Fundación Universitaria

SAN MATEO

TÉCNICO PROFESIONAL EN SOPORTE DE SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES

FUNDACIÓN UNIVERSITARIA SAN MATEO

ANÁLISIS DE VULNERABILIDADES EN DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO ANDROID

TRABAJO DE GRADO MODALIDAD DE OPCIÓN DE GRADO

HAROL CAMILO BERNAL MEDINA

DIRECTOR (A)

EDWARD REYES CORREDOR

BOGOTÁ

2022

NOTA DE SALVEDAD DE RESPONSABILIDAD INSTITUCIONAL

"La Fundación Universitaria San Mateo NO se hace responsable de los conceptos emitidos en el presente documento, el departamento de investigaciones velará por el rigor metodológico de la investigación".

CONTENIDO

ÍNDICE DE TABLAS

INDICE DE ANEXOS

ÍNDICE DE FIGURAS

DEDICATORIA

Dedico este trabajo a toda mi familia. Principalmente, a mis padres quienes con su apoyo incondicional me han brindado el apoyo y comprensión en los momentos malos y los no tan malos. Ellos me han enseñado a ser la persona que soy, mis principios, mis valores, mi perseverancia y esfuerzo, todo esto brindado siempre con amor y sin esperar nada a cambio.

También quiero dedicar este trabajo a mi tutor de grado, que con gran dedicación y esfuerzo brindaba cada una de sus tutorías, gracias a ellas pude encontrar el mejor camino hacia el desarrollo del presente proyecto.

Finalmente me dedico este proyecto por el hecho de no darme por vencido y mantener la perseverancia durante el desarrollo del mismo, sentir la satisfacción de poder finalizarlo.

AGRADECIMIENTOS

“Cuando la gratitud es tan absoluta, las palabras sobran”. Álvaro Mutis

Con esta frase inicio mis agradecimientos primeramente a Rocío por darme la vida y poder disfrutar de ella con todo y sus altibajos.

A Pedro por enseñarme valores como la humildad, responsabilidad y perseverancia.

A Kevin por ser mi hermano y el mejor amigo que he tenido.

A Edward por brindar sus conocimientos y virtudes para poder guiarme durante todo el proyecto.

A todos ustedes y los que faltaron nombrar, mi más profundo agradecimiento y mis más sinceros respetos

¡Gracias!

ABREVIATURAS

NIST: National Institute of Standards and Technology (Instituto Nacional de Estandares y Tecnologia).

IBM: International Business Machines (Máquina de Negocios Internacionales).

CVE: Common Vulnerabilities and Exposures (Vulnerabilidades y Exposiciones Comunes).

GSMA: Global System Mobile Association (Asociacion Global de Sistemas Moviles).

ESET: Compañía de software especializada en ciberseguridad.

ISO: International Organization for Standardization (Organización Internacional de Normalización).

IEC: International Electrotechnical Commission (Comisión Electrotécnica Internacional).

SGSI: Information Security Management System (Sistema de Gestión de Seguridad de la Información).

PDCA: Ciclo deming Plan,Do,Check and Act (Plan,Hacer,Verificar yActuar).

VPN: Virtual Private Network (Red Privada Virtual).

TI: Tecnología de la información

NTS SEIDOR: Compañía de integración de soluciones software especializada en movilidad, Cloud Computing y Mobile Device Management.

OWASP: Open Web Application Security Project (Proyecto Abierto de Seguridad de las Aplicaciones Web.)

TLS: Transport Layer Security (Seguridad de la capa de transporte.)

X.509: Formato de certificado estándar para claves públicas.

QR: Quick Response (Respuesta rápida.)

GPS: Global Positioning System (Sistemas de Posicionamiento Global.)

RESUMEN

Es evidente el uso frecuente de Smartphone en la actualidad, se pueden ver en diferentes contextos como centros comerciales, oficinas, reuniones e instituciones educativas entre otros; a nivel personal la seguridad juega un factor importante rigiéndose a la normativa NIST 800-155, norma desarrollada por el Instituto Nacional de Estándares y Tecnologías de los Estados Unidos. Se evidencia una serie de pruebas en vulnerabilidades, como test de implantación y análisis que permiten desarrollar buenas prácticas en las que se enfocan en la mitigación de estas, y a su vez cumple con los factores fundamentales en la seguridad de la información, como lo es la disponibilidad, integridad y confidencialidad de los dispositivos.

El objetivo de esta investigación será indagar en la documentación existente las vulnerabilidades a nivel de ciberseguridad, que presenta los dispositivos móviles con sistema operativo Android además de determinar las buenas prácticas para así evitar de manera eficiente las vulnerabilidades o amenazas descritas en este documento, todo ello sintetizado mediante una página web.

Esta investigación va dirigida hacia aquella población que puede obtener un dispositivo

Móvil que va desde personas mayores de dieciocho años de edad y hasta los cincuenta años, principalmente a las personas con poco o ningún conocimiento acerca de la seguridad en los dispositivos móviles.

Lo mencionado anteriormente se llevará a cabo mediante la metodología de la investigación en la que consiste recolectar información, analizar y finalmente mediante gráficos evidenciar los resultados obtenidos.

PALABRAS CLAVE: Sistema operativo; Android; Vulnerabilidades.

ABSTRACT

It is evident the frequent use of Smartphones nowadays, they can be seen in different contexts such as shopping malls, offices, meetings and educational institutions among others; at a personal level security plays an important factor, following the NIST 800-155 standard developed by the National Institute of Standards and Technologies of the United States. There is evidence of a series of tests on vulnerabilities, such as implementation tests and analysis that allow the development of good practices that focus on mitigating these, and in turn meets the fundamental factors in the security of information, such as availability, integrity and confidentiality of the devices.

The objective of this research will be to investigate in the existing documentation the vulnerabilities at the level of cybersecurity, which presents mobile devices with Android operating system in addition to determining good practices to efficiently avoid the vulnerabilities or threats described in this document, all synthesized through a web page.

This research is directed towards that population that can obtain a mobile device, ranging from people over the age of 18 to those

Mobile that goes from people older than six years old and up to sixty years old, mainly to people with little or no knowledge about security in mobile devices. The aforementioned will be carried out through the research methodology which consists of collecting information, analyzing and finally using graphs to demonstrate the results obtained.

KEYWORDS: Operating system; Android; Vulnerabilities.

INTRODUCCIÓN

El presente documento presenta las vulnerabilidades del sistema operativo Android, mediante el método de investigación; que determina las vulnerabilidades más frecuentes en los dispositivos móviles, además de las buenas prácticas para evitar de manera eficiente las amenazas descritas en el presente anexo.

Por otra parte, se busca como medio de acceso a la información aquí descrita, la creación y publicación de una página web, en donde se encontrará lo anteriormente mencionado.

La seguridad en dispositivos móviles se refiere a estar libre de peligros o riesgos de pérdidas de información o datos, al momento de usar dispositivos móviles. Hoy en día, los cibercriminales pueden hackear o piratear autos, cámaras de seguridad y hasta dispositivos diseñados para el cuidado de la salud. “Para 2025, podría haber más 75 millones de “cosas” conectadas a internet, incluidas cámaras, termostatos, cerraduras de puertas, televisores inteligentes, bombillas y muchos otros dispositivos”. *Artículo de IBM “¿Por qué es importante la ciberseguridad?”*

Por esta razón es de vital importancia tanto para las grandes industrias como para las personas, garantizar la seguridad de los dispositivos que frecuentan, ya que la tecnología a lo largo de los años o más bien desde su creación se ha vuelto indispensable para la vida diaria de cualquier persona, por ende, en un futuro nos veremos mucho más rodeados de dispositivos tecnológicos, que en gran medida llegan a volverse contraproducentes.

El propósito de este proyecto será analizar la documentación existente, referente a las vulnerabilidades de los dispositivos móviles Android, por medio del método investigativo, además de determinar las mejores prácticas y recomendaciones para disminuir la susceptibilidad a riesgos o peligros que vulneren los mismos.

La metodología de investigación es de carácter cualitativo ya que no se plantea una hipótesis, sino que se elabora una serie de conclusiones partiendo de los antecedentes de investigaciones similares dentro del

campo de la seguridad informática y el análisis de riesgos en sistemas operativos de Smartphone específicamente Android.

Unidad de Análisis

La unidad de análisis implementada en este trabajo investigativo está enfocada a los dispositivos móviles Android y sus usuarios, puesto que son un factor importante que interactúa de forma directa con dichos dispositivos, adicionalmente es un análisis que busca garantizar los pilares fundamentales de la seguridad informática, es por esto por lo que se vislumbra la necesidad de evaluar el tipo de información que se almacena y procesa en un Smartphone Android.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

Presentación del problema de investigación

Las vulnerabilidades de seguridad en los dispositivos móviles, con el paso del tiempo llegan aumentar cada vez más gracias a las actualizaciones, modificaciones entre otras mejoras que ayudan a un correcto funcionamiento de los mismos, pero de igual manera aumenta el desconocimiento de seguridad en los usuarios que usan estos dispositivos, por ende, el problema en qué radica esta investigación, es el de poder brindar información clara y precisa sobre el uso las vulnerabilidades que se presentan a la hora de usar un Smartphone, ya sean ejecutando actividades cotidianas como; navegar por internet, usar redes sociales, descargar apps entre otras.

Pregunta problema

Teniendo en cuenta lo anterior, y a través del desarrollo de un estudio de carácter investigativo ¿Qué vulnerabilidades comprometen la seguridad de la información en los dispositivos móviles Android?

Justificación

Teniendo en cuenta el desconocimiento en términos de seguridad que poseen los usuarios en dichos dispositivos; este entorno ha sido remotamente explorado pues hasta el momento se han demostrado muy pocos estándares en pro de mejorar en el aspecto de protección de la información, cabe aclarar que estos son realizados por grandes compañías norteamericanas y europeas, sin tener en cuenta en el mercado latinoamericano y particularmente en Colombia, de allí la necesidad de elaborar un estudio de carácter investigativo para el estado colombiano que permita :

1. Evidenciar las vulnerabilidades (en cuanto a seguridad de la información se refiere), que se presentan en los Smartphone (si es posible conocer las lasitudes y de ser posible disminuirlas).

2. Determinar el impacto que propician las vulnerabilidades encontradas frente a la información que estos dispositivos son capaces de almacenar. Ya que actualmente es más frecuente el uso del sistema operativo, se hace indispensable la identificación de factores en seguridad informática que se pueden ver expuesto si no se efectúan las configuraciones de seguridad necesarias.

3. Elaborar una página web que integre mejores prácticas de manejo para un uso seguro del dispositivo Smartphone. Dicho documento es una contribución a los usuarios del sistema operativo Android, en el cual se halla información detallada para contribuir a la seguridad de los dispositivos.

Objetivo general

Realizar un análisis de vulnerabilidades a nivel del sistema operativo Android en los dispositivos móviles que permita la creación de una página web que contenga las mejores prácticas y recomendaciones para proteger la información dentro de este tipo de dispositivos.

Objetivos específicos

Analizar la documentación existente de las vulnerabilidades de dispositivos móviles Android

Determinar las prácticas y recomendaciones para la protección de dispositivos móviles Android.

Sintetizar por medio de una página web las vulnerabilidades y recomendaciones para la protección de los dispositivos móviles.

CAPÍTULO II: MARCO TEÓRICO

Análisis de Vulnerabilidades en dispositivos móviles con sistema operativo Android.

Teniendo en cuenta que las vulnerabilidades en seguridad en dispositivos móviles es cada vez más inminente, por la razón de que cada vez es más fácil acceder a un dispositivo móvil y las diversas actualizaciones y herramientas que ofrece el sistema, pero esto en cierta medida llega a ser contraproducente, ya que la accesibilidad que tiene los usuarios al acceder a estos dispositivos resulta más sencillo para los piratas informáticos el poder vulnerar la información de los usuarios que usan dichos dispositivos, a continuación se presentan los antecedentes respecto a seguridad de la información refiere, teniendo en cuenta libros, artículos y demás material de información.

Antecedentes de la investigación

Se muestra un estudio en el sistema operativo Android en cuanto a vulnerabilidades de seguridad demuestra que durante el transcurso de los años la cantidad de vulnerabilidades va en crecimiento,

Se nota una gran diferencia entre el año 2016 y 2020, en 2016 se registraron 500 en comparación con el año 2020 en el que se registraron 859, qué es el número más alto de casos registrados desde el 2009.

"Datos de la página oficiaCVEDetails.com"

Se muestran estudios como el de Seguridad y Protección del Ecosistema Móvil., por parte de la Asociación GSM que es una organización mundial que conecta el ambiente móvil para encontrar, desarrollar y brindar innovaciones que son fundamentales para el entorno empresarial y el cambio social, en él se aprecian las principales problemáticas de protección al consumidor, la privacidad, seguridad pública y la seguridad en la

infraestructura, de la misma manera propone un variedad de potenciales problemas y las correctivas y acciones necesarias para resolverlos. Por otra parte, se hace un llamado de atención a los representantes de las políticas de seguridad para ampliar la visión sobre las cuestiones presentadas, y así contribuir en el progreso de soluciones.

GSMA. "Seguridad, Privacidad y Protección del Ecosistema Móvil". 2017

Una retroalimentación minuciosa en perspectiva de seguridad en dispositivos móviles del año 2018 comprende datos de vulnerabilidades, amenazas y los países en donde se registró la mayor suma de detecciones.

Podría decirse que Android es el sistema operativo móvil más usado en el mundo. Actualmente posee el 88% del mercado. En 2018 se revelaron 517 vulnerabilidades en Android, una disminución del 39% en comparación con el número total de vulnerabilidades reportadas en la plataforma en 2017, año en el que la cantidad de CVE marcó un alza histórica alcanzando los 842 fallos revelados.

D, Giusto Bilić. "Seguridad en Dispositivos Móviles: Resumen de lo que fue el 2018". Welivesecurity.com by ESET. 2018.

Bases teóricas o fundamentos conceptuales

El artículo “Vulnerabilidades más importantes en plataformas Android (2016)” tenemos la postura de Leaño Ardila Víctor Hugo, donde nos muestra las vulnerabilidades más importantes en las plataformas Android, la estructura del modelo de seguridad de Android y las vulnerabilidades más importantes para plataforma Android en el año 2016.

El artículo concluye lo siguiente:

“El crecimiento de usuarios de dispositivos móviles ha demostrado estar explotando, además, la plataforma de código abierto Android más asequible del mundo, convirtiendo así en un objetivo favorito de los piratas informáticos para perfeccionar sus estrategias de robo. El aumento de exploits y vulnerabilidades documentadas entre 2015 y 2016 representa un aumento del 9,9 %, lo que es alarmante para los fabricantes que buscan mejorar sus arquitecturas de seguridad y proporcionar productos confiables a sus clientes.”

El artículo experimental “Evaluación de vulnerabilidades de seguridad en Software Android en el año 2021” de Ing. Luis Torres Chavarría se brinda una propuesta con el fin de implementar controles en cuanto a las buenas prácticas en el uso de dispositivos móviles, para ello la propuesta se divide en 3 fases y se llega a la conclusión de lo siguiente:

“Bajo el Objetivo Específico 1, analizar las vulnerabilidades de los teléfonos móviles Android utilizando parámetros medibles y determinar el control de la norma ISO 27001:2013 en Costa Rica. La conclusión es que: de las 6 subcategorías identificadas de NIST SP 800-163 están relacionadas entre sí y 19 de las 11 subcategorías de ISO/IEC 27001 están relacionadas con el tema de las vulnerabilidades identificadas durante las pruebas con un teléfono móvil Android. Sistema operativo versión 6.0.1 Marshmallow, los resultados

fueron positivos ya que se comprobó que de la misma forma se pueden implementar los objetivos de control de la norma ISO 27001:2013. Sistema operativo que reduce el riesgo de pérdida de datos."

"Bajo el Objetivo Específico 2 Evaluar el crecimiento de la inseguridad informática en Costa Rica utilizando los controles establecidos en la norma ISO 27001:2013 examinando la vulnerabilidad de los teléfonos móviles Android en el 2021. Se concluyó que: El análisis se realizó sobre 1 elemento de control. El artículo 6 de la norma ISO 27001:2013 está directamente relacionado con los problemas de seguridad de los dispositivos móviles identificados en el estudio, fomentando su mitigación mediante la implementación de controles adecuados para abordarlos de forma global."

"Bajo el objetivo específico 3, elaborar una propuesta metodológica sobre vulnerabilidades en teléfonos móviles Android siguiendo los lineamientos de la norma ISO 27001:2013, que facilitará la comprensión de los riesgos de la telefonía móvil en Costa Rica en el 2021. Se concluyó que: La Guía A.9.3 de la La norma de responsabilidad de los usuarios ISO 27001:2013 Anexo a punto .9.3, formada por los usuarios del apartado A.9.3.1 sobre responsabilidad en la gestión de la información, es consistente con la causa principal de los problemas de seguridad de la información, el usuario es el eslabón más débil de la cadena de seguridad de la información. 1 anexo a la norma ISO 27001:2013, 7 de los cuales están adaptados a los resultados del estudio."

"Independientemente de la cantidad de controladores establecidos en el estándar que deben estar presentes, el usuario del teléfono móvil debe tener buenas prácticas, de lo contrario, esta es siempre la vulnerabilidad más atacable, porque los teléfonos inteligentes con sistema operativo Android pueden verse afectados física o remotamente. Daños con o sin internet solo por negligencia del usuario. Es recomendable abordar de manera más amplia la programación de aplicaciones móviles y sistemas operativos, donde a través de pruebas guiadas por metodologías de desarrollo seguras, comenzamos a ver resultados de aplicaciones o software

móviles más antiguos y confiables. Siempre se recomienda a los usuarios finales que analicen con más detalle qué tipo de información comparten en sus dispositivos móviles y redes sociales, donde fácilmente pueden ponerlos en riesgo por descuido o divulgación de información sensible."

Bases legales de la investigación

La Organización Internacional de Normalización o International Organization for Standardization (ISO), establece en la norma 27000 publicada en Octubre de 2005, comprobada en Septiembre de 2013 y finalmente promulgada en Diciembre de 2013.

Esta norma comprende las condiciones del sistema de gestión de seguridad de la información. Tiene su inicio en la BS (British Standard) 7799-2:2002 y es la normativa a avalar por auditores externos del SGSI de las organizaciones. Abarca el anexo A, en el que recopila los 14 objetivos de control y 114 controles que despliega la ISO IEC 27002:2005, la cual ofrece guías de implementación de SGSI con un nivel de especificación para ser escogidos y ser utilizados por las organizaciones en todas las fases del SGSI.

ISO 27001: Comprende las condiciones del sistema de gestión de seguridad de la información.

ISO 27002: Es el manual de buenas prácticas que detalla los objetivos de control y controles aconsejables en cuanto a seguridad de la información.

ISO 27003: Manual de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases

ISO 27005: Brinda las directrices para la mitigación del riesgo en la seguridad de la información.

ISO 27006: Determina los requisitos para la acreditación de entes auditores y la legalización de sistemas de gestión de la seguridad de la información.

ISO 27007: Es un manual de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

ISO 27008: Manual de auditoría de los controles seleccionados en el marco de implantación de un SGSI

ISO 27009: Es un manual acerca del uso y aplicación de los principios de ISO/IEC 27001 para el sector servicios específicos en emisión de certificaciones acreditadas de tercera parte.

ISO 27010: Manual para la gestión de la seguridad de la información cuando se comparte entre organizaciones.

ISO 27011: Manual de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del grupo de telecomunicaciones basada en ISO/IEC 27002:2005.

ISO 27013 : Manual de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

ISO 27014: Manual de gobierno corporativo de la seguridad de la información.

ISO 27017: Manual de seguridad para Cloud Computing

ISO 27018: Buena práctica para el control de la protección de datos de los servicios en la nube.

ISO 27032: Proporciona orientación para mejorar el estado de la ciberseguridad.

ISO 27033: Estándar dedicado a la seguridad de la red, que consta de 7 partes: gestión de la seguridad de la red, arquitectura de la seguridad de la red, escenarios de red de referencia, comunicación segura entre redes a través de puertas de enlace, acceso remoto, comunicación segura dentro de las redes a través de VPN y diseño e implementación de redes de seguridad.

ISO 27034: Un estándar dedicado a la seguridad de las aplicaciones informáticas, que consta de seis partes: conceptos generales, marco regulatorio organizacional, proceso de gestión de la seguridad de la aplicación, validación de la seguridad de la aplicación, estructura de datos y protocolos y controles de seguridad de la aplicación, guía de seguridad de la información para aplicaciones específicas en usar.

ISO 27035: Guía de gestión de incidentes de seguridad de la información.

ISO 27036: Guía para la seguridad de las relaciones con los proveedores, consta de cuatro partes: descripción general y conceptos, requisitos comunes, seguridad de la información en la cadena de suministro de las TIC, seguridad en entornos de servicios en la nube.

ISO 27037: Guía para la Identificación, Recolección, Adquisición y Preservación de Evidencia Digital.

ISO 27040: Guía de seguridad para medios de almacenamiento.

Las normas mencionadas anteriormente constituyen en gran medida a la base del proyecto investigativo, ya que aportan información importante en todo lo que seguridad de la información refieren, dichas normas muestran modelos a seguir para resguardar el activo más importante, la información, tanto en grandes organizaciones, como en los dispositivos de uso diario como los teléfonos móviles, que sería el eje central por el que se rige esta investigación.

Tomado de:https://www.eafit.edu.co/escuelas/administracion/publicaciones/panorama-contable/actualidad/Documents/Boletin-1-NORMAS-ISO-Y-SU-COBERTURA.pdf

CAPÍTULO III: DISEÑO METODOLÓGICO

Teniendo en cuenta que el objetivo del presente documento es analizar las vulnerabilidades y las buenas prácticas de seguridad en dispositivos con sistema operativo Android, se optó por el diseño de un marco de tipo investigativo recurriendo a la bibliografía y documentación disponible, además de las normas actualmente instituidas acerca de la seguridad de los dispositivos móviles.

Tipo de investigación

El tipo de investigación abordado es de carácter bibliográfico ya que se buscó toda la información relacionada con el tema de investigación: artículos, tesis, libros entre otros para este caso el "Análisis de las vulnerabilidades en dispositivos móviles con sistema operativo Android"

Identificar:

- Propósito: Investigación aplicada.
- Lugar: Investigación documental.
- Alcance: Investigación argumentativa.

Definir:

- **Investigación aplicada:** De acuerdo con Murillo (2008), la investigación aplicada se denomina "investigación practica o empírica" caracterizada por la búsqueda o aprovechamiento de los conocimientos obtenidos, mientras que otras se obtienen luego de investigaciones basadas en la aplicación práctica y la sistematización. El uso del conocimiento y la investigación que lleva a una forma organizada y sistemática de conocer la realidad.

  Tomado de: "LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTÍFICA" de Zoila Rosa Vargas Cordero 2009

  https://www.redalyc.org/pdf/440/44015082010.pdf

- **Investigación documental:** De acuerdo con Alfonso (1995), la investigación documental es un desarrollo científico, una sucesión sistemática de investigación, compilación, ordenamiento, estudio e interpretación de información o datos sobre un tema puntual. Como otras investigaciones, aportan a la creación de conocimiento.

  *Tomado de: "*FUNDAMENTOS DE LA INVESTIGACIÓN DOCUMENTAL Y LA MONOGRAFÍA*" de* Lic. Oscar Alberto Morales http://www.webdelprofesor.ula.ve/odontologia/oscarula/publicaciones/articulo18.pdf

- **Investigación argumentativa:** Este tipo de investigación se basa en fuentes documentales, es decir, todo tipo de documentos. Como subtipos de este tipo de investigación se encuentran la investigación bibliográfica, hemerografica y de archivo; la primera se basa en libros de consulta, la segunda en artículos o ensayos de revistas y periódicos, y la tercera en documentos encontrados en archivos, que pueden ser cartas, oficios, circulares, expedientes, entre otros.

Población

La presente investigación va dirigida a todas las personas con capacidad económica, que pueden obtener un Smartphone o dispositivo móvil, es decir personas que van en el rango de edad de los 18 a 55 años, siendo estas las personas que más hacen uso de estos dispositivos, de manera personal o laboral, además no solo se hace uso de un solo dispositivo en algunos casos se usan varios dispositivos y se vuelven de alguna manera indispensables.

Técnicas e instrumentos de recolección de datos

Dando respuesta a la pregunta problema planteado anteriormente se hace el uso de dos técnicas de recolección de datos que son fuentes abiertas y análisis de sitio web, integrando de manera clara y concisa las mencionadas anteriormente para así resolver la pregunta problema.

De acuerdo con lo anterior se presenta la versión del instrumento final usando los métodos de fuentes abiertas y análisis web, se expone lo siguiente:

Según el artículo "Unificación optima de características estáticas y dinámicas para el análisis de seguridad de teléfonos inteligentes" Autores Kumar,S Indu,S, Walia G.S. Volumen 35, Numero 1, 2023, Paginas 1035-1051.

"Los teléfonos móviles con sistema operativo Android se están volviendo muy populares en el mundo digital por sus aplicaciones estandarizadas en muchos campos. El aumento de la popularidad de la plataforma Android capta la atención de los desarrolladores de malware a diseñar aplicaciones maliciosas para alcanzar sus objetivos maliciosos. Así mismo, los métodos de análisis estáticos no detectan el comportamiento en tiempo de ejecución de las aplicaciones maliciosas. Para resolver estos inconvenientes, se plantea una combinación óptima de características estáticas y dinámicas para el análisis de seguridad de teléfonos inteligentes. La resolución propuesta usa características estáticas y dinámicas para generar un vector de características uniforme altamente diferenciable mediante una estrategia de difusión cruzada basada en gráficos. Además, el modelo de clasificación fundamentado en fusibles de la característica unificada distingue entre aplicaciones benignas y maliciosas. El marco de referencia propuesto se valida empíricamente mediante análisis cualitativos y cuantitativos, y los resultados se comparan con las soluciones existentes. La evaluación del rendimiento en los conjuntos de datos de referencia de Google play store, Debrin, Androzoo, AMD y CICMalDroid2020 mostro que la solución brindada funciona mejor que los métodos de última

generación. Se logró una precisión de reconocimiento promedio del 98.62% y una puntuación de F1 de 0,9916 2023, Prensa de ciencia de tecnología. Todos los derechos reservados."

Según el artículo "Impacto del análisis basado en híbridos en la detección de rasomware para sistemas Android" Autores Almohaini, R., Almomani, yo., Alkhayer, Volumen 11, Numero22, Noviembre de 2021, Numero de Articulo 10976. A. Laboratorio de Ingeniería de Seguridad, Departamento de Informática, Universidad Prince Sultan, Riad, 11586, Arabia Saudita.
Departamento de Informática, Escuela de Tecnología de la Información King Abdullah II, UIniversidad de Jordania, Amman, 11942, Jordania.

"El ransomware de Android es uno de los ataques más peligroso que va en aumento a un ritmo alarmante. Los ataques de ransomware generalmente se dirigen a los usuarios de Android bloqueando sus dispositivos o cifrando sus archivos de datos y luego pidiéndoles que paguen dinero para desbloquear sus dispositivos o recuperar sus archivos. Las soluciones presentes de detección de ransomware usan principalmente análisis dinámicos puntualmente para la detección de ransomware. Además, estos enfoques no funcionan correcta o frecuentemente fallan con técnicas de obcecación de código o aplicaciones benignas que usan métodos criptográficos para acceder a la API. Así mismo, la mayoría de ellos no detectan los ataques de ransomware de manera temprana. Por tanto, este documento plantea un sistema de rastreo hibrido que utiliza de manera efectiva el análisis estático y dinámico para detectar ransomware con alta exactitud. Para el análisis estático, el sistema hibrido planteado considero más de 70 motores antivirus de reciente generación. Para el análisis dinámico, este estudio investigo las herramientas dinámicas existentes y efectuó un estudio comparativo integral para hallar la herramienta idónea que se integre con la detección de ransomware cuando sea conveniente. Así evaluar el rendimiento del sistema mixto propuesto, analizar estética y dinámicamente más de cien muestras de ransomware. Los resultados de las pruebas mostraron que el análisis estático logro casi la

mitad de la precisión de detección (alrededor del 0-55%) en comparación con el análisis dinámico, que tuvo una precisión de 100. Por otra parte, en este estudio se describen algunas clases y métodos avanzados, y a las API utilizadas por estas aplicaciones de ransomware. Por último, se destacan algunos estudios de casos, incluidas aplicaciones fallidas y modelos de ransomware criptográfico.

2021. Licenciado MDPI, Basilea, Suiza."

Además de lo expuesto anteriormente tenemos los resultados de investigación indagados en la base de datos Scopus, una herramienta bibliográfica que contiene resúmenes y artículos de revistas científicas.

A continuación, se muestran los resultados de investigación:

Figura 1

Representación resultado de investigación Scopus imagen 1.

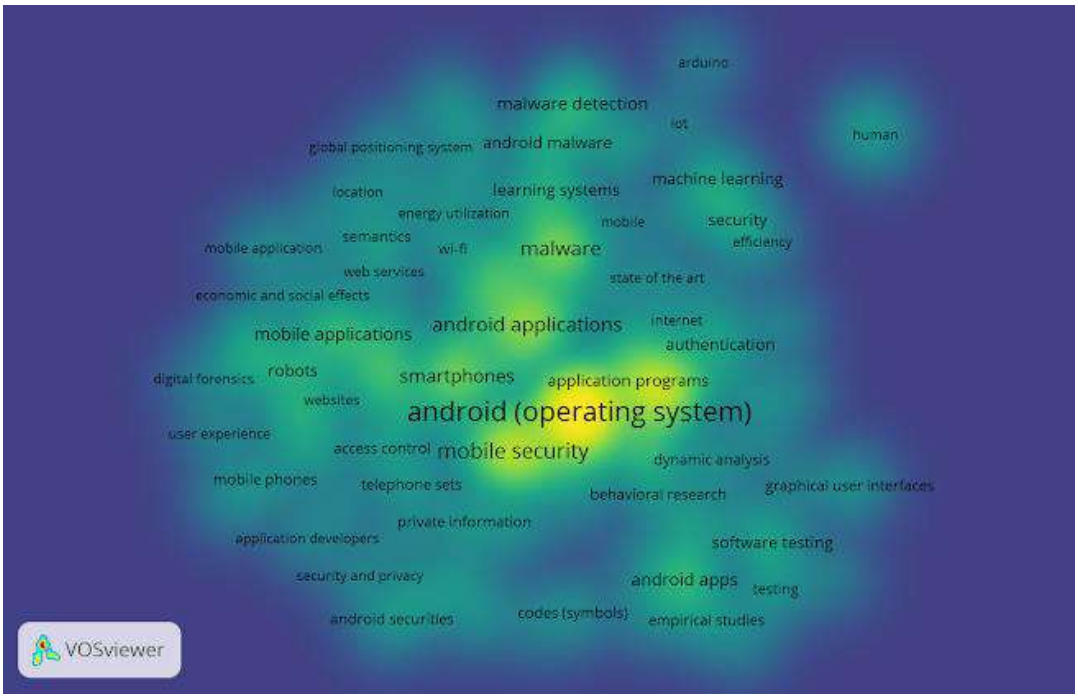


Figura 2

Representación resultado de investigación Scopus imagen 2

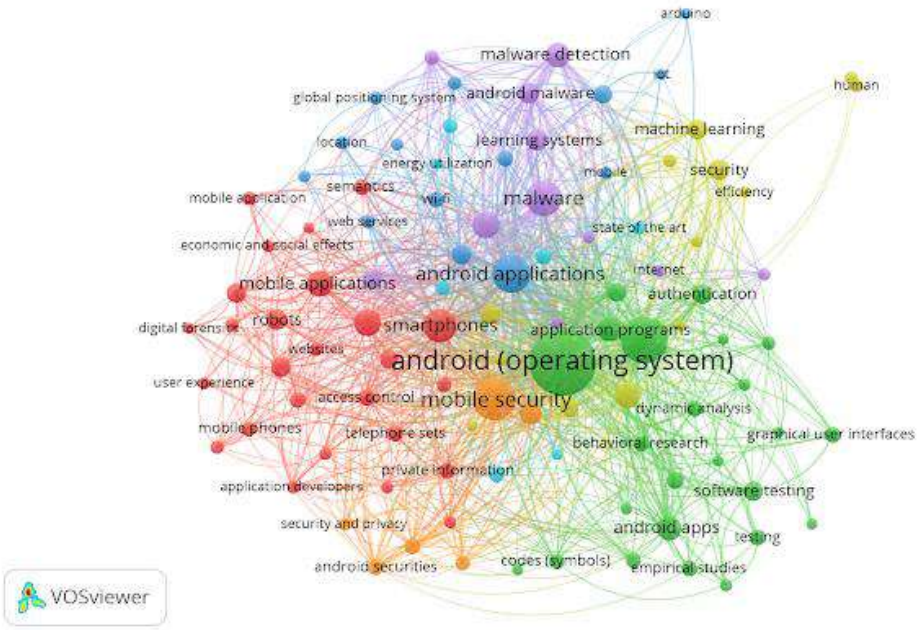
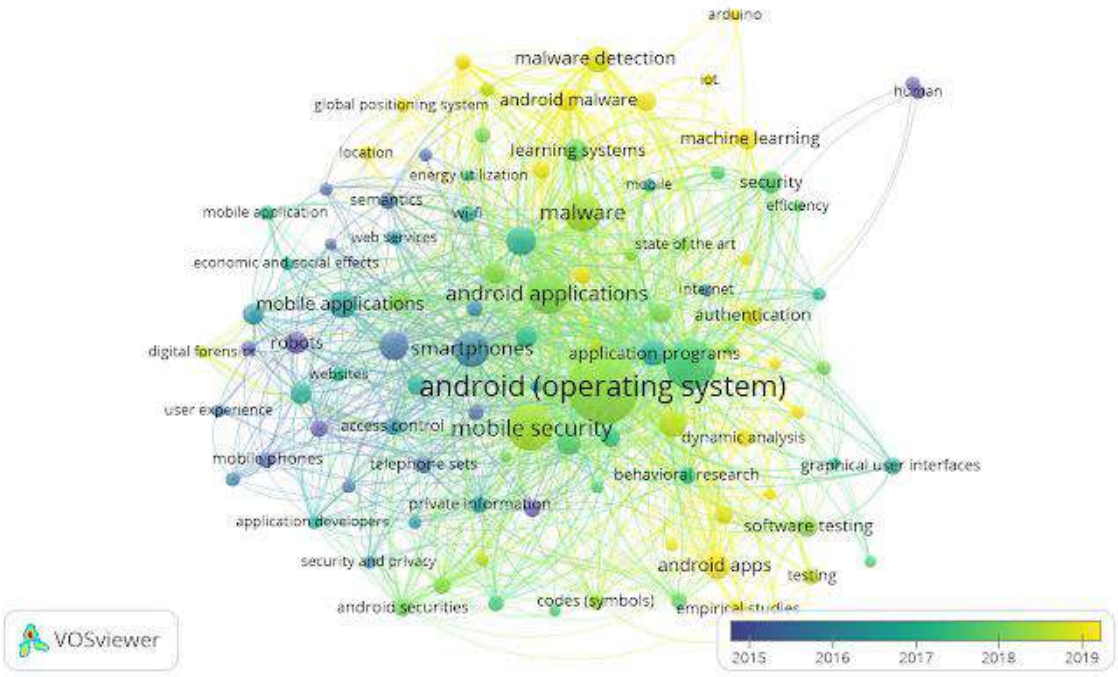


Figura 3

Representación resultado de investigación Scopus imagen 3



Resultados búsqueda Scopus

Anexo 1

CAPÍTULO III: RESULTADOS DE LA INVESTIGACIÓN

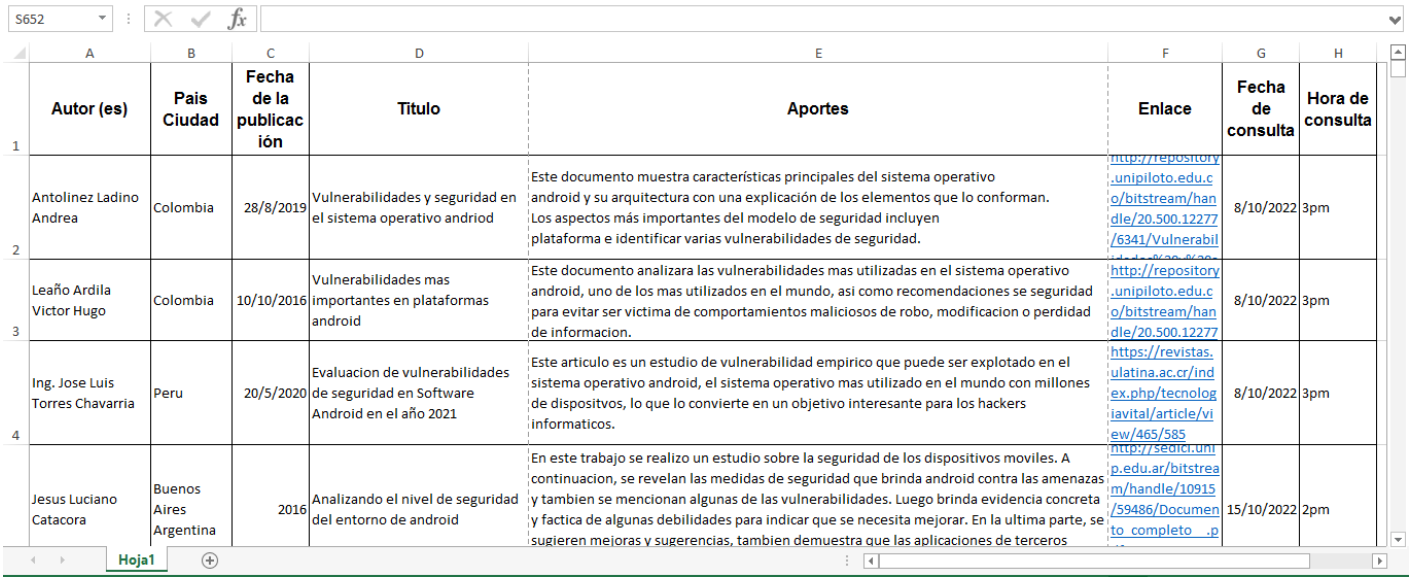
Actividades del objetivo específico no. 1

Para llevar a cabo los resultados del primer objetivo, se optó por crear tres actividades distintas las cuales son:

Primero, se realizó un levantamiento de información, soportados en citas bibliográficas, artículos libros, revistas, entre otros.

Figura 4

Actividad uno del objetivo uno.



	Autor (es)	Pais Ciudad	Fecha de la publicación	Titulo	Aportes	Enlace	Fecha de consulta	Hora de consulta
2	Antolinez Ladino Andrea	Colombia	28/8/2019	Vulnerabilidades y seguridad en el sistema operativo andriod	Este documento muestra características principales del sistema operativo android y su arquitectura con una explicación de los elementos que lo conforman. Los aspectos más importantes del modelo de seguridad incluyen plataforma e identificar varias vulnerabilidades de seguridad.	http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6341/Vulnerabil	8/10/2022	3pm
3	Leaño Ardila Victor Hugo	Colombia	10/10/2016	Vulnerabilidades mas importantes en plataformas android	Este documento analizara las vulnerabilidades mas utilizadas en el sistema operativo android, uno de los mas utilizados en el mundo, asi como recomendaciones se seguridad para evitar ser victima de comportamientos maliciosos de robo, modificacion o perdidad de informacion.	http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277	8/10/2022	3pm
4	Ing. Jose Luis Torres Chavarria	Peru	20/5/2020	Evaluacion de vulnerabilidades de seguridad en Software Android en el año 2021	Este articulo es un estudio de vulnerabilidad empirico que puede ser explotado en el sistema operativo android, el sistema operativo mas utilizado en el mundo con millones de dispositvos, lo que lo convierte en un objetivo interesante para los hackers informaticos.	https://revistas.ulatina.ac.cr/index.php/tecnologiavital/article/view/465/585	8/10/2022	3pm
	Jesus Luciano Catacora	Buenos Aires Argentina	2016	Analizando el nivel de seguridad del entorno de android	En este trabajo se realizo un estudio sobre la seguridad de los dispositivos moviles. A continuacion, se revelan las medidas de seguridad que brinda android contra las amenazas y tambien se mencionan algunas de las vulnerabilidades. Luego brinda evidencia concreta y factica de algunas debilidades para indicar que se necesita mejorar. En la ultima parte, se sugieren mejoras y sugerencias, tambien demuestra que las aplicaciones de terceros	http://sedici.unlp.edu.ar/bitstream/handle/10915/59486/Documento_completo_.p	15/10/2022	2pm

Anexo 2

Segundo, se llegó a un análisis de la información obtenida y así verificar las vulnerabilidades más comunes en los dispositivos móviles con sistema operativo Android.

Análisis de la Información Recolectada

De acuerdo con la información obtenida de diferentes fuentes bibliográficas, se logró obtener información suficiente para dar respuesta a las siguientes preguntas que son las bases de la presente investigación.

Tabla 1

Cuadro de preguntas actividad dos del objetivo uno.

Pregunta
1. ¿Cómo se estructura el esquema de seguridad de Android?
2. ¿Cuáles fueron las vulnerabilidades más importantes en 2016 para plataformas Android?
3. ¿Cuáles son las amenazas de seguridad más comunes en dispositivos móviles Android?
4. ¿Cuáles son las vulnerabilidades de seguridad más comunes en dispositivos móviles Android?
5. ¿Cuáles son las medidas de seguridad o buenas prácticas para mejorar la seguridad en los dispositivos móviles Android?

Nota: Esta tabla muestra las preguntas que se logran resolver con la presente investigación.

Análisis

Respuesta Pregunta 1

En respuesta a la primera pregunta, de acuerdo con lo investigado por la autora Antolinez Ladino Andrea en su artículo Vulnerabilidades y Seguridad en el Sistema Operativo Android indica los siguientes aspectos más importantes del modelo de seguridad de Android.

Application Sandbox

Android implementa la base de privilegio mínimo al ejecutar cada aplicación en lo que se denomina un espacio retirado. Dicho de otra forma, obligar a cada aplicación a tener acceso sin restricciones a sus correspondientes recursos.

El dispositivo de sandboxing de la aplicación se implementa a nivel de kernel y asigna a cada aplicación con pocos privilegios un UID de ID de usuario único. Lo que quiere decir que cualquier aplicación puede leer y modificar los archivos creados en el almacenamiento externo, como las tarjetas SD, con la única restricción de que tengan los permisos adecuados para escribir en el almacenamiento externo de ser necesario.

Cada aplicación de ejecuta opcionalmente como un proceso aparte del resto, con su concerniente espacio de direcciones.

Application Signing

Las aplicaciones Android deben incluir un certificado que indique al emisor de su clave pública. Android usa certificados para diferenciar entre dos aplicaciones distintas creadas por un mismo desarrollador.

Dicha información es pertinente para el sistema cuando decide otorgar el mismo permiso que la firma o permitir dos aplicaciones con el mismo UID. Varias aplicaciones firmadas con igual certificado pueden ratificar tener el mismo UID y, por consiguiente, dividir recursos entre ellas o ejecutarse en el mismo proceso.

Permisos

En cuanto a permisos se necesita un mecanismo mediante el cual la aplicación pueda dar acceso a los medios que necesita para lograr sus objetivos, y de igual manera tener cierta vigilancia sobre quien accede a ellos. La solución que brinda Android es que el sistema de permisos una parte primordial de su modelo de seguridad, es decir que la autorización requerida se otorgue o no durante la instalación de la aplicación dependiendo del tipo de autorización, del certificado, o en la mayoría de los casos, del consentimiento del usuario.

El sistema otorga automáticamente algunos permisos a pedido sin solicitar su permiso explícito.

Dependiendo del nivel de protección de una autorización en particular, el sistema determina el proceso a seguir para determinar si dicha autorización ha sido otorgada a la aplicación solicitante.

Delegación de Permisos

El Pendinglntenet está asociado con una acción deseada. Dicho objeto es solo no es más que una alusión de que pude ser referida a otra aplicación, para que esta se invoque en el momento que disponga, esta acción en específico, contando, al hacerlo con los consentimientos y autenticidad de la aplicación inicial.

Por otra parte, si una aplicación establece un objeto Pendinglntenet, a pesar de que deje de ejecutarse, las demás aplicaciones que lo recibieron podrán seguir utilizándolo.

Pero solo el mismo podrá ser anulado por la aplicación que lo generó y, de ser así todas las aplicaciones que estén usando este objeto deben de dejar se hacerlo.

Android Manifest

Todas las aplicaciones de Android deben incorporar en su directorio raíz un archivo XML nombrado AndroidManifest. Igualmente, se determina los permisos que requerirán la aplicación al momento de instalarse y los que serán exigidos por la misma.

Uno de los componentes más importantes del cuerpo de AndroidManifest, es donde, también de especificar algunas características de la aplicación mencionada, se incorporan los elementos que detallan los componentes de esta.

Análisis

Respuesta Pregunta 2

De acuerdo con el artículo Vulnerabilidades más importantes en las plataformas Android del autor Leaño Ardila Víctor Hugo, se puede concluir mediante una gráfica lo siguiente en materia de Vulnerabilidades presentadas en los últimos años.

Se puede concluir que la vulnerabilidad más relevante en los dispositivos con sistema operativo Android es la llamada “Gain Privileges” que consiste en explotar una configuración en el sistema operativo, que concede a los atacantes más privilegios administrativos con ello pueden hurtar datos secretos, ingresar software malicioso, estropear el sistema operativo o ensuciar la reputación de una compañía; con 236 casos.

La segunda vulnerabilidad más alta es DoS con 104 casos, esta vulnerabilidad se encontraba en el módulo mod_ssl de Apache (servidor web HTTP) lo cual permitía a un atacante remoto no autenticado provoque una denegación de servicio (DoS) en un sistema en particular.

Por otra parte, se evidencia que la vulnerabilidad más baja es la llamada “Memory Corruption”, con 38 casos respecto a la gráfica, esta trata en la que la memoria se altera sin ninguna asignación concreta, esto quiere decir que se transforma una parte especifica de la memoria esto a causa de errores de programación, que facilitan a los piratas informáticos ejecutar código malicioso.

De igual manera se evidencia que en las vulnerabilidades: SQL Injection, Xss, Directory Traversal, Http Response Splitting, Csrf y File Inclusion, no se reportaron casos.

Análisis

Respuesta Pregunta 3

Según con lo indagado en el artículo Analizando el nivel de seguridad del entorno Android del autor Jesús Luciano Catacora, se logra establecer las amenazas más comunes a las que están expuestos los usuarios de los dispositivos móviles con sistema operativo Android, analizando dicha información se logra demostrar de manera gráfica las amenazas que se encuentran en un rango más alto y las de menor rango.
De acuerdo con lo anterior se llega a concluir, que respecto a lo investiga en el artículo anteriormente mencionado se logra analizar lo siguiente:

Spoofing es la amenaza más común con un 28% respecto a la gráfica.

Malware se encuentra en segundo lugar con un 26%.

Ingeniería Social en tercer lugar con 21 %.

Phishing en cuarto lugar con un 17%.

Rooting y Jailbreaking en último con el 8% restante.

Estos porcentajes son un análisis a nivel del artículo de referencia, no representa datos verídicos, es tan solo un criterio personal.

Spoofing

Una definición a nivel general, un agresor origina un entorno que simula ser el real para engañar a una víctima. Dentro de este entorno, el afectado elige realizar una acción nociva sin darse cuenta lo que verdaderamente está haciendo. Pero las actividades que simulan ser razonables dentro del entorno falso pueden tener repercusiones judiciales para el afectado en el ámbito real. Habitualmente se adapta esta técnica

en el envío de e-mails, que constan en la creación de mensajes de correo electrónico con una dirección de remitente falso.

En el marco de las redes de computadoras, la amenaza del spoofing consiste esencialmente en que un individuo, de un host de una red, manipula la tecnología de red para abrirse paso a otro host de la misma red. Esta técnica no se usa con fines constructivos o legales, se usa para el hurto de información, una venganza u otro objetivo malicioso.

Malware

El malware es una de las amenazas de seguridad móvil más letales. El malware móvil es cualquier virus u otro software malicioso que tiene como fines especialmente dispositivos móviles para dañarlos.

Lo más común son troyanos, virus, spyware entre otros. Se puede usar malware móvil para el hurto de datos personales, monitorear la actividad de un usuario, enviar SMS que generan costos para los usuarios, implementar actividades destructivas, envío de mensajes de Spam por medio de mensajes de texto o correos electrónicos.

El spyware es un software espía en el interior del dispositivo; que recopila información del historial del navegador web, por ejemplo, SMS, correo electrónico, nombre de usuario y contraseña, detalles de facturas y tarjetas de crédito. Los caballos de troya o troyanos se disfrazan de aplicaciones que simulan ser legitimas e inofensivas, pero si se ejecutan brindan acceso remoto al equipo infectado. Por otra parte, el malware, presenta publicidad al usuario durante la instalación o uso para originar ganancias económicas a sus creadores.

Ingeniería Social

La ingeniería social es un ataque muy conocido en el entorno Pc, no usa aspectos técnicos para atacar el sistema, sino que se dirige al usuario y su capacidad de toma de decisiones.

Esto se lleva a cabo falsificando la información para que el usuario pueda asumir que el atacante es una persona confiable y aprueba que puede obtener información confidencial, como tipo administrador.

Este se diferencia del entorno Pc, que habitualmente se hace uso de antivirus o antimalware para escanear el contenido de un e-mail.

Phishing

Los delincuentes llegan a los usuarios a atreves del phishing, que les permite acceder a los sistemas creyendo en un mensaje falso. El phishing puede eludir sutilmente muchas de las medidas de seguridad de una organización. En un entorno móvil, un agresor a menudo usa mensajes de texto para entregar enlaces web que apuntan a aplicaciones descargables o páginas web de phishing que requieren identificación personal. Existen varias versiones de phishing para teléfonos inteligentes o teléfonos móviles normales, como el phishing a través de llamadas de voz y mensajes SMS.

En cuanto a las consecuencias del phishing, se puede argumentar que se puede engañar a los usuarios para que realicen pagos fraudulentos en su cuenta de teléfono móvil, por ejemplo, cuando un usuario recibe un mensaje de texto inconveniente que promete beneficios económicos a cambio de una suscripción de SMS, aun servicio específico.

Rooting y Jailbreaking

Ambas tecnologías ayudan a eliminar las restricciones de seguridad impuestas por el fabricante del teléfono inteligente para brindarle al usuario un control sobre el dispositivo. Esta tecnología brinda al usuario acceso a muchas características interesantes que de otro modo no estarían disponibles.

Por ejemplo, en versiones anteriores de iOS, no podía instalar un teclado de terceros, solo podía usar el teclado que venía con el dispositivo de forma predeterminada, a menos que tuviera jailbreak. pero esta característica cambió en Android con la introducción de iOS 8, las implementaciones de teléfonos inteligentes a menudo aprovechan las vulnerabilidades conocidas del sistema operativo para deshabilitar las funciones de seguridad que evitan que los usuarios y los programas realicen acciones peligrosas, como ejecutar comandos privilegiados, interactuar con el hardware a bajo nivel, modificando y eliminando los

archivos necesarios del sistema, por defecto el sistema operativo desinstala las aplicaciones incluidas. Por ejemplo, si tiene un dispositivo Android "rooteado", puede otorgar derechos de administrador a cualquier aplicación, rompiendo el modelo de espacio aislado. Este comportamiento permite que cualquier aplicación desinstale otras aplicaciones y, por lo tanto, revoque maliciosamente sus derechos de acceso.

Análisis

Respuesta Pregunta 4

Según con lo indagado en el artículo Analizando el nivel de seguridad del entorno Android del autor Jesús Luciano Catacora, se logra establecer las vulnerabilidades más comunes a las que están expuestos los usuarios de los dispositivos móviles con sistema operativo Android, analizando dicha información se logra demostrar de manera gráfica las vulnerabilidades que se encuentran en un rango más alto y las de menor rango.

Se llega a la conclusión, que respecto a lo investiga en el artículo anteriormente mencionado se logra analizar lo siguiente:

Uso de contenido no confiable es la vulnerabilidad más común con un 28% respecto a la gráfica.

Uso de redes desconocidas se encuentra en segundo lugar con un 24%.

Aplicaciones de origen desconocido en tercer lugar con 21 %.

Falta de controles físicos en cuarto lugar con un 17%.

Uso de servicios de ubicación en ultimo con el 10% restante.

Estos porcentajes son un análisis a nivel del artículo de referencia, no representa datos verídicos, es tan solo un criterio personal.

Uso de contenido no confiable

Los Smartphone pueden utilizar contenido no confiable y anónimo que se oculta o trata de defraudar al usuario con ciertas técnicas.

Unos de los ejemplos más claros son los códigos QR pueden dañar indirectamente el sistema porque los usuarios no saben exactamente qué contiene hasta que lo escanean y luego ingresan a un sitio web o ven la información que muestra el código en la pantalla. Una vez leído y convertido el código QR, el software de seguridad funciona, pero dista mucho de ser una prevención eficaz de accidentes. Si un usuario decodifica el código QR en datos que pueden ser leídos por un teléfono inteligente, esos datos pueden conducir a una trampa.

Por ejemplo, un código QR puede contener una URL maliciosa y redirigir al usuario a un sitio web falso que el atacante conoce y se hace pasar por un administrador autorizado del sitio web, decodifica un QR bien elaborado, ejecuta comandos que dañan los datos contenidos en el Smartphone y su sistema operativo.

Además, estos mensajes quedan almacenados en el Smartphone, lo que supone un riesgo de vulneración de la privacidad si acceden personas distintas al titular, ya que estos mensajes suelen contener información personal.

La tecnología SMS forma parte del estándar de tecnología GSM, que a su vez forma parte de las redes de segunda generación. Muchos operadores de telefonía móvil siguen utilizando redes GSM, que tienen una serie de vulnerabilidades relacionadas con la tecnología.

Uso de redes desconocidas

Los teléfonos inteligentes a menudo se conectan a redes fuera de la organización y la red hogar para acceder a Internet. Algunas de sus particularidades van más allá de los límites de las redes confiables, lo que permite a los usuarios llevar consigo su entorno de trabajo o entretenimiento siempre que haya una señal de red

inalámbrica disponible. Sin embargo, estas redes son vulnerables a las escuchas, lo que compromete la transmisión de información. Las siguientes son las vulnerabilidades más comunes en este ámbito:

- Las vulnerabilidades de las redes cableadas tradicionales se aplican a las tecnologías inalámbricas.
- Los datos confidenciales que no están encriptados y enviados entre dos dispositivos inalámbricos pueden ser interceptados y divulgados.
- En general, la configuración predeterminada para las conexiones de red no es adecuada, lo que hace que el dispositivo sea vulnerable. Por ejemplo, algunos teléfonos inteligentes que se encienden por primera vez tienen Bluetooth habilitado.
- Una conexión entre un teléfono inteligente y una computadora desconocida, generalmente para sincronizar o compartir contenido, presenta un riesgo porque la computadora puede adquirir un virus que puede infectar el teléfono.

Aplicaciones de origen desconocido

Las aplicaciones instaladas en los teléfonos inteligentes utilizan los recursos informáticos, como la potencia informática, la memoria y los periféricos externos, para completar una tarea. A pesar de las medidas tomadas por los mercados oficiales, todavía existe la posibilidad de que reciban malware, aunque la probabilidad es baja.

Para evitar infecciones de malware, se deben evitar, en la medida de lo posible, las alternativas pertenecientes al grupo de canales de distribución de aplicaciones de fuentes desconocidas. Esto se debe a que estos mercados generalmente no saben si existen medidas de seguridad y la tasa de infección también es más alta que la de los mercados oficiales.

Falta de controles físicos

La falta de controles físicos solo la puede mitigar el usuario, ya que solo él puede determinar lo que está en juego si pierde o le roban su teléfono inteligente. Todos los datos almacenados están en riesgo, así como los datos a los que se puede acceder indirectamente a través de los datos almacenados en el teléfono inteligente. Suponiendo que un atacante tiene el control físico del teléfono inteligente, es posible que pueda abrir la cubierta posterior del teléfono inteligente para quitar la tarjeta de memoria sd, lo que le permite al atacante copiar todos los datos cuando el propietario no está mirando el teléfono inteligente.

Otro ejemplo de ataque seria al identificar las manchas grasosas que el usuario deja en la superficie de la pantalla debido al tacto, usando sus dedos para obtener un patrón que coincida con el código de acceso para desbloquear la pantalla. Según una investigación que presenta un estudio sobre la factibilidad de este ataque a los dispositivos Android, dado que la mayoría de los smartphones cuentan con pantallas táctiles, una de las consecuencias de su uso es un residuo graso que deja el usuario, el cual puede ser utilizado para extraer información sensible ingresada por el usuario.

Uso de servicios de ubicación

Los teléfonos inteligentes generalmente tienen chips GPS que pueden ubicar rápidamente el dispositivo. Por lo general, tienen los llamados servicios de ubicación que median entre el GPS y las aplicaciones. Por ejemplo, existen aplicaciones que rastrean un teléfono inteligente utilizando servicios de ubicación para enviarlo a un tercero a través de una conexión a Internet.

De manera similar, la tecnología de geolocalización se puede definir como una falla en la seguridad de los datos que viola la privacidad de la ubicación. Se sugiere otro ejemplo para explicar y especificar este tipo de vulnerabilidad: algunas aplicaciones utilizan la función de geolocalización del teléfono inteligente para insertar automáticamente información llamada metadatos o metadatos en sus archivos. Estos metadatos incluyen información como la ubicación geográfica y la hora exacta en que se creó la imagen.

Análisis

Respuesta Pregunta 5

Según con lo indagado en el artículo Vulnerabilidades más importantes en plataformas Android, del autor Leaño Ardila Victor Hugo, se logra sentar algunas de las recomendaciones y buenas prácticas más importantes a tener en cuenta, lo siguiente es un análisis de dichas recomendaciones.

Bloqueo de Pantalla

Bloquear la pantalla con contraseña es la operación más sencilla y una de las primeras activadas para evitar el acceso no autorizado al Smartphone. Hay tres formas de bloquear la pantalla con una contraseña, son: PIN, patrón, o contraseña. Para acceder a esta configuración: el usuario debe ir al menú principal, luego a "Configuración", luego debe ir al submenú "Seguridad", dentro del cual debe seleccionar "Bloqueo de Seguridad". La selección de contraseña y el método de entrada tienen más de una ubicación posible. Si considera con qué frecuencia se desbloquea el dispositivo, es una buena opción para un método de PIN con una longitud razonable.

Si se considera ideal, puede elegir un método de contraseña con una clave alfanumérica segura. El patrón es el más fácil de usar, aunque también es fácil de adivinar por personas alrededor del usuario que ven el mismo movimiento repetidamente, y también tiene la capacidad de adivinarlo observando las huellas dactilares en la pantalla. Se recomienda deshabilitar la traza para que se muestre en la pantalla cuando se utiliza este método de entrada clave.

Añadir información de contacto en la pantalla de bloqueo

Hay una función que es simple y puede ser útil si se pierde un dispositivo y alguien lo encuentra con la intención de devolvérselo a su propietario. La función es mostrar información personal en una pantalla seleccionada por el usuario cuando el dispositivo está bloqueado. Esta información de puede ser un número de teléfono o una dirección de correo electrónico donde puede comunicarse con el propietario de, pero debe evitar mostrar información que amenace su privacidad y seguridad.

Para agregar esta información, el usuario debe ir al menú principal de la aplicación, seleccionar "Configurar", luego seleccionar "Seguridad" en el menú que se abre, y finalmente en "Información del propietario" es posible escribir cualquier texto.

Esta práctica de seguridad en mi opinión llegaría a ser contraproducente ya que un atacante tiene información de más fácil, y llega a hacer un blanco vulnerable.

Backup de datos

Los datos del dispositivo se pueden respaldar en la nube usando dos aplicaciones preinstaladas en Android: Google Photos y Google drive. También se pueden utilizar aplicaciones de terceros. Puedes subir cualquier tipo de archivo a Google drive, su capacidad es de 15 GB. Dado que ambos suben datos a la nube, se puede acceder a ellos desde cualquier computadora. Es posible sincronizar las imágenes del dispositivo con la nube de la aplicación Google Photos, para lograrlo se deben seguir los siguientes pasos: el usuario debe ir a la aplicación, luego seleccionar “Configuración” del menú general, luego “Protección anticopia”. y sincronización; y aquí puedes activar la sincronización de los datos procesados por la aplicación.

La carga de imágenes a la nube comienza de inmediato, las que aún no se han cargado se distinguen por un ícono específico. Con todo, esta característica le permite almacenar imágenes en la nube en sincronización con las imágenes en su dispositivo, lo que significa que cuando se agregan o eliminan de su dispositivo, también se hacen en la nube.

Google Play

Una gran cantidad de malware proviene de fuentes desconocidas, como mercados alternativos de Google Play. Es decir, no suele ser conveniente descargar apps de estos mercados porque el usuario no puede saber cómo se gestionan las apps disponibles y si son de confianza. Entonces instalar él es un proceso simple, directo y rápido, no debería causar problemas. Cuando un usuario instala aplicaciones de Google Play, admite una barrera de seguridad llamada “Bouncer”, que analiza aplicaciones descargadas y aplicaciones ya descargadas en busca de malware para detenerlas. Examina adecuadamente las cuentas de usuario en busca de actividades sospechosas para detenerlas.

La configuración de Android tiene una opción de que el sistema operativo solo aceptará aplicaciones de Google Play, esto se puede activar de la siguiente manera: Desde el menú general, debe seleccionar “Configuración”, luego desde el menú aparece, debe elegir “Seguridad”, por lo que finalmente puede desactivar la casilla “Fuentes desconocidas”.

Administrador de Dispositivos de Android

En Android, puede usar otra extensión para los productos de Google, el servicio Android Device Manager, que es un servicio integrado en el sistema operativo. Le permite buscar, bloquear o eliminar datos de teléfonos inteligentes de forma remota desde su computadora. - Puede configurar la ubicación geográfica donde se encuentra el teléfono inteligente, puede verlo en el mapa usando Google Maps.

1. El teléfono inteligente se puede configurar para que suene.

2. La pantalla del teléfono inteligente se puede bloquear. Puede establecer una contraseña para bloquear de forma remota su teléfono inteligente.

Al activarlo, te pedirá que ingreses una contraseña, un mensaje y un número de teléfono en la pantalla; Si se confirma esta información, el teléfono inteligente se bloqueará con una determinada pantalla en negro.

Multiusuario

Android puede tener varios perfiles de usuario, tienen su propia configuración general, cada perfil almacena información diferente sobre las aplicaciones instaladas. La información del usuario siempre está separada de otros usuarios. Finalmente, Android tiene otra función que puede mejorar la seguridad y organizar el contenido generado por el usuario en el dispositivo. Este usuario también tiene derechos especiales y configuraciones definidas solo por él.

El usuario principal siempre se está ejecutando, incluso si otros se están ejecutando en primer plano. Un usuario secundario puede ser cualquier usuario agregado al dispositivo, pero no un usuario principal. Un usuario secundario puede eliminarse a sí mismo y al usuario maestro, pero no puede afectar a otros usuarios del dispositivo. El proceso del sistema suspende a los usuarios secundarios que se ejecutan en segundo plano cuando el dispositivo necesita memoria adicional para operaciones realizadas por el usuario de primer plano.

Encriptación del dispositivo

Android puede realizar el cifrado de disco completo. Esto significa que todos los datos del usuario se pueden cifrar con una clave de cifrado basada en la contraseña o la contraseña proporcionada para bloquear la pantalla, después de lo cual se solicita la contraseña/clave cada vez el dispositivo está encendido. Si el dispositivo está encriptado, todos los datos de usuario generados se encriptan automáticamente antes de guardarlos en el disco; además, cualquier lectura futura descifrará automáticamente los datos antes de devolver la energía al proceso que solicitó la lectura. Este mecanismo puede brindar protección adicional en caso de robo o pérdida del dispositivo. Además de recomendarse para proteger la seguridad, este mecanismo también se utiliza para comprobar la integridad de los datos. Por otro lado, este mecanismo no tiene un efecto notable en el rendimiento, al menos en las computadoras más modernas.

Tercero, luego del análisis se realizó un cotejamiento de resultados, demostrados por medio de gráficos, que muestran las vulnerabilidades más comunes.

Resultado Pregunta 1

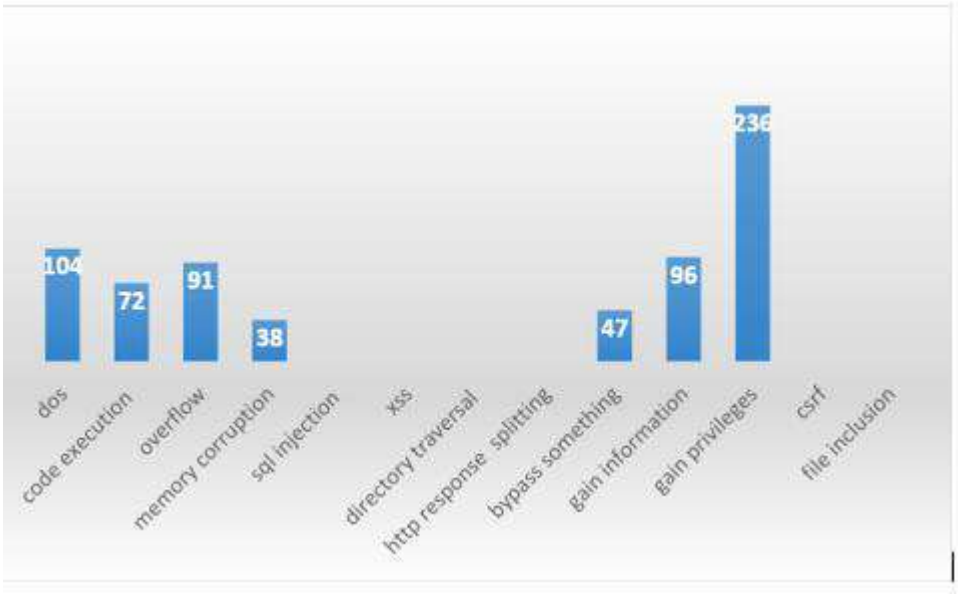
En conclusión el modelo de seguridad de Android aún sigue siendo desconocido para la mayoría de los usuarios que usan este sistema operativo en sus dispositivos móviles, de manera que a raíz de esto se presenta más oportunidades de ser atacado, esto podría evitarse si los usuarios quisieran informarse más respecto al tema, tal vez para algunos usuarios este tema parezca tedioso o cansado, pero si tenemos en cuenta que es toda nuestra información la que está en riesgo se llega a mitigar esta problemática, que al día de hoy es frecuente.

Resultado Pregunta 2

La grafica a continuación muestra las vulnerabilidades más comunes en los dispositivos móviles con sistema operativo Android en los últimos años.

Figura 5

Grafico de vulnerabilidades



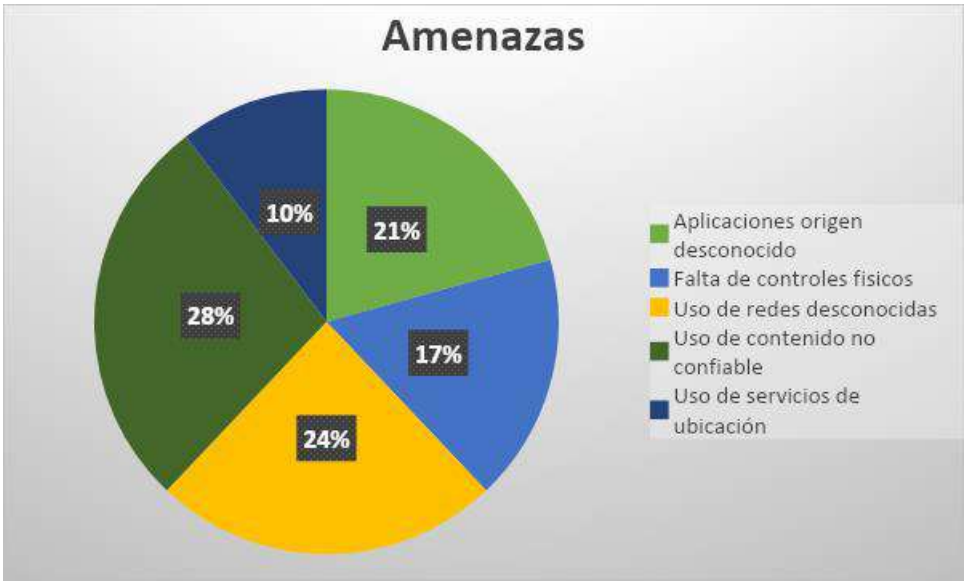
Nota: Este grafico representa las vulnerabilidades más comunes en los dispositivos con sistema operativo Android.

Resultado Pregunta 3

La grafica a continuación muestra las vulnerabilidades más comunes a nivel general en los dispositivos móviles con sistema operativo Android.

Figura 6

Gráfico de amenazas



Nota: Este grafico muestra las amenazas más comunes en los dispositivos móviles con sistema operativos móviles Android.

Resultado Pregunta 4

La grafica a continuación muestra las vulnerabilidades más comunes nivel del entorno de seguridad Android en los dispositivos móviles.

Figura 7

Gráfico de vulnerabilidades 2

Nota: Este grafico muestra las vulnerabilidades más comunes en Android.

Resultado Pregunta 5

La siguiente, es una conclusión respecto a las recomendaciones y buenas prácticas más importantes a tener en cuenta.

En conclusión las buenas y recomendaciones de seguridad expuestas en la actividad dos, algunas resultan fáciles de realizar y otras un poco más complicadas, ya que hay que tener en cuenta que de que no todos los usuarios cuentan con la suficiente información para realizarlas, o de lo contrario realizan estas prácticas que pueden resultar beneficiosas pero, a criterio personal llegan a ser contraproducentes, como por ejemplo el incluir información personal en la pantalla de bloqueo, puede que sea un gesto inofensivo desde una perspectiva general, pero para la visión de un atacante informático llega a ser un gran oportunidad de vulnerar la información del usuario, independientemente del contenido que se ingrese, cualquier dato por más irrelevante que parezca, toda información puede ser usada en contra el usuario.

Actividades del objetivo específico no. 2

Para llevar a cabo los resultados del segundo objetivo, se optó por crear tres actividades distintas las cuales son:

Primero, se realizó un levantamiento de información, soportados en artículos web, referencias bibliográficas, entre otros.

Figura 8

Actividad uno del objetivo dos.

Levantaminento de informacion					
Titulo de pagina	Autor	Fecha de publicacion	Aporte	Link	Titulo de articulo
INCIBE Instituto Nacional de Ciberseguridad	INCIBE	13/01/2016	El articulo brinda primeramente una introduccion acerca de la seguridad de la infromacion en los dispositivos moviles, da un vision general sobre las amenzas mas comunes a las que se ven expuestos los usuarios, luego da una serie de recomendaciones empezando por lo mas basico como por paracticas un poco mas avanzadas pero que se pueden implementar de manera sencilla.	https://www.incibe.es/protege-tu-empresa/blog/decalogo-buenas-practicas-seguridad-movil	Decalogo de buenas practicas en seguridad movil
SEIDOR nts	SEIDOR nts	13/09/2021	El articulo da una vision general de lo quelos atacantes informaticos buscan principalmente en los dispositvos moviles, brinda medidas basicas de seguridad en lo que a aplicaciones refiere.	https://www.nts-solutions.com/blog/seguridad-aplicaciones-moviles.html	Seguridad de las aplicaciones ¿Cómo garantizarlas?

Nota: La imagen representa el levantamiento de información basada en artículos web.

Anexo 3

Segundo, se llegó a un análisis de la información obtenida y así verificar las buenas prácticas y recomendaciones más comunes en los dispositivos y aplicaciones móviles con sistema operativo Android.

Análisis de la información recolectada

Buenas prácticas para de uso de información en dispositivos móviles Android.

Según lo indagado en los artículos web, y en especial el artículo “Decálogo de buenas prácticas en seguridad móvil “publicado por INCIBE, se puede establecer que entre las mejores prácticas para la protección de la información de los dispositivos móviles Android se puede analizar lo siguiente:

La seguridad móvil se ha transformado en uno de los pilares del plan de seguridad de la información de la compañía. Hoy en día dependemos de los dispositivos móviles para casi todo, y esto se ha convertido en el

objetivo de los ciber-delincuentes, ya que de ellos pueden extraer información muy importante y que puede ser ofertada en el mercado ilegal.

Para ello INCIBE, desde un punto de vista profesional brinda algunos consejos; lo más común es que las políticas de seguridad de datos establezcan claramente que no se recomienda el uso de redes fuera de la empresa y siempre usar una Red Privada Virtual de ser necesario.

Hay que tener en cuenta que para que los usuarios tomen en cuenta esta recomendación, se debe explicar el cómo usar y acceder a redes privadas virtuales. Además, se debe conocer las normas por las que se rige un entorno empresarial con relación a los dispositivos móviles y el trabajo remoto, y la información almacenada fuera de las instalaciones de la organización.

Por otra parte, las computadoras portátiles como el caso de los dispositivos móviles, constantemente tienen la opción de bloquear cuando no están en uso. Estos dispositivos deben tener esta función activa para que de forma automática se bloqueen cuando se no se usen por un tiempo prudente. De igual modo esto es una buena práctica y puede hacerlo el usuario mismo.

Algo a tener en cuenta es que un atacante puede realizar una copia del dispositivo y robar información importante. Además, las redes Wi-Fi y demás redes inalámbricas como la tecnología Bluetooth trasmiten ondas electromagnéticas en el aire. Esto quiere decir que pueden ser escuchados, sin importar si lo datos están encriptados, no podrá ser cifrada.

En cambio, a medida que aumentan el poder de cómputo, no tomara mucho tiempo en romper la seguridad de las conexiones mencionadas. De esta manera, el atacante descifra lo que se transmite por Wi-Fi.

En conclusión, el tener estos conceptos de buenas prácticas presentes en los usuarios ayudara a mitigar los ataques de cibercriminales, esto pude ser puesto en práctica tanto a nivel personal como en el ambiente corporativo.

Recomendaciones para la protección de dispositivos Android

En las páginas indagadas se encontraron varios artículos como el de “Seguridad de las aplicaciones móviles: ¿Cómo garantizarlas?” Publicado por NTS SEIDOR. De todo el referente indagado este en específico brinda medidas de seguridad a nivel de aplicaciones móviles, este se divide en dos categorías, la primera son requerimientos generales sugeridos para todas las aplicaciones móviles. La segunda a las aplicaciones que manejan datos altamente reservados, como por ejemplo el sector financiero, la industria de la salud o el sector corporativo.

De acuerdo lo anterior se logra analizar lo siguiente:

Según la postura de NTS SEIDOR las evoluciones tecnológicas van a un ritmo acelerado, casi que sin darnos cuenta. La acción de realizar llamadas y enviar mensajes, toda esta información importante de los usuarios queda almacenada en sus dispositivos móviles, por medio de aplicaciones que se usan diariamente.

Por ello este artículo brinda una serie de conceptos desde un punto de vista de desarrolladores de software, desde un ámbito general hasta funciones internas de las aplicaciones. Sin embargo, lo esencial es que se sea consciente de que al implementar instrumentos de seguridad en una aplicación es importante, sobre todo si se tiene en cuenta el gran volumen de usuarios que pueden hacer uso de esta.

Este articulo presenta medidas básicas de seguridad, para ello se hace hincapié en el uso del estándar de seguridad de aplicaciones móviles OWASP, dirigido a los desarrolladores de software, y así desarrollar aplicaciones seguras.

Entre las prácticas que se ofrecen están:

Uso de claves criptográficas, que son una cadena de caracteres que se usan en un algoritmo de encriptación para cambiar los datos y hacer que parezcan aleatorios.

Autenticación y control de sesiones, es el proceso de identificar un individuo sobre la base de sus credenciales, esto se hace para decidir si alguien es quien dice ser.

Comunicación con servicios, este el proceso en que la aplicación se comunica con el servidor allí es donde se debe garantizar la confidencialidad e integridad de los datos intercambiados.
Calidad del código, a pesar de que las apps no son tan vulnerables se deben seguir buenas prácticas y así asegurar el correcto funcionamiento de la aplicación.

En conclusión, cada día usamos más aplicaciones móviles y cada vez almacenan más y más datos sensibles de los usuarios. Por tanto, es muy importante estar al tanto de las nuevas medidas de seguridad e implementarlas de manera proactiva en su creación. La finalidad no solo debe ser que el usuario puede relacionarse con una buena experiencia de usuario, sino también se lleve una completa seguridad.

Tercero, luego del análisis se realizó un cotejamiento de resultados, demostrados por medio de tablas, las buenas prácticas y recomendaciones de seguridad en los dispositivos móviles Android.

Las siguientes tablas listan las buenas prácticas y las recomendaciones para la protección de la información y aplicaciones en dispositivos móviles.

Resultados del análisis

Tabla 2

Buenas prácticas de uso en dispositivos móviles Android

● **Compruebe si la política de seguridad de nuestra la empresa permite conexión a redes externas y cuales han de ser sus condiciones, esto puede aplicarse en el ámbito corporativo ya que hay que tener en cuenta que se maneja información importante y delicada.**
● **Nunca dejar el teléfono celular o dispositivo móvil en un lugar público. Por otra parte, si es necesario desconectarse del dispositivo, bloquearlo siempre como en los dispositivos corporativos. Incluso se pude configurar para que el dispositivo después de cierto lapso se bloque, una acción sencilla, pero de gran ayuda.**

● **Si está conectado de forma remota a una red corporativa asegurarse de crear una conexión VPN para así proteger la comunicación desde ambas partes.**
● **Cuando reciba correos electrónicos, desconfié de aquellos con archivos adjuntos sospechosos de fuentes desconocidas o no solicitadas, recordar que esto puede dejar una puerta abierta a posibles hackers.**
● **Nunca instales aplicaciones o software en el dispositivo y con mayor restricción si se trata de un equipo corporativo.**

Nota: Esta tabla muestra las buenas prácticas de uso en dispositivos móviles Android

Tabla 3

Recomendaciones para la protección de dispositivos y aplicaciones Android

● **No almacene datos confidenciales en el almacenamiento local del dispositivo y, si es de ser necesario, cifrar con un clave de dispositivo de almacenamiento seguro que requiera una previa autenticación.**
● **No escriba información confidencial en el registro del sistema ni en las copias de seguridad.**
● **No exponga información confidencial, como contraseñas o números de tarjetas, a través de la interfaz de usuario o las capturas de pantalla, y deshabilite el almacenamiento en cache del teclado de los campos de texto que contienen dicha información.**
● **No confié únicamente en la criptografía simétrica, cuyas claves se encuentran directamente en el código fuente de la aplicación.**
● **No utilice la misma clave de cifrado para diferentes propósitos.**
● **Los valores aleatorios son generados por un generador de números aleatorios bastante seguros.**
● **Usar un mecanismo de autenticación de dos factores para aplicaciones que manejen datos altamente confidenciales.**

● **Las sesiones y las credenciales deben caducar cuando el usuario ha estado inactivo durante un periodo de tiempo predeterminado.**
● **Los datos deben enviarse encriptados mediante el protocolo TLS.**
● **La aplicación debe ser verificada con el certificado X.509 del sistema remoto al disponer el canal seguro y solo se aceptan certificados firmados por una CA de confianza.**
● **La aplicación usa su propio repositorio de certificados o añade un certificado de servidor o una clave pública.**

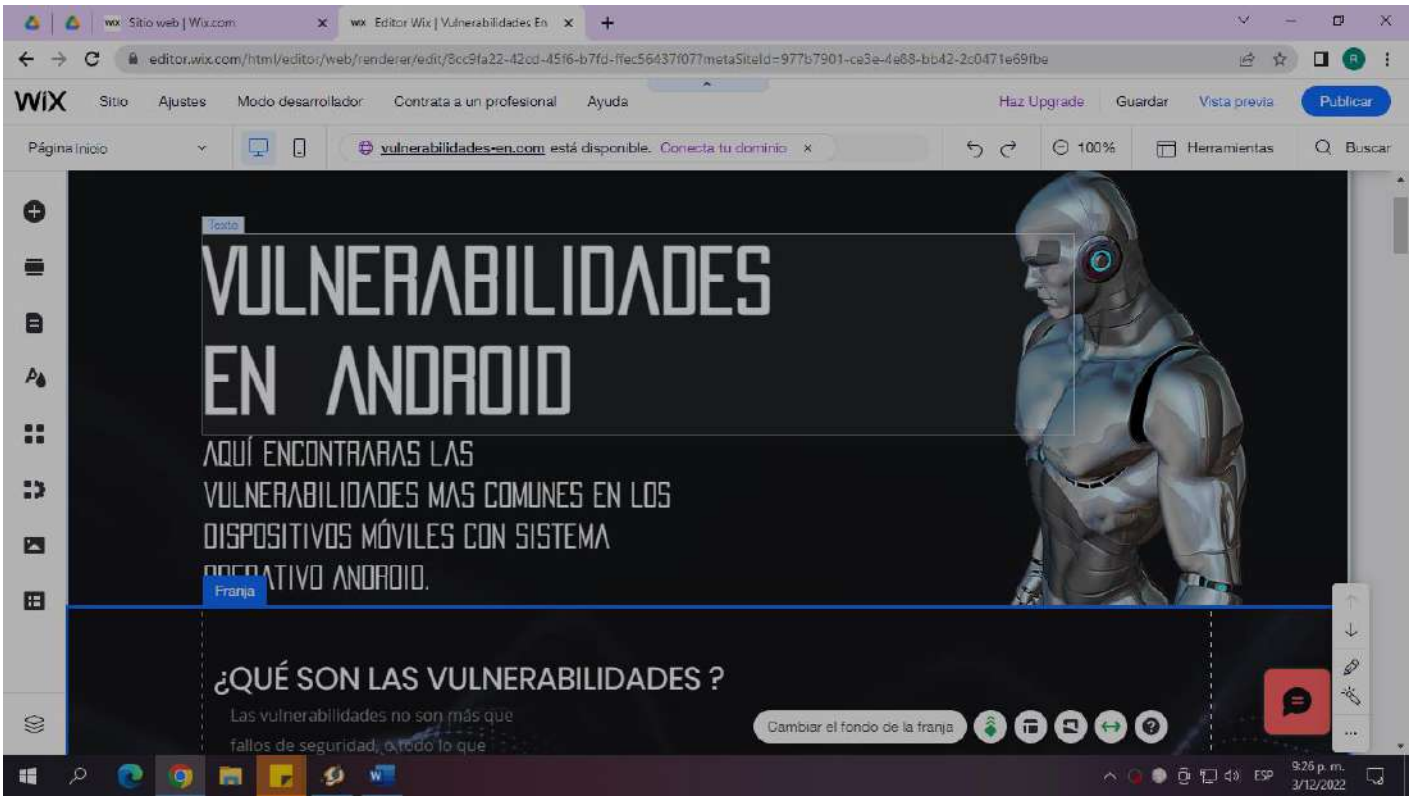
Nota: Esta tabla muestra recomendaciones para la protección de dispositivos y aplicaciones en dispositivos Android.

Actividades del objetivo específico no. 3

Para las actividades del objetivo tres se optó por la opción de evidenciar el proceso de la creación de las pagina web, por medio de imágenes, para ello las actividades realizadas de dividen en: primero plantilla de la página web vulnerabilidades más comunes en dispositivos móviles Android.

Figura 9

Plantilla página vulnerabilidades



Nota: Esta imagen muestra la plantilla seleccionada para la creación de la página web.

Segunda actividad inserción de la información en la página web.

Figura 10

Inserción de información a página web vulnerabilidades.

Nota: Esta imagen muestra el proceso de inserción de información en la página web.

Tercera actividad página web ya creada.

Figura 11

Resultado final página vulnerabilidades

Figura 12

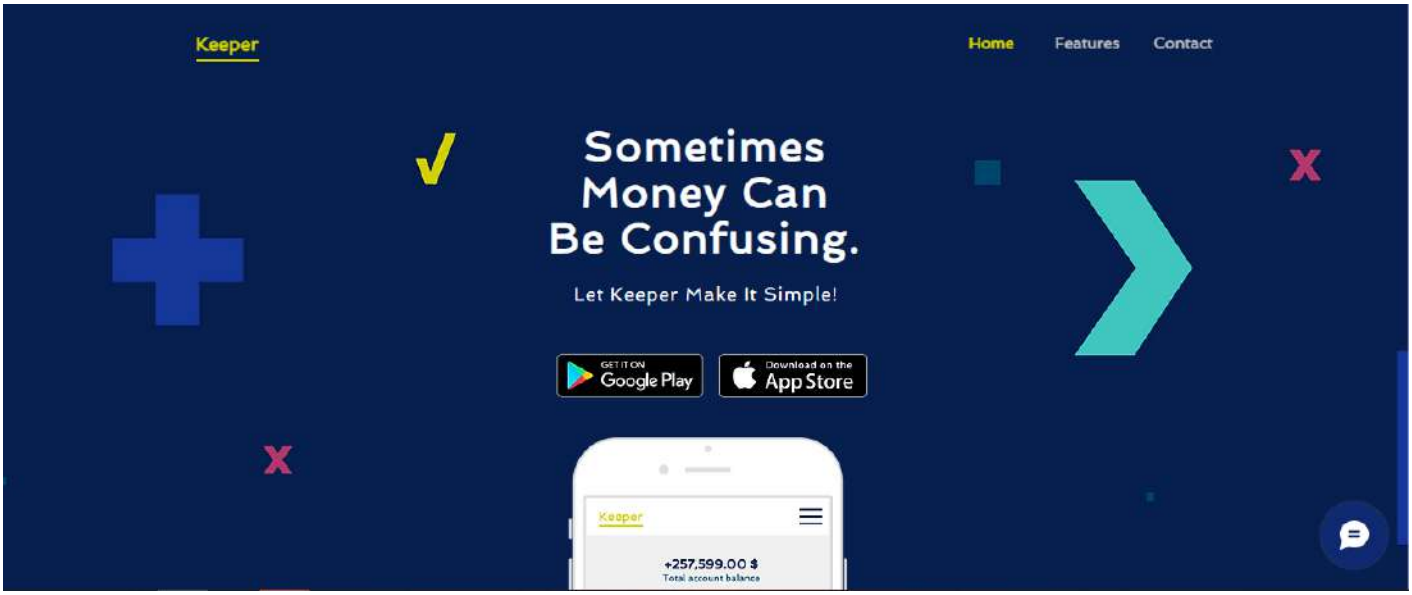
Figura 13

Página de recomendaciones y buenas prácticas de seguridad en Android.

Primera actividad

Figura 14

Plantilla página web recomendaciones y buenas practicas



Nota: La imagen muestra la plantilla seleccionada para la creación de la página web.

Segunda actividad

Figura 15

Inserción de información a página web recomendaciones y buenas practicas

Figura 16

Figura 17

Figura18

Resultado final página recomendaciones y buenas prácticas.

Nota: Las siguientes imágenes muestran el resultado final de la creación de la página web.

Figura 19

Figura 20

Figura 21

Figura 22


Administrador de Dispositivos de Android
04
En Android, puede usar otra extensión para los productos de Google, el servicio Android Device Manager, que es un servicio integrado en el sistema operativo. Le permite buscar, bloquear o eliminar datos de los teléfonos inteligentes de forma remota desde su computadora. Puede configurar la ubicación geográfica donde se encuentra el teléfono, puede verlo en el mapa usando Google Maps.
Con esto se puede:
1. El teléfono inteligente se puede configurar para que suene.
2. La pantalla del teléfono se puede bloquear. Puede establecer una contraseña para bloquear de forma remota su teléfono.
Al activar esto, te pedirá que ingreses una contraseña, un mensaje y un número de

Figura 23

Figura 24

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Una vez realizado el estudio de investigación del presente proyecto, se cuenta con información necesaria para llegar a las siguientes conclusiones:

Se llega a la conclusión de que la vulnerabilidad más común en los últimos años en los dispositivos móviles con sistema operativo Android es la llamada "Gain Privileges" esta consiste en explotar una configuración en específico lo cual concede a los atacantes muchos más privilegios de administrador, lo que causa el hurto de datos confidenciales, insertar software malicioso, dañar el sistema operativo o manchar la reputación de una organización.

Por otra parte, se logró sentar que la vulnerabilidad con casos más bajos es la llamada "memory corruption" con 38 casos registrados, esta consta en que la memoria se altera sin haber alguna asignación en concreto, en otras palabras, se transforma parte de la memoria por causa de errores de programación, que hace el trabajo de los piratas informáticos más fácil al ejecutar código malicioso.

En cuanto a amenazas según lo investigado se logra establecer que Spoofing es la técnica más común que consiste en la suplantación en el que una fuente desconocida se disfraza de una fuente confiable para quien recibe la información de esta manera los hackers obtienen datos sensibles de sus víctimas o para
Utilizar medios computacionales para llevar a cabo ciber ataques, además una de las amenazas menos comunes es el Rooting y Jailbreaking que consiste en eliminar las restricciones de seguridad declaradas por el fabricante del dispositivo móvil para así brindar al usuario control sobre el dispositivo, esto da acceso a muchas características interesantes que de otro modo no estarían disponibles.

A nivel general una de las vulnerabilidades más comunes en los dispositivos móviles con sistema operativo Android es la de uso de contenido no confiable, un ejemplo claro de esto es la tecnología de los códigos QR, estos pueden dañar indirectamente el sistema ya que el desconocimiento de los usuarios hacen que al escanear el código QR los lleva a páginas web maliciosas que solo el atacante conoce, decodifica este QR y ejecuta comandos que perjudican los datos almacenados en el dispositivo además del sistema operativo.

Se llegó a determinar que la amenaza menos común es la del uso de servicios de ubicación como bien se sabe por lo general todos los dispositivos móviles cuentan con chips GPS, que funcionan para rastrear en cuestión de segundos el dispositivo, pero además de esto la mayoría de las aplicaciones usan este servicio de ubicación, por esta razón algunas aplicaciones maliciosas que usan esto a su favor para enviar esta información a terceros usando la conexión a internet.

En cuanto a las buenas prácticas y recomendaciones para la protección de dispositivos se logra sentar practicas sencillas como el bloqueo de pantalla, backup de datos, el uso del administrador de dispositivos un sistema que viene integrado en Google, lo que permite buscar, bloquear o eliminar datos de los teléfonos de manera remota desde su computadora personal.
Además, Android tiene la ventaja de poder tener varios perfiles de usuario, de esta manera cada perfil almacena información distinta de acuerdo a las aplicaciones instaladas, también la encriptación del dispositivo resulta ser una buena opción ya que Android permite realizar el cifrado del disco completamente esto quiere decir que los usuarios pueden cifrar la información con una clave de cifrado basada en la contraseña insertada para el bloqueo de pantalla, de esta manera se solicitara la clave o contraseña cada vez que el dispositivo se encuentre encendido.

Todo lo mencionado anteriormente corresponde desde un punto de vista general los resultados de la ardua investigación especificando los conceptos más importantes y de mayor relevancia, descubriendo así información nueva y de utilidad para futuras investigaciones.