****

**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERÍA**

**Escuela Profesional de Ingeniería de Sistemas**

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

Curso: *Construcción de Software 1*

Docente: Mag. Ricardo Eduardo Valcárcel Alvarado

Integrantes:

Jose Luis Jarro Cachi 2020067148

**Tacna – Perú**

***2024***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CONTROL DE VERSIONES | | | | | |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | Jose Jarro Cachi | Mag. Ricardo Valcárcel | Mag. Ricardo Valcárcel | 14/09/2024 | Avance de la primera versión del documento |

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

**Documento de SRS**

**Versión *1.0***

**INDICE GENERAL**

**Contenido**

[**Desarrollo de Especificación de Requerimientos** 4](#_heading=h.gjdgxs)

[I) Generalidades de la empresa: 4](#_heading=h.30j0zll)

[1) Nombre de la Empresa: 4](#_heading=h.1fob9te)

[2) Visión: 4](#_heading=h.1fob9te)

[3) Misión: 4](#_heading=h.3znysh7)

[4) Organigrama: 4](#_heading=h.2et92p0)

[II) Visionamiento de la Empresa: 4](#_heading=h.tyjcwt)

[1) Descripción del problema: 4](#_heading=h.3dy6vkm)

[2) Objetivos de negocio: 4](#_heading=h.1t3h5sf)

[3) Objetivos de diseño: 4](#_heading=h.4d34og8)

[4) Alcance del proyecto: 4](#_heading=h.2s8eyo1)

[5) Viabilidad del sistema: 4](#_heading=h.17dp8vu)

[6) Información obtenida del levantamiento del sistema: 4](#_heading=h.3rdcrjn)

[III) Análisis de procesos: 4](#_heading=h.26in1rg)

[1) Diagrama del proceso actual-Diagrama de actividades 4](#_heading=h.lnxbz9)

[2) Diagrama del proceso propuesto-Diagrama de actividades inicial 4](#_heading=h.35nkun2)

[IV) Especificaciones de requerimiento de software: 4](#_heading=h.1ksv4uv)

[1) Cuadros de requerimiento funcionales Inicial: 4](#_heading=h.44sinio)

[2) Cuadro de requerimientos no funcionales: 4](#_heading=h.2jxsxqh)

[3) Cuadro de requerimientos funcionales final: 4](#_heading=h.z337ya)

[V) Fase de desarrollo: 4](#_heading=h.3j2qqm3)

[1) Perfiles de usuario: 4](#_heading=h.1y810tw)

[2) Modelo conceptual: 4](#_heading=h.4i7ojhp)

[3) Modelo Lógico: 5](#_heading=h.2xcytpi)

[VI) Conclusiones 5](#_heading=h.1ci93xb)

[VII) Recomendaciones 5](#_heading=h.3whwml4)

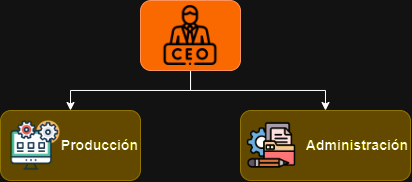
[VIII) Bibliografía 5](#_heading=h.2bn6wsx)

[IX) Webgrafía 5](#_heading=h.qsh70q)

**Desarrollo de Especificación de Requerimientos**

1. **Generalidades de la empresa:**
   1. Nombre de la Empresa:

* Secure AI Mobile
  1. Visión:
* Aspiramos a ser líderes globales en el desarrollo de soluciones tecnológicas avanzadas, resolviendo los desafíos más complejos de nuestros clientes mediante innovación continua y excelencia operativa. Nuestro objetivo es establecer estándares de calidad y eficiencia superiores en la configuración de software, impulsando el crecimiento y éxito de nuestros clientes a nivel mundial. Nos comprometemos a ser un referente en la transformación digital, guiando a las organizaciones hacia un futuro sostenible y competitivo.
  1. Misión:
* Nos especializamos en ofrecer soluciones tecnológicas de vanguardia que impulsan la eficiencia, seguridad y transformación digital de nuestros clientes. A través de un enfoque centrado en la excelencia y la colaboración, garantizamos una gestión integral de la configuración del software, priorizando la calidad y seguridad en cada fase del desarrollo. Nuestro compromiso es optimizar los procesos empresariales, reducir costos operativos y fortalecer la competitividad de nuestros clientes en un entorno tecnológico en constante evolución.
  1. Organigrama:



Descripción: Se colocó el presente organigrama con la intención de visualizar gráficamente la estructura organizacional de la empresa y señalar los departamentos que estarían involucrados en la ejecución del proyecto.

1. **Visionamiento de la Empresa:**
   1. Descripción del problema:

En proyectos de desarrollo de software, particularmente en entornos colaborativos, se presentan desafíos significativos en la gestión eficaz de recursos humanos y el monitoreo del progreso de las tareas. La ausencia de una plataforma centralizada y robusta para la gestión de estos aspectos puede dar lugar a retrasos en la entrega, falta de transparencia en el avance del proyecto y dificultades en la comunicación entre los miembros del equipo. Estas deficiencias pueden resultar en sobrecostos y en el incumplimiento de los plazos establecidos, afectando adversamente la satisfacción del cliente y comprometiendo la rentabilidad del negocio. La falta de un control adecuado sobre estos elementos críticos no solo disminuye la eficiencia operativa, sino que también limita la capacidad de la organización para alcanzar sus metas estratégicas y proporcionar soluciones de alta calidad a sus clientes.

En este contexto, Secure AI Mobile se posiciona como una empresa dedicada a abordar estas problemáticas mediante la implementación de soluciones tecnológicas avanzadas. Nuestra misión es optimizar la gestión de proyectos, proporcionando un marco integral y eficiente para la supervisión, coordinación y entrega de resultados. Al integrar herramientas de vanguardia, buscamos mejorar la visibilidad del progreso, facilitar la comunicación efectiva y garantizar el cumplimiento de los plazos y presupuestos establecidos, fortaleciendo así la capacidad de nuestras organizaciones clientes para alcanzar el éxito en sus iniciativas tecnológicas**.**

* 1. Objetivo General:

Desarrollar e implementar soluciones tecnológicas de vanguardia que optimicen la gestión de proyectos de software y mejoren la eficiencia en la administración de recursos humanos en entornos colaborativos. Nuestro objetivo es proporcionar herramientas integradas que garanticen una visibilidad clara del progreso, faciliten una comunicación efectiva y aseguren una coordinación fluida entre los equipos. Buscamos maximizar la puntualidad y el cumplimiento presupuestario de los proyectos, elevando así la satisfacción del cliente y potenciando la rentabilidad del negocio mediante la adopción de metodologías ágiles y tecnología avanzada.

* + 1. Objetivos Específicos:

**Facilitar el seguimiento del progreso de los proyectos**: Permitir a los equipos y gerentes visualizar en tiempo real cómo avanza cada etapa, lo que mejora la coordinación y el control del proyecto.

**Proporcionar un sistema eficiente para la asignación de roles y responsabilidades**: Asegurar que cada miembro del equipo tenga tareas claras y los cronogramas se cumplan de manera óptima.

**Desarrollar una herramienta de gestión de cronogramas**: Permitir no solo planificar las actividades, sino también recibir alertas sobre posibles retrasos y facilitar la reprogramación en caso necesario.

**Ofrecer la capacidad de generar informes detallados y métricas clave:** Para posibilitar a los responsables del proyecto el poder de tomar decisiones informadas y así optimizar los tiempos de entrega.

**Incorporar un sistema de control de calidad a lo largo del ciclo de vida del proyecto**: Garantizar que los productos entregados cumplan con los estándares definidos desde el inicio hasta su finalización.

**Diseñar una interfaz intuitiva y accesible**: Posibilitar al usuario, sin importar su nivel técnico, poder interactuar fácilmente con el sistema y acceder a toda la información relevante sobre sus proyectos.

* 1. Alcance del proyecto:

El proyecto tiene como objetivo el desarrollo e implementación de un aplicativo móvil avanzado para la evaluación de seguridad en dispositivos móviles. Este sistema integral está diseñado para identificar vulnerabilidades, evaluar riesgos y ofrecer recomendaciones para mejorar la protección de los dispositivos.

El aplicativo proporcionará funcionalidades clave, incluyendo un proceso de registro e inicio de sesión seguro, con accesos diferenciados según el rol de cada usuario. Permitirá la realización de análisis detallados de seguridad, generando reportes comprensivos que ofrecerán una visión clara del estado de seguridad del dispositivo y sugerencias específicas para la mitigación de riesgos.

Una característica esencial será el seguimiento en tiempo real, que permitirá a los usuarios monitorear constantemente el estado de seguridad de sus dispositivos, recibiendo alertas y actualizaciones sobre posibles amenazas. Además, el sistema integrará capacidades de análisis predictivo para anticipar vulnerabilidades y proponer soluciones preventivas.

La aplicación contará con una interfaz intuitiva y de fácil uso, permitiendo a los usuarios personalizar la configuración del análisis de seguridad según sus necesidades. También se incluirá soporte técnico continuo y actualizaciones periódicas para garantizar la efectividad del sistema frente a nuevas amenazas y cambios en el entorno de seguridad. En conjunto, el aplicativo ofrecerá una solución robusta para la gestión y protección de la seguridad en dispositivos móviles.

* 1. Viabilidad del sistema:

La viabilidad del sistema propuesto para la evaluación de seguridad en dispositivos móviles se analiza en términos técnicos, económicos y operativos.

* El proyecto es viable técnicamente, ya que el desarrollo del aplicativo se basa en tecnologías móviles modernas y prácticas de seguridad robustas. Utilizaremos frameworks y lenguajes de programación ampliamente aceptados, garantizando compatibilidad y escalabilidad con diferentes sistemas operativos móviles, como iOS y Android. Las herramientas para análisis de seguridad y evaluación predictiva estarán integradas con protocolos de seguridad avanzados para proteger la integridad y confidencialidad de los datos. La arquitectura del sistema estará diseñada para adaptarse a actualizaciones futuras y nuevos desafíos en el ámbito de la ciberseguridad.
* Es viable económicamente, ya que se el proyecto se ajusta a un presupuesto realista, que cubre el desarrollo, implementación, mantenimiento y soporte del sistema. La inversión inicial está orientada a la creación de una solución de alta calidad que pueda ofrecer retornos significativos a través de la mejora en la seguridad de los dispositivos móviles. Los costos se distribuirán entre el desarrollo de software, adquisición de licencias y herramientas necesarias, y la capacitación del personal. Se anticipa que la inversión en el aplicativo contribuirá a una reducción de costos asociados con incidentes de seguridad y mejorará la eficiencia operativa.
* Es viable operativamente, ya que la implementación del sistema será gestionada a través de un enfoque estructurado que incluye fases de planificación, desarrollo, pruebas y despliegue. Se ofrecerá capacitación y soporte técnico para garantizar una transición fluida y una adopción efectiva por parte de los usuarios. La interfaz intuitiva del aplicativo permitirá a los usuarios navegar y utilizar el sistema con facilidad, minimizando la curva de aprendizaje. Además, el soporte continuo y las actualizaciones periódicas asegurarán que el sistema permanezca eficaz frente a nuevas amenazas y tecnologías emergentes.
  1. Información obtenida del levantamiento del sistema:

El levantamiento del sistema ha proporcionado información esencial que ha guiado el desarrollo del aplicativo móvil para la evaluación de seguridad en dispositivos móviles. Este proceso reveló varios aspectos clave que han sido fundamentales para definir el enfoque y las características del sistema.

* Primero, se identificaron los requisitos del usuario, que destacan la necesidad de altos niveles de seguridad y privacidad para proteger la información sensible. Los usuarios exigen análisis exhaustivos de vulnerabilidades, alertas en tiempo real sobre amenazas potenciales y recomendaciones claras para mitigar riesgos. Además, se subrayó la importancia de una interfaz de usuario intuitiva y accesible, que facilite la navegación y el uso del sistema para personas con diversos niveles de experiencia técnica.
* Desde una perspectiva técnica, el sistema debe ser compatible con las principales plataformas móviles, como iOS y Android. Esto implica la utilización de tecnologías que permitan una integración efectiva con estos sistemas operativos y la incorporación de herramientas avanzadas para el análisis de seguridad y la evaluación predictiva, asegurando una protección robusta contra amenazas emergente.
* En términos operativos, los usuarios requieren capacitación adecuada para utilizar el sistema de manera efectiva, junto con soporte técnico continuo para resolver problemas y mantener el sistema actualizado. Se ha destacado la necesidad de realizar actualizaciones periódicas para adaptarse a nuevas amenazas y tecnologías, garantizando que el aplicativo se mantenga relevante y eficaz.
* El levantamiento también ha revelado ciertas limitaciones y desafíos. En particular, se han identificado restricciones en recursos y presupuesto que deben ser gestionadas eficientemente para cumplir con los objetivos del proyecto. La adaptación del sistema por parte de los usuarios finales también puede presentar desafíos, como resistencia al cambio o falta de familiaridad con nuevas tecnologías.

1. **Análisis de procesos:**
   1. Diagrama del proceso actual-Diagrama de actividades:

* **Proceso de identificación de la configuración**
  + Proceso actual de la identificación de la configuración.

Mapa de colores

Descripción generada automáticamente con confianza baja

*Nota: El archivo ‘Proceso actual de la identificación de la configuracion.png' se encuentra en la carpeta 'Anexos'.*

El diagrama de flujo muestra el proceso típico que sigue un usuario desde la descarga de una aplicación móvil hasta la modificación o aceptación de los permisos que esta solicita. El proceso está organizado en cinco áreas principales: Usuario, Interfaz, Aplicación, Configuración y Permisos. A continuación se detalla cada etapa:

* **Usuario**

**Inicio**: El proceso comienza cuando el usuario toma la acción inicial de descargar una aplicación móvil.

* + (*A*): El usuario decide descargar la aplicación sin verificar los permisos solicitados.

**Descarga la app sin revisar permisos**: Una vez descargada, la aplicación solicita permisos durante la instalación.

* + (*B*): La aplicación solicita permisos que pueden incluir acceso a funciones como la cámara, ubicación, o contactos.

**App solicita permisos durante la instalación**: En este punto, el usuario se enfrenta a la decisión de revisar o no los permisos solicitados por la aplicación.

* + (*C*): El sistema presenta al usuario una pantalla en la que se muestra una lista de permisos requeridos.

**¿El usuario revisa los permisos?**: Aquí, el proceso bifurca en dos caminos posibles.

* + (*D*): La decisión se basa en si el usuario revisa los permisos solicitados o los acepta sin leer.
* **Interfaz**
  + **¿El usuario revisa los permisos?**: Dependiendo de la decisión tomada:
    - **No**: Si el usuario no revisa los permisos, simplemente acepta todos los permisos predeterminados.
      * (*E*): El usuario otorga automáticamente todos los permisos solicitados por la aplicación.
    - **Sí**: Si el usuario decide revisar los permisos, la interacción continúa con la posibilidad de modificar esos permisos.
      * (*F*): El usuario intenta acceder a las opciones de modificación de permisos a través de la interfaz del sistema.
* **Aplicación**
  + **Usuario intenta modificar permisos**: Al optar por modificar los permisos, el usuario interactúa con las configuraciones internas de la aplicación.
    - (*F*): El usuario navega hacia la configuración de la aplicación en su dispositivo.
  + **Busca la sección de 'Aplicaciones'**: En la interfaz del dispositivo, el usuario localiza la sección donde se administra la configuración de aplicaciones.
    - (*G*): El usuario ingresa al menú de configuración de aplicaciones.
  + **Selecciona la app**: El usuario elige la aplicación que acaba de instalar para revisar los permisos que le ha otorgado.
    - (*H*): Dentro de la sección de aplicaciones, selecciona la app para revisar sus detalles.
  + **Revisa permisos otorgados**: El usuario puede visualizar la lista de permisos que la aplicación ha solicitado y aquellos que ya han sido concedidos.
    - (*I*): Se muestra al usuario los permisos activos y puede decidir si quiere modificarlos o dejarlos tal cual.
* **Configuración**
  + **¿Modificar permisos?**: El proceso llega a un nuevo punto de decisión. El usuario debe elegir si desea modificar los permisos predeterminados de la aplicación.
    - (*J*): El usuario evalúa si está satisfecho con los permisos concedidos o si prefiere cambiarlos.
    - **No**: Si el usuario no modifica los permisos, el proceso se dirige hacia la instalación final de la app con los permisos originales.
      * (*K*): La aplicación se instala con los permisos predeterminados y el proceso finaliza.
    - **Sí**: Si el usuario decide modificar los permisos, realiza cambios manuales en las configuraciones.
      * (*L*): El usuario ajusta los permisos de manera individual, aceptando o revocando según su preferencia.
* **Permisos**
  + **El usuario modifica manualmente los permisos**: En caso de que el usuario elija modificar permisos, puede realizar ajustes individuales.
    - (*L*): Los permisos seleccionados manualmente por el usuario se aplican a la aplicación.
  + **Fin**: Una vez que el usuario ha ajustado o aceptado los permisos, el proceso concluye con la configuración exitosa de la aplicación.
    - (*M*): El proceso finaliza y la aplicación está lista para ser utilizada con los permisos configurados.
* **Proceso Propuesto** 
  + Proceso Propuesto

Gráfico

Descripción generada automáticamente

*Nota: El archivo ‘Proceso actual de informe de estado.png' se encuentra en la carpeta 'Anexos'.*

* El diagrama de flujo describe el proceso que un usuario sigue al interactuar con una aplicación móvil para gestionar los permisos necesarios desde la configuración de seguridad del dispositivo. Este proceso se organiza en cinco áreas principales: Usuario, Interfaz, Aplicación, Configuración y Finalización. A continuación, se detalla cada etapa:
* **Usuario**
  + **Inicio**: El proceso comienza cuando el usuario decide gestionar los permisos de una aplicación.
  + **(A)**: El usuario abre la aplicación de configuración de seguridad en su dispositivo.
* **Interfaz**
  + - **Solicitud de Permisos**: Una vez dentro de la configuración de seguridad, la aplicación solicita los permisos necesarios para su funcionamiento.
    - **(B)**: La aplicación presenta un aviso para que el usuario otorgue acceso a los permisos requeridos.
* **Aplicación**
  + - **Decisión sobre la Aceptación de Permisos**: En este punto, el usuario debe decidir si acepta los permisos solicitados por la aplicación.
    - **(C)**: Se presenta una opción para que el usuario confirme si acepta los permisos necesarios.
* **Configuración**
  + - **Opciones tras la Decisión**: Dependiendo de la elección del usuario, el proceso bifurca en dos caminos:
    - **No**: Si el usuario decide no aceptar los permisos, el proceso sigue hacia una configuración predeterminada.
    - **(D)**: Se establecen los permisos de manera predeterminada, limitando las funcionalidades de la aplicación.
    - **Sí**: Si el usuario acepta los permisos, tiene la opción de modificar configuraciones y permisos adicionales.
    - **(E)**: El usuario accede a las configuraciones para ajustar permisos y opciones de la aplicación.
* **Finalización**
  + - **Fin del Proceso**: Una vez que el usuario ha modificado las configuraciones según su preferencia, el proceso concluye.
    - **(F)**: El proceso finaliza, y la aplicación está lista para ser utilizada con los permisos ajustados.
    - Esta narrativa resume de manera clara y estructurada el proceso que un usuario sigue al gestionar los permisos de una aplicación móvil, enfatizando la importancia de la toma de decisiones y la configuración adecuada para el uso óptimo de la aplicación en términos de seguridad y funcionalidad.
  1. Diagrama del proceso propuesto-Diagrama de actividades inicial:

1. **Especificaciones de requerimiento de software:**
   1. Cuadros de requerimiento funcionales Inicial:

|  |  |  |
| --- | --- | --- |
| ID | Requerimiento Funcional | Descripción |
| RF01 | **Login** | Pantalla de inicio de sesión donde los usuarios ingresan sus credenciales. |
| RF02 | **Register Screen** | Pantalla para el registro de nuevos usuarios que permite crear una cuenta en la aplicación. |
| RF04 | **Dashboard** | Pantalla principal que muestra un resumen de la seguridad del dispositivo tras el inicio de sesión. |
| RF04 | **Alertas y Notificaciones** | Sección para mostrar alertas sobre amenazas detectadas y notificaciones relevantes para el usuario. |
| RF05 | **Resumen de Seguridad** | Muestra un resumen visual de la situación de seguridad del dispositivo. |
| RF06 | **Configuración de Seguridad** | Pantalla que permite al usuario modificar las configuraciones de seguridad del dispositivo. |
| RF07 | **Escaneo de Seguridad** | Funcionalidad para realizar un escaneo de seguridad del dispositivo y detectar posibles vulnerabilidades. |
| RF08 | **Historial de Análisis** | Sección donde se almacena y muestra el historial de análisis realizados por la aplicación. |
| RF09 | **Aplicaciones Instaladas** | Sección que muestra todas las aplicaciones instaladas en el dispositivo y su estado de seguridad. |
| RF10 | **Detalles de App** | Pantalla que muestra detalles específicos sobre cada aplicación instalada, incluyendo permisos y configuraciones. |
| RF11 | **App Permissions** | Gestión de permisos que la aplicación solicita al usuario para acceder a funciones del dispositivo. |
|  |  |  |

* 1. Cuadro de requerimientos no funcionales:

|  |  |  |  |
| --- | --- | --- | --- |
| **Nro.** | **R.N Funcional** | **Descripción** | **Prioridad** |
| RNF01 | Rendimiento | La aplicación debe responder a las acciones del usuario en menos de 2 segundos. | Alta |
| RNF02 | Usabilidad | La interfaz de usuario debe ser intuitiva y fácil de navegar para todos los usuarios. | Alta |
| RNF03 | Seguridad | La aplicación debe garantizar la protección de los datos del usuario mediante cifrado. | Alta |
| RNF04 | Compatibilidad | La aplicación debe ser compatible con las versiones más recientes de Android e iOS. | Alta |
| RNF05 | Mantenibilidad | El código de la aplicación debe estar bien documentado y estructurado para facilitar su mantenimiento. | Media |
| RNF06 | Escalabilidad | La aplicación debe poder manejar un aumento en el número de usuarios sin comprometer el rendimiento. | Alta |
| RNF07 | Accesibilidad | La aplicación debe ser accesible para personas con discapacidades, siguiendo pautas de accesibilidad. | Media |
| RNF08 | Estética | El diseño visual debe ser atractivo y coherente con la identidad de la aplicación. | Media |
| RNF09 | Interoperabilidad | La aplicación debe poder integrarse con otras aplicaciones y servicios relevantes. | Baja |
| RNF10 | Fiabilidad | La aplicación debe tener una tasa de fallos baja, asegurando su disponibilidad en todo momento. | Alta |

* 1. Requerimientos funcionales final

|  |  |  |
| --- | --- | --- |
| ID | Requerimiento Funcional | Descripción |
| RF-1 | **Inicio de Sesión** | El usuario debe poder iniciar sesión en la aplicación utilizando su nombre de usuario y contraseña. |
| RF-2 | **Registro de Usuario** | El usuario debe poder registrarse en la aplicación proporcionando información personal y de contacto. |
| RF-3 | **Dashboard** | El usuario debe tener acceso a un dashboard que muestre información relevante sobre la seguridad del dispositivo. |
| RF-4 | **Alertas y Notificaciones** | La aplicación debe enviar alertas y notificaciones sobre posibles amenazas de seguridad. |
| RF-5 | **Configuración de Seguridad** | El usuario debe poder acceder a la configuración de seguridad y ajustar preferencias. |
| RF-6 | **Escaneo de Seguridad** | La aplicación debe permitir al usuario realizar un escaneo de seguridad del dispositivo. |
| RF-7 | **Historial de Análisis** | El usuario debe poder visualizar un historial de análisis realizados por la aplicación. |
| RF-8 | **Perfil de Usuario** | El usuario debe poder acceder y modificar su perfil de usuario dentro de la aplicación. |
| RF-9 | **Reporte de Análisis** | La aplicación debe generar y permitir la descarga de reportes sobre el estado de seguridad. |
| RF-10 | **Resumen de Seguridad** | El usuario debe poder ver un resumen de la seguridad del dispositivo y las aplicaciones instaladas. |
| RF-12 | **Detalles de Aplicación** | El usuario debe poder acceder a información detallada sobre cada aplicación instalada. |
| RF-13 | **Gestión de Permisos** | La aplicación debe permitir al usuario gestionar los permisos otorgados a cada aplicación instalada. |

1. **Fase de desarrollo:**
   1. Perfiles de usuario:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  | | --- | | **Perfil de Usuario** : Cliente | | **Descripcion:**Este perfil representa al cliente que utilizará la aplicación para gestionar la seguridad de su dispositivo | | **Funcionalidades:** | | Iniciar sesión y gestionar su perfil. Configurar permisos y configuraciones de seguridad. Realizar escaneos de seguridad y recibir resultados. Generar y revisar informes sobre el estado de seguridad. Ver y gestionar notificaciones relacionadas con la seguridad | |  |
|  |  |
| |  | | --- | | **Perfil de Usuario** : Soporte Técnico | | **Descripcion**: Este perfil es utilizado por el personal de soporte técnico que asiste a los usuarios en la configuración y solución de problemas. | | **Funcionalidades:** | | * Acceder a información del usuario para brindar soporte. * Ver historiales de análisis y configuraciones realizadas por el usuario. * Proporcionar asistencia en la configuración de la aplicación. * Generar tickets de soporte para problemas reportados. *  Comunicar cambios o actualizaciones importantes a los usuarios. | |  |

|  |
| --- |
| **Perfil de Usuario** : Administrador |
| **Descripcion:** Este perfil es utilizado por el administrador del sistema, encargado de gestionar y supervisar las configuraciones y el funcionamiento de la aplicación |
| **Funcionalidades:** |
| Gestionar cuentas de usuarios (crear, editar, eliminar).  Configurar políticas de seguridad para todos los usuarios.  Monitorear el uso y el rendimiento de la aplicación.  Revisar informes de análisis de seguridad de todos los usuarios.  Enviar notificaciones y alertas sobre cambios importantes en la seguridad. |

* 1. Modelo conceptual:
     1. Diagrama de paquetes:

Diagrama

Descripción generada automáticamente

* + 1. Diagrama de casos de uso:

Diagrama

Descripción generada automáticamenteCaso de uso : Inicio de Sesión

Caso de uso : Registro de Usuario

Diagrama

Descripción generada automáticamente con confianza media

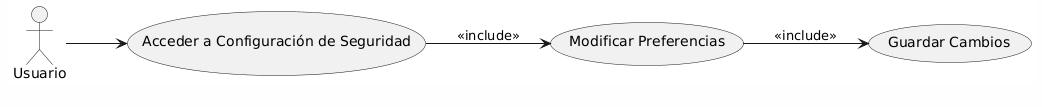
Diagrama

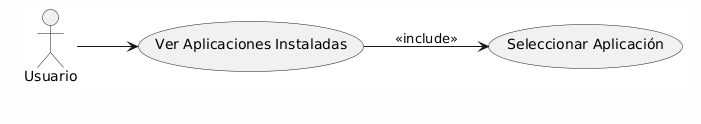
Descripción generada automáticamenteCaso de uso : Dashboard

Diagrama

Descripción generada automáticamenteDiagrama

Descripción generada automáticamenteCaso de uso : Alertas y Notificaciones

Caso de uso : Configuración de Seguridad

Caso de uso: escaneo de seguridad

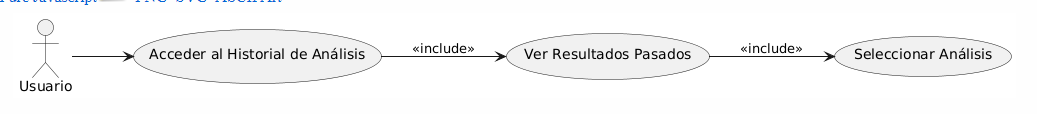
Caso de uso :Historial de análisis

Imagen que contiene Diagrama

Descripción generada automáticamenteCaso de uso: perfil de usuario

Diagrama

Descripción generada automáticamente con confianza mediaCaso de uso : Reporte de Análisis

Imagen que contiene Texto

Descripción generada automáticamenteCaso de uso :Resusmen de seguridad

Diagrama

Descripción generada automáticamenteCaso de uso :Aplicaciones Instaladas

Caso de uso: Detalles de Aplicación

Diagrama

Descripción generada automáticamente

**Narrativa del Caso de Uso: Inicio de Sesion**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea iniciar sesión en el sistema. El usuario deberá ingresar sus credenciales (usuario y contraseña). |
| **Precondiciones** | El usuario tiene que tener la aplicación instalada (apk) |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| 1. El usaurio debe ubicarse en la pantalla de su celular y luego tiene que realizar la bsuqueda del aplicacativo (apk) | 1. El usuario hace click en el icono de la aplicación y luego se le mostrara la pantalla de incio de sesion. |
| 1. El usuario visualiza la caja de texto donde se puede ingresar el correo electronico y debajo la caja de texto del apartado de contraseña , adeas de la caja de texto | 1. El sistema valida las credenciales. |
| 1. El usuario hace clic en "Iniciar Sesión". | 1. El sistema permite el acceso al sistema si las credenciales son correctas. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |
| El usuario no ingresa credenciales válidas o deja campos vacíos. | El sistema muestra un mensaje de error indicando que se deben ingresar credenciales válidas. |

**Narrativa del Caso de Uso: Registro de Usuario**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando un usuario desea registrarse en el sistema, proporcionando datos personales para crear una cuenta. |
| **Precondiciones** | El usuario debe acceder a la opción de registro. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| 1. El usuario accede a la opción de "Registro". | 2. El sistema muestra un formulario para ingresar datos personales y credenciales de acceso. |
| 3. El usuario ingresa los datos necesarios. | 4. El sistema valida los datos proporcionados. |
| 5. El usuario hace clic en "Registrar". | 6. El sistema guarda los datos en la base de datos y confirma el registro. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |
| El usuario no completa todos los campos requeridos. | El sistema muestra un mensaje de error indicando que todos los campos son obligatorios. |

**Narrativa del Caso de Uso: Acceder a Perfil de Usuario**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando un usuario autenticado desea acceder y modificar su perfil personal |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| 1. El usuario accede a la sección "Perfil de Usuario". | 2. El sistema muestra la información personal del usuario. |
| 3. El usuario edita la información del perfil. | 4. El sistema valida los cambios y guarda la información actualizada. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |
| El usuario no completa correctamente los campos al editar el perfil. | El sistema muestra un mensaje de error indicando los campos obligatorios. |

**Narrativa del Caso de Uso: Acceder al Dashboard**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando un usuario autenticado accede al dashboard para visualizar información de seguridad. |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| |  | | --- | | 1. El usuario accede a la sección "Dashboard". | | |  | | --- | | 2. El sistema muestra información de seguridad, incluyendo alertas y análisis recientes. | |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso: Recibir Alertas y Notificaciones**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el sistema envía alertas y notificaciones al usuario sobre posibles amenazas o eventos importantes. |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El sistema genera una alerta de seguridad. | El sistema envía la notificación al usuario, quien puede visualizar los detalles. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso: Iniciar Escaneo de Seguridad**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario decide realizar un escaneo de seguridad en su dispositivo para detectar posibles vulnerabilidades. |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario accede a la sección "Escaneo de Seguridad". | El sistema muestra las opciones de escaneo disponibles. |
| El usuario selecciona el tipo de escaneo y lo inicia. | El sistema ejecuta el escaneo y muestra los resultados una vez finalizado. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso: Ver Resultados del Escaneo**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea ver los resultados del escaneo de seguridad previamente realizado. |
| **Precondiciones** | El usuario debe haber realizado un escaneo de seguridad. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario accede a la sección de resultados de escaneo. | El sistema muestra los resultados del análisis, incluyendo las vulnerabilidades detectadas. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso: Acceder a Resumen de Seguridad**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea ver un resumen general del estado de seguridad de su dispositivo. |
| **Precondiciones** | El usuario debe acceder a la opción de registro. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario accede a la sección "Resumen de Seguridad". | El sistema muestra el estado general del dispositivo y los gráficos de seguridad. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso:** **Acceder al Historial de Análisis**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea ver el historial de análisis de seguridad realizados. |
| **Precondiciones** | El usuario debe acceder a la opción de registro. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario accede a la sección "Historial de Análisis". | El sistema muestra una lista de los análisis realizados en el pasado. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso:** **Generar Reporte de Análisis**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea generar un reporte detallado del análisis de seguridad realizado. |
| **Precondiciones** | El usuario debe haber realizado un escaneo de seguridad. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario selecciona la opción para generar un reporte de análisis. | El sistema genera el reporte en formato descargable y lo presenta al usuario. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso:** **Ver Aplicaciones Instaladas**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea ver la lista de aplicaciones instaladas en su dispositivo. |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario accede a la sección "Aplicaciones Instaladas". | El sistema muestra una lista de las aplicaciones instaladas en el dispositivo. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso:** **Analizar Aplicación Instalada**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario selecciona una aplicación instalada para analizarla y verificar si tiene vulnerabilidades de seguridad. |
| **Precondiciones** | El usuario debe estar autenticado y tener aplicaciones instaladas en el dispositivo. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario selecciona una aplicación de la lista. | El sistema muestra información detallada sobre la aplicación y analiza sus vulnerabilidades. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso:** **Consultar Base de Conocimientos**

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea consultar la base de conocimientos del sistema para buscar información sobre amenazas o vulnerabilidades. |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa del caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario accede a la sección "Base de Conocimientos". | El sistema muestra un buscador y permite consultar temas relacionados con seguridad. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

**Narrativa del Caso de Uso:** **Cerrar Sesión**

|  |  |
| --- | --- |
| **Diagrama de Secuencia del Caso de Uso Registro de Usuarios** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea cerrar sesión en el sistema. |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario selecciona la opción "Cerrar Sesión". | El sistema cierra la sesión del usuario y redirige a la pantalla de inicio de sesión. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |

* 1. Modelo Lógico:
     1. Análisis de objetivos:
     2. Diagrama de actividades con objetos:

Diagrama de Actividades con Objetos incluirá los objetos involucrados en las operaciones "Iniciar Sesión", "Registro de Usuario" y "Acceder a Perfil de Usuario".

Diagrama

Descripción generada automáticamente

**Narrativa de los Diagramas de Casos de Uso**

**1. Diagrama de Casos de Uso: Autenticación y Perfil de Usuario (RF-1, RF-2, RF-8)**

Este diagrama ilustra el proceso de autenticación y gestión del perfil de usuario dentro de la aplicación.

* **Inicio de Sesión**: El usuario inicia el proceso al intentar **Iniciar Sesión** en la aplicación.
  + **Validación de Credenciales**: Se verifica la autenticidad de las credenciales ingresadas. Este paso es fundamental para garantizar la seguridad del acceso.
  + **Mensaje de Error**: Si las credenciales no son válidas, se activa un **Mensaje de Error** que alerta al usuario.
* **Registro de Usuario**: Alternativamente, si el usuario no tiene una cuenta, puede optar por el **Registro de Usuario**.
  + **Verificación de Información**: Aquí, la aplicación comprueba que la información proporcionada cumpla con los requisitos establecidos.
    - **Confirmación de Registro**: Si la verificación es exitosa, el registro se confirma, permitiendo al usuario acceder a la plataforma.
    - **Mensaje de Error**: En caso de que la información no sea válida, se presenta un **Mensaje de Error**.
* **Acceso al Perfil de Usuario**: Una vez autenticado, el usuario puede **Acceder a su Perfil**.
  + **Modificación de Información**: El usuario tiene la opción de **Modificar Información de Perfil**.
    - **Guardar Cambios**: Finalmente, los cambios realizados se pueden **Guardar**, asegurando que el perfil esté actualizado.

Diagrama de Actividades con Objetos: Dashboard y Alertas (RF-3, RF-4)

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

**Diagrama de Casos de Uso: Dashboard y Alertas (RF-3, RF-4)**

Este diagrama aborda la interacción del usuario con el **Dashboard** y el sistema de alertas.

* **Acceso al Dashboard**: El usuario accede a un panel central donde puede visualizar información crucial.
  + **Visualización de Información de Seguridad**: Desde el dashboard, el usuario puede **Visualizar Información de Seguridad** que resume el estado general de la aplicación.
  + **Visualización de Alertas**: También puede **Visualizar Alertas**, manteniéndose informado sobre posibles riesgos.
* **Recepción de Alertas y Notificaciones**: El usuario puede recibir alertas en tiempo real.
  + **Mostrar Detalles de Amenaza**: Si una alerta se activa, el usuario tiene la opción de **Mostrar Detalles de Amenaza**, lo que proporciona información adicional sobre el riesgo identificado.

Diagrama de Actividades con Objetos: Seguridad y Escaneo (RF-5, RF-6, RF-10)

Diagrama

Descripción generada automáticamente

**Diagrama de Casos de Uso: Seguridad y Escaneo (RF-5, RF-6, RF-10)**

Este diagrama destaca las funciones de seguridad y escaneo dentro de la aplicación.

* **Acceso a Configuración de Seguridad**: El usuario inicia el proceso accediendo a la configuración de seguridad.
  + **Modificación de Preferencias**: En esta sección, puede **Modificar Preferencias** relacionadas con la seguridad.
    - **Guardar Cambios**: Después de realizar ajustes, el usuario debe **Guardar Cambios** para que se apliquen.
* **Iniciar Escaneo de Seguridad**: El usuario puede **Iniciar Escaneo de Seguridad** para evaluar el estado del sistema.
  + **Mostrar Resultados de Escaneo**: Una vez finalizado el escaneo, se presentan los **Resultados de Escaneo**.
    - **Generar Informe de Análisis**: Se puede **Generar Informe de Análisis** que detalla las vulnerabilidades detectadas.
    - **Mostrar Vulnerabilidades**: Además, el usuario tiene la opción de **Mostrar Vulnerabilidades** que pueden requerir atención.
* **Acceso a Resumen de Seguridad**: Finalmente, el usuario puede acceder a un **Resumen de Seguridad**.
  + **Ver Estado del Dispositivo**: Aquí puede **Ver Estado del Dispositivo**, obteniendo una visión general.
  + **Ver Gráficos de Seguridad**: También tiene la opción de **Ver Gráficos de Seguridad**, facilitando la interpretación de datos.

Diagrama de Actividades con Objetos: Historial y Reportes (RF-7, RF-9)

Diagrama

Descripción generada automáticamente

**Diagrama de Casos de Uso: Historial y Reportes (RF-7, RF-9)**

Este diagrama se centra en la gestión del historial de análisis y la generación de reportes.

* **Acceso al Historial de Análisis**: El usuario puede **Acceder al Historial de Análisis** realizado previamente.
  + **Ver Resultados Pasados**: Desde aquí, puede **Ver Resultados Pasados**, analizando la evolución de la seguridad.
    - **Seleccionar Análisis**: Puede elegir un análisis específico para obtener información detallada.
* **Generar Reporte de Análisis**: El usuario también tiene la opción de **Generar Reporte de Análisis**.
  + **Descargar Reporte**: Al finalizar, puede **Descargar Reporte** que resume los hallazgos y recomendaciones.

Diagrama de Actividades con Objetos: Aplicaciones y Gestión de Permisos (RF-11, RF-12, RF-13, RF-14)

Tabla

Descripción generada automáticamente con confianza media

**Diagrama de Casos de Uso: Aplicaciones y Gestión de Permisos (RF-11, RF-12, RF-13, RF-14)**

Este diagrama describe la interacción del usuario con las aplicaciones instaladas y la gestión de permisos.

* **Ver Aplicaciones Instaladas**: El usuario inicia accediendo a la lista de **Aplicaciones Instaladas** en el dispositivo.
  + **Seleccionar Aplicación**: Desde esta lista, puede **Seleccionar Aplicación** para obtener más detalles.
* **Ver Detalles de Aplicación**: Al seleccionar una aplicación, el usuario puede **Ver Detalles de Aplicación**.
  + **Ver Permisos**: Aquí, puede revisar los **Permisos** requeridos por la aplicación.
  + **Ver Consumo de Recursos**: También tiene la opción de **Ver Consumo de Recursos**, informándole sobre el uso de la memoria y la batería.
* **Gestionar Permisos de Aplicaciones**: El usuario puede **Gestionar Permisos de Aplicaciones**.
  + **Actualizar Permisos**: Desde aquí, puede **Actualizar Permisos** para ajustar las autorizaciones necesarias.
* **Personalizar Tema**: Finalmente, el usuario puede **Personalizar Tema**.
  + **Seleccionar Opciones**: Puede **Seleccionar Opciones** de personalización.
  + **Guardar Cambios**: Al finalizar, es crucial **Guardar Cambios** para aplicar su configuración.

* + 1. Diagrama de secuencia:

Diagrama de Secuencia: Autenticación y Perfil de Usuario (RF-1, RF-2, RF-8)

Una captura de pantalla de una computadora

Descripción generada automáticamente

Narrativa del Diagrama de Secuencia: Autenticación y Perfil de Usuario (RF-1, RF-2, RF-8)

|  |  |
| --- | --- |
| **Diagrama de Secuencia del Caso de Uso Autenticación y Perfil de Usuario (RF-1, RF-2, RF-8)** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea autenticarse o gestionar su perfil en el sistema. |
| **Precondiciones** | El usuario no debe estar autenticado si desea iniciar sesión.  El usuario debe estar autenticado para acceder al perfil. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario selecciona la opción "Iniciar Sesión". | El sistema solicita las credenciales del usuario. |
| El usuario ingresa su nombre de usuario y contraseña. | El sistema valida las credenciales. |
| Si las credenciales son válidas: | El sistema inicia la sesión y redirige al usuario al dashboard. |
| Si las credenciales son inválidas: | El sistema muestra un mensaje de error. |
| El usuario selecciona "Registro de Usuario". | El sistema solicita la información necesaria para el registro. |
| El usuario ingresa la información requerida. | El sistema verifica la información. |
| Si la información es válida: | El sistema confirma el registro y permite el inicio de sesión. |
| Si la información es inválida: | El sistema muestra un mensaje de error. |
| El usuario accede a su perfil. | El sistema muestra la información del perfil del usuario. |
| El usuario modifica su información de perfil. | El sistema solicita confirmar los cambios. |
| El usuario confirma los cambios. | El sistema guarda la nueva información en la base de datos. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |
| |  | | --- | | El usuario intenta iniciar sesión sin credenciales. | | El sistema muestra un mensaje indicando que se requieren credenciales. |

Interfaz de usuario gráfica

Descripción generada automáticamenteDiagrama de Secuencia: Dashboard y Alertas (RF-3, RF-4)

Narrativa del Diagrama de Secuencia: Dashboard y Alertas (RF-3, RF-4)

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario accede al dashboard para visualizar la información de seguridad y alertas. |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario accede al dashboard. | |  | | --- | | El sistema carga y muestra la información de seguridad. |  |  | | --- | |  | |
| El usuario solicita ver alertas. | El usuario solicita ver alertas. |
| |  | | --- | | El sistema notifica al  usuario sobre amenazas. |  |  | | --- | |  | | |  | | --- | | El usuario selecciona una alerta para ver más detalles. |  |  | | --- | |  | |
| |  | | --- | | El sistema muestra los  detalles de la amenaza. | |  |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |
| |  | | --- | | El usuario no tiene alertas. |  |  | | --- | |  | | El sistema muestra un mensaje indicando que no hay alertas. |

Diagrama de Secuencia: Seguridad y Escaneo (RF-5, RF-6, RF-10)

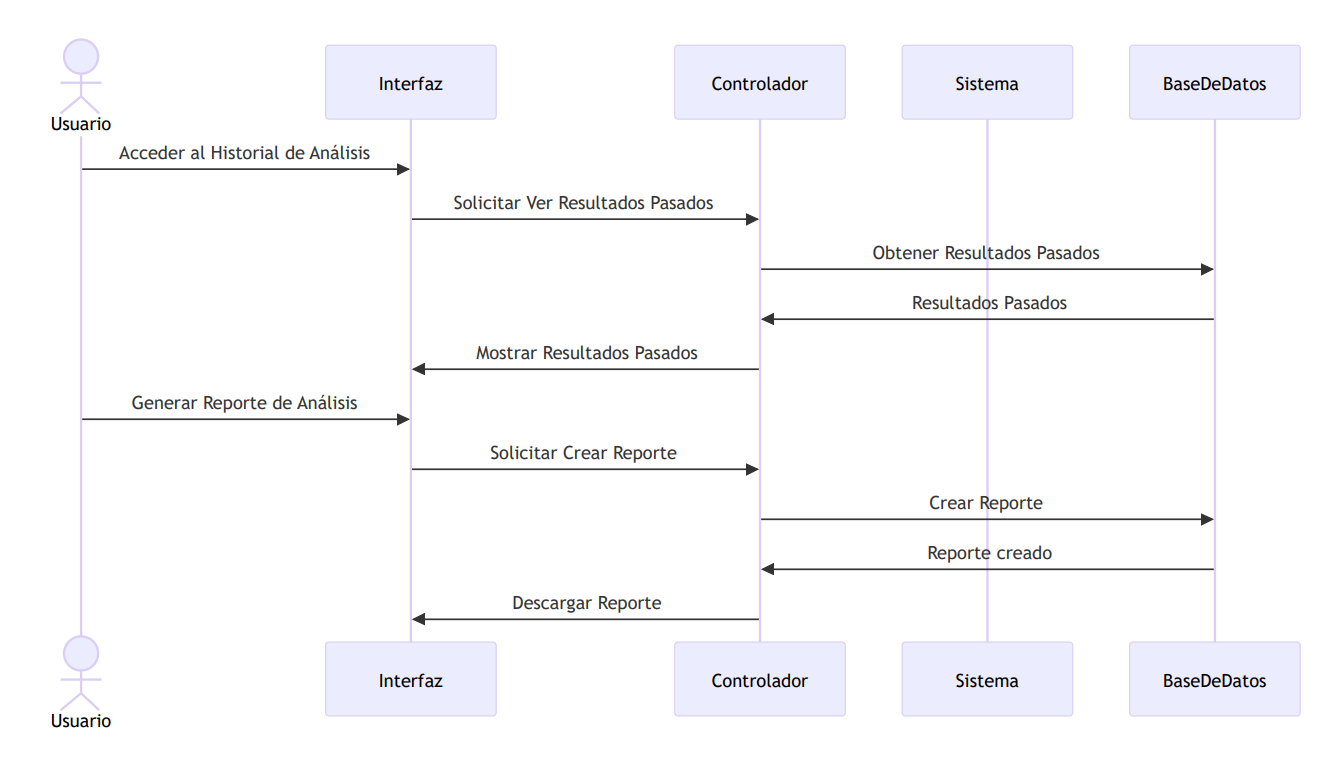
Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Narrativa del Diagrama de Secuencia: Seguridad y Escaneo (RF-5, RF-6, RF-10)

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario accede a la configuración de seguridad o inicia un escaneo de seguridad. |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario accede a la configuración de seguridad. | |  | | --- | | El sistema muestra las preferencias de seguridad. | |
| El usuario modifica las preferencias. | |  | | --- | | El sistema solicita confirmación de los cambios. |  |  | | --- | |  | |
| El usuario confirma los cambios. | El sistema guarda los cambios en la base de datos. |
| El usuario inicia un escaneo de seguridad. | El sistema comienza el escaneo. |
| El sistema muestra los resultados del escaneo. | El usuario selecciona ver el informe de análisis. |
| El sistema genera y muestra el informe. |  |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |
| El usuario intenta iniciar un escaneo sin permisos. | **El sistema muestra un mensaje indicando que no tiene permisos.** |

Diagrama de Secuencia: Historial y Reportes (RF-7, RF-9)



Narrativa del Diagrama de Secuencia: Historial y Reportes (RF-7, RF-9)

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea acceder al historial de análisis o generar un reporte. |
| **Precondiciones** | El usuario debe estar autenticado en el sistema. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario accede al historial de análisis. | El sistema carga y muestra los resultados pasados. |
| El usuario selecciona un análisis anterior. | |  | | --- | | El sistema muestra los detalles de ese análisis. | |
| El usuario solicita generar un reporte. | El sistema crea el reporte basado en los análisis seleccionados. |
| El sistema confirma la creación del reporte. | El usuario puede descargar el reporte generado. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |
| El usuario no tiene historial de análisis. | El sistema muestra un mensaje indicando que no hay análisis previos. |

Diagrama de Secuencia: Aplicaciones y Gestión de Permisos (RF-11, RF-12, RF-13, RF-14)

Diagrama

Descripción generada automáticamente con confianza media

Narrativa del Diagrama de Secuencia: Aplicaciones y Gestión de Permisos (RF-11, RF-12, RF-13, RF-14)

|  |  |
| --- | --- |
| **Narrativa caso de uso** | |
| **Tipo** | Obligatorio |
| **Versión** | V 1.0 |
| **Autor(es)** | Jose Luis JARRO CACHI |
| **Actores** | Usuario |
| **Descripción** | El caso de uso se inicia cuando el usuario desea ver un resumen general del estado de seguridad de su dispositivo. |
| **Precondiciones** | El usuario debe acceder a la opción de registro. |
| **Narrativa caso de uso** | |
| **Acción del Actor** | **Respuesta del Sistema** |
| El usuario ve las aplicaciones instaladas. | El sistema muestra el estado general del dispositivo y los gráficos de seguridad. |
| El usuario selecciona una aplicación. | |  | | --- | | El sistema muestra los detalles y permisos de la aplicación. | |
| El usuario gestiona permisos de la aplicación. | |  | | --- | | El sistema solicita actualizar los permisos seleccionados. | |
| El usuario confirma los cambios. | |  | | --- | | El sistema guarda los cambios en la base de datos. | |
| El usuario personaliza el tema de la interfaz. | |  | | --- | | El sistema muestra opciones de personalización. | |
| El usuario selecciona opciones y confirma cambios. | El sistema guarda los cambios y actualiza la interfaz. |
| **Flujo de Excepciones – FE1** | |
| Acción del Actor | **Respuesta del sistema** |
| El usuario intenta gestionar permisos sin autorización. | El sistema muestra un mensaje indicando que no tiene permisos. |

* + 1. Diagrama de clases:

Diagrama

Descripción generada automáticamente

**Diagrama de Clases: Descripción en Lenguaje Natural**

**Objetivo del Diagrama de Clases**

El diagrama de clases es una representación visual que muestra las diferentes entidades del sistema y cómo se relacionan entre sí. Este diagrama ayuda a entender la estructura general de la aplicación y los roles de cada clase.

**Clases Principales**

1. **Usuario**
   * **Atributos**:
     + **Nombre**: Representa el nombre del usuario.
     + **Correo**: El correo electrónico del usuario.
     + **Contraseña**: La contraseña utilizada para autenticarse.
     + **Rol**: Define el rol del usuario en el sistema (por ejemplo, administrador o cliente).
   * **Métodos**:
     + **Iniciar Sesión**: Permite al usuario acceder al sistema.
     + **Cerrar Sesión**: Permite al usuario salir del sistema.
     + **Modificar Perfil**: Permite al usuario actualizar su información personal.
2. **Perfil**
   * **Atributos**:
     + **Información Personal**: Contiene datos relevantes sobre el usuario.
     + **Configuración de Privacidad**: Define las preferencias de privacidad del usuario.
   * **Métodos**:
     + **Actualizar Información**: Permite al usuario cambiar su información personal.
3. **Dashboard**
   * **Atributos**:
     + **Datos de Seguridad**: Información sobre el estado de seguridad del sistema.
     + **Estadísticas**: Datos estadísticos relevantes para el usuario.
   * **Métodos**:
     + **Actualizar Datos**: Mantiene los datos del dashboard al día.
     + **Generar Alertas**: Crea alertas de seguridad basadas en la información actual.
4. **Alerta**
   * **Atributos**:
     + **Mensaje**: El contenido de la alerta.
     + **Nivel de Gravedad**: Indica cuán crítica es la alerta.
   * **Métodos**:
     + **Mostrar**: Presenta la alerta al usuario.
     + **Silenciar**: Desactiva temporalmente la alerta.
5. **Permiso**
   * **Atributos**:
     + **Tipo**: El tipo de permiso (por ejemplo, acceso a funciones específicas).
     + **Estado**: Indica si el permiso está activo o inactivo.
   * **Métodos**:
     + **Otorgar**: Asigna un permiso al usuario.
     + **Revocar**: Retira un permiso del usuario.

**Relaciones entre Clases**

* Un **Usuario** tiene un **Perfil**, lo que significa que cada usuario puede gestionar su información personal.
* El **Dashboard** muestra múltiples **Alertas**, informando al usuario sobre eventos críticos o cambios en el sistema.
* Un **Usuario** también gestiona **Permisos**, permitiéndole tener control sobre las funcionalidades disponibles en el sistema.

1. **Conclusiones:**

* El desarrollo del aplicativo móvil para la evaluación de dispositivos móviles representa un avance significativo en la mejora de la seguridad y el rendimiento de estos dispositivos, al ofrecer herramientas efectivas para analizar vulnerabilidades y proporcionar recomendaciones personalizadas. Este proyecto no solo proporciona una herramienta útil para usuarios y administradores, sino que también establece un marco robusto para la gestión de la ciberseguridad en un entorno cada vez más digitalizado, promoviendo así una mayor conciencia y proactividad en la protección de la información personal y la integridad de los dispositivos.
* El SRS proporciona una base sólida para el desarrollo del software, definiendo de manera clara y detallada los requisitos del sistema, lo que ayuda a evitar malentendidos durante el proceso de desarrollo.
* Al documentar los requisitos funcionales y no funcionales, el SRS permite que los desarrolladores tengan una comprensión clara de lo que se espera del sistema, lo que puede resultar en una implementación más eficiente y efectiva.
* El documento actúa como un puente de comunicación entre las partes interesadas, como clientes, desarrolladores y diseñadores, asegurando que todos estén alineados en cuanto a las expectativas y objetivos del proyecto.
* El SRS también proporciona un marco para gestionar cambios en los requisitos, lo que es esencial en entornos de desarrollo ágiles donde las necesidades pueden evolucionar a lo largo del tiempo.
* El SRS sirve como un documento de referencia durante todo el ciclo de vida del software, ayudando en la capacitación de nuevos miembros del equipo y en el mantenimiento del sistema a largo plazo
* La elaboración del SRS también ayuda a identificar riesgos potenciales en las etapas tempranas del desarrollo, permitiendo la implementación de estrategias de mitigación desde el inicio.

**Recomendaciones:**

* Realizar revisiones periódicas del SRS a medida que el proyecto avanza para asegurarse de que se mantenga actualizado y relevante.
* Considerar la incorporación de prototipos o maquetas en el SRS para proporcionar una mejor visualización de las interfaces y flujos de trabajo esperados.
* Proporcionar capacitación al equipo sobre cómo elaborar y utilizar un SRS de manera efectiva, asegurando que todos comprendan su importancia y utilicen el documento adecuadamente.
* Adoptar prácticas de desarrollo seguro desde el inicio del proyecto, garantizando que la aplicación esté protegida contra posibles vulnerabilidades.
* Implementar pruebas de usuario durante el desarrollo para recoger feedback sobre la usabilidad y funcionalidad de la aplicación, asegurando que cumpla con las necesidades reales de los usuarios.

1. **Bibliografía:**

Abdi, A., & Al-Azzawi, H. (2021). Data persistence in Flutter: A complete guide to using SQLite and other databases in Flutter apps. Springer.

González, M. A., & Díaz, J. (2022). Evaluación de la seguridad en dispositivos móviles. Revista de Seguridad Informática, 12(3), 45-60.

Gumbau, A. (2022). Flutter for web and mobile: Comprehensive guide to using SQLite databases. Software Development Times, 20(1), 22-30.

Hossain, M. (2021). Flutter for beginners: An introduction to app development using Flutter and Dart. Packt Publishing.

OWASP Foundation. (2021). OWASP mobile security testing guide. <https://owasp.org/www-project-mobile-security-testing-guide/>

Sullivan, D. (2018). Building mobile applications: The complete guide to creating effective mobile apps. App Development Press.