****

**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERIA**

**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

Documento de Arquitectura de Software

Versión *{1.0}*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CONTROL DE VERSIONES | | | | | |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | JJC,JRM Y JACZ | JJC,JRM Y JACZ | JJC,JRM Y JACZ | 17/06/2024 | Versión Original |

INDICE GENERAL

**Contenido**

[***1.***](#_heading=h.30j0zll) 5

[**1.1.**](#_heading=h.1fob9te) 5

[**1.2.**](#_heading=h.3znysh7) 7

[**1.3.**](#_heading=h.2et92p0) **¡Error! Marcador no definido.**

[**1.4.**](#_heading=h.tyjcwt) **¡Error! Marcador no definido.**

[***2.***](#_heading=h.3dy6vkm) 10

[2.1.1.](#_heading=h.1t3h5sf) 10

[2.1.2.](#_heading=h.26in1rg) 11

[***3.***](#_heading=h.lnxbz9) 15

[**3.1.**](#_heading=h.35nkun2) 15

[3.1.1.](#_heading=h.1ksv4uv) 15

[**3.2.**](#_heading=h.44sinio) 17

[3.2.1.](#_heading=h.z337ya) 17

[3.2.2.](#_heading=h.3j2qqm3) 24

[3.2.3.](#_heading=h.1y810tw) 27

[3.2.4.](#_heading=h.4i7ojhp) 28

[3.2.5.](#_heading=h.2xcytpi) 30

[3.2.6.](#_heading=h.1ci93xb) 32

[**3.3.**](#_heading=h.3whwml4) 32

[3.3.1.](#_heading=h.2bn6wsx) 33

[3.3.2.](#_heading=h.qsh70q) 33

[**3.4.**](#_heading=h.3as4poj) **¡Error! Marcador no definido.**

[3.4.1.](#_heading=h.1pxezwc) 35

[**3.5.**](#_heading=h.49x2ik5) 36

[3.5.1.](#_heading=h.2p2csry) 36

[***4.***](#_heading=h.147n2zr) 37

[**Escenario de Funcionalidad 8**](#_heading=h.3o7alnk)

[**Escenario de Usabilidad 8**](#_heading=h.23ckvvd)

[**Escenario de confiabilidad 9**](#_heading=h.ihv636)

[**Escenario de rendimiento 9**](#_heading=h.32hioqz)

[**Escenario de mantenibilidad 9**](#_heading=h.1hmsyys)

[**Otros Escenarios 9**](#_heading=h.41mghml)

1. INTRODUCCIÓN
   1. Propósito (Diagrama 4+1)

Creación De Diagrama 4+1 Para La App

Diagrama, Esquemático

Descripción generada automáticamente

El propósito de esta sección es detallar el Diagrama 4+1, que se utiliza para representar la arquitectura de la aplicación móvil "Evaluación de Seguridad de Aplicaciones". Este enfoque permite una comprensión holística del sistema a través de cinco vistas interrelacionadas, facilitando así el diseño, desarrollo y mantenimiento de la aplicación.

**1. Vista Lógica**

La vista lógica se centra en la estructura del sistema, describiendo los componentes principales y sus interacciones. Incluye clases y módulos como:

* **SecurityAnalyzer**: Realiza el análisis de seguridad de las aplicaciones.
* **RecommendationEngine**: Ofrece recomendaciones basadas en los permisos y vulnerabilidades detectadas.
* **ReportGenerator**: Genera informes detallados sobre el estado de seguridad.

**2. Vista de Desarrollo**

Esta vista describe la organización del código y los módulos que se implementarán. Incluye archivos clave como:

* **alertas\_notificaciones\_screen.dart**
* **configuracion\_seguridad\_screen.dart**
* **escaneo\_seguridad\_screen.dart**

Cada uno de estos archivos representa una funcionalidad específica dentro de la aplicación.

**3. Vista de Proceso**

La vista de proceso muestra los flujos de trabajo y la dinámica de la aplicación. Incluye diagramas de actividad que representan:

* El flujo de inicio de sesión.
* El proceso de análisis de seguridad.
* La generación de reportes, mostrando cómo se interactúa con los distintos módulos.

**4. Vista de Implementación**

Esta vista detalla la estructura de componentes y cómo se integran en el sistema. Incluye archivos como:

* **database\_helper.dart**: Maneja la conexión y operaciones de la base de datos.
* **main.dart**: Punto de entrada de la aplicación.
* **theme.dart**: Define el estilo visual y la apariencia de la aplicación.

**5. Vista de Despliegue**

La vista de despliegue representa la arquitectura física del sistema, incluyendo:

* La distribución de la aplicación en dispositivos móviles (iOS y Android).
* Consideraciones sobre el entorno de despliegue, como la seguridad en las comunicaciones y el almacenamiento de datos.
  1. Alcance

El alcance del proyecto "Aplicativo Móvil para la Evaluación de Seguridad en Dispositivos Móviles" define las funcionalidades, limitaciones y el contexto operativo de la aplicación, asegurando que todos los participantes comprendan sus objetivos. La aplicación analizará las aplicaciones instaladas en el dispositivo, revisando los permisos otorgados, lo que es esencial para ayudar a los usuarios a identificar riesgos asociados a permisos excesivos. Además, ofrecerá recomendaciones prácticas para mejorar la seguridad, como la revocación de permisos y la eliminación de aplicaciones sospechosas, y permitirá la generación de informes que detallen el estado de seguridad.

El desarrollo se centrará en dispositivos iOS y Android, considerando su amplia aceptación en el mercado. La efectividad del análisis dependerá de los permisos disponibles en el sistema operativo, lo que puede limitar el análisis en ciertas aplicaciones. El mantenimiento y las actualizaciones se basarán en el feedback del usuario y las amenazas emergentes, garantizando que la aplicación sea adaptable. Está dirigida a un amplio público, desde usuarios preocupados por su seguridad digital hasta profesionales de la seguridad, y se utilizará en diversas condiciones de red, con medidas para proteger los datos transmitidos. Aunque no se planea la integración con otros sistemas en esta fase, se dejará la puerta abierta para futuras expansiones. En resumen, el alcance del proyecto establece un marco claro que guía el desarrollo, maximizando su potencial de éxito en un contexto de creciente preocupación por la seguridad digital.

* 1. Definición, siglas y abreviaturas

 **API**: *Application Programming Interface* (Interfaz de Programación de Aplicaciones) - Conjunto de definiciones y protocolos que permiten la interacción entre diferentes software.

 **iOS**: *iPhone Operating System* - Sistema operativo móvil de Apple utilizado en dispositivos como iPhone y iPad.

 **Android**: Sistema operativo móvil desarrollado por Google, utilizado en una variedad de dispositivos móviles.

 **UI**: *User Interface* (Interfaz de Usuario) - Espacio donde interactúan los usuarios con la aplicación.

 **UX**: *User Experience* (Experiencia de Usuario) - Percepción general del usuario al interactuar con la aplicación.

 **KPI**: *Key Performance Indicator* (Indicador Clave de Desempeño) - Métrica utilizada para evaluar el éxito de un proyecto o aplicación.

* 1. Organización del documento

Este Documento de Arquitectura de Software (SAD) está estructurado para proporcionar una visión clara y detallada del "Aplicativo Móvil para la Evaluación de Seguridad en Dispositivos Móviles". A continuación, se describe la organización del contenido:

1. **Introducción**: Esta sección introduce el propósito del documento, el contexto del proyecto y su importancia en el ámbito de la seguridad de dispositivos móviles.
2. **Definiciones, Siglas y Abreviaturas**: Se definen términos clave, siglas y abreviaturas que se utilizarán a lo largo del documento, facilitando la comprensión de los conceptos técnicos.
3. **Alcance**: Aquí se delimita el alcance del proyecto, especificando las funcionalidades principales, las limitaciones y el contexto operativo de la aplicación.
4. **Diagrama 4+1**: Se presenta el Diagrama 4+1, que incluye las diferentes vistas del sistema (escenarios, lógica, procesos, implementación y despliegue) para ilustrar la arquitectura del software de manera visual.
5. **Requisitos Funcionales y No Funcionales**: En esta sección se detallan los requisitos que la aplicación debe cumplir, tanto en términos de funcionalidades específicas como de características de rendimiento, usabilidad y seguridad.
6. **Arquitectura del Software**: Se describe la arquitectura general del sistema, detallando los componentes principales, su interacción y cómo se organizan para cumplir con los requisitos establecidos.
7. **Plan de Pruebas**: Se presentan las estrategias y métodos para realizar pruebas en la aplicación, asegurando que se verifiquen y validen todos los requisitos definidos.
8. **Mantenimiento y Soporte**: Esta sección aborda las estrategias para el mantenimiento de la aplicación y el soporte al usuario, asegurando su operatividad y adaptabilidad a lo largo del tiempo.
9. **Conclusiones**: Se resumen los hallazgos y se discuten las implicaciones del proyecto en el contexto de la seguridad en dispositivos móviles, destacando su relevancia y potencial impacto.
10. **OBJETIVOS Y RESTRICCIONES ARQUITECTONICAS**
    1. Priorización de requerimientos

### Requerimientos Funcionales

|  |  |  |
| --- | --- | --- |
| 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-11 | **Aplicaciones Instaladas** | El usuario debe poder ver una lista de las aplicaciones instaladas en su dispositivo. |
| 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. |
| RF-14 | **Tema Personalizado** | El usuario debe poder personalizar el tema de la aplicación a su preferencia. |

### Requerimientos No Funcionales – Atributos de Calidad

|  |  |  |  |
| --- | --- | --- | --- |
| **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. Restricciones

*Restricciones adaptadas para el proyecto Aplicativo Movil para la evaluación en Dispositivos móviles -Flutte-Sqlite(local)*

|  |  |
| --- | --- |
| *ID* | *Descripción* |
| Alcance | El proyecto se enfoca en el desarrollo de un aplicativo móvil para la evaluación de la seguridad en dispositivos móviles, diseñado para usuarios de Android e iOS. La aplicación será compatible con dispositivos que operen con Android 7 y versiones superiores, así como con iOS 12 y posteriores. Su funcionalidad estará centrada en analizar las aplicaciones instaladas, revisar los permisos otorgados por el usuario y ofrecer recomendaciones de seguridad, todo de manera local, sin requerir conexión a Internet ni almacenar datos del usuario. |
| Tiempo | El proyecto se completará en un período de 120 días, desde la aprobación inicial hasta el cierre, incluyendo las fases de instalación y capacitación de los usuarios sobre el uso de la aplicación. |
| Costo | La inversión total estimada para el desarrollo del proyecto es de $13,420.00, considerando la utilización de tecnologías como Flutter para el desarrollo de la aplicación y garantizando una interfaz amigable y eficiente. |
| Calidad | Se aplicarán estándares de calidad que seguirán las mejores prácticas de desarrollo en Flutter, asegurando la eficiencia y el cumplimiento de los requisitos establecidos en la documentación del proyecto. |
| Recursos | Para el desarrollo se utilizará un entorno de trabajo adecuado, con equipos que tengan sistemas operativos compatibles y software de productividad estándar, además de herramientas específicas para el desarrollo en Flutter. |
| Riesgos | Se identifican varios riesgos potenciales, incluyendo problemas de comunicación dentro del equipo, un diseño inadecuado de la estructura de permisos, ausencias imprevistas de miembros del equipo, desviaciones en el presupuesto inicial y cambios no anticipados en los requisitos del proyecto. También se contempla la posible vulnerabilidad de seguridad que podría afectar la protección de los datos del usuario. |
| Satisfaccion del cliente | e espera que la aplicación cumpla completamente con los requisitos y expectativas de los usuarios, garantizando así su satisfacción y confianza en la herramienta para la evaluación de la seguridad en sus dispositivos móviles. |

# **REPRESENTACIÓN DE LA ARQUITECTURA DEL SISTEMA**

* 1. Vista de Caso de uso

### Diagramas 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

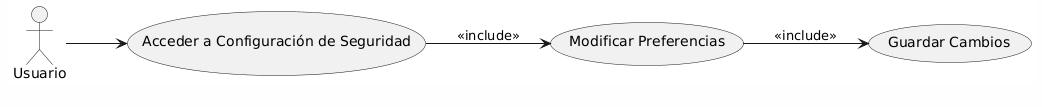
Diagrama

Descripción generada automáticamenteCaso de uso : Dashboard

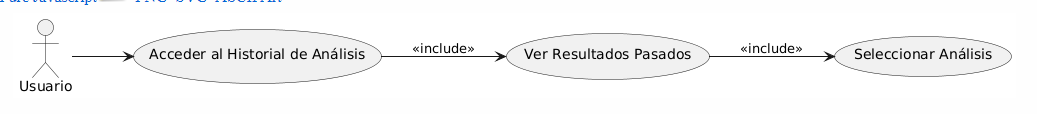
Diagrama

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

Diagrama

Descripción generada automáticamenteImagen 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

* 1. Vista Lógica

### 

### Diagrama de Subsistemas (paquetes)

Autenticacion

*Diagrama

Descripción generada automáticamente*

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteSeguridad

Configuración

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Historial y Reportes

Interfaz de usuario gráfica, Aplicación

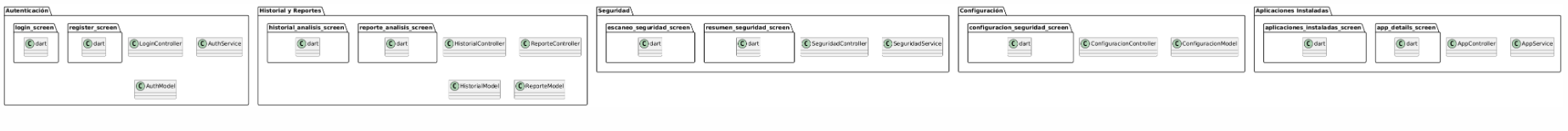
Descripción generada automáticamente

Aplicaciones Instaladas

Interfaz de usuario gráfica, Texto, Aplicación

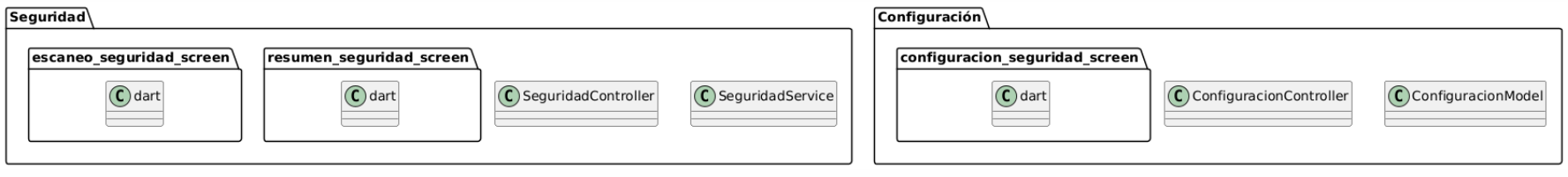
Descripción generada automáticamente

Diagrama Completo



Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente



**Narrativa de los Subsistemas de Paquetes**

**1. Autenticación**

* **Pantallas**:
  + login\_screen.dart: Pantalla donde el usuario ingresa sus credenciales de acceso.
  + register\_screen.dart: Pantalla de registro de nuevos usuarios.
* **Controladores**:
  + LoginController: Gestiona la lógica del inicio de sesión, como la validación de credenciales y el manejo de errores.
* **Servicios**:
  + AuthService: Interactúa con los modelos y la base de datos para validar las credenciales de los usuarios.
* **Modelos**:
  + AuthModel: Representa los datos de autenticación y los usuarios en el sistema.
* **Función**:
  + El subsistema de autenticación gestiona el acceso a la aplicación, proporcionando funcionalidades para que los usuarios inicien sesión o se registren en el sistema. El controlador maneja la lógica de interacción, el servicio conecta con la base de datos y el modelo contiene los datos del usuario.

**2. Seguridad**

* **Pantallas**:
  + escaneo\_seguridad\_screen.dart: Pantalla donde se ejecuta el análisis de seguridad del dispositivo.
  + resumen\_seguridad\_screen.dart: Muestra un resumen de los resultados del análisis de seguridad.
* **Controladores**:
  + SeguridadController: Maneja el proceso de escaneo y la interacción del usuario con las pantallas de seguridad.
* **Servicios**:
  + SeguridadService: Realiza el análisis de seguridad, escaneando aplicaciones y permisos del dispositivo.
* **Función**:
  + Este subsistema está dedicado a analizar el estado de seguridad del dispositivo, escaneando las aplicaciones instaladas y sus permisos. Proporciona alertas sobre posibles vulnerabilidades, ejecuta los análisis y muestra los resultados al usuario en forma de resumen.

**3. Configuración**

* **Pantallas**:
  + configuracion\_seguridad\_screen.dart: Pantalla que permite ajustar las configuraciones de seguridad.
* **Controladores**:
  + ConfiguracionController: Gestiona las preferencias de seguridad que el usuario define.
* **Modelos**:
  + ConfiguracionModel: Almacena y gestiona las configuraciones de seguridad personalizadas del usuario.
* **Función**:
  + Este subsistema permite que los usuarios configuren su experiencia en la aplicación, personalizando aspectos como el nivel de alerta, los permisos monitoreados y la frecuencia de los escaneos de seguridad.

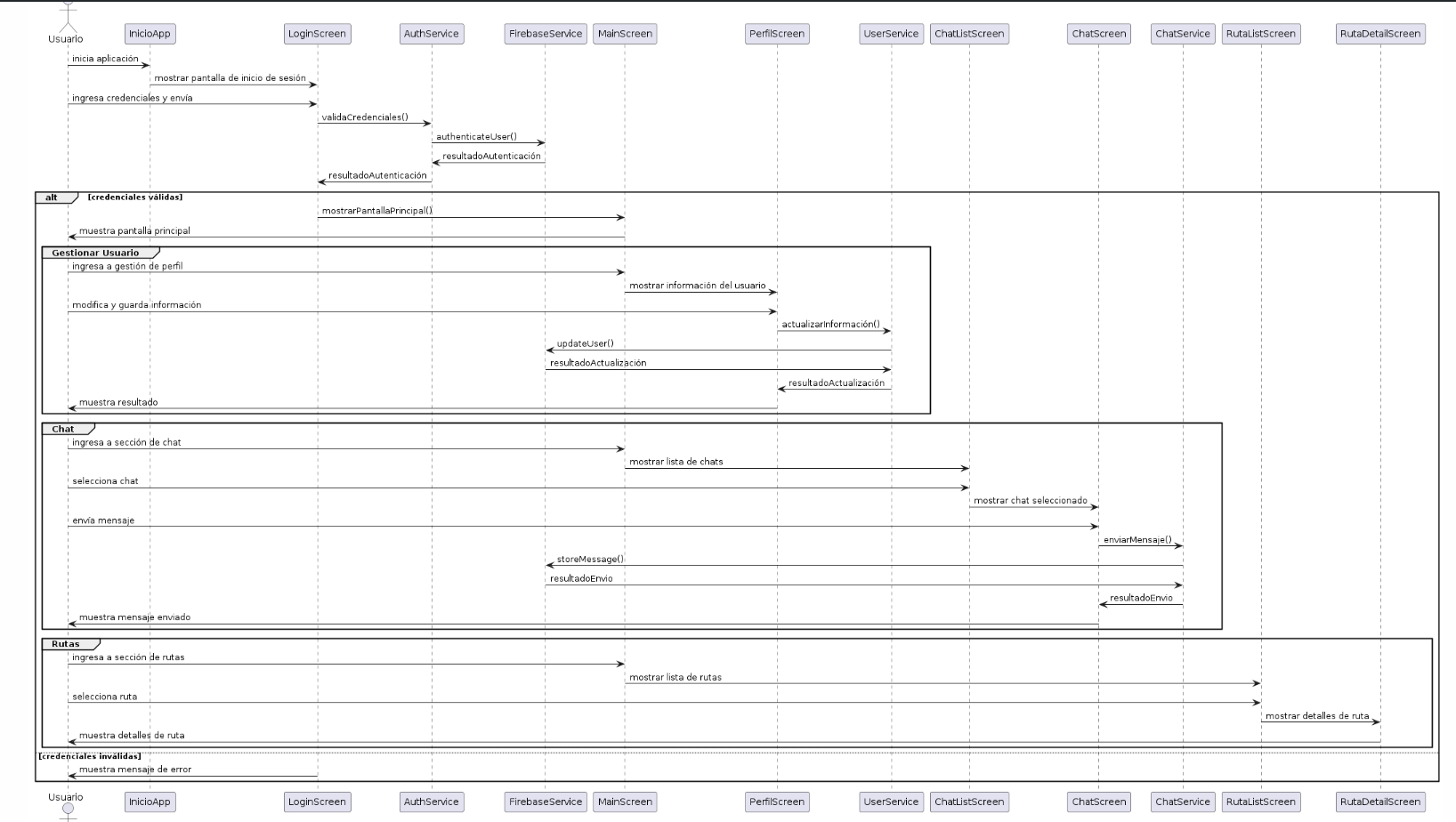
**4. Historial y Reportes**

* **Pantallas**:
  + historial\_analisis\_screen.dart: Pantalla que muestra el historial de los análisis de seguridad realizados.
  + reporte\_analisis\_screen.dart: Pantalla que permite generar reportes detallados de los análisis de seguridad.
* **Controladores**:
  + HistorialController: Gestiona la lógica del historial de análisis.
  + ReporteController: Controla la generación de reportes personalizados sobre los análisis realizados.
* **Modelos**:
  + HistorialModel: Almacena los datos de los análisis pasados.
  + ReporteModel: Representa los datos a incluir en los reportes generados.
* **Función**:
  + Este subsistema permite al usuario revisar los análisis de seguridad que se han realizado en su dispositivo y generar reportes que detallen las vulnerabilidades encontradas, así como las recomendaciones para mejorar la seguridad.

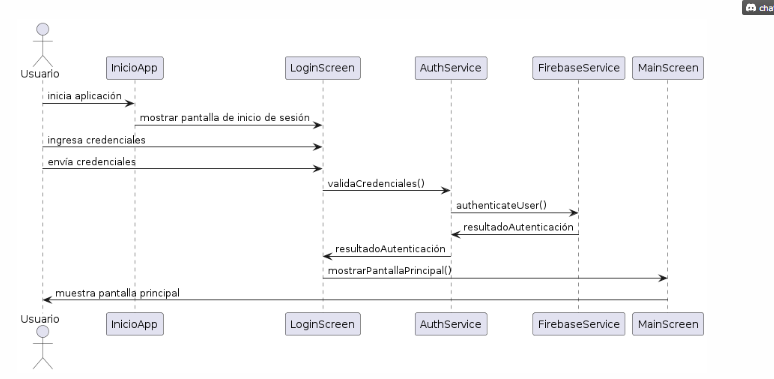
**5. Aplicaciones Instaladas**

* **Pantallas**:
  + aplicaciones\_instaladas\_screen.dart: Pantalla que lista todas las aplicaciones instaladas en el dispositivo.
  + app\_details\_screen.dart: Proporciona detalles de seguridad de cada aplicación, incluidos los permisos otorgados.
* **Controladores**:
  + AppController: Maneja la interacción con la lista de aplicaciones instaladas y proporciona información detallada sobre cada aplicación.
* **Servicios**:
  + AppService: Realiza consultas al sistema para obtener la lista de aplicaciones instaladas y los permisos de cada una.
* **Función**:
  + Este subsistema permite que el usuario vea todas las aplicaciones instaladas en su dispositivo, junto con información sobre los permisos que han sido otorgados a cada aplicación. También proporciona detalles de seguridad, alertando sobre aplicaciones con permisos potencialmente peligrosos.

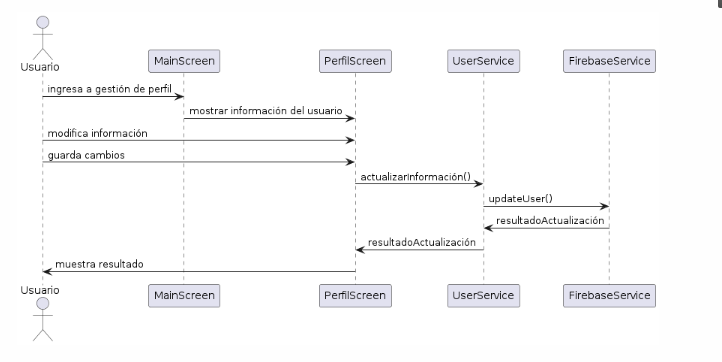
### Diagrama de Secuencia (vista de diseño)



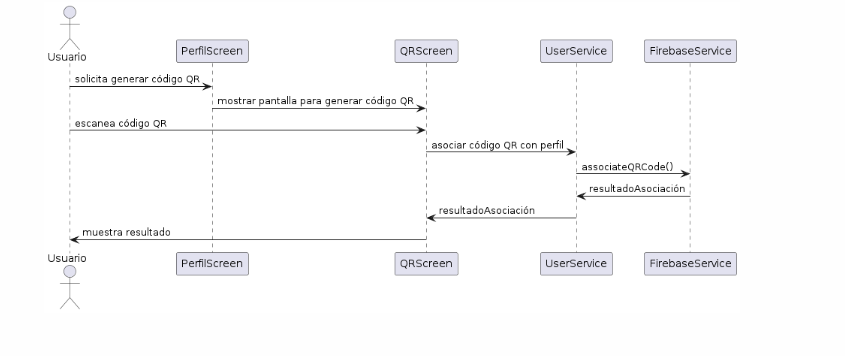
Caso de Uso: Usuario Autenticar

****

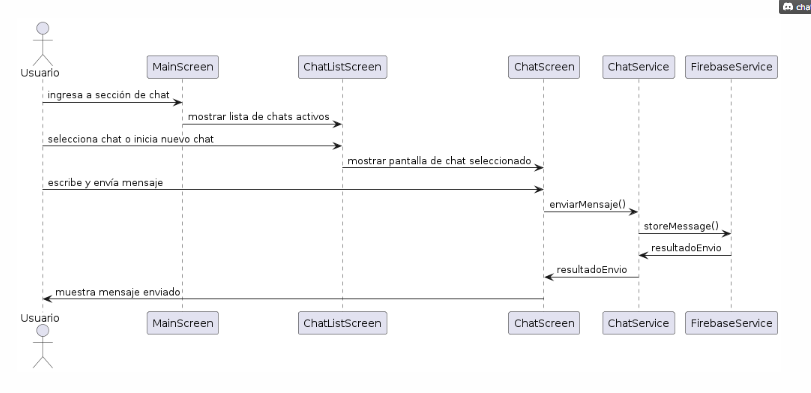
**Caso de Uso: Gestionar Usuario**

****

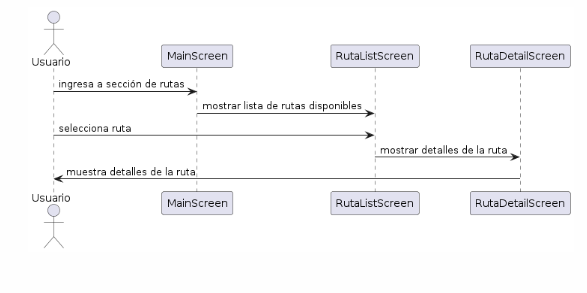
**generar código qr**

****

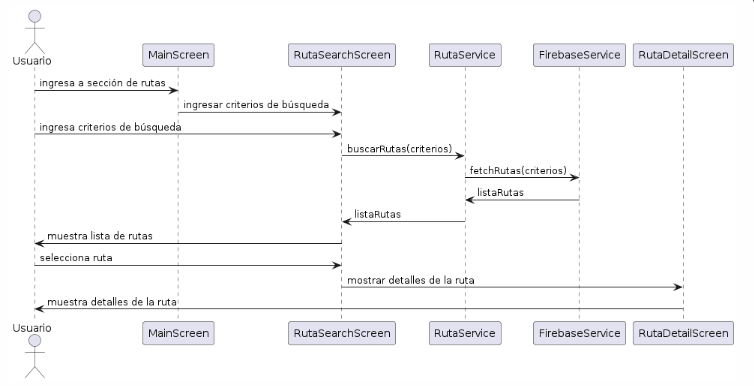
**Caso de Uso: Chat**

****

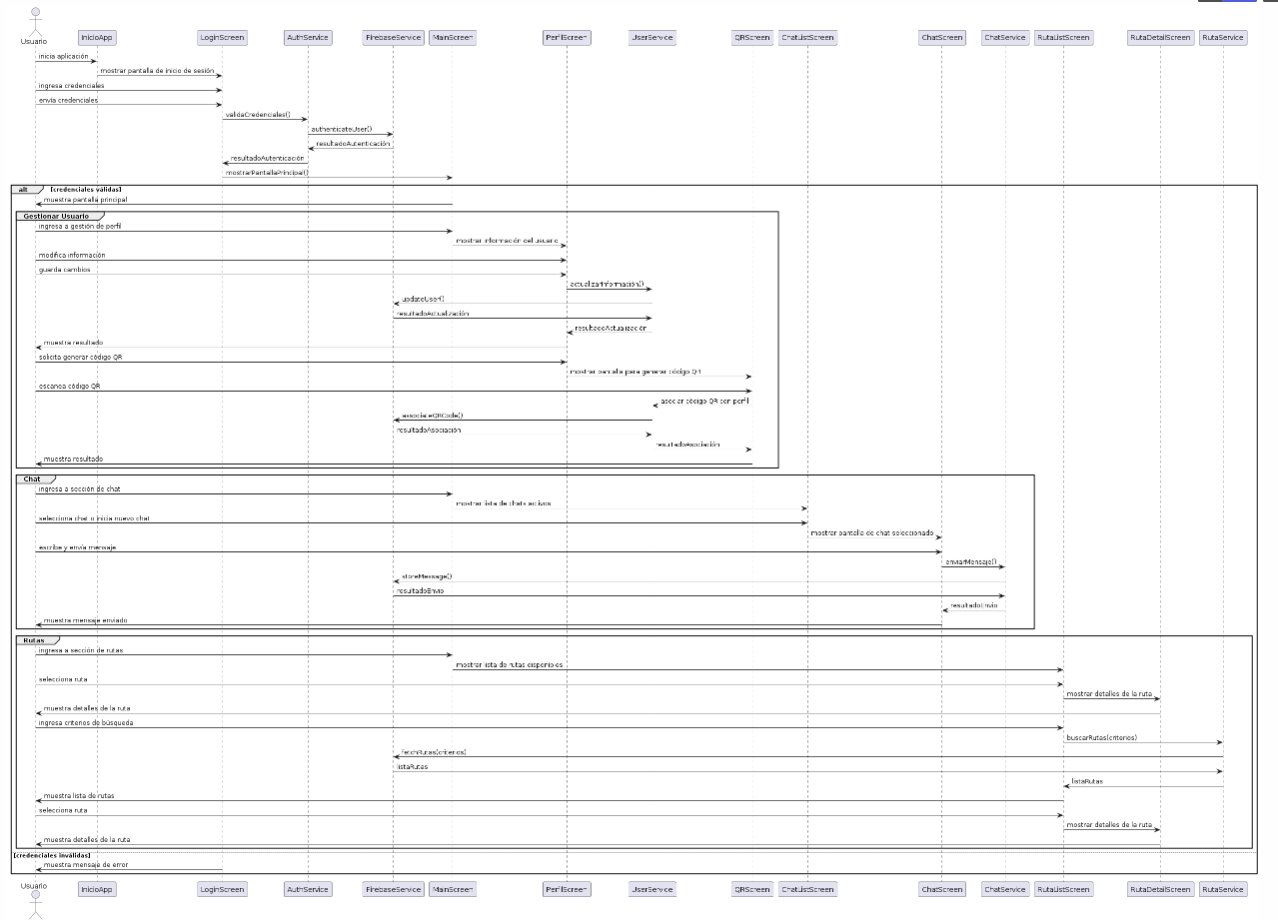
Caso de Uso: Rutas



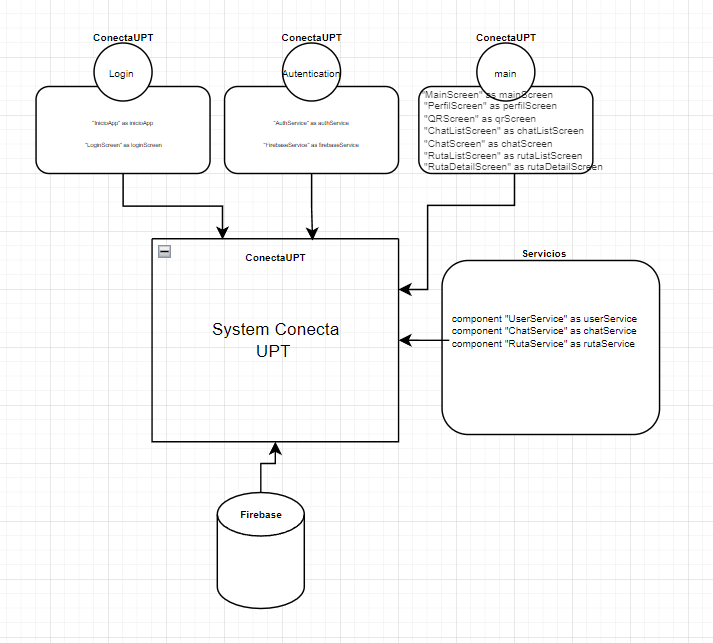
Escenario: Buscar ruta



**Diagrama de secuencia general**

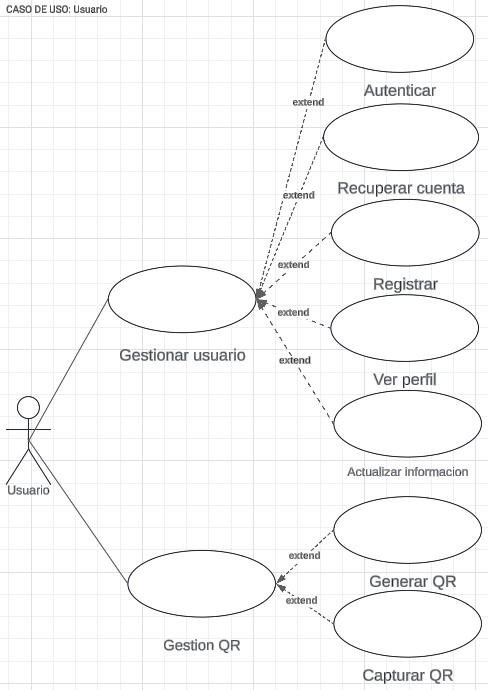
****

### Diagrama de Colaboración (vista de diseño)

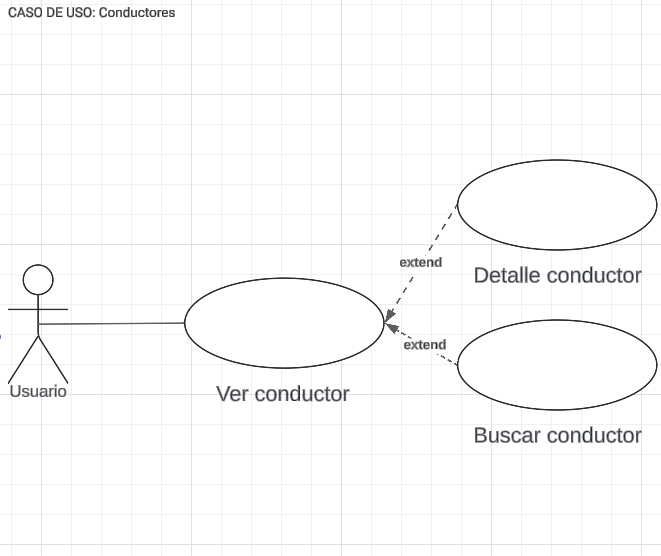


### Diagrama de Objetos

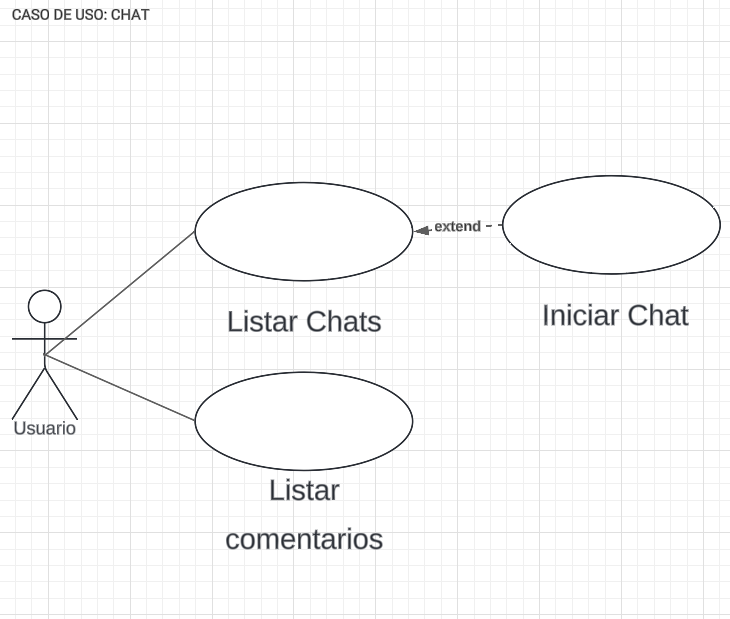
: Usuarios



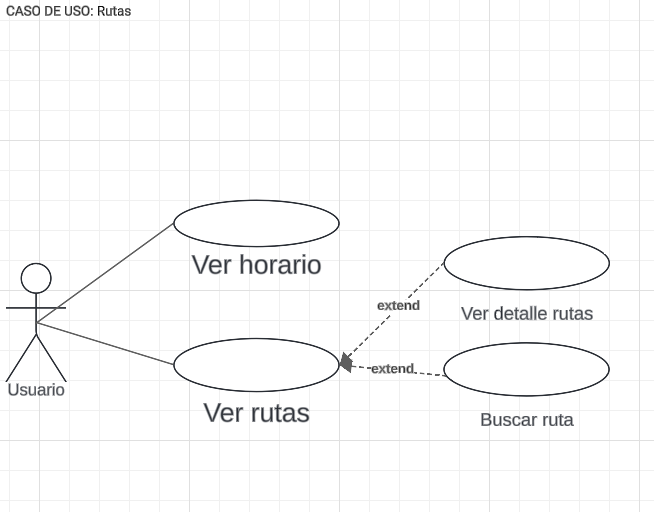
: Conductor



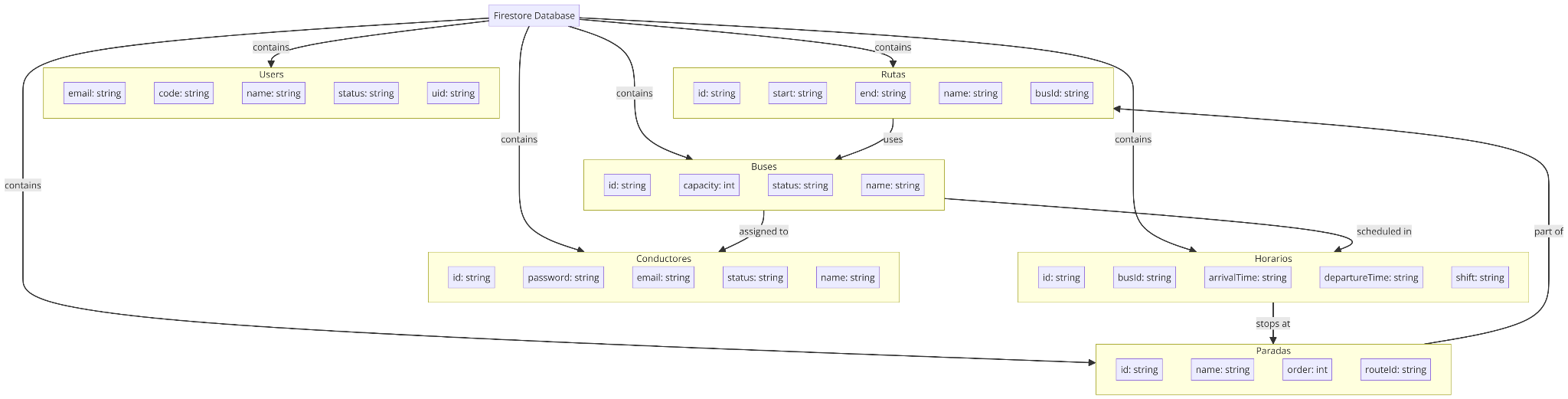
: Chat

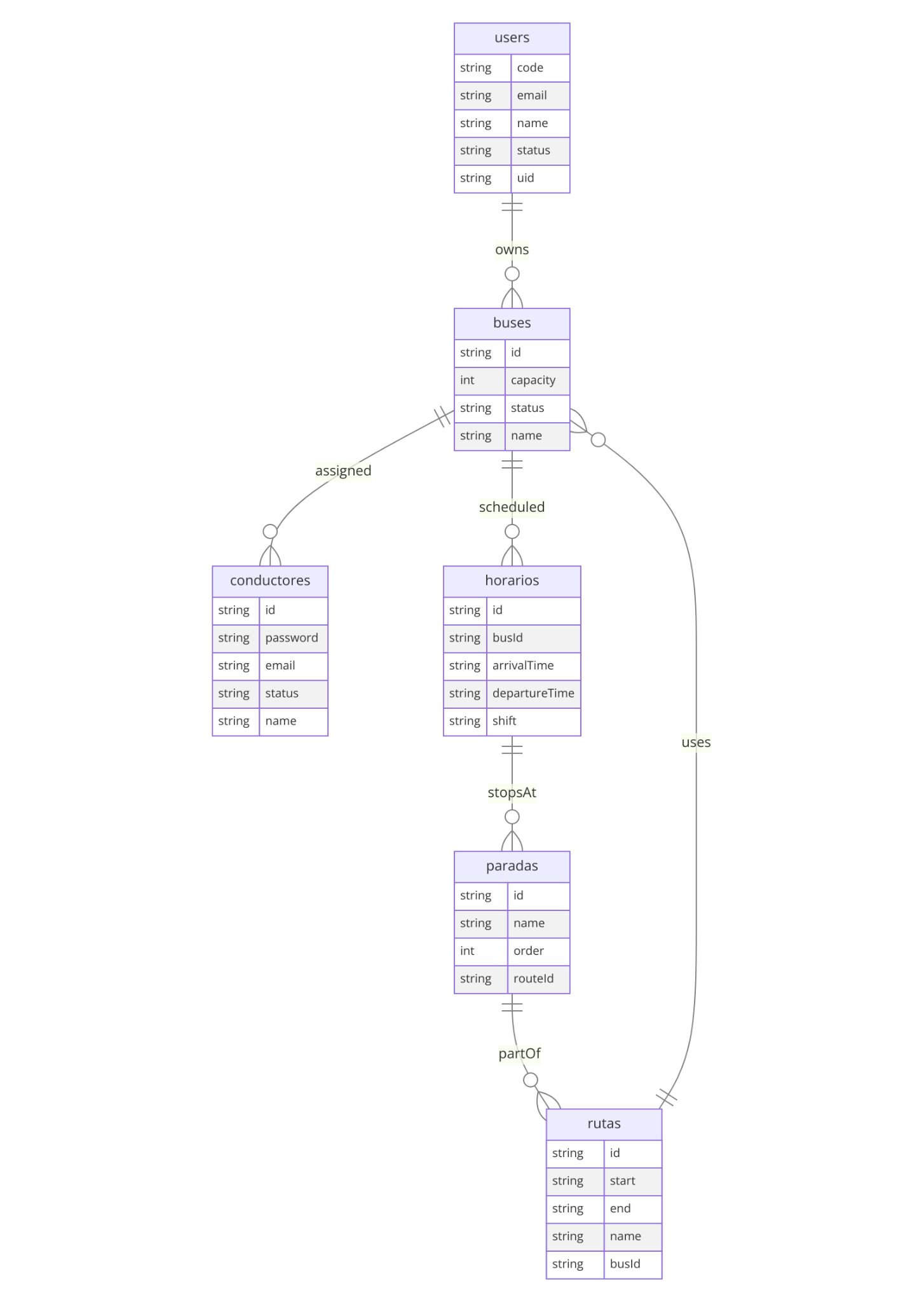


: Rutas



### Diagrama de Clases

Controladores:  


Modelo:  


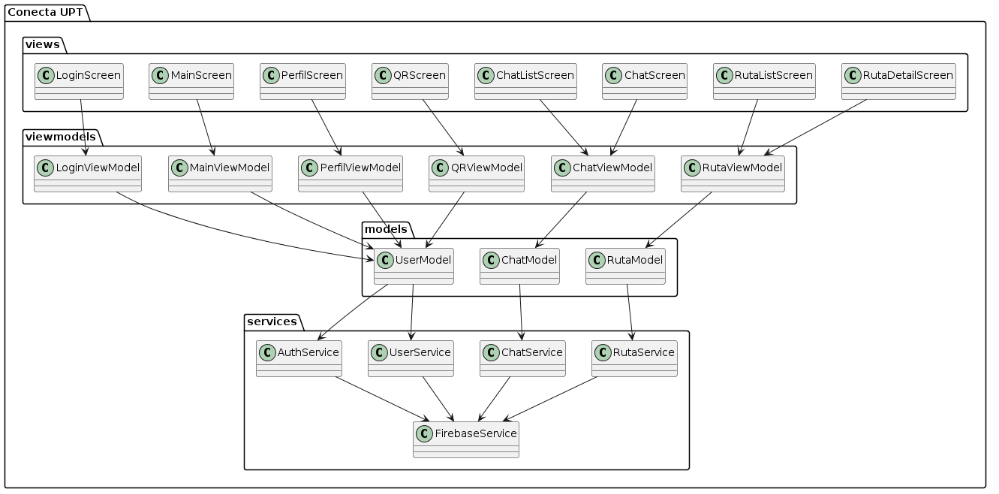
### Diagrama de Base de datos ( no relacional)

Modelo Físico

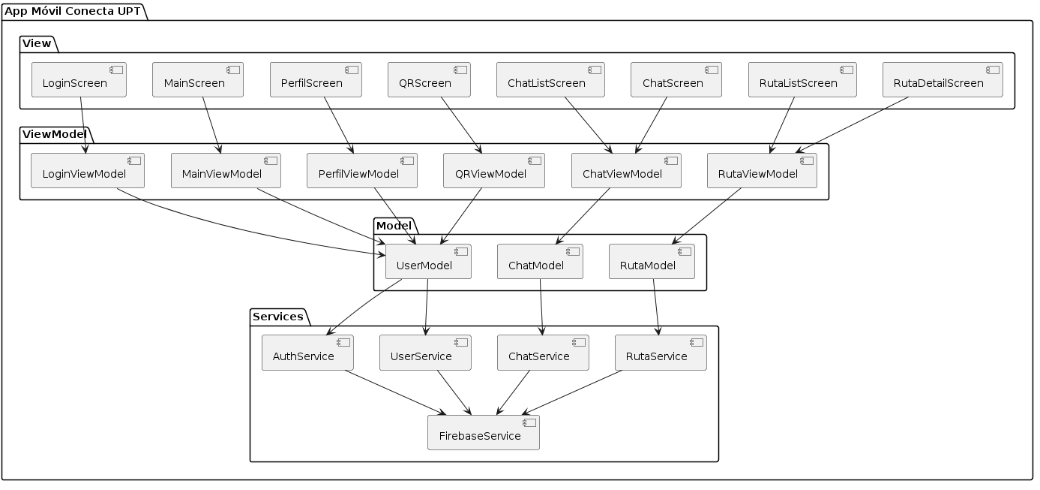


* 1. Vista de Implementación (vista de desarrollo)

*Este diagrama proporciona una vista clara de la estructura del código fuente de la aplicación "Conecta UPT", mostrando cómo los diferentes módulos y componentes están organizados e interconectados*

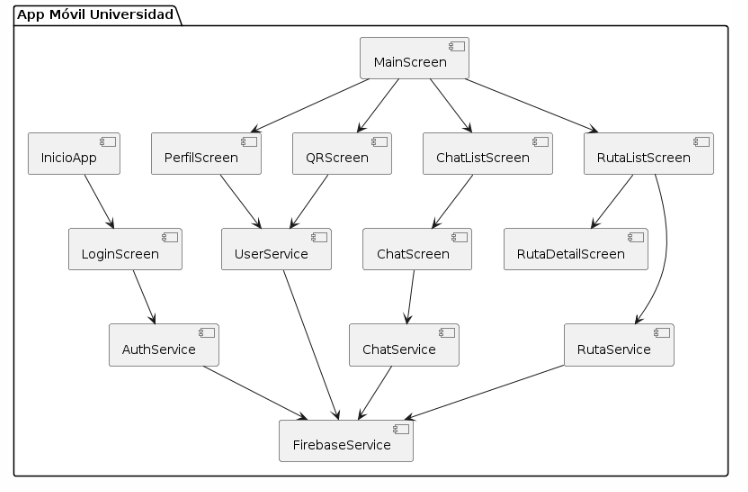
**

### Diagrama de arquitectura software

**

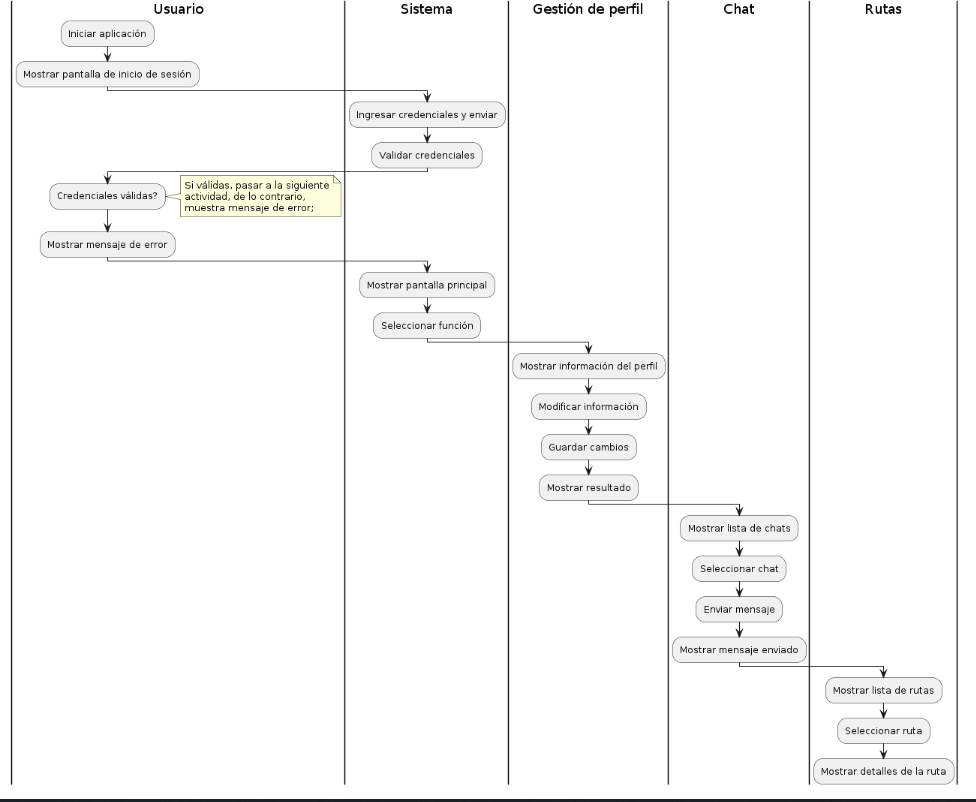
*Arquitectura Modelo MVVC*

### Diagrama de arquitectura del sistema (Diagrama de componentes)



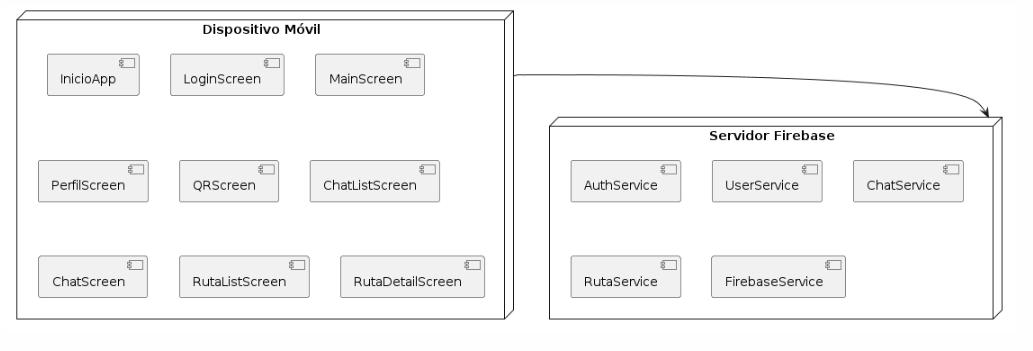
Vista de procesos

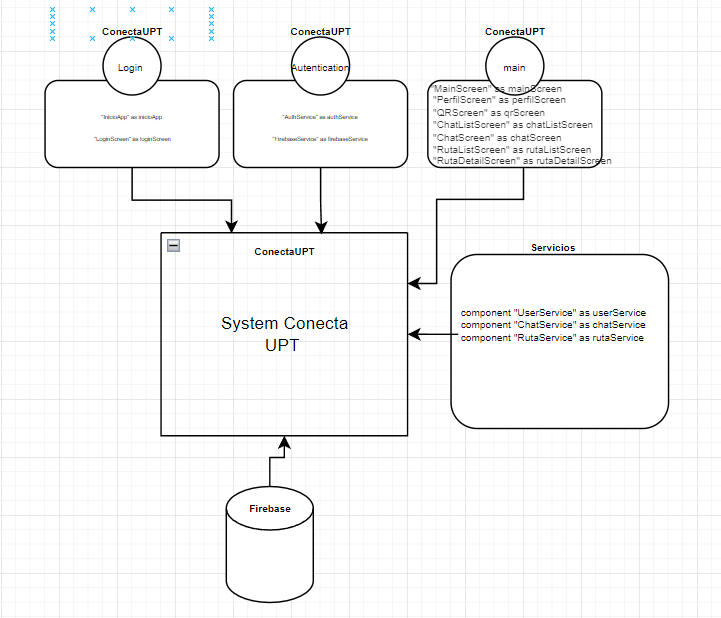
### Diagrama de Procesos del sistema (diagrama de actividad)



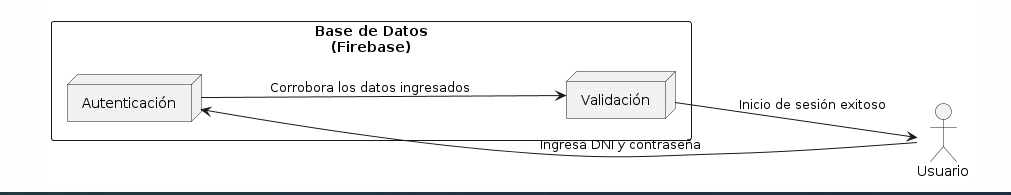
* 1. Vista de Despliegue (vista física)

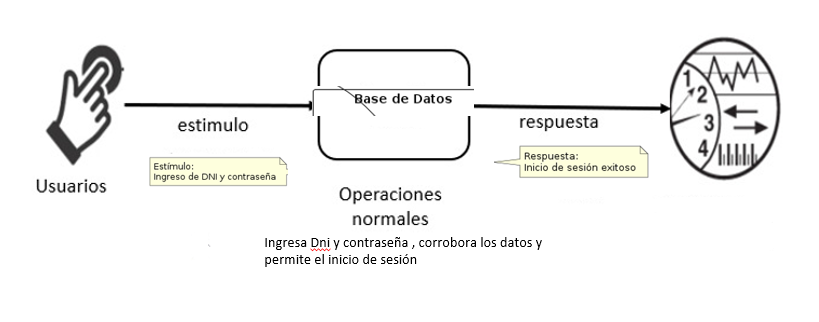
### Diagrama de despliegue

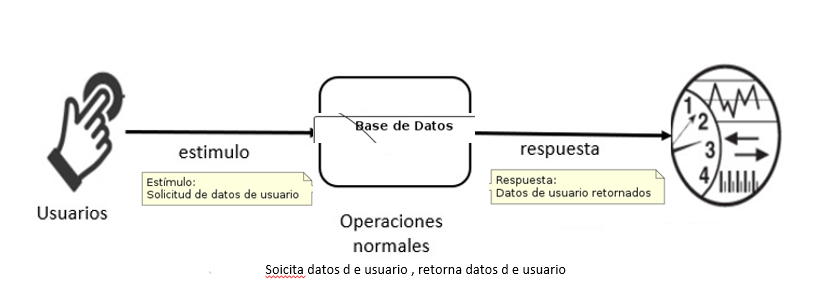


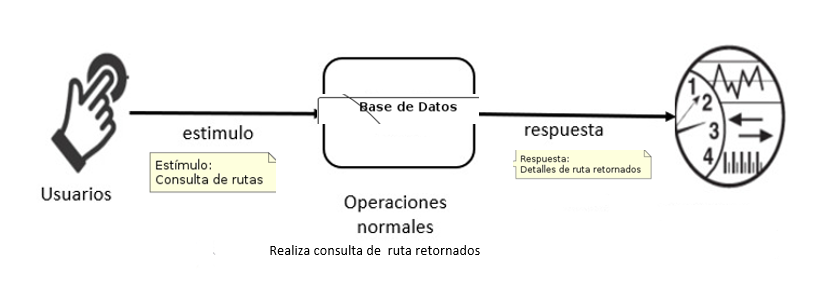


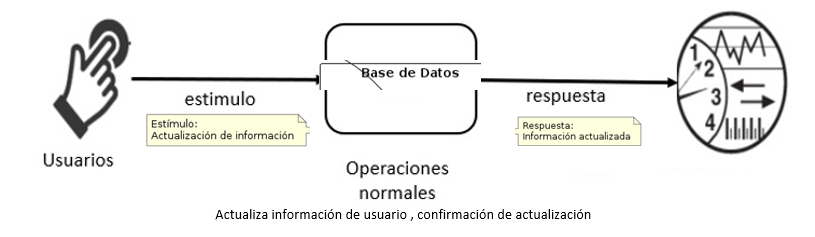
# **ATRIBUTOS DE CALIDAD DEL SOFTWARE**

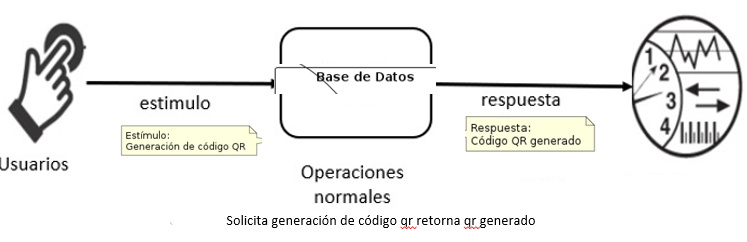


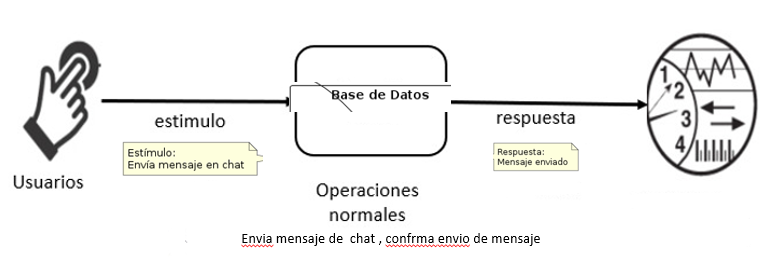


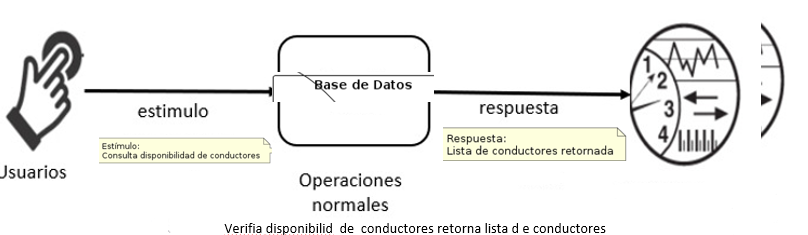












Lista de escenarios

Inicio de Sesión

Solicitud de Datos de Usuario

Consulta de Rutas

Actualización de Información

Generación de Código QR

Envío de Mensaje en Chat

Consulta de Disponibilidad de Conductores