante alto, incluso pueden llegar a la pérdida total de sus datos.

A través del S.O. mencionado se pueden ejecutar descargas gratuitas tanto de aplicaciones como de actualizaciones para este S.O., por ende también se incrementa la posibilidad de abrir las puertas a archivos adjuntos, virus o programas maliciosos, así mismo se presenta una amplia eventualidad y riesgos en la seguridad tanto de los dispositivos móviles, como de la información almacenada en éstos, dando extensas oportunidades a los hackers informáticos para el acceso ilícito y posterior uso inadecuado de información relevante para ellos, los usuarios de este software, generalmente no son conscientes de los riesgos y vulnerabilidades a los que están expuestos y por lo general tampoco tienen discernimiento de cómo prevenirlos o contrarrestarlos.

1.2 FORMULACION DEL PROBLEMA

Para el año 2018 en la sección de tecnología de la pagina ABC, en su artículo acerca de las amenazas en Android indicó “Más de tres millones de aplicaciones maliciosas han afectado a dispositivos con sistema operativo Android durante los nueve primeros meses de 2018, cifra que ya supera las amenazas identificadas a lo largo de 2017, a un ritmo de 11.700 «apps» maliciosas nuevas al día”[2]. Lo anterior, da un cierto panorama de intranquilidad en cuanto a la seguridad de la información relacionada con los dispositivos que cuentan con dicho sistema operativo. Basándose en éste tipo de publicaciones es valido formular la siguiente pregunta

[2] ABC REDES. Las amenazas en Android no dejan de crecer: hay 11.700 aplicaciones nuevas al día [En línea]. Madrid: Abc.es. 2018., Disponible en: https://www.abc.es/tecnologia/redes/abci-amenazas-android-no-dejan-crecer-11700-aplicaciones-maliciosas-nuevas-201811121812_noticia.html#vca=mod-sugeridos-p1&vmc=relacionados&vso=android-sigue-siendo-un-coladero-de-apps-maliciosas&vli=noticia.foto.tecnologia

¿De qué manera es posible identificar la seguridad que ofrece el Sistema Operativo Android Lollipop y sus versiones posteriores, para los usuarios del mismo?

2. JUSTIFICACION

Un dispositivo móvil es como una especie de mini computador (PC), lo que permite usarlos a nivel mundial para tareas cotidianas tanto personales, educativas como profesionales y laborales, estos se han vuelto prácticamente una necesidad, siendo usados por personas de diferentes rangos de edad, dichos terminales tienen a su servicio sistemas operativos como Android o IOS, de acuerdo con un artículo de Juan Antonio Pascual del 7 de Julio del 2018, publicado en la revista Computer Hoy, muestra como para el 2017 un 85.9% de teléfonos inteligentes fueron vendidos con sistema operativo Android, frente a un 16% con IOS, así como también revela que "Android sufre un problema crónico de fragmentación: sus últimas versiones no las usa casi nadie o tardan años en implantarse, porque hay muchos terminales antiguos o poco potentes. Los fabricantes tardan meses en adaptar la nueva versión por culpa de las capas personalizadas de Android, si es que lo hacen"[3].

Por otro lado, el pasado 8 de noviembre de 2017, en la sección Tecnosfera del periódico El Tiempo en línea, con respecto al uso del celular, según una encuesta realizada por Asomóvil (Asociación de la Industria Móvil de Colombia), revela que "el celular es el principal medio de información del 66 por ciento, mientras que 37 por ciento encuentra bastante relación entre el uso del celular y su productividad laboral. Entre tanto, 70 por ciento considera que los smartphones ayudan a enfocarse en las labores cotidianas, mientras que para 29 por ciento genera un efecto contrario"[4].

El 3 de enero del 2018, en el segmento de Tecnosfera, se dio a conocer que Android fue el SO con mayor vulnerabilidad, tal como lo indica el fragmento de su artículo informando que "las amenazas en la Play Store no han dejado de ser frecuentes; por el contrario, son comunes los casos de troyanos disfrazados de apps benignas que logran saltar los controles de seguridad de Google para afectar a los usuarios"[5].

Así como también de acuerdo con la sección entérate de Gobierno en Línea, Adrian Acosta un miembro de la Interporl de Argentina, dedicado al crimen digital "expuso

---

[3] PASCUAL, Juan. Android vs iPhone: la guerra de los smartphones en cifras [En línea]. Computer Hoy. 2018., Disponible en: https://computerhoy.com/reportajes/industria/android-vs-iphone-guerra-smartphones-cifras-271447 .

[4] TECNOSFERA. Vida social, en lo que más usan los colombianos el celular. [En línea]. Bogotá: El Tiempo.com. 2017., Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/uso-del-celular-y-el-internet-en-colombia-149384 .

[5] TECNOSFERA. Android, el sistema operativo con más vulnerabilidades en 2017. [En línea]. Bogotá: El Tiempo.com. 2018., Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/android-fue-el-sistema-operativo-con-mas-vulnerabilidades-en-2017-167314 .

los principales riesgos que existen en la red y los desafíos que traen tecnologías emergentes, las cuales son utilizadas por criminales para captar información personal y afectar la economía de las personas, las empresas y las entidades públicas"[6].

Por lo anterior, se evidencia la importancia de investigar, analizar, consolidar y dar a conocer las falencias, fallas, riesgos y vulnerabilidades que se puedan presentar, para verificar éste tema y reconocer si están en riesgo o no, dar a conocer al usuario dicha información, determinando si este SO (Sistema Operativo) es o no seguro, para que los usuarios finales tengan mayor conocimiento y por ende busquen la manera de implementar mayores controles de seguridad, mitigando y contrarrestando los posibles riesgos. Debido a que estos riesgos conllevan a un impacto económico por la pérdida de datos o información, así como un impacto social pues afecta directamente a los usuarios y por ello es preciso contribuir al conocimiento, comprensión y discernimiento de esta situación.

[6] GOBIERNO EN LÍNEA. Las tecnologías emergentes serán fundamentales para combatir el cibercrimen en Latinoamérica [En línea]. Bogotá: Entérate. 2018., Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/w3-article-80353.html

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un estudio del sistema operativo Android Lollipop y su evolución hasta la versión 10, para establecer la seguridad de la información que ofrece en los dispositivos móviles.

3.2 OBJETIVOS ESPECIFICOS

Analizar información del sistema operativo Android Lollipop y su evolución hasta la versión 10, mediante búsqueda en medios electrónicos y de soporte de este, para estimar la seguridad a la información que ofrece este sistema operativo al usuario.

Identificar vulnerabilidades y amenazas frecuentes al sistema operativo Android Lollipop y su evolución hasta la versión 10, mediante la búsqueda de información de incidentes, para clasificar finalidad y alcance de estos.

Proponer un manual de buenas prácticas de usuario, que permita mitigar los riesgos de la información asociados al sistema operativo Android Lollipop hasta la versión 10.

4. MARCO REFERENCIAL

Para el desarrollo de este estudio monográfico se hace necesario tener en cuenta los siguientes marcos, complementando aspectos fundamentales.

4.1 MARCO TEORICO

4.1.1 Ataques más comunes al Sistema Operativo Android: Para los usuarios de sistema operativo Android, existe una especie de tienda virtual, donde se pueden adquirir una diversidad de aplicaciones tanto gratuitas como con algún costo. En esta se puede encontrar una gran variedad de aplicaciones para todo tipo de gustos y de actividades, como por ejemplo: arte, diseño, belleza, compras, redes sociales, deportes, entretenimiento, fotografía, música, salud, viajes, en fin prácticamente para cualquier cosa que se ocurra encuentran un gran número de aplicaciones.
En noviembre de 2018, en la página del tiempo en la sección de Tecnósfera, fue publicado un artículo, en el cual dan a conocer que la compañía de ciberseguridad ESET, en el último semestre de 2018 identificó 29 apps, en la tienda virtual ya mencionada, las cuales contenían malware que robaban datos bancarios, utilizando código HTML el artículo dice “los cibercriminales que las crearon no solamente suplantaban instituciones financieras legítimas para robar las contraseñas sino que utilizaban complejas técnicas como por ejemplo: poder interceptar y redirigir mensajes de texto para evadir sistemas de doble factor de autenticación”[7]. Estas aplicaciones aparentaban ser para lectura de horóscopo, manejo de la batería, incluso aumento de rendimiento para el dispositivo.

Así como en los pc portátiles o de escritorio, en los dispositivos móviles también están expuestos a ataques, los más frecuentes se presentan a continuación:

Aplicaciones falsas: Aunque parezca difícil, no es imposible que los ciberdelincuentes logren incorporar aplicaciones falsas en la tienda play store, desde donde se cree estar descargando las apps de manera segura, aunque google se esfuerza por mantener seguridad. Pues sí, aquí también se encuentra peligro, tal es así que desde la plataforma de información sobre ciberseguridad The Hacker News, el pasado 3 de noviembre de 2017, Swati Khandelwal indicó que desde esta tienda oficial, se estaba descargando una aplicación de whtasapp falso “*According to Redditors, who first spotted this fake app on Friday, the app was not a chat app;*

[7] TECNOSFERA. Descubren 29 aplicaciones en Android que robaban datos bancarios. [En línea]. Bogotá: Eltiempo.com. 2018., Disponible en: http://origen.pre.eltiempo.com/tecnosfera/apps/29-apps-maliciosas-que-roban-sus-datos-bancarios-288478

instead, it served Android users with advertisements to download other apps"[8]. Que traduce… "Según Redditors, quien vio por primera vez esta aplicación falsa el viernes, la aplicación no era una aplicación de chat; en cambio, sirvió a los usuarios de Android con anuncios para descargar otras aplicaciones". Los usuarios creían descargar una actualización de la famosa red social Whatsapp, pero esta era una falsa aplicación dispuesta allí usando el nombre original, por un falso desarrollador de dicha app, cabe aclarar que tan pronto la tienda oficial se percató de dicha situación, procedió a la eliminación de esta falsa app.

Por otra parte está la Ingeniería Social, como es el caso cuando las personas se delatan, en una conversación cualquiera con un grupo de amigos, surge un tema, donde empiezan a hablar de las claves y oh sorpresa, empiezan a decir cuál es la técnica que utilizan para asignar claves a sus redes y aplicaciones, ¿Pecan por inocentes? No, pecan por ingenuos, pues creen que la conversación se dio ahí y que ahí murió, pero no se detienen a pensar si los que están dentro de la conversación son sus propios enemigos o si alguien está cerca escuchando y ni cuenta se han dado.

Por otro lado, en ocasiones se suele utilizar la misma contraseña para varios programas, redes o aplicaciones, pues les gana la pereza mental y les falla la memoria, error fatal, pues en algún momento han revelado la información de esta a alguien por un afán o cualquier otra situación que les haya llevado a esto, sin percatarse de que dicha contraseña la utilizan para otras cosas que no desean puedan tener acceso, pero si el enemigo está cerca, puede utilizar su tiempo y la información para intentar acceder a lo que le interesa y culminar el objetivo que lo incentiva.

El 21 de diciembre de 2017, el diario milenio informó que especialistas de Kaspersky Lab advirtieron acerca de un troyano llamado Loapi, el cual según indica éste artículo "se está difundiendo a través de campañas publicitarias bajo la apariencia de soluciones antivirus o de aplicaciones para adultos"[9], para lo cual reveló que dicho malware es apto para resguardarse a sí mismo, por lo tanto no permite que el usuario del equipo revoque sus permisos como administrador, ni su

[8] KHANDELWAL, Swati, Fake WhatsApp On Google Play Store Downloaded By Over 1 Million Android Users [En línea]. The Kacker News. 2017., Disponible en: https://thehackernews.com/2017/11/fake-whatsapp-android.html

[9] DPA. Nuevo virus de Android podría dañar físicamente tu teléfono [En línea]. Madrid: Milenio 2020. 2017., Disponible en: http://www.milenio.com/estilo/nuevo-virus-de-android-podria-danar-fisicamente-tu-telefono

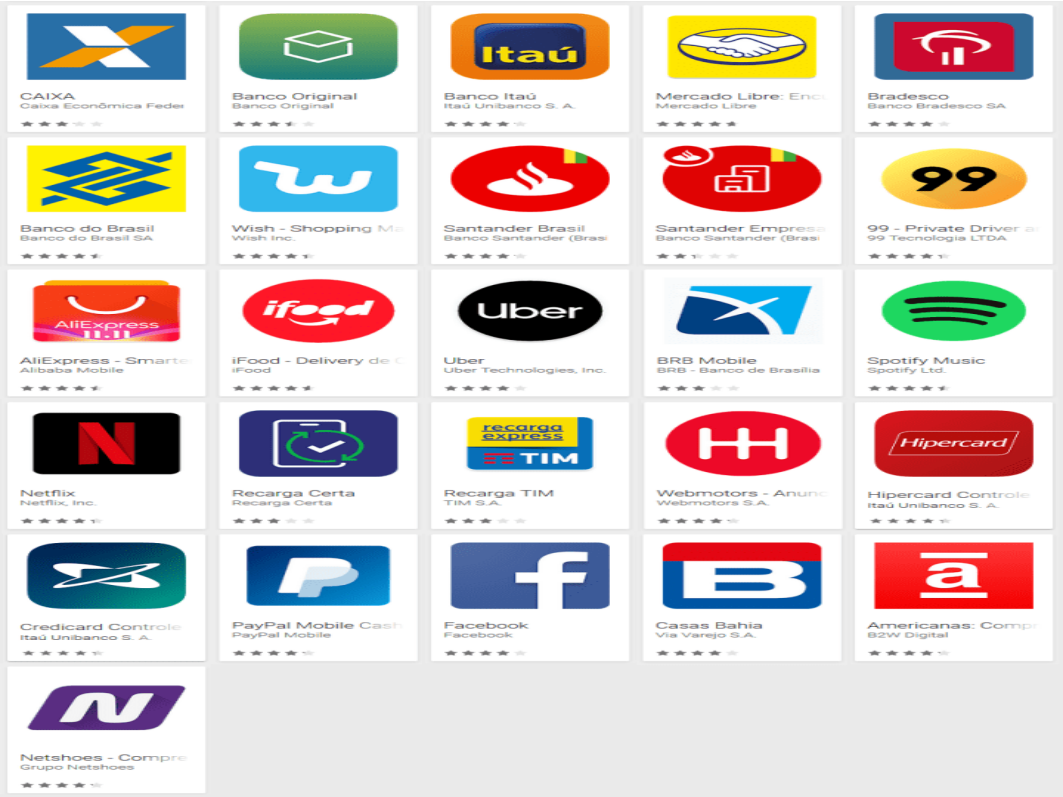
eliminación, mostrando falsos y repetitivos mensajes. Aparentemente la finalidad de los cibercriminales era tomar el control del dispositivo y robar información, pero con lo que no contaron es que éste troyano tiene la capacidad de implantar tanto trabajo en el dispositivo que la batería se puede sobrecalentar y averiar, estropeando el aparato y por ende perdiendo el control del mismo.

Según una publicación de Juan Manuel Harán el 30 de octubre de 2018, realizada en la página de welivesecurity, el investigador Lukas Stefanko de ESET, puso en conocimiento la existencia de un virus bancario, en la tienda de Google Play, destinado a usufructuarios de Android en Brasil, en el cual indica "Una vez instaladas, estas aplicaciones solicitaban a los usuarios la activación de los servicios de accesibilidad. De esta manera, el malware lo que hace es obtener el nombre y el contenido de aplicaciones legítimas que han sido ejecutadas. El objetivo de estas aplicaciones es engañar a los usuarios para que ingresen sus credenciales en el marco de una falsa actividad provocada por la infección. En este sentido, esta familia de troyanos tiene como fin afectar a unas 26 aplicaciones móviles legítimas, de las cuáles no todas son apps bancarias, sino también financieras, de entretenimiento, para social media, compras online, entre otras".[10]

A continuación, se puede evidenciar un listado de las apps afectadas por dicho malware:

[10] HARAN, Juan Manuel, Descubren malware bancario en Google Play dirigido a usuarios de Brasil [En línea]. Bogotá: Welivesecurity. 2018., Disponible en: https://www.welivesecurity.com/la-es/2018/10/30/descubren-malware-bancario-google-play-dirigido-usuarios-brasil/

Figura 1. Apps afectadas por virus bancario



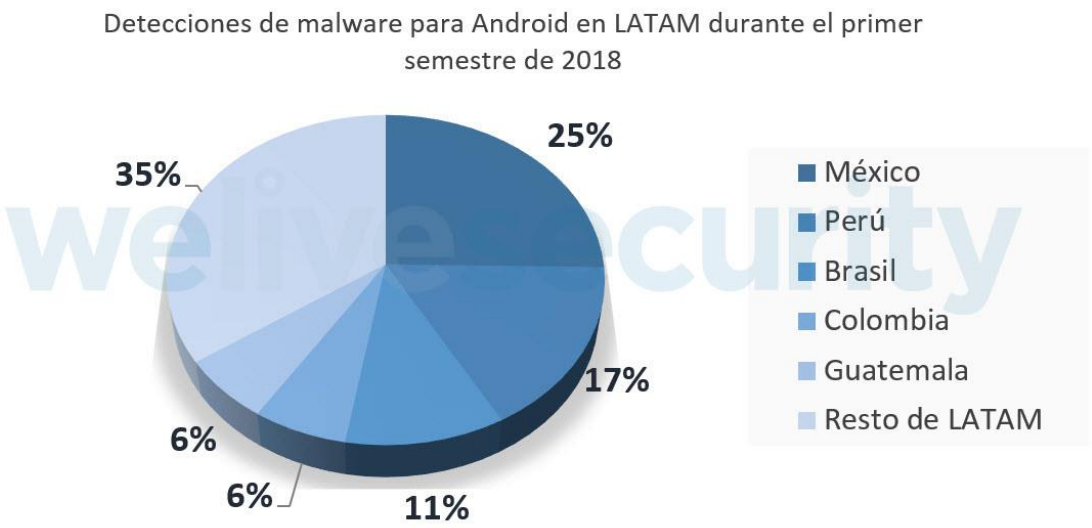
Fuente: HARAN, Juan Manuel. Descubren malware bancario en Google Play dirigido a usuarios de Brasil [imagen]. Welibersecurity.2018. Disponible en: https://www.welivesecurity.com/la-es/2018/10/30/descubren-malware-bancario-google-play-dirigido-usuarios-brasil/

Al parecer los desarrolladores de dicho código malicioso, no realizaron resguardo alguno para impedir la eliminación de estas aplicaciones, por lo que aparentemente lo único que se debe hacer es el proceso normal de desinstalación de las apps.

En una publicación de Giusto Denise, de agosto 6 de 2018, muestra una estadística con respecto a las detecciones de malware donde indica, “Si tomamos en cuenta solamente detecciones en países latinoamericanos, en 2018 los países con mayores detecciones fueron México (25%), Perú (17%) y Brasil (11%)”[11], observando que en cuanto a detección de malware se refiere, Colombia se encuetra en seguida de éstos paises, lo anterior tan solo para el primer semestre del año correspondiente a la publicación. Tal y como se muestra en la siguiente imagen:

[11] GIUSTO, Denise, Balance semestral de la seguridad móvil [En línea]. Bogotá: Welivesecurity. 2018., Disponible en: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/

Figura 2. Estadística detecciones de malware



Fuente: GIUSTO B, Denise. Seguridad en Android [imagen]. Welibesecurity. 2018. Disponible en: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/

4.1.2 Riesgos de seguridad en el Sistema Operativo Android. Recordando un artículo de Miguel Ángel Mendoza para una revista de seguridad de la información de la Universidad Nacional Autónoma de México llamado Riesgos de Seguridad en Android, hablando de las vulnerabilidades del software menciona "En cuanto al sistema operativo Android, generalmente las vulnerabilidades afectan de manera particular solo a algunas versiones del sistema y pueden ir desde permitir el acceso a la memoria física del dispositivo, hasta otorgar privilegios de administrador sobre el mismo"[12]. Lo que quiere decir que la seguridad se divide en dos tipos, tal y como se observa a continuación:

- La Seguridad lógica que se encarga de restringir y asegurar el software y la información que cada uno almacene, así como controlar quien accede a este y que manejo realiza, por ejemplo: se utilizan Controles de acceso, los cuales se encargan de la identificación y autenticación en el sistema, lo que permite prevenir el ingreso de personas no autorizadas.

Por otro lado se pueden definir roles, con ciertos permisos y modalidades de acceso, indicando que se le permite al usuario realizar frente a la información, tales como (lectura, escritura, ejecución, borrado, creación y búsqueda), así como también se

[12] MENDOZA LOPEZ, Miguel. Riesgos de Seguridad en Android. [En línea]. México: Universidad Nacional Autónoma de México. 2015,, Disponible en: https://revista.seguridad.unam.mx/numero23/riesgos-de-seguridad-en-android

realiza una generación de claves para llevar a cabo una transacción con cierta seguridad.
También se ejecutan Limitaciones a los servicios, mediante restricciones según la aplicación o el administrador del sistema.

- La seguridad física que se encarga de aplicar medidas para prevenir y controlar la información y proteger el hardware frente a una amenaza natural o una amenaza ocasionada por el hombre, como pueden ser los Desastres naturales tales como: Incendios que pueden ser provocados por manejos inadecuados de sustancias, de la parte electrónica o acumulación y filtración de líquidos o suciedad.

Así mismo se debe llevar a cabo una Seguridad del equipamiento, como por ejemplo: la temperatura adecuada y según el límite de humedad, la verificación de los conectores usados, como el cableado en cuanto a Interferencia por acción de campos eléctricos, el corte de cables y su correcto estado.

Dentro del uso de estas técnicas también se genera el uso inadecuado dado por el ser humano, ya sea de manera consciente o inconsciente, con o sin conocimientos, quien dependiendo de sus intensiones puede causar daños o robar información, generalmente sin que los afectados se percaten de dicha situación.

Entre los ataques más comunes uno de los más fáciles y usuales vistos por la mayoría de las personas es el **uso de información personal en cuentas falsas**, en las cuales se usan datos de una persona con fines ilícitos, en estas cuentas se usa información muy básica, la cual se puede obtener por diferentes medios, los más usados son las redes sociales, cuentas de correo, aplicaciones de mensajería instantánea etc. Debido a que en las redes sociales se puede configurar sus datos personales sin tener restricción alguna, este tipo de suplantación de identidad resulta ser muy convincente y difícil de detectar para otras personas.

Otro ataque de suplantación común en internet es el llamado "**phishing**", este método consiste en enviar correos electrónicos en los cuales son usados nombres de empresas, personas, anuncios falsos entre otros, estos mensajes solicitan al usuario diligenciar sus datos para poder acceder a sus cuentas, verificar datos los cuales son muy confidenciales u obtener premios, algunos usuarios no reconocen estos mensajes falsos, dejando expuesta su información y resultan siendo víctimas de grandes estafas. Entre los diferentes ataques de suplantación de identidad uno de los más eficaces y rápidos es el "**web spoofing** " este ataque consiste en enviar un link falso al usuario el cual lo re-direcciona a una página en común en la cual el usuario conoce y confía, ya estando vinculado en esta página el usuario puede usar sus servicios como si fuese la página real, pero al momento de redireccionar algún ingreso de cuenta el usuario es redireccionado a otra página al azar, para algunas personas es muy fácil saber que su información ha sido robada, otras piensan que

fue un simple error y no toman las precauciones necesaria para evitar ser estafados, suplantados entre otras acciones que se puede realizar con su información privada.

4.2 MARCO CONCEPTUAL

A continuación, se presentan los conceptos principales a tener en cuenta en este trabajo: Android, Dispositivos móviles, riesgos, amenazas y vulnerabilidades.

4.2.1 Android. Es un sistema operativo desarrollado con código abierto basado en Linux, especialmente para dispositivos móviles, para el 2005 fue comprado por Google, según venTICs.com Android "En el pasado hubo intento de terminales móviles usando 27able pero no calaron hasta que las tecnologías comenzaron a hacer más amigables los dispositivos, como por ejemplo: el uso de color, pantallas táctiles, bluetooth, wifi, alta velocidad, entre otros"[13]; adicionalmente comenta que Android tiene un uso bastante considerable en países con diversos mercados, complicados y muy exigentes, como lo son: Japón, Australia, Estados Unidos, Francia, Alemania, China, Italia, España, llegado a este punto indica que presentan al 2017 una participación considerable de este S.O.

4.2.2 Dispositivo móvil. Un dispositivo móvil es una especie de pc con contenidos de software, procesamiento, almacenamiento, conexión a internet y su principal característica que es pequeño para facilitar su portabilidad.

Entre los dispositivos existentes que permiten el uso del internet, se encuentran los dispositivos móviles, los cuales para su funcionamiento hacen uso de S.O, entre ellos el sistema operativo Android.

4.2.3 Riesgo. Riesgos, amenazas y vulnerabilidades, en este orden de ideas, el riesgo informático es la probabilidad de que se presente una amenaza haciendo la vulnerabilidad un hecho y no una hipótesis, generando daños y pérdidas importantes, la manera más factible de prevenir estos riesgos es el control informático y desarrollo con acciones, las cuales ayudan a supervisar toda la información, las funciones y actitudes de los procesos que se llevan a cabo con el fin de verificar si se están siguiendo los controles adecuados para identificar y evitar los eventos potenciales que puedan afectar a los datos y la información.

En la actualidad las tecnologías brindan diversas opciones, entre ellas la conexión a internet con una serie de facilidades nunca antes imaginadas. No obstante, así como brindan beneficios, también deja expuestos a una serie de riesgos, amenazas, vulnerabilidades y peligros.

El Nuevo diario en su artículo de Tecnología Empresarial dice lo siguiente "Los avances tecnológicos hacen que se cuente con más herramientas para combatir los

[13] VenTICs.com. Estadísticas de uso de Android por países. [En línea]. 2018., Disponible en: http://www.ventics.com/estadisticas-uso-android-paises/

ataques, pero cada día es más evidente que el factor humano es el talón de Aquiles de la seguridad de la información"[14].

Con la existencia de los anteriores elementos o componentes, en los dispositivos móviles con S.O. Android, a través de internet se pueden realizar descargas de múltiples aplicaciones y llevar a cabo su posterior ejecución, hasta aquí el panorama es realmente satisfactorio, pues se esta pasando por alto el hecho de las consecuencias que más adelante se pueden enfrentar y la importancia de los controles y cuidados que se deben tener en cuenta para evitar ser víctimas de ciberdelincuentes, los cuales pueden aprovecharse de la instalación de dichas aplicaciones y del uso del internet, para atacar a través de dichas herramientas.

Con los avances tecnológicos se generaron diversas formas y canales de interacción, apareciendo con ello la facilidad de realizar varias actividades en las redes, las cuales se pueden manipular para uso personal o profesional, estos pueden tener una connotación positiva o negativa dependiendo del uso dado por el ser humano, dichos medios tienen ventajas y desventajas, puesto que si no se saben utilizar se pueden correr bastantes riesgos, que incluso pueden traer consigo consecuencias muy graves.

Según Henry Villa en su proyecto de investigación relacionado con vulnerabilidades en los dispositivos móviles Android dice "El sistema operativo Android por defecto asegura las aplicaciones ejecutándoles dentro de un entorno aislado, y para la comunicación entre ellas hace uso de un sistema de mensajería (intents)"[15].

En Colombia se tipificaron los delitos informáticos con la Ley 1273 de 2009, los delitos informáticos han sido acogidos por los delincuentes, debido a su facilidad de cometer el crimen y pasar inadvertido, con el fin de encontrar las vulnerabilidades de los sistemas para ser accedidos por ellos y realizar sus actividades malintencionadas, causando daños o robando información.

Existen factores que por sus características generan un ambiente propicio para los ciberdelincuentes y son los siguientes:

---

[14] TECNOLOGÍA EMPRESARIAL. El Factor humano como amenaza interna a la seguridad de la información [En línea]. Managua: El Nuevo Diario. 2013., Disponible en https://www.elnuevodiario.com.ni/economia/300466-factor-humano-amenaza-interna-seguridad-informacio/

[15] VILLA YAÑEZ, Henry y CISNEROS BARAHONA, Andres. Detección de vulnerabilidades en aplicaciones que funcionan sobre el sistema operativo Android, mediante el desarrollo de una aplicación tecnológica. [En línea]. Revista Espacios. 2017., Disponible en: http://www.revistaespacios.com/a18v39n11/18391107.html

4.2.4 Anonimato. Debido a que es fácil pasar inadvertido con los delitos informáticos los criminales cibernéticos se sienten atraídos por este tipo de delito.

4.2.5 Jurisdicción legal inadecuada. La falta de normatividad adecuada o la normatividad débil y poco precisa, por causa de los avances tecnológicos con rapidez y frecuencia, son una tentación significativa para este tipo de criminales.

4.2.6 Crimen Vs Tecnología. El crimen es bastante antiguo, pero con la implementación de la tecnología y sus constantes avances, los criminales se aprovechan de esta, para ejecutar sus delitos.

4.2.7 Sentimientos negativos. Cuando una persona guarda rencor o resentimiento hacia otra, se siente atraído por este tipo de delitos con el fin de causar daño a una persona o entidad.

4.2.8 Sensación de adrenalina. Este tipo de criminales se ven tentados a cometer este tipo de delitos por la sensación de adrenalina o emoción que sienten cuando se auto retan para explotar un sistema y logran su objetivo.

Los delincuentes informáticos sacan provecho del valor e importancia que tienen estos activos para una empresa o persona y con ello pueden alterar, sustraer, modificar, dañar, robar o incluso secuestrar la información con el fin de obtener un beneficio ya sea económico, social o por satisfacción propia.

En algunas ocasiones se puede presentar que las personas cometan ciber-delitos, por el desconocimiento de las leyes y las normas o simplemente por el hecho de estar llevando a cabo experimentos que se desencadenan en dichas infracciones.

Con estos antecedentes es fácil detectar que los usuarios no dimensionan los riesgos, peligros y amenazas a los que constantemente están expuestos, generando de esta manera un camino bastante amplio para que los cibercriminales logren sus objetivos, por esto la importancia de una investigación, análisis, estudio y publicación de las falencias y/o los vacíos que se deben subsanar.

4.3 ANTECEDENTES

Para el desarrollo de este proyecto se tomaron como referencia trabajos similares relacionados con la seguridad especialmente en dispositivos móviles y el software usado en ellos para tener referencia acerca de las investigaciones realizadas anteriormente con respecto a las falencias que se pueden presentar en cuanto a seguridad de la información:

Tesina “Analizando el nivel de seguridad del entorno de Android”, presentado por Jesús Luciano Catacora a la Facultad de Informática de la Universidad Nacional de la Plata en el año 2016[16]. En este documento se aborda a los dispositivos móviles, en especial los smartphones junto con las falencias o deficiencias que pueden llevar a diferentes amenazas para la seguridad de la información lo que sirve como referencia para la presente monografía.

Tesina “Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones”, presentado por Sebastián Exequiel Pacheco Veliz y Carlos Damian Piazza Orlando a la Facultad de Informática de la Universidad Nacional de la Plata en el año 2016[17]. Escrito que trata de los sistemas operativos instalados en dispositivos como Notebooks, Smartphones y tablets contiguo a temas relacionados con la seguridad en ellos, dando una reseña para la motivación de la presente monografía.

“Guía para validar el nivel de seguridad de los permisos y uso de recursos de una aplicación móvil bajo plataformas Android”, trabajo de grado para optar por el titulo de especialista en Seguridad de Redes presentado por Cristian Giovanny Toro Sánchez, Jesús Alfredo Vargas Carvajal y Marien Hernández Vega a la facultad de Ingeniería de la Universidad Católica de Colombia en el año 2015[18]. Trabajo en el que se expresa la finalidad de validar la seguridad en las aplicaciones móviles en el sistema operativo Android, e indicando una guía de la relevancia de la seguridad en la información en éste caso para entidades que usan apps, concluyendo en el análisis realizado a la aplicación de una entidad un nivel de seguridad bajo, revelando las falencias encontradas y presentando algunas recomendaciones para

[16] CATACORA, Jesús Luciano. Analizando el nivel de seguridad del entorno de Android. Tesina de Licenciatura. La Plata: Universidad Nacional de La plata, Facultad de Informática, 2016. 184 p.

[17] PACHECO VELIZ, Sebastián Exequiel y PIAZZA ORLANDO, Carlos Damian. Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones. Tesina de Licenciatura. La Plata: Universidad Nacional de La plata, Facultad de Informática, 2016. 139 p.

[18] TORO SANCHEZ, Cristian Giovanny, VARGAS CARVAJAL, Jesús Alfredo y otro. Guía para validar el nivel de seguridad de los permisos y uso de recursos de una aplicación móvil bajo plataformas Android. Trabajo de grado. Bogotá D.C: Universidad Católica de Colombia, Facultad de Ingeniería, 2015. 72 p.

mitigar riesgos de seguridad, lo que ofrece pautas de fundamento para adelantar la presente investigación.

Proyecto “Seguridad en dispositivos móviles Android”, monografía presentada para optar por el titulo de especialista en Seguridad Informática presentado por Oscar Betancur Jaramillo y Sonia Elizabeth Eraso Hanrryr a la Escuela de Ciencias Básicas Tecnología e Ingeniería de la Universidad Nacional Abierta y a Distancia UNAD en el año 2015[19]. Investigación orientada al análisis del nivel de seguridad del sistema operativo Android en versión anterior a la Lollipop en la que coincide con la presente indagación en la importancia de la integridad de la información, fortaleciendo la exploración de las versiones del sistema operativo Android desde el lanzamiento de Lollipop hasta Android 10 para brindar información que permita debilitar los peligros a los que puedan estar expuestos los usuarios.

4.4 MARCO LEGAL

En el ámbito cibernético para Colombia se encuentran normas tales como el Código Penal Colombiano Ley 599 de 2000[20], que en su artículo 269 ítems del a hasta la j, exterioriza la definición para delitos relacionados con sistemas informáticos tales cómo:

- Acceso ilegal al sistema.
- Obstaculización ilegitima incluyendo a la red de comunicaciones.
- Interceptación de datos.
- Daño informático.
- Uso de software malintencionado.
- Infracción de información personal.
- Engaño en sitios web para obtener información personal.
- Situaciones de agravamiento penal.
- Robo a través de medios informáticos.
- Traspaso no autorizado de activos.

Posteriormente se expidió la ley 1273 de 2009 modificando el código penal en el sentido de adicionarle un nuevo ítem “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de

[19] BETANCUR JARAMILLO, Oscar y ERASO HANRRYR, Sonia Elizabeth. Seguridad en dispositivos móviles Android. Monografía. Bogotá: Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas Tecnología e Ingeniería, 2015. 109 p.

[20] LA POLICIA NACIONAL. Normatividad sobre delitos informáticos [En línea]. Código Penal Colombiano Ley 599 de 2000. 2020., Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

la información y las comunicaciones, entre otras disposiciones"[21].

Mas adelante El Congreso de Colombia expide la Ley Estatutaria 1581 de 2012, para la protección de datos personales[22] teniendo en cuenta el derecho de cada individuo a su intimidad propia, de su familia y a mantener su buen nombre tal y como lo indica la Constitución Política en su articulo 15[23].

Seguidamente a la ley expedida en el 2012 se expidió el decreto 1377 de 2013[24] regulando parcialmente la ley 1581, motivada para suministrar el adecuado cumplimiento del tratamiento y protección de datos personales.

Por otro lado existen medidas más generales tomando como ejemplo parte de las políticas de la Play store a las que deben acogerse los desarrolladores entre ellas se suma el tema de la protección infantil en la que indica "Las aplicaciones que incluyan contenido que sexualice a menores…con imágenes de abuso sexual infantil, se informará a las autoridades pertinentes y se eliminarán las cuentas de Google de todos los usuarios implicados en la distribución de este contenido"[25].

[21] DIARIO OFICIAL. Ley 1273 de 2009 [En línea]. El Congreso de Colombia Decreta. 2009., Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[22] DEFENSORIA.GOV. Ley Estatutaria 1581 de 2012. [En línea]. El Congreso de Colombia. 2012., Disponible en: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

[23] ALCALDIA MAYOR DE BOGOTA D.C. Constitución Política de 1991 [En línea].Régimen Legal de Bogotá D.C. 2020., Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

[24] ALCALDIA MAYOR DE BOGOTA D.C. Decreto 1377 de 2013 [En línea]. Régimen Legal de Bogotá D.C. 2020., Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646#0

[25] GOOGLE PLAY. Centro de Políticas de Desarrolladores [En línea]. Contenido Restringido. 2020., Disponible en: https://play.google.com/intl/es/about/restricted-content/child-endangerment/

4.5 MARCO HISTORICO

En Palo Alto California para el año 2003 se fundó Android Inc, quienes desarrollaban software para teléfonos móviles[26], compañía que posteriormente fue adquirida por Google en el año 2005, quien lanza la primer versión del sistema operativo Android Apple pie para finales del 2008, luego de eso iban lanzando versiones o actualizaciones a las que les iban dando nombres de dulces o sinónimos de ellos[27].

De acuerdo a un artículo en Microsoft Security Intelligence, para el 2010 se descubrió el primer virus para Android "Androidos/Fakeplayer, es un troyano que afecta a los dispositivos móviles que ejecutan el sistema operativo Android; envía un cierto mensaje SMS a números específicos, lo que puede afectar al usuario pues se cobra por la transacción sin su consentimiento, éste puede ser descargado como un estándar. Se presenta como una aplicación de reproductor de medios legítima"[28].

Para finales del 2014 fue lanzada la versión Lollipop, su logo o identificación gráfica era una chupeta, su última versión estable fue la 5.1.1, dentro de las características contempladas para ésta versión según un artículo de NDTV se pretendía "Entornos confiables, hablando de la pantalla de bloqueo, pronto podrá hacer que su teléfono detecte cuando está en un entorno confiable, que prescindirá del código de bloqueo. Esto podría ser provocado por la presencia de un dispositivo Bluetooth, como un reloj inteligente que usa todo el tiempo, un punto de acceso Wi-Fi específico u otros factores. Cuando el entorno se considere seguro, no tendrá que molestarse en desbloquear su teléfono"[29].

Según una tesis presentada por Teresa García en la ESPAMMFL, "Muchos usuarios creen que el uso de las aplicaciones móviles puede mejorar su vida, pues buscan aquellas que les sean más útiles para sí mismo. Varias de estas aplicaciones en línea recolectan datos de sus usuarios y de esta manera obtienen estadísticas e

---

[26] ELGIN, Ben. Google Buys Android for Its Mobile Arsenal [En línea]. Bloomberg Businessweek. 2005., Disponible en: https://www.webcitation.org/5wk7slvVb?url=http://www.businessweek.com/technology/content/aug2005/tc20050817_0949_tc024.htm

[27] AMADEO, Ron. A history of pre-cupcake Android codenames [En línea]. Android Police. 2012., Disponible en: https://www.androidpolice.com/2012/09/17/a-history-of-pre-cupcake-android-codenames/

[28] MICROSOFT. Trojan: AndroidOS/Fakeplayer.A [En línea]. Microsoft Security Intelligence. 2010., Disponible en: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%253AAndroidOS%252FFakeplayer.A

[29] NDTV. 8 New features in the next major Android reléase [En línea]. Gadgets 360ª. 2014., Disponible en: https://gadgets.ndtv.com/mobiles/news/android-l-8-new-features-in-the-next-major-android-release-548283

información necesaria para actualizar sus aplicaciones o desarrollar nuevas y de esta manera mantenerse en el mercado"[30].

Por otro lado El Nuevo diario en su artículo de Tecnología Empresarial dice lo siguiente "Los avances tecnológicos hacen que se cuente con más herramientas para combatir los ataques, pero cada día es más evidente que el factor humano es el talón de Aquiles de la seguridad de la información"[31].

Según un estudio de la Universidad Interamericana Recinto de Guayama, acerca de un caso de malware en Android, existen dos tipos de Hacker: ""Hacker" de Sombrero Negro – Este es un individuo que "hackea" con intención maliciosa y que entra a un activo de información o a un sistema sin autorización y "Hacker" de Sombrero Blanco – Este es el "hacker" que penetra sistemas en acuerdo con el propietario del sistema para probar la seguridad del mismo y documentar las debilidades para fortalecer y mejorar las defensas de la organización contra ataques maliciosos e intrusos"[32].

En un artículo publicado el 13 de mayo de 2017 por Jonathan Montoya, en el Colombiano.com menciona "en 2016, Android fue el sistema operativo más vulnerable, por encima de los de Apple, que había ocupado el primer lugar en años anteriores debido, por ejemplo, a la cantidad de bugs que se encontraron en el sistema operativo"[33]. "Otra causa es la rapidez con la que se puede poner un malware en el Play Store respecto al Apple Store. Esta última, explica Guisto, hace muchos controles durante un tiempo prolongado desde el momento en el que alguien sube una aplicación, se publica y se distribuye. "Eso a los cibercriminales no les sirve"[34].

Entrando en detalles las falencias de seguridad en los dispositivos móviles empiezan desde el momento en el cual se pasa por alto el hecho de asignar un pin

---

[30] GARCIA MOLINA, Teresa y MOREIRA PARRAGA, Jorge. Evaluación de protocolos de seguridad de las apps de redes sociales en dispositivos móviles Android [En línea]. Manabí: Escuela Superior Politécnica Agropecuaria de Manabí. 2016., Disponible en: http://repositorio.espam.edu.ec/handle/42000/299

[31] TECNOLOGÍA EMPRESARIAL. Op. Cit.

[32] DOMINICCI, José. Estudio de caso: malware en Android [En línea]. 2011., Disponible en: https://s3.amazonaws.com/academia.edu.documents/36682501/TopicPaper.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1527183432&Signature=HfgGt1FDeSVao8J6sJWZFSuYxcE%3D&response-content-disposition=inline%3B%20filename%3DMalware_en_Android.pdf

[33] MONTOYA GARCIA, Jonathan. ¿Por qué es más inseguro el sistema Android que iOS? [En línea]. Bogotá: El Colombiano.com. 2017., Disponible en: http://www.elcolombiano.com/tecnologia/seguridad-en-celulares-android-y-apple-YE6521203

[34] MONTOYA, Ibíd.

o código de acceso para el ingreso al dispositivo y posteriormente a sus aplicaciones.

Otra apertura a la vulnerabilidad es el tema de no usar software antivirus, pues si bien es un procedimiento utilizado en los PC, con más razón se debe implementar su uso en los dispositivos móviles, que llegan a contener incluso más información que la de un equipo de trabajo.

Actualmente algunas personas se dedican a utilizar estas redes para llevar a cabo delitos cibernéticos, ya sea por beneficio económico, social o por el reto que sienten de demostrar que los sistemas no son cien por ciento seguros como se esperaría, realizando así un uso inadecuado, irresponsable o irrespetuoso, generando daños incalculables.

A lo anterior, le sigue la tentación de una red Wifi abierta, pues para el ser humano lo gratuito suele ser atractivo, pero no advierte los peligros que dicha conexión conlleva, a través de dichas redes, se corre el riesgo de ser atacado por un malware o bien la información que se está manipulando a través de esta puede estar a los ojos de otros usuarios de la red, como por ejemplo: en el ataque Krack que traduce ataques de reinstalación de claves y da paso a la lectura de la información en red wifi, así como la inyección de malware y ransomware a través de este.

Ransomware: Es un programa maligno que codifica información almacenada en los dispositivos electrónicos, solicitando posteriormente un rescate para quitar la restricción creada a dicha información.

Otros ataques pueden ser el Cryptolocker que es la descarga de un virus que se realiza al abrir un enlace o archivo adjunto situado en el correo electrónico, el cual viene infectado y una vez instalado retiene la información captada por él, solicitando un pago para obtener una clave que permita acceder nuevamente a dicha información.

Por otro lado, también se está expuesto al Cryptowall que es un virus que se descarga al ingresar a sitios web maliciosos o aceptando actualizaciones falsas de sistema o aplicaciones, es utilizado para escanear y codificar la información que este en el equipo infectando mediante un Malware el sistema operativo Android.

Añadiendo otros como Skimming que realiza una exploración y escaneo de una información específica, como cuando se genera una búsqueda con palabras claves en un explorador web.

Pasando además por otros ataques como Web spoofing en donde el atacante crea un sitio web falso para que el usuario entre y éste monitoree sus acciones.

O sumándole el Smishing que es la práctica de adquirir información confidencial mediante mensajes de texto enviados a los usuarios de telefonía móvil, buscando que estos visiten links fraudulentos o realicen llamadas a números telefónicos indicados en dicho mensaje de texto.

También se puede encontrar el Trashing (cartoneo) que consiste en anotar el login y el password en algún lugar, información la cual puede ser utilizada por quien desea atacar.

Así mismo existen Ataques de monitorización, siendo éstos una(s) persona(s) que estudia a su víctima para atacarla en un futuro.

De lo anterior se desprende:

- Shoulder surfing: persona que espía al usuario personalmente para memorizar la información y luego usarla.
- Decoy (señuelos): programa con interface similar a la original pero creada con el fin de obtener la información, esta se guarda y el sistema realiza sus funciones normalmente.
- Scanning (búsqueda): scanear puertos de escucha en la mayor cantidad posible con el fin de guardar información.

Aun cuando en Colombia y otros países este tipo de delitos está regulado por leyes, los ciberdelincuentes constantemente se encuentran al acecho y los usuarios pueden estar facilitándoles el camino para llevar a cabo sus actos delictivos.

Adicionalmente junto con las características anteriormente descritas los siguientes factores de personalidad son intrínsecos de los delincuentes informáticos:

Falta de Ética: La profesión es una labor, actividad u ocupación, con la finalidad de brindar a la sociedad un bien o servicio específico con calidad y responsabilidad, teniendo en cuenta que para ejecutarla requiere de una recolección y acogimiento de conocimiento, prácticas y valores y con su aplicación o ejecución se obtiene un beneficio económico. Sin pasar por alto que, para llevarla a cabo con integridad no se debe aprovechar de las debilidades del otro, pues se estaría corrompiendo la esencia de brindar el bien o servicio. Para mantener dicha integridad, se requiere que las personas cuenten con la (virtud) habilidad de obrar bajo lineamientos del bien, verdad y justicia. Cuando se desvían o faltan los valores o principios, ya sea en el ámbito personal, económico o social, se pierde la ética profesional, es allí en donde se da lugar para este caso a cometer delitos informáticos.

Debido al deterioro de la integridad y la ética profesional, algunas personas caen en la tentación de realizar actividades al margen de la ley, como los delitos informáticos, ya sea por avaricia, por dañar a una persona o entidad o por el simple hecho de llamar la atención y demostrar que la tecnología no es cien por ciento segura como se esperaría.

Los delincuentes informáticos sacan provecho del valor e importancia que tienen estos activos para una empresa o persona y con ello pueden alterar, sustraer, modificar, dañar, robar o incluso secuestrar la información con el fin de obtener un beneficio ya sea económico, social o por satisfacción propia.

5. MATERIALES Y METODOLOGIA

5.1 METODOLOGIA

Teniendo en cuenta que se busca estudiar el SO Android versión Lollipop y junto con su evolución hasta la versión 10, con el fin de establecer la seguridad de la información contenida en los dispositivos que cuentan con dicho S.O, para la presente monografía se busca capturar una serie de información relacionada con éste tema, para ser consolidada, analizada y estudiada a través de metodología descriptiva y documental que implica la recolección y análisis de información.

Para lo anterior, se realiza la selección de un tema a tratar, delimitando dicho tema posteriormente; se lleva a cabo una recolección y recopilación de la información relacionada, la cual pasa por un proceso de análisis que finalmente conlleva a la elaboración de un informe para la respectiva muestra de los resultados obtenidos.

A partir de ello como primer paso se seleccionó el tema mencionado inicialmente, seguido a esto se procedió a delimitar la población en la que se enfocaría el estudio, por esta razón se concreto orientarlo a personas entre los 15 y los 65 años de edad, así mismo ser realizado en la ciudad de Bogotá D.C.

Siguiendo con la metodología se llevo a cabo la búsqueda de todos los antecedentes, fundamentos, noticias, reseñas y demás datos que contribuyen con el avance del estudio escogido, siendo esta plasmada en el documento a presentar como trabajo de grado.

Una vez completados los pasos anteriores se identifica la técnica a usar para la estimación y el análisis de la información, eligiendo para ello el muestreo no probabilístico “(o muestreo no aleatorio) es la técnica de muestreo donde los elementos son elegidos a juicio del investigador. No se conoce la probabilidad con la que se puede seleccionar a cada individuo”[35]. De igual manera éste método esta dividido en 5 tipos, optando para ésta investigación en la elección del muestreo por conveniencia “que se aplica cuando la muestra estadística a formar es seleccionada en el entorno próximo al investigador sin que medien requisitos específicos. La idea es facilitar el trabajo de quien va a desarrollar el estudio”[36].

Entonces para la captura de los datos que se pretenden recopilar con el fin de identificar la percepción e identificación de la seguridad en los usuarios del sistema operativo Android Lollipop y/o sus versiones posteriores, se procede a efectuar la

[35] UNIVERSO FORMULAS. Muestreo no probabilístico [En línea]. 2019.,Disponible en: https://www.universoformulas.com/estadistica/inferencia/muestreo-no-probabilistico/

[36] ENCICLOPEDIA ECONOMICA. Muestreo por conveniencia [En línea]. 2019., Disponible en: https://enciclopediaeconomica.com/muestreo-por-conveniencia/

encuesta que es una de las “estrategias más utilizadas en el área de investigación, dado que favorece la obtención de datos fundamentales para el análisis de diversas temáticas, permitiendo una mayor eficacia y rapidez en el procedimiento”[37].

5.2 MATERIALES

Registrado esto se continúa con el trámite de encuestas para identificar el punto de vista, conocimiento y la percepción de los usuarios seleccionados en el enfoque. La estructura de preguntas en el medio señalado se encuentra como documento anexo 1 de la presente monografía denominado Encuesta Online.

La encuesta titulada “Encuesta para Análisis de datos en Sistema Operativo Android”, le indica al encuestado que se realiza con el objetivo de identificar su percepción y conocimientos acerca de la seguridad en el Sistema Operativo Android desde la versión Lollipop lanzada en el 2014 hasta la versión 10 lanzada en 2019.

Para acceder al cuestionario aplicado se puede ingresar a través de la URL https://forms.gle/JH9t3S8LLvzAJCCx9 o como se mencionó anteriormente, en el anexo adjunto del presente documento también es posible verificar los ítems indagados.

Por ultimo los datos compilados en las respuestas recibidas, una vez clasificados y procesados arrojan un resultado que permite generar una deducción acerca del conocimiento o no de los usuarios del sistema operativo Android, junto con el grado de conocimiento que puedan tener los encuestados acerca de los lineamientos de seguridad que tiene este dispositivo para salvaguardar la información almacenada en los dispositivos utilizados por ellos. Lo anterior se realiza con el propósito de tener los resultados como insumos para la elaboración del manual de buenas prácticas de usuario.

[37] TU GIMNASIA CEREBRAL. Las encuestas – Qué son, características, cómo hacerlas [En línea]. Bogotá. 2014., Disponible en: http://tugimnasiacerebral.com/herramientas-de-estudio/que-es-una-encuesta-caracteristicas-y-como-hacerlas

6. DESARROLLO DE LOS OBJETIVOS ALINEADOS A LA METODOLOGÍA

6.1 ANALISIS DE INFORMACIÓN DEL SISTEMA OPERATIVO ANDROID LOLLIPOP HASTA LA VERSIÓN 10, PARA ESTIMAR LA SEGURIDAD A LA INFORMACIÓN QUE OFRECE ESTE SISTEMA OPERATIVO AL USUARIO.

En el 2014 Google buscando más seguridad en su sistema operativo para dispositivos móviles lanzó Android Lollipop o Android versión 5.0, es así como en esta versión se preocupa por el cifrado de la información de manera automática, cifrando todo el dispositivo en su primer arranque, también permite la configuración de las notificaciones que se desean ver con el dispositivo bloqueado, así como también teniendo en cuenta que en caso de pérdida del dispositivo existen opciones que permiten rastrearlo o borrar su contenido de manera remota, con el inconveniente que si llegasen a restaurarlo de fábrica, estas herramientas también perderían su utilidad y por ende con ella la opción de recuperar el aparato, por ello en esta versión se implementó la elección de contraseña para la ejecución de dicha restauración.

Android Marshmallow versión 6 lanzado en octubre de 2015 e identificado con un masmelo, admite el ahorro de batería cuando una aplicación no esta en uso la deja en espera limitando el consumo e implementa una funcionalidad de descanso que pone el dispositivo en suspensión automática, en cuanto a seguridad esta versión permite administrar los permisos a las aplicaciones permitiendo decidir que y cuando compartir, de la misma manera desactivar dichos permisos cuando se considere pertinente, adicionalmente incorpora el uso de huella dactilar para ser utilizada en el desbloqueo del dispositivo y/o inicio de sesión o autenticación en aplicaciones[38].

Android Nougat versión 7 lanzado en 2016, permite visualizar dos aplicaciones a la vez con un formato multiventana y con los dispositivos compatibles permite los gráficos en 3D o modo de realidad virtual, sin quitar merito a su versión anterior con esta también admite una duración de batería y por otro lado se pueden ordenar y personalizar los iconos de acceso rápido al contenido que se ajuste a las necesidades del usuario, de la misma manera dentro de las notificaciones se puede dar respuesta a las conversaciones sin necesidad de abrir la aplicación, también incorporó una función para ahorrar datos evitando que las aplicaciones en segundo plano accedan al consumo de datos del dispositivo, pero hay más opciones, dado que permite la configuración del tamaño del texto, de los iconos y de los elementos que se muestran en pantalla, es justo decir que no deja de lado la seguridad Android maneja cifrado y seguridad por capas y para Nougat incluye las actualizaciones del

[38] ANDROID. Android 6.0 Marshmallow [En línea]. 2015., Disponible en: https://www.android.com/intl/es_es/versions/marshmallow-6-0/

software en segundo plano, evitando la interrupción mientras ejecuta esta tarea, cifrado de archivos aislándolos u protegiendo los de cada usuario del aparato[39].

Android Oreo versión 8 lanzado en 2017 e identificado con una galleta como la golosina de la marca oreo, genera acceso a las aplicaciones de manera más rápida recordando los inicios de sesión, se pueden ver las novedades de las notificaciones y borrarlas deslizándolas con el dedo, igualmente sin dejar a un lado la seguridad incorpora Google Play Protect que ofrece defensa ante software malicioso[40].

Android Pie versión 9 lanzado en 2018 entra al mercado haciendo uso de la inteligencia artificial lo que revela a medida que el usuario da uso al dispositivo el sistema esta en un constante aprendizaje otorgando la mejora en la experiencia permanente de funcionamiento, ajustándose de manera automática a las preferencias de administración del aparato, en cuanto a seguridad con Pie las copias de seguridad son cifradas con la contraseña del aparato asignada por el usuario, esta versión incluye autenticación biométrica y un modulo de seguridad de hardware denominado StrongBox con la finalidad de proteger las claves privadas, de igual modo para las aplicaciones en segundo plano o las inactivas delimita el acceso a la cámara o al micrófono[41].

Android 10 lanzada en 2019 y como cada incorporación de versionamiento trae consigo nuevas funcionalidades, para este aporta sub titulación automática en videos o audios sin contar con conexión a internet, también se puede amplificar el sonido, filtrar el ruido que interfiere mejorando el audio, brinda más protección, permitiéndole al usuario inspeccionar y disponer del momento que desee compartir los datos del móvil por medio del ajuste y/o configuraciones de privacidad, es decir que el usuario elige que datos de su actividad en la web y en las apps permitirá almacenar lo que conlleva a la transparencia y control sobre los datos, de igual manera permite acceder a las actualizaciones en cuanto a seguridad se refiere a partir del lanzamiento de las mismas, trae un modo de enfoque que deja pausar aplicaciones temporalmente, contribuye con hábitos saludables estableciendo limites de tiempo de pantalla, supervisar la actividad de una aplicación, administrarla y restringir su contenido[42].

---

[39] ANDROID. Android 7.0 Nougat [En línea]. 2016., Disponible en: https://www.android.com/intl/es_es/versions/nougat-7-0/

[40] ANDROID. Android 8.0 Oreo [En línea]. 2017., Disponible en: https://www.android.com/versions/oreo-8-0/

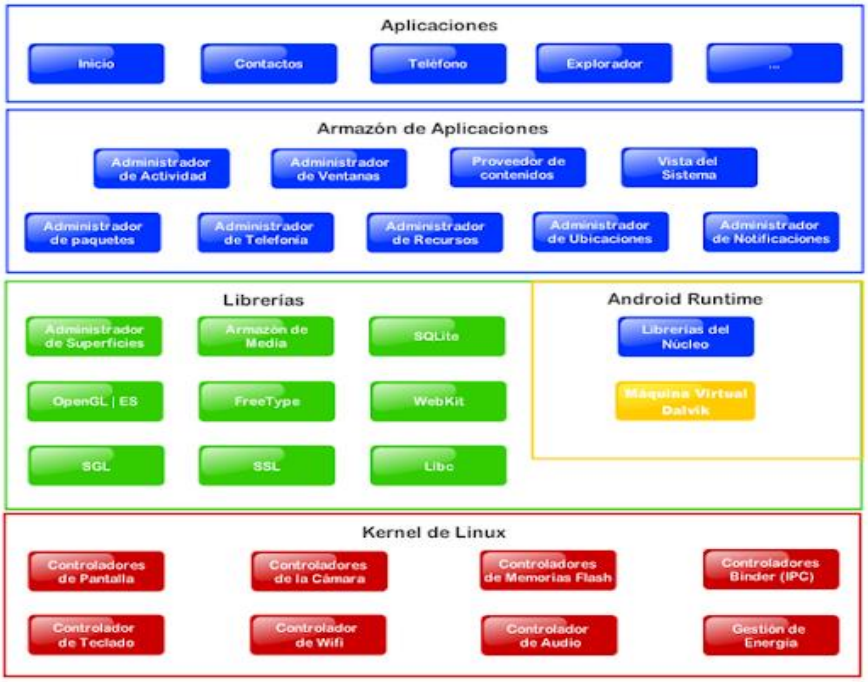
[41] ANDROID. Android 9 Pie [En línea]. 2018., Disponible en: https://www.android.com/versions/pie-9-0/

[42] ANDROID. Android 10 [En línea]. 2019., Disponible en: https://www.android.com/android-10/

6.1.1 Arquitectura de seguridad del sistema Android. El kernel es la médula de un sistema operativo, éste recibe las indicaciones transmitidas y/o dadas al software para que el hardware pueda ejecutarlas, el sistema operativo Android utiliza el Kernel de Linux, el cual con la participación de múltiples desarrolladores en una repetida sucesión de ataques, investigaciones y correcciones fue convirtiéndose en un núcleo que brinda seguridad y estabilidad, lo que otorga a Android características tales como esquema de autorizaciones fundamentadas en el usuario, aislamiento de procesos, mecanismo extensible para IPC (Inter Process Communication) seguro lo que significa la capacidad de comunicación y sincronización de procesos entre ellos y realizar limpieza de las partes inseguras, protegiendo los recursos del usuario aislando los unos de los otros[43].

La siguiente figura, muestra el entorno de Android en sus diferentes niveles, los principales bloques de construcción de la plataforma Android son Hardware del dispositivo, sistema operativo y tiempo de ejecución de las aplicaciones, para estas últimas hay dos fuentes las preinstaladas y las instaladas por el usuario[44].

Figura 3. Arquitectura de Android



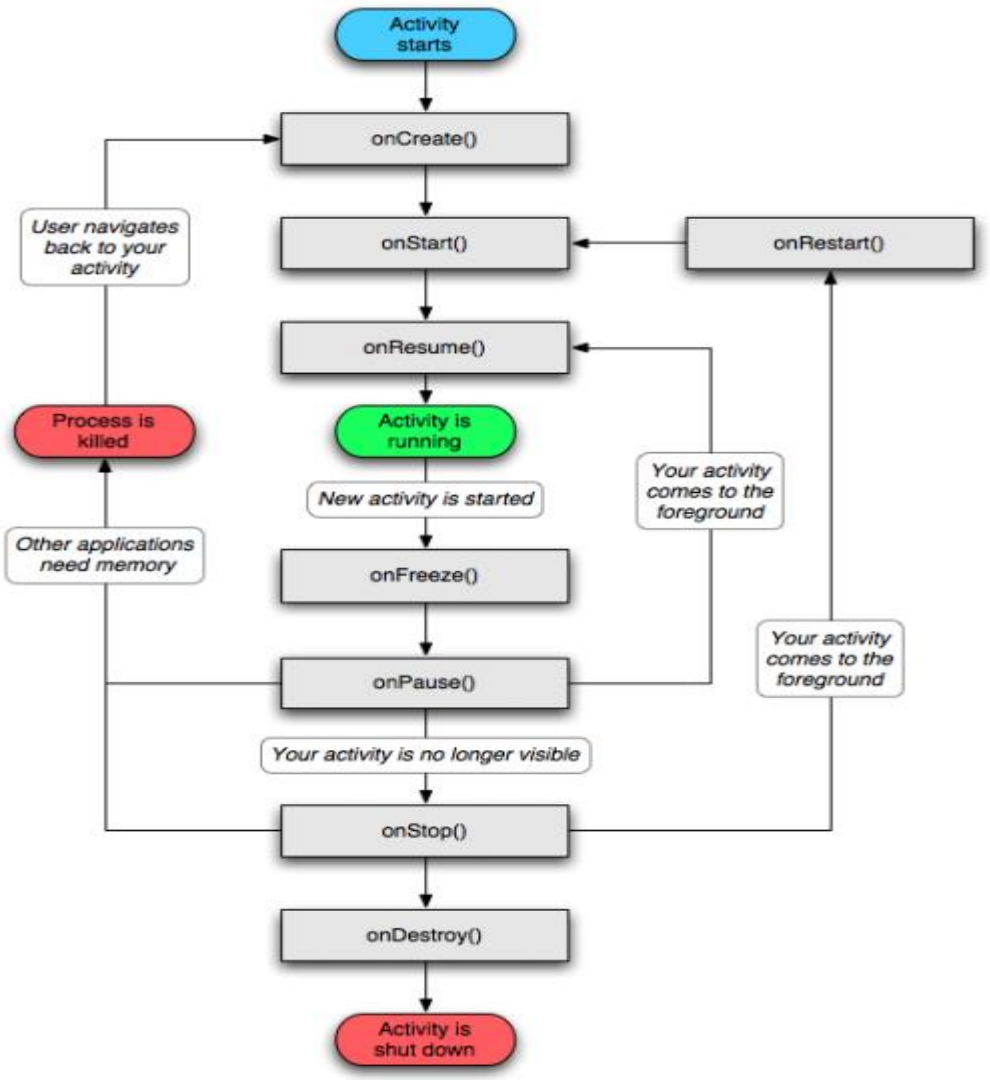
Fuente: SOFTWARE DE COMUNICACIONES. Arquitectura Android. [Arquitectura]. Disponible en: https://sites.google.com/site/swcuc3m/home/android/generalidades/2-2-arquitectura-de-android

[43] SOURCE.ANDROID. Seguridad del sistema y del núcleo [En línea]. 2020., Disponible en: https://source.android.com/security/overview/kernel-security?hl=es-419

[44] SOURCE. ANDROID. Asegure un dispositivo Android [En línea]. 2020., Disponible en: https://source.android.com/security

Cada actividad realizada por un usuario tiene un ciclo de vida como se muestra en la figura siguiente, la cual al momento de ejecutarse queda como en una especie de cache propiciando que cuando el consumidor la abandone y quiera retomarla mas adelante, dicha actividad funcione sin ningún inconveniente de manera rápida dependiendo de los recursos del dispositivo, cada proceso de una aplicación está formado por una o más actividades independientes[45].

Figura 4. Ciclo de vida de una actividad



Fuente: SOFTWARE DE COMUNICACIONES. Ciclo de vida de una actividad [Imagen]. En: Aplicaciones en Android. Disponible en: https://sites.google.com/site/swcuc3m/home/android/generalidades/aplicacionespag3

[45] SOFTWARE DE COMUNICACIONES. Aplicaciones en Android [En línea]. 2020., Disponible en: https://sites.google.com/site/swcuc3m/home/android/generalidades/aplicacionespag3

6.1.2 Clases de dispositivos que operan con sistema operativo Android.
Teléfonos inteligentes también llamados Smartphone
Ordenadores portátiles
Netbooks
Tabletas
Google TV
Relojes de pulsera
Para éste proyecto el enfoque es el Teléfono inteligente también llamados Smartphone con sistema operativo Android Lollipod hasta su evolución en versión 10.

6.1.3 Características de un celular inteligente o Smartphone. Los celulares anteriormente solo servían para hacer o recibir llamadas y mensajes de texto, con alguna que otra función como la configuración del reloj, un juego o almacenar una nota de texto, algunos empezaron a contar con características como una linterna integrada o la función de bloqueo con un pin numérico, este dispositivo utiliza ondas de radio para su funcionamiento. Ahora bien adicional a lo ya mencionado para un celular normal, lo que consigue hacer la diferencia con los teléfonos inteligentes son sus actuales características, una de ellas es que tolera instalación de programas independientemente de que sean desarrolladas por el fabricante del aparato, el operador o un tercero, alcanza un aumento de memoria o almacenamiento insertándole una sd, cuentan con cámara fotográfica cada vez mejorando aun mas su resolución, posee GPS, admite conectividad y navegabilidad por internet, permite el uso y administración de archivos en sus diferentes formatos, es multitarea y sobretodo debe tener para su funcionamiento instalado un sistema operativo[46].

6.1.4 Usos del celular. El celular sirve para tareas tan simples como una llamada, un mensaje de texto, incluso para configurar el reloj y que la alarma suene a determinada hora para levantarse o hacer una actividad especifica en un momento determinado, con el avance en tecnologías estos dispositivos en la actualidad tienen más funciones que anteriormente eran inimaginables, cuentan con conexión a internet ya sea con un plan de datos contratado o adquirido con el operador utilizado por el usuario o accediendo a una red wi-fi que significa fidelidad inalámbrica recurriendo a señales de radio[47] bien sea publica o privada es decir la primera es de fácil acceso siempre y cuando el dispositivo la detecte para su respectiva conexión generalmente en lugares públicos algunas requieren de usuario y

[46] TECNOLOGIA. Que es un Smartphone. [En línea]. 2020., Disponible en: https://www.areatecnologia.com/Que-es-un-smartphone.htm

[47] BELLIDO VEIZAGA, Wilfredo Jesús. Ethical Hacking: Hacking de Red Inalámbrica Wifi [En línea]. Revista de Información, Tecnología y Sociedad versión impresa ISSN 1997-4044. La Paz. 2013., Disponible en: http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100021&script=sci_arttext&tlng=es

contraseña suministrados por el establecimiento[48], la segunda ya es una red contratada en una entidad u hogar que permitirá la unión a ella con un usuario y una contraseña configurados por el cliente de la misma así como estableciendo un limite de dispositivos conectados[49], volviendo al tema teniendo acceso a internet permite desde realizar búsquedas sencillas en la web, descargar aplicaciones, realizar juegos online, ver películas y ejecutar diferentes tipos de transacciones, como por ejemplo transacciones bancarias, de igual manera el dispositivo sirve para escuchar la radio, música almacenada en la memoria del aparato del mismo modo que puede ser manejado como cámara fotográfica para cualquier tipo de eventos, almacenando los archivos bien sea en la memoria interna del dispositivo, en una sd extraíble o en la disponibilidad de la nube con la que cuente el usuario, para posteriormente ver los videos grabados o las imágenes que haya capturado, en cuanto a estética se refiere admite modificar la imagen de presentación de la pantalla tanto de inicio como de bloqueo hasta la forma en la que se visualizan los iconos o inclusive los botones del teclado del teléfono, a primera vista una serie de grandiosas opciones que facilitan la vida e incluso economizan tiempo, brindando la oportunidad de emplear dicho tiempo en la actividad que al usuario le apetezca.

Para mitad del 2019 en un artículo publicado en la sección de tecnología del periódico El Tiempo, la firma de auditoria Deloitte dio a conocer una información recopilada sobre el uso que dan los Colombianos al celular, en el cual revela que los usuarios parecen no inquietarse por la reserva o seguridad de datos, de los 928 encuestados el 59% usa el dispositivo para ver videos o publicaciones, seguido por un 57% que se dedica a la consulta en las redes sociales, muy cerca al 56% que lo usa para tomar fotografías, frente a un 48% que lo aprovecha para jugar y por ultimo un 39% que recurre a ver los videos que comparten por servicios de mensajería instantánea como WhatsApp[50].

Es así como se puede observar en la siguiente imagen publicada en un artículo del diario El País la tendencia mostrada para los sistemas operativos durante 5 años, en donde mientras el crecimiento de los sistemas operativos iOs y OS X son relativamente constantes, el sistema operativo Windows de los PC's muestra una caída frente al comportamiento del S.O. Android, el cual muestra un crecimiento en el transcurso del tiempo lo que permite manifestar que el uso del celular esta en aumento.

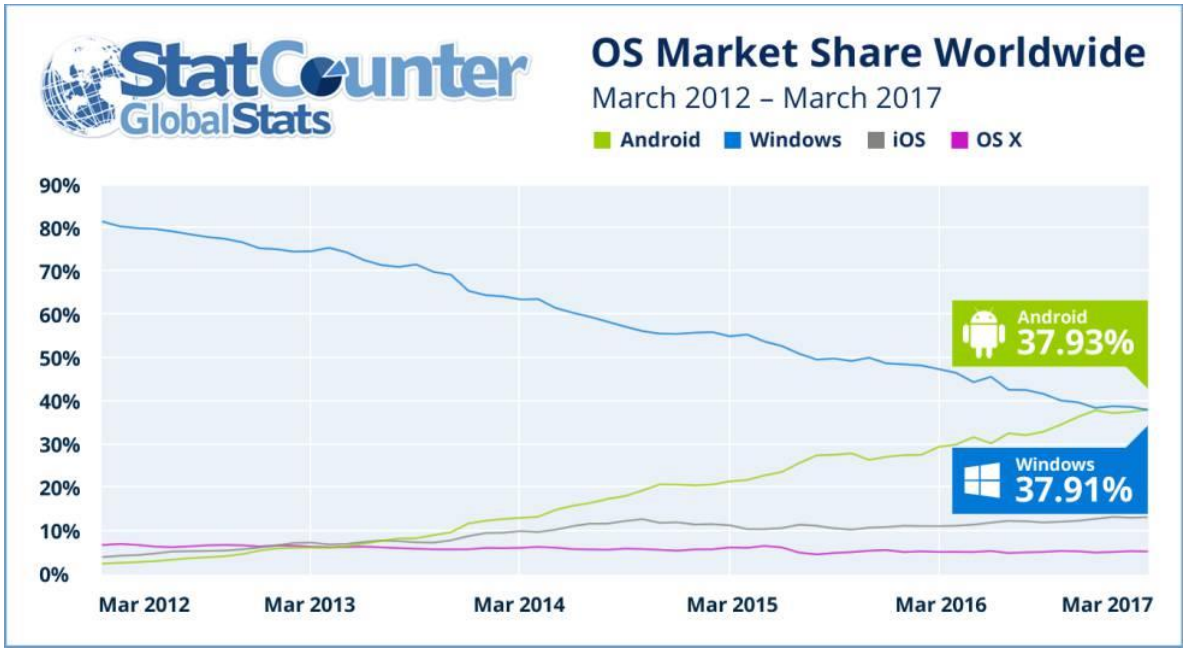
---

[48] FERRO VEIGA, José Manuel. Asesor/Gestor en seguridad privada integral: Curso superior en dirección de seguridad privada. José Manuel Ferro Veiga, 2020.

[49] CARBALLAR, José Antonio. WI-FI. Lo que se necesita conocer. RC Libros, 2010

[50] TECNOSFERA. Colombianos tocan su celular 2 mil veces al día en estas actividades. [En línea]. Bogotá: El Tiempo.com. 2019., Disponible en: https://www.eltiempo.com/tecnosfera/dispositivos/encuesta-de-consumo-movil-en-colombia-2019-389702

Figura 5. Crecimiento del Sistema Operativo Android



Fuente: MENDIOLA Z, José. Android ya es el sistema operativo más usado del mundo. [imagen]. El País. Disponible en: https://elpais.com/tecnologia/2017/04/04/actualidad/1491296467_396232.html

6.1.5 Android e Internet de las cosas. Internet de las cosas o Internet of Things con su respectiva abreviación IoT, al llegar aquí y para un adecuado alcance del termino mencionado se realiza un desglosé de las palabras que contiene ésta tecnología en concreto, Internet es una red o varias redes unidas con el fin de transmitir información y como es bien sabido cosas son objetos[51], en ese orden de ideas las cosas no se pueden conectar por si solas, es aquí donde el software entra a hacer parte de las cosas, para consentir la posibilidad de extraer, inyectar y/o recopilar información del funcionamiento de las cosas, para abrir la puerta a la conexión de estas a través de la red.

Al lado de ello surge la oportunidad para Android, en el que se permite el desarrollo de apps relacionadas con IoT, lo dicho aquí se puede soportar con artículos tales como el reportaje publicado por Alberto Martin en el 2014, titulado El internet de las cosas: Android en todas partes donde exterioriza “Muy pronto Android estará presente en todas las facetas de tu vida cotidiana. En tu casa, en tu coche, en la ropa que llevas puesta y en los gadgets que usas”[52], en definitiva se refiere la

[51] BARRIO ANDRES, Moisés. Internet de las cosas. Editorial Reus. 2018
[52] MARTIN, Alberto. El Internet de las cosas: Android en todas partes [En línea]. España. 2014., Disponible en: https://computerhoy.com/noticias/hardware/internet-cosas-android-todas-partes-13823

posibilidad de conexión a las cosas con las que las personas tienen contacto en su vida cotidiana. Mas adelante en el año 2018 la republica.net divulga "La empresa matriz de Google, Alphabet Inc, anunció durante la conferencia anual para desarrolladores, la versión oficial del sistema operativo Android Things 1.0, el sistema que buscará coronarse entre los dispositivos conectados al Internet de las Cosas (IoT)"[53]… Tal vez ya no esta tan lejos la experiencia que vivía Michael Knight en la serie el auto fantástico, donde controlaba el vehículo con su reloj, ya no es tan descabellada o futurista la acción de encender o apagar el TV desde el móvil o incluso controlar un electrodoméstico a través de un software.

Para no ir mas lejos se puede tomar como modelo de IoT en la vida actual uno de los ejemplos de innovación relacionados con el tema y publicado en el blog de un Instituto en Lima comunicando que "La empresa Dacor desarrolló un horno llamado Discovery IQ que tiene WI-FI y puede ser controlado vía Smartphone o Tablet. Reconoce muchas recetas y hacer el trabajo solo. Cuanto el plato está listo, envía un mensaje al usuario"[54]. Demostrando que dicha realidad esta mas cerca de lo que tal vez se pensaba.

Una vez recopilada la información anteriormente expuesta en cada uno de los numerales, se puede observar como las tecnologías van en un constante avance y en paralelo los software que a ellas acompañan, para éste caso el sistema operativo Android, el cual muestra con las evoluciones de sus versiones y actualizaciones el constante interés por consentir al usuario final y concederle la mejor calidad en cuanto a servicios y funcionalidades se refiere, naturalmente que no deja de lado la firme convicción de procurar la mejor protección en cuanto a seguridad del dispositivo y de la información que el contiene.

6.2 IDENTIFICACION DE VULNERABILIDADES Y AMENAZAS FRECUENTES AL SISTEMA OPERATIVO ANDROID LOLLIPOP HASTA LA VERSIÓN 10 MEDIANTE BÚSQUEDA DE INFORMACIÓN DE INCIDENTES, PARA CLASIFICAR FINALIDAD Y ALCANCE DE ESTOS.

Cuando se aborda la seguridad informática, se entiende que es la disciplina que busca la protección, integridad y privacidad de la información recopilada en un sistema informático y realizar una Gestión del riesgo informático que comprende un método para la realización de actividades que permitan identificar los riesgos y controlarlos.

---

[53] OBANDO, Mariangel. Google apuesta por el "Internet de las cosas" con Android Things [En línea]. LaRepublica.Net. 2018., Disponible en: https://www.larepublica.net/noticia/google-apuesta-por-el-internet-de-las-cosas-con-android-things

[54] IDAT. Internet de las cosas: 10 ejemplos innovadores [En línea]. Lima. 2019., Disponible en: https://www.idat.edu.pe/blog/internet-de-las-cosas-10-ejemplos-innovadores

Las amenazas se pueden clasificar en intencionales como tashing, phishing, propagación de código malicioso e ingeniería social, virus informático, Robo de información, fraudes, espionaje y no intencionales como las relacionadas con los fenómenos climáticos y desastres naturales.

En este caso se pueden presentar diferentes situaciones de acuerdo a la complejidad del ser humano, teniendo en cuenta que la información está expuesta a ser utilizada de manera inadecuada tanto dentro como fuera de los entornos en los que se maneja. Es tan así que por ejemplo: una persona interesada en conseguir algún tipo de información puede conseguirla a través de amenazas a un agente interno, por medio de extorsiones para obtener lo deseado.

6.2.1 Riesgos, descripción y conceptos. En el diario vivir y con los cambios y avances tecnológicos los dispositivos están expuestos a riesgos tanto físicos como lógicos, las diversas amenazas y vulnerabilidades de las que no están exentos, requieren de un control informático.

Es por ello que se requiere la realización de análisis y evaluaciones de las diferentes amenazas o peligros de los que pueden ser víctimas, para la búsqueda de métodos y alternativas que permitan generar la solución a las problemáticas establecidas.

Algunos de los términos relacionados con este tema son:

- Amenaza: Entorno o situación que representa peligro o daño.
- Análisis: Estudio de las situaciones, entornos o conductas que permitan conducir al entendimiento de las mismas.
- Aplicación de metodologías: Aplicación de prácticas o sistemas diseñados y elaborados para la protección.
- Ataque: Agresión con fines insanos.
- Control: Inspección y vigilancia ejercida para mantener dentro de los parámetros concertados.
- Criminalidad: Actos mediante los cuales cometen o realizan situaciones ilegales, hechos al margen de la ley.
- Evaluación: Valoración o apreciación realizada a las situaciones, entornos o conductas.
- Integridad: Conservación de las características que permitan la protección tanto de hardware como de software.

- Negligencia: Falta de eficacia, efectividad y pro actividad encaminada a mantener la respectiva seguridad de los hardware y software utilizados.

- Riesgos ambientales: Los peligros ambientales a los que están expuestos tales como incendios, inundaciones y demás condiciones relacionadas con factores del clima.

- Vulnerabilidad: Estado de fragilidad, puntos débiles mediante los cuales pueden ingresar los diferentes tipos de ataques.

Lo anterior se basa en la experiencia obtenida en el transcurso de la vida laboral y personal, la cual no está directamente relacionada con los temas de estudio, pero se pueden evidenciar como usuario interno o externo de dichos servicios, teniendo en cuenta que de alguna manera afecta ya sea directa o indirectamente.

En las vivencias personales se pueden evidenciar los riesgos que corren los diversos dispositivos tecnológicos, comenzando por los celulares, los cuales ya contienen en la mayoría del almacenamiento información personal, en la que al no tener presente los riesgos o vulnerabilidades que puede presentar, es susceptible a los ataques que las personas mal intencionadas deseen realizar, generando riesgos bastante altos como lo pueden ser el robo de la información, por ejemplo los datos de cuentas bancarias y demás información relevante para ser usada en actos criminales. Por lo anterior se deben realizar los respectivos análisis, pruebas y evaluaciones para determinar las vulnerabilidades y amenazas que se pueden presentar. Una vez detectadas se pueden realizar los respectivos estudios, procesos y procedimientos que permitan realizar los controles adecuados y necesarios para proporcionar seguridad.

6.2.2 Vulnerabilidades más frecuentes en el sistema Android Lollipop. En un boletín de seguridad de Android, en febrero de 2019 se publicó “La brecha de seguridad tiene que ver con las imágenes. En concreto con los archivos en formato .png., las fotografías pueden tener diferentes formatos: .jpg, .png, etc. El error de seguridad tiene que ver con este último, es decir, que con una simple imagen, un ciberdelincuente puede atacar cualquier dispositivo Android que tenga instaladas las versiones comprendidas desde Android 7.0 hasta la 9.0, que son las afectadas.”[55], evidenciando cierta fragilidad con la que cuentan algunas versiones del sistema operativo Android.

[55] ABC. Un nuevo y grave fallo de seguridad en Android deja vendidos a los usuarios por culpa de una simple foto [En línea]. Madrid. 2019., Disponible en: https://www.abc.es/tecnologia/informatica/software/abci-nuevo-y-grave-fallo-seguridad-android-deja-vendidos-usuarios-culpa-simple-foto-201902131742_noticia.html?ref=https%3A%2F%2Fwww.google.com%2F

Como es sabido las personas mal intencionadas hacen uso de toda clase de estrategias que les permita ejecutar sus planes, tal es así como en la etapa actual del 2020, en la que el mundo esta pasando por una pandemia, los cibercriminales hacen uso de sus tácticas, pues según un artículo publicado acerca del coronavirus menciona “Ahora, la empresa de ciberseguridad Kaspersky ha alertado sobre el efecto que está teniendo en España el virus informático Ginp. Un troyano que los atacantes camuflan como la aplicación Coronavirus Finder. Una «app», pensada para dispositivos Android, que –aparentemente- muestra al usuario las personas cercanas que están contagiadas. Sin embargo, su objetivo real pasa por robarle los datos bancarios a la víctima”[56].

6.2.3 Amenazas y/o ataques más frecuentes en el sistema Android Lollipod y sus versiones posteriores. La finalidad de una amenaza es ocasionar daños, para los sistemas operativos los perjuicios pueden ser presentados a través de malwares y virus, entonces un “Malware es un software escrito específicamente para dañar e infectar el sistema host, incluye virus junto con otros tipos de software como troyanos, gusanos, spyware y adware. Ahora virus es un tipo específico de malware por sí mismo. Es una pieza contagiosa de código que infecta el otro software en el sistema host y se propaga una vez que se ejecuta”[57].

Para entender un poco mejor lo anterior, es preciso aclarar que un host es el nombre que se utiliza para los dispositivos que a través de conexiones en red intercambian servicios en ella y los malware, adware y virus son básicamente software o código desarrollado para cumplir un determinado fin.

En Android los ataques más comunes son:

Hummingbad es un malware que básicamente logra descargar aplicaciones sin que el usuario se tome la molestia de autorizarlo a dar el permiso para que esto suceda[58].

Hiddad este troyano “se propaga mediante servidores maliciosos, tiendas no oficiales y sitios de malvertising, haciéndose pasar por falsas soluciones móviles de seguridad, reproductores de música y videos, actualizaciones del sistema, Flash

[56]ALONSO, Rodrigo. Ginp: el troyano bancario que utiliza el coronavirus para atacar a los españoles [En línea]. Madrid: ABC Redes. 2020., Disponible en: https://www.abc.es/tecnologia/redes/abci-ginp-troyano-bancario-utiliza-coronavirus-para-atacar-espanoles-202003270221_noticia.html

[57] PCPROTECT. Cuál es la diferencia entre un malware y un virus? [En línea]. 2017., Disponible en: https://support.pcprotect.com/es/kb/article/44/cual-es-la-diferencia-entre-un-malware-y-un-virus

[58] LUQUE, Santiago. El malware HummingBad ha vuelto y se cuela en más de 45 apps de Google Play [En línea]. Xacata Android. 2017., Disponible en: https://www.xatakandroid.com/sistema-operativo/el-malware-hammingbad-ha-vuelto-y-se-cuela-en-mas-de-45-apps-de-google-play

Player, WhatsApp y aplicaciones de pornografía"[59], logrando una vez instalado lanzar múltiples anuncios publicitarios, hiddad en especial se hace pasar por una aplicación que mide el pulso cardiaco pero su finalidad es lanzar anuncios publicitarios.

Malware bancario es el código malicioso que logra introducirse para conseguir usuarios y claves con el objetivo de obtener los recursos depositados en las cuentas hackeadas.

Secuestro del portapapeles para éste caso el software logra capturar la información copiada en el portapapeles, aunque no sólo hace eso también tiene la capacidad de editar la información allí contenida, es decir que por ejemplo si copio una dirección web y el dispositivo está infectado y dicha dirección fue accedida y modificada al tratar de ingresar a esa dirección se puede estar re-direccionando a un sitio web falso[60].

6.2.4 Ataques a la seguridad en redes. Todo dispositivo (parte física o hardware) requiere de un software (parte lógica) para su funcionamiento, los dispositivos a tratar en ésta monografía son los dispositivos móviles cuya parte lógica que permite su funcionamiento es el Sistema Operativo Android, ahora teniendo en cuenta que con el dispositivo móvil es inevitable la conexión en redes, lo que permite sacar el máximo provecho de estos aparatos junto con las funcionalidades que contiene cada uno de ellos. Es preciso tener en cuenta los pros y contras de todo escenario, esto conduce a informar que a través de dichas conexiones se abre la puerta a los delincuentes que operan en la red, es así como surge la relevancia de detallar conceptos de actores que se pueden encontrar en ellas, expuestos a continuación:

- Hacker: Persona discreta con altas capacidades de aprendizaje y absorción de información cuyo objetivo es obtener información para su uso personal y disfruta mientras lo hace le gusta explorar lo desconocido y le gustan los retos intelectuales ya que les gusta superarlos y mejorar.
- Habilidades básicas:
  - Programar
  - Aprendizaje rápido
  - Solución de problemas de manera general

- Crackers: Son hackers cuya intención es más que la investigación, sus objetivos son malintencionados violando un sistema.

[59] GIUSTO, Denise. Troyanos propagan adware entre usuarios de Android [En línea]. Welivesecurity. 2018., Disponible en: https://www.welivesecurity.com/la-es/2018/01/04/troyanos-adware-usuarios-android/

[60] REDESZONE.NET. Qué es el secuestro del portapapeles [En línea]. 2020., Disponible en: https://www.redeszone.net/tutoriales/seguridad/secuestro-portapapeles-evitarlo/

- Phreakers: Son personas con amplios conocimientos en telefonía es decir crackers de las redes de comunicación utilizando herramientas de hardware y software.

- Carding: Personas que usan o generan de manera ilegítima tarjetas de crédito de otras personas para su propio beneficio económico con ayuda del hacking y el cracking para conseguir la información.

- Trashing: Personas cuyas habilidades son rastrear y buscar información como contraseñas o directorios.

Diferentes habitantes del ciberespacio:

- Gurus: Personas quienes forman los nuevos hackers.

- Lamers o script – kidders: Personas con conocimientos vagos pero que fingen saber más con el fin de molestar.

- Copyhackers: Personas falsificadoras y comercializadoras de lo robado.

- Bucaneros: Personas que venden lo crackeado.

- Newbie: Personas que buscan aprender técnicas de un hacker en un sistema de fácil acceso.

- Wannaber: Persona cuyo deseo es ser hacker pero considera que no tiene tal habilidad.

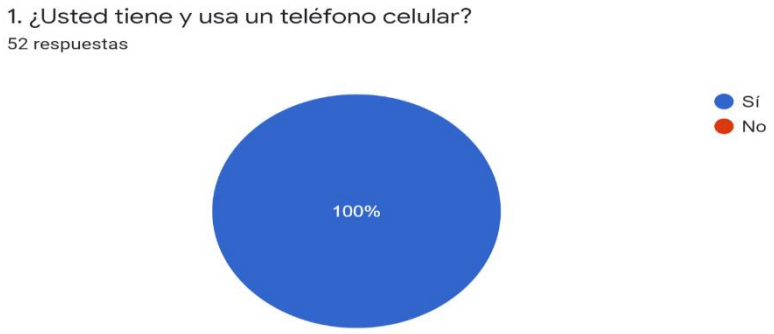
- Samural: Personas que tienen claro su objetivo y como llevarlo a cabo, trabaja por dinero y encargo.

- Piratas informáticos: Persona que realiza copias de soportes audiovisuales y realiza ventas ilegales.

6.2.5 Información recolectada encuesta para análisis de datos en Sistema Operativo Android. A través de encuesta realizada vía online, con la finalidad de identificar la apreciación de los usuarios del sistema operativo Android desde su versión Lollipop hasta la versión 10 en cuanto a usabilidad y seguridad se refiere, se identifica lo siguiente:

1. De las 52 personas encuestadas, el 100% cuenta con celular

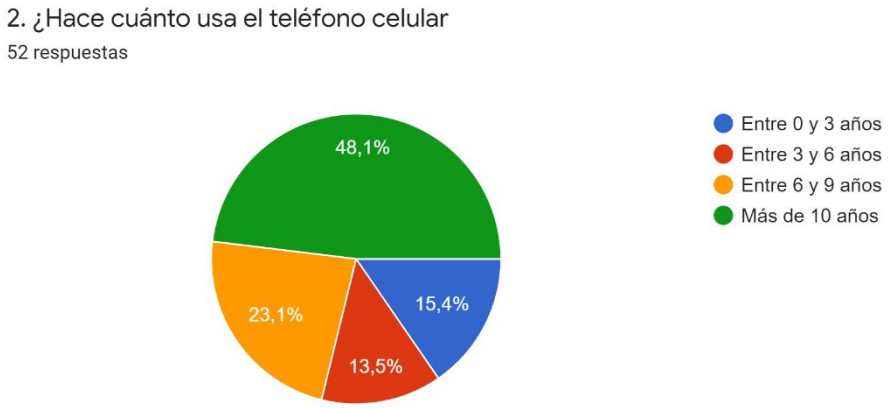
Figura 6. Personas que cuentan con teléfono celular



Fuente: Autor

2. De los encuestados el 48.1% reporto usar el celular desde hace más de 10 años, seguido entre el 15.4% y el 23.1% que reportan usarlo en un rango de 0 a 3 años y 6 a 9 años respectivamente, finalmente un 13.5% registra usar este dispositivo hace 3 a 6 años.

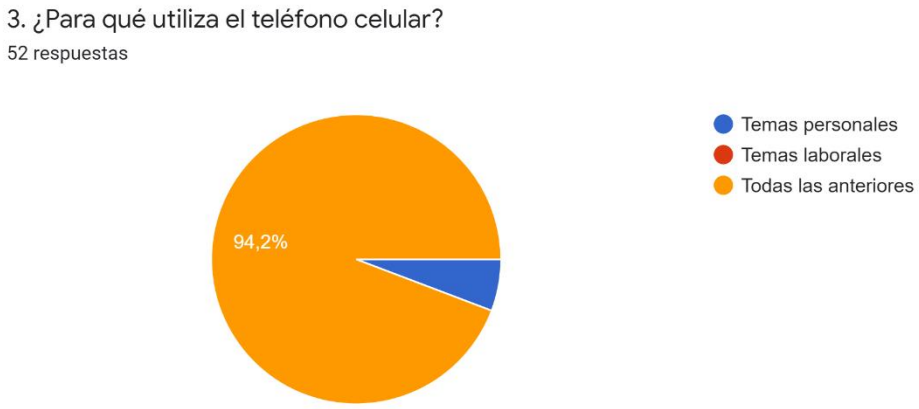
Figura 7. Tiempo que llevan usando el celular



Fuente: Autor

3. En cuanto a la utilidad que le dan a éste dispositivo se encuentra que el mayor porcentaje lo utiliza tanto para sus actividades personales como laborales, evidenciando que un 94.2 % lo usa para las dos actividades frente a un 5.8% que lo emplea solo para sus tareas personales.

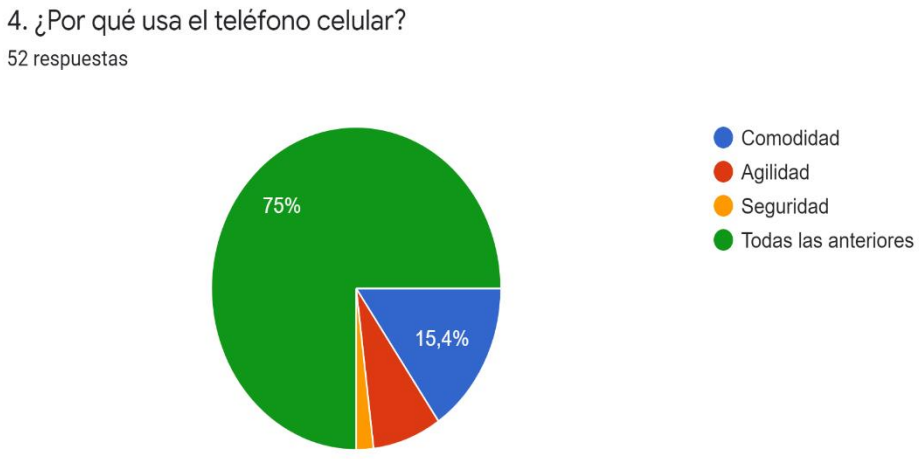
Figura 8. Actividades en las que se emplea el celular



Fuente: Autor

4. Entre las razones por las cuales las personas usan el celular se evidencian las características que brindan las tecnologías tales como la comodidad, agilidad y seguridad

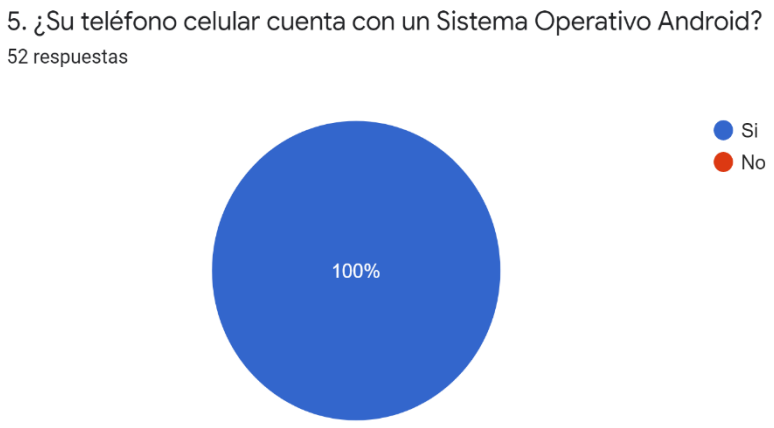
Figura 9. Motivos para usar el celular



Fuente: Autor

5. De la totalidad de los encuestados el 100% usa el sistema operativo Android

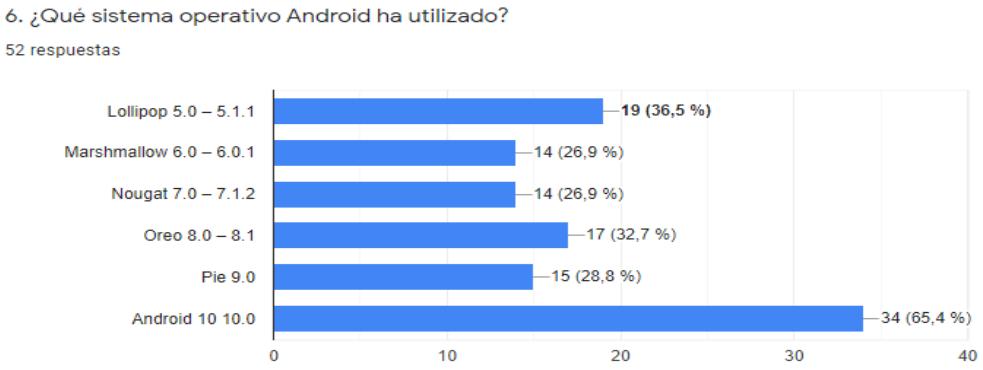
Figura 10. Sistema Operativo instalado en el celular



Fuente: Autor

6. En cuanto a las versiones del sistema operativo Android que han utilizado los participantes, desde la versión 5 Lollipop hasta la versión 10, es notable que las más usadas fueron la versión Lollipop y la versión 10, dejando ver que en su totalidad no realizaron actualización de versionamiento a medida que dichas actualizaciones salían al mercado.

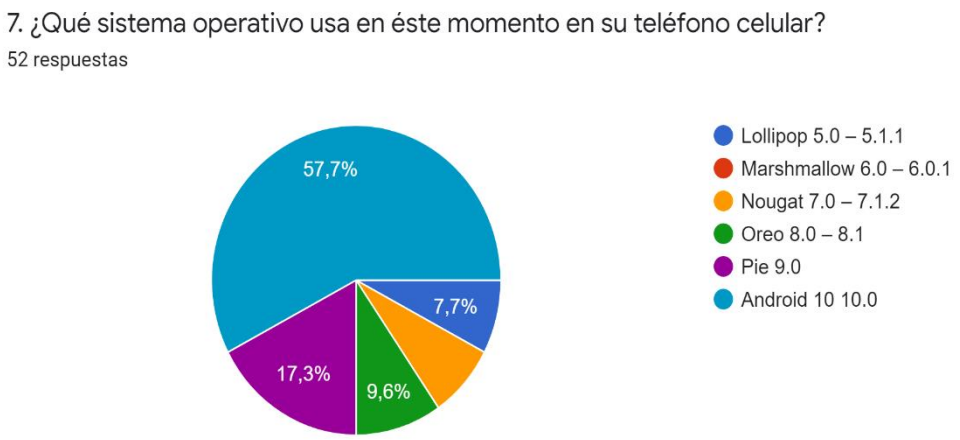
Figura 11. Versiones de Android usadas



Fuente: Autor

7. Actualmente la última versión estable lanzada por Google del sistema operativo es Android 10, y aunque un gran porcentaje (57.7%) ya lo está utilizando es evidente que no todos los usuarios de Android están manejando ésta última versión y aun un 7.7 % está usando la versión Android Lollipop, la cual ya no cuenta con soporte.

Figura 12. Versión de Android usada en la actualidad



Fuente: Autor

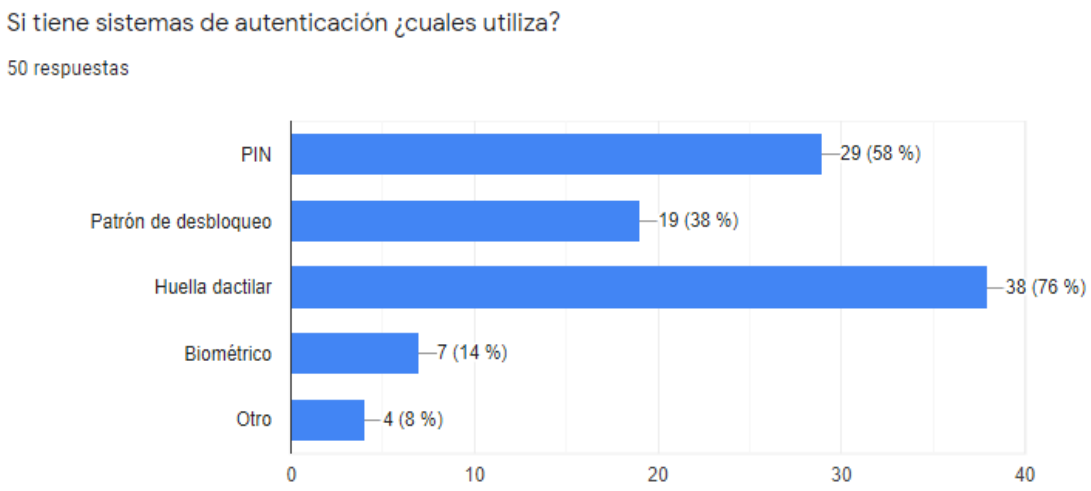
8. Ahora hablando de seguridad la mayoría de las personas que participaron en la encuesta usan algún sistema de autenticación para ingresar a los servicios y/o funcionalidades de su dispositivo.

Figura 13. Cuentan con algún sistema de autenticación para el acceso a los servicios del dispositivo

Fuente: Autor

Tales sistemas de autenticación para ejecutar cierta seguridad en el uso del dispositivo móvil en cuestión están en primer lugar la huella dactilar, seguida por el Pin y aunque en menor cantidad, pero no por ello menos importante el sistema biométrico.

Figura 14. Sistemas de autenticación usados en el celular



Fuente: Autor

9. Como se evidencia en el punto 3 las personas emplean su celular para tareas personales y laborales, lo que conduce a confirmar que por obvias razones la información que en mayor cantidad almacenan los usuarios tiene que ver con estas dos actividades, muy pocas almacenan información sólo personal.

Figura 15. Tipo de información que almacenan en el celular

Fuente: Autor

10. Entrando a la percepción de seguridad para los usuarios un 65.4% consideran que su celular es seguro, frente a un 34.6% que consideran lo contrario.

Figura 16. Percepción de seguridad de la información en el celular

Fuente: Autor

11. Continuando con la seguridad de la información un 88.5% consideran que saben cómo conservar a salvo la información que almacenan en sus dispositivos, a diferencia de un 11.5% que consideran lo contrario.

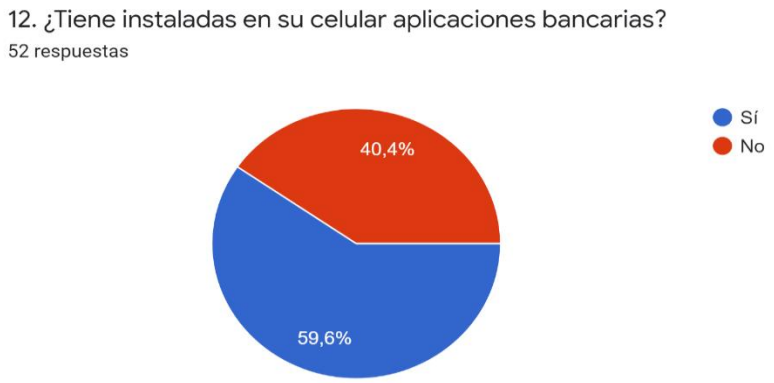
Figura 17. Percepción en cuanto a conocimiento de mantener segura la información almacenada en el dispositivo

Fuente: Autor

12. Teniendo en cuenta que por las características que presentan algunas aplicaciones para el interés del ciberdelincuente se indago entre los participantes si en sus dispositivos tienen apps bancarias, a lo cual un 59.6% respondió que si las tenía en su celular, siendo un poco más de la mitad de

los participantes los cuales en su mayoría seguramente en preguntas anteriores indican considerar que sus dispositivos son seguros.

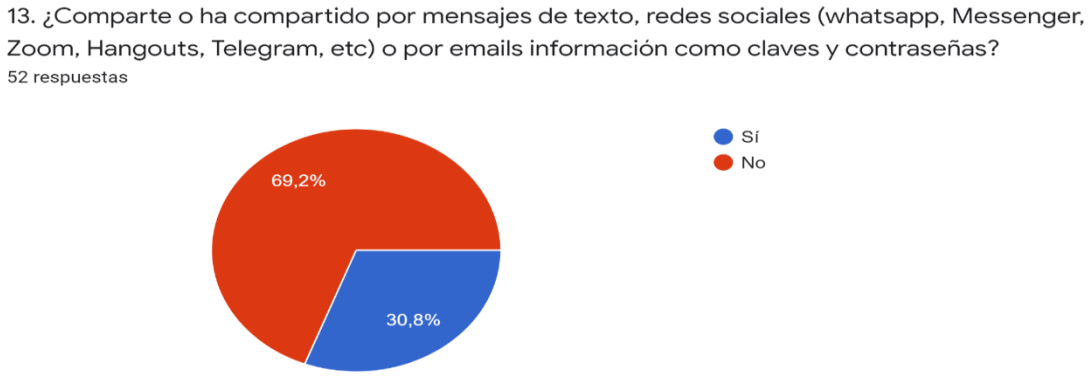
Figura 18. Uso de apps bancarias en el celular



Fuente: Autor

13. Otro de los usos más empleados en éstos dispositivos son las redes sociales y precisamente los que usualmente son empleados por los ciberdelincuentes, para aprovecharse del usuario, y bien aunque ésta redes son las más usadas los usuarios en su mayoría evitan compartir a través de estos medios información relacionada con claves y/o contraseñas, aunque es de alarmar que existe un cierto porcentaje que si lo hace.

Figura 19. Envíos de claves y/o contraseñas a través de mensajes



Fuente: Autor

Pues bien, se evidencia que el dispositivo celular es bastante usual y que éste es empleado para diversas labores o actividades, los encuestados en su totalidad usan el sistema operativo Android aunque no se debe desconocer que otros usuarios

puedan utilizar un sistema operativo diferente Android es el más usado en los dispositivos móviles, hablando de las actualizaciones de éste sistema operativo se muestra que los usuarios no van avanzando a la par con las actualizaciones o versiones lanzadas por el administrador del sistema operativo, dejando una posible brecha de seguridad.

Ahora pasando por la percepción de seguridad se revela que para los usuarios el celular es seguro y en la mayoría usan sistemas de autenticación que brindan cierta seguridad en cuanto a la información se refiere, aunque un porcentaje no muy bajo expone claves o contraseñas y posiblemente más datos confidenciales por medio de las apps que éstas tecnologías permiten emplear.

Entonces una vez recopilada la información del sistema operativo a analizar, los riesgos, peligros, amenazas y/o ataques a los que se encuentran expuestos los usuarios de tal sistema operativo y los delincuentes que en ellos pueden intervenir, se procede a elaborar un manual que contenga buenas prácticas que el usuario pueda implementar para contrarrestar los peligros a los que su información este expuesta.

6.3 MANUAL DE BUENAS PRÁCTICAS DE USUARIO, QUE PERMITA MITIGAR LOS RIESGOS DE LA INFORMACIÓN ASOCIADOS AL SISTEMA OPERATIVO ANDROID LOLLIPOP Y SUS VERSIONES POSTERIORES

Hablando de seguridad tanto en los dispositivos como la seguridad en redes, se busca la implementación de políticas y prácticas con el fin de prevenir y controlar el manejo, uso y manipulación de la red y sus recursos. Irradiando en la confidencialidad, integridad y vinculación de información en un sistema, en la búsqueda de la seguridad de la información para que no pueda ser accedida por criminales cibernéticos, las redes pueden ser privadas o públicas y son usadas en labores cotidianas.

Aunque tampoco es un secreto que el delincuente o ciberdelincuente también está constantemente activo y en búsqueda de las oportunidades a las que le pueda sacar provecho.

Por lo anteriormente expuesto no cabe la menor duda que los desarrolladores del Sistema Operativo Android van siempre enfocados en fortalecer éste software, brindándole seguridad al usuario final en paralelo a las funcionalidades que le brindan calidad a dicho usuario.

ASPECTOS A TENER EN CUENTA PARA CUIDAR O PROTEGER LA INFORMACION

TIPOS DE SEGURIDAD

Física equivalente al hardware:

Evite usar el celular en zonas publicas inseguras.
Mantenga su dispositivo fuera de fuentes de calor y de humedad.
Desconecte su celular tan pronto realice la carga completa de la batería.

Lógica equivalente al software:

Realizar las actualizaciones a la versión más reciente del sistema operativo es importante, pues ellas cuentan con los parches de seguridad desarrollados para contrarrestar las fallas de seguridad encontradas.

Realizar actualización constante del software, instalar aplicaciones y/o herramientas que permitan contrarrestar los virus o malware, con el fin de proteger la información.

Pantalla limpia y despejada, elimine las apps que no utilice y no hagan parte del sistema, eso evitará que se estén ejecutando en segundo plano y que puedan ser accedidas por software informático no deseado.

Implementar proceso de backup periódico y guardado fuera de línea, para posterior recuperación de información en caso de daños.

Verificar que no se instalen programas automáticamente.

Acceso controlado, verifique quienes tienen acceso a su dispositivo, la información y las aplicaciones contenidas en éste.

Utilizar diferentes contraseñas para las aplicaciones que manejen información confidencial e importante.

Cambiar contraseñas regularmente.

Implementar claves con patrones de parámetros seguros o complejos.

En las aplicaciones que se lo permitan utilice contraseñas que sean mayores de 8 caracteres, en los cuales pueda usar letras, números y símbolos con el fin de evitar que sean fácilmente descifradas y brinden una mayor seguridad a su información.

No enviar contraseñas a través de formularios o encuestas.

No descargar ni abrir archivos adjuntos de correos o remitentes desconocidos o extraños.

Navegar en páginas que utilicen el protocolo seguro de transferencia de hipertexto (https), no hacer uso de hipervínculos desconocidos o extraños.

Sea precavido con la información que pública y comparte en redes sociales, tenga en cuenta que a través de las redes sociales se puede viralizar cualquier tipo de información, por ello es importante que siempre piense que consecuencias puede acarrearle el compartir cierta información o documentación.

Cerrar las sesiones de sus cuentas cuando no las estén usando y evitar la navegación en sitios web no confiables, son buenas practicas para contrarrestar ataques.

7. CONCLUSIONES

A partir de la revisión bibliográfica se concluye que el componente humano tiene un papel importante en abrir o no las puertas a la inseguridad de los dispositivos con el S.O. Android, cuando las personas se concientizan de llevar a cabo buenas practicas, esto ayuda en la mitigación de las vulnerabilidades y riesgos a los que se está expuesto.

Dentro del estudio de seguridad en S.O. Android se puede concluir que un gran porcentaje de la población utiliza éste sistema operativo, empleando sus dispositivos para tareas personales y laborales, siempre es importante verificar la procedencia de las aplicaciones que se instalen y usen en los dispositivos, así como asegurarse de navegar en páginas seguras en la web y de no descargar archivos de fuentes sospechosas.

Después de analizar la información recopilada acerca del S.O. Android a nivel de seguridad se estimó que los usuarios lo perciben muy seguro y aun cuando en las tiendas oficiales de Android se esfuercen por garantizar la seguridad de las apps que se pueden encontrar allí, esto no asegura que todo lo encontrado en ésta sea cien por ciento seguro. Así mismo la seguridad informática no está completamente garantizada para un sistema operativo, bajo ningún medio y para ningún dispositivo, por lo tanto es importante la consulta en fuentes confiables del nivel de seguridad para lo que brindan las tecnologías.

Cabe señalar que las técnicas usadas en seguridad informática, así como pueden generar un ambiente y entorno satisfactorio, también pueden ser usadas de manera malintencionada dependiendo de la ética profesional y personal de las personas que la utilizan. Se debe estar preparado para todos los posibles usos que se le pueda dar a las ciencias y técnicas aplicadas en los ambientes informáticos y tecnológicos, para garantizar la seguridad de la información y de los medios que la salvaguardan.

8. RECOMENDACIONES

Teniendo en cuenta que un gran porcentaje de la seguridad depende de cada individuo, es importante tener en cuenta y llevar a cabo las siguientes indicaciones:

Utilizar y mantener actualizados los antivirus y antispyware.

No abrir ni descargar archivos adjuntos de remitentes extraños o desconocidos.

Navegar en páginas que utilicen el protocolo seguro de transferencia de hipertexto (https).

No hacer uso de hipervínculos desconocidos o extraños.

Hacer copias de seguridad (backup) periódicos de la información relevante de manera constante, facilitando una posterior recuperación en caso de daños.

Verificar que no se instalen programas automáticamente.

Asegurarse de no otorgar derechos de administrador del equipo a aplicaciones o personas desconocidas.

Mantener el antivirus y aplicaciones actualizadas.

El mejor método para la recuperación de la información afectada por un ransomware es la utilización de las copias de seguridad, es por esto que se deben realizar de manera periódica y en lo posible custodiarlas fuera de línea.

BIBLIOGRAFÍA

ABC. Un nuevo y grave fallo de seguridad en Android deja vendidos a los usuarios por culpa de una simple foto [En línea]. Madrid. 2019., Disponible en: https://www.abc.es/tecnologia/informatica/software/abci-nuevo-y-grave-fallo-seguridad-android-deja-vendidos-usuarios-culpa-simple-foto-201902131742_noticia.html?ref=https%3A%2F%2Fwww.google.com%2F

ABC REDES. Las amenazas en Android no dejan de crecer: hay 11.700 aplicaciones nuevas al día [En línea]. Madrid: Abc.es. 2018., Disponible en: https://www.abc.es/tecnologia/redes/abci-amenazas-android-no-dejan-crecer-11700-aplicaciones-maliciosas-nuevas-201811121812_noticia.html#vca=mod-sugeridos-p1&vmc=relacionados&vso=android-sigue-siendo-un-coladero-de-apps-maliciosas&vli=noticia.foto.tecnologia

ALBORS, Josep. Las 5 mejoras de seguridad de Android Lollipop.[En línea]. Bogotá: Welivesecurity. 2014., Disponible en: https://www.welivesecurity.com/la-es/2014/11/03/5-mejoras-seguridad-android-lollipop/ .

ALCALDIA MAYOR DE BOGOTA D.C. Constitución Política de 1991 [En línea].Régimen Legal de Bogotá D.C. 2020., Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

ALCALDIA MAYOR DE BOGOTA D.C. Decreto 1377 de 2013 [En línea]. Régimen Legal de Bogotá D.C. 2020., Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646#0

ALONSO, Rodrigo. Ginp: el troyano bancario que utiliza el coronavirus para atacar a los españoles [En línea]. Madrid: ABC Redes. 2020., Disponible en: https://www.abc.es/tecnologia/redes/abci-ginp-troyano-bancario-utiliza-coronavirus-para-atacar-espanoles-202003270221_noticia.html

AMADEO, Ron. A history of pre-cupcake Android codenames [En línea]. Android Police. 2012., Disponible en: https://www.androidpolice.com/2012/09/17/a-history-of-pre-cupcake-android-codenames/

ANDROID. Android 6.0 Marshmallow [En línea]. 2015., Disponible en: https://www.android.com/intl/es_es/versions/marshmallow-6-0/

ANDROID. Android 7.0 Nougat [En línea]. 2016., Disponible en: https://www.android.com/intl/es_es/versions/nougat-7-0/

ANDROID. Android 8.0 Oreo [En línea]. 2017., Disponible en: https://www.android.com/versions/oreo-8-0/

ANDROID. Android 9 Pie [En línea]. 2018., Disponible en: https://www.android.com/versions/pie-9-0/

ANDROID. Android 10 [En línea]. 2019., Disponible en: https://www.android.com/android-10/

ANDROID. Android Security 2015 Year in Review [En línea]. 2016., Disponible en: https://source.android.com/security/reports/Google_Android_Security_2015_Report_Final.pdf .

BELLIDO VEIZAGA, Wilfredo Jesús. Ethical Hacking: Hacking de Red Inalámbrica Wifi [En línea]. Revista de Información, Tecnología y Sociedad versión impresa ISSN 1997-4044. La Paz. 2013., Disponible en: http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100021&script=sci_arttext&tlng=es

BARRIO ANDRES, Moisés. Internet de las cosas. Editorial Reus. 2018

BETANCUR JARAMILLO, Oscar y ERASO HANRRYR, Sonia Elizabeth. Seguridad en dispositivos móviles Android. Monografía. Bogotá: Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas Tecnología e Ingeniería, 2015. 109 p.

CARBALLAR, José Antonio. WI-FI. Lo que se necesita conocer. RC Libros, 2010

CATACORA, Jesús Luciano. Analizando el nivel de seguridad del entorno de Android. Tesina de Licenciatura. La Plata: Universidad Nacional de La plata, Facultad de Informática, 2016. 184 p.

CENTRO CIBERNETICO POLICIAL. Skimming [En línea]. Bogotá. 2018., Disponible en: https://caivirtual.policia.gov.co/mural-cibercrimen/skimming .

CENTRO CIBERNETICO POLICIAL. Smishing, [En línea]. Bogotá. 2018., Disponible en: https://caivirtual.policia.gov.co/mural-cibercrimen/smishing .

DEFENSORIA.GOV. Ley Estatutaria 1581 de 2012. [En línea]. El Congreso de Colombia. 2012., Disponible en: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

DIARIO OFICIAL. Ley 1273 de 2009 [En línea]. El Congreso de Colombia Decreta. 2009., Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

DOMINICCI, José. Estudio de caso: malware en Android [En línea]. 2011., Disponible en: https://s3.amazonaws.com/academia.edu.documents/36682501/TopicPaper.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1527183432&Signature=HfgGt1FDeSVao8J6sJWZFSuYxcE%3D&response-content-disposition=inline%3B%20filename%3DMalware_en_Android.pdf

DPA. Nuevo virus de Android podría dañar físicamente tu teléfono [En línea]. Madrid: Milenio 2020. 2017., Disponible en: http://www.milenio.com/estilo/nuevo-virus-de-android-podria-danar-fisicamente-tu-telefono .

ECONOMIA Y NEGOCIOS. En el país hay más hogares con celular que con acueducto [En línea]. Bogotá: El Tiempo.com. 2017., Disponible en https://www.eltiempo.com/economia/finanzas-personales/colombianos-tienen-mas-celulares-que-servicio-de-agua-68584 .

ELGIN, Ben. Google Buys Android for Its Mobile Arsenal [En línea]. Bloomberg Businessweek. 2005., Disponible en: https://www.webcitation.org/5wk7sIvVb?url=http://www.businessweek.com/technology/content/aug2005/tc20050817_0949_tc024.htm

ENCICLOPEDIA ECONOMICA. Muestreo por conveniencia [En línea]. 2019., Disponible en: https://enciclopediaeconomica.com/muestreo-por-conveniencia/

FERRO VEIGA, José Manuel. Asesor/Gestor en seguridad privada integral: Curso superior en dirección de seguridad privada. José Manuel Ferro Veiga, 2020.

GARCIA MOLINA, Teresa y MOREIRA PARRAGA, Jorge. Evaluación de protocolos de seguridad de las app de redes sociales en dispositivos móviles Android [En línea]. Manabí: Escuela Superior Politecnica Agropecuaria de Manabí. 2016., Disponible en: http://repositorio.espam.edu.ec/handle/42000/299 .

GIUSTO, Denise, Balance semestral de la seguridad móvil [En línea]. Bogotá: Welivesecurity. 2018., Disponible en: https://www.welivesecurity.com/la-es/2018/08/06/balance-semestral-seguridad-movil/ .

GIUSTO, Denise. Troyanos propagan adware entre usuarios de Android [En línea]. Welivesecurity. 2018., Disponible en: https://www.welivesecurity.com/la-es/2018/01/04/troyanos-adware-usuarios-android/

GOBIERNO EN LÍNEA. Las tecnologías emergentes serán fundamentales para combatir el cibercrimen en Latinoamérica [En línea]. Bogotá: Entérate. 2018., Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/w3-article-80353.html .

GOOGLE PLAY. Centro de Políticas de Desarrolladores [En línea]. Contenido Restringido. 2020., Disponible en: https://play.google.com/intl/es/about/restricted-content/child-endangerment/ .

HARAN, Juan Manuel, Descubren malware bancario en Google Play dirigido a usuarios de Brasil [En línea]. Bogotá: Welivesecurity. 2018., Disponible en: https://www.welivesecurity.com/la-es/2018/10/30/descubren-malware-bancario-google-play-dirigido-usuarios-brasil/ .

IDAT. Internet de las cosas: 10 ejemplos innovadores [En línea]. Lima. 2019., Disponible en: https://www.idat.edu.pe/blog/internet-de-las-cosas-10-ejemplos-innovadores

KHANDELWAL, Swati, Fake WhatsApp On Google Play Store Downloaded By Over 1 Million Android Users [En línea]. The Kacker News. 2017., Disponible en: https://thehackernews.com/2017/11/fake-whatsapp-android.html .

LA POLICIA NACIONAL. Normatividad sobre delitos informáticos [En línea]. Código Penal Colombiano Ley 599 de 2000. 2020., Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

LUQUE, Santiago. El malware HummingBad ha vuelto y se cuela en más de 45 apps de Google Play [En línea]. Xacata Android. 2017., Disponible en: https://www.xatakandroid.com/sistema-operativo/el-malware-hammingbad-ha-vuelto-y-se-cuela-en-mas-de-45-apps-de-google-play

MARTIN, Alberto. El Internet de las cosas: Android en todas partes [En línea]. España. 2014., Disponible en: https://computerhoy.com/noticias/hardware/internet-cosas-android-todas-partes-13823

MENDOZA LOPEZ, Miguel. Riesgos de Seguridad en Android. [En línea]. México: Universidad Nacional Autónoma de México. 2015,, Disponible en: https://revista.seguridad.unam.mx/numero23/riesgos-de-seguridad-en-android

MICROSOFT. Trojan: AndroidOS/Fakeplayer.A [En línea]. Microsoft Security Intelligence. 2010., Disponible en: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%253AAndroidOS%252FFakeplayer.A

MONTOYA GARCIA, Jonathan. ¿Por qué es más inseguro el sistema Android que Ios? [En línea]. Bogotá: El Colombiano.com. 2017., Disponible en: http://www.elcolombiano.com/tecnologia/seguridad-en-celulares-android-y-apple-YE6521203 .

NDTV. 8 New features in the next major Android reléase [En línea]. Gadgets 360ª. 2014., Disponible en: https://gadgets.ndtv.com/mobiles/news/android-l-8-new-features-in-the-next-major-android-release-548283

BANDO, Mariangel. Google apuesta por el "Internet de las cosas" con Android Things [En línea]. LaRepublica.Net. 2018., Disponible en: https://www.larepublica.net/noticia/google-apuesta-por-el-internet-de-las-cosas-con-android-things

PACHECO VELIZ, Sebastian Exequiel y PIAZZA ORLANDO, Carlos Damian. Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones. Tesina de Licenciatura. La Plata: Universidad Nacional de La plata, Facultad de Informática, 2016. 139 p.

PASCUAL, Juan. Android vs iPhone: la guerra de los smartphones en cifras [En línea]. Computer Hoy. 2018., Disponible en: https://computerhoy.com/reportajes/industria/android-vs-iphone-guerra-smartphones-cifras-271447 .

PCPROTECT. ¿Cuál es la diferencia entre un malware y un virus? [En línea]. 2017., Disponible en: https://support.pcprotect.com/es/kb/article/44/cual-es-la-diferencia-entre-un-malware-y-un-virus

REDESZONE.NET. Qué es el secuestro del portapapeles [En línea]. 2020., Disponible en: https://www.redeszone.net/tutoriales/seguridad/secuestro-portapapeles-evitarlo/

SOFTWARE DE COMUNICACIONES. Aplicaciones en Android [En línea]. 2020., Disponible en: https://sites.google.com/site/swcuc3m/home/android/generalidades/aplicacionespag3

SOURCE. ANDROID. Asegure un dispositivo Android [En línea]. 2020., Disponible en: https://source.android.com/security

SOURCE.ANDROID. Seguridad del sistema y del núcleo [En línea]. 2020., Disponible en: https://source.android.com/security/overview/kernel-security?hl=es-419

TECNOLOGIA. Que es un Smartphone. [En línea]. 2020., Disponible en: https://www.areatecnologia.com/Que-es-un-smartphone.htm

TECNOLOGÍA EMPRESARIAL. El Factor humano como amenaza interna a la seguridad de la información [En línea]. Managua: El Nuevo Diario. 2013., Disponible en https://www.elnuevodiario.com.ni/economia/300466-factor-humano-amenaza-interna-seguridad-informacio/ .

TECNOSFERA. Android, el sistema operativo con más vulnerabilidades en 2017. [En línea]. Bogotá: El Tiempo.com. 2018., Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/android-fue-el-sistema-operativo-con-mas-vulnerabilidades-en-2017-167314 .

TECNOSFERA. Colombianos tocan su celular 2 mil veces al día en estas actividades. [En línea]. Bogotá: El Tiempo.com. 2019., Disponible en: https://www.eltiempo.com/tecnosfera/dispositivos/encuesta-de-consumo-movil-en-colombia-2019-389702

TECNOSFERA. Descubren 29 aplicaciones en Android que robaban datos bancarios. [En línea]. Bogotá: Eltiempo.com. 2018., Disponible en: http://origen.pre.eltiempo.com/tecnosfera/apps/29-apps-maliciosas-que-roban-sus-datos-bancarios-288478 .

TECNOSFERA. Vida social, en lo que más usan los colombianos el celular. [En línea]. Bogotá: El Tiempo.com. 2017., Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/uso-del-celular-y-el-internet-en-colombia-149384 .

TORO SANCHEZ, Cristian Giovanny, VARGAS CARVAJAL, Jesús Alfredo y otro. Guía para validar el nivel de seguridad de los permisos y uso de recursos de una aplicación móvil bajo plataformas Android. Trabajo de grado. Bogotá D.C: Universidad Católica de Colombia, Facultad de Ingeniería, 2015. 72 p.

TU GIMNASIA CEREBRAL. Las encuestas – Qué son, características, cómo hacerlas [En línea]. Bogotá. 2014., Disponible en: http://tugimnasiacerebral.com/herramientas-de-estudio/que-es-una-encuesta-caracteristicas-y-como-hacerlas

UNIVERSO FORMULAS. Muestreo no probabilístico [En línea]. 2019.,Disponible en: https://www.universoformulas.com/estadistica/inferencia/muestreo-no-probabilistico/

UPM, Lección 17: Datos Personales. Guía de Seguridad para Usuarios (intypedia) Malware [En línea]. 2013., Disponible en: https://www.youtube.com/watch?feature=player_embedded&v=qNKozIsD31M#! .

VenTICs.com. Estadísticas de uso de Android por países. [En línea]. 2018., Disponible en: http://www.ventics.com/estadisticas-uso-android-paises/ .

VILLA YAÑEZ, Henry y CISNEROS BARAHONA, Andres. Detección de vulnerabilidades en aplicaciones que funcionan sobre el sistema operativo Android, mediante el desarrollo de una aplicación tecnológica. [En línea]. Revista Espacios. 2017., Disponible en: http://www.revistaespacios.com/a18v39n11/18391107.html .

ANEXO

ANEXO 1. Encuesta Online

Encuesta para Análisis de datos en Sistema Operativo Android

Con el objetivo de identificar su percepción y conocimientos acerca de la seguridad en el Sistema Operativo Android desde la versión Lollipop lanzada en el 2014 hasta la versión 10 lanzada en 2019, se solicita su colaboración con el diligenciamiento de las siguientes preguntas:

*Obligatorio

1. ¿Usted tiene y usa un teléfono celular? *

- ◯ Sí
- ◯ No

2. ¿Hace cuánto usa el teléfono celular *

- ◯ Entre 0 y 3 años
- ◯ Entre 3 y 6 años
- ◯ Entre 6 y 9 años
- ◯ Más de 10 años

3. ¿Para qué utiliza el teléfono celular? *

- ◯ Temas personales
- ◯ Temas laborales
- ◯ Todas las anteriores

4. ¿Por qué usa el teléfono celular? *

- ◯ Comodidad
- ◯ Agilidad
- ◯ Seguridad
- ◯ Todas las anteriores

5. ¿Su teléfono celular cuenta con un Sistema Operativo Android? *

- ◯ Si
- ◯ No

Si no cuenta con Sistema Operativo Android. ¿Qué sistema operativo utiliza?

Tu respuesta

6. ¿Qué sistema operativo Android ha utilizado? *

- ☐ Lollipop 5.0 – 5.1.1
- ☐ Marshmallow 6.0 – 6.0.1
- ☐ Nougat 7.0 – 7.1.2
- ☐ Oreo 8.0 – 8.1
- ☐ Pie 9.0
- ☐ Android 10 10.0

7. ¿Qué sistema operativo usa en éste momento en su teléfono celular? *

- ◯ Lollipop 5.0 – 5.1.1
- ◯ Marshmallow 6.0 – 6.0.1
- ◯ Nougat 7.0 – 7.1.2
- ◯ Oreo 8.0 – 8.1
- ◯ Pie 9.0
- ◯ Android 10 10.0

8. Si usa Sistema Operativo Android, ¿tiene algún sistema de autenticación para acceder a los servicios de su teléfono celular? *

- ◯ SI
- ◯ No

Si tiene sistemas de autenticación ¿cuales utiliza?

- ☐ PIN
- ☐ Patrón de desbloqueo
- ☐ Huella dactilar
- ☐ Biométrico
- ☐ Otro

No utiliza sistema de autenticación ¿por qué?

Tu respuesta

9. ¿Qué tipo de información almacena en su teléfono celular? *

- ◯ Personal
- ◯ Laboral
- ◯ Todas las anteriores
- ◯ Ninguna de las anteriores

10. Considera que su teléfono celular es seguro para guardar información *

- ◯ Sí
- ◯ No

11. ¿Sabe cómo salvaguardar la información que contiene su teléfono celular? *

- ◯ Sí
- ◯ No

12. ¿Tiene instaladas en su celular aplicaciones bancarias? *

- ◯ Sí
- ◯ No

13. ¿Comparte o ha compartido por mensajes de texto, redes sociales (whatsapp, Messenger, Zoom, Hangouts, Telegram, etc) o por emails información como claves y contraseñas? *

- ◯ Sí
- ◯ No

Página 1 de 1 Enviar