UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

“PROPUESTA DE ELABORACIÓN DEL MANUAL DE PROCEDIMIENTOS EN EL PROCESO DE EVALUACIÓN DE SEGURIDAD EN UNA APLICACIÓN MÓVIL ANDROID BASADO EN LA METODOLOGÍA OWASP PARA LA EMPRESA ENTELGY 2020”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

TAYPE IGNACIO, LUIS ALDO

Villa El Salvador
2020

DEDICATORIA

Este proyecto lo dedico principalmente a DIOS porque él es creador de todo y permite que las cosas sucedan.

A mis padres que me han apoyado e influenciado en mi vida, guiándome y haciéndome una mejor persona de bien.

A mis hermanos por apoyarme en los momentos difíciles.

AGRADECIMIENTO

Primeramente, agradezco a la Universidad UNTELS por haberme aceptado y abierto las puertas para estudiar mi carrera y haberme brindando la oportunidad de titularme.

Agradezco a los diferentes maestros que han sido una fuente de sabiduría que me orientaron y guiaron para ser un excelente profesional.

Agradezco también a mi asesor por el tiempo, dedicación y paciencia para guiarme en el desarrollo de este trabajo de investigación.

Y para finalizar, agradezco a todos mis compañeros de clase durante todos los ciclos de Universidad ya que gracias al compañerismo, amistad y apoyo diario han aportado en mis ganas de seguir adelante en mi carrera profesional.

INDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

El desarrollo del presente trabajo propone un manual de procedimientos en el proceso de evaluación de seguridad en una aplicación móvil Android basado en la metodología de OWASP, para el uso del consultor de pentesting de la empresa ENTELGY, el trabajo tiene por objetivo determinar el nivel de seguridad de las aplicaciones móviles identificando potenciales vulnerabilidades que este se encuentre afectado y mitigar el riesgo asociado en caso sea explotada.

En el presente trabajo se estudiaron diferentes metodologías que estén basados en análisis de riesgos, complementando con la documentación oficial de OWASP y las técnicas de trabajo que se emplean en la empresa ENTELGY.

En el primer capítulo se elaboró el marco teórico que será utilizado para el entendimiento del trabajo de investigación. Esto incluye al sistema operativo Android y las aplicaciones móviles, así como sus tipos, las metodologías de análisis de riesgos, además de mencionar a la documentación oficial de OWASP respecto a seguridad de aplicaciones móviles, y así como también la definición de términos que se emplean en este trabajo de investigación.

En el segundo capítulo definimos las principales leyes y normativas que aplican a las políticas de información con el fin de establecer las pautas que aportan para el desarrollo del trabajo de investigación.

En el tercer capítulo se presentó la metodología de desarrollo del trabajo de investigación donde definimos la delimitación, la determinación y análisis del problema en que está enfocado el trabajo, el modelo de solución donde desarrollamos el diseño de la metodología y para concluir se mencionar los resultados de la investigación que se propuso en los objetivos del trabajo de investigación.

Finalmente se presentaron las conclusiones del trabajo y las recomendaciones a ser consideradas para investigaciones similares.

INTRODUCCIÓN

En la actualidad muchas organizaciones han lanzado al mercado aplicaciones que les permite a sus usuarios manejar información desde sus dispositivos móviles y tables de una manera más fácil y desde la comodidad de su hogar, sin embargo, existen muchas dudas sobre cómo se gestiona la seguridad en sus aplicaciones móviles. Los usuarios pueden bajar la aplicación a su dispositivo móvil a través de las tiendas desde las diferentes plataformas disponibles el cual les permiten manejar información financiera, contables, administrativos, incluso de uso general o cualquier dato importante y sensible.

Muchos de los usuarios desconocen y no tienen ni la remota idea de cómo estas aplicaciones hacen uso de su información personal. A eso se puede adicional los riesgos que puede presentar de como las aplicaciones han sido desarrollados durante su etapa programación y si estas han sido validadas y controlados correctamente, los cuales de no ser así podría significar que los usuarios podrían estar expuestos a ataques e incluso ser víctimas de robo de información, extorción, fraudes y otros delitos informáticos presentes dirigido por potenciales atacantes que se aprovechan de estas fallas de seguridad que contienen las aplicaciones móviles utilizadas a diario.

La seguridad de una aplicación móvil se presenta desde el momento que un usuario ingresa a la aplicación y este puede sufrir robo de identidad

o perdidas de datos valiosos y sensibles que puede ser reutilizado por un atacante para planificar un vector de ataque con fines delictivos o simplemente de diversión.

Este trabajo tiene como objetivo propones una manual de procedimientos para el proceso de evaluación en una aplicación móvil en plataforma Android basado en una metodología estándar aceptado a nivel mundial para lograr aplicaciones móviles más seguras y para que estas no puedan convertirse en blanco de ataques si no son protegidas correctamente. Es por eso por lo que hoy en día las empresas se ven en la necesidad de poner a prueba sus aplicaciones móviles, para descubrir posibles debilidades en seguridad y así ellos mismos corregirlos antes que sean víctimas de algún incidente que pueda perjudicar a la organización. Es por ello que las empresas se ven obligados de solicitar servicios de hacking ético para evaluar el nivel de seguridad de sus aplicaciones móviles, los cuales son brindados por especialistas en seguridad, para testear la aplicación.

Para ello los especialistas se basan en metodologías estándar ya establecidas que los guíen como evaluar de acuerdo con el tipo de escenario que estos presenten y le ofrezcan resultados más exactos.

OBJETIVOS

a. General

Proponer un manual de procedimientos para el proceso de evaluación de seguridad en una aplicación móvil Android basado en la metodología de OWASP Mobile Security Project., que permita seleccionar los requisitos de seguridad de aplicaciones móviles para los clientes de la empresa ENTELGY 2020.

b. Específicos

- Identificar la situación actual de la empresa ENTELGY, con respecto a la evaluación de seguridad de aplicaciones móviles Android de sus clientes.
- Describir el procedimiento de evaluación de seguridad en una aplicación móvil Android, según la estructura de la metodología propuesta.
- Elaborar el manual de procedimientos con los lineamientos para evaluar la seguridad en una aplicación móvil para plataformas Android, tomando como base la documentación de OWASP Mobile Security Project.

CAPÍTULO I: MARCO TEORICO

1.1. BASES TEÓRICAS

1.1.1. SISTEMA OPERATIVO ANDROID

Según (David, 2016) define a, “Android como un sistema operativo multidispositivo, inicialmente diseñado para teléfonos móviles. En la actualidad se puede encontrar también en múltiples dispositivos, como ordenadores, tabletas, GPS, televisores, discos duros multimedia, miniordenadores, cámaras de fotos, etcétera. Incluso se ha instalado en microondas y lavadoras. Está basado en Linux, que es un núcleo de sistema operativo libre, gratuito y multiplataforma”.

Según la (IDC, 2020), actualmente los sistemas Android y iOS comprenden más del 99% de la cuota del mercado de los sistemas operativos móviles.

1.1.2. APLICACIONES MÓVILES

Según (Gonzales, 2014), define a una aplicación móvil o app como un software diseñado para funcionar en teléfonos inteligentes y otros dispositivos móviles.

Existen varias formas en que se desarrollan una aplicación móvil. Según (Cuello & Vittote, 2013), las formas las formas de desarrollar una aplicación móvil son las siguientes:

A) Aplicación nativa:

Las aplicaciones nativas son desarrolladas específicamente para un sistema operativo móvil en concreto como Android o iOS, a partir del SDK (Software Development Kit) que estos proporcionan para su desarrollo. Este tipo de aplicaciones están integradas al teléfono que les permiten usar todas las características del hardware del dispositivo, como la cámara y los sensores (Cuello & Vittote, 2013) .

B) La aplicación web:

Las aplicaciones web son básicamente páginas web optimizadas para trabajar en un dispositivo móvil de manera que aparentemente se vean como una app nativa. Están basadas en HTML, JavaScript y CSS. No se emplea el SDK, por lo tanto, se puede programar de manera independiente al sistema operativo. Estas aplicaciones no requieren instalarse en el dispositivo, ya que solo necesitan de un navegador para poder visualizarse como un sitio web normal. Tienen algunas restricciones, ya que no permite aprovechar al máximo los componentes del hardware del teléfono (Cuello & Vittote, 2013).

C) Aplicación hibrida:

Las aplicaciones hibridas se ejecutan como una aplicación nativa, aunque sobre un navegador web embebido, llamado webview, es como una combinación entre las dos anteriores. Se suelen desarrollar en los lenguajes comunes de aplicaciones web, como HTML, CSS y JavaScript,

por lo que se pueden utilizar en las diferentes plataformas existentes; su interfaz de usuario por tanto será igualmente genérica y no estéticamente similar al del resto de aplicaciones de cada plataforma en concreto. Permiten el acceso a las capacidades del teléfono como si fueran aplicaciones nativas (Cuello & Vittote, 2013).

1.1.3. SEGURIDAD INFORMÁTICA

Es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

Según (Mifsud, 2012) “La seguridad informática consiste en la implantación de un conjunto de técnicas con el fin de preservar la confidencialidad, la integridad y la disponibilidad de información.

1.1.4. SEGURIDAD DE LA INFORMACIÓN:

Según (Godoy Lemus, 2014), "La seguridad de información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma".

1.1.5. ANÁLISIS DE RIESGO

Como se mencionó anteriormente, la Seguridad Informática consiste en proteger la información contra amenazas, minimizando los riesgos. Para cualquier organización es necesario conocer cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades (Gutierrez Amaya, 2012). Esto permite a las organizaciones establecer las medidas preventivas y correctivas para mejorar su seguridad, asignando de manera óptima sus recursos.

Existen diferentes metodologías para realizar análisis y gestión de riesgos. Algunas de ellas son:

A) ISO 31000:2018. Lineamientos para la Gestión de Riesgos:

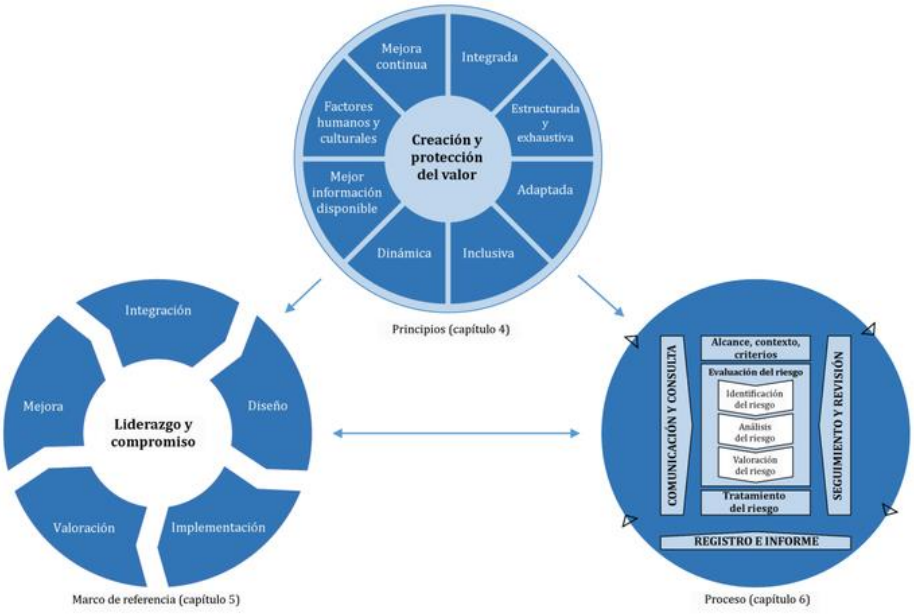
En esta guía, la gestión de riesgos se basa en principios, un marco y un proceso, los cuales están definidos en el mismo documento. El proceso de gestión de riesgos se compone de las siguientes etapas:

- Alcance, Contexto y Criterios.
- Valoración de Riesgos.

- Tratamiento de Riesgos.
- Comunicación y Consulta.
- Monitoreo y Revisión.
- Registro y Reporte.

Según la (ISO, 2018). El proceso, y su relación con los principios y el marco, se muestran de forma gráfica en la Figura No. 1.

Figura 1: Principios, Marco y Proceso de ISO 31000:2018



Fuente: ISO 31000:2018 - https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

B) ISO 27005:2011. Gestión de Riesgos de Seguridad de la Información:

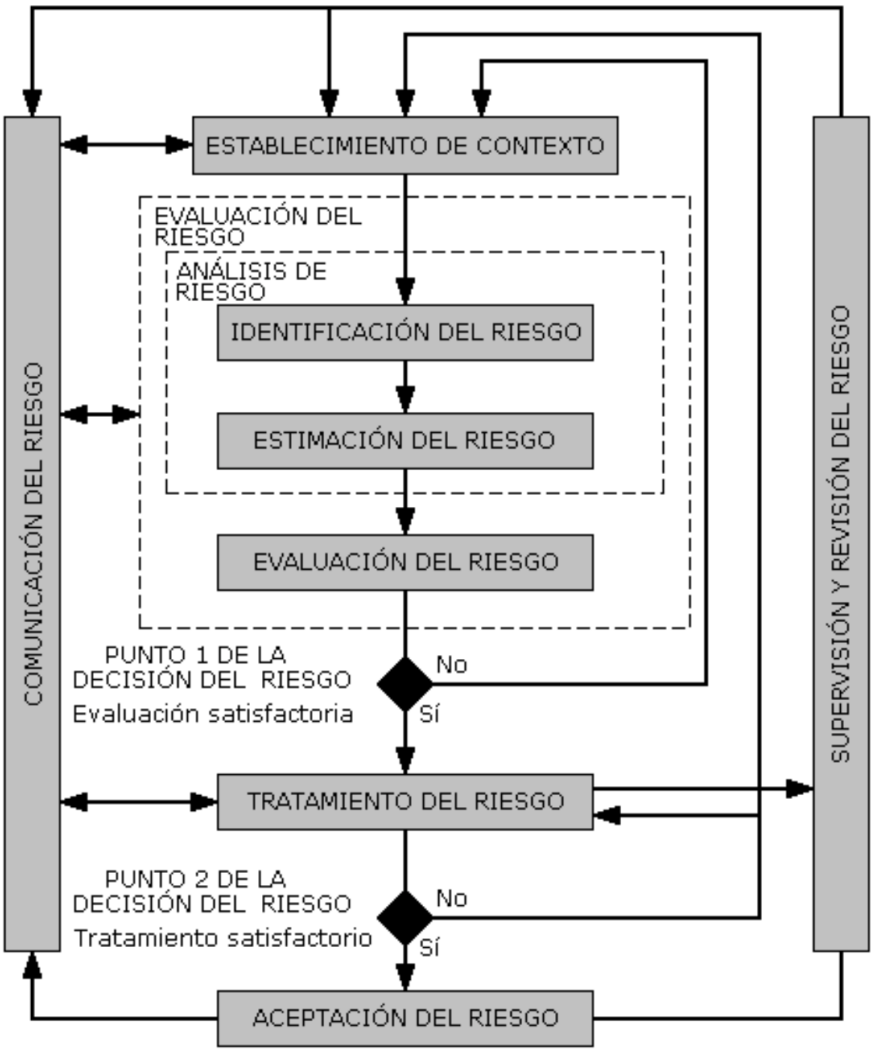
Esta norma cuenta con 7 pasos:

- Establecimiento del contexto.
- Identificación del riesgo.
- Estimación del riesgo.

- Evaluación del riesgo.
- Tratamiento del riesgo.
- Aceptación del riesgo.
- Comunicación del riesgo

Según (Espinosa T., Martínez P., & Amador D., 2014). Dichos pasos se muestran organizados de forma gráfica en la Figura No. 2.

Figura 2: Proceso de Gestión de Riesgos



Fuente: ISO 27005

C) AS/NZS ISO 31000:2009. Principios y lineamientos para la gestión de riesgos:

Consta de las siguientes fases:

- Establecer el contexto.
- Valoración del riesgo.
- Tratamiento del riesgo.
- Comunicación y Consulta.
- Monitoreo y Revisión.

Como se puede observar la similitud en las etapas que tienen ambos estándares. Por lo tanto, se podrá establecer las etapas que se incluirían en el trabajo propuesto. Están etapas se explican en forma general:

1.1.5.1. Establecimiento de contexto

El establecimiento de contexto es la fase inicial de un análisis de riesgos. Durante esta fase, se planifica la gestión de riesgos y se identifican aquellos elementos externos e internos que pueden afectar al negocio. De acuerdo con (Lizarzaburu, Barriga, Noriega, Luciano, & Mejia, 2017) en su marco de revisión ISO 31000, el establecimiento del contexto se resume en las siguientes actividades:

- Definición de objetivos y metas de las actividades.
- Definición de métodos utilizados en la evaluación de riesgos.
- Concretar la forma y el rendimiento cómo se evaluará el nivel de eficacia en la gestión de riesgo.

- Establecer responsables en el proceso de gestión de riesgo.
- Reconocer la relación con otros posibles proyectos.

1.1.5.2. **Evaluación de riesgos**

La evaluación de riesgos, en muchas de las metodologías mencionadas, se comprende en sub-fases:

- Identificación de riesgos.
- Análisis de riesgos.
- Evaluación de riesgos

(Lizarzaburu, Barriga, Noriega, Luciano, & Mejia, 2017), mencionan que en esta etapa se determinan qué riesgos se deben tratar y priorizar, basando las decisiones de tratamiento en políticas, normas y otros reglamentos definidos en la organización. Esta etapa ayuda a establecer la prioridad de los riesgos a ser tratados, y cómo serán tratados, con base en los niveles de riesgos obtenidos en la anterior etapa.

1.1.5.3. **Tratamiento de riesgos**

Según (Lizarzaburu, Barriga, Noriega, Luciano, & Mejia, 2017), existen cinco opciones para tratar los riesgos, las cuales son:

- Prevenir el riesgo.
- Aceptar el riesgo
- Quitar las fuentes del riesgo.
- Cambiar las posibilidades de ocurrencia.

- Aceptar el riesgo conjunto (con otras partes).

1.1.6. EVALUACIÓN DE SEGURIDAD DE APLICACIONES

Según RAE (2017), evaluar es “señalar el valor de algo”. Para el contexto de la presente investigación, se necesita señalar el valor de la seguridad de las aplicaciones móviles, para lo cual se deben establecer métricas que permitan comparar y medir resultados.

“Para proveer datos significativos, las métricas de seguridad de la información cuantificables deben estar basadas en metas y objetivos de desempeño de la seguridad de la información, y ser fáciles de obtener y factibles de medir” (NIST, 2008). Existen diferentes metas y objetivos de seguridad de la información para cada empresa, y para ello existen distintas formas de evaluar la seguridad.

Según (Mendoza, 2015), los siguientes métodos pueden utilizarse para evaluar la seguridad de la información dentro de una organización: Análisis de brechas (Gap Analysis), Evaluaciones de Vulnerabilidades y Pruebas de Penetración. Mendoza también menciona que los Modelos de Madurez son una herramienta útil para tener criterios objetivos al evaluar la seguridad.

A) Análisis de brechas (Gap Analysis):

Es un estudio preliminar que permite conocer la forma en la que se desempeña una organización en materia de seguridad de la información, con relación a las mejores prácticas reconocidas en la industria” (ISOTools Excellence, 2017). Un análisis de brechas es una herramienta que permite a las empresas conocer la diferencia existente entre el nivel

de seguridad actualmente implementado y el nivel de seguridad que se desea alcanzar, generalmente con criterios basados en normas y estándares de seguridad de la información.

B) La prueba de intrusión, test de penetración, o hacking ético:

Es un procedimiento que se realiza utilizando un conjunto de técnicas y métodos que simulan el ataque a un sistema. Los resultados de esta prueba permiten evaluar el nivel de seguridad de un sistema informático, red, o aplicación (Ramos Ramos, 2013). Este tipo de prueba permite evaluar el sistema, red o aplicación desde la perspectiva de un atacante malicioso, lo cual ayuda a sugerir mejoras para fortalecer la seguridad informática al descubrir y explotar los puntos débiles que pueden ser aprovechados para ocasionar daños al sistema.

Existen metodologías para evaluar la seguridad de la información de las empresas, en las cuales se definen los pasos a seguir durante todo el proceso. Algunas de ellas son:

A) OSSTMM (The Open Source Security Testing Methodology Manual):

Este manual es adaptable para casi cualquier tipo de auditoría, incluyendo test de penetración, hacking ético, evaluaciones de seguridad, evaluación de vulnerabilidades, equipo rojo, equipo azul, y otros" (Herzog, 2010). En este manual, (Herzog, 2010) describe 7 pasos para definir una evaluación de seguridad, los cuales son: 1) Definir los activos que se quieren proteger, con el fin de evaluar los controles que

los protegen para identificar sus limitaciones (Herzog, 2010). 2) Identificar el área alrededor de los activos que incluye mecanismos de protección y los procesos o servicios alrededor, donde toma lugar la interacción con los activos, llamado zona de compromiso (Herzog, 2010), 3) Definir todo lo que se encuentra fuera de la zona de compromiso que sea necesario para mantener los activos operativos. A esto se le llama alcance de la evaluación (Herzog, 2010). 4) Definir cómo el alcance interactúa consigo mismo y con el exterior. Estos son los vectores. Idealmente cada vector debería ser una evaluación separada (Herzog, 2010). 5) Identificar los equipos necesarios para cada prueba. Debido a que las interacciones pueden ocurrir en varios niveles, se las ha clasificado por función como cinco canales (humano, físico, inalámbrico, telecomunicaciones, y redes de datos) (Herzog, 2010). 6) Determinar la información que se quiere recolectar de la evaluación. Esto define el tipo de evaluación (blind, double blind, gray box, double gray box, tandem y reversal) (Herzog, 2010). 7) Asegurarse de que la evaluación de seguridad definida cumple con las reglas de compromiso, para evitar malentendidos, conceptos erróneos o falsas expectativas (Herzog, 2010).

B) PTES (Penetration Testing Execution Standard):

Es un estándar para test de penetración que fue originalmente creado en 2009 por Nickerson et al. (Shanley & Johnstone, 2015) y está formado por siete secciones principales, las cuales son: 1) Interacciones de Pre-

compromiso, 2) Colecta de Información, 3) Modelamiento de Amenazas, 4) Análisis de Vulnerabilidades, 5) Explotación, 6) Post Explotación y 7) Reporte (Nickerson et al, 2014).

C) ISSAF – Information Systems Security Assessment Framework:

Intenta cubrir todos los posibles dominios de una prueba de penetración desde la concepción hasta la finalización, y se divide en tres fases primarias: 1) Planeación y Preparación; 2) Evaluación; y 3) Reporte y Limpieza (Shanley & Johnstone, 2015).

D) OWASP – Open Web Application Security Project:

Es una organización sin fines de lucro que se dedica a desarrollar recursos para la seguridad del software (OWASP, 2017). OWASP inicialmente ha desarrollado recursos para la seguridad de aplicaciones web. Actualmente tiene desarrollados también recursos para la seguridad de aplicaciones móviles. Los recursos para la seguridad de aplicaciones móviles están creados bajo otro proyecto llamado OWASP Mobile Security Project.

De las metodologías que se explican anteriormente y por encontrar similitudes se puede caracterizar en distintas fases, lo cuales podrían definirse como:

- Definir el Alcance: En esta fase se incluye la recolección de información y definición del activo que son necesaria para realizar

la evaluación y el nivel de protección que este tiene. El objetivo es conocer que es lo que se va a evaluar y que requisitos de seguridad son necesarios a aplicarse.

- Realizar la evaluación: En esta fase se aplica todo lo relacionado a las pruebas de vulnerabilidades. En esta fase se aplican todas las técnicas que se propone emplear en este trabajo de investigación.

- Reporte de Resultados: Es el resultado final que es generado después de concluir las 2 fases, incluyendo la documentación final que será proporcionado al cliente para que tome las acciones que correspondan para mejorar la seguridad de su aplicación móvil Android.

Para evaluar aplicaciones móviles existen diferentes tipos de pruebas de seguridad. Según (Cornell, 2014), existen herramientas que realizan los siguientes tipos de pruebas:

- Pruebas Estáticas: Las pruebas estáticas, o análisis estático, son las que analizan la aplicación mientras está en reposo, ya sea a partir del código fuente o el binario de la aplicación (Cornell, 2014). Este tipo de pruebas buscan deficiencias en el código fuente de la aplicación, y se pueden realizar mediante herramientas automatizadas.

- Pruebas Dinámicas: Las pruebas dinámicas, o análisis dinámico, permiten observar el comportamiento de los sistemas en funcionamiento (Cornell, 56 2014). Existen herramientas que permiten capturar y analizar el tráfico que genera la aplicación, así como modificarlo para examinar las respuestas que se obtienen y los problemas de seguridad que pudieran existir, lo cual no es posible apreciar en un análisis estático.

- Pruebas Forenses: Este tipo de pruebas permiten examinar los datos que deja la aplicación después de ejecutarse (Cornell, 2014). Las pruebas forenses son útiles para verificar si los datos sensibles están siendo realmente eliminados del dispositivo, por ejemplo: contraseñas.

1.1.7. **OWASP MOBILE SECURITY PROJECT**

Con el objetivo de concientizar acerca de la seguridad web a través de la identificación de algunos de los riesgos más críticos a los que se enfrentan las organizaciones, en el 2003 nace el proyecto OWASP, Open Web Application Security Project o Proyecto Abierto de seguridad de aplicaciones Web, publicando en la lista de referencia de las principales amenazas vigentes y actualizándola periódicamente.

Como parte del proyecto en el 2014 surge el Mobile Security Project, con el objetivo de proporcionar los recursos adecuados a desarrolladores y equipos

de seguridad para reforzar la seguridad, concretamente de las aplicaciones móviles.

Para ello y de manera análoga a la lista de riesgos de aplicaciones web, se clasifican los riesgos de seguridad móvil y se proporcionan los controles enfocados a reducir tanto su impacto como la posible explotación.

1.1.7.1. Top 10 Mobile Risk

La lista de riesgos de aplicaciones móviles más recientes, publicada en 2016, deriva de la especial atención prestada a la capa de aplicación, la infraestructura de los servidores con los que se comunican las aplicaciones móviles, la integración entre ellas, los servicios de autenticación remota y las características específicas de las plataformas Cloud. Así pues, el listado TOP 10 de los riesgos de seguridad móvil publicado por OWASP. Es el incluido a continuación:

A) Uso inapropiado de la aplicación:

Riesgo que cubre el mal uso de las características de la plataforma o la falta de uso de los controles de seguridad de la plataforma. Puede incluir intenciones de Android, permisos de plataforma, uso indebido de TouchID, el llavero o algún otro control de seguridad que sea parte del sistema operativo móvil.

B) Almacenamiento inseguro de datos:

Los agentes de amenazas incluyen lo siguiente: un adversario que ha obtenido un dispositivo móvil perdido/robado; malware u otra

aplicación reempaquetada que actúa en nombre del adversario y que se ejecuta en el dispositivo móvil.

C) Comunicación insegura:

Cuando se diseña una aplicación móvil, los datos se intercambian comúnmente de manera cliente-servidor. Cuando la solución transmite sus datos, debe atravesar la red del operador del dispositivo móvil e Internet. Los agentes de amenazas pueden aprovechar las vulnerabilidades para interceptar datos confidenciales mientras viajan por el cable. Existen los siguientes agentes de amenaza:

D) Autenticación insegura:

Los agentes de amenazas que explotan las vulnerabilidades de autenticación suelen hacerlo a través de ataques automatizados que utilizan herramientas disponibles o personalizadas.

E) Criptografía insuficiente:

Los agentes de amenazas incluyen los siguientes: cualquier persona con acceso físico a datos que se hayan cifrado incorrectamente o malware móvil que actúe en nombre de un adversario.

F) Autorización insegura:

Los agentes de amenazas que aprovechan las vulnerabilidades de autorización suelen hacerlo mediante ataques automatizados que utilizan herramientas disponibles o personalizadas.

G) Calidad del código del cliente:

Los agentes de amenazas incluyen entidades que pueden pasar entradas que no son de confianza a llamadas de métodos realizadas dentro del código móvil. Estos tipos de problemas no son necesariamente problemas de seguridad en sí mismos, sino que conducen a vulnerabilidades de seguridad. Por ejemplo, los desbordamientos de búfer en versiones anteriores de Safari (una vulnerabilidad de mala calidad del código) llevaron a ataques de Jailbreak de alto riesgo. Los problemas de mala calidad del código generalmente se aprovechan a través de malware o estafas de phishing.

H) Alteración del código:

Normalmente, un atacante aprovechará la modificación del código a través de formas maliciosas de las aplicaciones alojadas en tiendas de aplicaciones de terceros. El atacante también puede engañar al usuario para que instale la aplicación mediante ataques de phishing.

I) Ingeniería inversa:

Un atacante normalmente descargará la aplicación de destino de una tienda de aplicaciones y la analizará dentro de su propio entorno local utilizando un conjunto de herramientas diferentes.

J) Funcionalidad externa:

Por lo general, un atacante busca comprender la funcionalidad extraña dentro de una aplicación móvil para descubrir una funcionalidad oculta en los sistemas backend. Por lo general, el atacante aprovechará la funcionalidad extraña directamente desde sus propios sistemas sin la participación de los usuarios finales.

1.1.7.2. Estándar de Verificación de Seguridad de Aplicaciones Móviles (MASVS)

El Estándar de Verificación de Seguridad de Aplicaciones Móviles (MASVS, en inglés Mobile Application Security Verification Standard) de OWASP, es un esfuerzo comunitario para establecer un marco de requisitos de seguridad necesarios para diseñar, desarrollar y probar aplicaciones móviles seguras en iOS y Android.

El MASVS se puede utilizar para establecer un nivel de confianza en la seguridad de las aplicaciones móviles. Los requerimientos fueron desarrollados con los siguientes objetivos en mente:

- Usar como una métrica: Para proporcionar un estándar de seguridad contra el cual las aplicaciones móviles existentes

pueden ser comparadas por desarrolladores y los propietarios de las aplicaciones;

- Utilizar como guía: Proporcionar una guía durante todas las fases del desarrollo y prueba de las aplicaciones móviles;

- Usar durante la contratación: Proporcionar una línea de base para la verificación de seguridad de aplicaciones móviles.

El MASVS define dos niveles estrictos de verificación de seguridad (L1 y L2), así como un conjunto de requisitos de resistencia a la ingeniería inversa (MASVS-R) flexible, es decir, adaptable a un modelo de amenaza específico de la aplicación. Los niveles MASVS-L1 y MASVS-L2 contienen requerimientos genéricos de seguridad recomendados para todas las aplicaciones móviles (L1) y para aplicaciones que manejan datos altamente sensibles (L2). MASVS-R cubre los controles de seguridad adicionales que se pueden aplicar si la prevención de las amenazas del lado del cliente son un objetivo de diseño.

A) V1: Requisitos de Arquitectura, Diseño y Modelo de Amenazas:

Además de los controles técnicos, MASVS requiere que existan procesos que garanticen que la seguridad se ha abordado

explícitamente al planificar la arquitectura de la aplicación móvil, y que se conocen los roles funcionales y de seguridad de todos los componentes (Mueller & Schleier, OWASP Mobile Application Security Verification Standard v1.0, 2018). Este grupo de requerimientos verifica que la seguridad se haya tomado en cuenta desde que la aplicación comenzó a planificarse, por tanto, no verifica controles técnicos, sino más bien la documentación de la aplicación.

B) V2: Requerimiento en el almacenamiento de datos y la Privacidad:

Los requerimientos de este grupo se centran en la protección de datos sensibles, refiriéndose a información de identificación personal, datos altamente confidenciales y cualquier otro dato que debe ser protegido por ley o por razones de conformidad (Mueller & Schleier, OWASP Mobile Application Security Verification Standard v1.0, 2018). El almacenamiento inseguro de datos puede facilitar el robo y la fuga de información, lo cual impactaría en la confidencialidad de la información, generando daños en la reputación de la aplicación y del negocio, incumplimiento de cláusulas de confidencialidad, mal uso de la información obtenida, entre otros.

C) V3: Requerimiento de Criptografía:

El propósito de estos controles es asegurarse de que la aplicación utiliza criptografía según las mejores prácticas de la industria, incluyendo: Uso de librerías conocidas y probadas; Configuración y elección de primitivas criptográficas apropiado; Cuando se requiere de randomización se selecciona el generador debido (Mueller & Schleier, OWASP Mobile Application Security Verification Standard v1.0, 2018).

D) V4: Requerimientos de Autenticación y Manejo de Sesiones:

MASVS define algunos requerimientos básicos sobre cómo manejar las cuentas y sesiones del usuario (Mueller & Schleier, OWASP Mobile Application Security Verification Standard v1.0, 2018). Los requerimientos definidos en este grupo verifican aspectos relacionados con cuentas de usuario y manejo de sesiones, como ser el uso de tokens, doble factor de autenticación cierre de sesión tanto del lado del cliente como del lado del servidor, entre otros.

E) V5: Requerimientos de Comunicación de la red:

Los controles enumerados en esta categoría tienen por objetivo asegurar la confidencialidad e integridad de la información intercambiada entre la aplicación móvil y los servicios del servidor (Mueller & Schleier, OWASP Mobile Application Security Verification

Standard v1.0, 2018). La comunicación a través de la red debe estar protegida, dado que el internet no se considera un canal seguro y la información podría ser interceptada por terceros si no se aplican los controles recomendados

F) V6: Requerimientos de Interacción con la Plataforma:

Estos controles revisan que se utilicen las APIs de la plataforma y componentes estándar de una manera segura (Mueller & Schleier, OWASP Mobile Application Security Verification Standard v1.0, 2018). En este grupo de requerimientos se considera la interacción entre la aplicación y el sistema operativo, por ejemplo, permisos de usuario. También considera que la comunicación entre aplicaciones se realice de manera segura.

G) V7: Requerimientos de Calidad de Código y Configuración del Compilador:

Estos controles buscan asegurar que se siguieron las buenas prácticas de seguridad básicas en el desarrollo de la aplicación y que se activaron las funcionalidades “gratuitas” ofrecidas por el compilador (Mueller & Schleier, OWASP Mobile Application Security Verification Standard v1.0, 2018). Prácticas de seguridad recomendadas en todo tipo de desarrollo se incluyen en este grupo, como ser el manejo de excepciones, debug deshabilitado, y demás aspectos relacionados con el código.

H) V8: Requerimientos de Resistencia ante la Ingeniería Inversa:

La falta de estos controles no genera vulnerabilidades – sino que, están pensados para incrementar la resistencia contra la ingeniería inversa de la aplicación (Mueller & Schleier, OWASP Mobile Application Security Verification Standard v1.0, 2018). Este grupo de requerimientos es el conjunto de requisitos R mencionado anteriormente, los cuales deben ser verificados si la aplicación lo requiere de acuerdo con su análisis de riesgo. Este grupo de controles no debe ser el único que se verifica en una aplicación, sino que debe estar combinado con el nivel 1 (L1) o nivel 2 (L2), es decir, se debe verificar también el cumplimiento de los requisitos mínimos para garantizar el nivel de seguridad de la aplicación.

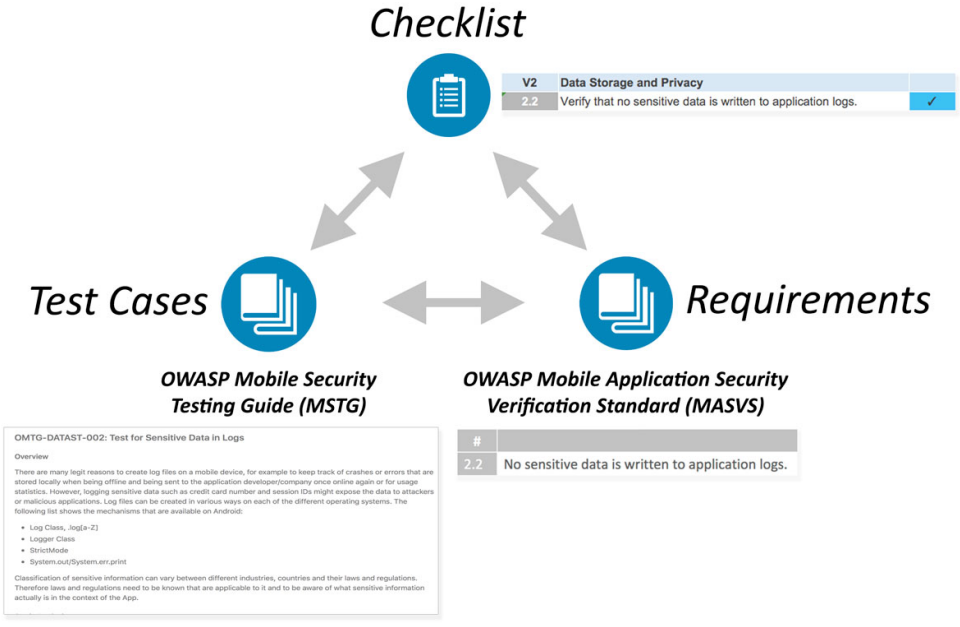
1.1.7.3. Mobile Security Testing Guide

Es un manual desarrollado para las pruebas de seguridad en aplicaciones móviles. Describe procesos y técnicas para verificar los requerimientos listados en Mobile Application Security Verification Standard (MASVS), y provee una línea base para evaluaciones de seguridad completas y consistentes (Mueller & Schleier, Mobile Security Testing Guide Release 1.0, 2018). Esta guía describe aspectos técnicos para la verificación de los requisitos de seguridad en plataformas Android e iOS. Se incluyen la búsqueda de palabras claves en el código y el uso de herramientas de análisis.

1.1.7.4. Mobile Security Checklist

Esta guía está estrechamente relacionada con el Estándar de verificación de seguridad de aplicaciones móviles de OWASP (MASVS). MASVS define un modelo de seguridad de aplicaciones móviles y enumera los requisitos de seguridad genéricos para las aplicaciones móviles. Puede ser utilizado por arquitectos, desarrolladores, probadores, profesionales de seguridad y consumidores para definir y comprender las cualidades de una aplicación móvil segura. El MSTG se asigna al mismo conjunto básico de requisitos de seguridad ofrecidos por MASVS y, según el contexto, se pueden usar individualmente o combinados para lograr diferentes objetivos.

Figura 3: Documentación OWASP sobre seguridad en Aplicaciones Móviles



Fuente: https://owasp.org/www-project-web-security-testing-guide/

1.2. DEFINICIÓN DE TÉRMINOS BÁSICOS

Auditoria:

Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse.

Auditoria informática:

Proceso de recoger agrupar y evaluar evidencias para determinar si un sistema de información mantiene y salvaguarda la integridad de los datos de una organización, utilizando eficazmente los recursos y cumpliendo con las leyes y regulaciones establecidas.

Seguridad Informática:

Cualidad de un sistema informático exento de peligro.

Hacking:

Se le llama hacking a un conjunto de técnicas para acceder a un sistema informático sin autorización.

Malware:

El malware es un término general que se le da a todo aquel software que perjudica a la computadora. La palabra malware proviene del término en ingles malicious software, y en español es conocido con el nombre de código malicioso.

OWASP:

El proyecto abierto de seguridad en aplicaciones (Open Web Application Security Project por sus siglas en inglés) es una comunidad abierta dedicada a facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones que puedan ser confiables.

CAPÍTULO II: MARCO JURIDICO

Para el presente trabajo se realizó una búsqueda de las principales leyes y normas aplicables a las políticas de información con el fin de tener conocimiento jurídico que aportan para el desarrollo del proyecto de investigación.

2.1. Ley de protección de datos personales “LEY Nº 29733”

Artículo 1. Objeto de la Ley

La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

Artículo 17. Confidencialidad de datos personales

El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales.

El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional.

2.2. ley de delitos informáticos “LEY Nº 30096”

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

Artículo 2. Acceso ilícito

El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado

Artículo 3. Atentado contra la integridad de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Artículo 4. Atentado contra la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Artículo 7. Interceptación de datos informático

El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático,

específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa

CAPÍTULO III: METODOLOGIA DE DESARROLLO DEL TRABAJO PROFESIONAL

3.1. DELIMITACIÓN DEL TRABAJO

El siguiente proyecto abarcar el área de proyecto de baja tensión, limitándose por lo siguiente:

A) **Campo:** Hacking Ético

B) **Área:** Ciberseguridad

C) **Aspectos:** Aplicación Móvil Android

D) **Tema:** Propuesta del manual de procedimientos estándar para el proceso de evaluación de seguridad en una aplicación móvil Android basado en la metodología OWASP para los clientes de la empresa ENTELGY.

E) **Espacial:** El estudio ira dirigido a la empresa ENTELGY, ubicado en el distrito de Miraflores y para sus actuales y potenciales clientes.

F) **Temporal:** El presente trabajo se realizará desde agosto a diciembre del 2020, tomando en cuenta a la documentación del proyecto OWASP, se estudiará los aspectos de seguridad en aplicaciones móviles Android y la situación actual de la empresa ENTELGY, durante dicho periodo de tiempo.

3.2. DETERMINACIÓN U ANÁLISIS DEL PROBLEMA

3.2.1. DESCRIPCION DEL PROBLEMA

ENTELGY es una empresa dedicada a la consultoría, outsourcing y tecnología que aboga por la internacionalización, y cuenta con en tres áreas especializadas, entre ellas el área dedicada a la ciberseguridad. Uno de los servicios que brinda es el pentesting a aplicaciones móviles y otros sistemas informáticos para diversos clientes, el cual solicitan sus servicios para evaluar la seguridad de sus aplicaciones, orientados para diversas necesidades, pudiendo ser tan simples como realizar consultas, o tan complejas como procesar transacciones financieras con información sensible. Los clientes de Entelgy buscan que su aplicación móvil obtenga un nivel de seguridad en función a su objetivo, propósito o los riesgos que este pueda estar expuesto. Por lo cual el cliente busca identificar potenciales vulnerabilidades, con el fin de ellos mismos puedan corregir y/o mitigar para alcanzar un nivel de seguridad aceptable.

ENTELGY se caracteriza por el uso riguroso de marcos metodológicos con referencia internacionales que abarcan diversos aspectos de seguridad para las aplicaciones móviles, pero eso se hace uso de un amplio listado de controles muy rigurosos, de los cuales muchos de ellos son innecesarios para aquellas aplicaciones que no necesitan una revisión a profundidad. Lo que ha ocasiona que las evaluaciones de seguridad estén enfocadas únicamente al cumplimiento total de los

requisitos basados en algún estándar de seguridad universal, e inclusive si no tienen relevancia para el propósito que tiene la aplicación móvil, debido a que el cliente solo tiene la expectativa de poder obtener resultados certeros que les pueda indicar en especial a las vulnerabilidades que tengan los riegos más críticos basados en las característica del negocio, incluido con sus respectivas recomendaciones para así subsanarlos y fortalecer la seguridad de la aplicación hasta un nivel que el cliente considere aceptable, sin necesidad de emplear todos los requisitos de seguridad definidos en estándares actuales que emplea la empresa.

Para analizar, en el contexto de la ENTELGY, relacionado con la evaluación de las aplicaciones móviles Android se presenta la Tabla No. 1 un análisis FODA, que servirá para identificar las causas de mayor incidencia del problema.

Tabla 1. Analisis FODA de la empresa ENTELGY

Debilidades	**Amenazas**
- Las metodologías que se emplean en la empresa son muy amplias para evaluar aplicaciones móviles.	- Aparición de nuevas vulnerabilidades para aplicaciones móviles.
- El tiempo que dedica la empresa a una evaluación de seguridad puede pasar el tiempo propuesto que necesita la aplicación y como el cliente lo requiere.	- Avance tecnológico en los dispositivos móviles y sus aplicaciones.

Fortalezas	Oportunidades
- Personal con experiencia en aplicaciones móviles.	- Existencia de una guía de OWASP que identifica las principales vulnerabilidades en aplicaciones móviles, en diferentes plataformas.
- Calidad de servicio de pruebas con los clientes, así como el soporte en caso de algún incidente.	- Existencia de herramientas de software libre que permiten analizar la seguridad de aplicaciones móviles y están recomendados por OWASP.

Fuente: Elaboración propia

A partir del Analisis FODA, se pudo concluir que una de las causas de mayor incidencia en el problema de ENTELGY es el uso de metodologías estándares que abarcar muchos criterios de evaluación y en resultan ser amplias y estas evalúan aspectos que no aplican de manera relevante en las aplicaciones móviles de sus clientes, por lo cual se tendrá que acoplar a un procedimiento de trabajo que se adapte a las necesidades y requisitos de seguridad de cada cliente basado en los riesgos que estos están expuestos.

3.2.2. **JUSTIFICACIÓN DEL PROBLEMA**

El desarrollo del presente trabajo pretende incluir diferentes niveles de revisión en la evaluación de requisitos de seguridad de las aplicaciones móviles por parte de la empresa ENTELGY hacia sus clientes, tomando en cuenta el nivel de seguridad solicitado por cada cliente en función a los riesgos más elevados que sus aplicaciones móviles estuviesen expuestos. A la misma vez se espera de ENTELGY pueda realizar las evaluaciones de

seguridad de aplicaciones móviles de manera más eficiente en el uso de todos sus recursos.

Se espera, con la aplicación de este manual pueda ofrecer a los clientes de ENTELGY un servicio más personalizado, así como beneficiar a la empresa para reducir el tiempo, costo y dificultad para evaluar las aplicaciones móviles que requieran un nivel de seguridad especifico. A su vez ofrecer a los clientes la oportunidad de escoger el nivel de profundidad de revisión para sus aplicaciones móviles en función de sus necesidades y característica de negocio, así como el riesgo que se encuentren expuestos.

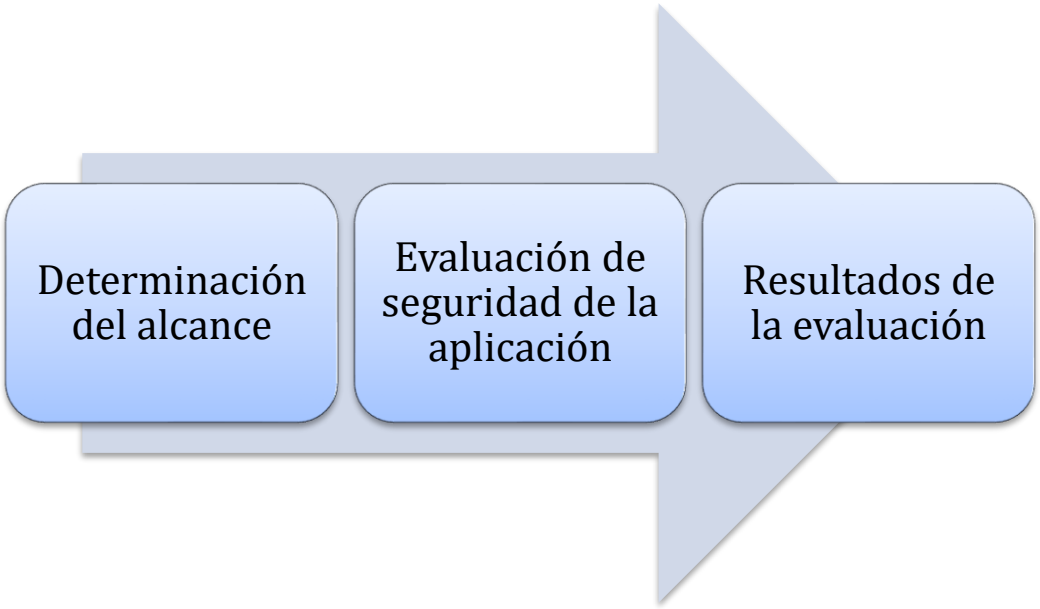
Por otra parte, si no se realiza esta propuesta de trabajo no se podrá contar con una herramienta muy útil y necesaria que beneficiará tanto a ENTELGY como a sus clientes para optimizar eficientemente las evaluaciones de seguridad en aplicaciones móviles; quedando finalmente como una empresa poco competitiva a las necesidades actuales.

3.3. MODELO DE SOLUCIÓN PROPUESTO

3.3.1. DISEÑO METODOLÓGICO

El trabajo de investigación está compuesto por 3 fases, las cuales permitirán alcanzar el objetivo del trabajo.

Figura 4 **:** Metodología implementada en el proyecto



Fuente**:** Elaboración propia

FASE 1: DETERMINACIÓN DEL ALCANCE

Esta fase establece el análisis a la aplicación móvil para identificar el alcance de la evaluación y los requisitos que serán revisados.

FASE 2: EVALUACIÓN DE SEGURIDAD DE LA APLICACIÓN

En esta fase se realiza la evaluación de los requisitos de seguridad propuestos.

FASE 3: RESULTADO DE LA EVALUACIÓN

En esta fase se obtiene la documentación elaborada que será dirigido para el cliente y los demás responsables.

Cada fase estará compuesta por los siguientes elementos:

- **Entrada:** Son los datos e insumos necesarios para ser procesados.
- **Procesamiento:** Las acciones a realizar utilizando los recursos de la entrada.
- **Salida:** Son los resultados que se van a obtener posterior al procesamiento.

3.4. RESULTADOS

3.4.1. ANALISIS DE LA SITUACION ACTUAL DE ENTELGY

3.4.1.1. ENTELGY

Entelgy es empresa de Consultoría, Outsourcing y Tecnología que aboga por la internacionalización y que cuenta con tres áreas de especialización en Ciberseguridad, Digital y EBS (Enterprise Business Solution).

Entelgy tiene la misión de aportar soluciones de negocio gracias a la actitud y al talento de sus profesionales.

Con un modelo empresarial de desarrollo sostenido a largo plazo, Entelgy cuenta con más de 400 Clientes, 1500 Profesionales, una oferta de alto valor y un gran reconocimiento del Mercado.

Entelgy, a través de su empresa InnoTec System, especialista en seguridad tecnológica, prevención y gestión de riesgos, ofrece soluciones orientadas a la creación de una verdadera cultura de la seguridad en las organizaciones. Uno de los servicios que brinda Entelgy es el pentesting de aplicaciones móviles, el cual empresas solicitan los servicios para evaluar la seguridad de sus aplicaciones móviles con diferentes propósitos y características.

3.4.1.2. SITUACION ACTUAL DE ENTELGY

De acuerdo con la entrevista realizado al jefe del área de ciberseguridad de la empresa ENTELGY (ANEXO 02), se identifica lo siguiente, respecto a la metodología actual de trabajo para realizar evaluaciones de seguridad de aplicaciones móviles.

A) Analisis Previo:

Antes de evaluar la seguridad de una aplicación móvil se hace un análisis de contexto con el fin de identificar ciertos criterios: como el rubro de la empresa, los datos involucrados, el funcionamiento de la aplicación, los permisos de la aplicación, entre otros datos útiles.

B) Requisitos de seguridad:

Los requisitos de seguridad para aplicaciones móviles que emplea ENTELGY en su metodología están basados en las dimensiones de seguridad: confidencialidad, integridad y disponibilidad.

C) Metodología estándares:

La metodología que emplea ENTELGY para evaluar la seguridad de las aplicaciones móviles están basados en OWASP Mobile Top Ten.

D) Metodología de trabajo actual:

La metodología de trabajo actual de ENTELGY está compuesto por las siguientes fases: Analisis de Contexto, Recopilación de información, Analisis automatizado, Validación de falsos positivos, Explotación de vulnerabilidades, Retest (en caso sea necesario) y Elaboración de informes.

E) Duración:

En promedio una evaluación de seguridad de una aplicación móvil puede llegar a durar hasta 2 semanas.

F) Hallazgos:

El hallazgo de resultados en las aplicaciones móviles se clasifica según el nivel de riesgo en: Críticos, Altos, Medios, Bajo e Informativos.

G) Recomendaciones:

Al terminar una revisión se elaboran los informes con las recomendaciones considerando como prioritarios las vulnerabilidades críticas y altas.

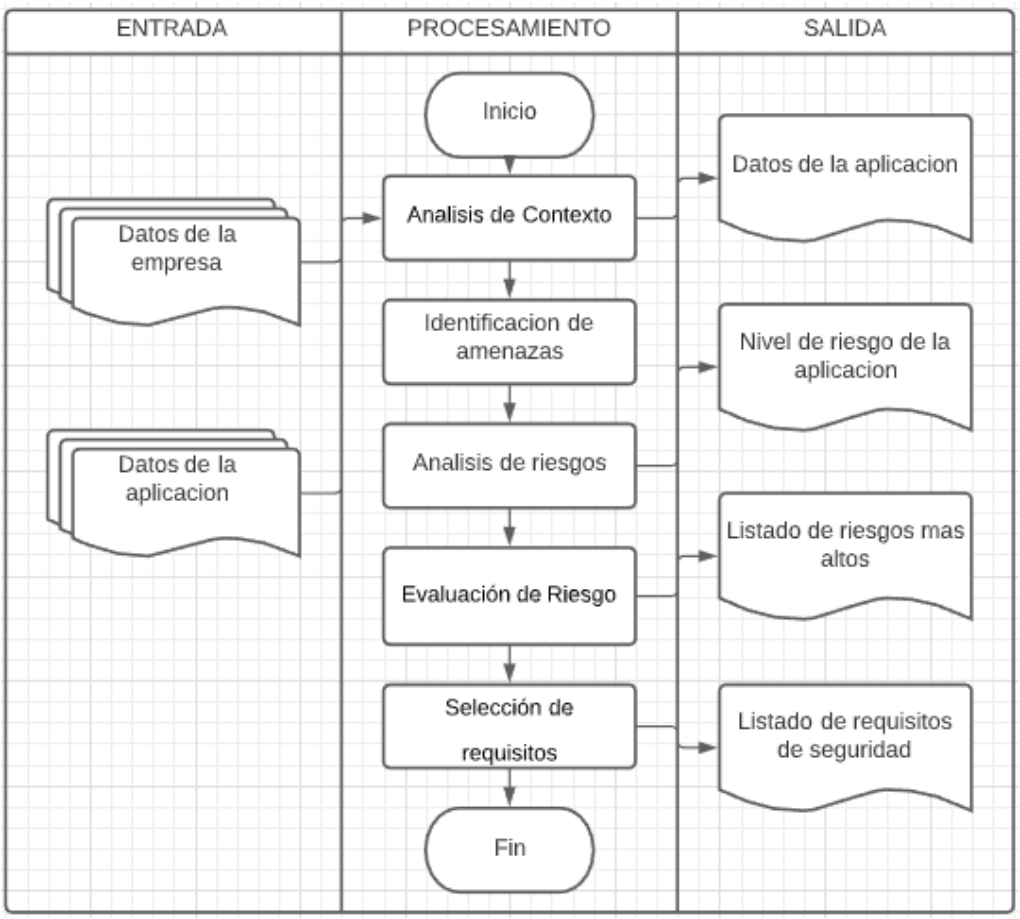
3.4.2. PROCEDIMIENTO DE EVALUACIÓN DE SEGURIDAD EN UNA APLICACIÓN MÓVIL ANDROID

Se describe el procedimiento de evaluación de seguridad de una aplicación móvil Android, así como los elementos de entrada y los elementos de salida.

3.4.2.1. FASE 1: DETERMINACIÓN DEL ALCANCE

Para realizar una adecuada revisión de seguridad que nos permita medir la protección contra los riesgos más críticos de una aplicación móvil es necesario medir los riesgos que la aplicación se encuentra expuesta. La finalidad de este análisis nos permitirá identificar cuáles son los riesgos más significativos que este expuesto la aplicación móvil y en qué puntos se deberá enfocar la evaluación. Por eso mismo en esta fase no se tendrá en cuenta la etapa de tratamientos de riesgos, ya que no se menciona aun las acciones como se mitigará el riesgo. En la siguiente tabla se muestra un resumen de esta fase:

Figura 5: Diagrama de flujo – Determinar el alcance



Fuente: Elaboración propia

A continuación, en la Tabla 2, se describe al responsable y las actividades que está compuesto la fase para determinar el alcance de la evaluación:

Tabla 2: Actividades – Fase 1 - Determinar el alcance

N°	Responsable	Actividades
		Inicio
1	Evaluador	Análisis de Contexto
1.1	Evaluador	- Obtener Datos de la Empresa - Obtener Datos de la Aplicación Móvil
1.2	Evaluador	- Análisis de Misión, Visión y Objetivos - Identificación de la Normativa - Categorización de la Aplicación Móvil
2	Evaluador	Identificación de Amenazas
2.1	Evaluador	- Identificación y Valoración de Activos

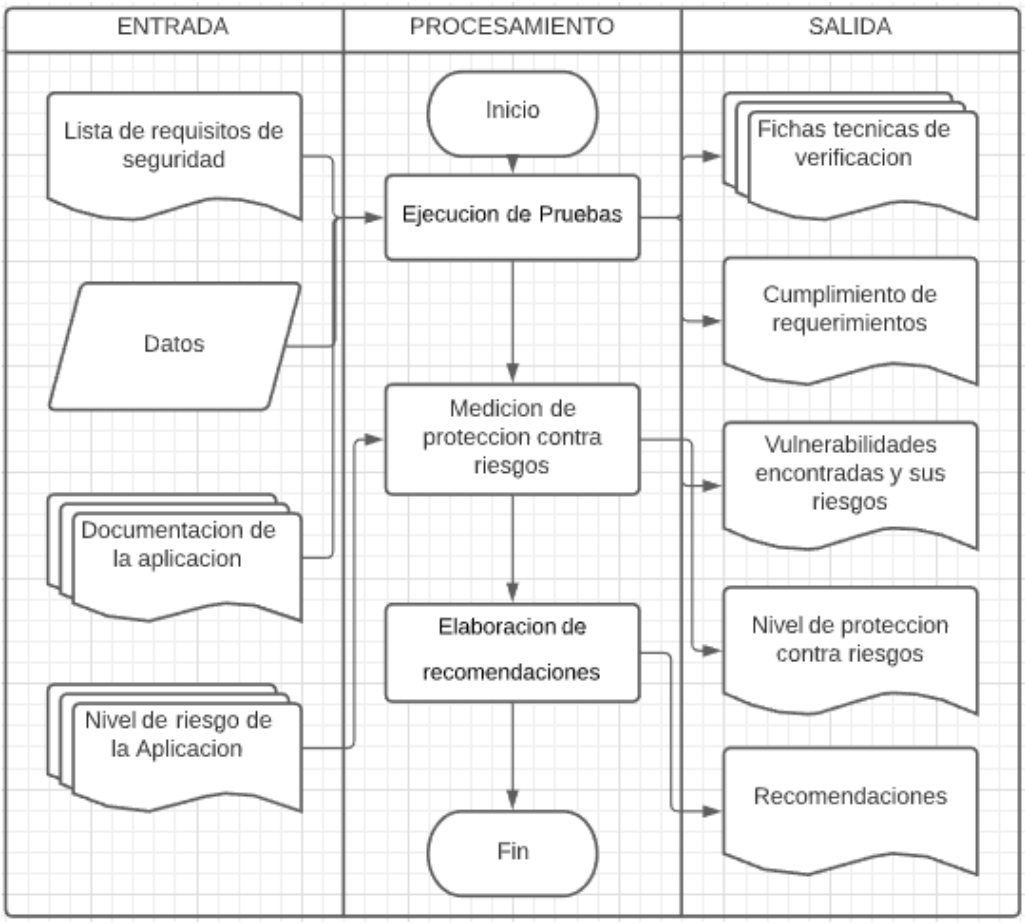
		- Identificación de Amenazas por elemento clave
3	Evaluador	Análisis de Riesgo
3.1	Evaluador	- Probabilidad - Impacto - Cálculo de Nivel de Riesgo
4	Evaluador	Evaluación de Riesgos
4.1	Evaluador	- Selección de los Riesgos más Altos
5	Evaluador	Selección de Requisitos de Seguridad para Evaluar
6		**Fin**

Fuente: Elaboración propia

3.4.2.2. **FASE 2: EVALUACIÓN DE SEGURIDAD DE LA APLICACIÓN**

Después de determinado el alcance de la evaluación, e identificado los requisitos a evaluar se procede a realizar las pruebas correspondientes para poder verificar si algunos de los requisitos de seguridad se cumplen o no. En la siguiente tabla se muestra un resumen de esta fase:

Figura 6: Diagrama de Flujo - Evaluar la seguridad de la aplicación móvil



Fuente: Elaboración propia

A continuación, en la Tabla 3, se describe al responsable y las actividades que está compuesto la fase para evaluar la seguridad de una aplicación móvil Android:

Tabla 3: Actividades – Fase 2 – Evaluación de Seguridad de la aplicación

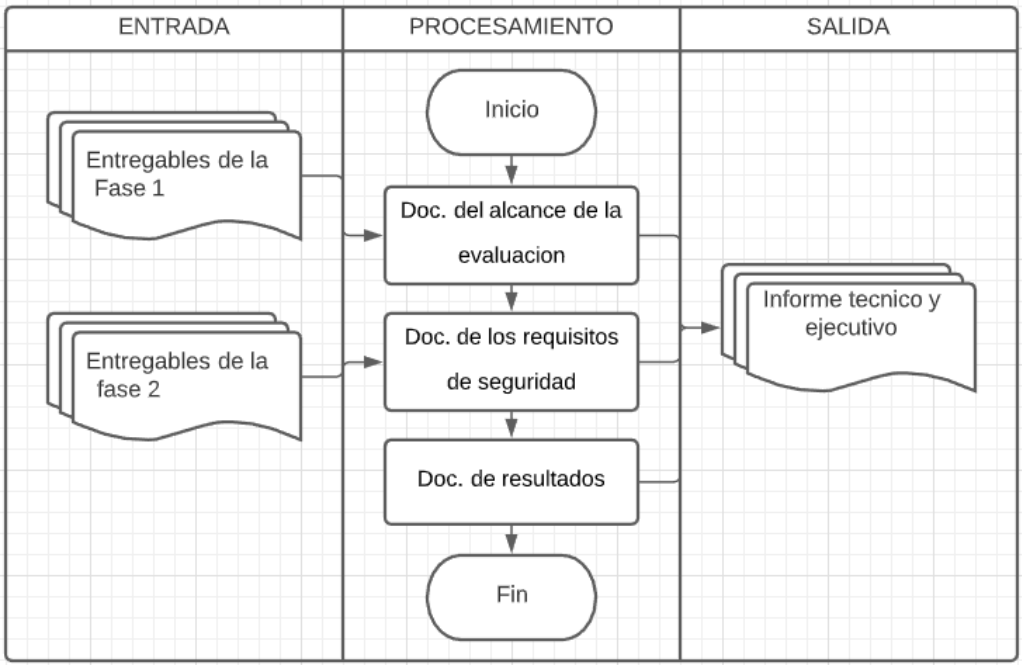
N°	Responsable	Actividades
		Inicio
1	Evaluador	Ejecución de Pruebas
1.1	Evaluador	- Revisión de Documentación - Análisis Estático - Análisis Dinámico - Análisis Forense - Pruebas de Ingeniería Inversa
2	Evaluador	Medición de Protección contra Riesgos
2.1	Evaluador	- Requisitos de Seguridad Seleccionados - Requisitos de Seguridad Evaluados - Requisitos de Seguridad Cumplidos - Cálculo de Probabilidad Residual - Cálculo de Nivel de Riesgo Residual - Gráfico de Nivel de Riesgo Residual
3	Evaluador	Elaboración de Recomendaciones
		Fin

Fuente: Elaboración propia

3.4.2.3. FASE 3: RESULTADOS DE LA EVALUACIÓN

Una vez concluida la evaluación se elabora la documentación respecto a la evaluación y se procede hacer entrega a los responsables que corresponde. En la imagen se muestra un resumen de esta fase:

Figura 7: Diagrama de Flujo - Resultados de la evaluación



Fuente: Elaboración propia

A continuación, en la Tabla 4, se describe al responsable y las actividades que está compuesto la fase para los resultados de la evaluación:

Tabla 4: Actividades - Fase 3 – Resultados de la Evaluación

N°	Responsable	Actividades
		Inicio
1	Evaluador	Documentación del Alcance de la Evaluación
2	Evaluador	Documentación de la Evaluación de Requisitos de Seguridad
3	Evaluador	Documentación de Resultados
		Fin

Fuente: Elaboración propia

3.4.3. MANUAL DE PROCEDIMIENTOS PARA LA EVALUACIÓN DE SEGURIDAD EN UNA APLICACIÓN MÓVIL ANDROID

El manual de procedimientos tiene como objetivo dar las pautas a seguir para realizar una evaluación de seguridad en una aplicación móvil Android siguiendo la estructura de la metodología propuesta y tener en cuenta para poder aplicarse:

3.4.3.1. FASE 1: DETERMINACIÓN DEL ALCANCE

Para realizar una evaluación de seguridad que permita medir la protección contra los riesgos más altos de una aplicación móvil, será necesario identificar y medir los riesgos a los que se encuentra expuesta la aplicación. El objetivo de este análisis es determinar cuáles son los riesgos más significativos a los que está expuesta la aplicación móvil y en los que se debería enfocar la evaluación de esta. Es por eso por lo que no se toma en cuenta la fase de tratamiento del riesgo, ya que no se hará foco aún en las acciones que se deberían realizar para mitigar cada uno de los riesgos.

ELEMENTOS DE ENTRADA

Los elementos de entrada para estará dividida en 2 partes: la primera compuesta por los datos de la empresa y las segunda respecto a los datos de la aplicación.

A) Datos de la Empresa

- **Misión y Visión:** Son datos que compone la empresa y son de suma importancia incluir en nuestro análisis para comprender el core de la empresa.

- **Rubro de la empresa:** Se identifica el rubro que pertenece la empresa, así como los temas regulatorios para evitarse posibles sanciones legales. Las empresas que son del mismo rubro manejan actividades y servicios similares que conlleva una aplicación móvil, lo cual facilita el entendimiento para solicitar datos del funcionamiento de la aplicación. El rubro de la empresa permitirá al evaluador tomar ciertas acciones respectos a la cantidad de usuarios que acceden a la aplicación, así como permite identificar posibles riesgos relacionados a las características del rubro. Para fines del análisis del contexto se describe los siguientes ejemplos de rubros de empresas: bancarios, gobierno, comercio, servicio, salud, etc.

- **Servicio y/o actividades de la empresa:** Entender la actividad que se dedica la empresa nos permite tener un mayor entendimiento del negocio, así como comprender el funcionamiento de la aplicación móvil.
- **Otros datos relevantes:** Son datos que puedan ser necesarios y complementan para poder comprender el negocio.

B) Datos de la Aplicación

- **Datos de la aplicación móvil:** nombre de la aplicación, nombre del paquete, versión, tamaño, fecha de actualización, versión compatible entre otros datos.

- **Objetivo de la aplicación móvil:** Se considera el propósito en que fue creado la aplicación móvil.

- **Usuarios de la aplicación móvil:** Se considera diferentes escenarios por los diferentes actores y roles que pueda contener la aplicación móvil.

- **Clientes:** El escenario más común es que la aplicación ya este disponible para los clientes de la empresa, entonces la empresa ya no tiene ningún control sobre los

dispositivos en los que se instala la aplicación móvil y los riesgos varían.

- **Mapa de Navegación de la aplicación:** Nos permite identificar los elementos claves de la aplicación, así como las opciones que contiene la aplicación a evaluar, las cuales podrán ser analizadas una por una para identificar los riesgos que este tenga.

- **Permisos solicitados:** Se tendrán que listar los permisos que contiene la aplicación para analizar los riesgos que estos puedan estar asociados, se debe solicitar todos los registros para realizar un buen análisis.

- **Otros datos relevantes:** Que puedan ser útiles para complementar la información, así como los términos de referencia que muestran las condiciones del servicio contratado.

ELEMENTOS DE PROCESAMIENTO

Con los datos obtenidos se realizará el análisis con el fin que nos permitan obtener el alcance que tendrá la evaluación de la aplicación móvil. Se describen todas las actividades que complementan esta fase para determinar el alcance de la evaluación.

Tabla 5: Procedimiento - Analisis de Contexto

Procedimiento 01: Análisis de Contexto
Descripción: Permite analizar aspecto respecto al entorno interno y externo de la empresa que se consideraran dentro de la evaluación de la aplicación móvil. Los formularios se encuentran en el ANEXO 03 Y 04.
Pasos 1. Análisis de la visión, misión y objetivos. 2. Identificación de la normativa. 3. Categorización de la aplicación.

Fuente: Elaboración propia

- **Análisis de Misión, Visión y Objetivos:** Se verificará que los objetivos de la aplicación estén alineados a la visión, misión de la empresa. La aplicación móvil no será el objetivo principal de la empresa, sino será un apoyo para que la empresa pueda lograr sus objetivos. La misión y visión de la empresa se comparar con los objetivos de la aplicación, para corroborar si aplican principios de Gobierno TI.

- **Identificación de la Normativa:** Se identifican las normativas que regulan las actividades de la empresa y deberán estar considerados en la aplicación, para considerar todos los escenarios posibles.

- **Categorización de la aplicación:** De acuerdo con el objetivo de la aplicación se podrá definir la categoría a la cual pertenece la aplicación móvil, se podría considerar por ejemplo los siguientes: banca móvil, consulta de datos, aplicación informativa, etc.

Tabla 6: Procedimiento - Identificación de Amenazas

Procedimiento 02: Identificación de Amenazas
Descripción: Con los datos obtenidos anteriormente se procede a identificar las amenazas que se encuentra la aplicación móvil.
Pasos 1. Identificación y valoración de activos 2. Identificación de amenazas por cada elemento clave

Fuente: Elaboración propia

- **Identificación y valoración de activos:** En este punto se considera únicamente a la información que maneja y los servicios que presta la aplicación móvil, no se consideran activos superiores de los que pueda depender la aplicación incluidos servidores, software, personal que maneja la información, ni otros. Utilizando el mapa de navegación se

puede identificar dichos componentes o activos en cada una de las opciones disponibles.

- **Identificación de amenazas por cada elemento:** El objetivo es determinar lo que le podría ocurrir al activo en cada escenario, ya sea dato o servicio, y cuáles de sus dimensiones se verían afectadas.

Tabla 7: Procedimiento - Analisis de riesgo

Procedimiento 03: Análisis de riesgo
Descripción: Posterior a identificar las amenazas y los activos, se deberá valorar la influencia del riesgo sobre cada activo en dos sentidos: probabilidad y degradación, o el impacto.
Pasos 1. Análisis de la probabilidad 2. Análisis del impacto 3. Cálculo del nivel del riesgo potencial

Fuente: Elaboración propia

- **Analisis de probabilidad:** Este valor considera que tan probable se materialice una amenaza sobre el activo. En este punto todavía la aplicación no es evaluada, la probabilidad se deberá estimar sin tomar en cuenta las salvaguardas que puedan existir, ya que aún no se conocen. Para esta metodología se define la siguiente escala cualitativa: muy alto, alto medio, bajo y muy bajo.

- **Analisis del impacto:** Este valor indica que tanto daño ocasionaría la materialización de una amenaza a un activo. Se puede también definir una escala cualitativa similar a la probabilidad con sus respectivos puntajes: muy alto, alto, medio, bajo y muy bajo.

- **Cálculo de nivel del riesgo potencial:** Este valor se determina, de forma numérica, mediante la multiplicación entre la probabilidad y el impacto de cada amenaza. Dentro de este punto se puede obtener el nivel de riesgo potencial por amenaza mediante la multiplicación de impacto con la probabilidad:

  Nivel de Riesgo = Probabilidad x Impacto

  Se identifican cinco niveles de riesgo: Muy alto, alto, medio, bajo y muy bajo.

  El nivel de Riesgo Potencial de una aplicación es el promedio de los niveles de riesgo de todas las amenazas identificadas.

Tabla 8: Procedimiento – Evaluación de riesgos

Procedimiento 04: Evaluación de riesgos
Descripción: Se evalúan todos los resultados anteriormente y se seleccionar los riesgos más altos, para dar más énfasis a la mitigación.
Pasos 1. Selección de riesgos más altos

Fuente: Elaboración propia

- **Selección de riesgos más altos:** En esta etapa se seleccionarán los riesgos más importantes para la aplicación móvil y la empresa, tomando en cuenta el riesgo aceptable definido por la empresa y/o algún termino de referencia en caso de que se haya definido, ya que el cliente es el que escoge la profundidad que tendrá la evaluación. De esta manera se dará más énfasis a los activos expuestos a los mayores riesgos.

Tabla 9: Procedimiento – Selección de Requisitos de Seguridad

Procedimiento 05: Selección de requisitos de seguridad a evaluar
Descripción: Utilizando la lista de los riesgos más altos, se seleccionarán los requisitos de seguridad que, de cumplirse mitigarán dichos riesgos.
Pasos 1. Selección de requisitos de seguridad

Fuente: Elaboración propia

- **Selección de requisitos de seguridad:** Los requisitos se obtienen del Mobile Application Security Verification Estándar (MASVS) del proyecto OWASP, después de haber identificado los riesgos más altos.

ELEMENTOS DE SALIDA

Como resultado del procesamiento, se obtendrá lo siguiente:

- **Datos de la aplicación móvil:** Se obtiene de la fase anterior.

- **Relación Mapa de navegación – Datos - Servicios:** En este punto se listan en una tabla todas las opciones de la aplicación móvil, ejemplo “iniciar sesión en la aplicación”.

- **Nivel de riesgo de la aplicación:** Este puntaje se utiliza para medir posteriormente la protección de la aplicación contra los riesgos.

- **Lista de riesgos más altos:** Después del análisis de riesgo se obtiene un listado con los riesgos mas altos de la aplicación móvil. Esta lista contiene: el riesgo, los activos que afecta, probabilidad, impacto y el nivel de riesgo.

- **Lista de requisitos de seguridad:** Los requisitos se obtiene de la lista de riesgos mas altos, considerando aquellos que mitigarían algún riesgo. Estos son los requisitos de seguridad a evaluar para medir la protección contra los riesgos.

3.4.3.2. FASE 2: EVALUACIÓN DE SEGURIDAD DE LA APLICACIÓN

Luego de haber determinado el alcance de la evaluación, y los requisitos a ser evaluados se procederá a realizar las pruebas correspondientes para verificar si cada uno de los requisitos se cumplen.

ELEMENTOS DE ENTRADA

- **Lista de riesgos más altos:** registrado de la fase anterior.

- **Lista de requisitos de seguridad:** registrado de la fase anterior.

- **Aplicación Móvil:** Se obtendrá el archivo .APK de la aplicación móvil para realizar las pruebas en él.

- **Documentación de la Aplicación Móvil:** El cliente proporcionará documentación sobre la arquitectura, diseño y modelado de amenazas de la aplicación.

ELEMENTOS DE PROCESAMIENTO

En base a elementos de entradas se podrá realizar la evaluación de los requisitos de seguridad en la aplicación móvil.

Tabla 10: Procedimiento – Ejecución de pruebas

Procedimiento 01: Ejecución de Pruebas
Descripción: Las pruebas para cada uno de los requisitos seleccionados se realizarán utilizando como guía al Mobile Security Testing Guide. Estas pruebas brindarán como

resultado un listado de los requerimientos que se cumplen y los que no. Los aspectos por revisar, de los requerimientos de Mobile Application Security Verification Standard.
Pasos 1. Revisión de la documentación 2. Análisis Estático 3. Análisis Dinámico 4. Análisis Forense 5. Pruebas de Ingeniería Inversa

Fuente: Elaboración propia

- **Revisión de Documentación:** La categoría V1: Requisitos de Arquitectura, Diseño y Modelado de Amenazas, contiene requisitos que verifican si la aplicación ha sido diseñada considerando la seguridad, por tanto, no se verifica de manera técnica, sino mediante la revisión de la documentación de la aplicación móvil.

- **Análisis Estático:** La aplicación será sometida a un análisis estático mediante herramientas automatizadas propuesto por el proyecto OWASP. El resultado permitirá obtener una vista inicial de las posibles vulnerabilidades que pueda tener la aplicación, las cuales tendrán que ser verificadas manualmente para evitar falsos positivos.

- **Análisis Dinámico:** Permitirá verificar aquellos requisitos que no se hayan revisado durante el análisis estático, a través de observar el comportamiento de la aplicación.

- **Análisis Forense:** De ser requerido, permitirá verificar la correcta eliminación de los datos sensibles.

- **Pruebas de Ingeniería Inversa:** Estas pruebas se realizarán si la aplicación lo requiere según el resultado de su análisis de riesgos. Este tipo de pruebas permitirán medir la protección de la aplicación contra ataques de ingeniería inversa para obtener el código fuente.

Tabla 11: Procedimiento – Medición de protección contra riesgos

Procedimiento 02: Medición de Protección contra Riesgos
Descripción: Luego de las pruebas realizada a la aplicación móvil, se habrá obtenido una lista de aquellos requisitos que sí se cumplen en la aplicación y aquellos que no. Cada requisito verificado contribuye a la mitigación de uno o más riesgos, de manera que, si para uno de los riesgos se cumplen todos los requisitos asignados, se minimiza la probabilidad de ocurrencia de la amenaza, reduciendo también el nivel de dicho riesgo.
Pasos 1. Medición de protección contra los riesgos

Fuente: Elaboración propia

- **Medición de protección contra los riesgos:**

Tabla 12: Procedimiento – Elaboración de recomendaciones

Procedimiento 03: Elaboración de recomendaciones
Descripción: Se elaborarán recomendaciones para cada una de las vulnerabilidades encontradas.
Pasos 1. Elaborar recomendaciones de las vulnerabilidades.

Fuente: Elaboración propia

- **Elaborar recomendaciones de las vulnerabilidades:** Las recomendaciones se basan en los requisitos que no se cumplen en el proceso de análisis anterior y ocasionan que el riesgo esté presente y con nivel altos que podrían perjudicar a la aplicación o a la empresa. Se tendrá que desarrollar por cada vulnerabilidad hallada.

ELEMENTOS DE SALIDA

Como resultado del procesamiento en esta fase se obtendrá la siguiente información:

- **Fichas técnicas de verificación de requisitos de seguridad:** Las pruebas realizadas para verificar el cumplimiento de los requisitos de seguridad definidos se deberán documentar con la finalidad de respaldar los resultados.

- **Cumplimiento de Requerimientos:** Posterior de ejecutar las pruebas, se obtiene una lista de verificación con los requisitos seleccionados para la evaluación para la evaluación, indicando aquellos que si se cumplen y aquellos que no cumple. Mediante esta lista se podrá obtener un porcentaje de cumplimiento de los requisitos necesarios para la aplicación móvil.

- **Vulnerabilidades encontradas y sus riesgos:** Para cada requerimiento que no se cumple se determina que existe un riesgo. De la ejecución de todas las pruebas se realizará una lista de vulnerabilidades encontrados y que causan que el requerimiento no se cumpla.

- **Nivel de Protección contra los riesgos identificados.**

- **Recomendaciones:** Se obtendrá las recomendaciones para cada riesgo que se encuentre en noveles superiores a los aceptables por el cliente.

3.4.3.3. FASE 3: RESULTADOS DE LA EVALUACIÓN

Una vez terminada la evaluación se documentarán los trabajos realizados y se entregarán a la instancia correspondiente de la organización

ELEMENTOS DE ENTRADA

Se hará uso de los datos obtenidos de las dos fases anteriores.

Fase 1	- Datos de la aplicación móvil. - Nivel de riesgo de la aplicación. - Lista de riesgos más altos. - Lista de requisitos de seguridad.
Fase 2	- Fichas técnicas de verificación de requisitos de seguridad.

- Cumplimiento de Requerimientos. - Vulnerabilidades encontradas y sus riesgos. - Nivel de Protección contra los riesgos identificados. - Recomendaciones.

Fuente: Elaboración propia

ELEMENTOS DE PROCESAMIENTO

- Documentación del Alcance de la Evaluación.
- Documentación de la Evaluación de Requisitos de Seguridad.
- Documentación de Resultados.

ELEMENTOS DE SALIDA

Como resultado se obtendrán los siguientes documentos que serán entregados a la instancia correspondiente:

- **Informe técnico:** En este informe se establece el detalle de todos los procedimientos que se realizaron sobre las fases de evaluación de la aplicación móvil y sus resultados.

- **Informe ejecutivo:** En este informe solo se podrán los resultados de ambas fases, tanto el listado de riesgos, vulnerabilidades y el nivel de protección contra los riesgos.

CONCLUSIONES

Del proyecto realizado se concluye lo siguiente:

- El presente trabajo contribuye a la empresa ENTELGY con la propuesta de un manual de manual de procedimientos práctico de fácil uso para evaluar el nivel de seguridad de una aplicación móvil Android de manera adecuada y más optima, basándose en la metodología del OWASP en complemente con la metodología de análisis de riesgos, y cumpliendo cada uno de los puntos planteados en el objetivo.
- Mediante la explicación teórica se identificaron los requisitos de seguridad para aplicaciones móviles para plataformas Android, y que se describe en el estándar OWASP Mobile Security Verification Standard, que agrupa un conjunto de requisitos de seguridad para cada aspecto que puede tener una aplicación móvil, a diferencia del OWASP Top Ten Mobile Risk, el cual nos guía para verificar en base a los 10 riesgos más frecuentes que presentan las aplicaciones móviles. El OWASP Mobile Security Verification Standard se puede utilizar en conjunto con la guía Mobile Security Testing Guide y la lista de verificación Mobile Security Checklist, ambos pertenecientes al Proyecto OWASP. El manual emplea los requisitos de seguridad mencionados en el OWASP Mobile Security Verification Standard, el cual es seleccionado posterior a un proceso de análisis de riesgo para poder tener más claro, cuales aplicaran en la evaluación basándonos en las características del negocio del cliente, así como la misma aplicación y los riesgos más altos. Posterior a ello, podremos hacer uso del Mobile Security Testing Guide que brinda detalles como poder mitigar las amenazas que se

han identificado en la fase anterior y así ofrecer al evaluar de la empresa Entelgy una herramienta para brindar recomendaciones que serán desarrollados en los informes finales.

- En el marco jurídico se establece las principales leyes y normas aplicables a las políticas de información con el fin de tener conocimiento jurídico que aportan para el desarrollo y ejecución del proyecto propuesto y está fundamentado básicamente en los lineamientos tanto de la empresa y nacionales.
- En la metodología de desarrollo del proyecto está basado en la explicación teórica y está se encuentra dividida en: la delimitación temporal y espacio del trabajo, donde se explicó el alcance que abarco el proyecto; se determina el problema que propicia el inicio de la propuesta, basándonos en una mejora aprovechando las oportunidades de la empresa; se plantea el modelo que sostiene la propuesta basándonos en las metodología actuales para evaluar la seguridad de las aplicaciones, estructurándolo en 3 etapas o fases que planteamos en el diseño de la metodología; y para concluir se establece las pautas para desarrollar el manual de procedimientos propuesto donde se detalla cada etapa de evaluación que guiara al personal de Entelgy a realizar una correcta verificación de seguridad de acuerdo a los riesgos que esté presente o este expuesto y asociarlo a alguno de los requisitos de OWASP Mobile Security Verification Standard, el cual el resultado final nos permitirá mostrar el nivel de protección que tiene la aplicación contra los riesgos de la aplicación evaluada para beneficio del cliente.

RECOMENDACIONES

- Para futuros trabajos de investigación a la propuesta se recomienda que se pueda emplear alguna metodología de mejora continua, como el ciclo de Deming y puedan aportar a la calidad de las pruebas de seguridad.

- Como segunda recomendación, aparte de emplear en las pruebas la verificación de los requisitos de seguridad definidas en Mobile Security Testing Guide, se sugiere no solo limitarse a lo que explica esta guía propuesta, sino también adicionar en base de su experiencia y conocimientos algunas pruebas adicionales que pueda complementar si los requisitos se cumplen totalmente.

- La propuesta también se podría emplear en otra plataforma, como iOS, pero se tendrá que considerar que algunos niveles de riesgos pueden ser diferentes para cada plataforma, donde algunos requisitos varían y se tendrá que emplear un mejor análisis.

BIBLIOGRAFÍA

Cornell, D. (24 de Marzo de 2014). *Combine herramientas en las pruebas de seguridad para apps móviles*. Obtenido de https://searchdatacenter.techtarget.com/es/respuesta/Combine-herramientas-en-las-pruebas-de-seguridad-para-apps-moviles

Cuello, J., & Vittote, J. (2013). *Diseñando apps para móviles.* Catalina Duque Giraldo.

David, R. (2016). *Desarrollo de aplicaciones para Android I.* España: Ministerio de Educación, Cultura y Deporte.

Godoy Lemus, R. (2014). Seguridad de la Informacion. *Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica*, 374.

Gonzales, M. (2014). *Aplicaciones móviles en nutrición, dietética y hábitos saludables; análisis y consecuencia de una tendencia a la alza.* Madrid, España: Nutrición Hospitalaria, vol 30.

Gutierrez Amaya, C. (16 de Agosto de 2012). *Welivesecurity*. Obtenido de ¿Qué es y por qué hacer un Análisis de Riesgos?: https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

Herzog, P. (2010). *OSTMM 3 The Open Source Security Testing Methodology Manual.* ISECOM.

IDC. (14 de Septiembre de 2020). *IDC Corporate USA*. Obtenido de IDC Corporate: https://www.idc.com/promo/smartphone-market-share/os

Lizarzaburu, E., Barriga, G., Noriega, L., Luciano, L., & Mejia, P. (2017). Gestión de Riesgos Empresariales:. *Revista Espacios*, 21.

Mendoza, M. Á. (13 de Agosto de 2015). *¿Cómo medir el estado de la seguridad de la información?* Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2015/08/13/como-medir-estado-seguridad-informacion/

Mifsud, E. (26 de Marzo de 2012). *MONOGRÁFICO: Introducción a la seguridad informática*. Obtenido de http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?format=pdf

OWASP. (21 de Diciembre de 2018). *OWASP Mobile Security Testing Guide*. Obtenido de https://owasp.org/www-project-mobile-security-testing-guide/#tab=Main

OWASP. (s.f.). *OWASP mobile security*. Obtenido de https://owasp.org/www-project-mobile-security/

Ramos Ramos, J. L. (2013). PRUEBAS DE PENETRACIÓN O PENT TEST. *Revista de Información, Tecnología y Sociedad*, 8.

Ten, P. M.-T. (13 de Febrero de 2017). Obtenido de Projects/OWASP Mobile Security Project - Top Ten: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

Zambrano, R. (2012). *Técnicas de Análisis de Malware en dispositivos móviles basados en Android.* Buenos Aires, Argentina: Universidad de Buenos Aires. Facultad de Ciencias Económicas.

ANEXOS

ANEXO 01: REQUISITOS DE SEGURIDAD - ANDROID

ID	Verificación detallada de requerimientos	Nivel 1	Nivel 2
V1	**Arquitectura, Diseño y Modelado de Amenazas**		
1.1	Todos los componentes se encuentran identificados y asegurar que son necesarios.	✓	✓
1.2	Los controles de seguridad nunca se aplican sólo en el cliente, sino que también en los respectivos servidores.	✓	✓
1.3	Se definió una arquitectura de alto nivel para la aplicación y los servicios y se incluyeron controles de seguridad en la misma.	✓	✓
1.4	Se identificó claramente la información considerada sensible en el contexto de la aplicación móvil.	✓	✓
1.5	Todos los componentes de la aplicación están definidos en términos de la lógica de negocio o las funciones de seguridad que proveen.		✓
1.6	Se realizó un modelado de amenazas para la aplicación móvil y los servicios en el que se definieron las mismas y sus contramedidas.		✓
1.7	Todos los controles de seguridad poseen una implementados centralizada.		✓
1.8	Existe una política explícita sobre el uso de claves criptográficas (si se usan) a través de todo su ciclo de vida. Idealmente siguiendo un estándar de gestión de claves como el NIST SP 800-57.		✓
1.9	Existe un mecanismo para forzar las actualizaciones de la aplicación móvil.		✓
1.10	La implementación de medidas de seguridad es una parte esencial durante todo el ciclo de vida del desarrollo de software de la aplicación.		✓
1.11	Existe una política de divulgación responsable y es llevada a cabo adecuadamente.		✓
1.12	La aplicación debería de cumplir con las leyes y regulaciones de privacidad.	✓	✓
V2	**Almacenamiento de datos y la Privacidad**		
2.1	Las funcionalidades de almacenamiento de credenciales del sistema deben de ser utilizadas para almacenar información sensible, tal como información personal, credenciales de usuario o claves criptográficas.	✓	✓
2.2	No se debe almacenar información sensible fuera del contenedor de la aplicación o del almacenamiento de credenciales del sistema.	✓	✓
2.3	No se escribe información sensible en los registros (logs) de la aplicación.	✓	✓
2.4	No se comparte información sensible con servicios externos salvo que sea una necesidad de la arquitectura.	✓	✓
2.5	Se desactiva la caché del teclado en los campos de texto que contienen información sensible.	✓	✓
2.6	No se expone información sensible mediante mecanismos de comunicación entre procesos (IPC).	✓	✓
2.7	No se expone información sensible como contraseñas y números de tarjetas de crédito a través de la interfaz o capturas de pantalla.	✓	✓
2.8	No se incluye información sensible en las copias de seguridad generadas por el sistema operativo.		✓
2.9	La aplicación elimina toda información sensible de la vista cuando la aplicación pasa a un segundo plano.		✓
2.10	La aplicación no conserva ninguna información sensible en memoria más de lo necesario y la memoria se limpia trás su uso.		✓
2.11	La aplicación obliga a que exista una política mínima de seguridad en el dispositivo, como que el usuario deba configurar un código de acceso.		✓
2.12	La aplicación educa al usuario acerca de los tipos de información personal que procesa y de las mejores prácticas en seguridad que el usuario debería seguir al utilizar la aplicación.		✓
2.13	No se guarda ningún tipo de información sensible de forma local en el dispositivo móvil. En su lugar, esa información debería ser obtenida desde un sistema remoto sólo cuando es necesario y únicamente residir en memoria.		✓
2.14	En caso de ser necesario guardar información sensible de forma local, ésta debe de ser cifrada usando una clave derivada del hardware de almacenamiento seguro, el cual debe requerir autenticación previa.		✓
2.15	El almacenamiento local de la aplicación debe de ser borrado trás un número excesivo de intentos fallidos de autenticación.		✓
V3	**Criptografía**		
3.1	La aplicación no depende únicamente de criptografía simétrica cuyas claves se encuentran directamente en el código fuente de la misma.	✓	✓
3.2	La aplicación utiliza implementaciones de criptografía probadas.	✓	✓
3.3	La aplicación utiliza primitivas de seguridad que son apropiadas para el caso particular y su configuración y parámetros siguen las mejores prácticas de la industria.	✓	✓
3.4	La aplicación no utiliza protocolos o algoritmos criptográficos ampliamente considerados obsoletos para su uso en seguridad.	✓	✓
3.5	La aplicación no reutiliza una misma clave criptográfica para varios propósitos.	✓	✓
3.6	Los valores aleatorios son generados utilizando un generador de números aleatorios suficientemente seguro.	✓	✓
V4	**Autenticación y Manejo de Sesiones**		
4.1	Si la aplicación provee acceso a un servicio remoto, un mecanismo aceptable de autenticación como usuario y contraseña es realizado en el servidor remoto.	✓	✓
4.2	Si se utiliza la gestión de sesión por estado, el servidor remoto usa tokens de acceso aleatorios para autenticar los pedidos del cliente sin requerir el envío de las credenciales del usuario en cada uno.	✓	✓
4.3	Si se utiliza la autenticación basada en tokens sin estado, el servidor proporciona un token que se ha firmado utilizando un algoritmo seguro.	✓	✓
4.4	Cuando el usuario cierra sesión se termina la sesión también en el servidor.		
4.5	Existe una política de contraseñas y es aplicada en el servidor.	✓	✓
4.6	El servidor implementa mecanismos, cuando credenciales de autenticación son ingresadas una cantidad excesiva de veces.	✓	✓
4.7	Las sesiones y los tokens de acceso expiran luego de un tiempo predefinido de inactividad.	✓	✓
4.8	La autenticación biométrica, si la hay, no está asociada a eventos (p. ej. usando una API que simplemente retorna "true" o "false"), sino basada en el desbloqueo del keychain/keystore (almacenamiento seguro).		✓
4.9	El sistema remoto implementa un mecanismo de segundo factor de autenticación (2FA) y lo impone consistentemente.		✓
4.10	Para realizar transacciones críticas se requiere una autenticación adicional (step-up).		✓
4.11	La aplicación informa al usuario acerca de todas las actividades sensibles en su cuenta. El usuario es capaz de ver una lista de los dispositivos conectados, información contextual (dirección IP, localización, etc.), y es capaz de bloquear ciertos dispositivos.		✓
4.12	Los modelos de autorización deberían de ser definidos e impuestos por el sistema remoto.	✓	✓

V5	**Comunicación a través de la red**		
5.1	La información es enviada cifrada utilizando TLS. El canal seguro es usado consistentemente en la aplicación.	✓	✓
5.2	Las configuraciones del protocolo TLS siguen las mejores prácticas de la industria, o lo hacen lo mejor posible en caso de que el sistema operativo del dispositivo no soporte los estándares recomendados.	✓	✓
5.3	La aplicación verifica el certificado X.509 del sistema remoto al establecer el canal seguro y sólo se aceptan certificados firmados por una CA de confianza.	✓	✓
5.4	La aplicación utiliza su propio almacén de certificados o realiza _pinning_ del certificado o la clave pública del servidor. Bajo ningún concepto establecerá conexiones con servidores que ofrecen otros certificados o claves, incluso si están firmados por una CA de confianza.		✓
5.5	La aplicación no depende de un único canal de comunicaciones inseguro (email o SMS) para operaciones críticas como registro de usuarios o recuperación de cuentas.		✓
5.6	La aplicación sólo depende de bibliotecas de conectividad y seguridad actualizadas.		✓
V6	**Interacción con la Plataforma**		
6.1	La aplicación requiere la cantidad de permisos mínimamente necesaria.	✓	✓
6.2	Todo dato ingresado por el usuario o cualquier fuente externa debe ser validado y, si es necesario, saneado. Esto incluye información recibida por la UI o mecanismos IPC como los Intents, URLs y datos provenientes de la red.	✓	✓
6.3	La aplicación no expone ninguna funcionalidad sensible a través esquemas de URL salvo que dichos mecanismos estén debidamente protegidos.	✓	✓
6.4	La aplicación no expone ninguna funcionalidad sensible a través de mecanismos IPC salvo que dichos mecanismos estén debidamente protegidos.	✓	✓
6.5	JavaScript se encuentra deshabilitado en los WebViews salvo que sea necesario.	✓	✓
6.6	Las WebViews se configuran para permitir el mínimo de los esquemas (idealmente, sólo https). Esquemas peligrosos como file, tel y app-id están deshabilitados.	✓	✓
6.7	Si objetos nativos son expuestos en WebViews, debe verificarse que cualquier componente JavaScript se carga exclusivamente desde el contenedor de la aplicación.	✓	✓
6.8	La serialización de objetos, si se realiza, debe implementarse utilizando API seguras.	✓	✓
6.9	La aplicación se protege contra ataques de tipo screen overlay. (sólo Android)		✓
6.10	La caché, el almacenamiento y los recursos cargados (JavaScript, etc.) de las WebViews deben de borrarse antes de destruir la WebView.		✓
6.11	Verificar que la aplicación impide el uso de teclados de terceros siempre que se introduzca información sensible.		✓
V7	**Calidad de Código y Configuración del Compilador**		
7.1	La aplicación es firmada y provista con un certificado válido, cuya clave privada está debidamente protegida.	✓	✓
7.2	La aplicación fue publicada en modo release y con las configuraciones apropiadas para el mismo (por ejemplo, non-debuggable).	✓	✓
7.3	Los símbolos de depuración fueron eliminados de los binarios nativos.	✓	✓
7.4	Cualquier código de depuración y/o de asistencia al desarrollador (p. ej. código de test, backdoors, configuraciones ocultas) debe ser eliminado. La aplicación no hace logs detallados de errores ni de mensajes de depuración.	✓	✓
7.5	Todos los componentes de terceros se encuentran identificados y revisados en cuanto a vulnerabilidades conocidas.	✓	✓
7.6	La aplicación captura y gestiona debidamente las posibles excepciones.	✓	✓
7.7	Los controles de seguridad deniegan el acceso por defecto.	✓	✓
7.8	En código no administrado, la memoria es solicitada, utilizada y liberada de manera correcta.	✓	✓
7.9	Las funcionalidades de seguridad gratuitas de las herramientas, tales como minificación del byte-code, protección de la pila, soporte PIE y conteo automático de referencias, se encuentran activadas.	✓	✓

V8	**Resistencia ante la Ingeniería Inversa**	**R**
	Impedir el Análisis Dinámico y la Manipulación	
8.1	La aplicación detecta y responde a la presencia de un dispositivo rooteado, ya sea alertando al usuario o finalizando la ejecución de la aplicación.	✓
8.2	La aplicación impide la depuración o detecta y responde a la misma. Se deben cubrir todos los protocolos de depuración.	✓
8.3	La aplicación detecta y responde a cualquier modificación de ejecutables y datos críticos de la propia aplicación.	✓
8.4	La aplicación detecta la presencia de herramientas de ingeniería inversa o frameworks comunmente utilizados.	✓
8.5	La aplicación detecta y responde a ser ejecutada en un emulador.	✓
8.6	La aplicación detecta y responde ante modificaciones de código o datos en su propio espacio de memoria.	✓
8.7	La aplicación implementa múltiples mecanismos de detección para los puntos del 8.1 al 8.6. Nótese que, a mayor cantidad y diversidad de mecanismos usados, mayor será la resistencia.	✓
8.8	Los mecanismos de detección provocan distintos tipos de respuestas, incluyendo respuestas retardadas y silenciosas.	✓
8.9	La ofuscación se aplica a las defensas del programa, lo que a su vez impide la desofuscación mediante análisis dinámico.	✓
	Atadura del Dispositivo	
8.10	La aplicación implementa un “enlace al dispositivo” utilizando una huella del dispositivo derivado de varias propiedades únicas al mismo.	✓
	Impedir la comprensión	
8.11	Todos los archivos ejecutables y bibliotecas correspondientes a la aplicación se encuentran cifrados, o bien los segmentos importantes de código se encuentran cifrados o "empaquetados" (packed). De este modo cualquier análisis estático trivial no revelará código o datos importantes.	✓
8.12	Si el objetivo de la ofuscación es proteger código propietario, debe utilizarse un esquema de ofuscación apropiado para la tarea particular y robusto contra métodos de desofuscación manual y automatizada, considerando la investigación actual publicada. La eficacia del esquema de ofuscación debe verificarse mediante pruebas manuales. Nótese que, siempre que sea posible, las características de aislamiento basadas en hardware son preferibles a la ofuscación.	✓
	Impedir el Eavesdropping	
8.13	A modo de defensa en profundidad, además de incluir un refuerzo (hardening) sólido de la comunicación, puede implementarse el cifrado de datos (payloads) a nivel de aplicación como medida adicional contra ataques de eavesdropping.	✓

ANEXO 02: ENTREVISTA REALIZADA

UNIVERSIDAD NACIONAL TECNOLOGIA DE LIMA SUR

FACULTAD DE INGENIERA Y GESTION

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

Entrevista dirigida al jefe del área de ciberseguridad

Objetivo General: Identificar la situación actual de la empresa Entelgy con respecto a la evaluación de seguridad de aplicaciones móviles Android de sus clientes.

Preguntas

Planificación

1. Previo a una evaluación de seguridad de aplicación móvil. ¿Se realiza algún análisis que permite determinar el nivel de seguridad que debería tener la aplicación?
2. ¿Siempre aplican los mismos requisitos de seguridad para todas las aplicaciones móviles?
3. ¿El cliente es el que define los criterios para evaluar su aplicación móvil?
4. ¿Bajo qué metodologías o estándares internacionales están realizando sus evaluaciones de seguridad en aplicaciones móviles?

Evaluación

5. En promedio ¿Cuántos días demora evaluar la seguridad de una aplicación móvil?
6. ¿Cómo califican los hallazgos que se encuentran en la evaluación?

Informe de resultados

7. ¿Las recomendaciones son elaborados para todas las vulnerabilidades, incluyendo las menos relevantes?

ANEXO 03: FORMULARIO 01 - DATOS DE LA EMPRESA Y LA APLICACIÓN MOVIL

FORM 01: DATOS DE LA EMPRESA Y LA APLICACIÓN MOVIL	
DATOS DE LA EMPRESA	
MISION	
VISION	
Rubro de la empresa:	
Servicios y/o actividades	
Otros datos relevantes	
DATOS DE LA APLICACIÓN	
Nombre de la Aplicación	
Nombre del Paquete	
Versión de la Aplicación	
Tamaño de la Aplicación	
Ultima Actualización	
Versión min. Soportado (Android)	
Objetivo de la Aplicación	
Usuarios de la aplicación	
Mapa de Navegación	
Permisos solicitados	
Otros	

ANEXO 04: FORMULARIO 02 - ANALISIS DE CONTEXTO

FORM 02: ANALISIS DE CONTEXTO	
Procesamiento	
Analisis de la Misión, Visión y Objetivos:	¿El objetivo de la aplicación esta alineado con la misión, visión de la empresa?
	SI/NO
Identificación de la Normativa	
Categoría de la Aplicación Móvil	

ANEXO 05: FORMULARIO 03 - IDENTIFICACION DE AMENAZAS

FORM 03: IDENTIFICACION DE AMENAZAS					
Procesamiento					
Identificación y valoración de activos					Identificación de Amenazas por cada elemento clave
Lista de Opciones	Información	Sensibilidad	Servicios	Criticidad	

ANEXO 06: FORMULARIO 04 - ANALISIS Y EVALUACION DE RIESGOS

FORM 04: ANALISIS Y EVALUACION DE RIESGOS							
Procesamiento							
Analisis de Riesgo							Evaluación de Riesgos
Amenazas	Probabilidad		Impacto		Nivel de Riesgo		Selección de los riesgos mas Altos
Amenaza 01		0		0		0	
Amenaza 02		0		0		0	
Amenaza 03		0		0		0	
					Sumatoria de Riesgos	0	
					Nivel de Riesgo Potencial Promedio		
						0	