****

**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERÍA**

**Escuela Profesional de Ingeniería de Sistemas**

**Proyecto**

**Desarrollo de un Aplicativo Móvil para la Evaluación de Seguridad en Dispositivos Móviles**

Curso: *Construcción de Software I*

Docente: *Mag. Ricardo Eduardo Valcarcel Alvarado*

Integrantes:

***Jarro Cachi, Jose Luis (2020067148)***

**Tacna – Perú**

***2024***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CONTROL DE VERSIONES | | | | | |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | Jose Jarro | Jose Jarro | Jose Jarro | 29/06/2024 | Versión Original |

**Desarrollo de un Aplicativo Móvil para la Evaluación de Seguridad en Dispositivos Móviles**

**Versión *{1.0}***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CONTROL DE VERSIONES | | | | | |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | Jose Jarro | Jose Jarro | Jose Jarro | 29/06/2024 | Versión Original |

**ÍNDICE GENERAL**

[**1. Introducción 5**](#_heading=h.pz67h4jhm4e)

[1.1. Propósito 5](#_heading=h.447y4fo1olbt)

[1.2. Alcance 5](#_heading=h.6b4lp64pzj5y)

[1.3. Definiciones, Siglas y Abreviaturas 5](#_heading=h.fa8qau5hinm6)

[1.4. Referencias 5](#_heading=h.aajy9w796blp)

[1.5. Visión General 5](#_heading=h.t567sbncuzak)

[**2. Posicionamiento 5**](#_heading=h.uqro4gp3fwdi)

[2.1. Oportunidad de negocio 5](#_heading=h.auv04gphkppm)

[2.2. Definición del problema 5](#_heading=h.i0o7jzgszk18)

[**3. Descripción de los interesados y usuarios 5**](#_heading=h.ovaux8u5xapd)

[3.1. Resumen de los interesados 5](#_heading=h.11xyy2jz51df)

[3.2. Resumen de los usuarios 5](#_heading=h.9iqpajnmnkeb)

[3.3. Entorno de usuario 5](#_heading=h.g8zly4idm1bu)

[3.4. Perfiles de los interesados 5](#_heading=h.usd3sb3xsjl4)

[3.5. Perfiles de los usuarios 5](#_heading=h.x2ma20g3fi79)

[3.6. Necesidades de los interesados y usuarios 6](#_heading=h.tvq9l6pjm0e2)

[**4. Vista General del Producto 6**](#_heading=h.r7xbzgv86n0g)

[4.1. Perspectiva del producto 6](#_heading=h.762mohi8m2wh)

[4.2. Resumen de capacidades 6](#_heading=h.7xrxsef1ebaw)

[4.3. Suposiciones y dependencias 6](#_heading=h.iibx5jlzb4ev)

[4.4. Costos y precios 6](#_heading=h.6pn3os4ah0ia)

[4.5. Licenciamiento e instalación 6](#_heading=h.gxfcpfru5jv1)

[**5. Características del producto 6**](#_heading=h.kmhs9ty7xsy3)

[**6. Restricciones 6**](#_heading=h.6me7m2v9y4wp)

[**7. Rangos de calidad 6**](#_heading=h.64qco53m18e0)

[**8. Precedencia y Prioridad 6**](#_heading=h.u0t8rtx30yt)

[**9. Otros requerimientos del producto 6**](#_heading=h.ytlg0y8m4n8d)

[9.1. Estándares legales 6](#_heading=h.m081zwhr5n5t)

[9.2. Estándares de comunicación 6](#_heading=h.vmm5c8ytftz)

[9.3. Estándares de cumplimiento de la plataforma 7](#_heading=h.13ucquo3plme)

[9.4. Estándares de calidad y seguridad 7](#_heading=h.w815adnhvd84)

[**Conclusiones 7**](#_heading=h.uvdpsopc0bg)

[**Recomendaciones 7**](#_heading=h.z4bzlog00lau)

[**Bibliografía 7**](#_heading=h.d4lklzhq5p1p)

[**Webgrafía 7**](#_heading=h.8ijjh7nv0ddk)

## **1. Introducción**

En la actualidad, con el uso masivo de dispositivos móviles, la seguridad de estos se ha vuelto una preocupación crucial para los usuarios. Las aplicaciones que instalamos en nuestros teléfonos a menudo requieren permisos que, sin que nos demos cuenta, pueden comprometer la seguridad y privacidad de nuestra información. En muchos casos, estas aplicaciones tienen acceso a datos sensibles o realizan acciones sin que el usuario tenga un control claro de las implicaciones.

La aplicación que se desarrollará está enfocada en proporcionar una herramienta eficiente y fácil de usar que permita a los usuarios tener una visión clara y precisa sobre la **seguridad** de su dispositivo móvil. La aplicación permitirá monitorear los permisos otorgados a las aplicaciones instaladas, alertando sobre posibles riesgos y brindando la posibilidad de evaluar si dichos permisos son seguros o representan una amenaza potencial. Adicionalmente, se integrará un sistema de **escaneo de red** y del dispositivo en busca de virus o datos dañinos, lo que ofrecerá una capa adicional de protección.

El desarrollo de esta solución se realizará utilizando **Flutter**, un framework que permite crear aplicaciones multiplataforma con una interfaz de usuario fluida y de alto rendimiento. Se empleará **SQLite** como base de datos local para garantizar la privacidad del usuario, ya que no se dependerá de servicios en la nube, asegurando así que los datos permanecen en el dispositivo.

En cuanto al modelo de negocio, se implementará una estrategia de **monetización dual**. Por un lado, se ofrecerá un sistema de suscripción que dará acceso a funciones avanzadas de la aplicación, y por otro, se incluirá publicidad en la parte inferior de la pantalla, diseñada de forma no intrusiva para mantener una experiencia de usuario óptima.

Este proyecto no solo tiene como objetivo proporcionar una herramienta eficaz de **seguridad móvil**, sino también empoderar a los usuarios para que tomen el control sobre la seguridad de sus dispositivos y su información personal, en un contexto en el que las amenazas digitales son cada vez más frecuentes y sofisticadas.

### **1.1. Propósito**

El propósito de este proyecto es crear una aplicación móvil que permita a los usuarios gestionar y mejorar la **seguridad de sus dispositivos** mediante el monitoreo de los permisos de aplicaciones, el análisis de redes conectadas, y la detección de posibles amenazas como virus o archivos maliciosos. La herramienta está diseñada para ofrecer **alertas proactivas** sobre riesgos potenciales y ayudar a los usuarios a tomar medidas informadas para proteger sus datos y su privacidad.

El proyecto tiene como objetivo desarrollar una **solución accesible y fácil de usar**, que no dependa de servicios en la nube, utilizando **Flutter** como framework de desarrollo y **SQLite** como base de datos local. Adicionalmente, se plantea un modelo de negocio que combine **suscripciones** para características avanzadas y la **inclusión de publicidad** de manera no intrusiva, asegurando la sostenibilidad y accesibilidad del producto.

De manera específica, esta aplicación busca:

* Proveer una **herramienta simple** y efectiva para auditar los permisos de las aplicaciones móviles.
* Facilitar el **análisis de seguridad** de redes y dispositivos para identificar amenazas activas.
* Ayudar a los usuarios a **mejorar la seguridad** de sus dispositivos con sugerencias y alertas de posibles vulnerabilidades.

Este propósito busca abordar la necesidad creciente de soluciones de **seguridad móvil**, ofreciendo una experiencia de usuario optimizada y una protección confiable.

### **1.2. Alcance**

El alcance de este proyecto está definido para desarrollar una aplicación móvil que facilite a los usuarios la gestión y mejora de la seguridad de sus dispositivos móviles. El proyecto abarcará las siguientes áreas clave:

### **1.2.1 Funcionalidades Incluidas**

* **Monitoreo de Permisos de Aplicaciones**:
  + **Visualización**: Los usuarios podrán revisar y gestionar los permisos otorgados a cada aplicación instalada en su dispositivo.
  + **Alertas**: Se notificará a los usuarios sobre permisos que pueden representar un riesgo de seguridad.
  + **Acciones**: Los usuarios tendrán la opción de modificar o revocar permisos desde la aplicación.
* **Escaneo de Seguridad del Dispositivo**:
  + **Análisis de Virus**: La aplicación detectará y alertará sobre la presencia de virus y archivos maliciosos en el dispositivo.
  + **Recomendaciones**: Se proporcionarán instrucciones para eliminar amenazas detectadas y mejorar la seguridad del dispositivo.
* **Análisis de Red**:
  + **Escaneo de Red**: La aplicación escaneará la red Wi-Fi a la que el dispositivo está conectado para identificar posibles vulnerabilidades y riesgos.
  + **Alertas**: Se alertará a los usuarios sobre posibles problemas de seguridad en la red, como dispositivos desconocidos o configuraciones inseguras.
* **Interfaz de Usuario**:
  + **Desarrollo**: Utilizando **Flutter**, se creará una interfaz de usuario que será intuitiva y fácil de usar, proporcionando una experiencia fluida en múltiples plataformas móviles.
  + **Diseño**: La aplicación tendrá un diseño atractivo y funcional, optimizado para la navegación y la interacción del usuario.
* **Base de Datos Local**:
  + **Almacenamiento**: **SQLite** se utilizará para gestionar datos localmente en el dispositivo, garantizando la privacidad y seguridad de la información del usuario.
  + **Sin Nube**: No se emplearán servicios en la nube para el almacenamiento de datos, evitando posibles riesgos asociados con la transferencia de datos a servidores externos.

### **1.2.2 Exclusiones**

* **Servicios en la Nube**:
  + La aplicación no utilizará almacenamiento en la nube ni servicios de procesamiento de datos externos, centrando toda la gestión de datos en el dispositivo del usuario.
* **Análisis de Amenazas Avanzadas**:
  + No se incluirán características de análisis de amenazas avanzadas, como integración con sistemas de inteligencia artificial para detección de amenazas emergentes.
* **Soporte para Otras Plataformas**:
  + El desarrollo se limitará a dispositivos móviles y no abarcará plataformas adicionales como **ordenadores de escritorio** o **sistemas operativos no móviles**.

### **1.2.3 Modelo de Negocio**

* **Suscripción**:
  + **Funciones Avanzadas**: Se ofrecerá un modelo de suscripción para acceder a funciones adicionales y avanzadas de la aplicación.
  + **Versión Gratuita**: Habrá una versión básica gratuita con funcionalidades esenciales para atraer a los usuarios y permitirles probar la aplicación.
* **Publicidad**:
  + **Ubicación**: La aplicación incluirá espacios publicitarios en la parte inferior de la interfaz, de manera no intrusiva para no interrumpir la experiencia del usuario.
  + Este alcance detalla claramente las funcionalidades que serán implementadas, así como las limitaciones del proyecto, asegurando una comprensión clara y compartida de los objetivos y restricciones.

### **1.3. Definiciones, Siglas y Abreviaturas**

### **1.3.1 Definiciones**

* **Aplicación Móvil (App)**: Programa de software diseñado para ser ejecutado en dispositivos móviles como teléfonos inteligentes y tabletas. En este contexto, se refiere a la aplicación que proporciona herramientas para la gestión de la seguridad del dispositivo móvil.
* **Permisos de Aplicaciones**: Autorizaciones que una aplicación solicita para acceder a ciertos recursos o información del dispositivo, como contactos, cámaras o ubicación.
* **Escaneo de Seguridad**: Proceso mediante el cual la aplicación analiza el dispositivo en busca de amenazas potenciales, como virus o archivos maliciosos.
* **Red Wi-Fi**: Conjunto de dispositivos conectados a través de una red inalámbrica que permite el intercambio de datos. La aplicación analizará la red Wi-Fi a la que está conectado el dispositivo para detectar posibles riesgos.
* **Base de Datos Local**: Sistema de almacenamiento de datos que se encuentra en el propio dispositivo del usuario, en lugar de utilizar servicios en la nube.

### **1.3.2 Siglas y Abreviaturas**

* **API (Application Programming Interface)**: Interfaz de Programación de Aplicaciones. Conjunto de reglas y herramientas que permiten la comunicación entre diferentes software o servicios.
* **Flutter**: Framework de desarrollo de aplicaciones móviles creado por Google, que permite la creación de aplicaciones para múltiples plataformas desde una sola base de código.
* **SQLite**: Sistema de gestión de bases de datos relacional ligero que se utiliza para almacenar datos localmente en aplicaciones móviles.
* **UI (User Interface)**: Interfaz de Usuario. Elementos visuales y controles con los que los usuarios interactúan en una aplicación.
* **UX (User Experience)**: Experiencia del Usuario. Conjunto de percepciones y reacciones del usuario resultantes de la interacción con una aplicación o sistema.
* **SaaS (Software as a Service)**: Software como Servicio. Modelo de distribución de software en el que las aplicaciones se hospedan en servidores y se accede a ellas a través de Internet.

### **1.4. Referencias**

* **Libros:**
  + R. E. (2021). *Mobile Application Security: Protecting Mobile Devices and Data*. Wiley.
  + Chien, E., & Harkins, S. (2020). *The Essential Guide to Mobile Security*. Apress.
* **Artículos de Revista:**
  + Zhang, K., Yang, Y., & Kuo, Y. (2019). A survey of mobile application security: Issues and solutions. *IEEE Access, 7*, 159365-159380. https://doi.org/10.1109/ACCESS.2019.2949298
  + Nasr, S., & Alwabel, M. (2020). Permission management and security analysis of mobile applications. *Journal of Cybersecurity, 14*(2), 112-124. https://doi.org/10.1093/cyber/cyaa005
* **Páginas Web:**
  + Google. (2023, January 15). *Flutter documentation*. https://flutter.dev/docs
  + SQLite. (2023). *SQLite Database Documentation*. https://sqlite.org/docs.html

### **1.5. Visión General**

#### 1.5.1 Objetivo del Proyecto

El objetivo principal de la aplicación móvil es proporcionar una solución integral y accesible para la gestión de la seguridad en dispositivos móviles. La aplicación está diseñada para cumplir con los siguientes propósitos:

* **Visualización y Gestión de Permisos**: Facilitar a los usuarios la revisión y modificación de los permisos otorgados a las aplicaciones instaladas en sus dispositivos. Esta funcionalidad permitirá a los usuarios controlar el acceso que cada aplicación tiene a sus datos y funcionalidades, contribuyendo a una mejor gestión de la privacidad y seguridad.
* **Detección de Amenazas y Análisis de Seguridad**: Ofrecer un escaneo exhaustivo del dispositivo para identificar malware, virus y otras amenazas potenciales. Adicionalmente, la aplicación evaluará la seguridad de la red a la que el dispositivo está conectado, identificando vulnerabilidades y proporcionando recomendaciones para mejorar la protección del usuario.
* **Recomendaciones y Protección del Usuario**: Proporcionar sugerencias prácticas basadas en los resultados del análisis de seguridad para optimizar la protección del dispositivo. Las recomendaciones podrán incluir la eliminación de aplicaciones inseguras, ajustes de configuración y actualizaciones necesarias para fortalecer la seguridad del dispositivo frente a amenazas emergentes.

#### 1.5.2 Contexto del Proyecto

El contexto actual está marcado por un incremento en la sofisticación de las amenazas digitales y una mayor cantidad de permisos solicitados por las aplicaciones móviles, generando una creciente preocupación entre los usuarios. La mayoría de las soluciones disponibles en el mercado no integran de manera efectiva la gestión de permisos con un análisis exhaustivo de seguridad. Este proyecto tiene como objetivo llenar esta laguna, proporcionando una plataforma integral que aborde de manera efectiva las necesidades de seguridad de los usuarios móviles.

#### 1.5.3 Alcance del Proyecto

El alcance del proyecto incluye el desarrollo de una aplicación móvil utilizando Flutter para la interfaz de usuario y SQLite para la gestión de datos locales. La aplicación se diseñará sin dependencia de servicios en la nube para asegurar el control completo sobre los datos del usuario y mejorar la eficiencia operativa. Las características clave del proyecto son:

* **Interfaz de Usuario Amigable**: Diseño intuitivo para facilitar la navegación y el uso de las funciones de seguridad.
* **Herramientas de Gestión de Permisos**: Funcionalidades que permiten a los usuarios revisar y ajustar permisos de aplicaciones de forma clara y sencilla.
* **Escaneo de Seguridad**: Capacidades para detectar y analizar amenazas en el dispositivo y la red.

#### 1.5.4 Modelo de Negocio

El modelo de negocio propuesto para la aplicación incluirá dos componentes principales:

1. **Suscripción Premium**: Ofrecimiento de características avanzadas y actualizaciones continuas mediante un modelo de suscripción, permitiendo a los usuarios acceder a herramientas adicionales para mejorar la protección de su dispositivo.
2. **Publicidad In-App**: Integración de anuncios en la parte inferior de la aplicación para generar ingresos adicionales sin interferir significativamente en la experiencia del usuario.

#### 1.5.5 Beneficios Esperados

La implementación de la aplicación proporcionará varios beneficios significativos, incluyendo:

* **Mejora en la Seguridad del Dispositivo**: Integración de gestión de permisos y análisis de seguridad para ayudar a los usuarios a proteger sus dispositivos contra amenazas y vulnerabilidades.
* **Conciencia y Control del Usuario**: Incremento en la conciencia de los usuarios sobre la seguridad de sus dispositivos, proporcionando herramientas para decisiones informadas sobre la protección de sus datos.
* **Experiencia de Usuario Optimizada**: Interfaz intuitiva y funciones avanzadas en una plataforma única para facilitar la gestión de la seguridad sin necesidad de conocimientos técnicos especializados.

## **2. Posicionamiento**

### **2.1. Oportunidad de negocio**

En el entorno actual de tecnología móvil, la seguridad de los dispositivos y la gestión de permisos se han convertido en preocupaciones primordiales para los usuarios. Con el aumento de las amenazas cibernéticas y las brechas de datos, existe una creciente demanda por soluciones que ofrezcan una protección integral y fácil de usar. La oportunidad de negocio para esta aplicación reside en:

* **Creciente Conciencia de Seguridad**: Los usuarios de dispositivos móviles están cada vez más conscientes de la importancia de la seguridad y la privacidad de sus datos. Este cambio en la percepción crea una demanda significativa para herramientas que puedan simplificar la gestión de permisos y detectar amenazas de manera efectiva.
* **Falta de Soluciones Integradas**: Muchas de las soluciones actuales en el mercado se centran únicamente en aspectos específicos de la seguridad, como el escaneo de malware o la gestión de permisos, pero no integran ambas funcionalidades en una sola plataforma. Esto crea una brecha en el mercado que esta aplicación busca llenar, ofreciendo una solución holística para la seguridad móvil.
* **Modelo de Negocio Atractivo**: El modelo de negocio propuesto, que incluye una combinación de suscripción premium y publicidad in-app, está diseñado para maximizar el alcance del mercado mientras proporciona un flujo de ingresos sostenible. La opción de suscripción ofrece características avanzadas, mientras que la publicidad permite ofrecer una versión básica gratuita para atraer a una audiencia más amplia.

### **2.2. Definición del problema**

A pesar de la disponibilidad de múltiples herramientas de seguridad para dispositivos móviles, los usuarios enfrentan varios problemas críticos que esta aplicación busca resolver:

* **Gestión Ineficiente de Permisos**: Los usuarios a menudo tienen dificultades para entender y gestionar los permisos que cada aplicación tiene sobre sus datos y funcionalidades. Esto puede resultar en una exposición innecesaria de información personal y una mayor vulnerabilidad a amenazas.
* **Falta de Visibilidad sobre Amenazas**: Las aplicaciones existentes pueden no proporcionar un análisis exhaustivo de las amenazas potenciales, incluyendo malware, virus, y vulnerabilidades en la red. Los usuarios necesitan una herramienta que les permita identificar y abordar estos riesgos de manera proactiva.
* **Desconocimiento de Medidas de Seguridad**: Los usuarios pueden carecer de conocimiento sobre las mejores prácticas para proteger sus dispositivos y datos. La falta de recomendaciones claras y prácticas puede llevar a una mayor exposición a riesgos de seguridad.

## **3. Descripción de los interesados y usuarios**

### **3.1. Resumen de los interesados**

Los interesados son individuos, grupos u organizaciones que tienen un interés directo o indirecto en el proyecto y cuyos requisitos y expectativas deben ser considerados para el éxito del mismo. Para este proyecto, los interesados principales incluyen:

* **Usuarios Finales**: Los individuos que utilizarán la aplicación para gestionar la seguridad de sus dispositivos móviles. Su satisfacción y seguridad son prioridades clave para el desarrollo del proyecto.
* **Desarrolladores y Equipo Técnico**: Incluye los programadores, diseñadores y expertos en seguridad que desarrollarán y mantendrán la aplicación. Su participación es crucial para asegurar que la aplicación funcione correctamente y se mantenga actualizada frente a nuevas amenazas.
* **Inversores y Financiadores**: Entidades o individuos que proporcionan financiamiento para el desarrollo del proyecto. Sus expectativas en cuanto a retorno de inversión y éxito comercial deben ser gestionadas adecuadamente.
* **Autoridades Reguladoras**: Organismos que pueden establecer normativas y regulaciones relacionadas con la privacidad y seguridad de los datos. Cumplir con sus requisitos es esencial para el cumplimiento legal del proyecto.

### **3.2. Resumen de los usuarios**

Los usuarios de la aplicación son los individuos que interactuarán directamente con la aplicación para gestionar la seguridad de sus dispositivos móviles. Los principales grupos de usuarios incluyen:

* **Usuarios Generales**: Personas que desean mejorar la seguridad de sus dispositivos móviles mediante la gestión de permisos y la detección de amenazas. Buscan una herramienta fácil de usar que les brinde tranquilidad y control sobre sus datos personales.
* **Usuarios Avanzados**: Individuos con un mayor conocimiento técnico que buscan características avanzadas y configuraciones personalizables para una protección más robusta. Estos usuarios pueden estar más interesados en las funcionalidades premium ofrecidas mediante suscripción.

### **3.3. Entorno de usuario**

El entorno de usuario se refiere al contexto en el que la aplicación será utilizada y los factores que pueden influir en su funcionamiento. Para este proyecto, el entorno de usuario incluye:

* **Dispositivos Móviles**: La aplicación estará diseñada para funcionar en una variedad de dispositivos móviles, incluyendo smartphones y tablets con sistemas operativos Android e iOS.
* **Redes de Datos**: La aplicación realizará análisis de la red para detectar vulnerabilidades. Los usuarios pueden estar conectados a redes Wi-Fi públicas o privadas, lo que puede influir en la efectividad del análisis de seguridad.
* **Configuraciones del Dispositivo**: Los diferentes niveles de configuración de seguridad y permisos en los dispositivos de los usuarios pueden afectar la capacidad de la aplicación para gestionar y analizar permisos.

### **3.4. Perfiles de los interesados**

Los perfiles de los interesados proporcionan una visión detallada de las expectativas y necesidades de cada grupo clave:

* **Desarrolladores**: Buscan una guía clara y requisitos precisos para desarrollar la aplicación de manera efectiva. Requieren acceso a herramientas y recursos técnicos, así como una comprensión de las expectativas del usuario.
* **Inversores**: Se enfocan en el potencial de retorno de inversión y el éxito comercial del proyecto. Esperan informes regulares sobre el progreso del desarrollo y la viabilidad del mercado.
* **Autoridades Reguladoras**: Requieren que la aplicación cumpla con todas las normativas y estándares de seguridad y privacidad aplicables. Se enfocan en el cumplimiento legal y la protección de datos personales.

### **3.5. Perfiles de los usuarios**

Los perfiles de los usuarios definen las características y necesidades específicas de los diferentes tipos de usuarios finales:

* **Usuarios Generales**: Buscan una aplicación intuitiva y fácil de usar que les permita gestionar la seguridad de sus dispositivos sin complicaciones. Valoran la simplicidad y la accesibilidad de las funcionalidades básicas.
* **Usuarios Avanzados**: Necesitan características avanzadas como configuraciones personalizables y herramientas de análisis detallado. Buscan una experiencia más técnica y son dispuestos a pagar por funciones adicionales mediante suscripción.

### **3.6. Necesidades de los interesados y usuarios**

Las necesidades de los interesados y usuarios deben ser claramente identificadas y abordadas para garantizar el éxito del proyecto:

* **Para los Desarrolladores**: Necesitan especificaciones técnicas detalladas, un entorno de desarrollo adecuado y soporte continuo para abordar cualquier problema que surja durante el proceso de desarrollo.
* **Para los Inversores**: Requieren un plan de negocio sólido, análisis de mercado, y proyecciones financieras para justificar su inversión y asegurar un retorno positivo.
* **Para las Autoridades Reguladoras**: Debe garantizarse el cumplimiento de todas las leyes y regulaciones pertinentes, incluyendo las relacionadas con la privacidad de los datos y la protección del usuario.
* **Para los Usuarios Generales**: Necesitan una aplicación que sea fácil de usar, con una interfaz intuitiva y funciones que mejoren su seguridad sin causarles inconvenientes.
* **Para los Usuarios Avanzados**: Buscan una aplicación que ofrezca características avanzadas y la capacidad de personalizar su experiencia para satisfacer sus necesidades específicas de seguridad.

## **4. Vista General del Producto**

### **4.1. Perspectiva del producto**

La aplicación para la gestión de la seguridad del dispositivo móvil es una solución integral diseñada para proporcionar a los usuarios una herramienta completa de protección y administración de permisos en sus dispositivos. La perspectiva del producto incluye:

* **Propósito**: El propósito principal de la aplicación es ofrecer una plataforma única que permita a los usuarios evaluar y gestionar los permisos de las aplicaciones instaladas, así como detectar y remediar amenazas como malware y vulnerabilidades de red. La aplicación proporciona una solución centralizada para la seguridad móvil, simplificando la gestión y aumentando la protección del usuario.
* **Audiencia Objetivo**: La aplicación está destinada tanto a usuarios generales que buscan una solución sencilla y efectiva para mejorar la seguridad de sus dispositivos, como a usuarios avanzados que requieren características más sofisticadas y configuraciones personalizables.
* **Funcionalidad Principal**: La aplicación ofrecerá características clave como la visualización de permisos de aplicaciones, escaneo de amenazas en el dispositivo, análisis de la red y recomendaciones de seguridad. Además, se integrará una función de escaneo de vulnerabilidades y detección de datos dañinos, proporcionando un enfoque integral para la seguridad móvil.

### **4.2. Resumen de capacidades**

El resumen de capacidades detalla las funcionalidades principales que la aplicación ofrecerá a los usuarios:

* **Gestión de Permisos**: Permite a los usuarios visualizar y gestionar los permisos otorgados a cada aplicación instalada en el dispositivo. Los usuarios podrán ajustar permisos de manera granular para mejorar la privacidad y la seguridad.
* **Escaneo de Amenazas**: Incluye herramientas para detectar malware, virus y otros tipos de amenazas en el dispositivo. El escaneo se realizará de manera periódica y bajo demanda, proporcionando alertas y recomendaciones para mitigar riesgos.
* **Análisis de Red**: Ofrece funcionalidades para analizar la red a la que está conectado el dispositivo, identificando posibles vulnerabilidades y amenazas relacionadas con la conexión de red.
* **Recomendaciones de Seguridad**: Basado en los análisis realizados, la aplicación proporcionará recomendaciones personalizadas para mejorar la seguridad del dispositivo, como la eliminación de aplicaciones potencialmente dañinas o la actualización de configuraciones de seguridad.
* **Modelo de Negocio**: La aplicación se ofrecerá con un modelo freemium, proporcionando acceso a funcionalidades básicas de forma gratuita, mientras que características avanzadas estarán disponibles a través de una suscripción premium. Además, se incluirán opciones de publicidad en la versión gratuita para generar ingresos adicionales.

### **4.3. Suposiciones y dependencias**

Las suposiciones y dependencias identifican los factores críticos que pueden afectar el desarrollo y la operación del producto:

* **Suposiciones**:
  + Los usuarios tienen dispositivos móviles con versiones de sistema operativo compatibles (Android e iOS).
  + La conexión a internet es necesaria para las actualizaciones de la aplicación y para el análisis de amenazas en tiempo real.
  + Los usuarios están dispuestos a pagar por características premium y a interactuar con anuncios en la versión gratuita.
* **Dependencias**:
  + **Recursos Técnicos**: El desarrollo y mantenimiento de la aplicación dependen de herramientas y tecnologías específicas, como Flutter para el desarrollo y SQLite para la gestión de datos locales.
  + **Cumplimiento Legal**: La aplicación debe cumplir con las leyes y regulaciones de protección de datos y privacidad, lo que puede requerir actualizaciones y ajustes según las normativas locales e internacionales.
  + **Actualización de Amenazas**: La eficacia del escaneo de amenazas depende de la actualización continua de las bases de datos de malware y vulnerabilidades.

### **4.4. Costos y precios**

La sección de costos y precios proporciona una visión general de los aspectos financieros asociados con el desarrollo y la operación de la aplicación:

* **Costos de Desarrollo**: Incluyen los costos asociados con el desarrollo de software, como la contratación de desarrolladores, diseñadores y expertos en seguridad, así como la compra de herramientas y licencias necesarias.
* **Costos Operativos**: Comprenden los gastos relacionados con la operación continua de la aplicación, como el mantenimiento del servidor (en caso de futuras actualizaciones que requieran conectividad en la nube), el soporte al cliente y la actualización de bases de datos de amenazas.
* **Modelo de Precios**:
  + **Versión Gratuita**: Incluye funcionalidades básicas con anuncios integrados.
  + **Suscripción Premium**: Ofrece características avanzadas y una experiencia libre de anuncios por una tarifa mensual o anual.
  + **Publicidad In-App**: Genera ingresos adicionales mediante la inclusión de anuncios en la versión gratuita de la aplicación.

### **4.5. Licenciamiento e instalación**

Esta sección describe los aspectos relacionados con el licenciamiento y el proceso de instalación de la aplicación:

* **Licenciamiento**:
  + La aplicación se ofrecerá bajo una licencia de software que define los términos y condiciones de uso, así como las restricciones aplicables a la distribución y modificación del software.
  + Las versiones premium y las características adicionales se basarán en un modelo de suscripción, con licencias específicas para el acceso a funcionalidades avanzadas.
* **Instalación**:
  + La aplicación estará disponible para su descarga e instalación desde las tiendas de aplicaciones oficiales (Google Play Store para Android y App Store para iOS).
  + El proceso de instalación será sencillo y directo, con un asistente de configuración inicial para guiar a los usuarios a través de los pasos necesarios para configurar la aplicación y comenzar a usarla.

## **5. Características del producto**

En esta sección, se detallan las características principales de la aplicación de gestión de seguridad móvil. La finalidad es ofrecer una visión clara de las funcionalidades que el producto proporcionará y cómo estas atenderán las necesidades de los usuarios. A continuación, se describen las características clave:

#### 5.1 Gestión de Permisos de Aplicaciones

* **Visualización de Permisos**: Los usuarios podrán ver todos los permisos concedidos a cada aplicación instalada, como acceso a la cámara, micrófono, contactos, y ubicación.
* **Ajuste de Permisos**: Permite modificar o revocar permisos específicos, otorgando control sobre qué datos pueden acceder las aplicaciones.
* **Alertas de Permisos Inusuales**: Notificaciones para permisos que no suelen ser necesarios para el funcionamiento de las aplicaciones, ayudando a identificar posibles riesgos.

#### 5.2 Escaneo de Amenazas

* **Análisis de Malware**: Escaneos periódicos para detectar malware, virus y otros software maliciosos, con informes detallados sobre cualquier amenaza encontrada.
* **Detección de Datos Dañinos**: Identificación de datos corruptos o dañinos, con opciones para eliminar o reparar estos datos.
* **Historial de Escaneos**: Acceso a un historial de escaneos y resultados, facilitando el seguimiento continuo de la salud del dispositivo.

#### 5.3 Análisis de Red

* **Monitoreo de Conexiones de Red**: Análisis de la red a la que está conectado el dispositivo para identificar vulnerabilidades o amenazas.
* **Alertas de Actividad Sospechosa**: Notificaciones sobre actividades sospechosas en la red, como conexiones a redes inseguras.
* **Informe de Seguridad de Red**: Informes sobre el estado de la red con recomendaciones para mejorar la seguridad de la conexión.

#### 5.4 Recomendaciones de Seguridad

* **Sugerencias Personalizadas**: Recomendaciones basadas en el análisis de seguridad para mejorar la protección del dispositivo.
* **Consejos Educativos**: Información sobre buenas prácticas de seguridad móvil para ayudar a los usuarios a proteger sus datos.

#### 5.5 Modelo de Negocio

* **Versión Gratuita**: Funcionalidades básicas con anuncios en la parte inferior para generar ingresos.
* **Suscripción Premium**: Acceso a características avanzadas y una experiencia sin anuncios, con opciones de pago mensual o anual.
* **Publicidad In-App**: Anuncios ubicados en la parte inferior de la aplicación en la versión gratuita para mantener la generación de ingresos sin interrumpir la experiencia del usuario.

#### 5.6 Interfaz de Usuario y Experiencia

* **Diseño Intuitivo**: Interfaz fácil de usar y navegar, adecuada para usuarios de todos los niveles.
* **Personalización**: Opciones para ajustar notificaciones y el aspecto visual de la aplicación.
* **Soporte Multilenguaje**: Disponibilidad en varios idiomas para alcanzar una audiencia global.

#### 5.7 Integraciones Futuras

* **Compatibilidad con Dispositivos IoT**: Posibilidad de integrarse con dispositivos IoT para una seguridad más amplia.
* **Actualizaciones Continuas**: Mejoras regulares para añadir nuevas funcionalidades y adaptarse a amenazas emergentes.

## **6. Restricciones**

La sección de **Restricciones** en el documento de visión define las limitaciones y condiciones que deben considerarse durante el desarrollo y la implementación del producto. Identificar y documentar estas restricciones es esencial para gestionar expectativas y planificar de manera efectiva. A continuación, se detallan las restricciones clave del proyecto para la aplicación de gestión de seguridad móvil:

#### 6.1 Limitaciones Técnicas

* **Compatibilidad de Dispositivos**: La aplicación se desarrollará en Flutter, lo que garantiza compatibilidad con la mayoría de los dispositivos móviles modernos. Sin embargo, la compatibilidad completa con versiones anteriores de sistemas operativos o dispositivos de bajo rendimiento podría ser limitada. Específicamente, la aplicación podría enfrentar dificultades en dispositivos con versiones antiguas de Android o iOS debido a restricciones de hardware o software.
* **Limitaciones de SQLite**: Aunque SQLite es una opción robusta para almacenamiento local, tiene limitaciones en comparación con soluciones de bases de datos basadas en la nube. Las limitaciones incluyen la capacidad de almacenamiento y la falta de soporte para ciertas características avanzadas como la sincronización en tiempo real y el análisis en la nube. Esto puede afectar la capacidad de la aplicación para manejar grandes volúmenes de datos o integrarse con otras aplicaciones y servicios de manera eficiente.

#### 6.2 Restricciones de Seguridad

* **Acceso a Permisos del Sistema**: Debido a las políticas de seguridad y privacidad de los sistemas operativos móviles, la aplicación puede tener acceso limitado a ciertos permisos y funciones del sistema. Por ejemplo, las aplicaciones móviles generalmente no pueden acceder a información de otros procesos en el dispositivo, lo que podría limitar la capacidad de la aplicación para realizar análisis de seguridad exhaustivos.
* **Protección de Datos**: La aplicación debe cumplir con regulaciones y estándares de protección de datos, como el GDPR en Europa o la CCPA en California. Las restricciones en el manejo y almacenamiento de datos personales pueden limitar las capacidades de análisis y la recopilación de datos, requiriendo mecanismos adicionales para garantizar el cumplimiento normativo.

#### 6.3 Restricciones Financieras

* **Presupuesto de Desarrollo**: El desarrollo de la aplicación está sujeto a un presupuesto limitado, lo que puede restringir la implementación de ciertas características avanzadas o la contratación de personal adicional para el desarrollo y pruebas. Este presupuesto también puede afectar la capacidad para realizar actualizaciones frecuentes o invertir en campañas de marketing extensas.
* **Modelo de Ingresos**: La dependencia de modelos de ingresos basados en suscripción y publicidad puede influir en el diseño de la aplicación y en la experiencia del usuario. Las restricciones relacionadas con la colocación de anuncios y la estructura de precios de la suscripción deben ser cuidadosamente equilibradas para maximizar la rentabilidad sin comprometer la satisfacción del usuario.

#### 6.4 Restricciones de Tiempo

* **Cronograma de Desarrollo**: El proyecto debe adherirse a un cronograma de desarrollo establecido, lo que puede limitar el tiempo disponible para la implementación de características adicionales o para pruebas exhaustivas. Los plazos ajustados pueden afectar la calidad final del producto y la capacidad para abordar problemas o implementar mejoras sugeridas durante el desarrollo.
* **Actualizaciones y Mantenimiento**: El tiempo disponible para el mantenimiento y la actualización continua del producto puede ser limitado. Esto puede restringir la capacidad para abordar rápidamente nuevas amenazas de seguridad o para implementar mejoras basadas en comentarios de los usuarios.

#### 6.5 Restricciones Regulatorias

* **Cumplimiento de Normativas**: La aplicación deberá cumplir con diversas normativas y regulaciones de seguridad móvil y privacidad, las cuales pueden imponer restricciones adicionales sobre las características y funcionalidades del producto. Las leyes locales e internacionales deben ser consideradas para asegurar que la aplicación no infrinja ninguna normativa.

#### 6.6 Restricciones Operativas

* **Dependencia de la Conectividad**: Algunas funcionalidades, como el análisis en la nube o el monitoreo en tiempo real, pueden depender de una conexión a Internet estable. La falta de conectividad puede limitar la eficacia de ciertas características de la aplicación y afectar la experiencia del usuario.

## **7. Rangos de calidad**

La sección de **Rangos de Calidad** en un documento de visión define los criterios y estándares que el producto debe cumplir para ser considerado exitoso en términos de calidad. Esta sección proporciona una guía clara sobre cómo se medirá la calidad del producto y qué expectativas deben cumplirse para garantizar la satisfacción del usuario y el cumplimiento de los requisitos del proyecto. A continuación, se detallan los rangos de calidad clave para la aplicación de gestión de seguridad móvil:

#### 7.1 Criterios de Rendimiento

* **Velocidad de Respuesta**: La aplicación debe responder a las interacciones del usuario en un plazo de menos de 2 segundos para garantizar una experiencia de usuario fluida. Las operaciones de escaneo y análisis deben completarse en un tiempo razonable, no superior a 5 minutos, dependiendo del tamaño de los datos y la complejidad del análisis.
* **Estabilidad**: La aplicación debe funcionar sin fallos ni errores críticos. Se establece un objetivo de no más del 1% de fallos por usuario al mes. La estabilidad se medirá a través de pruebas rigurosas y el monitoreo continuo de errores reportados por los usuarios.
* **Uso de Recursos**: La aplicación debe ser eficiente en el uso de recursos del dispositivo, incluyendo CPU, memoria y batería. El consumo de batería debe ser optimizado para no superar el 10% de la batería del dispositivo durante un uso prolongado. La aplicación debe utilizar menos del 20% de la memoria RAM disponible durante las operaciones de escaneo.

#### 7.2 Criterios de Seguridad

* **Protección de Datos**: La aplicación debe cumplir con los estándares de protección de datos, garantizando la seguridad de la información personal del usuario. Los datos deben ser cifrados en tránsito y en reposo, cumpliendo con las normativas de protección de datos como GDPR y CCPA.
* **Detección de Amenazas**: El sistema de escaneo debe tener una tasa de detección de malware y amenazas del 95% o más. Los falsos positivos deben ser inferiores al 5% para minimizar la interrupción en la experiencia del usuario.
* **Actualizaciones de Seguridad**: La aplicación debe ser actualizada al menos una vez al mes para abordar nuevas amenazas de seguridad y vulnerabilidades. Las actualizaciones deben ser implementadas de manera eficiente para asegurar que el producto esté siempre protegido contra los riesgos emergentes.

#### 7.3 Criterios de Usabilidad

* **Facilidad de Uso**: La aplicación debe ser intuitiva y fácil de navegar, con una curva de aprendizaje mínima. Las pruebas de usabilidad deben mostrar una tasa de éxito del 90% o más en tareas comunes realizadas por nuevos usuarios.
* **Accesibilidad**: La aplicación debe ser accesible para personas con discapacidades, cumpliendo con las directrices de accesibilidad del contenido web (WCAG). Se debe proporcionar soporte para lectores de pantalla y opciones de personalización de interfaz para mejorar la accesibilidad.
* **Soporte Multilenguaje**: La aplicación debe ofrecer soporte para al menos 3 idiomas principales, con traducciones precisas y culturalmente apropiadas. La calidad de las traducciones debe ser verificada por hablantes nativos para asegurar la claridad y precisión.

#### 7.4 Criterios de Compatibilidad

* **Compatibilidad de Dispositivos**: La aplicación debe ser compatible con las versiones de sistema operativo móvil más utilizadas (Android 10 y superiores, iOS 14 y superiores). Se debe garantizar el funcionamiento en una gama amplia de dispositivos, desde teléfonos de gama baja hasta gama alta.
* **Interoperabilidad**: La aplicación debe integrarse de manera efectiva con otros servicios y aplicaciones móviles según sea necesario, como servicios de correo electrónico y herramientas de análisis. Las integraciones deben funcionar correctamente sin causar conflictos o fallos en el sistema.

#### 7.5 Criterios de Escalabilidad

* **Escalabilidad del Rendimiento**: La aplicación debe ser capaz de manejar un aumento en el número de usuarios y datos sin degradar el rendimiento. Debe soportar un crecimiento en la base de usuarios de hasta un 50% anual sin requerir rediseños significativos.
* **Escalabilidad de Funcionalidades**: La arquitectura de la aplicación debe permitir la adición de nuevas funcionalidades y características en el futuro sin afectar negativamente a las características existentes. Las nuevas características deben integrarse de manera fluida y eficiente.

## **8. Precedencia y Prioridad**

La sección de **Precedencia y Prioridad** en un documento de visión define el orden de importancia y la secuencia en la que se deben abordar las características, funcionalidades y requisitos del producto. Establecer precedencias y prioridades es crucial para gestionar los recursos eficientemente, garantizar que se cumplan los objetivos del proyecto y satisfacer las expectativas de los usuarios. A continuación, se detallan las precedencias y prioridades clave para la aplicación de gestión de seguridad móvil:

#### 8.1 Precedencia de Funcionalidades

* **Escaneo de Seguridad**: La capacidad de escanear el dispositivo móvil en busca de malware, vulnerabilidades y amenazas debe ser la funcionalidad principal y prioritaria. Esto incluye el desarrollo de un motor de escaneo eficiente y preciso que pueda identificar y mitigar riesgos de seguridad. La implementación de esta funcionalidad debe completarse en las primeras fases del desarrollo, ya que es esencial para la propuesta de valor del producto.
* **Gestión de Permisos de Aplicaciones**: La funcionalidad para revisar y gestionar los permisos de las aplicaciones instaladas en el dispositivo es una característica complementaria crítica. Debe permitir a los usuarios ver qué permisos están siendo solicitados por cada aplicación y ajustar o revocar permisos según sea necesario. Esta funcionalidad debe ser implementada inmediatamente después del escaneo de seguridad para proporcionar una protección adicional y control sobre la privacidad del usuario.
* **Análisis de Red**: La capacidad para escanear la red y detectar posibles vulnerabilidades o amenazas, como la presencia de virus o datos dañinos, es una característica importante pero de menor prioridad en comparación con el escaneo de seguridad y la gestión de permisos. Esta funcionalidad debe ser desarrollada después de haber establecido las capacidades fundamentales del producto y optimizada según los resultados de las pruebas iniciales.

#### 8.2 Prioridades de Desarrollo

* **Alta Prioridad**:
  + **Rendimiento y Estabilidad**: Asegurar que la aplicación funcione de manera estable y eficiente en una variedad de dispositivos es crucial. Esto incluye pruebas exhaustivas para garantizar que la aplicación no tenga fallos críticos y que el rendimiento sea óptimo bajo condiciones normales de uso.
  + **Protección de Datos**: Implementar mecanismos sólidos para proteger la información personal del usuario, cumpliendo con normativas como GDPR y CCPA, debe ser una prioridad alta. La seguridad de los datos es fundamental para la confianza del usuario y la integridad del producto.
* **Media Prioridad**:
  + **Usabilidad y Accesibilidad**: La interfaz de usuario debe ser intuitiva y accesible para todos los usuarios, incluidas las personas con discapacidades. Aunque es fundamental para la experiencia del usuario, su desarrollo puede seguir a las funcionalidades centrales una vez que estas estén establecidas y funcionando.
  + **Compatibilidad**: Asegurar que la aplicación sea compatible con las versiones actuales de los sistemas operativos móviles y una gama amplia de dispositivos es importante, pero puede ser abordado después de implementar las funcionalidades clave.
* **Baja Prioridad**:
  + **Escalabilidad de Funcionalidades**: Aunque es importante planificar la escalabilidad para futuras actualizaciones y características adicionales, esta prioridad puede ser gestionada después de haber asegurado el éxito de las funcionalidades principales y el rendimiento general de la aplicación.
  + **Soporte Multilenguaje**: La integración de soporte para múltiples idiomas puede ser implementada en fases posteriores, una vez que las funcionalidades principales estén operativas y el producto esté estable en el mercado inicial.

#### 8.3 Plan de Implementación

* **Fase 1: Implementación Inicial**: Enfocada en las funcionalidades de escaneo de seguridad y gestión de permisos, junto con el desarrollo de una infraestructura estable para el manejo de datos y la protección de la privacidad.
* **Fase 2: Expansión de Funcionalidades**: Incorporación de capacidades de análisis de red y refinamiento de características existentes basadas en los comentarios de los usuarios y pruebas de rendimiento.
* **Fase 3: Optimización y Escalabilidad**: Mejora de la escalabilidad y la integración de soporte multilenguaje, junto con la implementación de características adicionales según la demanda del mercado y el feedback de los usuarios.

## **9. Otros requerimientos del producto**

Esta sección cubre aspectos adicionales esenciales para garantizar el éxito, la conformidad y la seguridad de la aplicación de gestión de seguridad móvil. Estos requerimientos abarcan estándares legales, de comunicación, de cumplimiento de plataforma y de calidad y seguridad, y son cruciales para una implementación adecuada y eficaz del producto.

### **9.1. Estándares legales**

**Cumplimiento Normativo**: La aplicación debe adherirse a las leyes y regulaciones pertinentes en cada región donde esté disponible. Esto incluye, pero no se limita a, las regulaciones de protección de datos como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos, y otras legislaciones locales que puedan aplicarse. Es esencial garantizar que la recolección, almacenamiento y procesamiento de datos personales se realicen de acuerdo con estas normativas.

**Políticas de Privacidad y Términos de Uso**: Deben desarrollarse políticas de privacidad claras y accesibles, que expliquen cómo se recopilan, utilizan y protegen los datos del usuario. Los términos de uso deben detallar las responsabilidades y derechos tanto del usuario como del proveedor de la aplicación. Estas políticas deben estar disponibles dentro de la aplicación y en el sitio web asociado.

### **9.2. Estándares de comunicación**

**Seguridad de la Comunicación**: La aplicación debe implementar protocolos de comunicación segura, como HTTPS y TLS, para cifrar la transmisión de datos entre el dispositivo del usuario y los servidores. Esto protegerá la información contra interceptaciones y accesos no autorizados.

**Notificaciones y Alertas**: Las comunicaciones en tiempo real, como notificaciones de amenazas y alertas de seguridad, deben ser confiables y entregarse sin demoras significativas. Se deben establecer mecanismos robustos para asegurar que estas comunicaciones sean precisas y oportunas.

### **9.3. Estándares de cumplimiento de la plataforma**

**Requisitos de las Tiendas de Aplicaciones**: La aplicación debe cumplir con los lineamientos y políticas establecidas por las principales tiendas de aplicaciones, como Google Play Store y Apple App Store. Esto incluye directrices sobre privacidad, seguridad y prácticas de desarrollo aceptables. La aplicación debe ser revisada y aprobada por estas plataformas antes de su publicación.

**Compatibilidad y Actualizaciones**: Debe garantizarse la compatibilidad con las versiones actuales de los sistemas operativos móviles y una variedad de dispositivos. La aplicación debe ser actualizada regularmente para adaptarse a cambios en las plataformas y mejorar su funcionalidad y seguridad.

### **9.4. Estándares de calidad y seguridad**

* **Normas de Calidad del Software**: La aplicación debe seguir estándares de calidad como los establecidos por la norma ISO/IEC 25010, que incluye aspectos como funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y portabilidad. Estas normas aseguran que el producto sea robusto y cumpla con las expectativas del usuario.
* **Pruebas de Seguridad y Auditorías**: Se deben realizar pruebas de seguridad exhaustivas y auditorías de código para identificar y corregir vulnerabilidades. Las pruebas deben incluir análisis de penetración y revisiones de seguridad para asegurar que la aplicación esté protegida contra amenazas emergentes y ataques cibernéticos.
* **Soporte y Gestión de Incidencias**: La aplicación debe contar con un sistema eficiente para la gestión de incidencias y un equipo de soporte técnico disponible para resolver problemas reportados por los usuarios. Este soporte debe incluir actualizaciones regulares y soluciones rápidas para cualquier problema que surja.

## **Conclusiones**

* La aplicación propuesta ofrece una solución integral para identificar y gestionar problemas de seguridad en dispositivos móviles. Su capacidad para analizar permisos, detectar vulnerabilidades y escanear redes establece una barrera robusta contra amenazas potenciales, alineándose con las crecientes preocupaciones sobre la seguridad móvil.
* Con una interfaz amigable y capacidades avanzadas, la aplicación no solo cumple con los requisitos técnicos, sino que también proporciona una experiencia de usuario intuitiva. Esto es crucial para fomentar la adopción generalizada y efectiva de la herramienta.
* La combinación de suscripciones y publicidad en la parte inferior de la app permite una monetización efectiva sin comprometer la experiencia del usuario. Este modelo es flexible y se adapta a diferentes estrategias de mercado y preferencias del usuario.
* La solución está diseñada para ser adaptable a futuras actualizaciones y escalable para incluir nuevas características y mejoras, garantizando su relevancia a largo plazo en el dinámico campo de la seguridad móvil.

## **Recomendaciones**

* Es recomendable realizar actualizaciones periódicas para abordar nuevas amenazas y vulnerabilidades emergentes. Mantener un equipo dedicado a la investigación y desarrollo asegurará que la aplicación se mantenga a la vanguardia de la seguridad móvil.
* Implementar un proceso riguroso de pruebas beta para recopilar retroalimentación de usuarios reales antes del lanzamiento definitivo. Esto permitirá identificar y corregir problemas antes de la distribución general.
* Desarrollar materiales educativos y recursos dentro de la aplicación para informar a los usuarios sobre prácticas de seguridad móvil y cómo maximizar el uso de las herramientas ofrecidas.
* Realizar un seguimiento continuo de las tendencias y cambios en el mercado de aplicaciones de seguridad para ajustar la estrategia de monetización y las características del producto según las expectativas del usuario y las condiciones del mercado.

## **Bibliografía**

**Libros:**

* R. E. (2021). *Mobile application security: Protecting mobile devices and data*. Wiley.
* Chien, E., & Harkins, S. (2020). *The essential guide to mobile security*. Apress.

**Artículos de Revista:**

* Zhang, K., Yang, Y., & Kuo, Y. (2019). A survey of mobile application security: Issues and solutions. *IEEE Access, 7*, 159365-159380.<https://doi.org/10.1109/ACCESS.2019.2949298>
* Nasr, S., & Alwabel, M. (2020). Permission management and security analysis of mobile applications. *Journal of Cybersecurity, 14*(2), 112-124.<https://doi.org/10.1093/cyber/cyaa005>

## **Webgrafía**

**Páginas Web:**

* Google. (2023, January 15). *Flutter documentation*.<https://flutter.dev/docs>
* SQLite. (2023). *SQLite database documentation*.<https://sqlite.org/docs.html>