Evaluación de vulnerabilidades de seguridad en Software Android en el año 2021
Evaluation of security vulnerabilities in Android Software in the year 2021

Ing. José Luis Torres Chavarría
Universidad Latina, Costa Rica
luistc1911@hotmail.com

Recibido 25/mar/2020
Aprobado 20/may/2020

Resumen-
Este artículo es un análisis experimental de las vulnerabilidades que pueden explotarse en el sistema operativo Android, siendo este el más utilizado en el todo el mundo por millones de dispositivos, lo que le convierte en un objetivo interesante para los piratas informáticos. No existe ningún software 100% seguro y, cuánto mayor es su cuota de mercado más fácil es que los usuarios, expertos de seguridad y piratas informáticos descubran nuevas vulnerabilidades con las que atacar a los usuarios. Es prácticamente imposible llevar un seguimiento de todas las vulnerabilidades de Android y comprobarlas, una a una, en nuestro dispositivo. La vulnerabilidad mas débil en toda la superficie de un ataque es el usuario, la seguridad de la información depende en gran medida del uso adecuado o no que se le de a este. Los incidentes de seguridad en dispositivos con S.O Android se han incrementado de manera alarmante debido a malos hábitos de seguridad, como por ejemplo el uso de redes inalámbricas públicas, la utilización de contraseñas débiles, el uso deliberado de redes sociales o mensajería instantánea donde se comparte información sensible sin ningún tipo de cuidado, como numero de tarjetas, numero de cuentas, lugar de vacaciones, bancos de preferencia, condición económica entre otra información personal que puede ser utilizada por los ciberdelincuentes para llevar a cabo ataques como ingeniería social, Phishing, envío de archivos o aplicaciones maliciosas, escalamiento de privilegios por wifi, por medio de un centro de comando y control donde realizan interceptación de las tramas de red con datos de usuarios (man in the middle), con contraseñas de sus redes sociales o incluso información bancaria. De acuerdo con esto, en este artículo se pretende reflexionar acerca de los diferentes aspectos relacionados a dicho problema de seguridad, que no solo afecta a dispositivos móviles con S.O Android, sino cualquier otro fabricante, ya que como se menciono anteriormente no existe un sistema operativo 100% seguro. A continuación se describirán las amenazas mas comunes hasta el día de hoy, y se darán posibles recomendaciones ara lograr minimizar el impacto al riesgo asociado a malas prácticas de seguridad de la información en dispositivos móviles con S.O Android.

Palabras Claves. *Android, Dispositivo, Amenazas, Vulnerabilidades, Phishing, man in the middle*

Abstract Context:
This article is an experimental analysis of the vulnerabilities that can be exploited in the Android operating system, which is the most used worldwide by millions of devices, which makes it an interesting target for hackers. There is no 100% secure software, and the higher its market share, the easier it is for users, security experts and hackers to discover new vulnerabilities with which to attack users. It is practically impossible to keep track of all Android vulnerabilities and check them, one by one, on our device. The weakest vulnerability on the entire surface of an attack is the user, the security of the information depends largely on the proper use or not that is given to it. Security incidents on devices with Android OS have increased alarmingly due to poor security habits, such as the use of public wireless networks, the use of weak passwords, the deliberate use of social networks or instant messaging where it is shared Sensitive information without any kind of care, such as number of cards, number of accounts, place of vacations, preferred banks, economic condition among other personal information that can be used by cybercriminals to carry out attacks such as social engineering, Phishing, shipping of files or malicious applications, escalation of privileges by wifi, through a command and control center where they intercept network frames with user data (man in the middle), with passwords of their social networks or even banking information . In accordance with this, this article aims to reflect on the different aspects related to said security problem, which not only affects mobile devices with Android OS, but any other manufacturer, since as mentioned above there is no operating system 100% sure. The most common threats to date will be described below, and possible recommendations will be given to minimize the impact of the risk associated with poor information security practices on mobile devices with Android OS.

Keywords: *Android, Device, Threats, Vulnerabilities, Phishing, man in the middle*

I. INTRODUCCIÓN

Los resultados de la investigación arrojaron que conforme va pasando el tiempo el riesgo a las vulnerabilidades en dispositivos móviles se va reduciendo, la factura de vulnerabilidades también se va reduciendo pero en cuanto a los hábitos operativos de los usuarios dejan en evidencia que se debe tocar el tema con más atención. Las norma ISO 27001:2013 brinda una guía para una adecuada gestión de la seguridad informática aportando controles para mediar que se está haciendo bien y cuáles son las mejores prácticas que se requieren adoptar prestar atención en ese campo.

Según el medio de comunicación Andro4all (2021), centrado en contar todas las novedades sobre el mundo de Android, En el año 2003 se fundó la empresa Android Inc. Su intención era mejorar la experiencia del usuarios de cámaras digitales, donde en 2005 fue adquirida por Google.

Existen diferentes pasos que debemos seguir e identificar para tener hábitos operativos correctos, así como configuraciones de contexto de los dispositivos y no menos importante hacer seguimiento de los riesgos en el tiempo en la gestión de las vulnerabilidades desde el punto de vista cibernético.

Según Herrera y Giovanny (2017) no existe suficiente sensibilización para que el propio usuario no ponga en riesgo su propia seguridad y la de los sistemas informáticos en los cuales

interactúa, puesto que es él mismo, el que le otorga en determinadas ocasiones, acceso completo a los delincuentes a sus dispositivos móviles y por medio de estos a la infraestructura y plataformas tecnológicas de cualquier organización (p.20).

Durante la investigación de este proyecto se cuantificaron las diferentes vulnerabilidades que podrían existir a raíz del buen o mal uso que los usuarios les dan a sus dispositivos, por lo consiguiente es imprescindible cumplir con medidas o controles compensatorios que ayuden a mitigar el riesgo de un ataque.

Al conocer las amenazas más comunes en todos los dispositivos móviles, los usuarios y organizaciones tendrán mayor visibilidad del tipo de vulnerabilidades a las que están expuestos permitiendo actuar con mayor rapidez ante estas amenazas, dentro de lo que se conoce como la superficie de ataque, contando con robustos sistemas de gestión de riesgos digitales, para evitar verse afectado por estas.

En la mayoría de casos los "dolores de cabeza" tanto en compañías como usuarios es la falta de visibilidad en cuanto a las vulnerabilidades y amenazas existentes, esta tarea se vuelve cada día mas difícil de monitorear debido al número de vulnerabilidades contenidas y el porcentaje de vulnerabilidades creciente exponencialmente todos los días, por lo que es muy importante entender que esto expone cada día más a grandes riesgos sumado a la gran falta de controles compensatorios aumenta el riesgo de sufrir un ataque cibernético a dispositivos móviles.

Es ciertamente en épocas festivas o temas de afectación mundial como por ejemplo, navidad, emergencias sanitarias (pandemias), como la vivida actualmente con el Covid19, donde los atacantes se enfocan en este tipo de actividades para ejecutar y diseñar sus exploits y sus ataques para poder enmascarar estas ejecuciones bajo información del momento que los usuarios lo vean con ojos más familiarizados, lo que lo convierte en maneras sencillas de expandir virus o ataques de día cero o bien Phishing en los cuales se encuentra una alta tasa de víctimas sin mayores esfuerzos. Por lo que con cada acontecimiento que suceda mundialmente, se disparan también los ataques en todos los ámbitos tecnológicos y obviamente los usuarios Android no son la excepción.

Según Check Point, en su Informe de Seguridad Móvil 2021 “El aumento del teletrabajo durante la pandemia de COVID-19 ha supuesto una gran expansión de la superficie de ataque móvil, lo cual ha provocado que el 97% de las empresas se enfrenten a amenazas de este tipo procedentes de varios vectores de ataque. En este sentido y con la previsión de que el 60% de los trabajadores serán usuarios de dispositivos móviles en 2024”.

En cuanto a las tecnologías operacionales en manufactura, energía o servicios críticos de los países se ven también muy expuestos a sufrir de ataques a sus sistemas y detrás de todos estos intentos de vulnerar la seguridad de la información se encuentran implícitos diferentes intereses, ya sea económicos o sociales en donde se busca mostrar el poder que tienen y el control que pueden ejercer sobre grandes organizaciones ingresando a sus sistemas sin ser detectados, borrando rastros y deteniendo sus operaciones, teniendo un control completo de estas hasta que se les haga un pago para devolver a la empresa su autonomía.

Según indica el último informe “El estado de la tecnología operativa y la ciberseguridad” de Fortinet, (2021), El 90 % de las empresas de servicios críticos recibió un ciberataque en el último año,

Este dato es prácticamente igual al del estudio

de 2020, lo que confirma que es un problema que no se ha resuelto.

Esto lo ponemos de ejemplo para entender mejor desde otra perspectiva el enfoque de la investigación y la importancia de entender cómo suceden estos ataques y en dónde también son víctimas los usuarios de dispositivos móviles de diferentes sistemas operativos pero mayormente usuarios con el sistema operativo Android, ya que, es el que tiene mayor participación del mercado por lo tanto le convierte en también en el objetivo más visible para los atacantes.

Canalys reporta que el mercado de smartphones creció 27% en el primer trimestre de 2021 respecto al año anterior, un importante aumento después de un 2020 problemático para toda la industria.

La norma ISO 27001:2013, se brindan controles de seguridad necesarios para lograr adaptase a las mejores prácticas de seguridad de la información para garantizar la confidencialidad, integridad y disponibilidad de la información.

Como principal objetivo del artículo está el hacer conciencia de los lectores sobre temas de ciberseguridad, seguridad de la información y en general reflexionar sobre los problemas de seguridad que existen en dispositivos móviles con sistema operativo Android, siendo el mas atacado por los ciberdelincuentes para sustraer información confidencial de los usuarios. El artículo introduce conceptos básicos de seguridad, S.O. Android, antecedentes y estadísticas, continuando con una serie de recomendaciones finales que se deben tener ante estos problemas de seguridad.

A-Antecedentes del problema

Existen muchas personas con pocos o nulos conocimientos acerca el adecuado uso de la información personal que se comparte en redes sociales, u otros medios de comunicación por medio del dispositivo móvil, el cual se ha convertido en nuestra computadora personal significando así también un mayor riesgo en caso de perder el dispositivo o ser atacado por un delincuente cibernético.

Parte de lo que ha contribuido a esta problemática y a la carencia de conocimientos técnicos en temas relacionados a ciberataques a dispositivos móviles en este caso específico sobre dispositivos móviles con sistema operativo android, es la falta de información disponible en medios informativos y redes sociales debido a que es muy poco compartida por su naturaleza ilegal en muchos casos, sin embargo es importante evangelizar en temas de ciberseguridad en todos los ámbitos y con mas razón en el tema de los dispositivos móviles en donde se concentra gran parte de la población cibernética.

En el libro de Carneiro, Toscano, y Díaz (2021), se refieren que educar es ayudar a las personas a transformarse, a realizar su potencial máximo, a liberarse de trabas y grilletes que impiden el florecer natural de los talentos de cada persona (p.18).

B-Fundamentos teóricos

1-Seguridad

La seguridad de la información, según ISO 27001:2013, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización (p.11).

Tomando en cuenta que un dispositivo celular es una computadora y por ende se deben tener todos los cuidados requeridos para el resguardo de la información, se debe tener en consideración la debida protección de este ante posibles personas mal intencionadas que quieran robar datos o hasta el mismo dispositivo por lo que es igualmente necesario tener restricciones tanto de ingreso al sistema como la protección física de este.

Según la Universidad Unir (Universidad Internacional de la Rioja, España), la seguridad

informática es el nivel de madurez en seguridad que tiene una organización. (2020).

Lo que nos va a llevar a tener mayor seguridad en nuestros dispositivos móviles, muy necesario hoy en día como ya se ha mencionado anteriormente el impacto que puede tener un ataque de día cero, un ransomware o cualquier otro tipo de ataque, es incalculable por lo que la seguridad en los dispositivos móviles es también una tarea que debemos tener clara y actualizada.

Contar con un antivirus de paga, sería una buena opción ya que esta nos va a proveer de una protección mayor en cuanto a que tienen una mayor cobertura de la superficie de ataque por lo tanto generan mayor valor agregado a la hora de realizar sus escaneos.

Jori Hamilton (2021) en su artículo "Seguridad de los dispositivos móviles: Preocupaciones y soluciones para 2021 y más adelante" sobre el antivirus… "al combinar este software con un firewall ayudará a bloquear cualquier tráfico no deseado. Actualiza ambos programas cada vez que haya una nueva versión, para proteger tu sistema contra las amenazas más recientes."

Según la EALDE (Business School, 2021), existen diferentes amenazas de seguridad informática en dispositivos móviles dentro de las cuales se destacan:

2-Ataque de malware:

Suelen utilizar un software malicioso para generar daños en el móvil.

3-Phishing:

Son correos electrónicos (aunque se puede utilizar cualquier otro medio de mensajería) en los que se suplanta la identidad de una persona o entidad de confianza de la víctima, para hacerle pulsar un enlace, donde en realidad se encuentra software malicioso que puede infectar a la víctima.

4-Man in the middle:

Consiste en obtener información sensible mediante la instalación de puntos de acceso a Internet, en lugares públicos, con redes libres. Así, cuando los usuarios se conectan, dan acceso a su información a los atacantes de forma involuntaria.

5-Alteraciones del sistema operativo:

Alterar el sistema operativo del terminal móvil implica riesgos, dado que alteramos su configuración inicial. De esta forma, se podrían deshabilitar, por ejemplo, las restricciones de seguridad que posee por defecto.

6-Fugas de información:

Esta amenaza de seguridad en dispositivos móviles sucede cuando una app, que teóricamente es legítima, en realidad captura datos nuestros, y los transmite a terceros.

7-Vulnerabilidad

En términos de seguridad informática puede ser definido como "una debilidad del sistema informático que puede ser utilizada para causar un daño."

INCIBE (2020) en su Glosario de términos de ciberseguridad: se refiere a una vulnerabilidad como Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos. Las empresas deben ser conscientes de estos riesgos y mantener una actitud preventiva, así como llevar un control de sus sistemas mediante actualizaciones periódicas (p.38)

7-Amenaza

En un ambiente informático una amenaza es la probabilidad de que se materialice una vulnerabilidad causando daños.

Según INCIBE (2020) También debemos tener en cuenta que una amenaza puede convertirse en una vulnerabilidad, sino se aplican las medidas de seguridad oportunas mediante

parches o actualizaciones de software y herramientas de protección adecuadas (antivirus, antimalware, etc.)

8-Seguridad de la información

Es la protección de la información y de los sistemas de información de intrusiones y accesos no permitidos.

Rojas Valduciel (2016), enfoca la seguridad de la información como las medidas y actividades que procuran proteger los activos de información, entendiéndose éstos como los conocimientos o datos que tienen valor para una organización, en sus diferentes formas y estados, a través de la reducción de riesgos a un nivel aceptable, mitigando las amenazas latentes.

II. Propuesta

De acuerdo con la información obtenida por medio de las metodologías aplicadas se valida la necesidad de implementar controles en cuanto a buenas prácticas en el uso de dispositivos móviles, con el objetivo de mitigar riesgos y amenazas en cuanto a pérdida de la información. En el planteamiento para la aplicación de controles de seguridad de la Información para el uso de dispositivos móviles Android, se tomará como referencia el flujo de la información que se genera en los usuarios encuestados a través de las herramientas tecnológicas y redes sociales.

El Sistema de Gestión de la Información propuesto dentro del presente proyecto exige que siga una serie de requisitos para que se establezca. Permitiendo proceder metodológicamente para efectuar una identificación de amenazas en el mal uso de los dispositivos móviles dado un alcance determinado, diferenciar entre el análisis y evaluación del riesgo en malos hábitos de uso de dispositivos móviles para garantizar la seguridad de la información.

Los usuarios pueden mantener su información segura en su dispositivo móvil o ponerla en riesgo por el simple hecho de no saber gestionar adecuadamente la seguridad de la información en sus dispositivos móviles, lo que ha llevado a la información a ser considerada como un activo principal y la seguridad de los datos es esencial para su adecuado resguardo y conservación.

C-Justificación de la propuesta

En Costa Rica los delitos informáticos están en constante crecimiento, lo cual expone a grandes amenazas a todos los usuarios que utilicen sistemas de procesamiento de información en la red, específicamente usuarios de dispositivos móviles quienes en su gran mayoría constituyen el objetivo más perseguido por los ciberdelincuentes, por lo que el riesgo de que los datos se vean expuestos a daños o pérdidas irreparables es muy alto causando un impacto negativo para las víctimas de dispositivos móviles.

Mediante el análisis inicial sobre el uso y hábitos de los usuarios en dispositivos móviles Android (Encuesta), se logró confirmar la necesidad de implementar un Sistema de Gestión de Seguridad de la Información para brindar controles adecuados en el uso de dispositivos móviles, lo cual acarrea cambios importantes y el compromiso de todos los usuarios de estos.

La principal justificación de este proyecto de investigación es el aporte a través de la implementación, la concientización e importancia de la seguridad de la información; al ser implementadas permitirán mejorar la seguridad de la información en dispositivos móviles Android, asegurando cumplir los principios de la seguridad de la información: Disponibilidad, Integridad y Confidencialidad.

D-Desarrollo de la propuesta.

Para el desarrollo de la propuesta se dividieron

en 4 fases las cuales se presentan a continuación.

Fase l Diagnóstico

Nuestra población comprende a todas aquellas personas que sean usuarios activos de dispositivos móviles ubicadas en Costa Rica, que en 2021, según un estudio realizado por el INEC (Instituto de Estadística y Censo) 2000-2020 se estimó que Costa Rica tendría para el año 2021, una población de (5,163 038), en donde aproximadamente el 70% de la población (3.614.126) posee edades entre 15 a 64 años, quedando cerca del 30% de personas fuera del objetivo de la investigación (1.548.911) por lo que ésta población no es tomada en cuenta como objeto de estudio por considerarse como usuarios no activos de dispositivos móviles.

La Investigación centró su unidad de análisis en la población de Costa Rica que van entre los 15 y 65 años (3.614.126) concentrándose en este rango de edad la mayor cantidad de personas que utilizan un dispositivo móvil. A esta muestra se le asigna un nivel de confianza del 90% y un margen de error del 5% , por lo que una muestra representativa de la población en este proyecto es de entre 300-500 a la cual

INEC, Estimación de la Población para el año 2021.

CUADRO 1

Costa Rica: Población total por sexo, según años calendario 2011-2050

Año	Población		
	Total	Hombres	Mujeres
2018	5 003 402	2 523 072	2 480 330
2019	5 058 007	2 549 677	2 508 330
2020	5 111 238	2 575 550	2 535 688
2021	5 163 038	2 600 660	2 562 378

Fuente: INEC, 2021

se le realiza una encuesta para conocer hábitos de uso y posibles vicios de seguridad, se conformará una muestra probabilística, y de los datos obtenidos se tomaran decisiones para formular controles estratégicos de seguridad informática en el uso de dispositivos móviles, basados en la norma ISO 27001:2013.

"La muestra… es un conjunto de elementos seleccionados de una población de acuerdo a un plan de acción previamente establecido (muestreo), para obtener conclusiones que pueden ser extensivas hacia toda la población" (Salazar. C.P, Del Castillo .S, 2018, p.13).

En esta fase se procede a realizar la encuesta a un total de 304 usuarios con dispositivos móviles.

Primeramente se procede a realizar la encuesta a un total de 304 usuarios con dispositivos móviles, de los cuales el 79% afirmó utilizar un dispositivo móvil con sistema operativo Android, posteriormente realizada la encuesta a estos usuarios, se analizó cada una de las respuestas receptadas por los encuestados y se empezó con el proceso de tabulación. Notándose a través de los resultados que no existen controles adicionales para la seguridad de la información por parte del 58% de los encuestados, ya que, estos indican no utilizar ningún antivirus en sus móviles como medida alternativa referente a la seguridad de la información dentro de sus dispositivos, pero el 42% indicó si manejar un software adicional de detección para Software malicioso o malware.

Referente al entorno de red donde los usuarios gestionan la descargas de sus aplicaciones el 40% no establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados, ya que, descargan aplicaciones desde cualquier fuente desconocida sin realmente tener conciencia de la protección de las aplicaciones o los controles de Seguridad que estas puedan tener. Se considera que estos no establecen medidas de protección para transacciones Online ya que el 50% Utiliza usted redes inalámbricas públicas para conectarse a internet sin establecer acuerdos de confidencialidad antes de realizar intercambios de información en estas redes.

Se comprobó mediante las encuestas que la seguridad de los datos de los dispositivos móviles Android es vulnerable mediante la

utilización mensajería instantánea y redes sociales de los encuestados, debido a que el 55% lo utilizan con cierta frecuencia para realizar lo referente a sus operaciones diarias y compartir información sensible por medio de estos medios, lo que puede ocasionar acceso a la información de la sensible de estas a través de técnicas como Phishing y también se confirmó que dichos usuarios no saben reconocer el modo-programador cuando esta activo en sus dispositivos pudiendo ser la puerta para la perdida de información, por lo que estas vulnerabilidades son muy riesgosas y pueden ser aprovechadas por personas malintencionadas.

Fase 2 Preparación

Se desarrollan los objetivos específicos de la propuesta donde para el primer objetivo se realizan análisis de las posibles amenazas y vulnerabilidades en dispositivos móviles. Para el desarrollo de este objetivo se extrajeron de la norma ISO 27001:2013 los principales controles aplicables para cada respuesta de la encuesta en el cual serán analizadas según los controles actuales de la norma, esto revelará el nivel de adecuación de los controles en la gestión de la seguridad de la información de los dispositivos móviles Android.

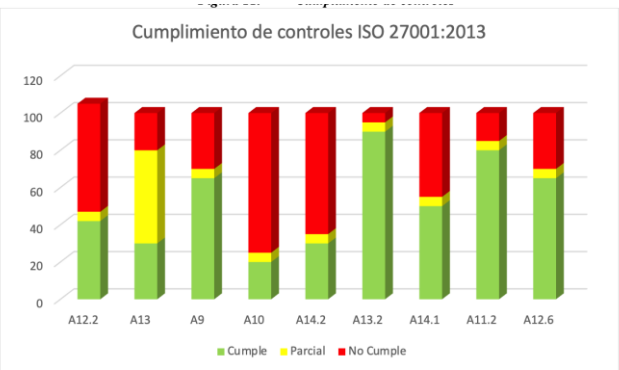
Siendo los usuarios con mayor incumplimiento de controles quienes no utilizan un antivirus en sus dispositivos, representando el 58% del total de encuestados, sumado que el 98% utiliza medios de mensajería instantánea para compartir información sensible en donde es muy común que estos datos sean capturados para cometer un ataque.

Con el propósito de evaluar el cumplimiento de cada pregunta del cuestionario, con base en evaluaciones parciales por grupos de controles, se presenta el siguiente gráfico, donde se podrá apreciar el nivel de adaptabilidad de los controles con respecto a la realidad de uso de los encuestados su estado actual y cuales controles son necesarios cumplir según la norma ISO 27001:2013.

Dentro del segundo objetivo esta el evaluar el crecimiento de la inseguridad informática en Costa Rica, mediante los controles establecidos en la norma ISO 27001:2013, examinando las vulnerabilidades en dispositivos móviles Android en el 2021. Por lo tanto, para el desarrollo de este objetivo se tomó la norma en la que se catalogaron los controles que aplican a las vulnerabilidades identificadas. Con respecto a las vulnerabilidades identificadas en el incumplimiento de ciertos controles, se presenta la siguiente desglose de controles donde se realizará un análisis para determinar los objetivos de control requeridos para mitigar posibles amenazas siguiendo las recomendaciones de la norma. Se detalla a continuación los controles mas importantes a ser implementados ya que son estos los que mayores deficiencias presentaron según el resultado de los encuestados y hacia donde se debe presentar mayor atención y de los cuales representarían un dato muy importante para aplicar el estudio de riesgos.

Figura 1 *Cumplimiento de controles ISO*

A.12.2 Protección contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia



Fuente: Elaboración propia, 2021

apropiada de los usuarios, para proteger contra códigos maliciosos. debido al gran numero de usuarios que no utilizan antivirus en sus dispositivos.

A13. Seguridad en las Comunicaciones. Se debe proteger adecuadamente la información incluida en la mensajería electrónica. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. al utilizar herramientas de mensajería electrónica para la transferencia de datos.

A9. Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. se recomienda establecer el doble factor de autenticación de los dispositivos móviles.

A10. Criptografía. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información, por ejemplo gestión de contraseñas seguras de mas de 10 caracteres.

A.14 Adquisición, desarrollo y mantenimiento de sistemas. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización, esto por cuanto el 71% de los encuestados desconocen el modo-programador de los dispositivos móviles, esto al estar activado dota al ciber atacante de privilegios total para el acceso y modificación del dispositivo.

Para el objetivo tres se diseña una propuesta metodológica de las vulnerabilidades en dispositivos móviles Android, mediante los controles de la norma ISO 27001:2013, facilitando la comprensión de los riesgos en dispositivos móviles en Costa Rica en el 2021. Para el desarrollo de este objetivo, se toma la norma y se clasifican los riesgos en los activos relacionados a la seguridad de la información por medio la metodología Magerit se identifican las principales amenazas de acuerdo a las vulnerabilidades identificadas y se aplican los controles correspondientes.

Los grupos de interés o partes interesadas pueden ser usuarios con dispositivos móviles con sistema operativo Android como también usuarios de otros fabricantes (sociedad en general) ya que es de interés general contar con controles en función de la seguridad de la información.

En esta fase se conoce un poco sobre el entorno en el que los usuarios y dispositivos móviles son utilizados en función de garantizar la seguridad de la información que es el objeto de estudio. En promedio En la actualidad, existen 5.270 millones de usuarios únicos de teléfonos móviles en el mundo. El número total de usuarios móviles únicos en todo el mundo creció en 97 millones en los últimos 12 meses. Según los últimos datos de GSMA Intelligence.

Como se puede observar en la página de DataReportal para su revista “Digital Around the Word” de los dispositivo conectados a internet para abril 2021, representan un 92,8% de conexión a internet, estos por su versatilidad y facilidad de uso se han convertido para las personas en el centro de operaciones bancarias, entretenimiento, comunicación, compras, etc. Significando más de dos terceras partes de la población utilizando su dispositivo móvil en internet. Por esta razón, es que gestionar tanto los riesgos como la seguridad en los dispositivos móviles se vuelve tan necesario. Fuente: https://datareportal.com/global-digital-overview.

El primer paso es identificar los activos de información en el entorno de la seguridad de la información para el procesamiento de datos en

los dispositivos móviles con sistema operativo Android, analizar los datos recopilados y posteriormente realizar un catalogo de activos. Es importante señalar que para estructurar estos activos se decidió utilizar la metodología MAGERIT. Por lo tanto, los grupos son los siguientes:

E-Catálogo de activos:

Nombre del activo: [D] Datos/Información

Descripción: Toda la información guardada en el dispositivo Móvil

Clasificación de activos: [files] ficheros, [backup] copias de respaldo, [conf] datos de configuración, [int] datos de gestión interna, [password] credenciales (ej. contraseñas), [auth] datos de validación de credenciales, [acl] datos de control de acceso
[log] registro de actividad, [source] código fuente, [exe] código ejecutable, [test] datos de prueba.

Nombre del activo: [SW] Software

Descripción: Todos los programas y aplicaciones que se encuentran instalados en el dispositivo móvil y que realizan el procesamiento de la información. Como sistema operativo, herramientas de procesamiento de texto, envío de mensajes, redes sociales etc.

Clasificación de activos: [browser] navegador web [www] servidor de presentación, [app] servidor de aplicaciones, [email_client] cliente de correo electrónico, [file] servidor de ficheros [dbms] sistema de gestión de bases de datos, [office] ofimática, [av] antivirus, [os] sistema operativo [backup] sistema de backup

Nombre del activo: [HW] Hardware

Descripción: Dispositivo que permite el procesamiento de la información (datos, aplicaciones y servicios).

Clasificación de activos: [Mobile] informática móvil

Nombre del activo: [COM] Redes wifi

Descripción: Equipos de telecomunicaciones que permiten el intercambio de información e interconectar dispositivos móviles y computadoras

Clasificación de activos: PSTN] red telefónica, [X25] X25 (red de datos), [wifi] red inalámbrica, [Mobile] telefonía móvil [sat] por satélite, [Internet] Internet.

Nombre del activo: [P] Personal

Descripción: Son todos los usuarios de dispositivos móviles Android que explotan todos los elementos anteriormente citados.

Clasificación de activos: responsable del dispositivo móvil.

Terceras personas que utilizan estos dispositivos móviles.

Nombre del activo: [keys] Claves criptográficas

Descripción: Son las llaves criptográficas que permiten autenticar las partes.

Clasificación de activos: info] protección de la información,

[encrypt] claves de cifra, [shared_secret] secreto compartido, (clave simétrica) (Por ejemplo, DES, 3-DES, AES, etc.), [public_encryption] clave pública de cifra (Por ejemplo, RSA, Diffie-Hellman, curvas elípticas, etc.).

[public_decryption] clave privada de descifrado (2) [sign] claves de firma [shared_secret] secreto compartido (clave simétrica) [public_signature] clave.

Fase 3 Planificación

Una vez que los activos de información han sido Identificados se realiza su valoración, esto para identificar que tan crítico resultaría el impacto que representaría una posible materialización de amenazas como, intrusión del dispositivo, exposición de la información confidencial, robo de información o suplantación de identidad por mencionar algunas.

Criterios de evaluación de los activos

[Crítico] Una falla en este activo representaría un impacto crítico para el usuario.

[Alto] Una falla de este activo afectaría por un periodo de tiempo al usuario.

[Medio] Una falla de este activo tiene una importancia media para el usuario.

[Bajo] Una falla de este activo afecta en menor grado al usuario.

[Muy Bajo] Una falla de este activo es imperceptible para el usuario.

Criterio de evaluación del impacto de ocurrencia de una amenaza.

Para un usuario de dispositivo móvil Android, la ejecución de una amenaza en su dispositivo podría representar un riesgo para su información confidencial como por ejemplo intrusión del dispositivo por ciberdelincuentes, daños físicos del dispositivo o robo de este. Por lo que son distintas las amenazas a los que están expuestos los usuarios de dispositivos móviles. El criterio de evaluación del impacto de una amenaza es el siguiente:

[5] Muy alto| [4] Alto| [3] Medio| [2] Bajo| [1] Muy Bajo

Criterio de evaluación de la probabilidad de ocurrencia de una amenaza.

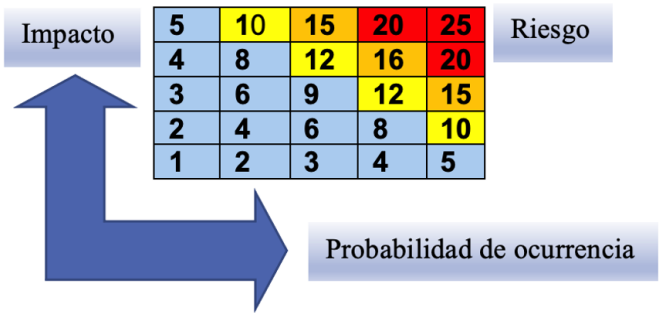
Posteriormente, se realiza lo que es la probabilidad de ocurrencia en que una amenaza podría materializarse. A continuación se presenta una tabla con el criterio de probabilidad de que una amenaza se materialice y afecte las actividades los usuarios de dispositivos móviles Android.

[5] Muy alta/Mas de una vez al mes | [4] Probable/Una vez cada mes | [3] Posible/Una vez cada [3] meses | [2] Muy poco probable/Una vez cada 6 meses | [1] muy rara vez/Una vez cada año

Realización de la matriz de riesgo.

Una vez realizado la tabla de criterios de evaluación de probabilidad de que se materialice una amenaza representando un impacto en la seguridad de la información, se procederá a realizar la matriz de riesgo para calcular el riesgo que dicha amenaza representa si se llegara a materializar.

Figura 2 *Criterios de evaluación de riesgos*



Fuente: Magerit, 2018

Posteriormente a la matriz de riesgo se deberán calificar los riesgos y se abordará cada uno con referencia a la siguiente tabla.

Según Magerit 2018, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (p.7).

Tabla 1 *Valoración del riesgo*

Criticidad	Descripción
Crítico	Se requiere atención inmediata
Alto	Se requiere atención
Medio	Pueda ser objeto de estudio para su tratamiento
Bajo	No se requieren acciones

Fuente: *Magerit, 2018*

Valoración de los activos.

Al ser identificado cada activo de información, se procede a darle un valor, un grado de importancia y si es vulnerado que tan critico, perjudicial o que tanta afectación representa para la seguridad de la información en

dispositivos móviles. Magerit 2018, se refiere a estas características como "atributos que hacen valioso un activo".(p.15).

Resultados relevantes de la valoración de activos.

Atributos de valoración [D] Disponibilidad| [I] Integridad de los datos| [C] Confidencialidad de la información después de la valoración de activos según la criticidad de cada uno representan una valoración alta correspondientes a los tres atributos: Copias de respaldo, Contraseñas, Datos de control de acceso, Dispositivo Móvil y el personal.

Identificación de amenazas y vulnerabilidades.

Una vez realizada la valoración de los activos para identificar las posibles amenazas en la seguridad de la información de los dispositivos móviles Android, se procede a estimar que tan vulnerable es el activo si se llegara a materializar una amenaza, así como, un análisis de la frecuencia con la que podría ocurrir dicha amenaza. La clasificación de las amenazas se realiza de acuerdo al catálogo de amenazas sugeridas por la metodología MAGERIT.

[N] Desastres Naturales

[I] Origen Industrial

[E] Errores y fallos no intencionados

[A] Ataques Intencionados

[Datos] Los datos se exponen a fallos no intencionados, manipulación de registro de los datos, interceptación, modificación deliberada y divulgación de los datos de información.

[Redes] El activo Redes se expone a ataques intencionados con y análisis del tráfico de red.

[Software] El activo Software se expone a fallos no intencionados, difusión de software dañino y vulnerabilidades de los programas

[Hardware] El activo Hardware se expone a desastres naturales, daños por agua, avería de origen físico o lógico, fallos no intencionados, errores de mantenimiento / actualización de equipos, robo, ataque destructivo,

[Personal] El activo personal se expone a errores de los usuarios, errores de configuración, manipulación de la configuración, suplantación de la identidad del usuario, abuso de privilegios de acceso, ingeniería social.

[Criptografía] El activo Criptografía se expone a ataques intencionados y acceso no autorizado.

Realizada la enumeración de las amenazas para cada activo, se procede a realizar el análisis del riesgo de cada activo en función a sus vulnerabilidades y amenazas identificadas anteriormente.

Evaluación de activos con riesgo crítico.

[Datos] Destrucción de la información. [25], Alteración accidental de la información. [20], Fugas de información. [20].

[Redes] Interceptación de información (escucha) [25] y Ataques informáticos [20].

[Software] Suplantación de identidad del usuario [20], Difusión de software dañino [25], Vulnerabilidades de los programas [20].

[Hardware] Avería de origen físico y lógico [25]

[Personal] Suplantación de identidad del usuario [25], Divulgación de información [20] y Suplantación de identidad [25].

[Criptografía] Abuso de privilegios de acceso [25] y Acceso no autorizado [20]

Una vez obtenido el resultado de riesgos se procede a gestionar el riesgo residual de los activos de información seleccionados para la respectiva valoración de riesgos, para lo cual en la siguiente tabla se establece el tratamiento de los riesgos según su nivel de criticidad.

Descripción	Riesgo	Tratamiento
Acceso no autorizado	Riesgo Alto	Prevenir el riesgo

Abuso de privilegios de acceso	Riesgo Alto	Prevenir el riesgo
Ataques informáticos	Riesgo Medio	Disminuir el riesgo
Destrucción de la información	Riesgo Alto	Prevenir el riesgo
Fugas de información	Riesgo Medio	Disminuir el riesgo
Divulgación de información	Riesgo Medio	Disminuir el riesgo
Suplantación de identidad del usuario	Riesgo Alto	Prevenir el riesgo
Difusión de software dañino	Riesgo Medio	Disminuir el riesgo
Vulnerabilidades de los programas	Riesgo Medio	Disminuir el riesgo
Alteración accidental de la información	Riesgo Medio	Disminuir el riesgo
Interceptación de información (escucha)	Riesgo Bajo	Reducir el riesgo
Avería de origen físico y lógico	Riesgo Bajo	Reducir el riesgo

III. Conclusiones

Al finalizar las diferentes etapas que demandó esta investigación, donde se recopiló información, la cual, fue analizada, evaluada por diferentes metodologías y llevada a pruebas que nos arrojaron diferentes resultados, se concluye que si se cumplió con los objetivos propuestos donde se determinan las siguientes conclusiones.

El tema de investigación sobre el sistema operativo Android es muy amplio, abarca temas de seguridad, en hardware o software, actualizaciones, temas de vulnerabilidades, amenazas, también temáticas sobre la superficie de ataque en Android en dispositivos root y no root los cuales son diferentes aristas para atacar o encontrar una solución al problema.

Para el objetivo especifico 1 Analizar las vulnerabilidades en dispositivos móviles Android, mediante parámetros medibles, estableciendo controles de la norma ISO 27001:2013 en Costa Rica. Se concluye que: de las 6 subclases de la NIST SP 800-163 identificadas se relacionan 4 de ellas y de los 114 sub-controles de la norma ISO/IEC 27001, 19 tienen relación con el problema de las vulnerabilidades identificadas en la investigación.

En cuanto a las pruebas realizadas al dispositivo móvil con Sistema Operativo Android versión 6.0.1 Marshmallow, los resultados fueron positivos, conforme se comprobó que es posible aplicar los objetivos de control de la norma ISO 27001:2013 a través del mismo sistema operativo, mitigando el riesgo de pérdida de datos.

Para el objetivo especifico 2 Evaluar el crecimiento de la inseguridad informática en Costa Rica, mediante los controles establecidos en la norma ISO 27001:2013, examinando las vulnerabilidades en dispositivos móviles Android en el 2021. Se concluyó que: El análisis realizado a los 14 controles de la norma ISO 27001:2013, 6 están directamente alineados a los problemas de seguridad en dispositivos móviles hallados en la investigación, favoreciendo en cuanto a la mitigación de estos al tener los controles pertinentes para su tratamiento a nivel global.

Para el objetivo especifico 3 Diseñar una propuesta metodológica de las vulnerabilidades en dispositivos móviles Android, mediante los controles de la norma ISO 27001:2013, facilitando la comprensión de los riesgos en dispositivos móviles en Costa Rica en el 2021. Se concluyó que: Según el control A.9.3 del anexo a de la norma ISO 27001:2013 sobre responsabilidades del

usuario el cual esta constituido por el sub-control A.9.3.1 sobre responsabilidades del usuario en el manejo de los datos, y esto esta alineado con la principal causa de problemas de seguridad de la información, el usuario, siendo este el eslabón mas débil de la cadena en la seguridad de la información. 14 anexos a de la norma ISO 27001:2013, 7 están alineados a los resultados de la encuesta.

Analizado los datos obtenidos del portal The Ultimate Security Vulnerability datasource (CVE Details), que diariamente actualiza la página basada en las fuentes NVD (National Vulnerability Database) situado en Estados Unidos De América, se comprobó que para el año 2021, Overflow, Execute Code y Bypass Something, son los tipos de vulnerabilidades más frecuente en el sistema operativo de Android.

Sin importar la cantidad de controles que fueron señalados de la norma que deben existir, el usuario de dispositivos móviles debe tener hábitos de buenas prácticas, de lo contrario éste será siempre la vulnerabilidad mas atacada, ya que los Smartphones con sistema operativo Android puede sufrir daños tanto físicos o remotos con o sin internet solamente con el descuido del usuario.

IV. Recomendaciones

Se recomienda a los usuarios con dispositivos Android, tener presente siempre la actualización de sus aplicaciones móviles y del sistema operativo para impedir que se presenten vulnerabilidades por falta de actualizaciones.

Se recomienda el uso de aplicaciones libres pero sobre todo de pago ya que de las primeras se podrían realizar explotaciones de un mayor numero de vulnerabilidades.

Generar concientización de la población en temas de amenazas y vulnerabilidades en dispositivos móviles con sistemas operativo Android por medio de la creación de campañas informativas.

Se recomienda abordar mas ampliamente la temática de la programación de aplicaciones y sistemas operativos móviles en donde mediante de pruebas guiadas por metodologías de desarrollo seguro se empiecen a ver resultados de aplicaciones móviles o software mas robustas y confiables.

Se recomienda a los usuarios finales realizar siempre un análisis mas detallado del tipo de información que están compartiendo en sus dispositivos móviles y en redes sociales donde podrían verse vulnerados con mucha facilidad a causa de un descuido o revelar información sensible.

Se recomienda a los especialistas en seguridad de la información compartir mas de nuestros saberes en esta temática a toda la población en un momento critico en el que la seguridad informática es tan requerida en un mundo donde todos los días salen amenazas nuevas y cada vez mas sofisticadas con mayores niveles de daños realizados a los usuarios.

V. Referencias

Canalys (2021), Global Smartphone Market, EEUU, tomado de: https://www.canalys.com/newsroom/canalys-worldwide-smartphone-market-Q1-2021

Check Point Software Technologies Ltd., (2021), Informe de Seguridad Móvil 2021. tomado de: https://www.checkpoint.com/

Herrera. C y Giovanny. A (2017), [Tesis de maestría] Riesgos de seguridad asociados al uso de dispositivos móviles personales, Universidad Internacional de la Rioja, Colombia.

EALDE Business School, (2021), Amenazas de seguridad informática en dispositivos móviles, Madrid, España, Tomado de: https://www.ealde.es/seguridad-dispositivos-moviles/

Fortinet, (2021), informe "El estado de la tecnología operativa y la ciberseguridad" tomado de: https://www.fortinet.com/

Jori Hamilton, (2021), artículo "Seguridad de los dispositivos móviles: Preocupaciones y soluciones para 2021 y más adelante", EEUU.
Tomado de: https://www.globalsign.com/es/blog/mobile-device-security-concerns-and-solutions

Rojas Valduciel, H. (2016). Seguridad de la Información, Seguridad Informática y Ciberseguridad:¿Son sinónimos? Recuperado de: file:///Users/macrt/Downloads/420-1655-2-