UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas

Proyecto:

Sistema Gestor de contraseñas: ChargePass

Curso: *Construcción de software II*

Docente: Mag. Ricardo Eduardo Valcárcel Alvarado

Integrantes:

Chambe Torres, Edgard Reynaldo	(2019064917)
Nina Vargas, Luigui Augusto	(2019065166)
Condori Vargas,Tomas Yoel	(2018000487)

Tacna – Perú

2025

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	Chambe Torres, Edgard Reynaldo Nina Vargas, Luigui Augusto Tomas Condori Vargas	Patrick Cuadros	Patrick Cuadros	25/04/2024	Versión 1

Sistema Gestor de contraseñas: ChargePass

Documento de Arquitectura de Software

Versión *{1.0}*

ÍNDICE GENERAL

1. INTRODUCCIÓN

1.1. Propósito

Este documento de arquitectura de software (SAD) tiene como objetivo proporcionar una visión clara y estructurada de la arquitectura del sistema ChargePass, destacando cómo esta arquitectura responde a los requerimientos críticos tanto funcionales como no funcionales.

ChargePass es una aplicación móvil desarrollada en Flutter e integrada con Firebase, cuyo propósito es mejorar la seguridad digital de los usuarios a través de la generación, almacenamiento y gestión segura de contraseñas. El sistema incluye funcionalidades como autenticación de usuarios mediante validación por correo electrónico, generación automática o personalizada de contraseñas robustas, y almacenamiento cifrado de credenciales en la nube.

1.2. Alcance

El alcance del proyecto ChargePass se centra en mejorar la seguridad digital de los usuarios mediante el desarrollo de una aplicación móvil intuitiva y confiable para la generación, almacenamiento y gestión de contraseñas seguras. La solución contempla un sistema de registro con verificación por correo electrónico, asegurando que solo usuarios autenticados puedan acceder al sistema.

La aplicación permitirá la generación de contraseñas robustas mediante dos métodos: automáticamente, cumpliendo con criterios de seguridad (como longitud, uso de mayúsculas, números y caracteres especiales), o manualmente, a través del ingreso de un token personalizado. Además, todas las contraseñas serán almacenadas de forma segura utilizando técnicas de cifrado y respaldadas en Firebase.

El sistema contempla funcionalidades clave como la gestión de contraseñas por usuario, recuperación mediante correo electrónico, y control de acceso basado en roles.

1.3 Definición, siglas y abreviaturas

- **Firebase:** Plataforma de desarrollo de aplicaciones móviles y web que ofrece servicios como autenticación, almacenamiento en la nube y base de datos en tiempo real, utilizada como backend en ChargePass.

- **Auth:** Abreviatura de "Authentication", hace referencia al módulo de autenticación de Firebase que gestiona el inicio de sesión, registro y recuperación de cuentas.

- **Flutter:** Framework de desarrollo de interfaces móviles multiplataforma, desarrollado por Google, utilizado para construir la aplicación móvil de ChargePass.

- **Token:** Cadena de caracteres utilizada para representar información segura como claves de sesión o contraseñas personalizadas.

- **UI (User Interface):** Interfaz de usuario, es la capa visual con la que interactúan los usuarios dentro de la aplicación.

- **UX (User Experience):** Experiencia del usuario, hace referencia a la facilidad, fluidez y satisfacción del usuario al interactuar con la aplicación.

- **AES (Advanced Encryption Standard):** Algoritmo de cifrado simétrico utilizado en ChargePass para proteger las contraseñas almacenadas.

- **API:** Application Programming Interface, conjunto de métodos que permiten que diferentes módulos del sistema o servicios externos se comuniquen entre sí.

- **MFA (Multi-Factor Authentication):** Autenticación de múltiples factores, mecanismo de seguridad previsto como mejora futura para ChargePass.

1.4 Organización del Documento

Las referencias aplicables son:

1. Documento de Visión de Proyecto.

2.Documento de Factibilidad

2. Documento de Especificación de Requerimientos de Software

2. REPRESENTACIÓN DE ARQUITECTURA

2.1. Requerimientos Funcionales

Tabla 1: Cuadro de Requerimientos funcionales

REQUERIMIENTOS FUNCIONALES			
Código	**Nombre**	**Descripción**	**Prioridad**
RF - 001	Registro de Usuario	El sistema debe permitir a los usuarios registrarse proporcionando su correo electrónico y una contraseña. Al ingresar sus datos, el sistema verificará si el correo tiene un formato válido y si la contraseña cumple con los requisitos mínimos de seguridad, como longitud y uso de caracteres especiales. Una vez validados estos campos, el sistema registrará al usuario utilizando Firebase Authentication y almacenará su información adicional en Firestore. Si el registro es exitoso, el usuario podrá recibir un correo de verificación para completar el proceso.	**Alta**
RF - 002	Verificación de Correo	Después de registrarse, el sistema debe enviar un código de verificación al correo electrónico del usuario. Este correo contendrá un enlace de validación, que, al ser clicado, confirmará la validez del correo y activará la cuenta del usuario. La verificación del correo electrónico es esencial para garantizar que la cuenta está asociada a una dirección válida y accesible. El sistema dependerá de Firebase Authentication para enviar este correo de verificación.	**Alta**
RF - 003	Inicio de Sesión con Validación	Solo los usuarios que hayan verificado su correo electrónico podrán iniciar sesión con sus credenciales (correo y contraseña). Si un usuario intenta iniciar sesión sin haber verificado su correo, el sistema le informará que debe completar el proceso de verificación. El proceso de inicio de sesión será gestionado por Firebase Authentication, que validará tanto las credenciales del usuario como el estado de verificación del correo. Si la verificación ha sido completada, el sistema permitirá el acceso al usuario.	**Alta**

RF - 004	Generación Automática de Claves	El sistema debe ofrecer una opción para generar contraseñas seguras automáticamente. Las contraseñas generadas deberán cumplir con criterios de seguridad, como una longitud mínima y el uso de caracteres especiales, números y letras mayúsculas. Los usuarios podrán utilizar esta opción para obtener una contraseña segura sin necesidad de crearla manualmente. Esta función estará disponible en el modal de contraseñas, y las contraseñas generadas serán validadas automáticamente para asegurar que cumplen con los requisitos de seguridad.	**Alta**
RF - 005	Generación Manual con Token	Además de la generación automática, el sistema debe permitir a los usuarios generar una contraseña personalizada mediante un token único. Este token servirá como base para la creación de la contraseña. El sistema validará si el token es único y garantizará que la contraseña creada a partir de él cumpla con los requisitos de seguridad. Este proceso permitirá a los usuarios tener más control sobre la creación de sus contraseñas mientras se mantiene un nivel adecuado de seguridad.	**Baja**

Fuente: Elaboración propia del equipo de trabajo

En la Tabla 1 se presentan los requerimientos funcionales iniciales del proyecto del esta estructura asegura que el proceso de registro, verificación, y autenticación sea claro, seguro y fácil de usar para los usuarios, mientras se mantiene la protección de sus datos a lo largo de todas las interacciones con la aplicación.

2.2. **Requerimientos No Funcionales**

Tabla 2: Cuadro de Requerimientos No funcionales

Código	Nombre	Descripción
RNF-001	Rendimiento	El sistema debe ser capaz de gestionar múltiples registros de usuarios, inicios de sesión y verificación de correos sin retrasos significativos. Las consultas de autenticación y verificación de usuarios deben completarse en menos de 2 segundos bajo condiciones normales de carga. La interfaz de usuario debe ser reactiva y permitir una experiencia fluida al manejar más de 1000 intentos de inicio de sesión por minuto.
RNF-002	Seguridad	Todas las comunicaciones entre el cliente y el servidor, así como entre Firebase Authentication y Firestore, deben ser cifradas utilizando HTTPS para garantizar la integridad y confidencialidad de los datos del usuario. Además, las contraseñas deben ser encriptadas antes de ser almacenadas en Firestore utilizando un servicio de encriptación robusto. El sistema debe cumplir con los estándares de seguridad más altos para proteger los datos sensibles, como las credenciales de inicio de sesión.
RNF-003	Disponibilidad	El sistema debe estar disponible un 99.9% del tiempo durante el horario de operación. Esto implica que las funciones críticas como el registro de usuarios, la verificación de correos y el inicio de sesión deben ser accesibles sin interrupciones. El tiempo de inactividad no debe exceder las 2 horas por mes, asegurando que los usuarios puedan realizar todas las operaciones sin problemas, incluso en momentos de alta demanda.
RNF-004	Portabilidad	La aplicación debe ser completamente funcional en dispositivos móviles que utilicen sistemas operativos Android e iOS, ya que se desarrollará utilizando Flutter. Además, la aplicación debe garantizar que los usuarios puedan acceder a la funcionalidad de autenticación y gestión de contraseñas sin problemas, sin importar el dispositivo que utilicen. Esto incluye la compatibilidad con diversas versiones de sistemas operativos y dispositivos con distintas resoluciones de pantalla.

Fuente: Elaboración propia del equipo de trabajo

En la Tabla Nº 2 tenemos la tabla de requerimientos no funcionales asegurando que tu aplicación no solo cumpla con las funcionalidades básicas de registro, inicio de sesión y gestión de contraseñas, sino que también sea rápida, segura, confiable y accesible en diferentes dispositivos. Cada uno de estos aspectos contribuye a la experiencia del usuario, garantizando que el sistema pueda manejar de manera eficiente la interacción de los usuarios con la plataforma mientras mantiene la seguridad y la disponibilidad.

3. REPRESENTACIÓN DE LA ARQUITECTURA DEL SISTEMA

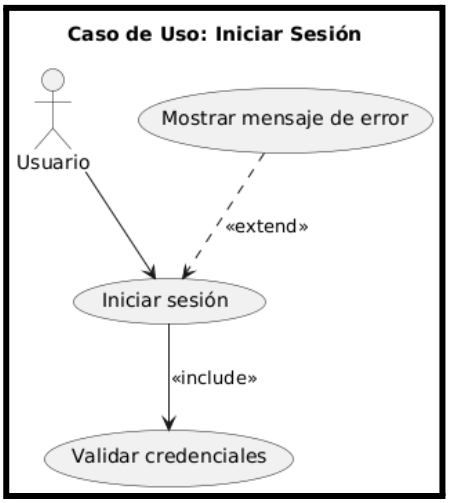
3.1. Vista de caso de uso

En esta sección se muestran los Casos de Uso relevantes para la arquitectura, así como también a los principales Actores,su desarrollo del presente software implica que la arquitectura sea adecuada para poder suministrar esa funcionalidad.

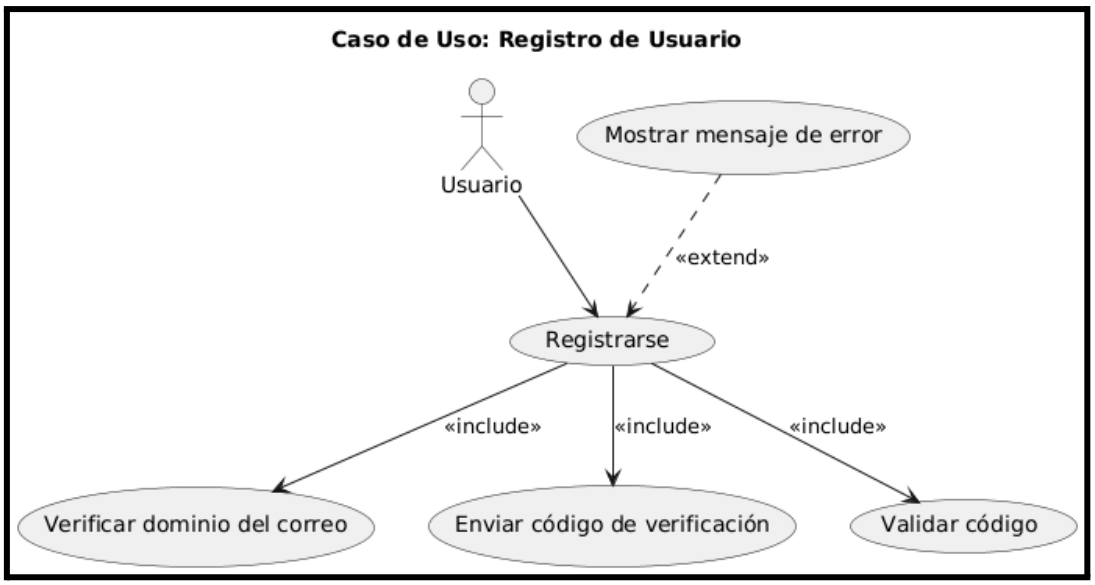
3.1.1. Diagrama de Casos de Uso

RF-001: Autenticar con Correo Electrónico

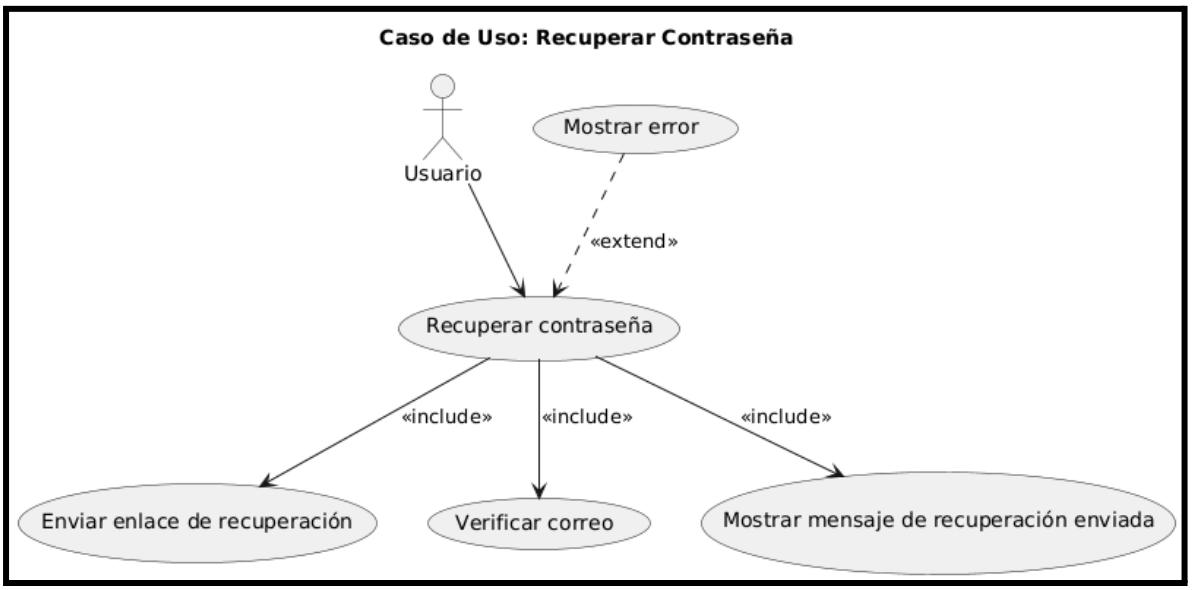
Gráfico 07:Diagrama de Caso de Usos Iniciar Sesión



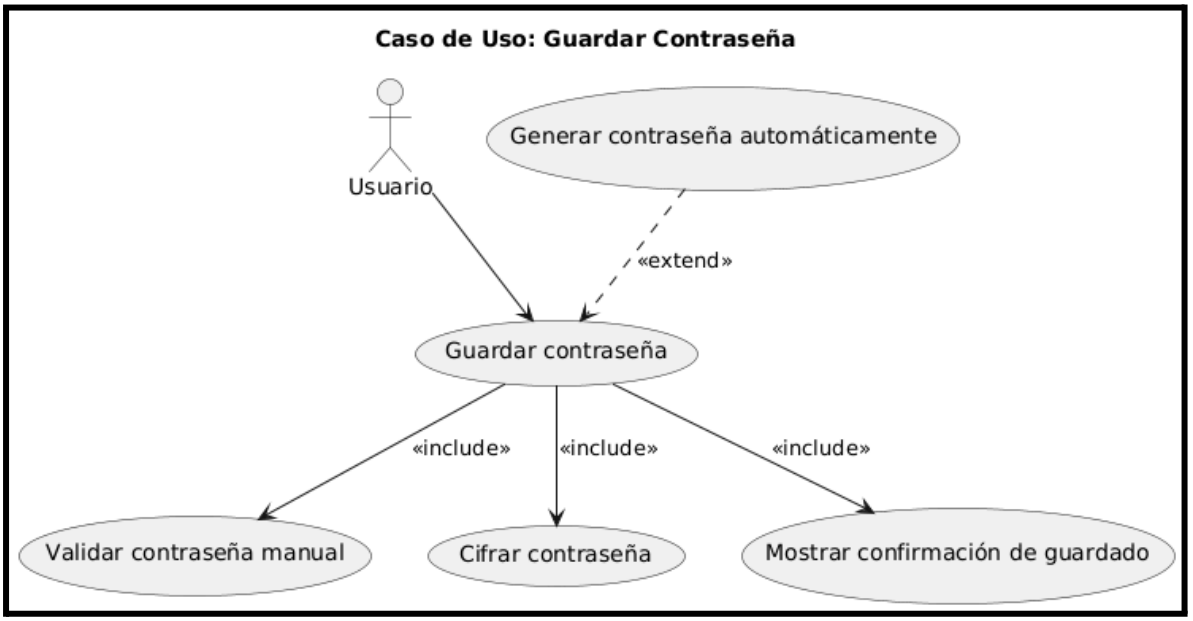
RF-002: Autenticar con Correo Electrónico



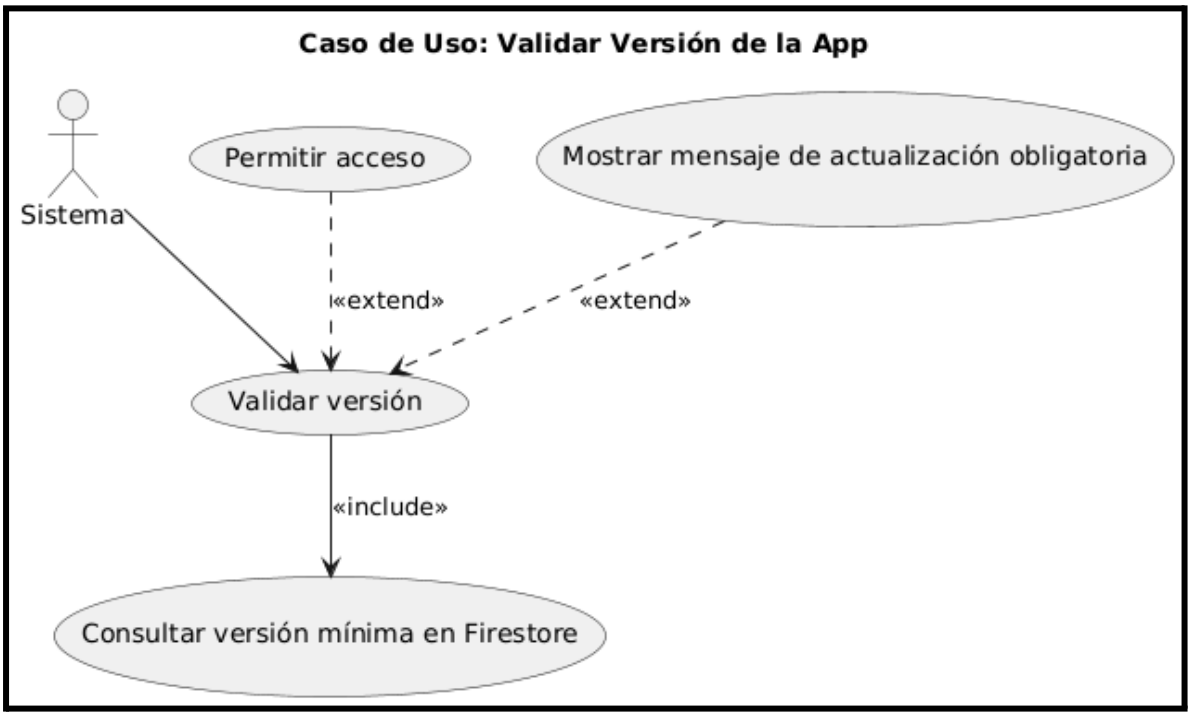
RF-001: Autenticar con Correo Electrónico - Recuperar Contraseña



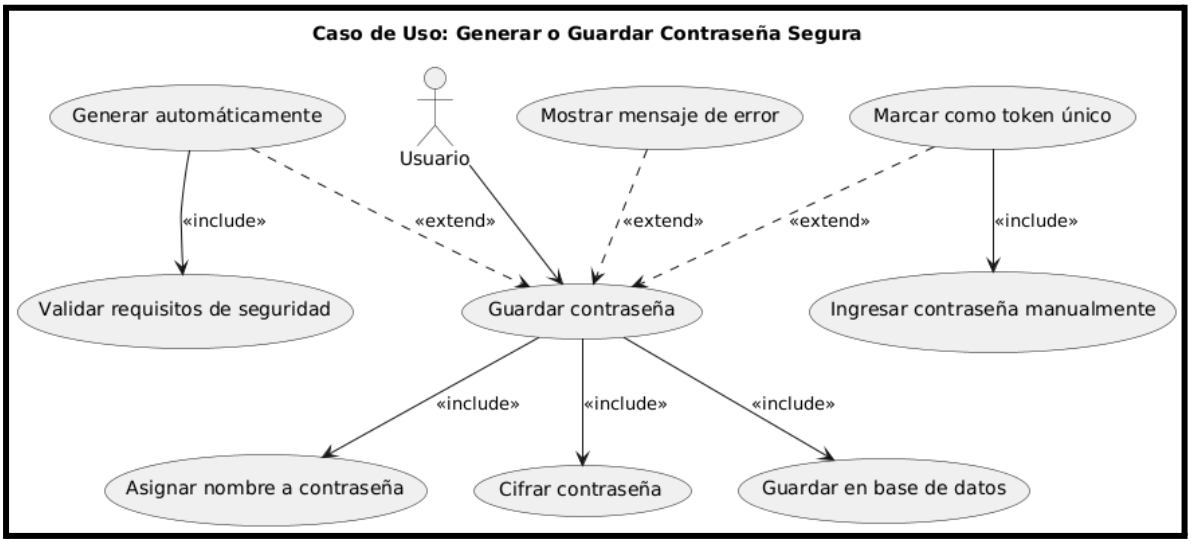
RF-002:Verificación con Correo- Guardar Contraseña



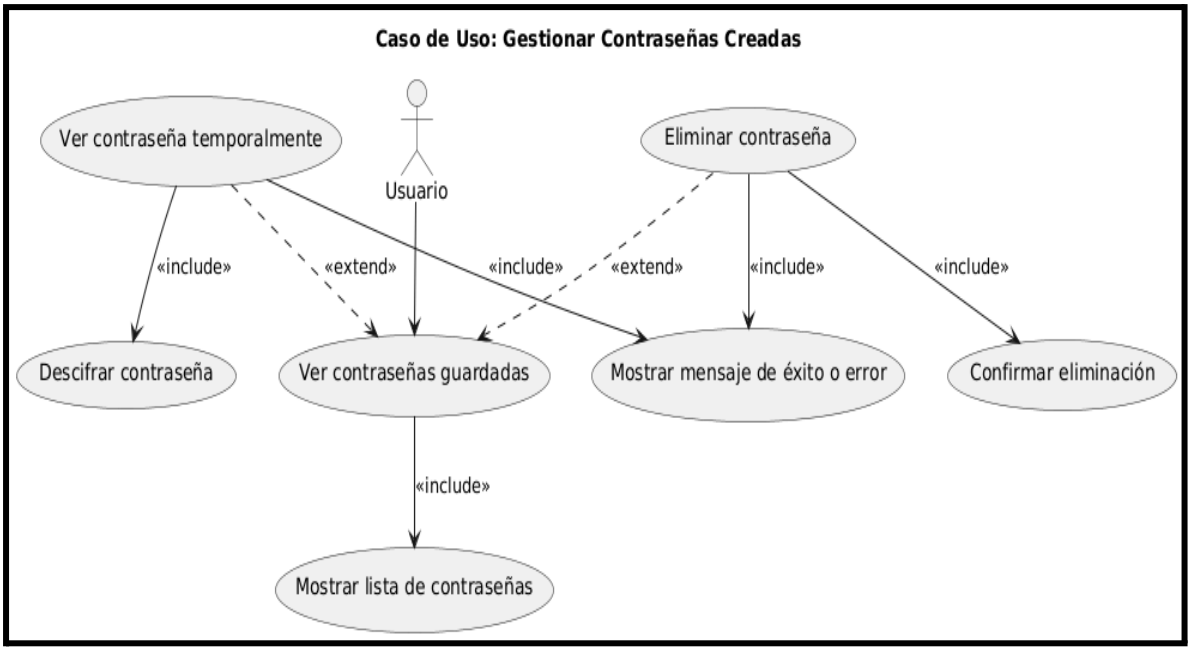
RF-002: Autenticar con Correo Electrónico - Validar Versión de la App



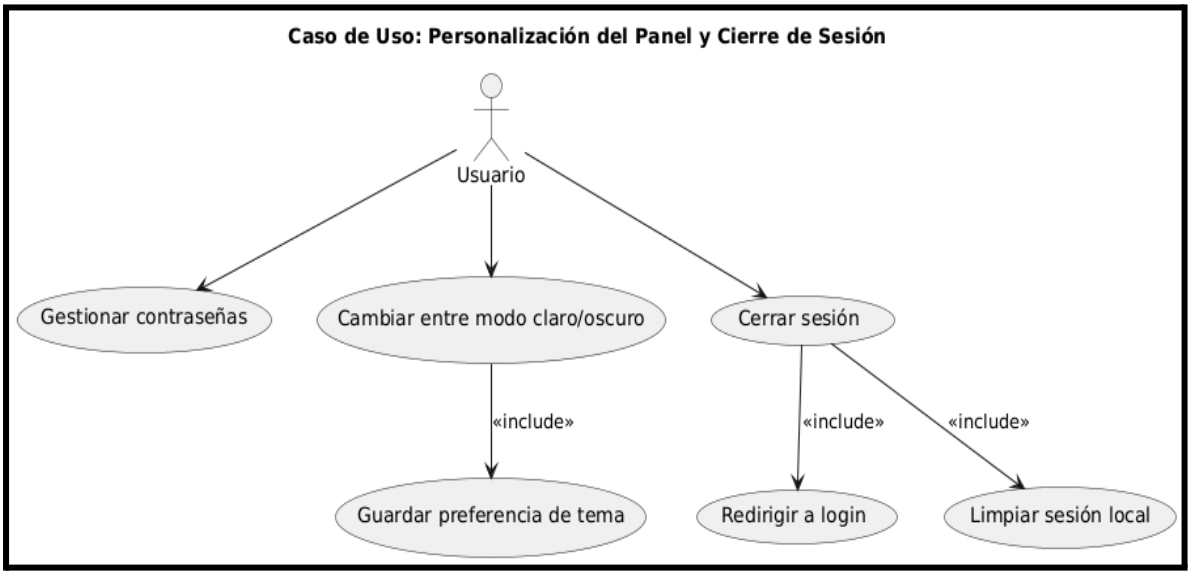
RF-004: Generación Automática de Claves - Generar o guardar Contraseña



RF-004: Generación Automática de Claves - Generar o guardar Contraseña



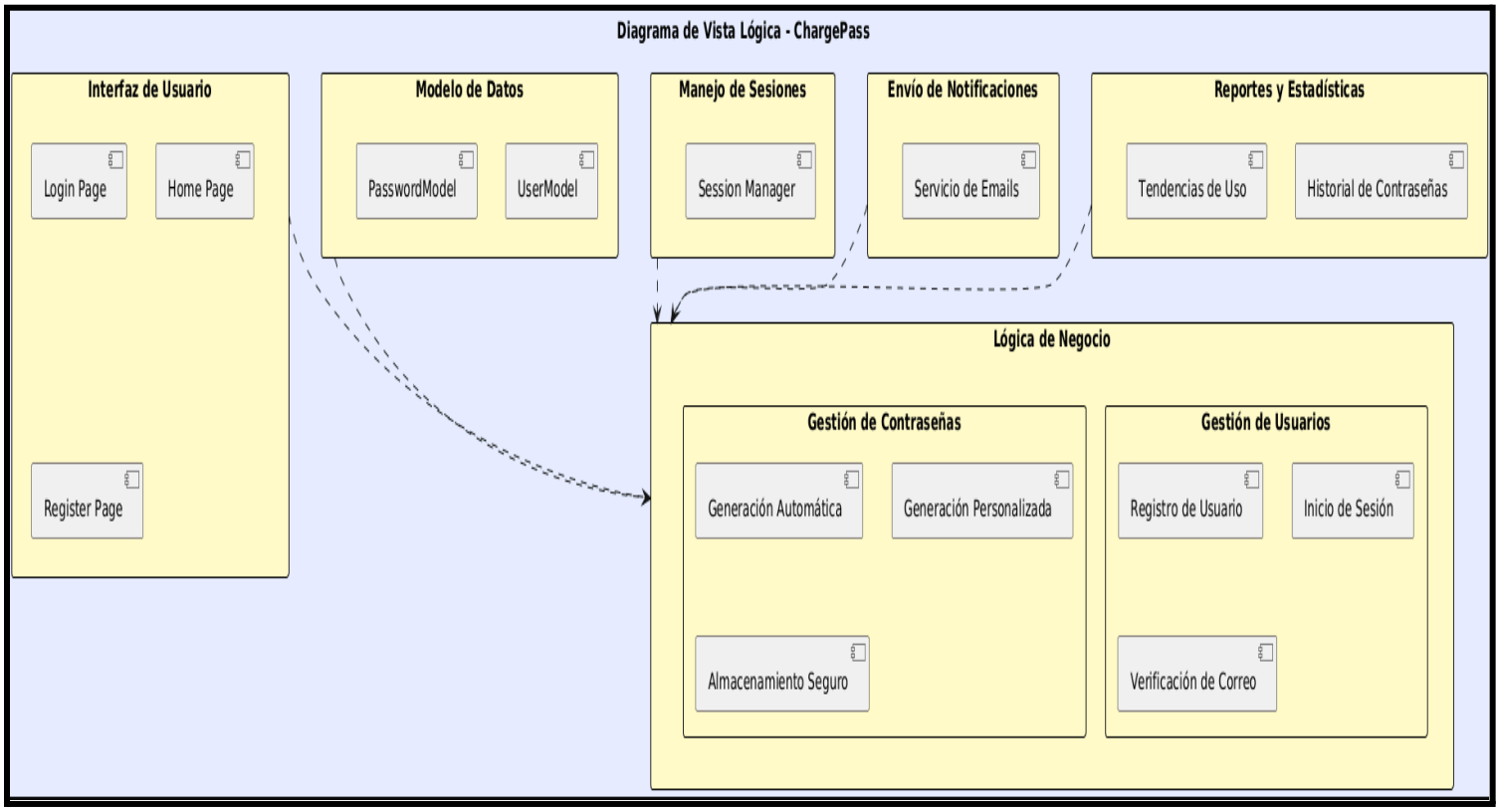
RF-005: Autenticar con Personalización del panel y cierre de sesión.



.

3.2. **Vista Lógica**

Gráfico 07:Diagrama de Vista Lógica

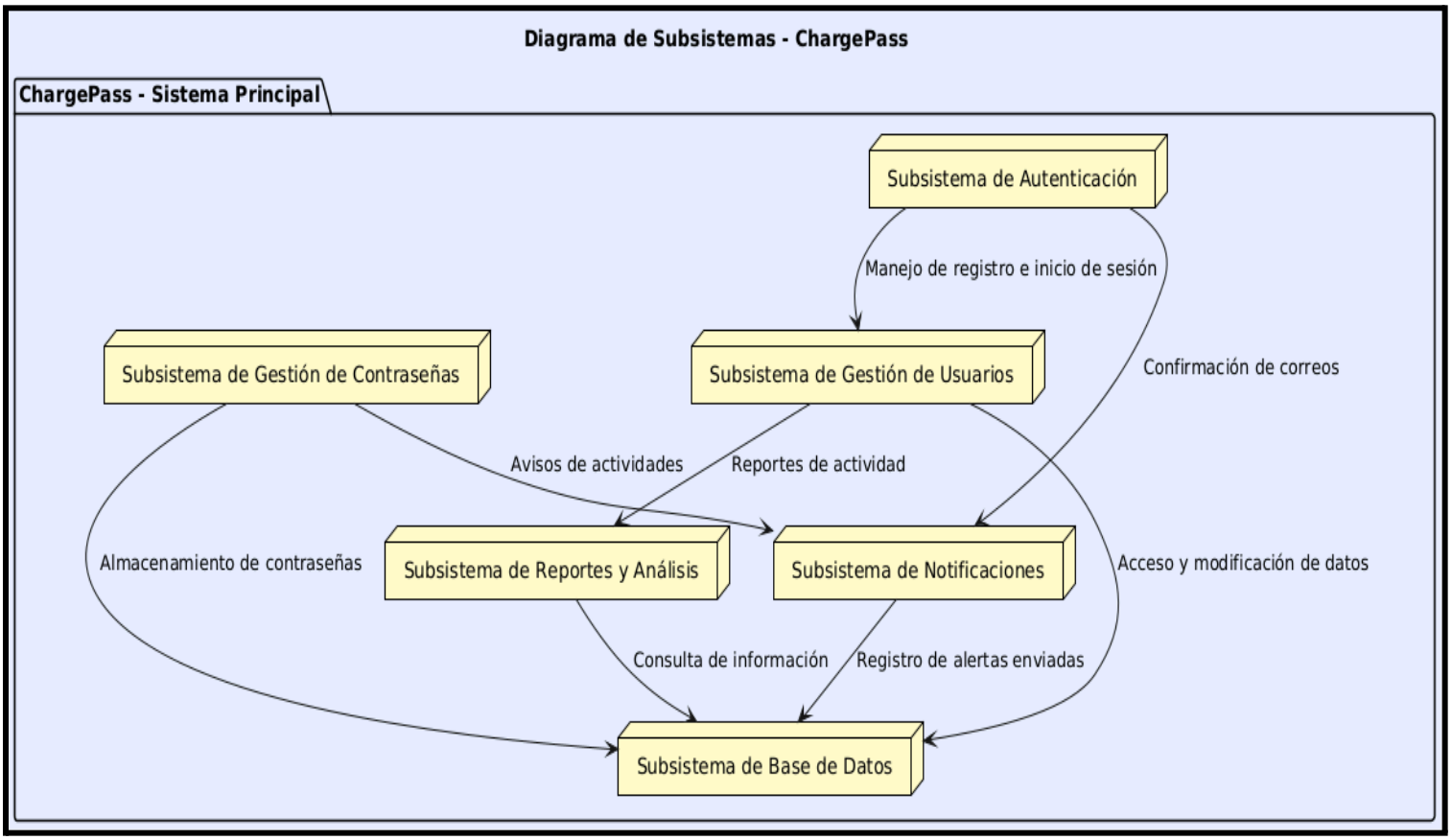


Fuente: Elaboración propia del equipo de trabajo

En el gráfico 07 :Apreciamos el diagrama de la vista de la arquitectura lógica que describe y representa los componentes lógicos que intervienen en la aplicación y su relación entre ellos.

3.2.1. Diagrama de Subsistemas

Gráfico 08:Diagrama de Subsistemas Paquetes del APP



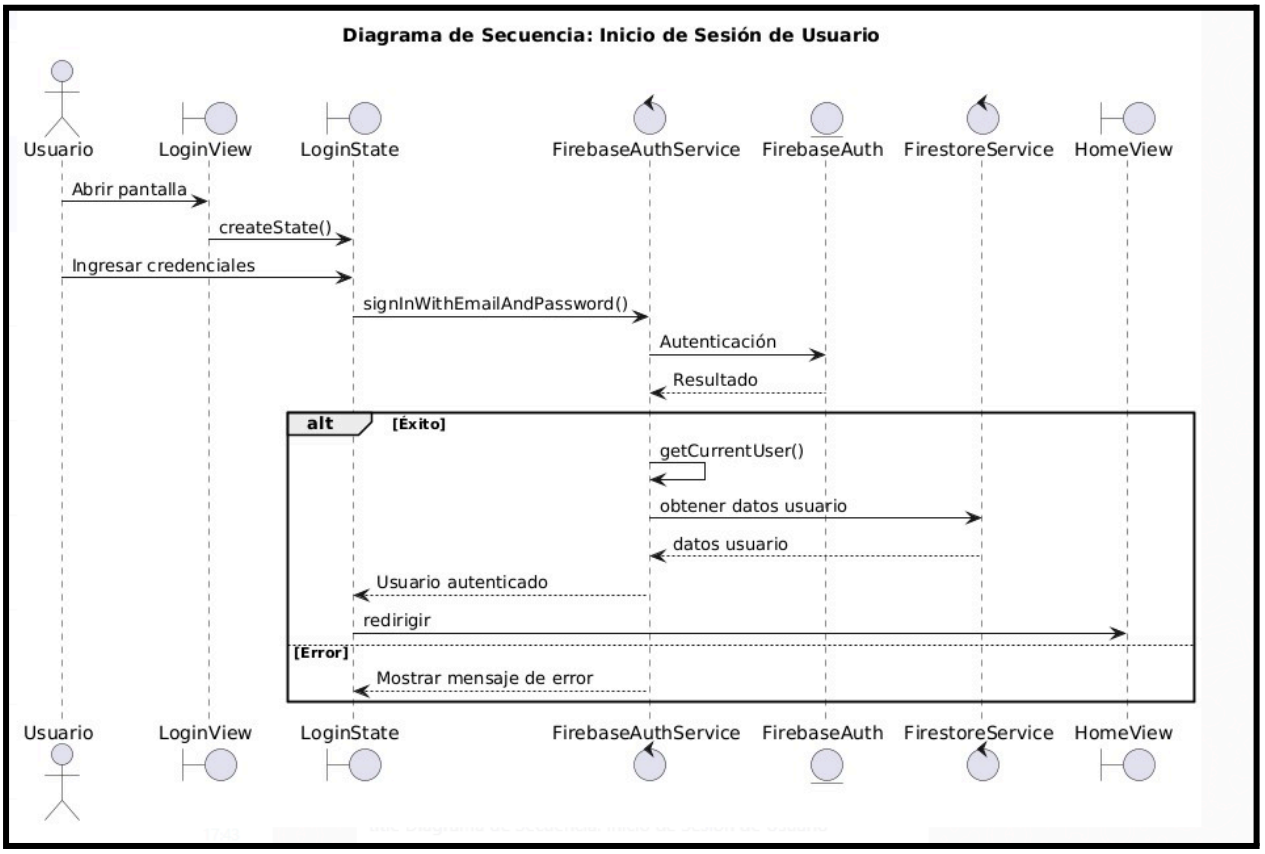
Fuente: Fuente: Elaboración propia del equipo de trabajo

En el gráfico 08: En el Diagrama de Paquetes nos permite visualizar la organización y disposición de los diversos elementos del sistema Web.

3.2.2. Diagrama de Secuencia con Objetos (vista de diseño)

1.1 Diagrama de Secuencia – Casos de Uso – Autenticar Usuario

Gráfico 09:Diagrama de Secuencia - Autenticar Usuario

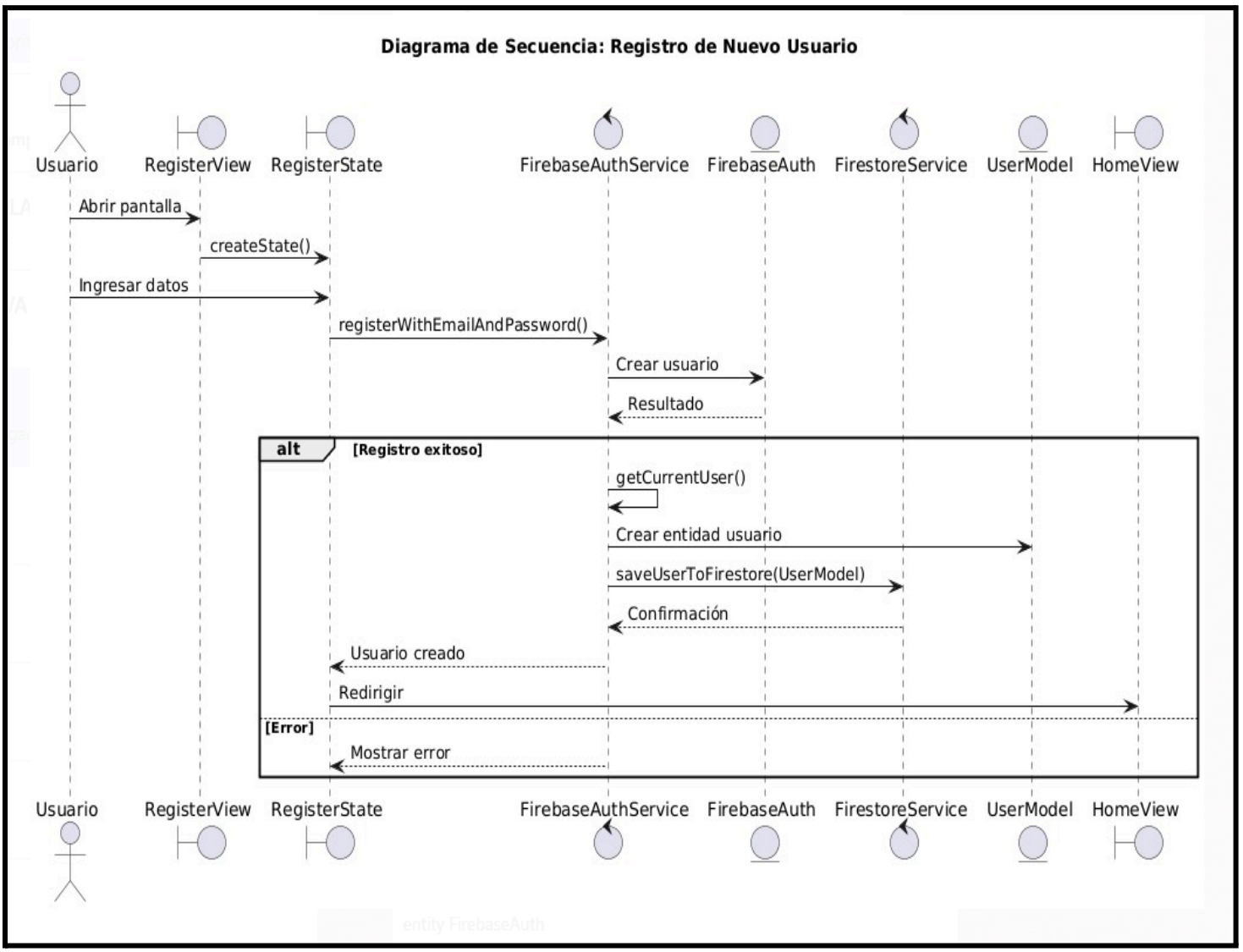


Fuente: Elaboración propia del equipo de trabajo

En la gráfica Nº 09 : El usuario para este caso inicia sesión, luego ingresa los datos de usuario, password para después darle al botón de iniciar sesión. Finalmente, accede al Dashboard principal la cual mostrará dependiendo del rol las funcionalidades del sistema.

1.2 Diagrama de Secuencia – Casos de Uso – Gestionar Usuario

Gráfico 10:Diagrama de Casos de Uso - Gestionar Usuario - Registrar



Fuente: Elaboración propia del equipo de trabajo

En la gráfica Nº 10 : El administrador selecciona en el dashboard el botón gestionar usuario,luego ingresa los datos a llenar en el formulario,rol y estado del nuevo usuario para después darle al botón de registrar.

Gráfico 39 :Diagrama de Secuencia - Recuperación de Contraseña

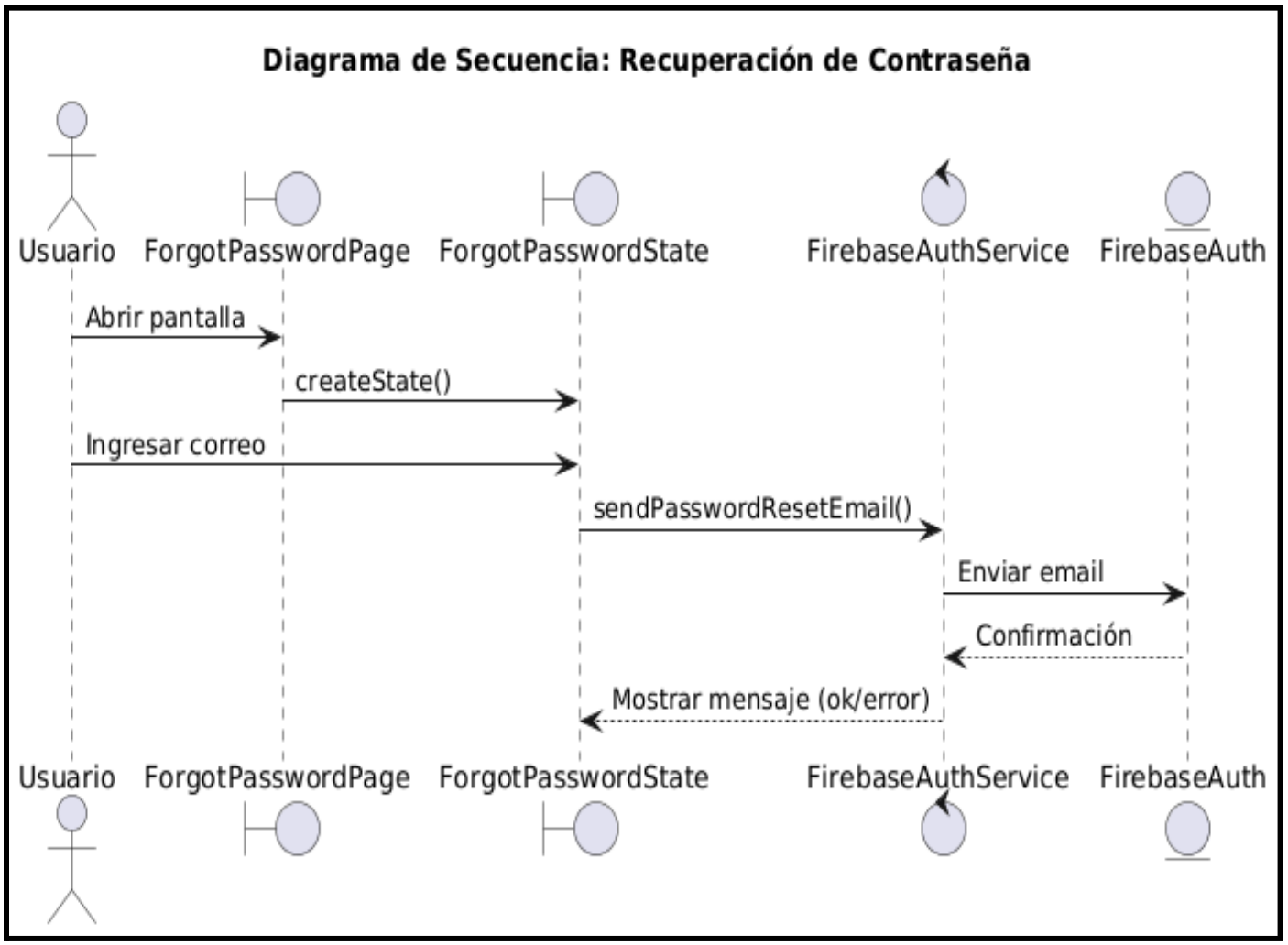
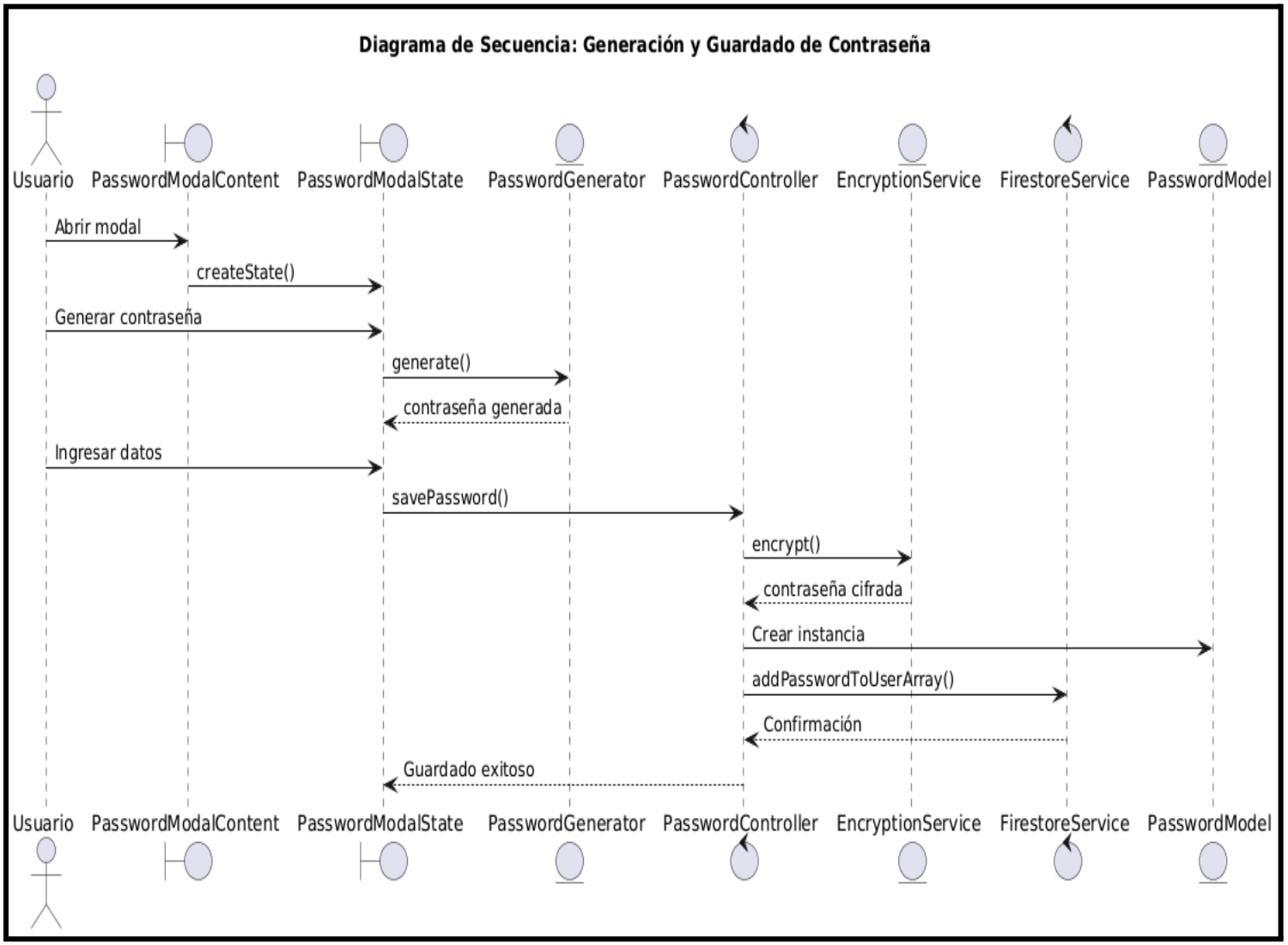
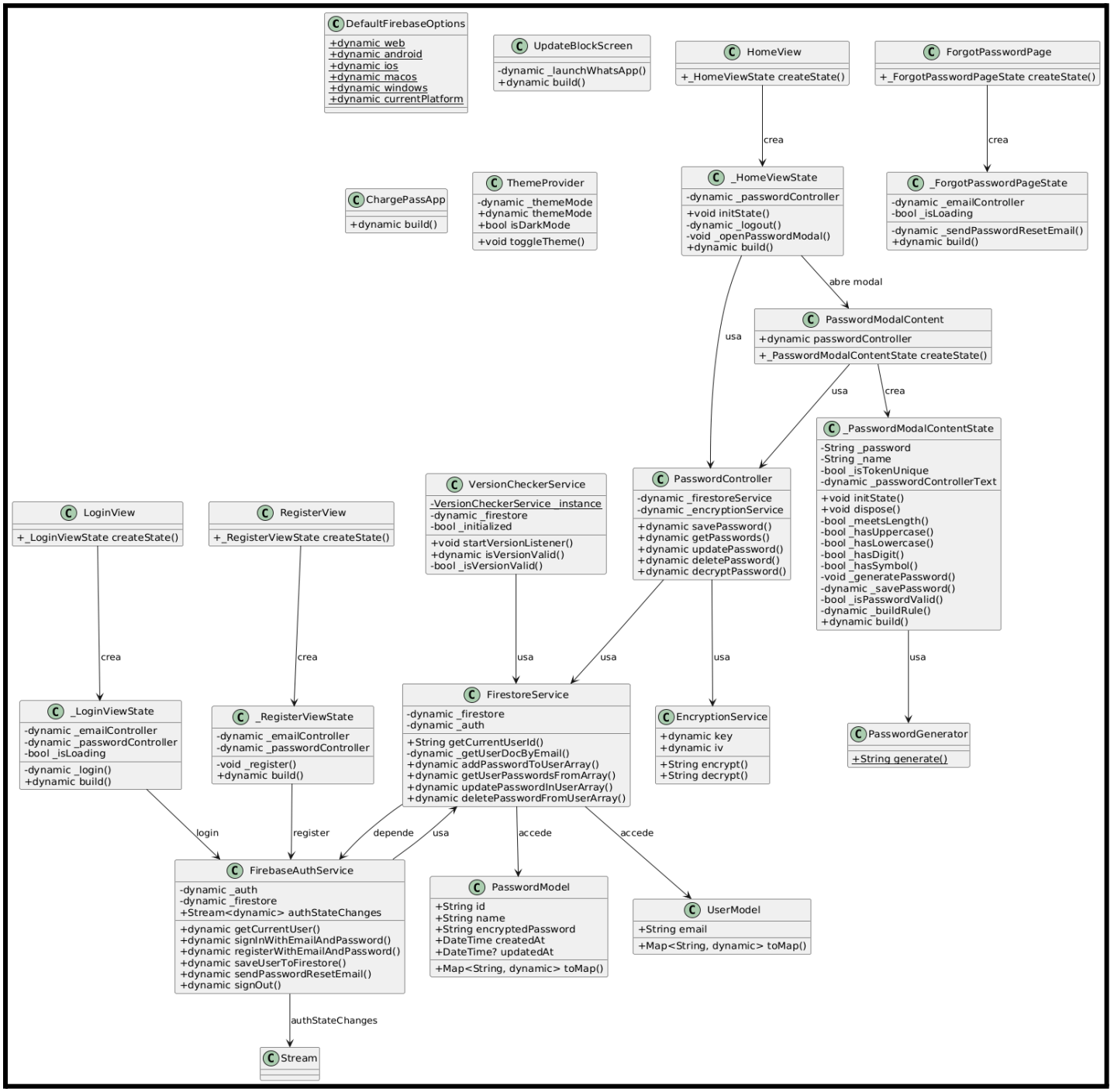


Gráfico 40:Diagrama de Casos de Uso - Gestionar Usuario - Buscar



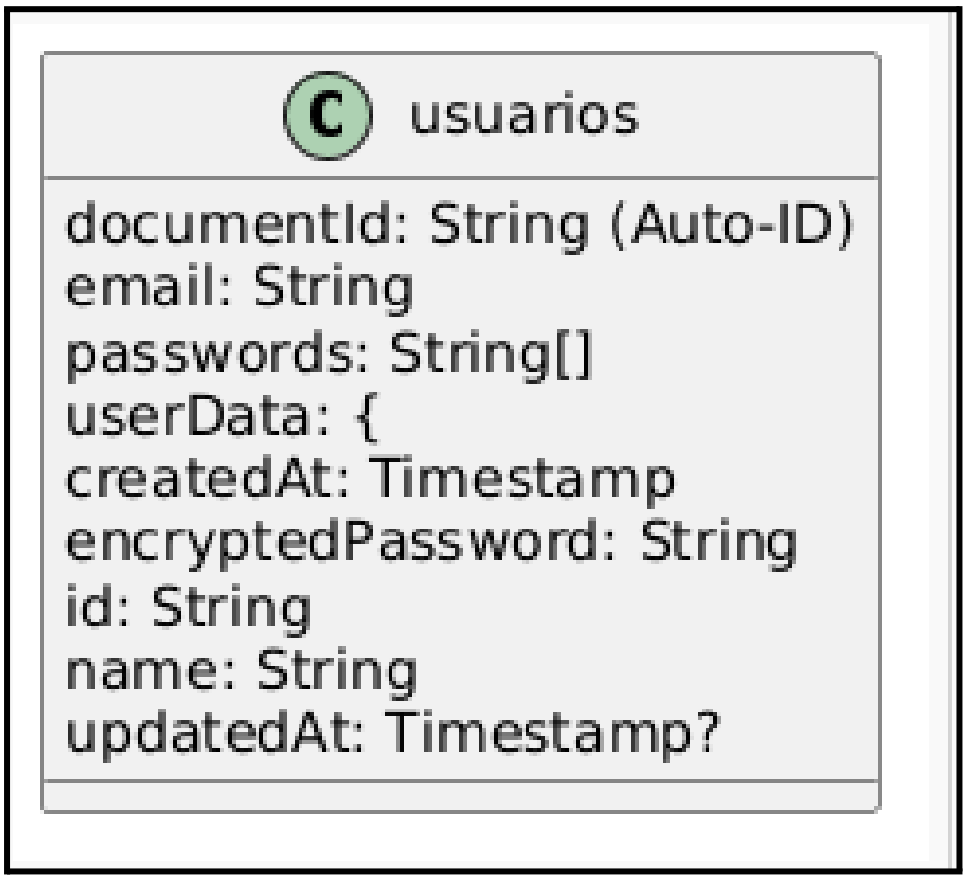
3.2.3. Diagrama de Clases

Gráfico 26: Diagrama de Clases del Proyecto



3.2.4. Diagrama de Base de Datos (Diseño)

Gráfico 27: Diagrama de Base de Datos



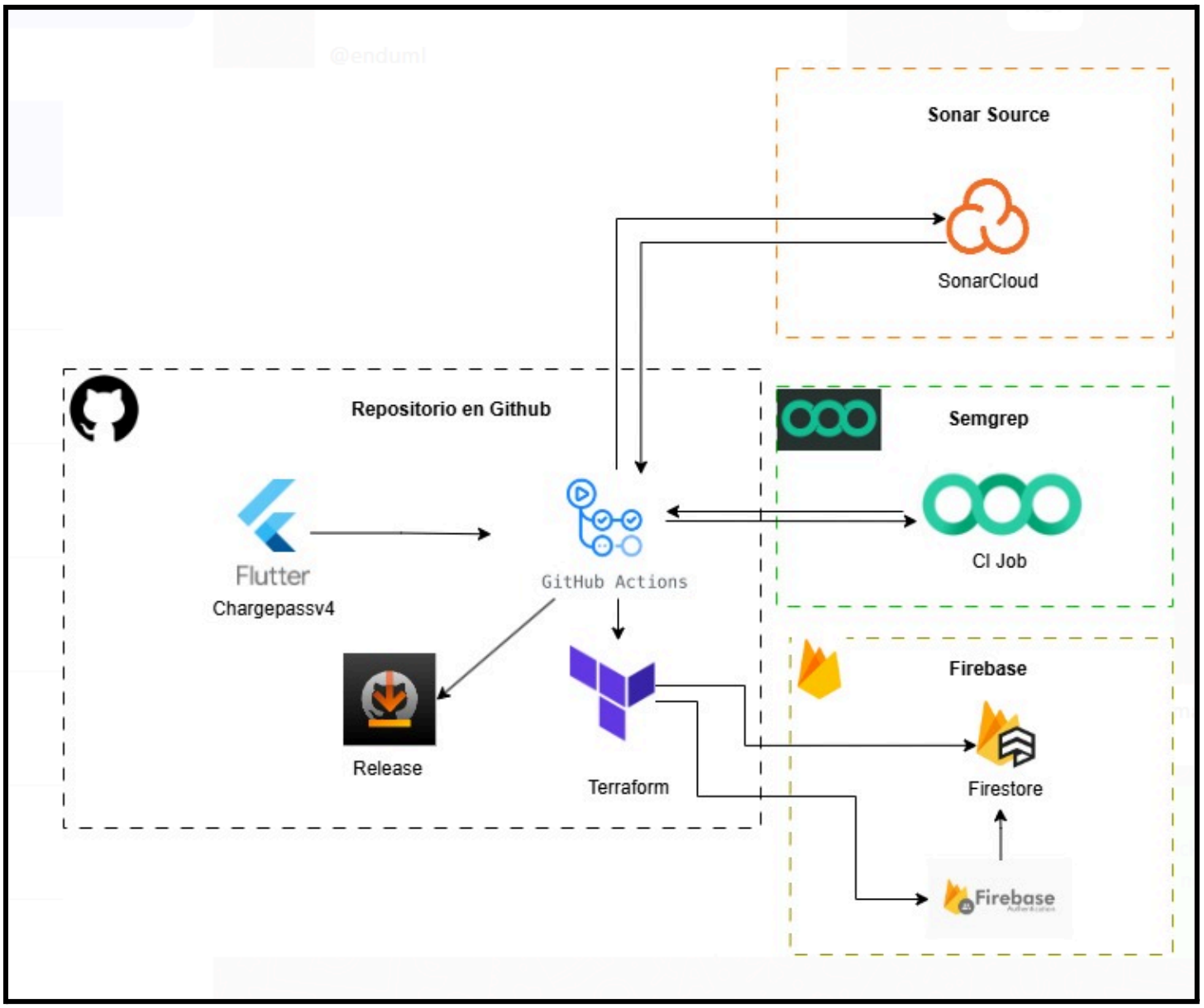
Fuente: Elaboración propia del equipo de trabajo

En la gráfica Nº 27 : Apreciamos el gráfico de nuestro Diagrama de Base de Datos con Firebase

3.3. Vista de Implementación

3.3.1. Diagrama de arquitectura del Proyecto

Gráfico 29: Diagrama de Arquitectura Proyecto

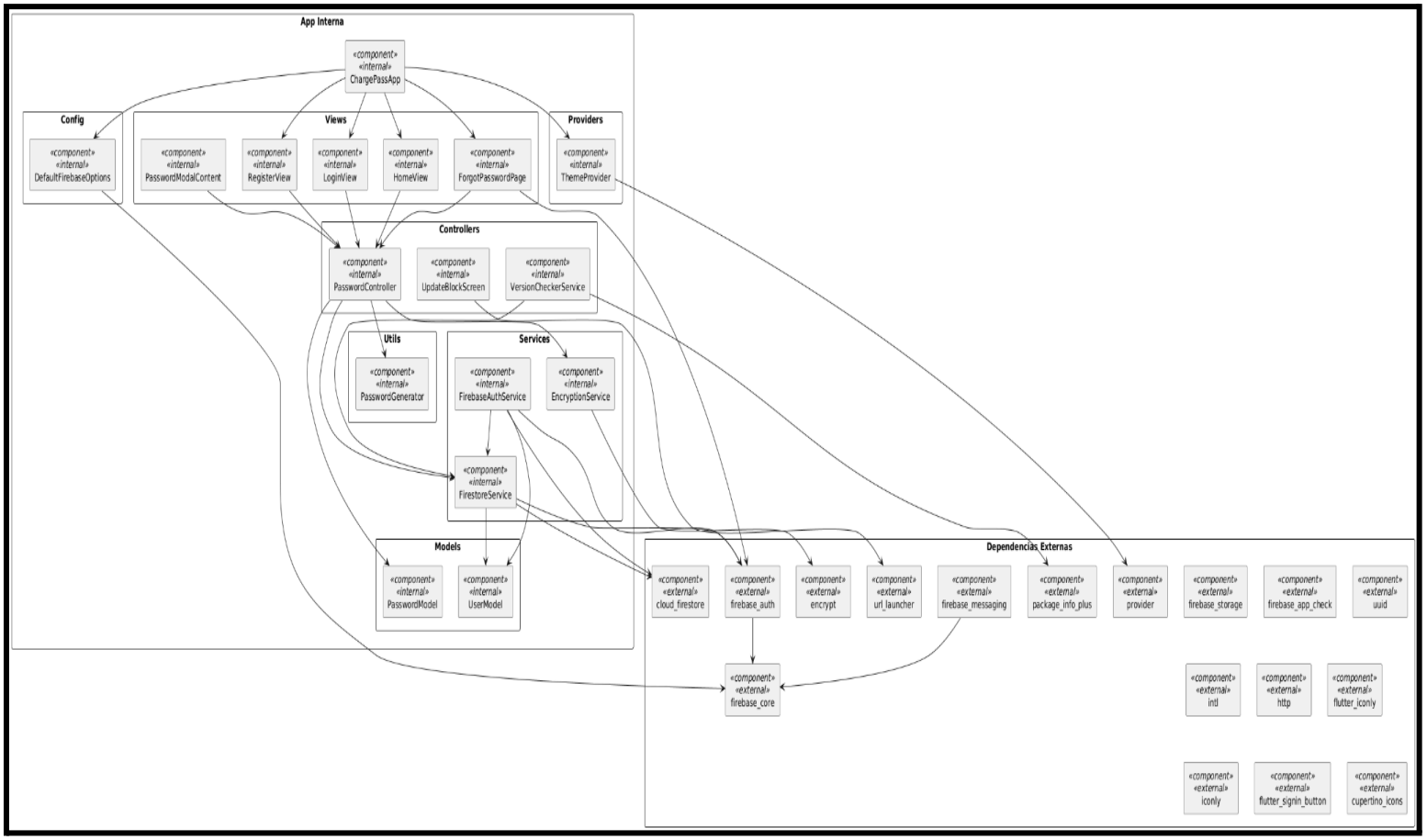


Fuente: Elaboración propia del equipo de trabajo

En la gráfica Nº 29 : Apreciamos el diagrama de arquitectura de software (Diseño).La arquitectura implementa un flujo de datos bidireccional, permitiendo tanto la recolección de información desde los sensores como el control desde la aplicación de usuario. Esta estructura garantiza escalabilidad y una clara separación de responsabilidades entre las diferentes capas del sistema.

3.3.2. Diagrama de arquitectura del sistema (Diagrama de componentes)

Gráfico 30: Diagrama de Componentes



Fuente: Elaboración propia del equipo de trabajo

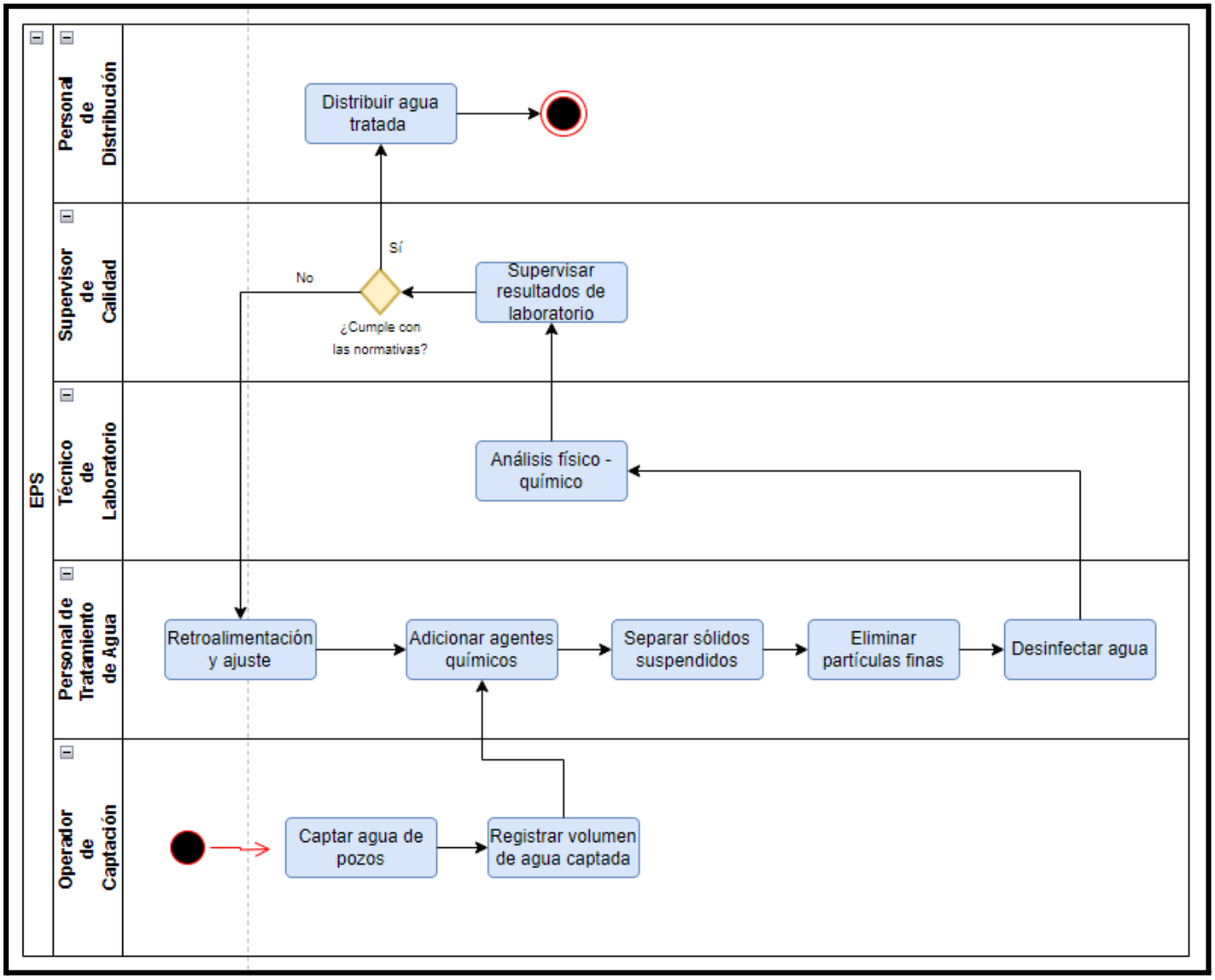
En la gráfica Nº 30 : Apreciamos el diagrama de arquitectura de software (Diseño).La arquitectura implementa un flujo de datos bidireccional, permitiendo tanto la recolección de información desde los sensores como el control desde la aplicación de usuario. Esta estructura garantiza escalabilidad y una clara separación de responsabilidades entre las diferentes capas del sistema.

3.4. Vista de Procesos

3.4.1. Diagrama de procesos del sistema

- **Diagrama de proceso actual**

Gráfico 33:Diagrama de Procesos Actual de la empresa para Supervisar la Calidad de Agua

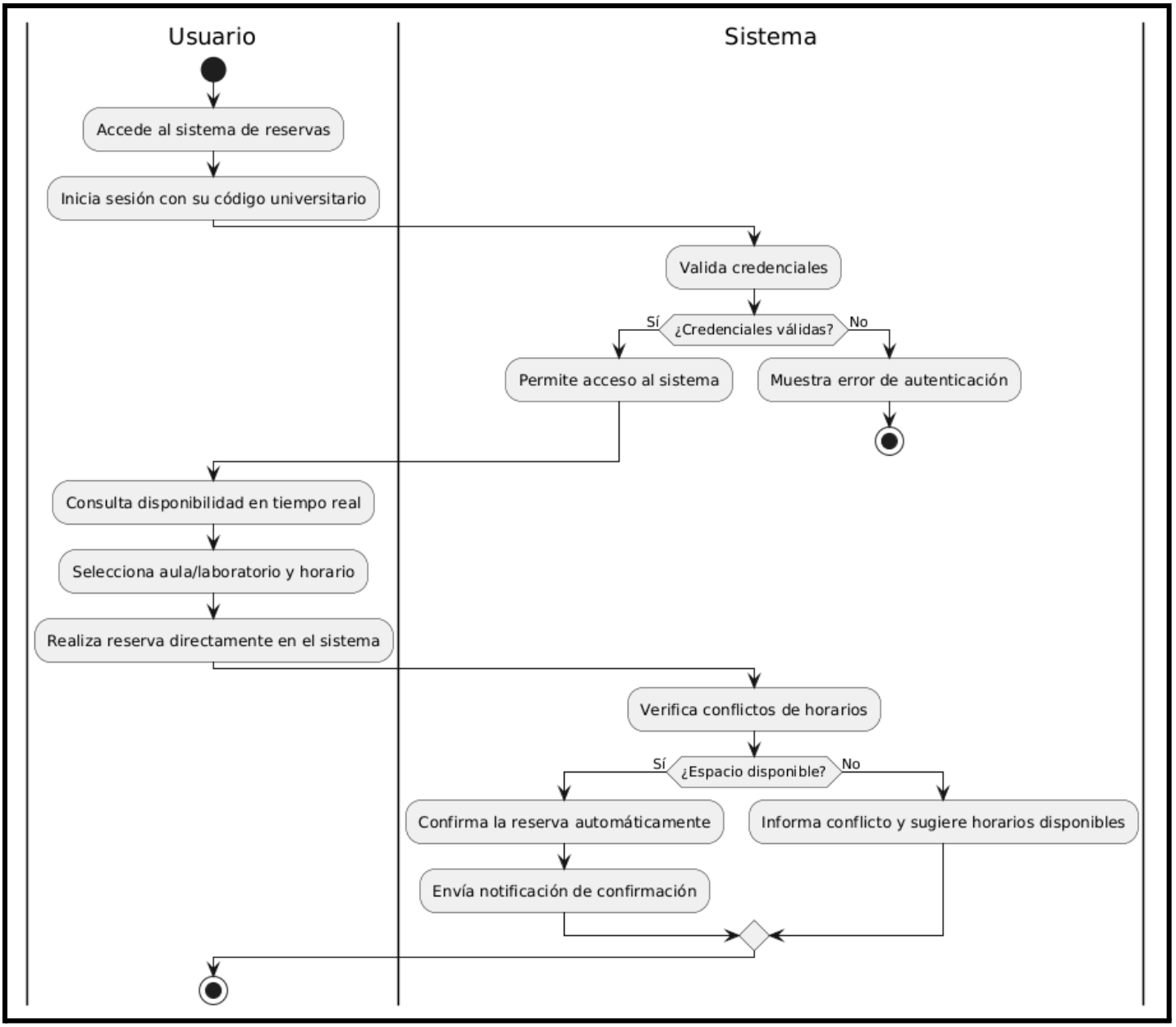


Fuente: Elaboración propia del equipo de trabajo

En el gráfico 33 :Se representa la funcionalidad del proceso actual de la empresa para la supervisión de la calidad de agua.

- **Diagrama de proceso propuesto**

Gráfico 34: Diagrama de Proceso Propuesto



Fuente: Elaboración propia del equipo de trabajo

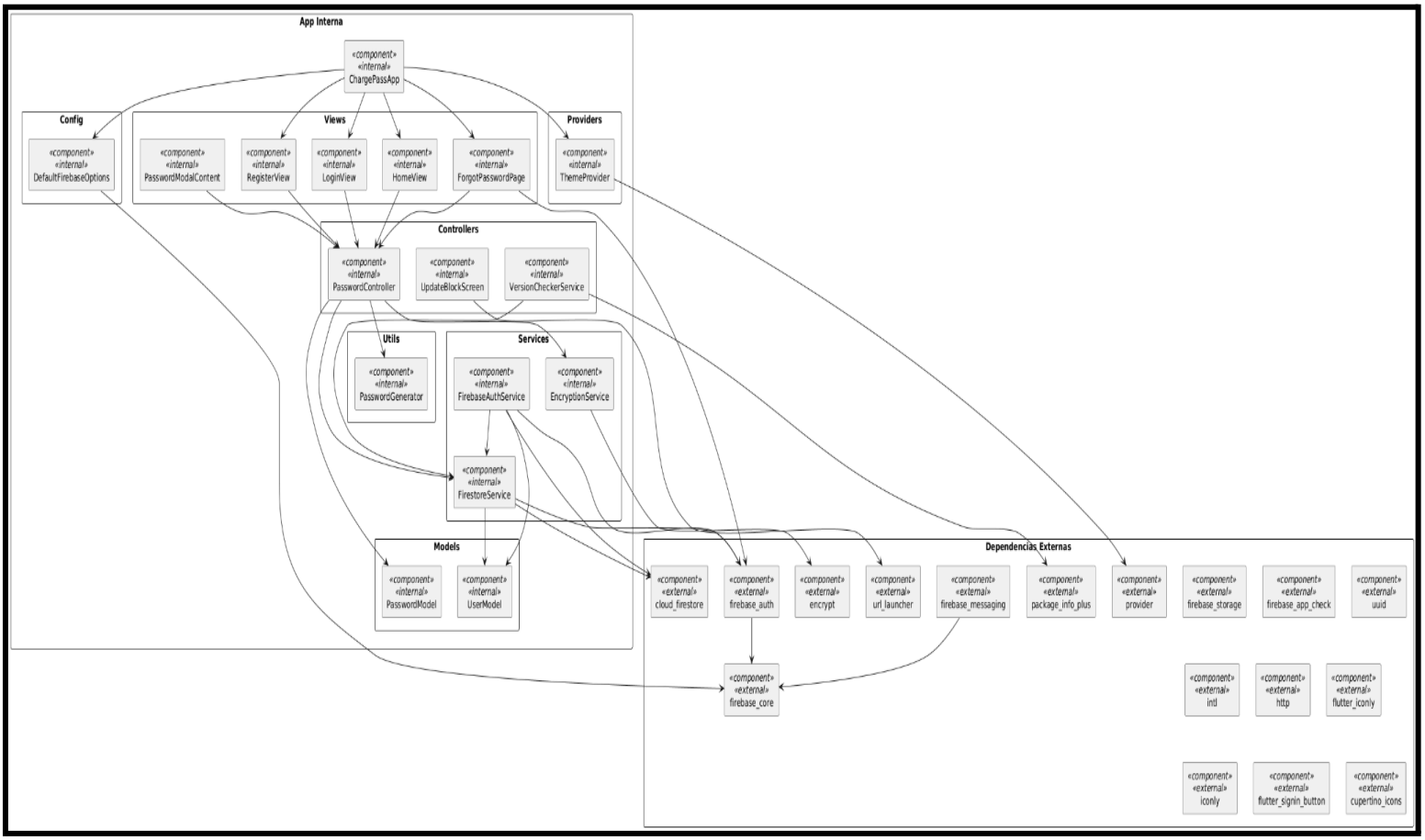
Se representa la funcionalidad de las actividades del proceso propuesto.

Fuente: Elaboración propia del equipo de trabajo

3.5. Vista de Despliegue

3.5.1. Diagrama de despliegue del Sistema

Gráfico 35: Diagrama de Despliegue del Sistema



Fuente: Elaboración propia del equipo de trabajo

En el gráfico N° 35 :Apreciamos el diagrama de despliegue del aplicativo movil Chargepass, nos ofrece una visión clara de la arquitectura del sistema, mostrando cómo cada componente se integra en el entorno para gestion de contraseñas seguras.

4. ATRIBUTOS DE CALIDAD DEL SOFTWARE

4.1. Escenario de Funcionalidad

La funcionalidad del sistema web debe garantizar que todas las acciones y procesos necesarios para cumplir los requerimientos establecidos se ejecuten correctamente.

Tabla 03: Atributos de Calidad Funcionalidad

1. Fuente: Usuarios, administradores
2. Estímulo: Realizar acciones como autenticar, gestionar usuarios, sensores y canales, grabar lecturas y generar reportes.
3. Entorno: Sistema en operación.
4. Artefacto: Sistema (Sistema Web)
5. Respuesta: Sistema web (plataforma IoT para la gestión de sensores de calidad del agua).
6. Medida de la Respuesta: El sistema debe completar correctamente las operaciones solicitadas por los usuarios, como la autenticación, gestión de sensores, canales y usuarios,etc**.**
7. Atributo de calidad afectado: Funcionalidad.

Fuente: Elaboración propia del equipo de trabajo

En la tabla N° 03 : Apreciamos los atributos de Calidad de Software, Escenario de Funcionalidad en las cuales se determinaron 7 criterios.

4.2. Escenario de Usabilidad

Para este caso el sistema implementado debe ser fácil de usar e intuitivo para todos los usuarios, permitiendo el acceso y la operación sin mayores dificultades.

Tabla 04: Atributos de Calidad Usabilidad

1. Fuente: Usuarios del sistema.
2. Estímulo: Interacción con el sistema (uso diario).
3. Entorno: Sistema web operativo.
4. Artefacto: Sistema Web
5. Respuesta: Interfaz sencilla y amigable que permita a los usuarios navegar fácilmente, aprender rápidamente y realizar acciones con pocos pasos.
6. Medida de la Respuesta: El usuario debe aprender a utilizar el sistema en el menor tiempo posible
7. Atributo de calidad afectado: Usabilidad

Fuente: Elaboración propia del equipo de trabajo

En la tabla N° 04 : Apreciamos los atributos de Calidad de Software, Escenario de Usabilidad en las cuales se determinaron 7 criterios.

4.3. Escenario de Rendimiento

El sistema debe ofrecer un buen rendimiento, especialmente en cuanto a la rapidez de respuesta y la capacidad de manejar un volumen considerable de datos provenientes de los sensores.

Tabla 05: Atributos de Calidad Rendimiento

1. Fuente: Lecturas de sensores y generación de reportes.
2. Estímulo: Gran cantidad de datos almacenados y consultados.
3. Entorno: Sistema en operación continua.
4. Artefacto: Sistema web (gestión de sensores y reportes).
5. Respuesta: El sistema debe procesar las lecturas en tiempo real y generar reportes en menos tiempo posible.
6. Medida de la Respuesta: El tiempo de respuesta debe ser inferior a 7 segundos para lecturas en tiempo real y menos de 5 segundos para generar reportes.
7. Atributo de calidad afectado: Rendimiento

Fuente: Elaboración propia del equipo de trabajo

En la tabla N° 05 : Apreciamos los atributos de Calidad de Software, Escenario de Rendimiento en las cuales se determinaron 7 criterios.

4.4. Escenario de Mantenibilidad

La mantenibilidad es la habilidad de un sistema de someterse a cambios con un grado de facilidad. Esos cambios pueden afectar componentes, servicios, características e interfaces cuando se agrega o se cambia la funcionalidad corrigiendo errores y satisfaciendo nuevos requerimientos de negocios.

Tabla 06: Atributos de Calidad Mantenibilidad

1.Fuente: Administradores
2.Estímulo: Necesidad de realizar ajustes o correcciones en las funciones del sistema.
3.Entorno: Sistema en explotación.
4.Artefacto: Sistema Web
5.Respuesta: El sistema debe permitir realizar cambios o ajustes sin afectar la operatividad ni generar errores inesperados.
6.Medida de la Respuesta: Los errores deben diagnosticarse y corregirse en un tiempo promedio de 2 horas o menos.
7.Atributos de Calidad: Mantenibilidad

Fuente: Elaboración propia del equipo de trabajo

En la tabla N° 06 : Apreciamos los atributos de Calidad de Software, Escenario de Mantenibilidad en las cuales se determinaron 7 criterios.

4.5. Escenario de Adaptabilidad

El sistema debe ser accesible desde cualquier navegador web y dispositivo, adaptándose a distintos tamaños de pantalla y resoluciones.

Tabla 07: Atributos de Calidad Adaptabilidad

1. Fuente: Dispositivos de los usuarios.
2. Estímulo: Acceso desde diferentes navegadores y dispositivos (PC, tablet, móvil).
3. Entorno: Sistema en explotación.
4. Artefacto: Sistema web.
5. Respuesta: El sistema debe visualizarse correctamente en todos los navegadores y dispositivos.
6. Medida de la Respuesta: El sistema debe ser probado y compatible con al menos 5 navegadores y 3 tipos de dispositivos.
7. Atributo de calidad afectado: Adaptabilidad

Fuente: Elaboración propia del equipo de trabajo

En la tabla N° 07 : Apreciamos los atributos de Calidad de Software, Escenario de Adaptabilidad en las cuales se determinaron 7 criterios.

4.6. Escenario de Seguridad

El sistema deberá impedir, en la medida de todo lo posible, los fallos de seguridad como intrusos que puedan acceder a la página web haciéndose pasar por usuarios con determinados permisos dentro de esta, o el acceso a los datos, pudiendo modificarlos, borrarlos o extraerlos.

Tabla 08: Atributos de Calidad Seguridad

1. Fuente: Usuarios e intrusos potenciales.
2. Estímulo: Intentos de acceso a datos sensibles o de intrusión.
3. Entorno: Sistema en explotación.
4. Artefacto: Sistema web, base de datos, y servidores.
5. Respuesta: El acceso al sistema debe estar restringido por medio de autenticación segura y protección de datos.
6. Medida de la Respuesta: Número de intrusiones o accesos no autorizados detectados debe ser cero.
7. Atributo de calidad afectado: Seguridad

Fuente: Elaboración propia del equipo de trabajo

En la tabla N° 08 : Apreciamos los atributos de Calidad de Software, Escenario de Seguridad en las cuales se determinaron 7 criterios.

4.7. Escenario de Confiabilidad

El sistema debe ser fiable, garantizando que las funciones críticas como la grabación de lecturas y la generación de alertas se realicen sin fallos.

Tabla 09: Atributos de Calidad Confiabilidad

1. Fuente: Usuarios y sensores.
2. Estímulo: Realización de operaciones críticas (grabar lecturas, generar alertas).
3. Entorno: Sistema en operación continua.
4. Artefacto: Sistema web.
5. Respuesta: El sistema debe mantener su funcionalidad y disponibilidad en todo momento sin interrupciones.
6. Medida de la Respuesta: Disponibilidad del sistema en al menos el 99.9% del tiempo.
7. Atributo de calidad afectado: Confiabilidad.

Fuente: Elaboración propia del equipo de trabajo

En la tabla N° 09 : Apreciamos los atributos de Calidad de Software, Escenario de Confiabilidad en las cuales se determinaron 7 criterios.

Tabla 10: Atributos de Calidad Confiabilidad

1. Fuente: Proceso de inicio de sesión y verificación con código enviado por correo.
2. Estímulo:Múltiples intentos de inicio de sesión con diferentes cuentas.
3. Entorno: Plataforma en operación continua con conexión al servicio de correo SMTP.
4. Artefacto: Módulo de autenticación y componente de correo.
5. Respuesta: El sistema debe generar, enviar y validar correctamente el código sin errores.
6. Medida de la Respuesta: Tasa de error de envío/validación menor al 1%.
7. Atributo de calidad afectado: Confiabilidad.

Fuente: Elaboración propia del equipo de trabajo

En la tabla N° 09 : Apreciamos los atributos de Calidad de Software, Escenario de Confiabilidad en las cuales se determinaron 7 criterios para la autenticación de correo electrónico.