UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas

Sistema Gestor de contraseñas: ChargePass

Curso: *Patrones de Software*

Docente: Mag. *Patrick Cuadros Quiroga*

Integrantes:

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

Tacna – Perú

2025

Sistema Gestor de contraseñas: ChargePass

Documento de Especificación de Requerimientos de Software

Versión 1.0

ÍNDICE GENERAL

INTRODUCCIÓN

I. Generalidades de la Empresa

1) Nombre de la Empresa

ChargePass

2) Visión

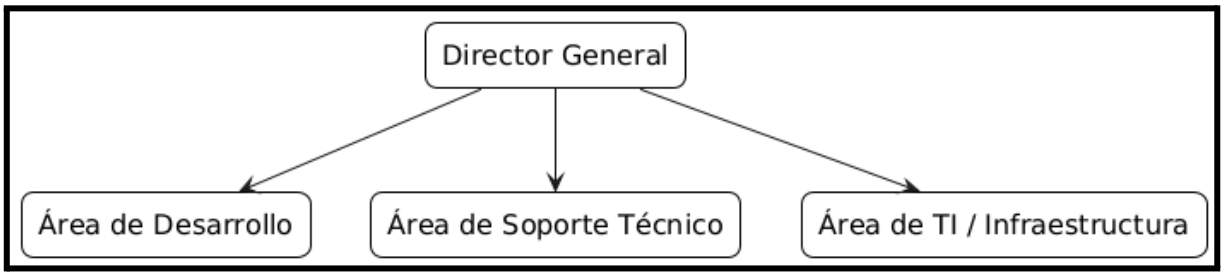
Ser una plataforma de referencia a nivel nacional en la gestión segura de contraseñas, reconocida por su confiabilidad, facilidad de uso y compromiso con la protección de la identidad digital de sus usuarios.

3) Misión

Desarrollar e implementar una solución tecnológica eficiente, segura e intuitiva que permita a los usuarios generar, almacenar y gestionar contraseñas personalizadas, garantizando su autenticación mediante verificación por correo electrónico y promoviendo buenas prácticas en la seguridad digital.

4) Organigrama

Gráfico 01:Organigrama de la Empresa



Fuente: Gráfico elaborado por el equipo de trabajo

II. Visionamiento de la Empresa

1) Descripción del Problema

En la actualidad, muchas personas utilizan contraseñas débiles, repetidas o poco seguras debido a la dificultad para recordar múltiples credenciales complejas. Esta situación incrementa el riesgo de accesos no autorizados, robo de identidad digital y vulnerabilidades en la protección de información sensible. A pesar de que existen diversas herramientas para la gestión de contraseñas, muchas de ellas no ofrecen un proceso de autenticación previo confiable, ni garantizan una experiencia accesible y segura desde dispositivos móviles.

Además, el registro de usuarios sin una verificación adecuada puede abrir la puerta a registros fraudulentos o bots, lo que compromete la seguridad del sistema y la privacidad de los usuarios. La falta de mecanismos robustos de validación y generación segura de contraseñas limita la efectividad de estos sistemas como herramientas de protección real frente a amenazas cibernéticas comunes.

En este contexto, surge la necesidad de una solución moderna, intuitiva y segura que permita a los usuarios registrarse de manera confiable mediante verificación por correo electrónico, generar contraseñas robustas de forma automática o personalizada, y almacenarlas de manera segura. El desarrollo de ChargePass, una aplicación móvil construida con Flutter y respaldada por Firebase, busca cubrir esta necesidad, integrando funcionalidades clave como el control de acceso autenticado, la validación de identidad y la generación y gestión de contraseñas seguras, con una visión orientada a proteger la identidad digital de los usuarios y prevenir accesos indebidos

2) Objetivos de Negocios

- Mejorar la seguridad digital de los usuarios mediante la implementación de una aplicación móvil que permita la generación, almacenamiento y gestión de contraseñas seguras, reduciendo el riesgo de accesos no autorizados y vulnerabilidades comunes.

- Garantizar autenticación confiable asegurando que solo usuarios verificados puedan acceder al sistema, a través de un proceso de validación por correo electrónico, fortaleciendo la integridad de los registros y evitando cuentas fraudulentas.

- Facilitar la toma de decisiones del usuario brindando herramientas claras para la creación automática o personalizada de contraseñas, permitiendo elegir entre opciones seguras adaptadas a distintos niveles de complejidad o necesidades.

- Reducir la dependencia de métodos inseguros de gestión de contraseñas, como el almacenamiento manual o repetitivo, automatizando el proceso de generación y almacenamiento con respaldo seguro en Firebase, lo que también optimiza la experiencia del usuario y minimiza errores humanos.

3) Objetivos de Diseño

- Desarrollar una aplicación móvil intuitiva que permita a los usuarios gestionar contraseñas seguras mediante generación automática, almacenamiento encriptado y autenticación biométrica, mejorando la seguridad digital accesible para todos los perfiles de usuarios.
- Implementar una arquitectura robusta que integre Flutter para la interfaz multiplataforma y Firebase para la gestión segura de datos, garantizando confiabilidad en el almacenamiento y sincronización de credenciales.
- Diseñar funcionalidades de alerta temprana para contraseñas vulnerables o repetidas, y opciones de respaldo seguro que permitan recuperar acceso sin comprometer la protección de los datos.
- Crear una solución escalable con capacidad para incorporar futuras mejoras como integración con navegadores, gestión de equipos y adaptación a nuevos estándares de ciberseguridad, asegurando su vigencia ante evoluciones tecnológicas.

4) Alcance del proyecto

La solución se presenta como una aplicación móvil (y eventualmente web) que cubre el siguiente conjunto de funcionalidades clave:

- Registro de usuarios con verificación por correo electrónico.
- Inicio de sesión únicamente después de la verificación exitosa del correo.
- Generación de contraseñas mediante:
- Opción automática con criterios de seguridad establecidos (longitud, caracteres especiales, etc.).
- Opción manual mediante el ingreso de un token personalizado.
- Almacenamiento seguro de los registros de contraseña.

Control de acceso y autenticación mediante Firebase Auth.

Posibilidad futura de:

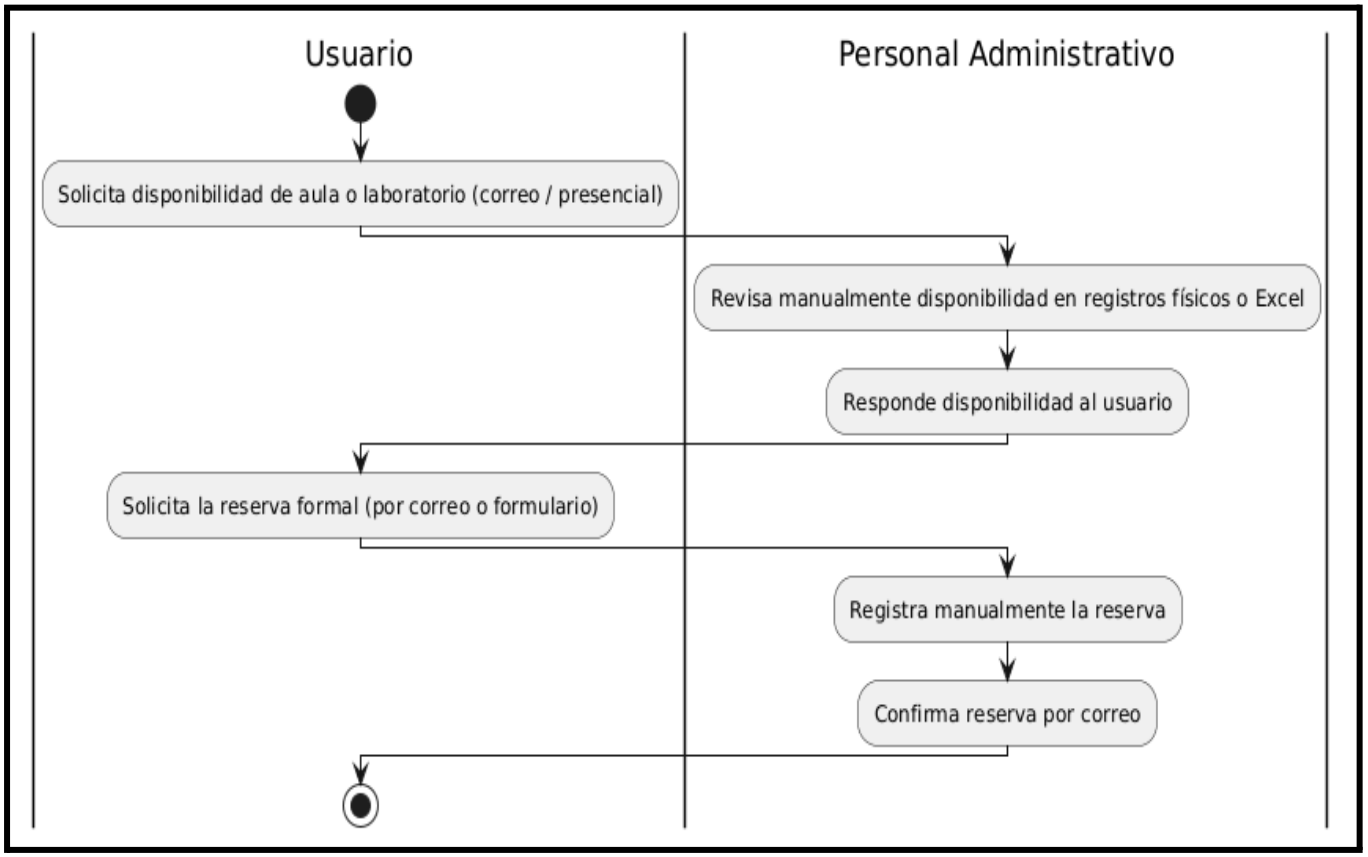
- Limitar registros según dominios de correo válidos.
- Implementar extensiones de seguridad (ej. autenticación multifactor, validaciones de dispositivo).

III. Análisis de Procesos

A. Diagrama del Proceso

1. Diagrama de Proceso Actual

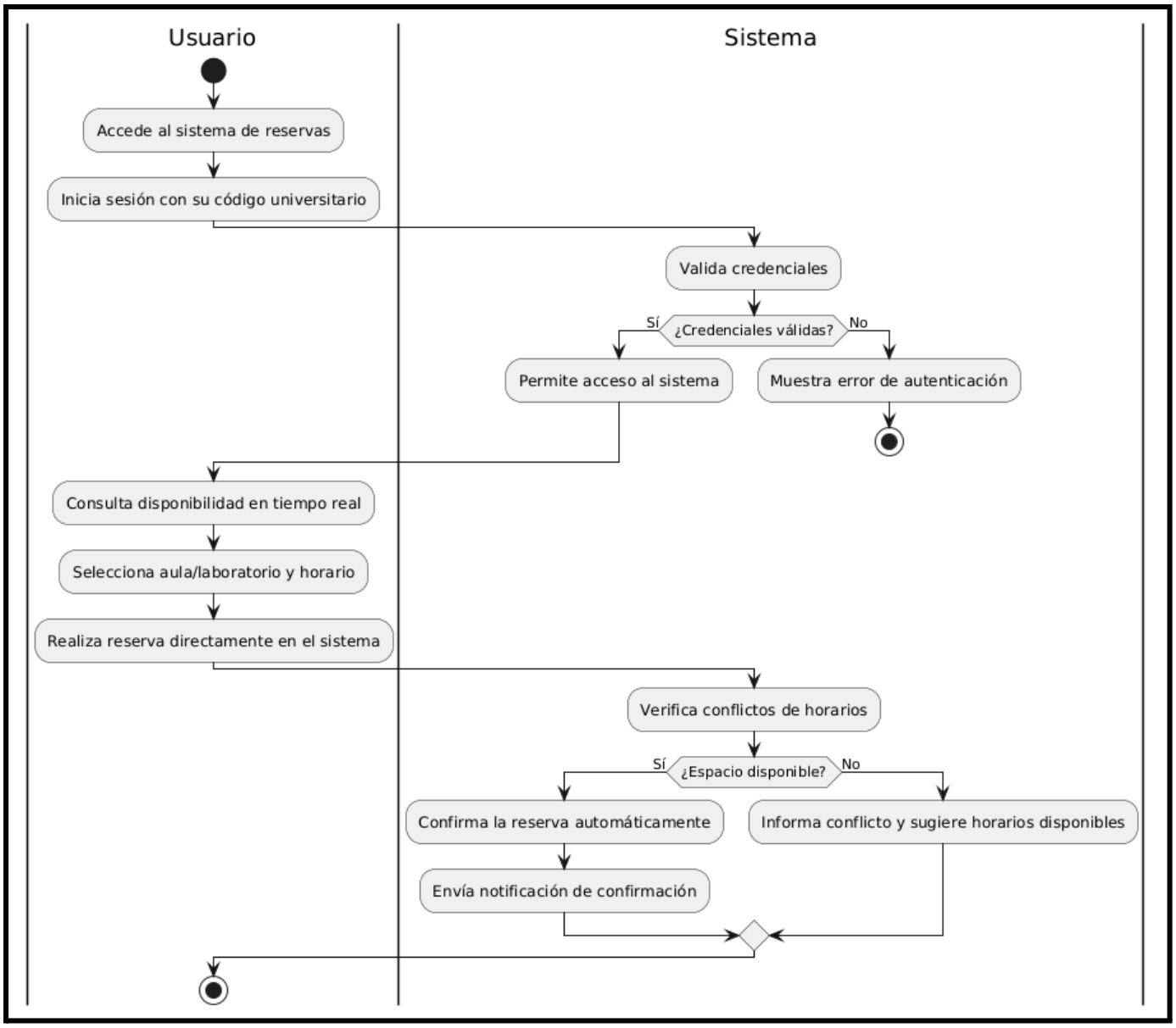
Gráfico 02:Diagrama de Procesos Actual de la empresa



Fuente: Elaboración propia del equipo de trabajo
En el gráfico 02 :Se representa la funcionalidad del proceso actual de la empresa.

2. Diagrama de Proceso Propuesto

Gráfico 03: Diagrama de Proceso Propuesto



Fuente: Elaboración propia del equipo de trabajo

En el gráfico N° 3 se representa la funcionalidad de las actividades del proceso propuesto.

IV. Especificación de Requerimientos de Software

A. Cuadro de Requerimientos funcionales Inicial

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.

B. Cuadro de 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.

V. Fase de Desarrollo

1. Perfiles de Usuario

Tabla 3:Perfil del Usuario Administrador

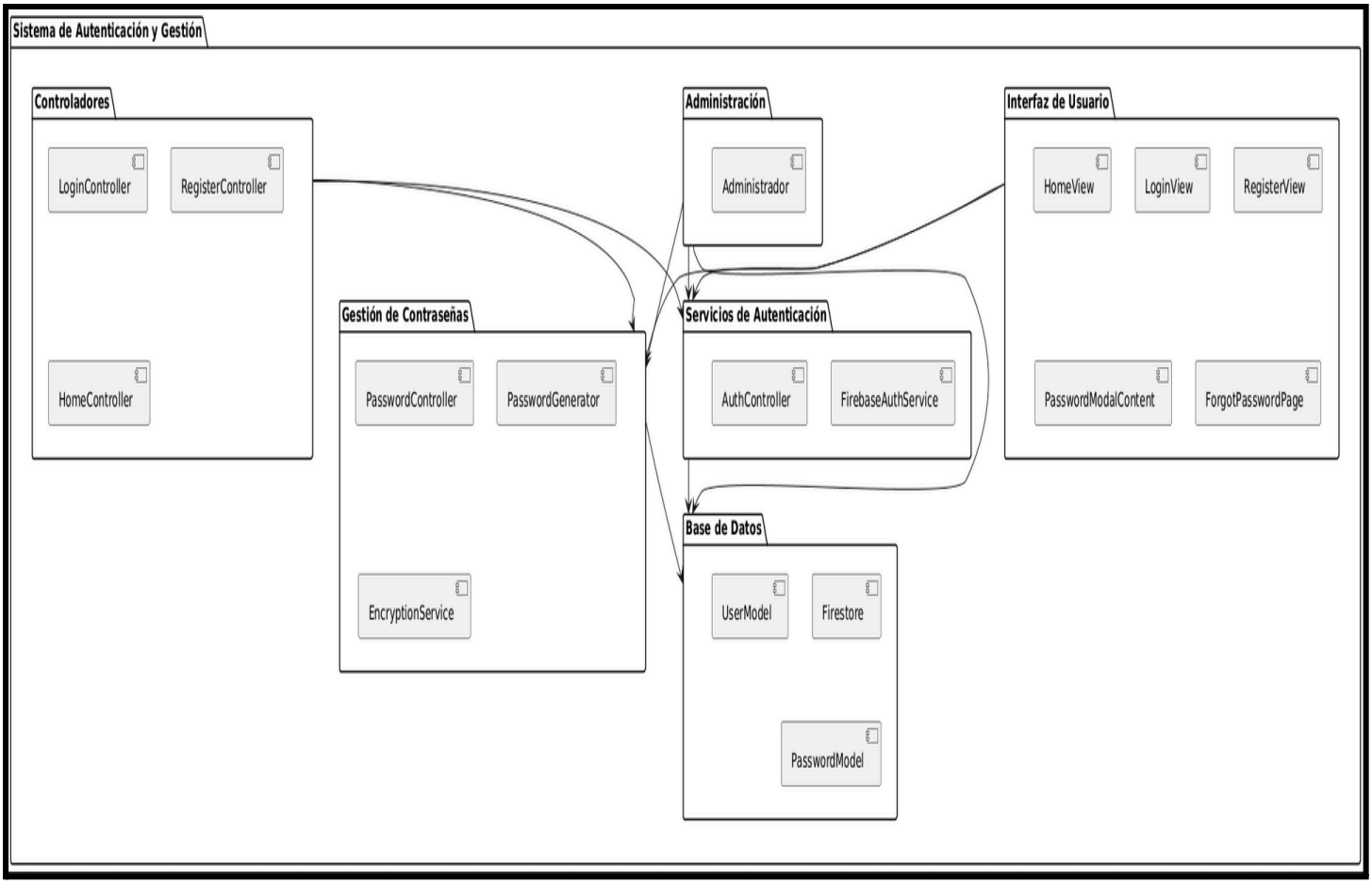
PERFIL DE USUARIO ADMINISTRADOR	
Representante	Administrador del Sistema
Descripción	El administrador es el usuario con el mayor nivel de acceso y control dentro del sistema. Su responsabilidad principal es gestionar la configuración general del sistema, usuarios, roles, contraseñas y gestionar aspectos críticos de seguridad y verificación. El primer administrador se crea directamente en la base de datos por el equipo de desarrollo o implementación. Una vez dentro, este administrador podrá gestionar y crear otros usuarios administradores o regulares, asignar roles y permisos, y supervisar las operaciones del sistema.
Tipo	Usuario con privilegios completos
Método de Creación	El primer usuario administrador será creado manualmente en la base de datos por el equipo de desarrollo o implementación. Este administrador inicial tendrá la capacidad de gestionar la creación de nuevos usuarios, así como asignar roles y permisos desde el sistema.
Responsabilidades	● Gestionar la creación de usuarios administradores y regulares. ● Asignar roles y permisos para garantizar el acceso adecuado a los recursos. ● Supervisar el proceso de registro de usuarios y la verificación de correos electrónicos. ● Gestionar la configuración de contraseñas seguras y procesos de recuperación. ● Garantizar que todos los procesos de autenticación y verificación de usuarios se ejecuten correctamente. ● Resolver problemas técnicos relacionados con el acceso de usuarios, inicio de sesión y generación de contraseñas. ● Supervisar el sistema para asegurarse de que no haya fallos en la autenticación y gestión de contraseñas.
Criterios de Éxito	● Configuración y gestión efectiva del aplicativo y sus componentes. ● Respuesta oportuna y efectiva a problemas técnicos y solicitudes de usuarios. ● Correcta gestión de permisos y accesos para usuarios y dispositivos.
Implicación	El administrador debe estar altamente involucrado en el funcionamiento del sistema. Es responsable de la supervisión continua de la plataforma, la gestión de la seguridad y la accesibilidad, y la resolución de problemas técnicos que puedan surgir con el acceso o la autenticación de usuarios.
Comentarios de Problemas	Es crucial que el administrador pueda identificar y resolver problemas técnicos complejos, como fallos en el proceso de verificación de correos electrónicos, problemas en el inicio de sesión o contraseñas no válidas. Las demoras o fallos en la gestión del sistema pueden afectar gravemente la operatividad y la experiencia de los usuarios. La rapidez en la respuesta a estas situaciones es fundamental para mantener la eficiencia del sistema.

Fuente: Elaboración propia del equipo de trabajo,En la Tabla Nº3. Tenemos la descripción del perfil Usuario esta adaptación del perfil del usuario administrador se alinea con las funciones y responsabilidades específicas de la plataforma que estás desarrollando, asegurando que el sistema de gestión de usuarios y contraseñas funcione de manera segura y eficiente.

2. Modelo Conceptual

a. Diagrama de Paquetes

Gráfico 06:Diagrama de Paquetes del Aplicativo Movil



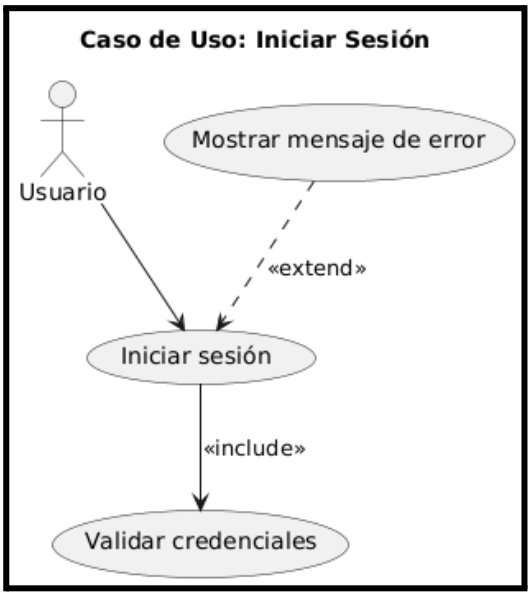
Fuente: Elaboración propia del equipo de trabajo

En el gráfico 06: En el Diagrama de Paquetes nos permite visualizar la organización y disposición de los diversos elementos del proyecto ,las dependencias de los paquetes en base a los requerimientos definidos de nuestro proyecto.

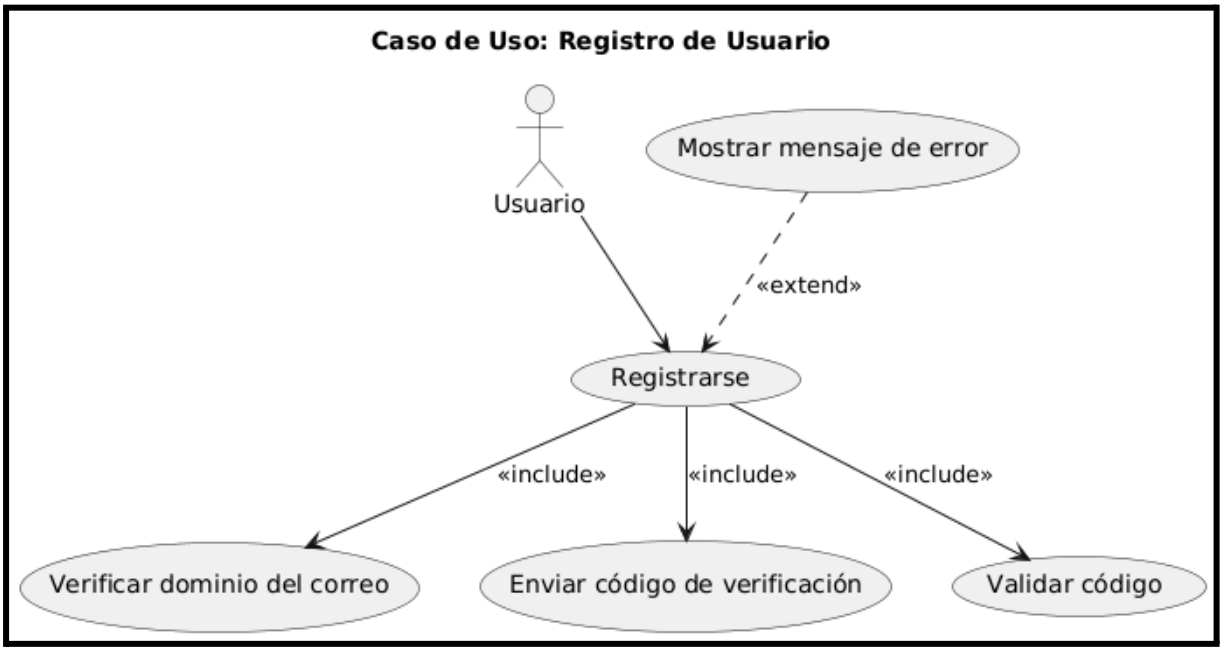
b. Diagrama de Casos de Uso

RF-001: Autenticar con Correo Electrónico

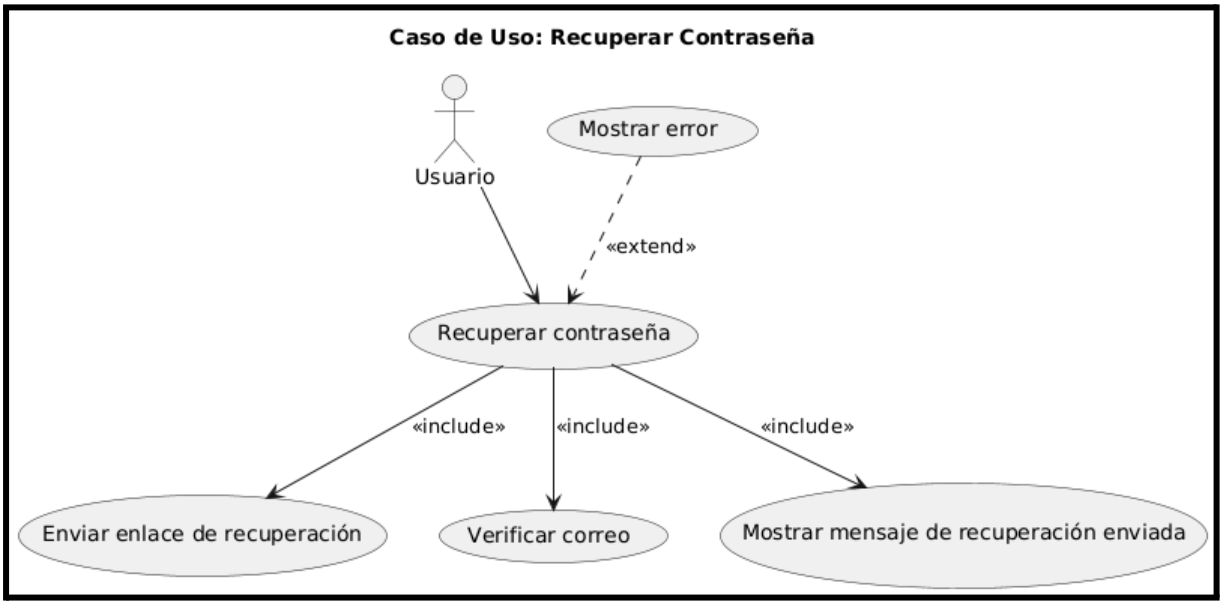
Gráfico 07:Diagrama de Caso de Usos Iniciar Sesión



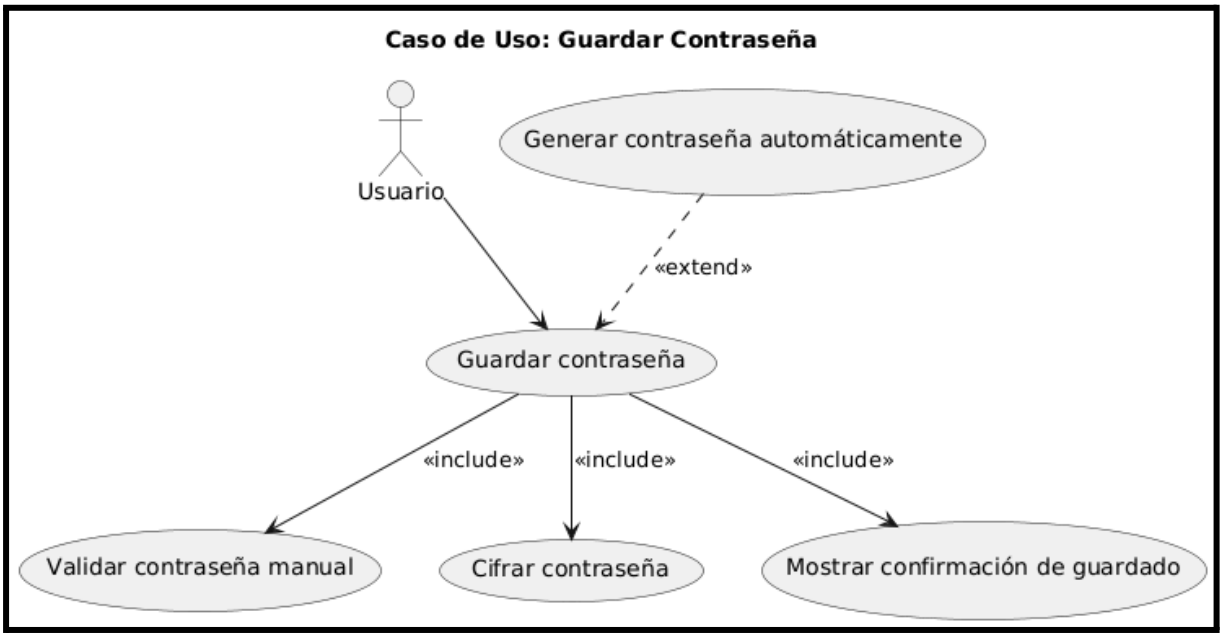
RF-002: Autenticar con Correo Electrónico



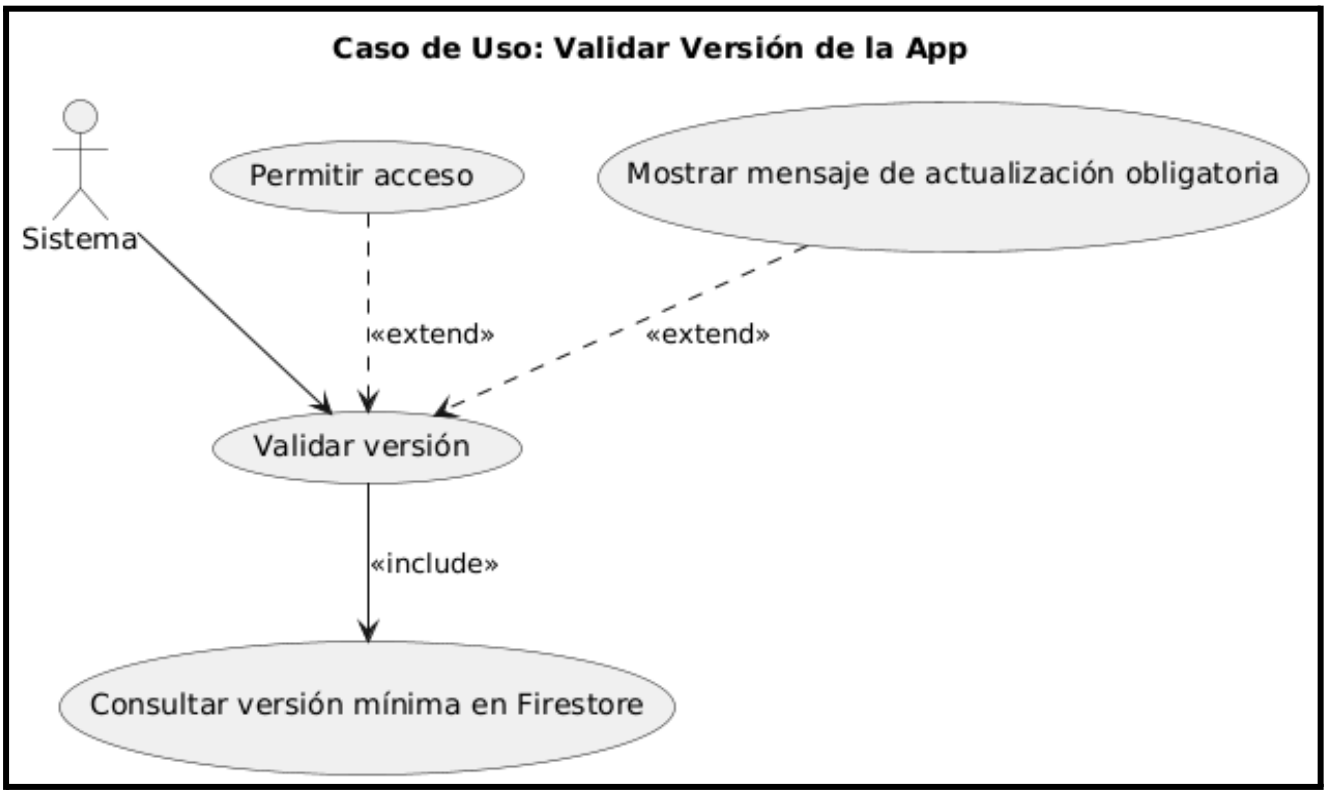
RF-001: Autenticar con Correo Electrónico - Recuperar Contraseña



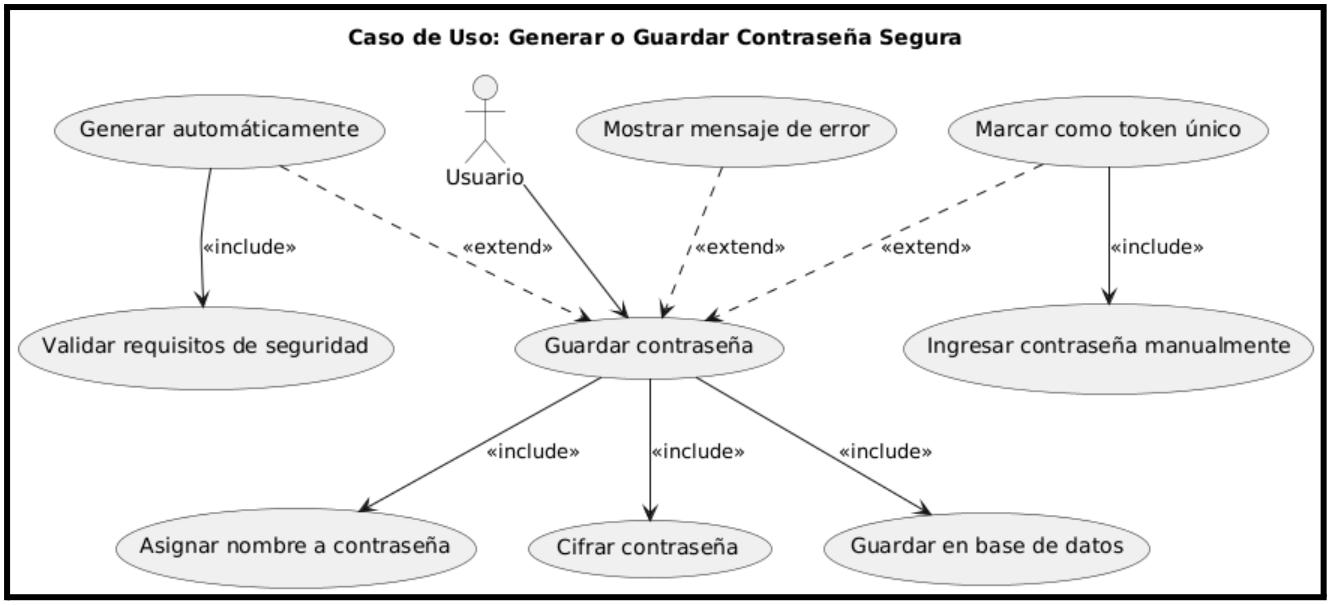
RF-002:Verificación con Correo- Guardar Contraseña



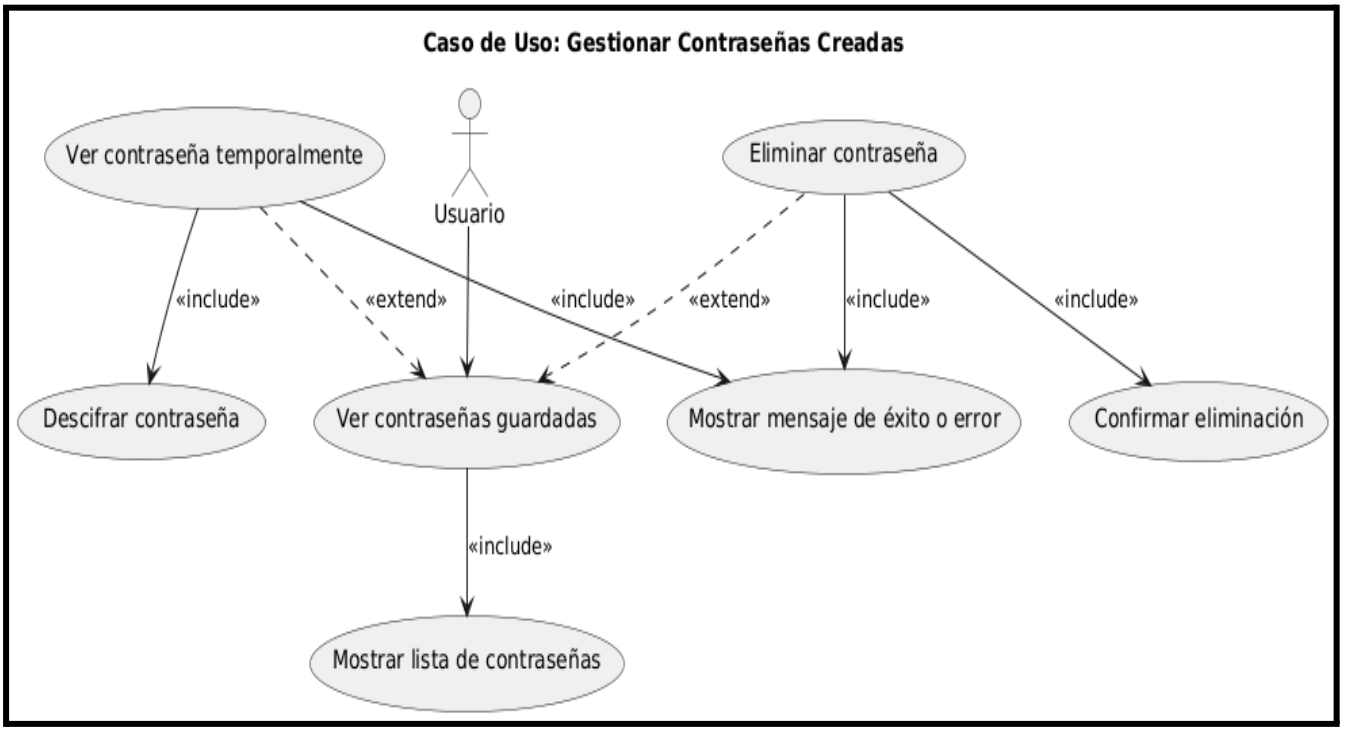
RF-002: Autenticar con Correo Electrónico - Validar Versión de la App



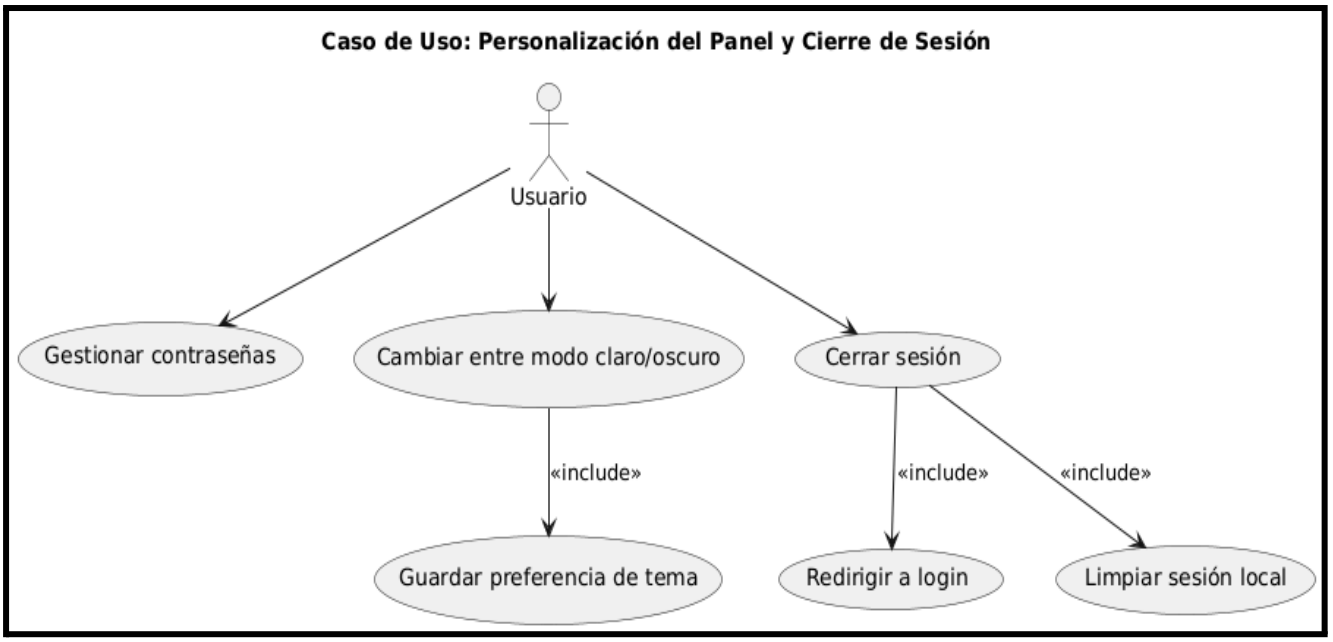
RF-004: Generación Automática de Claves - Generar o guardar Contraseña



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



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



c. Escenarios de Caso de Uso (Narrativa)

Caso de uso 01 - Autenticar Usuario

AUTENTICAR USUARIO	
Tipo	Obligatorio
Versión	3.0
Autores:	Edgard Reynaldo Chambe Torres Luigui Augusto Nina Vargas
Actores	Administrador
Descripción	El usuario ingresa al sistema mediante credenciales previamente registradas. El sistema valida los datos y redirige al dashboard correspondiente según su rol (Administrador con acceso completo o Empleado con funciones limitadas).
Precondiciones	1. El usuario debe estar registrado en la base de datos. 2. Las credenciales (usuario/contraseña) deben ser válidas.
NARRATIVA DE CASO DE USO	
Acción del Actor	**Respuesta del Sistema**
1. El usuario accede a la pantalla de login.	**2.** El sistema muestra una interfaz limpia con un fondo blanco con un login centrado y abajo de ello una imagen de un usuario,abajo de ello: - Un formulario centrado con las Etiquetas: ➢ Nombre de Usuario ➢ Contraseña Debajo de las dos etiquetas ,un campo de texto para cada uno de ellas y dentro un mensaje de referencia a colocar: ➢ “Introduce tu nombre de usuario” ➢ “Ingresa tu contraseña” Y mostrará el botón abajo: ➢ Iniciar Sesión
3. Ingresa credenciales y presiona *"Iniciar Sesión"*.	**4.** Validar los datos en la base de datos.

	5. El sistema valida las credenciales y carga el panel principal del usuario: Se apreciara una pantalla limpia de fondo blanco ,arriba un mensaje “Sistema de Web Agua IOT**”** con una opción para minimizar el Menú de opciones desplegables del dashboard que tiene un logo arriba de las opciones y al otro lado derecho un logo de usuario con el nombre del Usuario Logueado. Debajo de ellos apreciamos el panel limpio color blanco con un mensaje de bienvenida dependiendo del rol de usuario,en el caso del Administrador verá : “**Bienvenido al Panel de Administrador** Has iniciado sesión como administrador. Dashboard del Administrador En el caso del Empleado verá : - Bienvenido al Panel de Empleado - Has iniciado sesión como empleado. En el menú de opciones al lado izquierdo de la pantalla: ➢ Según el Rol Administrador o Empleado ,podrá tener acceso a las funcionalidades del sistema). En el caso del Rol Administrador tendrá Acceso al Menú de opciones en el dashboard: ➢ Inicio ➢ Grabar Lecturas ➢ Gestion Canales ➢ Gestión de Sensores ➢ Gestionar Usuarios ➢ Gestionar Canales ➢ Generar Reporte ➢ Cerrar Sesión

	En el caso del Rol Empleado tendrá Acceso a los botones: ➢ Inicio ➢ Grabar Lecturas ➢ Generar Reporte ➢ Cerrar Sesión
6. El usuario visualiza el dashboard principal a utilizar.	
Flujo de Excepciones	
1. El usuario ingresa incorrectamente su "Nombre de usuario" "Contraseña" o solo ingresa su usuario o viceversa, y presiona"Iniciar Sesión".	**2.** El sistema valida y detecta los datos incorrectos o faltantes.
	3. El sistema muestra un mensaje de error: "Error: El correo o la contraseña son incorrectos" y solicita al usuario que intente nuevamente.
4. El usuario deja un campo vacío y presiona Iniciar Sesión.	5. El sistema muestra un mensaje de error: "Por favor, complete todos los campos".

Fuente: Elaboración propia del equipo de trabajo

En la Tabla Nº 06 tenemos la especificación del caso de uso de autentificar usuario donde se describe detalladamente los pasos desde que el usuario ingresa a la página de sesión hasta que sus datos sean validados por el sistema y finalmente se les muestre la interfaz correspondiente a sus datos.

Caso de Uso 02 – Gestionar Usuario

GESTIÓN USUARIOS	
Tipo:	Obligatorio
Versión:	3.0
Autores:	Edgard Reynaldo Chambe Torres Luigui Augusto Nina Vargas
Actores:	Administrador
Descripción:	De acuerdo al tipo de usuario se obtendrá el control de acceso de los usuarios del sistema.El sistema proporcionará herramientas para la administración de usuarios, permitiendo la creación, actualización y gestión de roles de usuario. Los administradores podrán agregar nuevos usuarios al sistema, actualizar la información de los usuarios existentes y modificar sus roles y permisos según las necesidades organizativas. Asimismo, podrán gestionar el estado de las cuentas, asegurando que solo los usuarios activos tengan acceso a la plataforma.
Precondiciones:	El Administrador debe autenticarse para usar el sistema
Postcondiciones:	Los cambios realizados en los usuarios (adición, actualización) se reflejan en la base de datos y el listado de usuarios se actualiza automáticamente.
NARRATIVA DE CASO DE USO	
REGISTRAR USUARIO	
Acción del Actor	**Respuesta del sistema**
1. El administrador ingresa al Panel principal del sistema una vez autenticado.	2. El sistema valida la credencial y carga el panel principal del Administrador: ➢ Se apreciará una pantalla limpia de fondo blanco ,arriba un mensaje “Sistema de Web Agua IOT” con una opción para minimizar el Menú de opciones del panel que tiene un logo arriba de las opciones y al otro lado derecho un logo de usuario con el nombre del Usuario Logueado. ➢ Debajo de ellos apreciamos el panel limpio color blanco con un mensaje de bienvenida dependiendo del rol de usuario,en este caso el Administrador verá :

	"**Bienvenido al Panel de Administrador** Has iniciado sesión como administrador. Dashboard del Administrador ➢ En el menú de opciones al lado izquierdo de la pantalla: El Rol Administrador tendrá Acceso al Menú de opciones en el panel: ➢ Inicio ➢ Grabar Lecturas ➢ Gestion Canales ➢ Gestión de Sensores ➢ Gestionar Usuarios ➢ Gestionar Canales ➢ Generar Reporte ➢ Cerrar Sesión
3. El administrador seleccionará el botón "Gestionar Usuarios".	4. El sistema le mostrará un listado a través de una tabla de los usuarios registrados en el sistema web con la información en cada columna a mostrar: ➢ IdUsuario ➢ Nombre ➢ Apellido ➢ DNI ➢ Correo ➢ Nombre de Usuario ➢ Rol(Administrador/Empleado) ➢ Estado(Activo/Inactivo) ➢ Acciones: ● Botón "Editar" ➢ Un texto arriba de la tabla de usuarios registrados "Lista de Usuarios" y debajo de la tabla del listado: ● Un botón "Registrar Usuario" Una barra de Búsqueda (arriba del listado de la tabla) y su botón "Buscar".

5. El administrador Selecciona el botón “Registrar Usuario”.	6. El sistema muestra el formulario de registro con un texto al inicio “Registrar Nuevo Usuario” y con los campos de texto a completar : ● Nombre ● Apellido ● DNI ● Nombre Usuario ● Correo ● Contraseña ● Rol(Seleccionar Rol “Empleado ,Administrador) ● Estado (Activo/Inactivo) Además dos botones debajo del formulario: ● Registrar ● Cancelar
7. El administrador llena todos los campos del formulario y hace clic en el botón : Registrar.	8. El sistema valida los campos ingresados y registra los datos por el Administrador, direccionando a la lista de usuarios actualizada con el nuevo registro.
9. El administrador visualizará el listado del nuevo usuario agregado.	
BUSCAR USUARIO	
10. El administrador seleccionará el botón Gestionar Usuarios.	11. El sistema le mostrará un listado a través de una tabla de los usuarios registrados en el sistema web con la información en cada columna a mostrar: ➢ IdUsuario ➢ Nombre ➢ Apellido ➢ DNI ➢ Correo ➢ Nombre de Usuario ➢ Rol(Administrador/Empleado) ➢ Estado(Activo/Inactivo) ➢ Acciones: ● Botón “Editar” ➢ Un texto arriba de la tabla de usuarios registrados “Lista de Usuarios” y debajo del texto: ● Un botón “Registrar Usuario”

	Una barra de Búsqueda (arriba del listado de la tabla) y su botón “Buscar”.
12. El usuario ingresará el nombre de usuario o rol en la barra de búsqueda y hará clic en “Buscar”	13. El sistema mostrará los usuarios que coincidan con la búsqueda ingresada.
14. El administrador verá el usuario buscado en el listado.	
EDITAR USUARIO	
15. El Administrador dará clic sobre el usuario en el listado de los usuarios y luego dará clic en el botón “Editar”,ubicado en la columna de Acciones.	16. El sistema muestra los campos del formulario llenos con los datos del usuario seleccionado y un mensaje arriba “Editar Usuario”: ➢ Nombre ➢ Apellido ➢ DNI ➢ Nombre Usuario ➢ Correo ➢ Contraseña ➢ Rol(Seleccionar Rol “Empleado ,Administrador) ➢ Estado (Activo/Inactivo) Además dos botones debajo del formulario: ● Guardar Cambios ● Cancelar
17. El Administrador modifica algún campo del formulario y hace clic en el botón : “Guardar Cambios”.	18. El sistema valida los campos y actualiza los datos ingresados del usuario seleccionado.
	19. El sistema actualizará la lista de los usuarios con el nuevo cambio y le direccionará al Administrador al listado de usuarios.
20. El Administrador visualizará el listado actualizado con el usuario modificado.	
FLUJO DE EXCEPCIONES	
21. Si el administrador intenta registrar un usuario con un DNI o nombre de usuario que ya existe.	22. El sistema mostrará un mensaje de error indicando que el dato debe ser único.

23. Si el administrador no completa todos los campos requeridos al intentar registrar o actualizar un usuario.	24. El sistema mostrará un mensaje de error pidiendo que se completen los campos obligatorios.

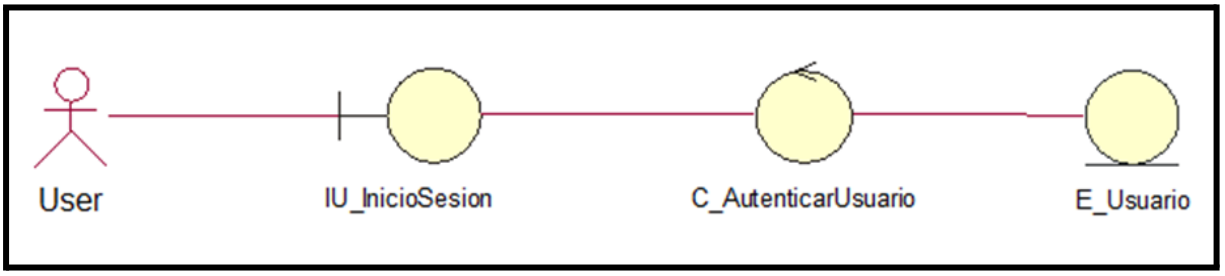
Fuente: Elaboración propia del equipo de trabajo

En la Tabla Nº 07 tenemos la especificación del caso de uso de Gestion Usuarios ,donde el Administrador será el encargado de poder registrar ,rol de usuario,etc. y sus respectivos flujos de excepciones.

1. Modelo Lógico

a. Análisis de Objetos

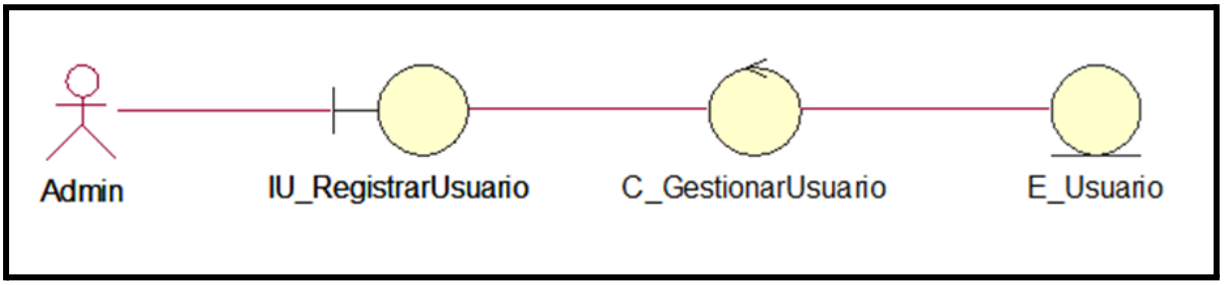
Gráfico 14 – Diagrama de Analisis de Objetos - Autenticar Usuario



Fuente: Elaboración propia del equipo de trabajo

En la gráfica Nº 14 : Diagrama de análisis de Objetos de Autenticar Usuario,apreciamos la IU,objeto Control y la Entidad Usuario.

Gráfico 15 – Diagrama de Analisis de Objetos -Registrar Usuario



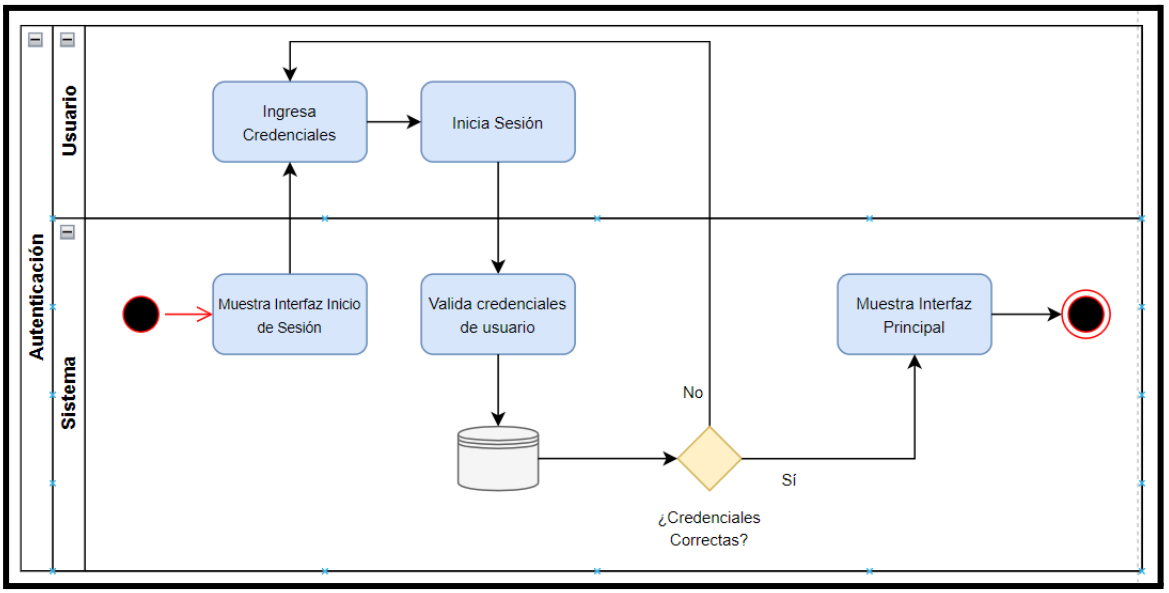
Fuente: Elaboración propia del equipo de trabajo

En la gráfica Nº 15 : Diagrama de análisis de Objetos de Registrar Usuario ,apreciamos al actor Admin,la IU,objeto Control GestionarUsuario y la Entidad Usuario.

b. Diagrama de Actividades con objetos

1. Diagrama de Actividades - Autenticar Usuario

Gráfico 20 – Diagrama de Actividades - Autenticar Usuario

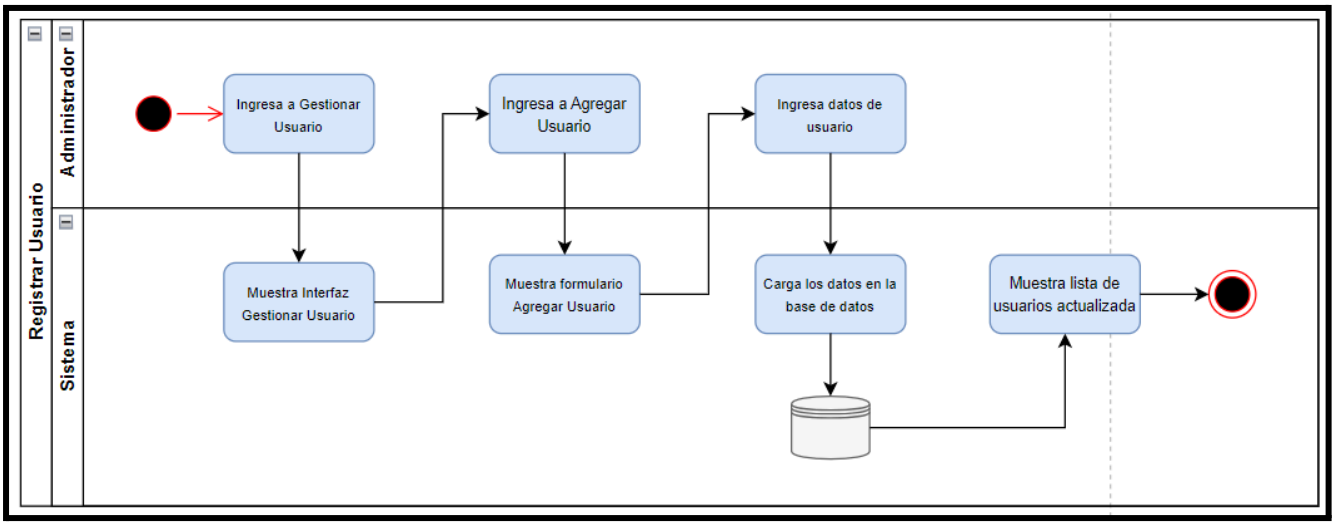


Fuente: Elaboración propia del equipo de trabajo

En el gráfico 20 :Apreciamos el diagrama de actividades del caso de uso Autenticar Usuario,desde el inicio de la muestra de la interfaz del inicio de sesión hasta mostrar la Interfaz Principal.

2. Diagrama de Actividades - Registrar Usuario

Gráfico 21 – Diagrama de Actividades - Registrar Usuario



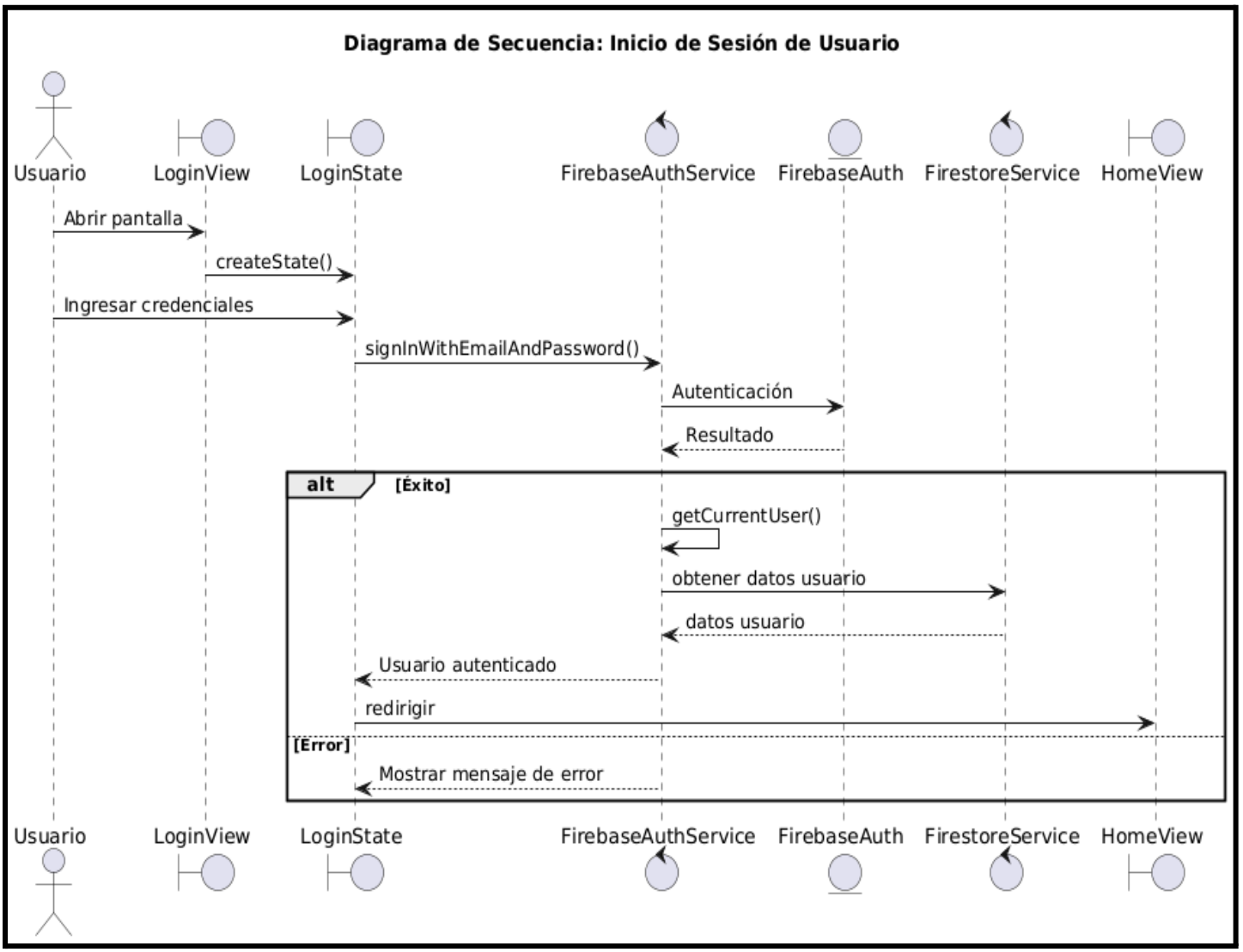
Fuente: Elaboración propia del equipo de trabajo

En el gráfico 21 :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.

C. Diagrama de Secuencia

1.1 Diagrama de Secuencia – Casos de Uso – Autenticar Usuario

Gráfico 37 : Diagrama de Casos de Uso - Inicio de Sesión de Usuario



1.2 Diagrama de Secuencia – Casos de Uso – Registro de Nuevo Usuario

Gráfico 38:Diagrama de Secuencia - Registro de Nuevo Usuario

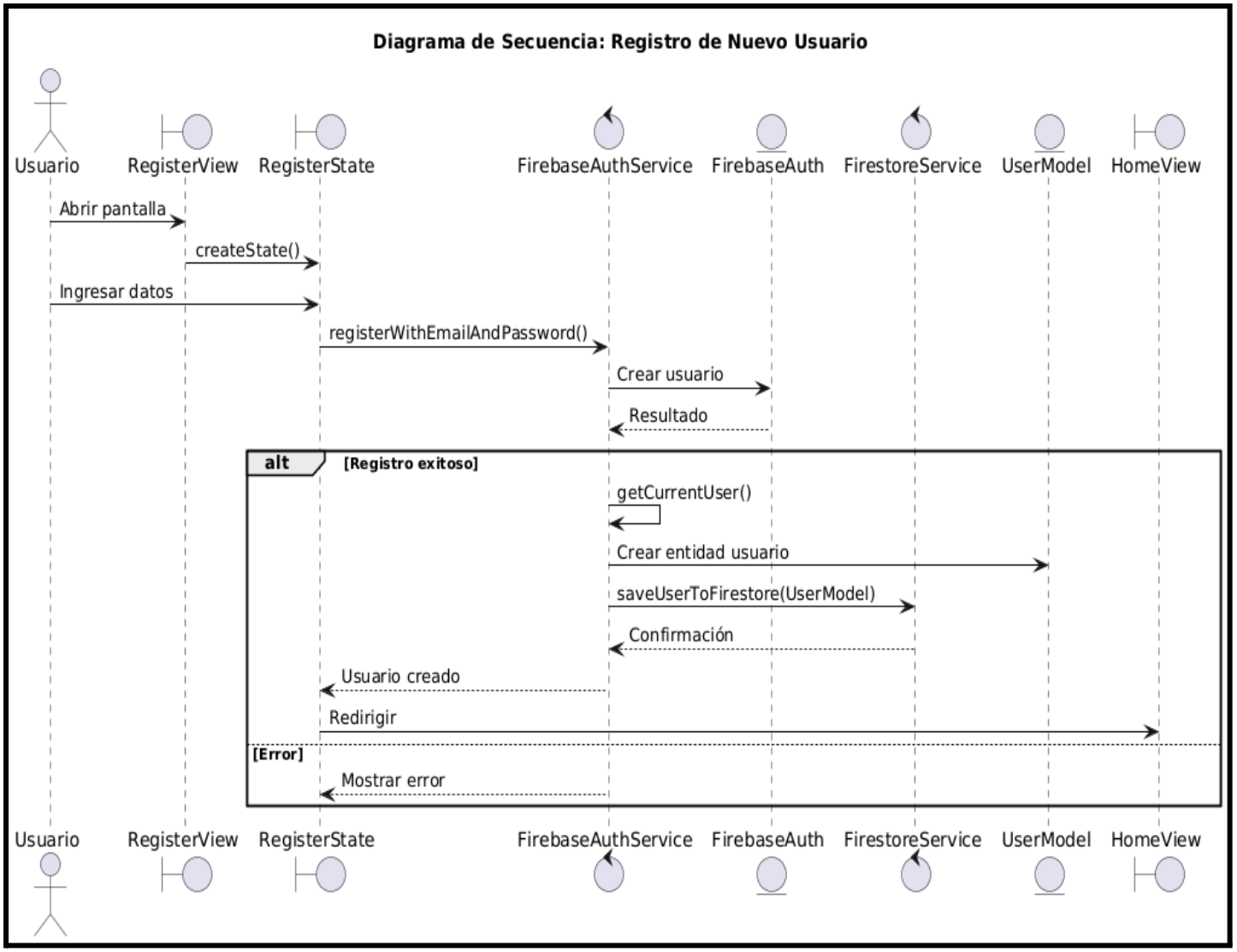


Gráfico 39 :Diagrama de Secuencia - Recuperación de Contraseña

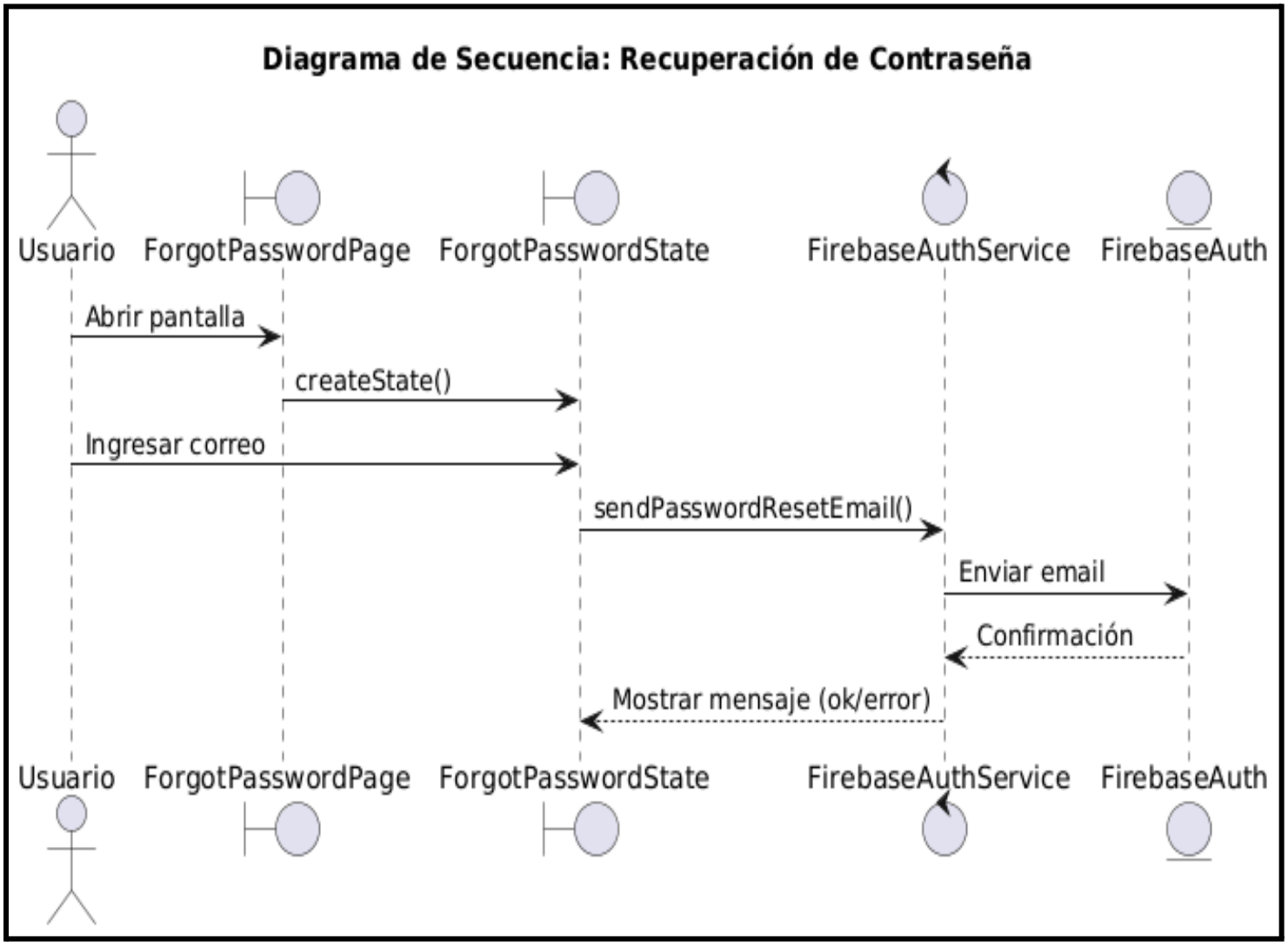
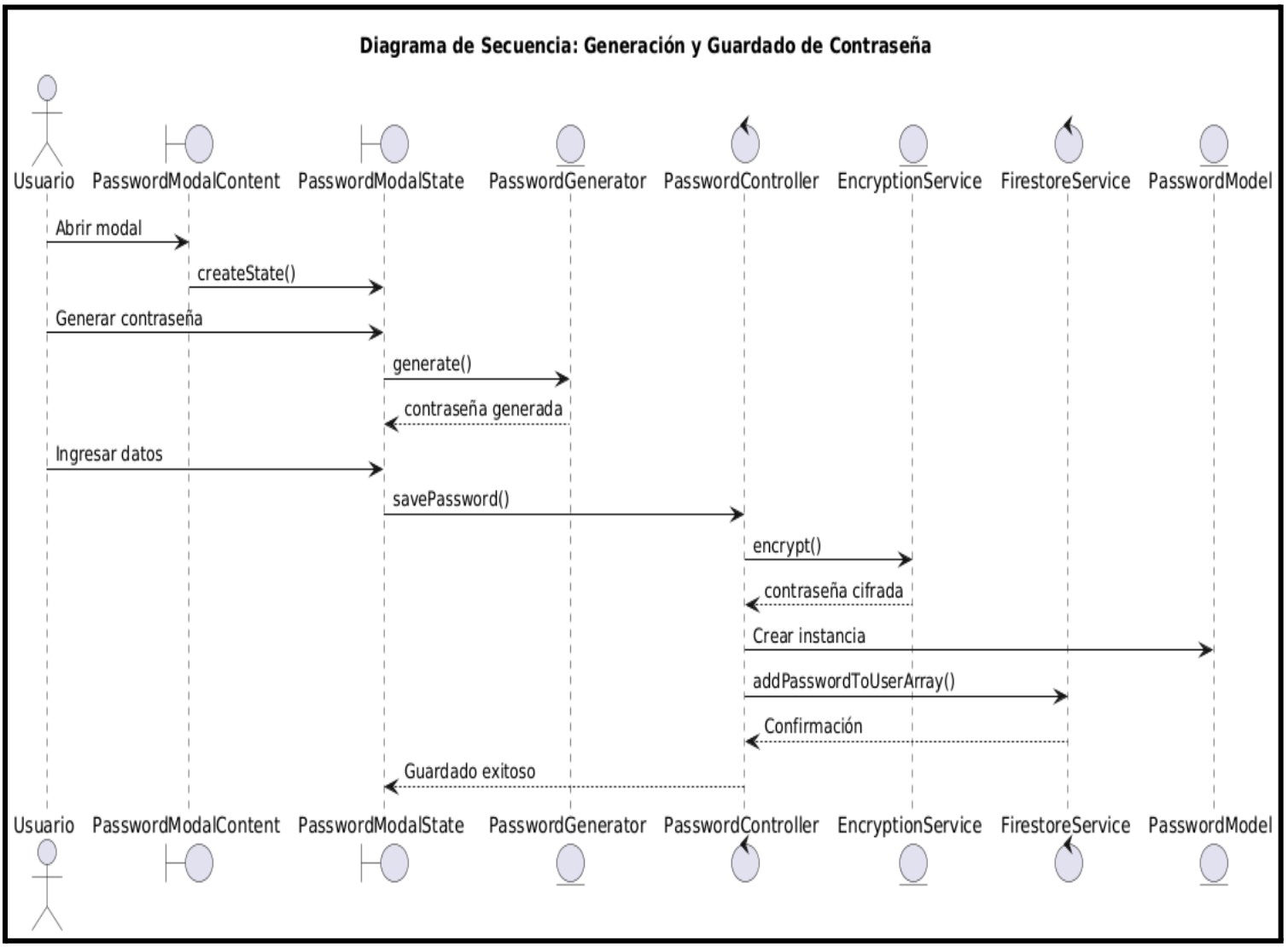
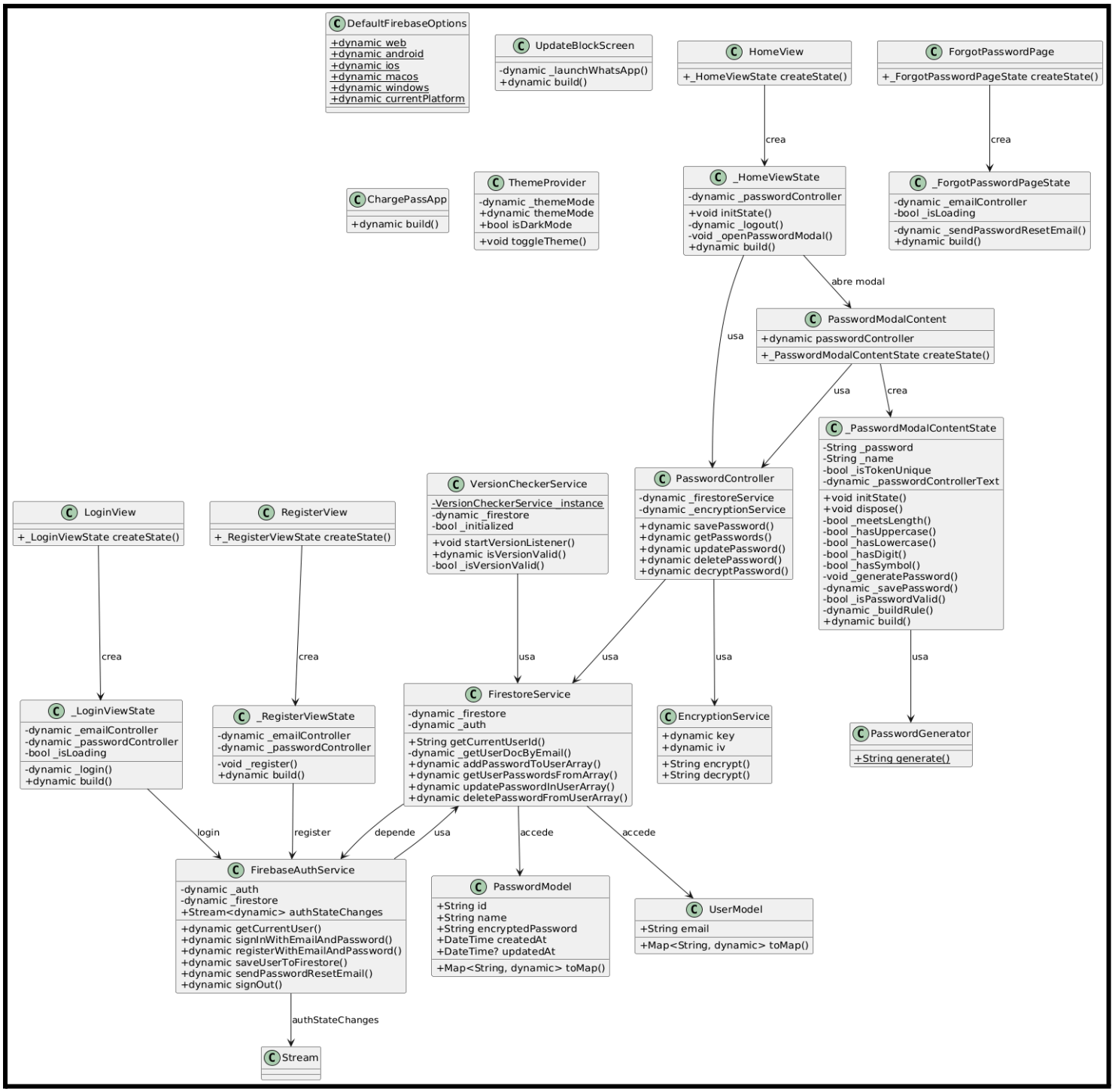


Gráfico 40:Diagrama de Casos de Uso - Gestionar Usuario - Buscar



d. Diagrama de Clases

Gráfico 57:Diagrama de Clases del Proyecto



CONCLUSIONES

- El uso de la documentación FD03-SRS nos proporciona un marco de trabajo para poder diseñar y analizar a través de procesos y narrativas y así obtener un óptimo desarrollo de nuestro proyecto.

- La implementación de un aplicativo móvil basado en firebase y flutter optimizará la gestión de la seguridad en la gestión de contraseñas seguras optimizando la recolección y análisis de datos.

- La automatización del monitoreo y la eliminación de métodos manuales contribuirán a una significativa reducción de costos operativos y a una mejor asignación de recursos.

- Los análisis de viabilidad económica indican que el proyecto es financieramente sólido, con un VAN positivo, alta TIR y un atractivo Índice de Rentabilidad.

- La arquitectura basada en la aplicación móvil y la interfaz amigable facilitarán la adopción del sistema, minimizando la curva de aprendizaje para los operadores.

- Los nuevos cambios implementados en base a los nuevos requerimientos enriquecerán a las mejoras del proyecto y tener una base sólida a implementar.