UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Informe sobre la seguridad y vulnerabilidad de las aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas.
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable.
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor:
Ing. Zaruma Sanchez Edison Giovanny
Tutor:
Msc. Toasa Guachi Renato Mauricio PhD. Urdaneta Herrera Maryory

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Msc. Toasa Guachi Renato Mauricio con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Informe sobre la seguridad y vulnerabilidad de las aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas.

Elaborado por: Edison Giovanny Zaruma Sanchez, de C.I: 1724198617, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO TOASA GUACHI

_____

Mg. Toasa Guachi Renato Mauricio

ORCID:0000-0002-2138-300X

APROBACIÓN DEL TUTOR

Yo, PhD Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Informe sobre la seguridad y vulnerabilidad de las aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas.

Elaborado por: Edison Giovanny Zaruma Sanchez, de C.I: 1724198617, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

PhD Urdaneta Herrera Maryory

ORCID:0000-0001-8773-53

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Edison Giovanny Zaruma Sanchez con C.I: 1724198617, autor/a del proyecto de titulación denominado: Informe sobre la seguridad y vulnerabilidad de las aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.

3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2024

Firma
Orcid: 0009-0002-9329-9533

Tabla de contenidos

APROBACIÓN DEL TUTOR II
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE IV
INFORMACIÓN GENERAL 4
Contextualización del tema 4
Problema de investigación 5
Objetivo general 6
Objetivos específicos 6
Vinculación con la sociedad y beneficiarios directos: 6
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO 8
1.1 Contextualización general del estado del arte 5
1.2 Proceso investigativo metodológico 6
1.2.1 Metodología de investigación Mixta 9
1.2.2 Tipo de investigación 10
1.2.2.1 Investigación descriptiva 10
1.2.2.2 Investigación no experimental 10
1.2.3. Población 10
1.2.4. Muestra 11
1.3 Análisis de resultados 8
1.3.1 Encuesta 12
1.3.2 Análisis de la entrevista 16
CAPÍTULO II: PROPUESTA 17
2.1. Fundamentos teóricos aplicados 17
2.2. Descripción de la propuesta 21
2.3 Validación de la propuesta 24
2.4 Matriz de articulación de la propuesta 26
CONCLUSIONES 28
RECOMENDACIONES 29
REFERENCIAS BIBLIOGRÁFICAS 1
ANEXOS 4

Índice de tablas

Tabla 1: Calculo de la muestra 11
Tabla 2: Sistemas operativos..... 12
Tabla 3:Banca móvil 13
Tabla 4: Seguridad de banca móvil 14
Tabla 5: Conocer sobre la seguridad de la banca móvil..... 15
Tabla 6: Matriz comparativa de Android e iOS 23
Tabla 7: Matriz de articulación..... 26

Índice de figuras

Figura 1: Sistemas operativos 12
Figura 2: Banca móvil 13
Figura 3: Seguridad de Banca móvil 14
Figura 4: Conocer sobre la seguridad de la banca móvil 15
Figura 5: Diagrama de arquitectura de Android 18
Figura 6: Diagrama de arquitecturta iOS 19
Figura 7: Estructura de la propuesta 22

INFORMACIÓN GENERAL

Contextualización del tema

El hacking ético es esencial para la evolución de las empresas, desde la funcionalidad básica hasta la seguridad de sus sistemas. Este artículo proporciona un análisis preliminar de los conceptos y características de un dispositivo móvil, los diversos riesgos a los que está expuesto y las vulnerabilidades que se deben conocer para realizar un hacking ético. (Baquero y Hernandez,2018).

El hacking ético no solo se enfoca en áreas sensibles como secretos comerciales de empresa y datos confidenciales de los clientes. También se enfoca en descubrir fallas en sistemas e infraestructuras digitales, como errores de software, evaluar los riesgos de seguridad y participar de manera constructiva en la corrección de fallas de seguridad descubiertas. (IONOS, 2024).

Evaluar la seguridad informática e identificar fallas en sistemas, redes o infraestructuras. Para ello, utilizan las mismas habilidades, métodos y técnicas que los hackers convencionales, por lo que, en lugar de aprovechar cualquier vulnerabilidad que descubran para beneficio personal, los hackers éticos las documentan y brindan asesoramiento sobre cómo remediarlas para que las organizaciones puedan fortalecer su seguridad informática. (España, 2024).

Hoy en día es innegable que los dispositivos móviles han tomado una posición protagónica en el día a día de las personas y están muy arraigados en sus rutinas y hábitos. Debido a la distribución masiva de estos dispositivos técnicos tanto en entornos personales como en los lugares de trabajo de las organizaciones, existe una mayor conciencia de la necesidad imperante de investigar cuidadosamente tanto los eventos relacionados como los posibles problemas de seguridad emergentes.

Los problemas de seguridad que rodean a estos dispositivos son notablemente similares a los de las computadoras tradicionales. Sin embargo, esta comparación sigue siendo insuficiente si tenemos en cuenta el complicado hecho inherente al campo de los dispositivos móviles: su amplia y diversa base de usuarios, que los conecta a diferentes contextos y escenarios, abarcando tanto el trabajo profesional como lo personal (Bergman,2018).

La exposición natural a la comunidad de usuarios, que aumenta la prevalencia de su uso en múltiples contextos, otorga a estos dispositivos una vulnerabilidad adicional, aumentando las amenazas potenciales a su integridad y seguridad. En este sentido, el entorno laboral y el ámbito personal confluyen en una simbiosis compleja, donde las interacciones diarias con estos dispositivos pueden actuar como vector de ataque o fuente de fugas sensibles que pueden desencadenar un efecto dominó con consecuencias no deseadas.

En definitiva, el dispositivo móvil en la vida actual ha dado lugar a una profunda reflexión en las organizaciones, lo que les ha llevado a considerar detenidamente tanto los aspectos accidentales como las posibles circunstancias relacionadas con la seguridad. Las similitudes inherentes en los desafíos de seguridad en comparación con las computadoras tradicionales adquieren matices únicos debido a la combinación de usuarios y escenarios en los que operan estos dispositivos, lo que agrega complejidad y desafíos a la investigación de seguridad. (Scambray,2018)

La importancia de proteger software y redes ayuda a prevenir ciberataques fortaleciendo toda la estructura interna de los sistemas y los servidores de las empresas antes de que alguien pueda acceder al sistema y poner en peligro a una organización. Por lo tanto, contar con el servicio de un hacker ético para testear y brindar seguridad a todos los clientes que proporcionen información confidencial para realizar transacciones con la empresa en cuestión.

Las entidades financieras y las empresas que fabrican y producen nuevos productos, como software, plataformas o aplicaciones, están obligadas a cumplir con las regulaciones para probar sus productos, por lo que es crucial contar con el servicio de un hacker ético para testear y poder brindar seguridad a todos los clientes o personas que proporcionen algún tipo de información confidencial para realizar una transacción con la empresa en cuestión. (Servnet, 2024).

La tecnología continúa avanzando y, por supuesto, los métodos de infiltración en los sistemas de ciberseguridad se están actualizando y mejorando para concretar sus amenazas. Por lo tanto, los sistemas deben probarse continuamente para resistir ataques y mantener la confianza.

Problema de investigación

En la actualidad, las aplicaciones móviles presentan vulnerabilidades de seguridad en el sistema de servicios financieros lo que están poniendo en riesgo los datos confidenciales, el acceso a los servicios de back-end, almacenamiento de datos inseguros, fuga de datos no intencionados, cifrado débil y más se encontraron en las aplicaciones de banca, tarjeta de crédito y pagos móviles (Orrous, 2019).

Las aplicaciones probadas actualmente carecen de protecciones de código binario, fuga de datos involuntaria, un cifrado débil, lo que potencialmente permite a los atacantes descifrar datos confidenciales, además las vulnerabilidades que presentan los sistemas operativos Android e IOS y el uso de la aplicación de la banca móvil se ve como un riesgo latente a los usuarios. (Orrous, 2019).

En el ámbito informático, se encuentran vulnerabilidades en el aspecto de seguridad de las diferentes aplicaciones, más aún en la banca móvil ya que trata de las finanzas de cada persona, esto podría deberse a la falta de conocimiento de los usuarios de la seguridad que ofrecen los sistemas operativos moviles Android e iOS para la banca móvil y como usarla de forma segura para mitigar amenazas.

Pregunta

¿Por qué realizar un informe de seguridad para Aplicaciones Bancarias Móviles en Sistemas móviles Android e iOS mediante Ethical Hacking, para mitigar amenazas?

Objetivo general

Elaborar un informe de seguridad y vulnerabilidad en aplicaciones móviles bancarias con sistema operativo Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas.

Objetivos específicos

- Conceptualizar fundamentos teóricos de bancas móviles, sistemas operativos Android e iOS para identificar vulnerabilidad en el sistema informático.
- Diagnosticar la situación actual de la aplicación banca móvil, mediante Ethical Hacking para proporcionar medidas de seguridad.
- Elaborar informe sobre seguridad y vulnerabilidad de aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas
- Validar el informe con un experto en seguridad informática para obtener su opinión sobre la viabilidad y efectividad de la propuesta con el documento de validación.

Vinculación con la sociedad y beneficiarios directos:

La vinculación con la sociedad es para un grupo de personas que cuentan con una banca móvil de; bancos, cooperativas y pequeñas empresas de microcrédito más relevantes en la ciudad de Quito, quienes directamente serán los beneficiarios de la elaboración del informe de seguridad de las aplicaciones bancarias en los sistemas operativos Android e iOS mediante

técnicas de Ethical Hacking, ya que al presentar un informe de las debilidades y beneficios que tiene los respectivos sistemas, el usuario de la banca móvil podrá elegir la mejor opción, también habrá beneficiarios indirectos como los demás grupos de trabajo y sus familias debido al conocimiento que adquieren, el grupo directamente beneficiario recomendara el uso correcto para la aplicación de las bancas móviles.

Al realizar el informe de seguridad sobre las aplicaciones bancarias móviles mediante técnicas de Ethical Hacking, se protege el dinero y los datos personales de los usuarios, se fortalece la confianza en la banca digital, se previenen ciberataques a gran escala, se promueven buenas prácticas de seguridad y se reduce el riesgo de delitos financieros, lo que beneficia a la sociedad en general, identifica y corregir posibles vulnerabilidades en las aplicaciones bancarias móviles, se protege el dinero y los datos personales de los usuarios contra posibles robos o fraudes cibernéticos, de esta manera el proyecto se vincula en beneficio a la sociedad.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

La seguridad en dispositivos móviles es un tema cada vez más relevante debido al aumento en el uso de smartphones y tablets en todo el mundo.

1.1. Contextualización general del estado del arte

En su proyecto Análisis de aplicaciones móviles basadas en Android, utilizadas en la banca electrónica de Ecuador, el autor José Luis Palacios menciona en el análisis de aplicaciones A, B y C que se requiere un mayor control sobre el proceso de desarrollo de aplicaciones móviles debido a las deficiencias actuales como la inclusión de datos de clientes en el código de aplicación, el firmado de la aplicación mediante el uso de la firma digital o el uso de la firma digital. Todo esto puede contener información confidencial.

En el estudio realizado por Helene Aguirre Mindeguia en el 2018, con el tema Ciberseguridad en aplicaciones móviles bancarias menciona que el análisis reveló que todos los bancos tenían fallas en sus aplicaciones oficiales, principalmente debido a errores en el código. La vulnerabilidad más frecuente fue la inyección potencial de SQL.

El autor Andrade Toscano en el 2019, en su estudio titulado Análisis de la Seguridad de Aplicaciones Móviles Bancarias, menciona: Con el análisis realizado con Wireshark, tenemos una mejor comprensión de cómo se crea el tráfico entre el cliente final y el servidor bancario. Debido a la gran cantidad de tráfico en tiempo real entre el cliente y el servidor, la banca digital puede detectar errores en el tráfico de datos (retransmisión y segmentos no capturados) que son comunes en estas aplicaciones.

En su tesis el autor Bravo Duarte en el 2019, con su título Análisis de la Seguridad de Aplicaciones Móviles Bancarias, menciona que: Este análisis muestra que un 44% de las aplicaciones analizadas utilizan tecnologías biométricas y que cada una de las aplicaciones utiliza una versión más actualizada de Android. Después de analizar estas aplicaciones con el plugin FindBugs, no se encontraron muchos errores, lo que da al usuario una cierta seguridad y confiabilidad de estas aplicaciones.

Según David Gonzales Morte en el año 2019, realizó un estudio de dispositivos móviles, vulnerabilidades y auditoria de seguridad en aplicaciones móviles, en el cual, menciona: Que uno de los principales problemas localizados en cuanto a los dispositivos del sistema operativo

iOS es la duración de la batería, mientras que en el sistema Android hay diferentes versiones, pero el cual también tiene falencias.

En su estudio Santiago Rodríguez en el 2020, con el tema La administración y gestión del riesgo en el giro de negocio bancario frente a un ecosistema delincuencial mixto menciona que: La utilización de Internet no tiene una conciencia adecuada por parte de los usuarios, comienza la dependencia hacia los proveedores sin establecer medidas de seguridad adecuadas y la información se empieza almacenar en dispositivos extraíbles con pocas medidas de seguridad. Ante este desarrollo, los ciberdelincuentes comienzan a buscar vulnerabilidades.

El autor Héctor Pauta Martillo en el 2020, en su estudio titulado Auditoria de seguridad a aplicaciones en iOs y Android menciona que: La descarga diaria de aplicaciones móviles desde sitios oficiales o no oficiales ha provocado un aumento exponencial de amenazas y malware destinados a dispositivos móviles, especialmente para las plataformas más populares como iOS y Android. Investigaciones recientes indican que las aplicaciones son susceptibles a ataques cibernéticos.

Según el autor Marcelo Lozano publicado en el 2022, con el tema Aplicaciones críticas bancarias menciona que: La seguridad y privacidad de los datos financieros es de suma importancia en las finanzas integradas, ya que se están compartiendo datos financieros entre diferentes proveedores que brindan servicios. Las empresas que ofrecen servicios financieros integrados deberian implementar medidas de seguridad más adecuadas para garantizar que la data financiera de los clientes estén protegidos y no se utilicen de manera indebida.

1.2. Proceso investigativo metodológico

El proyecto "Seguridad en Dispositivos Móviles" se llevó a cabo mediante una investigación de tipo mixta, descriptivo, no experimental que tuvo como objetivo recopilar, analizar información de las principales amenazas y vulnerabilidades de seguridad en dispositivos móviles, así como las herramientas y medidas de seguridad disponibles para mitigar estos riesgos.

1.2.1 Metodología de investigación Mixta

Una investigación mixta se basa tanto investigación cuantitativa como cualitativa y de esta manera provee una aproximación holística que combina y analiza datos estadísticos con perspectivas contextualizadas a un nivel más profundo. Los métodos de investigación son un elemento clave para la construcción de un conocimiento válido sobre un fenómeno particular,

por lo que conocer en qué consisten, cuáles son sus características y de qué depende la elección de uno u otro resulta fundamental para todo investigador (Sánchez, 2023).

La metodología de trabajo utilizada en este proyecto se basó en un enfoque de investigación mixta, que combinó tanto la recopilación y análisis de datos cuantitativos como cualitativos. Se aplicó un análisis estadístico descriptivo para los datos cuantitativos, mientras que se utilizó el análisis de contenido para los datos cualitativos obtenidos a partir de las entrevistas y las observaciones. Se utilizó software especializado para el análisis de los datos cuantitativos, así como para la elaboración de gráficos y tablas que permitieran una visualización clara y precisa de los resultados obtenidos.

1.2.2 Tipo de investigación

1.2.2.1. Investigación descriptiva

Aquel que busca comprender la realidad utilizando un lenguaje formal para recopilar información y registrando el mundo mediante herramientas conceptuales, sin necesariamente obtener respuestas al porqué de las cosas, sino estudiar la proporción en la que se dan. (Naturales, 2021)

1.2.2.2. Investigación no experimental

Es una investigación no experimental, las variables no se manipulan y solo se observa el fenómeno en un contexto natural para luego proceder con el análisis.

Por lo tanto, este proyecto se basa en una investigación descriptiva ya que se describa cada una de las ventajas y desventajas de los sistemas operativos mediante mediante Ethical Hacking y no experimental porque no se manipularán los datos, sino más bien se darán a conocer las falencias de dichos sistemas Android e iOS.

1.2.3. Población

Es un conjunto de elementos con unas características similares sobre el cual se pretende hacer un estudio estadístico que puede ser un grupo de personas, grupo de productos defectuosos que se quieren examinar, grupo de animales que se pretenden investigar (Balderix, 2024).

Por lo antes expuesto, la investigación se realizará a las personas que cuenten con una banca móvil en el área de desarrollo que utilizan el sistema operativo Android e iOS para realizar un análisis de seguridad mediante Ethical Hacking

1.2.4 Muestra

La muestra es un subconjunto que se extrae de una población, por lo tanto, en este proyecto se trabajará con parte de la población quienes serán los encuestados para obtener resultados.

Parámetros:

n = Tamaño de muestra buscado
N = Tamaño de la Población o Universo
Z = Parámetro estadístico que depende el Nivel de Confianza
e = Erro de estimación máximo aceptado
p = Probabilidad de que ocurra el evento estudiado (éxito)
q = (1 – p) = Probabilidad de que no ocurra el evento estudiado

Tabla 1.

Calculo de la muestra

Parámetro	Valor
N	1000
Z	1,96
p	50%
q	50%
e	3%

$$\boldsymbol{n} = \frac{N * Z_{\alpha}^{2} * p * q}{e^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

Tamaño de muestra "n" = 100

En la tabla 1, se evidencia el tamaño de la muestra

Después de obtener el tamaño de la muestra se realizará una encuesta a las personas que utilizan la aplicación banca móvil de: Bancos, Cooperativas y microempresas de crédito más sobresalientes de la ciudad de Quito, para medir que conocen sobre la seguridad de la aplicación de banca móvil y en qué sistema operativo utilizan iOS o Android, mientras que la entrevista se lo aplicara a un experto en sistemas el Señor Ing. Franklin Tandalia, quien con sus respuestas ayudara a la validación de la propuesta.

1.3. Análisis de resultados

1.3.1. Encuesta

La siguiente encuesta se lo realizo a 100 personas utilizan la aplicación banca móvil de: Bancos, Cooperativas y microempresas de crédito más sobresalientes de la ciudad de Quito.

1. ¿Usted con cuál de los siguientes sistemas operativos cuenta?

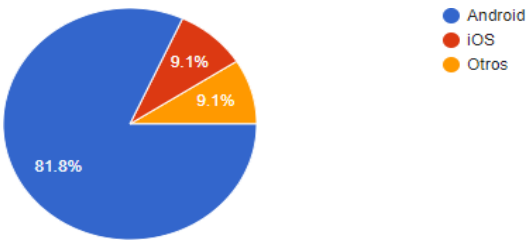
Tabla 2.

Sistemas operativos

Opciones	Porcentaje	Total
Android	81.8%	100%
iOS	9.1%	
Otros	9.1%	

Figura 1.

Sistemas operativos



En la Figura 1 se puede observar que, el 81.8% se encuentra sistema Android, el 9.1% por el sistema iOS y el 9.1 por otros sistemas operativos móviles

Análisis de resultados

Con la data obtenida, podemos ver que el 81.8% de los encuestados cuenta con un dispositivo Android, mientras que solo el 9.1% utiliza iOS y otro 9.1% utiliza otros sistemas operativos. Este análisis sugiere una popularidad por Android entre los encuestados, por otro lado, iOS y otros sistemas operativos parecen tener una base de usuarios más pequeña en esta muestra específica.

2.- ¿Usted cuenta con la banca móvil?

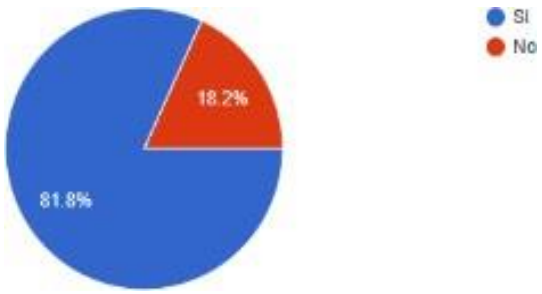
Tabla 3.

Banca móvil

Opciones	**Porcentaje**	**Total**
Si	81.8%	100%
No	18.2%	

Figura 2:

Banca móvil



En la Figura 2 se puede observar que, el 81.8% posee banca móvil, el 18.2% no posee banca móvil dentro de sus dispositivos móviles.

Análisis de resultados

En la tabla se puede observar que el 81.8% de los encuestados cuenta con banca móvil, mientras que el 18.2% no la utiliza. Esto sugiere que la mayoría de los encuestados han adoptado la banca móvil como una forma de gestionar sus finanzas.

3.- ¿Conoce usted sobre la seguridad de su banca móvil en el sistema Android o iOS?

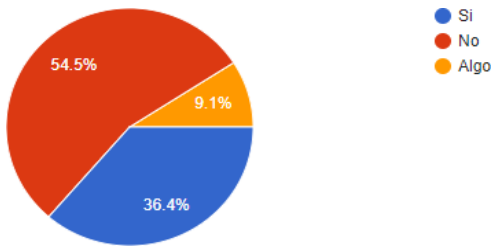
Tabla 4.

Seguridad de banca móvil

Opciones	Porcentaje	Total
Si	36,4%	100%
No	54,5%	
Algo	9,1%	

Figura 3.

Seguridad de Banca móvil



En la Figura 3 se puede observar que, el 36.4% si conoce sobre seguridad móvil, el 9.1% conoce un poco del tema y el 54.5% no conoce de seguridad en banca móvil

Análisis de resultados

En base a los resultados, se observa que 54.5% indica que no tiene conocimiento sobre la seguridad de su banca móvil mientras que el 36.4% de los encuestados afirma conocer en los sistemas Android e iOS. Solo el 9.1% tiene un conocimiento parcial sobre este tema, por lo tanto, la información que tienen los usuarios es insuficiente sobre las medidas de seguridad implementadas en las aplicaciones bancarias móviles y los sistemas operativos.

5.- Le gustaría conocer sobre la seguridad de su banca móvil en el sistema Android e iOS.

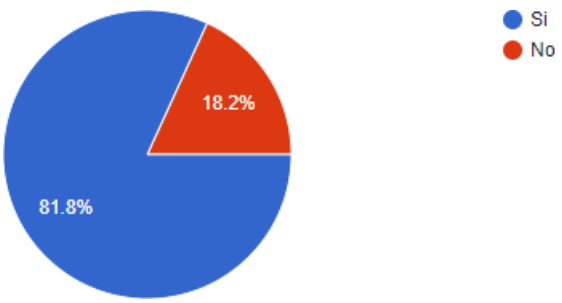
Tabla 5.

Conocer sobre la seguridad de la banca móvil

Opciones	Porcentaje	Total
Si	81,8%	100%
No	18,2%	

Figura 4.

Conocer sobre la seguridad de la banca móvil



En la Figura 4 se puede observar que, el 81.8% se encuentra sistema Android, el 9.1% por el sistema iOS y el 9.1 por otros sistemas operativos móviles

Análisis de resultados

Con los datos proporcionados, el 81.8% de los encuestados estaría interesado en conocer sobre la seguridad de su banca móvil en los sistemas Android e iOS, mientras que el 18.2% restante no tiene interés en este tema, por lo tanto, sería beneficioso proporcionar información detallada y accesible sobre la seguridad de la banca móvil en Android e iOS para satisfacer la demanda de conocimientos en este campo y ayudar a los usuarios a tomar decisiones informadas sobre su seguridad en línea.

1.3.2 Análisis de la entrevista

La siguiente entrevista se la aplicó a un experto en sistemas el Señor Ing. Franklin Tandalia, quien con sus respuestas ayudó a medir la seguridad de la banca móvil en los sistemas operativos Android e iOS y la validación de la propuesta.

Según las respuestas obtenidas por el experto en el caso de iOS, es conocida por su enfoque en la seguridad y la privacidad. Apple implementa medidas como el sandboxing de aplicaciones, la verificación en dos pasos y el cifrado de datos para proteger la información del usuario. Además, la App Store de Apple tiene un proceso de revisión de aplicaciones que ayuda a prevenir la distribución de aplicaciones maliciosas, mientras que Android es un sistema más abierto, lo que puede llevar a una mayor exposición a malware y otras amenazas. Sin embargo, Google también ha implementado varias medidas de seguridad, como Google Play Protect, que escanea las aplicaciones en busca de malware, y actualizaciones regulares de seguridad. En general, tanto iOS como Android pueden considerarse seguros para la banca móvil, siempre y cuando se tomen precauciones adecuadas, sin embargo los riesgos de seguridad que pueden enfrentar los usuarios son Phishing y suplantación de identidad, Malware: robar información personal o bancaria del dispositivo, Fallas de seguridad en la aplicación: vulnerabilidades que podrían ser explotadas por hackers para acceder a la información del usuario, Robo de dispositivos, la información bancaria almacenada en él podría estar en riesgo, Intercepción de datos: La información transmitida entre la aplicación bancaria móvil y el servidor del banco podría ser interceptada por hackers si no está cifrada adecuadamente, por eso es importante conocer la seguridad de aplicaciones bancarias por distintas razones una de ellas es la protección de datos personales, prevención de fraudes, cumplimiento normativo, confianza del usuario además conocer la seguridad de aplicaciones bancarias móviles en Android para proteger la información personal y financiera de los usuarios, prevenir fraudes, cumplir con las normativas y generar confianza entre los clientes. Además se menciona sobre la Técnica de Ethical Hacking identifica vulnerabilidades mediante la evaluación de la seguridad (penetration testing) en las aplicaciones bancarias móviles para identificar puntos débiles en su seguridad, análisis de código: Mediante el análisis estático y dinámico del código de la aplicación, ingeniería inversa: Los Ethical Hackers pueden utilizar técnicas de ingeniería inversa para analizar cómo funciona la aplicación y descubrir posibles vulnerabilidades, en este caso las recomendaciones que proporciona el experto es Mantener el software actualizado, utilizar contraseñas seguras, habilitar la autenticación de dos factores, evitar redes Wi-Fi públicas entre otras.

CAPÍTULO II: PROPUESTA

En el siguiente capítulo se detallan los fundamentos teóricos aplicados en la propuesta, donde se especifican los conceptos principales y sus bases teóricas.

2.1 Fundamentos teóricos aplicados

Confidencialidad de Datos: La información financiera, como números de cuenta, contraseñas y transacciones, debe mantenerse confidencial. La pérdida de confidencialidad puede llevar al robo de identidad o al acceso no autorizado a cuentas bancarias (LOPD, 2024)

Integridad de Datos: Es esencial que los datos no se modifiquen de manera no autorizada. Cualquier cambio no autorizado en los datos financieros podría dar lugar a transacciones fraudulentas o pérdida de fondos (Calle, 2018).

Disponibilidad de Servicios: Los servicios bancarios móviles deben estar disponibles para los usuarios cuando los necesiten. La falta de disponibilidad debido a ataques de denegación de servicio (DoS) o fallos de seguridad puede afectar negativamente a los usuarios y dañar la reputación del banco (Calle, 2018).

Prevención de Fraude: Las aplicaciones bancarias móviles deben protegerse contra el fraude, como el phishing y el malware. Los usuarios deben poder confiar en que están interactuando con la aplicación oficial de su banco (PowerDMARC, 2024).

Cumplimiento Normativo: Muchos bancos están sujetos a regulaciones estrictas, como PCI DSS (para proteger los datos de tarjetas de crédito) o GDPR (para proteger la privacidad de los datos personales). El incumplimiento de estas regulaciones puede resultar en sanciones financieras y legales (PowerDMARC, 2024).

Confianza del Cliente: La seguridad de la información es fundamental para ganar y mantener la confianza de los clientes. Los usuarios confiarán en las aplicaciones bancarias móviles si sienten que sus datos y transacciones están protegidos de manera adecuada (Calle, 2018).

Responsabilidad Legal y Reputación: Los bancos son legalmente responsables de proteger la información de sus clientes. Las brechas de seguridad pueden resultar en demandas legales y dañar la reputación de la institución financiera (Araujo, 2023).

2.1.2 Arquitectura de Sistemas Operativos Móviles:

Comprender la arquitectura subyacente de los sistemas operativos Android e iOS, incluyendo el kernel, el espacio de usuario y los componentes clave.

La arquitectura de Android: Se basa en el kernel de Linux y está diseñada para proporcionar una plataforma abierta y flexible para dispositivos móviles. Se compone de:

Kernel de Linux: La capa más baja de Android. Se encarga de la administración de hardware, como la gestión de memoria, la administración de dispositivos y los controladores de hardware (España, 2024).

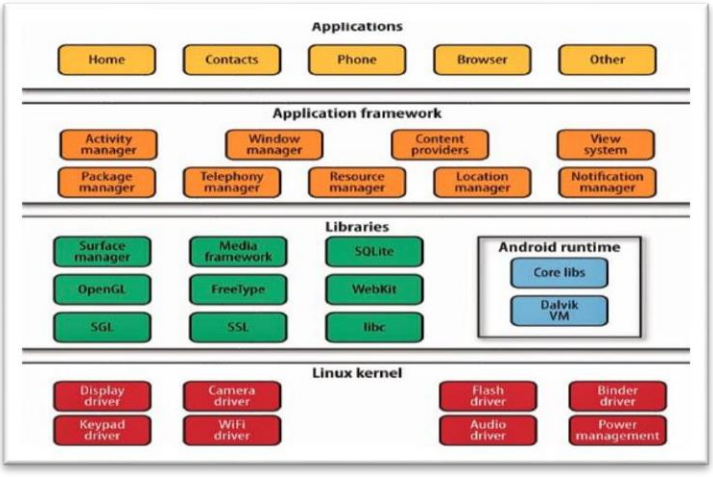
Librerías: Encima del kernel se encuentran las librerías de Android. Estas librerías proporcionan funcionalidades esenciales para el sistema, como la gestión de gráficos, acceso a bases de datos, comunicaciones por red y más (Gómez, 2019).

Máquina Virtual Dalvik/ART: Android utiliza una máquina virtual especializada (Dalvik antes y ART en versiones más recientes) para ejecutar aplicaciones. Convierte el código Java en bytecode y lo ejecuta de manera eficiente (Gómez, 2019).

Arquitectura Android

Figura 5.

Diagrama de arquitectura de Android



En la figura 5, se evidencia la imagen tomada de Aprendiendo Sobre La Arquitectura De Android (Revelo, 2020)

Arquitectura de iOS: Es el sistema operativo de Apple para dispositivos móviles, también tiene una arquitectura específica:

Kernel de XNU: iOS utiliza el kernel XNU (X is Not Unix), que es una combinación de un microkernel y componentes de Unix. Este kernel se encarga de la administración del hardware y de las operaciones básicas del sistema (Geeks, 2022).

Capa de Abstracción de Hardware (HAL): Esta capa proporciona una interfaz de programación de aplicaciones (API) para interactuar con el hardware del dispositivo, como la cámara, el acelerómetro y el GPS (Geeks, 2022).

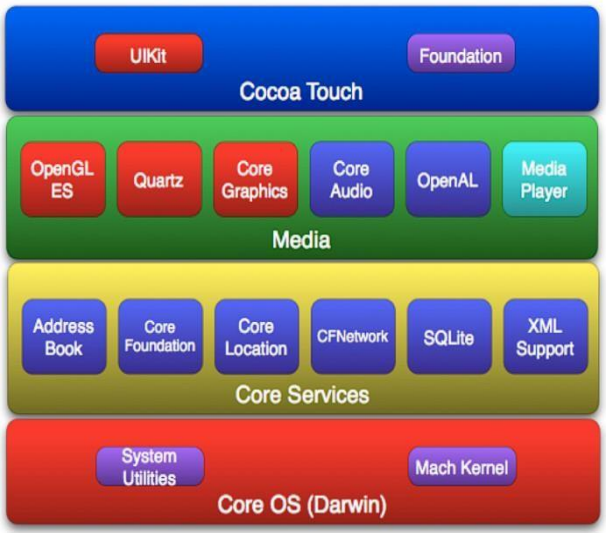
Frameworks de Sistema: iOS utiliza varios frameworks para proporcionar funcionalidades clave, como UIKit para la interfaz de usuario, Core Data para la gestión de datos y Core Location para la ubicación geoespacial (Geeks, 2022).

Capa de Aplicaciones: Aquí se encuentran las aplicaciones preinstaladas y las aplicaciones de terceros que los usuarios instalan desde la App Store. Cada aplicación se ejecuta en su propio espacio aislado para garantizar la seguridad y la estabilidad del sistema (Geeks, 2022).

Arquitectura IOS

Figura 6.

Diagrama de arquitectura iOS



En la figura 6 se evidencia la imagen tomada de Aprendiendo Sobre La Arquitectura De IOS (Revelo, 2020)

2.1.3. Ethical hacking

Los hackers éticos son expertos en seguridad de la información que irrumpen en los sistemas informáticos por asignación explícita. Esta variante del hacking se considera éticamente justificable debido al consentimiento de la "víctima". El objetivo del ethical hacking es descubrir las deficiencias de los sistemas e infraestructuras digitales, como, por ejemplo, los errores de software, evaluar los riesgos de seguridad y participar de manera constructiva en la corrección de los fallos de seguridad descubiertos. Una prueba de estrés para la seguridad del sistema puede tener lugar en cualquier momento, a veces incluso después de un hackeo ilegal. Sin embargo, lo ideal sería que los hackers éticos se anticiparan a los ciberdelincuentes y, al hacerlo, evitaran daños mayores (IONOS D. G., 2024).

2.1.4. Amenazas Comunes en Dispositivos Móviles:

Malware: Aplicaciones maliciosas diseñadas para robar información, espiar al usuario o dañar el dispositivo (Calle, 2018).

Phishing: Mensajes o sitios web falsos que engañan a los usuarios para que revelen información personal o financiera (Suarez, 2023).

Spyware: Aplicaciones que recopilan información personal del usuario sin su consentimiento (Suarez, 2023).

Ransomware: Malware que cifra los datos del dispositivo y exige un rescate para su recuperación (Suarez, 2023).

2.1.5. Herramientas de Análisis

Herramientas de análisis estático: Estas herramientas examinan el código fuente en busca de problemas como vulnerabilidades de seguridad, errores de programación, violaciones de estándares de codificación y malas prácticas (Bambu, 2022).

Herramientas de análisis dinámico: Estas herramientas ejecutan el programa y monitorizan su comportamiento en busca de problemas como fugas de memoria, caídas del sistema y vulnerabilidades que solo se manifiestan durante la ejecución. (Bambu, 2022).

2.1.6. ASPECTOS DE SEGURIDAD

Las actualizaciones de Seguridad son añadidos o modificaciones de parte del código de programas, sistemas operativos o aplicaciones, cuya misión es mejorar aspectos de funcionalidad y mucho más importante, cuestiones que afectan a la seguridad de nuestros dispositivos y la información que contienen (Dagara, 2021).

La fragmentación en Android se mantenido como uno de los problemas más importantes de dicho sistema operativo, y es una realidad que no ha cambiado con el paso de los años, pero en 2018 decidió restringirla y se limitó a uso interno (Ros, 2023).

En Android, la política de permisos se refiere a cómo las aplicaciones solicitan y gestionan el acceso a funciones y datos del dispositivo. Los usuarios pueden otorgar o denegar permisos específicos (como acceso a la cámara, ubicación o contactos) a las aplicaciones mientas que en iOS, también existe una política de permisos similar (Fuentes, 2023).

Android como iOS tienen procesos de revisión para las aplicaciones antes de que estén disponibles en sus respectivas tiendas (Google Play Store y App Store). Estas revisiones buscan detectar malware, contenido inapropiado y otras amenazas potenciales (Dagara, 2021).

Las tiendas de aplicaciones son plataformas donde los usuarios pueden descargar aplicaciones para sus dispositivos. Google Play Store es la tienda de aplicaciones para Android, mientras que la App Store es la tienda de aplicaciones para iOS. Ambas tiendas implementan medidas de seguridad (Fuentes, 2023).

Encriptación de Datos actualmente Android y iOS utilizan técnicas de encriptación para proteger los datos almacenados en los dispositivos. Esto incluye datos personales, contraseñas, fotos y más. La encriptación ayuda a prevenir el acceso no autorizado (Angeles, 2020).

La autenticación de usuarios es fundamental para seguridad. Android e iOS ofrecen métodos de autenticación, como contraseñas, PIN, huellas dactilares o reconocimiento facial, para garantizar que solo los usuarios autorizados puedan acceder al dispositivo y sus datos (Ros, 2023).

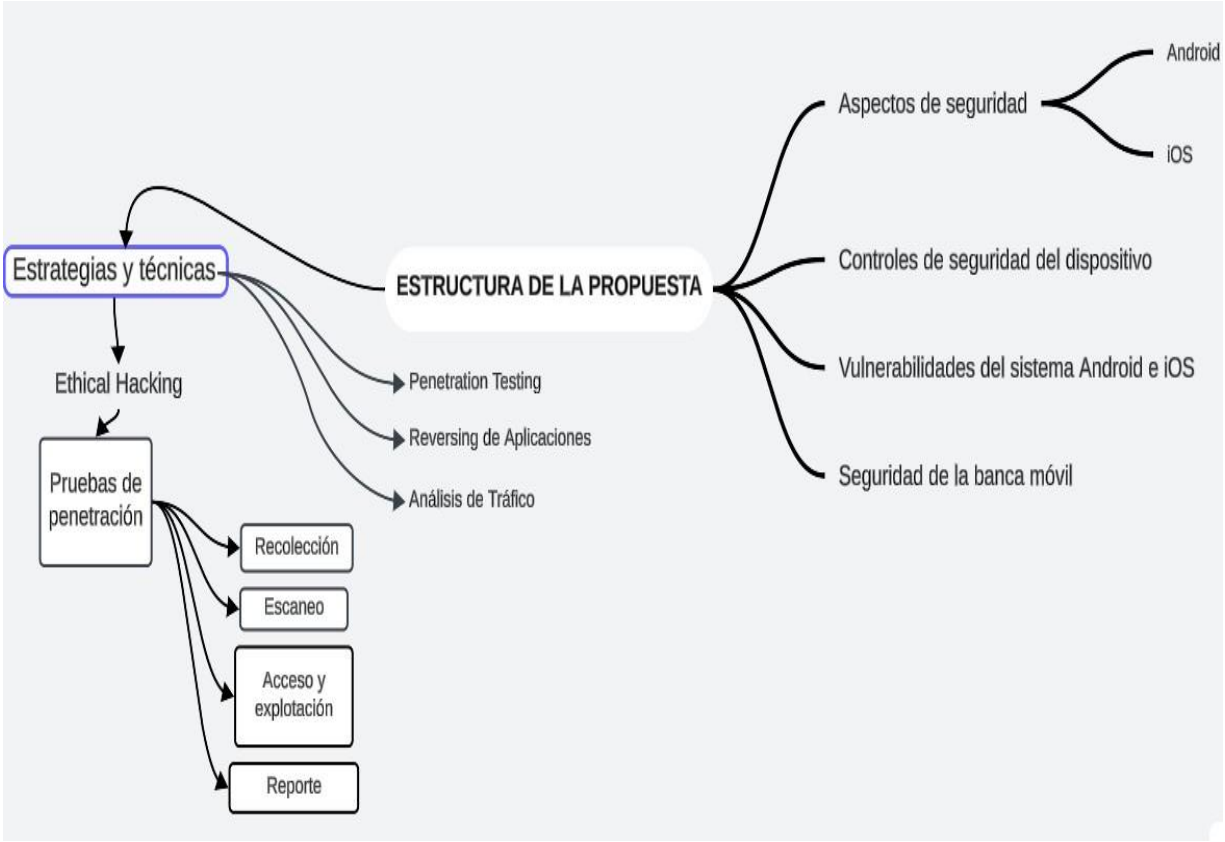
2.2. DESCRIPCIÓN DE LA PROPUESTA

a. Estructura general

En el siguiente esquema se presenta los aspectos de seguridad de Android e iOS, controles del dispositivo, vulnerabilidades del sistema Android e iOS, seguridad de banca móvil usando la técnica Ethical Hacking basados en Reversing de aplicaciones, análisis de tráfico, pruebas de penetración y sus respectivas fases como recolección, escaneo, acceso y explotación finalmente el reporte.

Figura 7.

Estructura de la propuesta



En la figura 7, se evidencia la imagen de elaboración propia sobre la estructura de la propuesta

b. Explicación del aporte

Con el siguiente informe sobre Seguridad Informática en Aplicaciones Móviles Matriz Comparativa entre iOS y Android evalúa la seguridad informática en las plataformas móviles iOS y Android, se analiza diferentes aspectos de seguridad para identificar las fortalezas y debilidades de cada plataforma, además se determina las reglas de seguridad en los sistemas operativos antes mencionados, para aplicaciones bancarias móviles.

Matriz comparativa de Android e iOS

Tabla 6:

Matriz comparativa de Android e iOS

Aspecto de Seguridad	iOS	Android
Actualizaciones de Seguridad	Frecuentes y rápidas	Irregulares y lentas
Fragmentación de Versiones	Baja	Alta
Política de Permisos	Más restrictiva	Menos restrictiva
Revisión de Aplicaciones	Rigurosa	Menos rigurosa
Tiendas de Aplicaciones	App Store (Controlada)	Google Play (Abierta)
Encriptación de Datos	SSL/TLS implementado	SSL/TLS implementado
Autenticación de Usuarios	Autenticación biométrica y PIN	Autenticación biométrica y PIN
Actualización de Software	Actualizaciones regulares	Irregularidades en actualizaciones
Protección de la Capa de Aplicación (App Shielding)	Implementado	Implementado
Política de Permisos	Restringida	Granular, pero menos estricta
Pruebas de Penetración	Realizadas regularmente	Irregularidades en las pruebas
Control de Integridad	Fuerte control de integridad	Control de integridad menos riguroso
Política de Privacidad	Transparente	Varía según la aplicación

Se puede observar en la tabla 6 las características de cada sistema operativo móvil siendo estos Android e iOS

Seguridad en Android e iOS

Descarga aplicaciones de tiendas oficiales. Trata de no descargar apps de sitios web de terceros, ya que nunca podrás saber si son legítimos y seguros, utiliza contraseñas seguras. Una contraseña segura debe contener letras mayúsculas y minúsculas, junto con caracteres especiales y números. No incluyas detalles demasiado personales que puedan identificarte, por ejemplo, el nombre de tu mascota o tu lugar de nacimiento (Cedeño, 2022).

Evita iniciar sesión en aplicaciones usando Facebook. Muchas aplicaciones y sitios web le permiten iniciar sesión en tus servicios rápidamente usando el perfil de Facebook. Sin embargo, si tu Facebook está comprometido, los piratas informáticos pueden acceder fácilmente a todas

las demás cuentas vinculadas a él. Luego pueden robar tu identidad y lanzar ataques de ingeniería social contra tus amigos y otros contactos (Cedeño, 2022).

Actualiza tu software a tiempo. Las actualizaciones de iOS y Android corrigen errores y agregan nuevas funciones de seguridad. Es tentador posponer las actualizaciones para más tarde, pero si lo haces, te estás poniendo en riesgo.

Usa una VPN. Una red privada virtual oculta su dirección IP y encripta tu tráfico, mitigando el riesgo de ser pirateado. Si te conectas a menudo a una Wifi pública, es imprescindible tener una VPN en Android o, si usa Apple, una VPN para iPhone, ya que los ciberdelincuentes pueden usar puntos de acceso falsos para infectar tu dispositivo con malware (Appmaster, 2024).

Las aplicaciones NordVPN para iOS y Android vienen con la función Dark Web Monitor, que notifica a los usuarios si alguna vez se filtran sus datos personales en la dark web. Con una cuenta de NordVPN, puede proteger hasta seis dispositivos diferentes: smartphones, portátiles, routers y más, NordVPN también tiene la función Protección contra amenazas que lo ayuda a identificar archivos cargados de malware, evita que acceda a sitios web maliciosos y bloquea rastreadores y anuncios intrusivos en el acto (Calzado, 2018).

c. Estrategias y técnicas

Para llevar a cabo la evaluación de seguridad, se utilizó una combinación de técnicas de Ethical Hacking, que incluyen:

Reversing de Aplicaciones: Se realizó un análisis estático y dinámico de las aplicaciones bancarias móviles para identificar posibles vulnerabilidades en el código y en la comunicación con servidores (Comperencia, 2020).

Penetration Testing: Se llevaron a cabo pruebas de penetración para evaluar la resistencia de las aplicaciones ante intentos de explotación de vulnerabilidades conocidas y desconocidas.

Análisis de Tráfico: Se utilizó herramientas para analizar el tráfico que se genera en la red por las aplicaciones, con el fin de identificar posibles fugas de información o transmisiones no seguras de datos (Comperencia, 2020).

2.3. VALIDACIÓN DE LA PROPUESTA

La validación de la propuesta basado en Ethical Hacking en análisis de seguridad en las bancas móviles en los sistemas operativos Android e iOS se llevó a cabo mediante la validación de un experto, como lo es el señor. Ing. Franklin Marcelo Tandalla, quien reviso la propuesta y validó mediante criterios de calidad como alcance se tendrá la propuesta y su representación en la generación, la contundencia y conveniencia de la propuesta para solucionar el problema

planteado, el cual dio su punto de vista y validez de la propuesta que se puede observar en el (anexo 3).

En el proyecto realizado para que la propuesta tenga validez con el tema titulado Informe sobre la seguridad y vulnerabilidad de las aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas. se llevó a cabo mediante la validación de un experto, el señor. Ing. Marco Vinicio Herrera Castro quien reviso la propuesta y basándose en criterios de calidad como la capacidad de implementación de la propuesta considerando que los contenidos sean aplicables para beneficio de la sociedad, la base de conceptos y teorías propias de manera sistémica y articulada, los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta para que sea válida (anexo 4).

2.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 7: *Matriz de articulación*

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Seguridad de banca móvil en los sistemas Android e iOS	Uno de los principios de Ethical Hacking es pentesting es una técnica específica para descubrir puntos débiles que un atacante real podría explotar (López, 2023).	La metodología se basa en los principios de Ethical Hacking, se busca garantizar la seguridad de las aplicaciones bancarias en Android e iOS.	Escaneo de vulnerabilidades. - Análisis estático y dinámico de código. - Pruebas de penetración.	Informe detallado de las vulnerabilidades encontradas y soluciones propuestas.	Software de escaneo de vulnerabilidades, herramientas de análisis de código, herramientas de Ethical Hacking.
Ethical Hacking	Utilización de enfoques de Ethical Hacking para evaluar la seguridad de aplicaciones móviles	Aplicación de una metodología estructurada que incluye fases de recolección de	- Identificación de amenazas. - Evaluación de la seguridad en	Informe detallado de la metodología utilizada y resultados obtenidos en cada fase.	Documentación de la metodología y herramientas de evaluación de amenazas.

	bancarias (Comperencia, 2020).	información, análisis de riesgos y pruebas de penetración.	capas. - Análisis de tráfico.		
Vulnerabilidades de los sistemas operativos	El Uso de herramientas especializadas para Ethical Hacking y seguridad móvil para detectar vulnerabilidades (Velasquez, 2020)	Selección de herramientas basadas en su eficacia y capacidad para identificar vulnerabilidades específicas en aplicaciones bancarias móviles.	- Burp Suite para pruebas de penetración. - OWASP Zap para escaneo de seguridad. - Herramientas de análisis estático de código.	Herramientas Específicas para Dispositivos Móviles para detectar vulnerabilidades de los sistemas y banca móvil.	Registro de actividades en las herramientas, informes de escaneo y resultados de pruebas de penetración.

CONCLUSIONES

Aunque el diseño y el funcionamiento de iOS y Android no pueden ser más distintos, ambos sistemas son extremadamente estables y ofrecen niveles de seguridad extremadamente altos frente a posibles amenazas y vulnerabilidades. Ellos son opciones confiables para utilizar nuestro teléfono móvil con tranquilidad debido a su robusto código, testeos continuos y medidas preventivas. Aunque iOS puede seguir siendo un poco más seguro que Android en términos de seguridad, esto no implica que Android sea un sistema operativo confiable. La seguridad no debe ser un problema a la hora de elegir entre iOS y Android.

En análisis de seguridad para las aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking, percibe las vulnerabilidades de seguridad como una preocupación significativa, ya que la información financiera y personal que se maneja a través de estas aplicaciones son sensibles lo que hace que la seguridad sea una prioridad clave para los usuarios.

Al elaborar el informe de seguridad y vulnerabilidad para las aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking reveló la presencia de múltiples vulnerabilidades significativas que podrían ser explotadas por actores malintencionados. Estas vulnerabilidades van desde problemas de configuración hasta debilidades en el diseño de las plataformas

Es importante la seguridad cibernética en el ámbito financiero ya que es beneficioso proporcionar información detallada y accesible sobre la seguridad de la banca móvil en Android e iOS para satisfacer la demanda de conocimientos en este campo y ayudar a los usuarios a tomar decisiones informadas sobre su seguridad en línea.

RECOMENDACIONES

Dado este alto nivel de preocupación, es fundamental que las empresas y desarrolladores de aplicaciones bancarias móviles trabajen activamente para identificar y mitigar las vulnerabilidades de seguridad, así como para dar informes al usuario sobre las medidas de protección que deberían tomar al utilizar estas aplicaciones.

Se recomienda que los usuarios mantengan sus dispositivos actualizados con las versiones más recientes de los sistemas operativos y aplicaciones. Los fabricantes deben priorizar las actualizaciones de seguridad para abordar rápidamente las vulnerabilidades recién descubiertas.

Los desarrolladores de aplicaciones deben realizar pruebas rigurosas de seguridad antes de lanzar nuevas aplicaciones en las tiendas de aplicaciones. Esto incluye pruebas de penetración y evaluaciones de vulnerabilidades para garantizar que las aplicaciones no expongan datos sensibles ni creen puntos de entrada para ataques.

Los usuarios deben ser educados sobre cómo proteger su privacidad y cómo otorgar permisos a las aplicaciones de manera informada. Los sistemas operativos deberían ser más transparentes en cuanto a qué datos que recopilan y cómo son utilizados, brindando al usuario un mayor control sobre sus datos personales.

REFERENCIAS BIBLIOGRÁFICAS

Angeles, C. (2020). *VI Curso Seguridad en Comunicaciones Móviles.* Obtenido de VI Curso Seguridad en Comunicaciones Móviles: https://angeles.ccn-cert.cni.es/es/cursos-stic/seguridad-comunicaciones-moviles

Appmaster. (2024). *Seguridad de aplicaciones móviles: prácticas recomendadas con software para creación de aplicacione.* Obtenido de Seguridad de aplicaciones móviles: prácticas recomendadas con software para creación de aplicacione: https://appmaster.io/es/blog/software-de-seguridad-de-aplicaciones-moviles-para-la-creacion-de-aplicaciones

Araujo, A. (2023). *análisis de malware y por qué es importante*. Obtenido de análisis de malware y por qué es importante: https://blog.hackmetrix.com/analisis-de-malware/

Balderix, A. (2024). *Probabilidad y estadistica* . Obtenido de Probabilidad y estadistica : https://www.probabilidadyestadistica.net/poblacion-y-muestra/

Bambu, m. (06 de 2022). *Análisis de código: Dinámico vs. Estático*. Obtenido de Análisis de código: Dinámico vs. Estático: https://bambu-mobile.com/analisis-de-codigo-dinamico-vs-estatico/#:~:text=%C2%BFQu%C3%A9%20es%20el%20an%C3%A1lisis%20de%20c%C3%B3digo%3F%20El%20an%C3%A1lisis,antes%20de%20que%20el%20programa%20salga%20al%20p%C3%BAblico.

Calle, D. (2018). *Arquitectura de Redes Móviles.* Obtenido de 2.7 Arquitectura de Redes Móviles:: https://bibdigital.epn.edu.ec/bitstream/15000/892/1/CD-1775%282008-11-05-11-47-40%29.pdf

Calzado, S. (2018). *LAS TECNOLOGÍAS EMERGENTES (BLOCKCHAIN). CONCEPTO. .* Obtenido de LAS TECNOLOGÍAS EMERGENTES (BLOCKCHAIN). CONCEPTO. : https://cetic.es/wp-content/uploads/2020/03/Tema-106.-Tecnolog%C3%ADas-emergentes.pdf

Cedeño, C. (2022). *Ingeniería inversa: beneficios y ejemplos reales de un ingenioso enfoque para diseñar productos*. Obtenido de Ingeniería inversa: beneficios y ejemplos reales de un ingenioso enfoque para diseñar productos: https://www.cinconoticias.com/ingenieria-inversa/

Comperencia. (2020). *Ethical Hacking*. Obtenido de Ethical Hacking: https://competencia.com.ec/smart-hacking-hacking-etico-de-redes-sistemas/?gad_source=1&gclid=CjwKCAiA6KWvBhAREiwAFPZM7nOUB_eq70wOd5VJ_3epWST_Hm0X5EVdzkSQWvz5GYp4AKIa1a8QuBoCDFMQAvD_BwE

Cybersegurity. (02 de 2024). *EC-Council Cybersecurity Exchange Logo*. Obtenido de EC-Council Cybersecurity Exchange Logo: https://www.bing.com/search?pglt=43&q=ethical+hacking+process&cvid=8095d4dae133426b81ec88cfa28c275b&gs_lcrp=EgZjaHJvbWUqBggCEAAYQDIGCAAQABhAMgYIARBFGDsyBggCEAAYQDIGCAMQABhAMgYIBBAAGEAyBggFEAAYQDIGCAYQABhAMgYIBxAAGEAyBggIEEUYPNIBCDI2NjBqMGoxqAIAsAIA&FORM=A

Dagara. (2021). *La importancia de las actualizaciones de seguridad*. Obtenido de La importancia de las actualizaciones de seguridad: https://dagara.net/la-importancia-de-las-actualizaciones-de-seguridad/

España, D. (01 de 2024). *Deloitte*. Obtenido de Deloitte: https://www2.deloitte.com/es/es/blog/cyber-pills/2021/hacking-etico-que-es-y-como-aprenderlo.html

Fuentes, r. (2023). *Protección del dispositivo en Seguridad de Windows*. Obtenido de Protección del dispositivo en Seguridad de Windows: https://support.microsoft.com/es-es/windows/protecci%C3%B3n-del-dispositivo-en-seguridad-de-windows-afa11526-de57-b1c5-599f-3a4c6a61c5e2

Geeks, B. (12 de 2022). *Arquitectura del sistema operativo IOS*. Obtenido de Arquitectura del sistema operativo IOS: https://barcelonageeks.com/arquitectura-del-sistema-operativo-ios/

IBM. (2022). *las pruebas de penetración*. Obtenido de las pruebas de penetración: https://www.ibm.com/es-es/topics/penetration-testing

IONOS, D. G. (01 de 2024). *IONOS* . Obtenido de IONOS : https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-ethical-hacking/

Jordan, G. (12 de 2019). *ARQUITECTURA DE LOS SISTEMAS COMPUTACIONALES MOVILES*. Obtenido de ARQUITECTURA DE LOS SISTEMAS COMPUTACIONALES MOVILES: https://idoc.pub/documents/arquitectura-de-los-sistemas-operativos-moviles-1430woxo6j4j

LOPD. (03 de 2024). *LOPD DIRECTA* . Obtenido de LOPD DIRECTA : https://lopddirecta.es/que-es-confidencialidad-y-un-ejemplo/#:~:text=La%20confidencialidad%20es%20uno%20de%20los%20pilares%20fundamentales,la%20integridad%20y%20la%20privacidad%20de%20los%20datos.

López, J. (03 de 2023). *pentesting*. Obtenido de pentesting: https://auditech.es/blog/pentesting-que-es-y-para-que-sirve/#:~:text=Pentesting%20(Examen%20de%20Penetraci%C3%B3n)%3A,la%20seguridad%20de%20un%20sistema.

Martinez, G. (2015). *PROTECCION DE USUARIOS DE LOSSERVICIOS FINANCIEROS. NUEVOREGIMEN DE COMISIONES Y CARGOSBANCARIOS.* Mexico : Bepres .

Mixedeal. (2020). *Redes móviles 1G, 2G, 3G,4G y 5G*. Obtenido de Redes móviles 1G, 2G, 3G,4G y 5G: https://www.mixideal.com/blog/tecnologia/redes-moviles-1g-2g-3g-4g-y-5g-cuales-son-sus-diferencias

Moes, T. (2023). *SoftwareLab Logo*. Obtenido de SoftwareLab Logo: https://softwarelab.org/es/blog/que-es-ios/

Naturales, C. (2021). *Concepto*. Obtenido de Concepto: https://concepto.de/tipos-de-investigacion/

Orrous, R. (07 de 2019). *Fallas de seguridad en aplicaciones*. Obtenido de Fallas de seguridad en aplicaciones: https://es.linkedin.com/pulse/fallas-de-seguridad-en-aplicaciones-bancarias-exponen-roman-klavijo#:~:text=Vulnerabilidades%20como%20la%20falta%20de%20protecciones%20binarias%2C%20almacenamiento,de%20banca%2C%20tarjeta%20de%20cr%C3%A9dito%20y%20pagos%20m%C

Pablo, S. (octubre de 2023). *Questionpro* . Obtenido de Questionpro : https://www.questionpro.com/blog/es/metodos-de-investigacion/

Palacios, J. (2018). *Análisis de Seguridad de las Aplicaciones Móviles Basadas en Android, Utilizadas en la Banca Electrónica del Ecuador*. Obtenido de Análisis de Seguridad de las Aplicaciones Móviles Basadas en Android, Utilizadas en la Banca Electrónica del Ecuador: http://bibdigital.epn.edu.ec/handle/15000/19469

PowerDMARC. (03 de 2024). *PowerDMARC*. Obtenido de PowerDMARC: https://powerdmarc.com/es/cyber-security-in-banking/

Ros, I. (2023). Fragmentación en Android. *Fragmentación en Android*.

Salary. (29 de Marzo de 2022). *Ethical hacker*. Obtenido de Ethical hacker: https://www.salary.com/research/salary/posting/ethical-hacker-salary

Servnet. (02 de 2024). *Hacking ético: en qué consiste*. Obtenido de Hacking ético: en qué consiste: https://www.servnet.mx/blog/hacking-etico

Sobers, R. (Abril de 2021). *Varonis*. Obtenido de https://www.varonis.com/blog/data-breach-statistics

Suarez, G. (2023). *principales amenazas de seguridad móvil y cómo prevenirlas*. Obtenido de principales amenazas de seguridad móvil y cómo prevenirlas: https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-mobile-security/top-6-mobile-security-threats-and-how-to-prevent-them/

tecnológico, D. (julio de 2023). Muy Tecnologías. *Android*. Tecnologías Android .

Velasquez, C. (2020). *Engaño a los atacantes .* España: Esp.

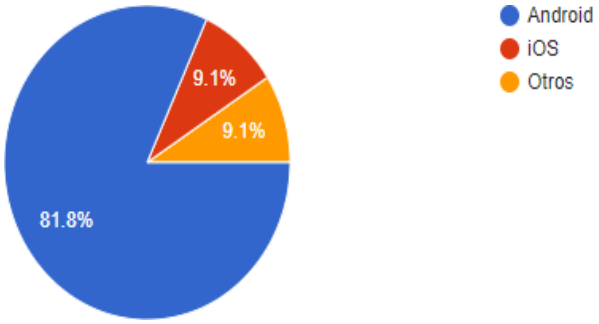
Zaharia, A. (febrero de 2022). *Terrifying cybercrime* . Obtenido de Terrifying cybercrime : https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

ANEXO 1 ENCUESTA

La encuesta se lo realizo a 100 personas que trabajan en el área de desarrollo de la entidad bancaria Produbanco.

1. ¿Usted con cuál de los siguientes sistemas operativos cuenta?

Opciones	Porcentaje	Total
Android	81.8%	100%
iOS	9.1%	
Otros	9.1%	

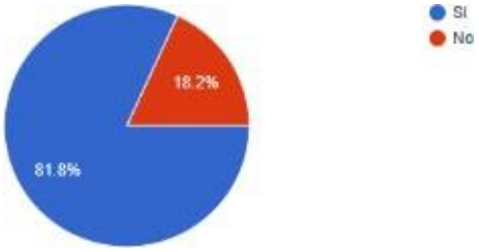


Análisis de resultados

Con los datos obtenidos, podemos ver que el 81.8% de los encuestados cuenta con un dispositivo Android, mientras que solo el 9.1% utiliza iOS y otro 9.1% utiliza otros sistemas operativos. Este análisis sugiere una popularidad por Android entre los encuestados, por otro lado, iOS y otros sistemas operativos parecen tener una base de usuarios más pequeña en esta muestra específica.

2.- ¿Usted cuenta con la banca móvil?

Opciones	Porcentaje	Total
Si	81.8%	100%
No	18.2%	

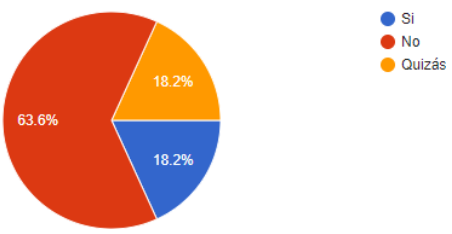


Análisis de resultados

En la tabla se puede observar que el 81.8% de los encuestados cuenta con banca móvil, mientras que el 18.2% no la utiliza. Esto sugiere que la mayoría de los encuestados han adoptado la banca móvil como una forma de gestionar sus finanzas.

3.- ¿Usted cree que exista alguna desventaja en tener la banca móvil en un sistema operativo Android o iOS?

Opciones	Porcentaje	Total
Si	63.6%	100%
No	18,2%	
Quizás	18,2%	

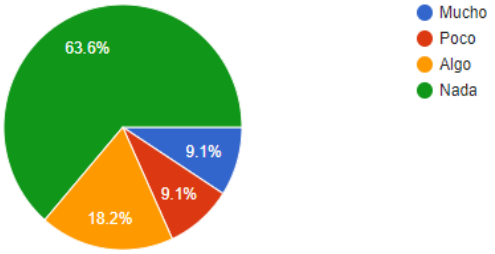


Análisis de resultados

Con los datos proporcionados, podemos observar que el 63.6% de los encuestados cree que existen desventajas en tener la banca móvil en un sistema operativo Android o iOS, mientras que el 18.2% no percibe ninguna desventaja y otro 18.2% está indeciso en duda, con estos resultados los encuestados tiene preocupaciones o percepciones negativas sobre la banca móvil en estos sistemas operativos.

4.- ¿Has escuchado hablar sobre Ethical Hacking aplicado a sistemas operativos?

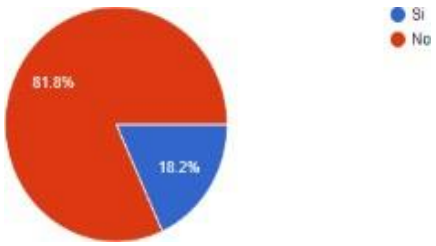
Opciones	**Porcentaje**	**Total**
Mucho	63.6%	100%
Poco	9,1%	
Algo	18,2%	
Nada	9,1%	



En la gráfica, podemos observar que el 63.6% de los encuestados ha escuchado mucho sobre Ethical Hacking aplicado a sistemas operativos, mientras que el 18.2% ha escuchado algo al respecto. Solo el 9.1% ha escuchado poco y otro 9.1% no ha escuchado nada sobre este tema, en este caso el nivel relativamente alto de familiaridad con el concepto de Ethical Hacking aplicado a sistemas operativos entre los encuestados. La mayoría parece tener al menos cierto grado de conocimiento sobre este tema, lo que podría indicar un interés o una conciencia creciente sobre la importancia de la seguridad informática y la protección de los sistemas operativos.

5.- ¿Cree usted que tener su banca Móvil en los sistemas operativos Android e iOS es completamente seguro?

Opciones	Porcentaje	Total
Si	18.2%	100%
No	81.8%	

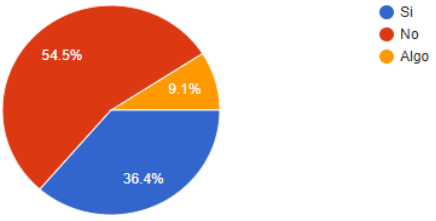


Análisis de resultados

En los resultados obtenidos, podemos ver que el 81.8% de los encuestados cree que tener su banca móvil en los sistemas operativos Android e iOS no es completamente seguro, mientras que el 18.2% restante no comparte esta opinión, por lo que es importante tener en cuenta que la percepción de seguridad puede variar según la experiencia personal, la información recibida y las preocupaciones individuales sobre la seguridad cibernética.

6.- ¿Conoce usted sobre la seguridad de su banca móvil en el sistema Android o iOS?

Opciones	Porcentaje	Total
Si	36,4%	100%
No	54,5%	
Algo	9,1%	

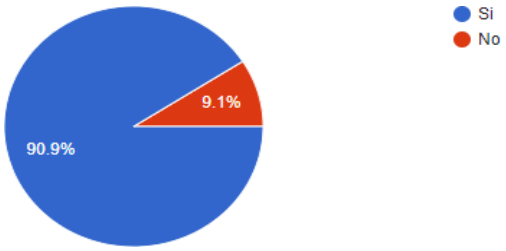


Análisis de resultados

En base a los resultados, se observa que 54.5% indica que no tiene conocimiento sobre la seguridad de su banca móvil mientras que el 36.4% de los encuestados afirma conocer en los sistemas Android e iOS. Solo el 9.1% tiene un conocimiento parcial sobre este tema, por lo tanto, la información que tienen los usuarios es insuficiente sobre las medidas de seguridad implementadas en las aplicaciones bancarias móviles y los sistemas operativos.

7.- ¿Consideras importante conocer las ventajas de seguridad que ofrecen Android e iOS en este tipo de aplicaciones?

Opciones	**Porcentaje**	**Total**
Si	90.9%	100%
No	9.1%	

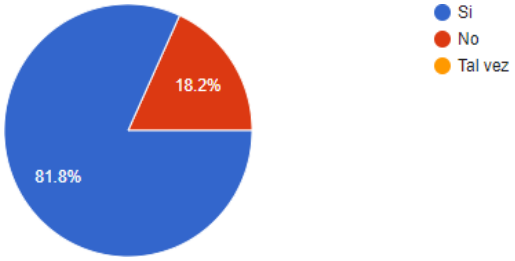


Análisis de resultados

Con los datos obtenidos, se observa que el 90.9% de los encuestados considera importante conocer las ventajas de seguridad que ofrecen Android e iOS en este tipo de aplicaciones, mientras que el 9.1% no comparte esta opinión, por lo que los encuestados valoran la importancia de estar informados sobre las ventajas de seguridad que ofrecen Android e iOS en las aplicaciones de banca móvil. Esto indica una conciencia y preocupación por la seguridad de sus datos financieros y personales al utilizar estas plataformas.

8.- ¿Crees que las vulnerabilidades de seguridad en aplicaciones bancarias móviles son un problema grave?

Opciones	Porcentaje	Total
Si	81,8%	100%
No	18,2%	
Algo	0,0 %	

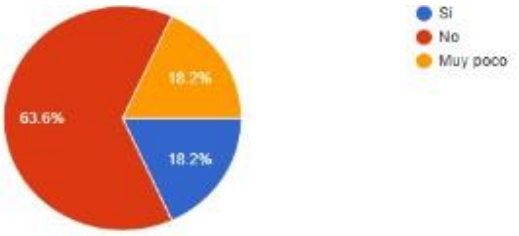


Análisis de resultados

Con los resultados obtenidos, se observa que el 81.8% de los encuestados considera que las vulnerabilidades de seguridad en aplicaciones bancarias móviles son un problema grave, mientras que el 18.2% piensa que no es un grave problema las vulnerabilidades de seguridad en aplicaciones bancarias, esta percepción puede atribuirse a la sensibilidad de la información financiera y personal que se maneja a través de estas aplicaciones, lo que hace que la seguridad sea una prioridad clave para los usuarios.

9.- ¿Conoce usted sobre la seguridad de su banca móvil en el sistema Android iOS?

Opciones	Porcentaje	Total
Si	18,2%	100%
No	63,6%	
Muy poco	18,2%	

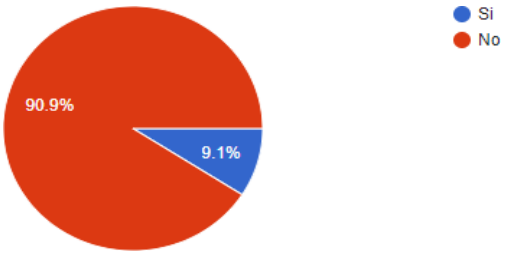


Análisis de resultados

El 63.6% indica que no tiene conocimiento sobre la seguridad de su banca móvil mientras que el 18.2% de los encuestados afirma conocer sobre la seguridad de su banca móvil en los sistemas Android e iOS, además, el 18.2% restante dice conocer muy poco sobre este tema, en este caso, se resalta la importancia de educar a los usuarios sobre la seguridad de la banca móvil en Android e iOS, ya que la mayoría parece tener un conocimiento limitado o nulo sobre este tema.

10.- ¿Conoce usted sobre el papel de la ética y la legalidad en el contexto del Ethical hacking aplicado a aplicaciones bancarias móviles?

Opciones	**Porcentaje**	**Total**
Si	9.1%	100%
No	90.9%	



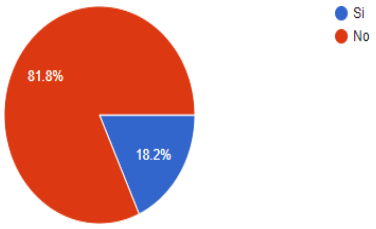
Análisis de resultados

El 90.9% de los encuestados no está familiarizado con el papel de la ética y la legalidad en el contexto del Ethical Hacking aplicado en bancas móviles, mientras que 9.1% de los encuestados afirma conocer sobre el papel de la ética y la legalidad en el contexto del Ethical Hacking aplicado a aplicaciones bancarias móviles, es fundamental que los usuarios y profesionales de la seguridad cibernética comprendan la

importancia de realizar pruebas éticas y legales para identificar y corregir vulnerabilidades en las aplicaciones bancarias móviles, sin infringir las leyes o comprometer la integridad de los sistemas.

11.- ¿Conoce usted sobre la seguridad de su banca móvil en el sistema Android o iOS?

Opciones	Porcentaje	Total
Si	18,2%	100%
No	81,8%	

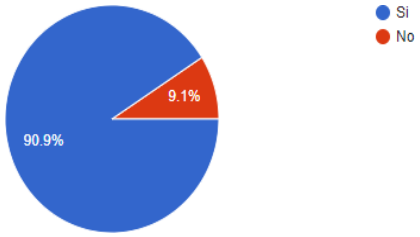


Analisis de resultados

El 81.8% de los encuestados no conoce sobre la seguridad de su banca móvil en los sistemas Android e iOS, mientras que el 18.2% restante afirma conocer sobre este tema, en este caso, surge la necesidad de aumentar la conciencia y la educación sobre la seguridad de la banca móvil en Android e iOS.

12.- ¿Consideras que las empresas desarrolladoras de aplicaciones bancarias móviles deberían invertir más en seguridad?

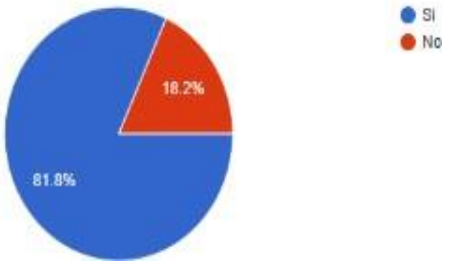
Opciones	Porcentaje	Total
Si	90,9%	100%
No	9,1%	



Con las encuestas realizadas, se observa que 90.9% de los encuestados considera que las empresas desarrolladoras de aplicaciones bancarias móviles deberían invertir más en seguridad, mientras que el 9.1% restante no comparte esta opinión, por lo cual es importante mayor inversión en seguridad por parte de las empresas desarrolladoras de aplicaciones bancarias móviles.

13.- ¿Consideras importante conocer las ventajas de seguridad que ofrecen Android e iOS en este tipo de aplicaciones?

Opciones	**Porcentaje**	**Total**
Si	81,8%	100%
No	18,2%	

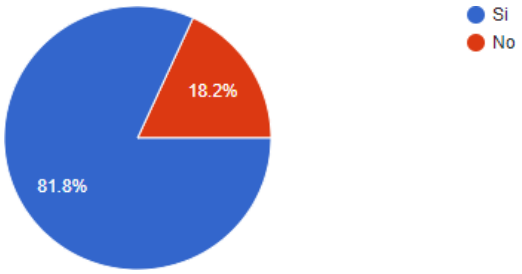


Análisis de resultados

El 81.8% de los encuestados considera importante conocer las ventajas de seguridad que ofrecen Android e iOS en aplicaciones bancarias móviles, mientras que el 18.2% restante no comparte esta opinión, esto indica que la mayoría de los encuestados valoran la información sobre las ventajas de seguridad que ofrecen los sistemas operativos Android e iOS en las aplicaciones bancarias móviles. Esto sugiere una conciencia de la importancia de elegir plataformas seguras para realizar transacciones financieras móviles y una preocupación por la protección de la información personal y financiera.

14.- ¿Te gustaría participar en talleres o cursos sobre seguridad en aplicaciones bancarias móviles y Ethical Hacking?

Opciones	Porcentaje	Total
Si	81,8%	100%
No	18,2%	

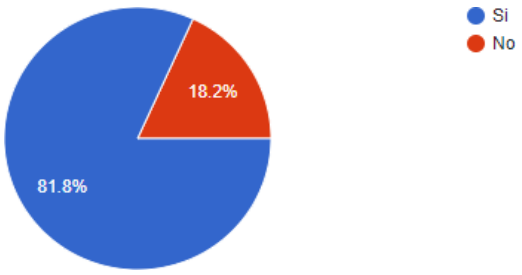


Análisis de resultados

Con los resultados obtenidos el 81.8% de los encuestados estaría interesado en participar en talleres o cursos sobre seguridad en aplicaciones bancarias móviles y Ethical Hacking, mientras que el 18.2% restante no está interesado, para lo cual, existe un alto nivel de interés en la educación y capacitación en seguridad cibernética relacionada con las aplicaciones bancarias móviles y Ethical Hacking, dado este nivel de interés, sería beneficioso ofrecer talleres y cursos sobre seguridad en aplicaciones bancarias móviles y Ethical Hacking para satisfacer la demanda y ayudar a los usuarios a proteger mejor sus datos financieros y personales.

15.- Le gustaría conocer sobre la seguridad de su banca móvil en el sistema Android e iOS.

Opciones	Porcentaje	Total
Si	81,8%	100%
No	18,2%	



Análisis de resultados

Con los datos proporcionados, el 81.8% de los encuestados estaría interesado en conocer sobre la seguridad de su banca móvil en los sistemas Android e iOS, mientras que el 18.2% restante no tiene interés en este tema, por lo tanto, sería beneficioso proporcionar información detallada y accesible sobre la seguridad de la banca móvil en Android e iOS para satisfacer la demanda de conocimientos en este campo y ayudar a los usuarios a tomar decisiones informadas sobre su seguridad en línea.

ANEXO 2 ENTREVISTA

Entrevista

La entrevista se lo aplicó a un experto en sistemas el Señor Ing. Franklin Tandalia, quien con sus respuestas ayudó a medir la seguridad de la banca móvil en los sistemas operativos Android e iOS y la validación de la propuesta.

1. **¿Qué opina usted sobre la seguridad de la banca móvil en el sistema operativo iOS y Android?**
2. **¿Qué riesgos de seguridad pueden enfrentar los usuarios de aplicaciones bancarias móviles?**
3. **¿Por qué es importante conocer la seguridad de las aplicaciones bancarias móviles en Android e iOS?**
4. **¿Cómo pueden las técnicas de Ethical Hacking ayudar a identificar y mitigar vulnerabilidades en las aplicaciones bancarias móviles?**
5. **¿Qué recomendaciones daría a los usuarios de aplicaciones bancarias móviles para mejorar la seguridad de sus productos?**

ANEXO 3 INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAELESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega: Señor Ing. Franklin Marcelo Tandalla Quimbita con número de cedula 172108748-2, se solicita de su valiosa cooperación para evaluar la siguiente propuestadel proyecto de titulación: Informe sobre la seguridad y vulnerabilidad de las aplicacionesbancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que sele pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ing. Franklin Marcelo Tandalla Quimbita

Título obtenido
Ingeniero en Informática - UTPL
Cédula de Identidad
172108748-2
E- mail
frarastayo@gmail.com
Institución de Trabajo
Instituto Superior Universitario Sucre
Cargo
Docente de la Carrera de Desarrollo de Software
Años de experiencia en el área
10 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5,
  Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Informe sobre la seguridad y vulnerabilidad de las aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas.

Indicador	*Descripción*	**Muy adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco adecuado**	**Inadecuado**
Impacto	*El alcance que tendrá la propuesta ysu representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	*X*				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	*X*				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	*X*				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	*X*				

Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde*	*X*				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
	total	*35*				

Observaciones:

_____
_____
_____

Recomendaciones

_____
_____
_____

Quito, miércoles 6 de marzo de 2024:

Firmado electrónicamente por:

FRANKLIN MARCELOTANDALLA QUIM 

_____

Firma del especialista

ANEXO 4 INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAELESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega: Señor Ing. Marco Vinicio Herrera Castos con número de cedula 0301715843, se solicita de su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: Informe sobre la seguridad y vulnerabilidad de las aplicacionesbancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas.

Sus criterios son de suma importancia para la realización de este trabajo, por lo que sele pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ing. Marco Vinicio Herrera Castos

Título obtenido
Ingeniero en sistemas
Cédula de Identidad
0301715843
E- mail
marcovinicio.hc@hotmail.com
Institución de Trabajo
Produbanco
Cargo
Especialista en Calidad
Años de experiencia en el área
5 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5,
  Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Informe sobre la seguridad y vulnerabilidad de las aplicaciones bancarias móviles en los sistemas operativos Android e iOS mediante técnicas de Ethical Hacking para mitigar amenazas.

Indicador	*Descripción*	**Muy adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco adecuado**	**Inadecuado**
Impacto	*El alcance que tendrá la propuesta ysu representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	*X*				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	*X*				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	*X*				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	*X*				

Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursosdisponibles*	*X*				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
	Total	*35*				

Observaciones:

_____
_____
_____

Recomendaciones

_____
_____
_____

Quito, viernes 8 de marzo de 2024:

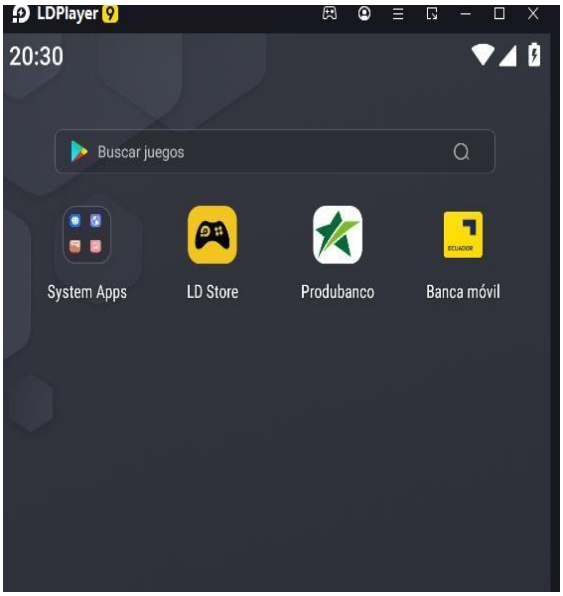
_____

Firma del especialista

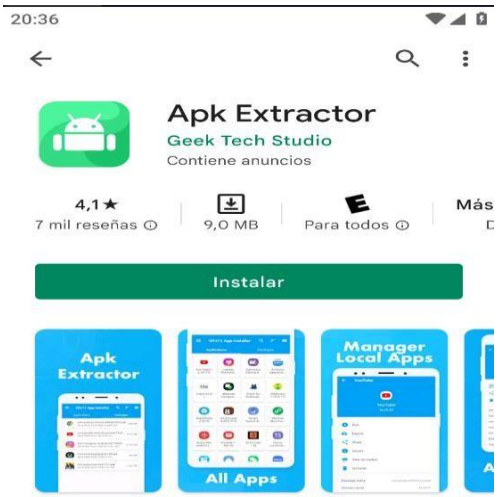
Resultados Obtenidos

Se procede con la instalación de un emulador Android dentro del sistema operativo de Windows Obtener los apk de las aplicaciones bancarias móviles del sistema Android Entidades Financieras Banco Produbanco y Banco Pichincha

Con esto se procede a realiza la instalación de los aplicativos mencionados dentro del emulador utilizado para las pruebas LDPlayer

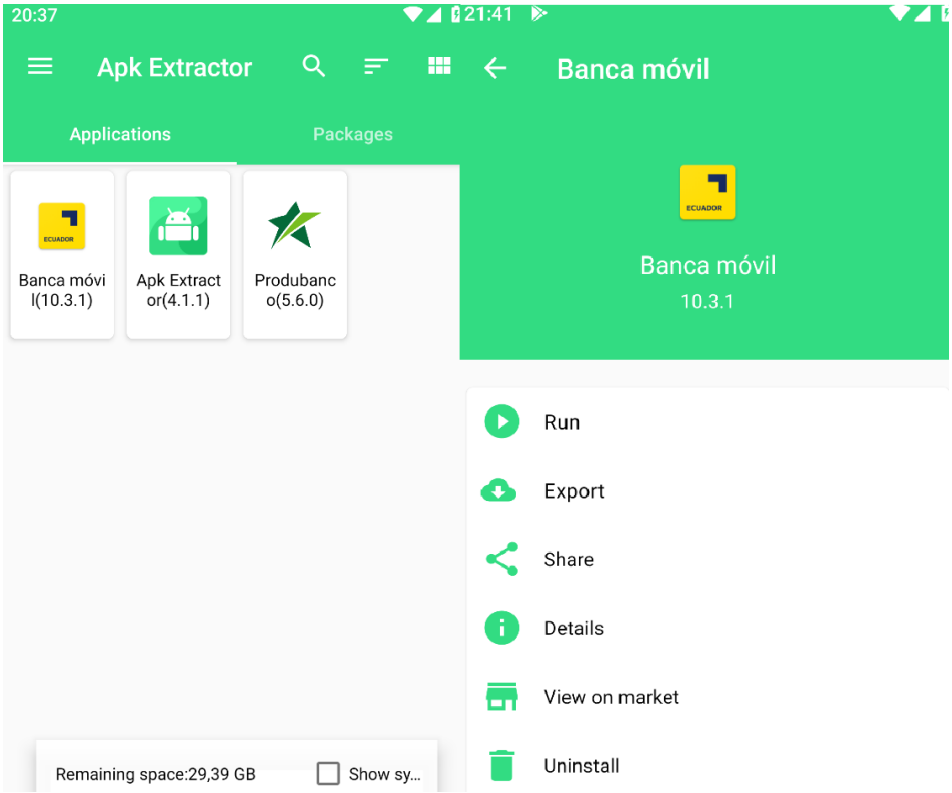


Se utiliza la aplicación APK extractor para obtener los archivos ya instalados dentro del emulador Android en Windows



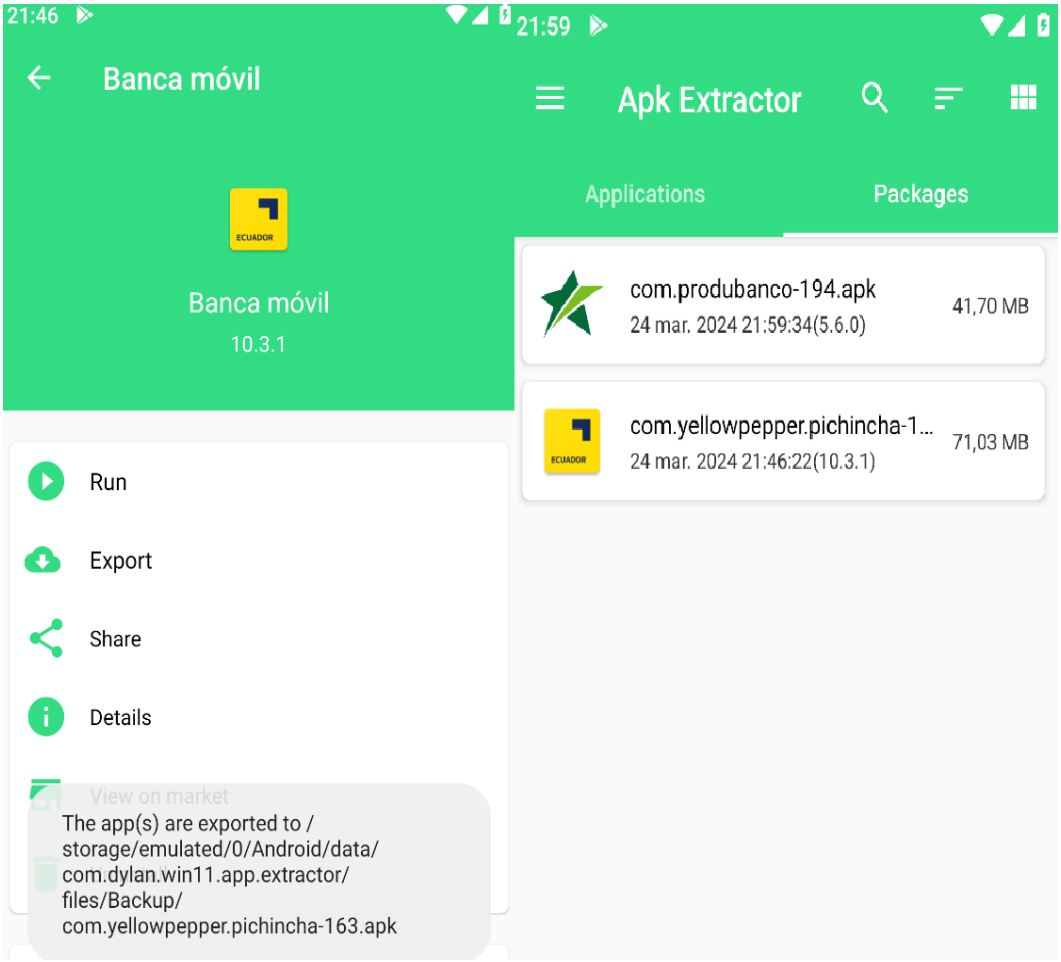
Una vez abierto el aplicativo podemos observar las aplicaciones instaladas y de las cuales se puede generar el archivo apk del sistema Android

Como se puede observar en las imágenes los apk instalados en el emulador son Banca Movil de Banco Pichincha y Produbanco de Grupo Promerica, los cuales procederemos a obtener su apk para realizar las pruebas de seguridad



Dentro de las opciones más relevantes del apk extractor la que se utilizara es la opción de run con la cual obtendremos el apk de la aplicación y la opción de Details en la cual se encontrara la información de la apk

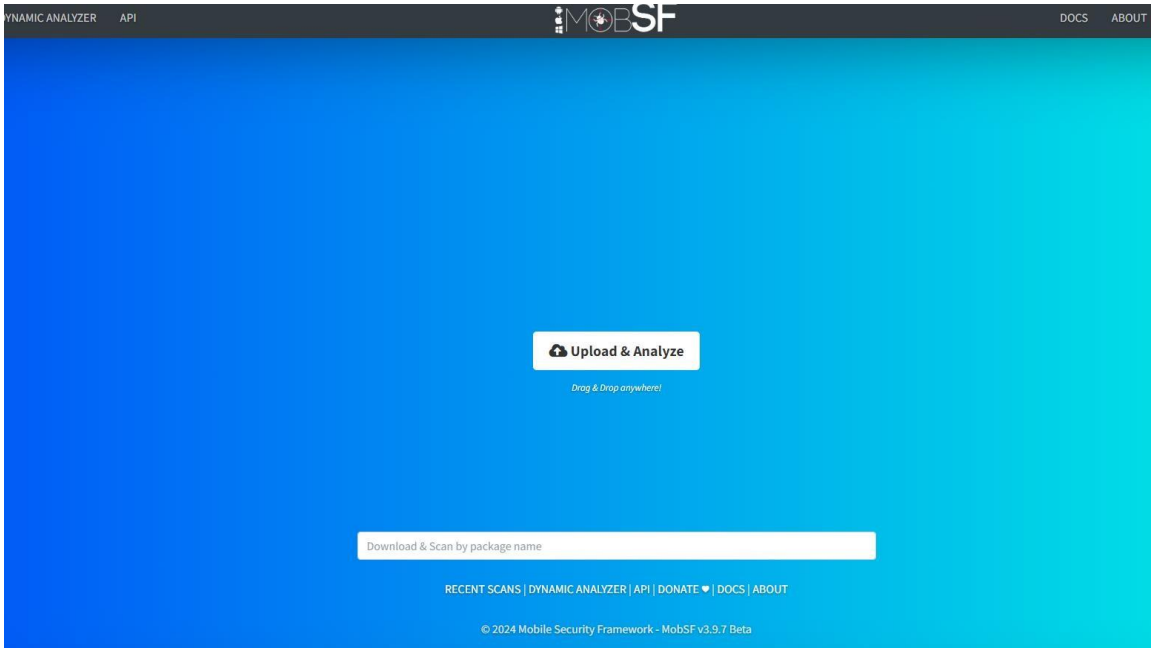
En las siguientes opciones validamos la funcionalidad de la aplicación APK Extractor con la opción Run donde se aprecia que se generaron los archivos. apk de Banca Movil y de Produbanco



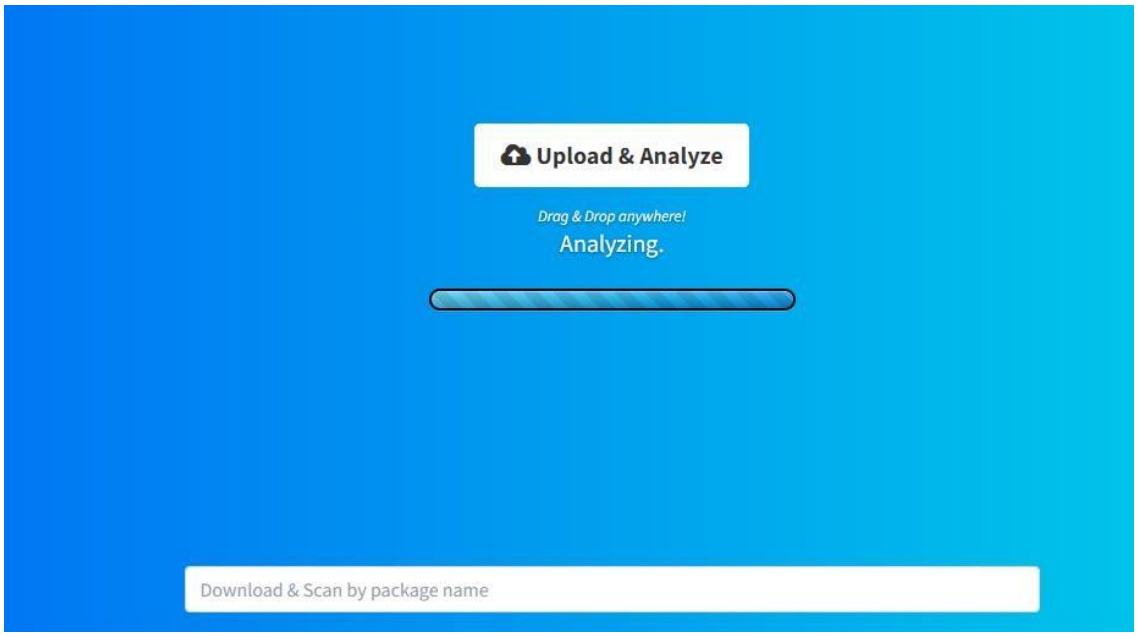
Una vez obtenido los apk procedemos con la instalación del aplicativo MOBSF dentro del sistema operativo Kali Linux

MobSF es una herramienta de pruebas automatizadas de seguridad estática y dinámica de código abierto diseñada para detectar vulnerabilidades de seguridad en aplicaciones móviles iOS y Android.

Ingresamos al Kali Linux e iniciamos la aplicación MobSF

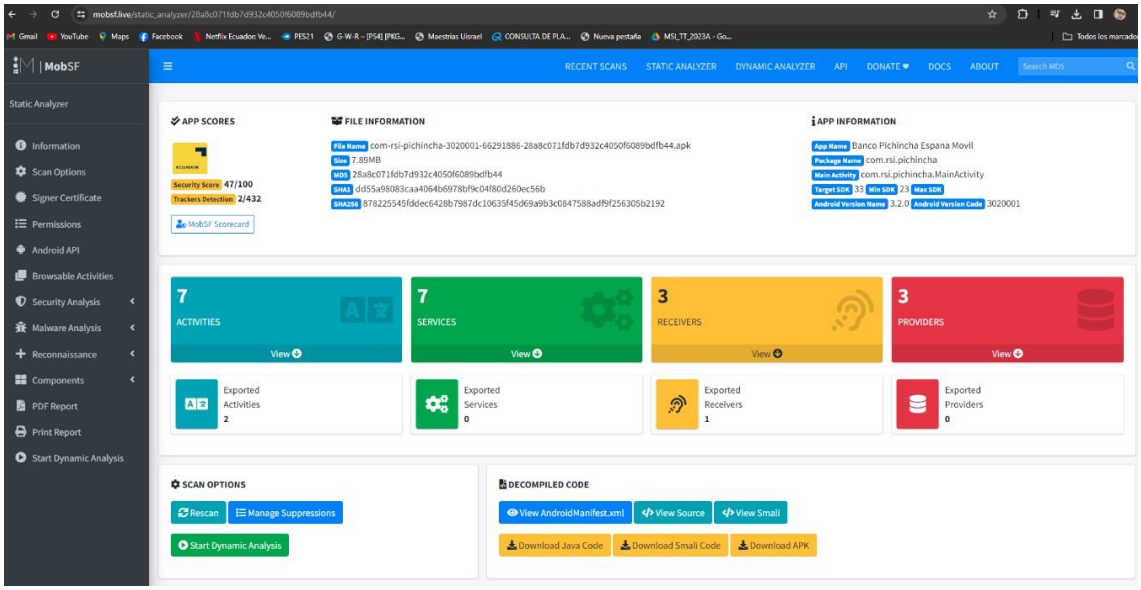


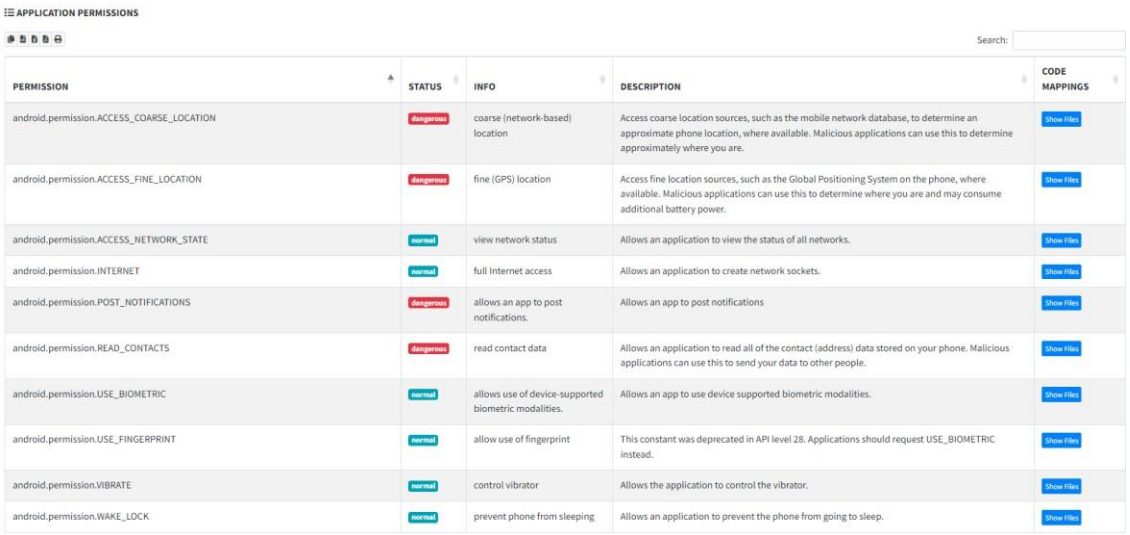
Y realizamos la carga de los apk dentro de la opción Upload & Analyze el cual se encarga de validar el contenido del apk.



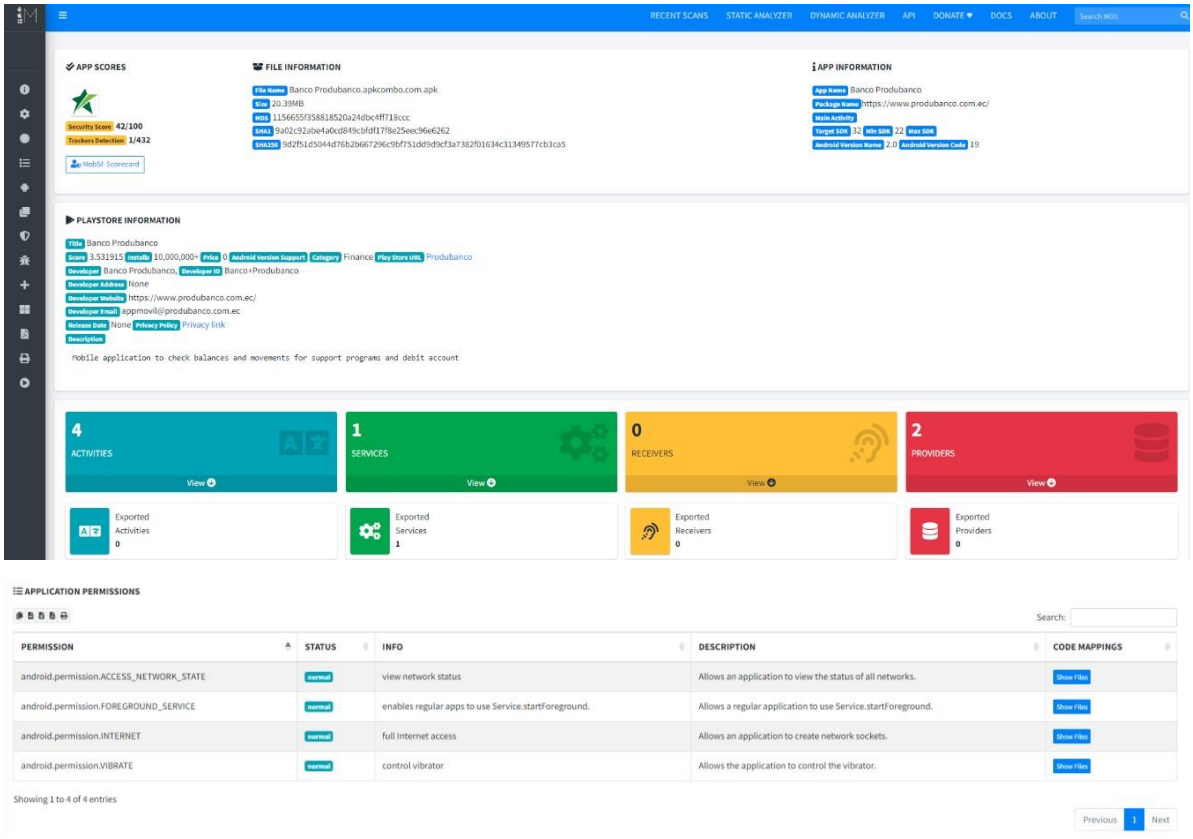
Dependiendo del tamaño del apk y de la conexión a intenet se puede visualizar el resultado obtenido por la aplicación MobSF en Kali Linux

Pichincha





Produbanco



En conclusión, se puede observar que las aplicaciones muestran entre sus debilidades las siguientes opciones:

- Permiso de localización
- Permiso de uso de red
- Permiso de acceso a notificaciones
- Permiso de acceso a contactos

Las cuales pueden ser una brecha de seguridad que pueden ser aprovechada por un Hacker, para lo cual se recomienda lo siguiente:

- Ten precaución si te conectas a redes de WiFi abiertas
- Realiza copias de seguridad
- Mantenlo actualizado
- Descarga aplicaciones solo de fuentes oficiales