

**UNIVERSIDAD TÉCNICA FEDERICO SANTA
MARÍA
VIÑA DEL MAR - CHILE**



**“DISEÑO Y PROTOTIPADO DE SISTEMA
DE ACCESO RESIDENCIAL
INTELIGENTE”**

BENJAMÍN BETTY DÍAZ

**PROFESOR GUÍA: GABRIEL JARA
PROFESOR CORREFERENTE: PATRICIO SANTANDER**

2025



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo: Diseño y prototipado de sistema de accesos residencial inteligente

Nombre del candidato(a): Benjamín Renato Betty Díaz

Carrera / Grado: Ingeniería en Informática

Campus: Viña del Mar **Departamento:** Electrotecnia e Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Gabriel Jara Bulnes, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

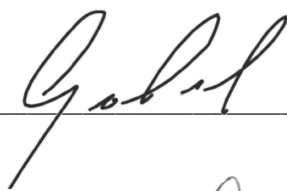
☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

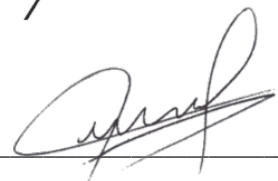
Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 03-08-2026 **Firma:** 

Estudiante o Candidato(a):

Fecha: 03/08/2026 **Firma:** 

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

DEDICATORIA

A mis padres, por su sacrificio para que yo cumpliera mis metas, pueda estudiar y completar mi carrera. A mis familiares y amigos por su apoyo y entregarme la fuerza para salir adelante en momentos difíciles. Y, por último, a mis compañeros que conocí durante estos años, que me brindaron ayuda constante para seguir fortaleciendo mis conocimientos.

RESUMEN

Resumen—El presente trabajo de título aborda la problemática de la inseguridad y la ineficiencia operativa en los controles de acceso residencial, un punto crítico donde convergen la vulnerabilidad ante delitos violentos y la gestión manual obsoleta. El objetivo principal fue diseñar y desarrollar un sistema móvil inteligente que automatice la validación de identidad sin requerir costosa infraestructura hardware industrial.

Para lograrlo, se implementó una arquitectura híbrida utilizando el framework Flutter para el desarrollo de una aplicación multiplataforma, integrada con servicios en la nube (*Firebase*) para la gestión de datos en tiempo real. La solución incorpora tecnologías de Inteligencia Artificial, específicamente Google ML Kit para el reconocimiento de patentes vehiculares (LPR) *on-device* y AWS Rekognition para la verificación biométrica facial en la nube.

La relevancia de este proyecto radica en la democratización de la seguridad avanzada, ofreciendo una herramienta accesible y escalable capaz de mitigar riesgos y modernizar la gestión comunitaria.

Palabras Clave—Control de Acceso; Biometría Facial; Reconocimiento de Patentes (LPR); Seguridad Residencial; Aplicación Móvil.

ABSTRACT

Abstract—This thesis addresses the issues of insecurity and operational inefficiency in residential access controls, a critical point converging vulnerability to violent crimes and obsolete manual management. The main objective was to design and develop an intelligent mobile system that automates identity validation without requiring expensive industrial hardware infrastructure.

To achieve this, a hybrid architecture was implemented using the Flutter framework for cross-platform application development, integrated with cloud services (Firebase) for real-time data management. The solution incorporates Artificial Intelligence technologies, specifically Google ML Kit for on-device License Plate Recognition (LPR) and AWS Rekognition for cloud-based facial biometric verification.

The relevance of this project lies in the democratization of advanced security, offering an accessible and scalable tool capable of mitigating risks and modernizing community management.

Keywords—Access Control; Facial Biometrics; License Plate Recognition (LPR); Residential Security; Mobile Application.

GLOSARIO

Android: Sistema operativo móvil basado en el núcleo Linux y otro software de código abierto, diseñado principalmente para dispositivos móviles con pantalla táctil como teléfonos inteligentes y tabletas.

API (Application Programming Interface): Conjunto de definiciones y protocolos que permite que dos aplicaciones de software se comuniquen entre sí.

Autenticación: Proceso de verificar la identidad de un usuario, dispositivo o sistema.

AWS (Amazon Web Services): Plataforma de servicios de computación en la nube ofrecido por Amazon, que proporciona potencia de cómputo, almacenamiento de bases de datos y entrega de contenidos.

BaaS (Backend-as-a-Service): Modelo de servicio en la nube que permite a los desarrolladores externalizar la gestión de la infraestructura del lado del servidor (backend), como bases de datos y autenticación.

Biometría Facial: Tecnología que utiliza características físicas únicas del rostro humano (patrones faciales) para identificar o verificar la identidad de una persona de manera digital.

Bitácora Digital: Registro electrónica, cronológico e inmutable de los eventos ocurridos en el sistema, que sustituye al libro de actas físico y permite la trazabilidad y auditoría de los accesos.

Cloud Computing (Computación en la Nube): Disponibilidad bajo demanda de recursos del sistema informático, especialmente almacenamiento de datos y capacidad de cómputo, sin una gestión activa directa por parte del usuario.

Cloud Functions: Funcionalidad de *serverless* (sin servidor) que permite ejecutar código de backend automáticamente en respuesta a eventos activados por funciones de Firebase y solicitudes HTTPS.

Dart: Lenguaje de programación optimizado para clientes, desarrollado por Google, que se utiliza para escribir aplicaciones móviles, de escritorio, backend y web. Es el lenguaje base del framework Flutter.

Deep Learning (Aprendizaje Profundo): Subconjunto del aprendizaje automático (Machine Learning) estructurado como redes neuronales artificiales, utilizado por AWS Rekognition para analizar imágenes con alta precisión.

Edge Computing (Computación en el Borde): Paradigma de computación distribuida que acerca el cálculo y el almacenamiento de datos a la ubicación donde se necesitan, para mejorar los tiempos de respuesta. El uso de LPR en el dispositivo móvil (*on-device*) es un ejemplo de esto.

ENUSC (Encuesta Nacional Urbana de Seguridad Ciudadana): Instrumento estadístico oficial en Chile utilizado para medir la victimización y la percepción de inseguridad en la población.

FCM (Firebase Cloud Messaging): Solución de mensajería multiplataforma que permite enviar mensajes y notificaciones de forma gratuita y segura a dispositivos iOS, Android y web.

Firebase: Plataforma de desarrollo de aplicaciones móviles y web de Google que proporciona herramientas y servicios para ayudar a los desarrolladores a crear, mejorar y escalar sus aplicaciones.

Firestore: Base de datos NoSQL flexible, escalable y en la nube de Firebase, utilizada para almacenar y sincronizar datos en tiempo real entre los usuarios de la aplicación.

Flutter: Framework de código abierto creado por Google para desarrollar aplicaciones nativas compiladas multi-plataforma (Android, iOS, Web) a partir de una única base de código.

Frontend: Parte de un sistema de software que interactúa directamente con el usuario (la interfaz gráfica de la aplicación móvil).

Integridad de Datos: Garantía de que la información registrada es exacta, completa y no ha sido alterada sin autorización.

iOS: Sistema operativo móvil creado y desarrollado por Apple Inc. exclusivamente para su hardware (iPhone, iPad).

IoT (Internet of Things / Internet de las Cosas): Red de objetos físicos ("cosas") que llevan incorporados sensores, software y otras tecnologías con el fin de conectar e intercambiar datos con otros dispositivos y sistemas a través de Internet.

JSON (JavaScript Object Notation): Formato ligero de intercambio de datos, fácil de leer y escribir para los humanos y fácil de analizar y generar para las máquinas.

JWT (JSON Web Token): Estándar abierto que define una forma compacta y autónoma de transmitir información de forma segura entre partes como un objeto JSON, utilizado comúnmente para la autenticación de usuarios.

Latencia: Tiempo que tarda un paquete de datos en viajar desde un punto de origen hasta un punto de destino.

LPR (License Plate Recognition): Tecnología de reconocimiento de matrículas vehiculares que utiliza reconocimiento óptico de caracteres (OCR) para leer automáticamente los números de registro de los vehículos.

Machine Learning (Aprendizaje Automático): Rama de la inteligencia artificial que permite que las máquinas aprendan de los datos y mejoren su rendimiento sin ser programadas explícitamente para cada tarea.

Material Design 3: Sistema de diseño de código abierto de Google que proporciona pautas, componentes y herramientas para crear interfaces de usuario intuitivas y estéticas.

Multi-tenant (Multi-inquilino): Arquitectura de software en la que una sola instancia de software sirve a múltiples clientes o "inquilinos" (en este caso, múltiples condominios), garantizando el aislamiento de datos entre ellos.

NoSQL (Not Only SQL): Categoría de sistemas de gestión de bases de datos que no utilizan el modelo relacional tabular tradicional, permitiendo mayor flexibilidad en la estructura de los datos.

OCR (Optical Character Recognition): Tecnología que permite convertir diferentes tipos de documentos, como imágenes escaneadas o fotos, en datos de texto editables y buscables.

On-Device: Procesamiento de datos que ocurre directamente en el dispositivo del usuario (smartphone) en lugar de enviarse a un servidor externo, mejorando la velocidad y privacidad.

Push Notification (Notificación Push): Mensaje que se envía desde un servidor a una aplicación instalada en un dispositivo móvil, apareciendo en la pantalla del usuario incluso si la aplicación no está abierta.

QR (Quick Response Code): Código de barras bidimensional capaz de almacenar datos codificados. Se utiliza en el proyecto para generar pases de visita encriptados.

SaaS (Software as a Service): Modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de TIC y se accede a ellos vía Internet.

SDK (Software Development Kit): Conjunto de herramientas de desarrollo de software que permite a los programadores crear aplicaciones para un sistema concreto.

Serverless: Modelo de ejecución en la nube en el que el proveedor de la nube gestiona dinámicamente la asignación de recursos del servidor, cobrando solo por el tiempo de cómputo real consumido.

Smartphone: Teléfono móvil con capacidades avanzadas de computación y conectividad, que sirve como la plataforma de hardware principal para la solución propuesta.

TLS (Transport Layer Security): Protocolo criptográfico diseñado para proporcionar seguridad en las comunicaciones a través de una red informática.

UI (User Interface / Interfaz de Usuario): El medio por el cual el usuario y un sistema informático interactúan, en particular el uso de dispositivos de entrada y software.

UX (User Experience / Experiencia de Usuario): Conjunto de factores y elementos relativos a la interacción del usuario con un entorno o dispositivo concretos, cuyo resultado es la generación de una percepción positiva o negativa del servicio.

Índice

ÍNDICE DE FIGURAS	12
ÍNDICE DE TABLAS.....	14
INTRODUCCIÓN	15
CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA.....	16
1.1 Contexto	16
1.2 Descripción de la problemática	18
1.2.1 Análisis de los Actores Involucrados.....	18
1.3 Propuesta de Solución	19
1.4 Objetivos	20
1.4.1 Objetivo General	20
1.4.2 Objetivos Específicos	20
1.5 Justificación	21
1.6 Alcances y Limitaciones	22
CAPÍTULO 2: MARCO CONCEPTUAL.....	23
2.1 Metodología de Desarrollo	23
2.1.1 Metodología Ágil e Incremental	23
2.2 Fundamentos de Seguridad y Control de Acceso	24
2.2.1 Control de Acceso Físico vs Lógico	24
2.2.2 Autenticación de Identidad	24
2.3 Tecnologías de Verificación Avanzada	25
2.3.1 Biometría Facial (Reconocimiento Facial)	25
2.3.2 Reconocimiento Óptico de Caracteres (OCR) y LPR	25
2.4 Arquitectura y Herramientas de Desarrollo	27
2.4.1 Flutter (Desarrollo Móvil)	27
2.4.2 Firebase (Backend-as-a-Service)	27
2.4.3 Servicios de Inteligencia Artificial en la Nube (AWS).....	28

2.5	Marco Legal y Normativo	29
2.5.1	Protección de Datos Personales (Ley N° 19.628)	29
2.5.2	Nueva Ley de Copropiedad Inmobiliaria (Ley N° 21.442)	29
2.5.3	Normativa de Seguridad Privada (OS10 de Carabineros)	29
CAPÍTULO 3: PROPUESTA DE SOLUCIÓN		30
3.1	Modelado y Arquitectura del Sistema	30
3.1.1	Diagramas de Caso de Uso	30
3.1.2	Proceso de Gestión de identidad y Enrolamiento	33
3.1.3	Diagramas de Flujo Operativos	39
3.2	Modelo de Datos (Diseño de Base de Datos)	50
3.2.1	Modelo Conceptual Relacional	50
3.3	Diseño de la Interfaz de Usuario (UI)	58
3.3.1	Vistas por Rol de Usuario	58
3.4	Modelo de Seguridad y Privacidad de Datos	73
3.4.1	Autenticación y Control de Acceso	73
3.4.2	Seguridad en la Base de Datos	73
3.4.3	Protección de Datos Sensibles y Biometría	74
CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN		75
4.1	Validación Funcional (Matriz de Pruebas)	75
4.1.1	Análisis de Resultado de las Pruebas Funcionales	76
4.2	Validación Comparativa: Eficiencia Operativa	77
4.2.1	Metodología de la Prueba	77
4.2.2	Resultados Cuantitativos	78
4.2.3	Análisis de Resultados	79
4.2.4	Conclusión de la Validación Operativa	79
4.3	Validación de Usabilidad (Experiencia de Usuario)	80
4.3.1	Metodología y Participantes	80

4.3.2	Cálculo y Resultados del Cuestionario SUS.....	81
4.3.3	Análisis e Interpretación de Resultados.....	82
CAPÍTULO 5: CONCLUSIONES		84
REFERENCIAS BIBLIOGRAFICAS		86
ANEXO		87

ÍNDICE DE FIGURAS

Figura 1: Resultados ENUSC 2024 Fuente:	16
Figura 2: Servicio de análisis de imágenes y video Amazon Rekognition.	25
Figura 3: Librería de aprendizaje automático en el dispositivo Google ML Kit	26
Figura 4: Logotipo del framework de desarrollo multiplataforma Flutter.	27
Figura 5: Plataforma de desarrollo de aplicaciones Google Firebase.....	28
Figura 6: Ecosistema de servicios de computación en la nube de Amazon Web Services.	28
Figura 7: Diagrama de Casos de Uso del Administrador	31
Figura 8: Diagrama de Casos de Uso del Guardia.....	32
Figura 9: Diagrama de Casos de Uso del Residente	33
Figura 10: Diagrama de Flujo Invitación a Residente como Administrador	34
Figura 11: Diagrama de Flujo Activación de cuenta del Residente	35
Figura 12: Diagrama de Flujo Invitación a Guardia como Administrador	36
Figura 13: Diagrama de Flujo Activación Cuenta de Guardia	38
Figura 14: Diagrama de Flujo Control de Acceso Vehicular	40
Figura 15: Diagrama de Flujo Control de Acceso Residente	42
Figura 16: Diagrama de Flujo de Generación código QR y Verificación	44
Figura 17: Diagrama de Flujo de Visita no Anunciada	46
Figura 18: Diagrama de Flujo Configuración Modular	48
Figura 19: Colección Condominios.....	50
Figura 20: Colección Administradores	51
Figura 21: Colección condo_types	51
Figura 22: Colección Guardias	52
Figura 23: Colección Residentes	53
Figura 24: Sub-Colección GrupoFamiliar	54
Figura 25: Sub-Colección Vehiculos	55
Figura 26: Colección Visitas	55

Figura 27: Colección notificaciones_visita.....	56
Figura 28: Colección Eventos.....	57
Figura 29: Vista de Inicio en la aplicación del Residente.	59
Figura 30: Vista para generar un pase de Visita en la interfaz del Residente.	60
Figura 31: Vista para visualizar las próximas visitas en la interfaz del Residente.....	61
Figura 32: Vista para agregar/eliminar mis vehículos como Residente	62
Figura 33: Vista de Cuenta en la interfaz del Residente.....	63
Figura 34: Vista de verificaciones en la interfaz del Guardia.	64
Figura 35: Vista de Bitácora Digital en la interfaz del Guardia	65
Figura 36: Vista para notificar Visita en la interfaz del Guardia.	66
Figura 37: Vista de cuenta en la interfaz del Guardia	67
Figura 38: Vista de Dashboard en la interfaz del Administrador	68
Figura 39: Vista para invitar y visualizar residente en la interfaz del Administrador.....	69
Figura 40: Vista para invitar, visualizar y eliminar guardias en la interfaz del Administrador	70
Figura 41: Vista de Bitácora Digital en la interfaz del Administrador	71
Figura 42: Vista de Cuenta y Configuración de módulos en la interfaz del Administrador	72
Figura 43: Servicio de autenticación y gestión de usuarios Firebase Authentication.....	73

ÍNDICE DE TABLAS

Tabla 1: Matriz de Pruebas Fuente: Elaboración Propia.....	75
Tabla 2: Comparación de pasos para el ingreso de visita (Manual vs Sistema QR) Fuente: Elaboración Propia.....	77
Tabla 3: Comparación de pasos para el ingreso visita (Manual vs Notificación en App) Fuente: Elaboración Propia.....	77
Tabla 4: Comparación de pasos ingreso vehicular (Manual vs App con LPR) Fuente: Elaboración Propia	78
Tabla 5: Comparativa de Tiempos de Operación (Manual vs App) Fuente: Elaboración Propia	78
Tabla 6: Tareas asignadas para encuesta SUS Fuente: Elaboración Propia.....	80
Tabla 7: Puntaje SUS Guardia Fuente: Elaboración Propia	81
Tabla 8: Puntaje SUS Residente Fuente: Elaboración Propia	82

INTRODUCCIÓN

En la última década, la seguridad ciudadana se ha posicionado como una de las principales preocupaciones en Chile, impulsada por un aumento en la percepción de inseguridad y la ocurrencia de delitos violentos en zonas residenciales. En este contexto, las comunidades habitacionales (edificios y condominios) dependen en gran medida de sus puntos de control de acceso para garantizar la seguridad de los residentes. Sin embargo, la gestión de estos accesos sigue basándose mayoritariamente en procesos manuales, libros de bitácora físicos y el criterio subjetivo del personal de seguridad, lo que genera vulnerabilidades, lentitud operativa y ausencia de datos para la toma de decisiones.

El presente trabajo tiene como propósito abordar esta problemática mediante el diseño y desarrollo de un sistema móvil inteligente, capaz de transformar un dispositivo *smartphone* estándar en una herramienta de validación de identidad avanzada. Aprovechando las capacidades de procesamiento local y servicios de computación en la nube, la solución automatiza la lectura de patentes vehiculares y la verificación biométrica facial de peatones, digitalizando integralmente el flujo de ingreso sin incurrir en los altos costos de infraestructura de seguridad tradicional.

Si bien el alcance de este proyecto se centra en la validación mediante tecnologías móviles disponibles y servicios *cloud*, el desarrollo se ha realizado bajo una arquitectura modular y escalable. Esto sienta las bases técnicas necesarias para que, en etapas futuras, el sistema pueda complementarse e integrarse con ecosistemas más complejos, incluyendo cámaras IP externos y dispositivos de IoT para la apertura automatizada de barreras.

CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA

1.1 Contexto

En el escenario actual de seguridad pública, la protección de los espacios residenciales se ha posicionado como una de las prioridades fundamentales para la ciudadanía. La percepción de inseguridad ha alcanzado niveles críticos; según la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) 2024, el 87,7% de la población percibe que la delincuencia en el país ha aumentado. Esta realidad, sumada al incremento de delitos violentos, ha obligado a las comunidades a reevaluar sus protocolos de control de acceso.

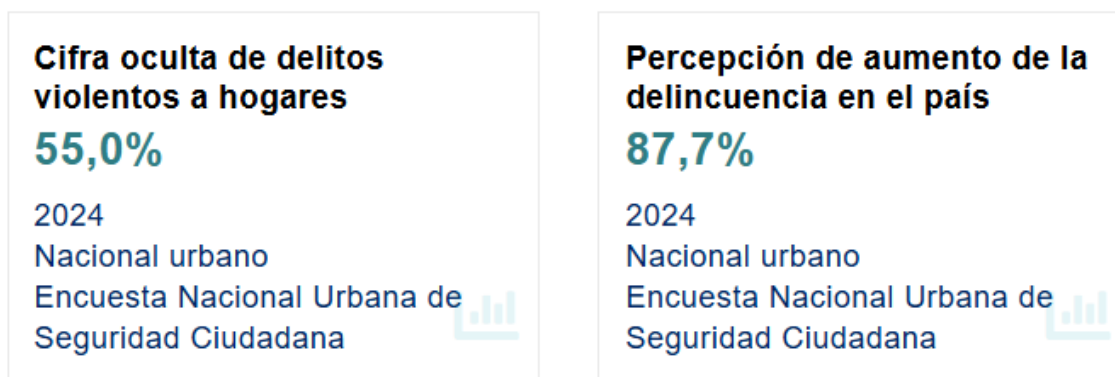


Figura 1: Resultados ENUSC 2024

Fuente: <https://www.ine.gob.cl/estadisticas/sociales/seguridad-publica-y-justicia/seguridad-ciudadana>

En este contexto, numerosos condominios, edificios y entornos residenciales que requieren de un conserje o guardia, enfrentan un problema tecnológico: mientras otros servicios cotidianos se han digitalizado completamente, el control de acceso sigue dependiendo, en su gran mayoría, de procesos manuales y herramientas obsoletas. El uso de llaves físicas, controles remotos universales no encriptados y el registro en libros de bitácoras constituye el estándar operativo.

Este modelo tradicional presenta vulnerabilidades estructurales significativas. La dependencia del criterio humano para la validación de identidad facilita la suplantación, mientras que el registro manual en papel conlleva errores de legibilidad, pérdida de datos y una nula capacidad de auditoría en tiempo real. Además, situaciones cotidianas como la llegada de visitas imprevistas o el ingreso vehicular en horas punta suelen generar congestión y demoras, afectando la calidad de vida de los residentes.

El presente trabajo de título aborda esta problemática mediante el diseño y desarrollo de un Sistema de Acceso Residencial Inteligente. Esta solución centraliza la operación en una aplicación móvil modular con roles definidos (Guardia, Residente, Administración, Visita) e integra tecnologías de vanguardia como biometría facial, reconocimiento de patentes (LPR) y notificaciones en tiempo real, coordinándose en un futuro potencial con dispositivos IoT para la automatización de acceso físicos.

1.2 Descripción de la problemática

El proceso actual de control de acceso en la mayoría de los condominios chilenos carece de estándares tecnológicos de validación, lo que deriva en una operación reactiva en lugar de preventiva. Se han identificado cuatro ejes críticos que definen el problema:

- **Vulnerabilidad en la Identificación:** No existen mecanismos robustos para confirmar que quien ingresa es realmente la persona autorizada. El guardia debe confiar en su memoria visual o en la posesión de un control remoto físico, el cual es fácilmente clonable o transferible. Esto expone a la comunidad a riesgos de seguridad como robos o ingresos no autorizados.
- **Gestión Ineficiente de Visitas:** La autorización de visitas suele realizarse mediante mecanismos informales (llamadas telefónicas, citofonía), interrumpiendo la labor de vigilancia del guardia. La falta de un protocolo digital para “visitas no anunciadas” genera incertidumbre y tiempos de espera innecesarios en portería.
- **Ausencia de Trazabilidad y Auditoria:** El registro en libros de papel (“bitácora manual”) impide la búsqueda rápida de información. En caso de un incidente de seguridad, auditar quién ingresó y cuándo resulta en una tarea lenta y muchas veces infructuosa debido a la ilegibilidad, deterioro o adulteración de los registros físicos.
- **Rigidez Operativa:** Los sistemas de seguridad actuales suelen ser soluciones “paquete” cerradas que no se adaptan a las distintas realidades de los condominios (ej. Edificios vs Condominios de casas), obligando a las comunidades a pagar por hardware costos que no utilizan o a prescindir de tecnología por falta de presupuesto.

1.2.1 Análisis de los Actores Involucrados

La problemática afecta de manera diferenciada a los distintos actores del ecosistema residencial:

- **Guardia:** Sufre de sobrecarga cognitiva al tener que validar identidades, registrar datos a mano y contestar citófonos simultáneamente, lo que induce al error humano.
- **Residente:** Experimenta inseguridad y molestias por demoras en el acceso o la burocracia para autorizar a sus visitas y familiares.
- **Administración:** Carece de datos fidedignos para la toma de decisiones y la gestión de la seguridad, operando “a ciegas” sin métricas de flujo o incidentes.

1.3 Propuesta de Solución

Para mitigar estas problemáticas, se propone el desarrollo de una aplicación móvil integral que actúe como el núcleo de la seguridad y operación del condominio. La propuesta de valor se basa en sustituir el hardware costoso por software inteligente, utilizando los sensores de los dispositivos móviles para realizar validaciones complejas.

La solución se diferencia por su arquitectura modular flexible, permitiendo que cada comunidad active o desactive funcionalidades según políticas internas (por ejemplo, habilitar LPR pero desactivar biometría).

El sistema incorpora:

- Validación Biométrica: Uso de reconocimiento facial para validar la identidad de residentes y su grupo familiar sin necesidad de credenciales físicas.
- Control Vehicular Avanzado (LPR): Implementación de reconocimiento óptico de caracteres mediante la cámara del dispositivo móvil del guardia para validar patentes vehiculares en tiempo real contra una base de datos autorizada.
- Gestión de Visitas en Tiempo Real: Un flujo digital que permite al guardia notificar visitas no anunciadas directamente a la app del residente para su aprobación inmediata, eliminando el uso del citófono.
- Bitácora Digital Inteligente: Registro automático e inmutable de todos los eventos (ingresos, rechazos, notificaciones), accesible mediante filtros avanzados para auditoría inmediata.

1.4 Objetivos

1.4.1 Objetivo General

Desarrollar y validar un sistema integral de gestión de acceso residencial basado en una aplicación móvil, que automatice la verificación de identidad peatonal y vehicular mediante tecnologías biométricas, reconocimiento de patentes y códigos QR, mejorando la seguridad, la trazabilidad de la información y la eficiencia operativa de la conserjería.

1.4.2 Objetivos Específicos

1. Diseñar una arquitectura de software escalable que soporte múltiples roles de usuario y permita la configuración flexible de módulos funcionales según las necesidades del recinto.
2. Implementar mecanismos de validación segura, integrando servicios de reconocimiento facial y lectura de patentes (LPR) para el control de acceso peatonal y vehicular, reduciendo el riesgo de suplantación.
3. Desarrollar un sistema de bitácora digital y notificaciones, que registre automáticamente y en tiempo real todos los eventos de acceso, permitiendo además una comunicación fluida para la autorización remota de visitas imprevistas.

1.5 Justificación

La implementación de este sistema se justifica por la necesidad crítica de modernizar la seguridad residencial mediante una solución que sea, simultáneamente, accesible económicamente y escalable tecnológicamente. A diferencia de las infraestructuras tradicionales que dependen de hardware industrial costoso (como tótems o cámaras LPR dedicadas), esta propuesta innova al aprovechar la capacidad de procesamiento de los smartphones estándar para ejecutar validaciones complejas de biometría y lectura de patentes.

Esta estrategia democratiza el acceso a la seguridad de alta tecnología para comunidades con presupuestos limitados. La alineación de esta solución con la problemática actual radica en su capacidad de respuesta: la automatización del ingreso vehicular mediante LPR reduce drásticamente el tiempo de detención en el acceso, disminuyendo la ventana de oportunidad para delitos. Asimismo, la digitalización de la bitácora no solo elimina la vulnerabilidad de los registros físicos, sino que transforma los datos de acceso en información auditable y fidedigno, facilitando la gestión administrativa y la colaboración forense con las autoridades en caso de incidentes.

1.6 Alcances y Limitaciones

Es importante delimitar el perímetro del proyecto para gestionar las expectativas de la solución propuesta.

Este proyecto contempla el desarrollo de la aplicación móvil para los sistemas operativos Android e iOS, incluyendo los módulos de Guardia, Residente, Visitas y Administración. Se incluye la integración con servicios de nube para el procesamiento de imágenes y almacenamiento de datos.

El sistema se diseña como una herramienta de apoyo a la decisión humana del guardia, no como un reemplazo total del personal. La efectividad del reconocimiento LPR y facial dependerá de las condiciones de iluminación y la calidad de la cámara del dispositivo móvil utilizado por el personal de seguridad. No se contempla en esta etapa la integración física con barreras automáticas (IoT).

CAPÍTULO 2: MARCO CONCEPTUAL

El presente capítulo tiene como objetivo establecer las bases teóricas, técnicas y normativas que sustentan el desarrollo del “Sistema de Acceso Residencial Inteligente”. Se profundiza en los conceptos de seguridad físicas, las tecnologías de desarrollo de software móvil y los servicios seleccionados, así como en el marco legal chileno que regular el tratamiento de datos sensibles y la seguridad privada.

2.1 Metodología de Desarrollo

Para garantizar un desarrollo ordenado y eficiente, que permita adaptarse a los cambios y validar tempranamente las funcionalidades críticas, se ha seleccionado una metodología de trabajo ágil.

2.1.1 Metodología Ágil e Incremental

A diferencia de los modelos tradicionales en cascada, donde los requisitos se congelan al inicio, este proyecto utiliza un enfoque iterativo. Esto permite dividir el desarrollo en módulo funcionales (ej. Primero autenticación, luego biometría, finalmente LPR) que diseñan, implementan y prueban de forma cíclica. Esto asegura que cada componente funcione correctamente antes de integrarse al sistema mayor, reduciendo el riesgo de errores críticos en la etapa final.

2.2 Fundamentos de Seguridad y Control de Acceso

El control de acceso es una disciplina de la seguridad que se encarga de regular quién puede entrar a un lugar y cuándo. En el contexto residencial, este concepto ha evolucionado desde barreras puramente físicas hacia sistemas lógicos e inteligentes.

2.2.1 Control de Acceso Físico vs Lógico

Tradicionalmente, los condominios dependen del control físico (barreras, rejas, puertas) operado mediante mecanismos simples (llaves, controles remotos). Este proyecto introduce el control de acceso lógico, que utiliza software para decidir si una barrera física debe abrirse. La principal ventaja del control lógico es la trazabilidad: mientras que una llave no deja registro de cuándo fue usada ni por quién, un sistema digital registra la identidad, la hora exacta y el método de verificación de cada evento, creando una bitácora inmutable para auditorías futuras.

2.2.2 Autenticación de Identidad

La seguridad informática define tres factores para verificar la identidad de una persona:

1. Algo que sabes: Una contraseña o PIN.
2. Algo que tienes: Una tarjeta, llave o celular.
3. Algo que eres: Características biométricas (huella, rostro).

Los sistemas actuales fallan porque dependen solo de “lo que tienes” (control remoto), el cual es transferible o puede ser robado. Esta propuesta eleva el estándar al integrar “lo que eres” (biometría) y “lo que tienes” (el smartphone verificado), robusteciendo significativamente la seguridad del recinto.

2.3 Tecnologías de Verificación Avanzada

La parte innovadora de este proyecto radica en democratizar tecnologías que usualmente requieren hardware costoso, implementándolas mediante software en dispositivos móviles estándar.

2.3.1 Biometría Facial (Reconocimiento Facial)

La biometría facial es una tecnología capaz de identificar o verificar a una persona a partir de una imagen digital de su rostro. El proceso funciona detectando la cara en la imagen y midiendo características únicas (distancia entre ojos, forma de la mandíbula, contorno de nariz) para generar un “mapa” o vector matemático.

En el contexto de este proyecto, la tecnología se utiliza para certificar que la persona que se presenta frente al guardia corresponde inequívocamente a un residente registrado. Este mecanismo elimina la dependencia de credenciales físicas – susceptibles de robo o extravío – y mitiga el riesgo de suplantación de identidad, dado que el rostro constituye un atributo intransferible. Para ello, se integra AWS Rekognition, un servicio de visión computacional en la nube que compara la imagen capturada en tiempo real contra una base de datos segura de rostros enrolados, garantizando una alta precisión y tiempos de respuesta compatibles con la operación en portería.



Figura 2: Servicio de análisis de imágenes y video Amazon Rekognition.

Fuente: Amazon Web Services

2.3.2 Reconocimiento Óptico de Caracteres (OCR) y LPR

El reconocimiento automático de matrículas (LPR o *License Plate Recognition*) es una aplicación específica de la tecnología OCR (*Optical Character Recognition*), que permite convertir texto dentro de una imagen en datos procesables por una computadora.

Lo que hace este sistema es capturar una imagen del vehículo, localiza la región de la patente, segmenta los caracteres y los traduce a texto alfanumérico (ej. “ABCD12”).

A diferencia de los sistemas tradicionales que usan cámaras fijas costosas en los pórticos, este proyecto implementa LPR móvil utilizando la cámara del celular del guardia y la librería Google ML Kit. Esto permite procesar la imagen directamente en el dispositivo (*on-device*), ofreciendo una validación instantánea sin depender de la latencia de internet, lo cual es crítico para el flujo vehicular.



Figura 3: Librería de aprendizaje automático en el dispositivo Google ML Kit
Fuente: Google Developers Blog

2.4 Arquitectura y Herramientas de Desarrollo

Para construir una solución moderna, escalable y mantenible, se ha seleccionado una arquitectura basada en la nube (*Cloud-Native*) y desarrollo multiplataforma.

2.4.1 *Flutter* (Desarrollo Móvil)

Flutter es un kit de desarrollo de software (SDK) de código abierto creado por Google. Se diferencia de otras opciones por utilizar el lenguaje *Dart* y un motor de renderizado propio.

Esto permite desarrollar aplicaciones nativas para Android e iOS desde un único código base. Esto es vital para el proyecto, ya que los residentes y guardias puedan tener diferentes tipos de teléfonos. *Flutter* garantiza que la interfaz y la lógica de negocio (como el escáner LPR) funcionen idénticamente en ambos sistemas operativos, reduciendo los tiempos y costos de desarrollo a la mitad.



Figura 4: Logotipo del framework de desarrollo multiplataforma Flutter.

Fuente: Flutter Dev

2.4.2 *Firebase* (*Backend-as-a-Service*)

Firebase es una plataforma de desarrollo de Google que proporciona infraestructura de servidor gestionada, permitiendo centrarse en la lógica de la aplicación sin administrar servidores físicos.

- *Authentication*: Gestiona el inicio de sesión seguro y la identidad de los usuarios, soportando correos y contraseñas encriptadas.
- *Cloud Firestore*: Una base de datos NoSQL, alojada en la nube que permite almacenar y sincronizar datos en tiempo real. Es el "cerebro" donde se guarda la información de usuarios, vehículos y la bitácora de eventos.
- *Cloud Functions*: Permite ejecutar código de backend en respuesta a eventos (como la creación de una solicitud de visita) para enviar notificaciones push de manera segura, manteniendo la lógica sensible fuera del dispositivo del usuario.



Figura 5: Plataforma de desarrollo de aplicaciones Google Firebase.
Fuente: Google Firebase Brand Guidelines.

2.4.3 Servicios de Inteligencia Artificial en la Nube (AWS)

Amazon Web Services (AWS) proporciona la potencia de cómputo para las tareas más complejas.

AWS Rekognition es un servicio SaaS (*Software as a Service*) de análisis de imágenes y videos. A diferencia de procesar el reconocimiento facial en el celular (lo que puede llegar a ser lento o inseguro), AWS recibe la imagen, realiza el cotejo biométrico con algoritmos de aprendizaje profundo (*Deep Learning*) y devuelve el resultado con un nivel de confianza, garantizando escalabilidad y seguridad de los datos biométricos.



Figura 6: Ecosistema de servicios de computación en la nube de Amazon Web Services.
Fuente: Lituus Analytics.

2.5 Marco Legal y Normativo

El desarrollo de soluciones tecnológicas para seguridad en Chile no ocurre en un vacío legal. El proyecto se adhiere estrictamente a la normativa vigente para asegurar su viabilidad ética y legal.

2.5.1 Protección de Datos Personales (Ley N° 19.628)

Esta ley regula el tratamiento de datos de carácter personal en registros o bancos de datos.

La aplicación maneja datos sensibles (RUT, patentes) y datos biométricos (rostros).

El diseño del sistema debe cumplir con el principio de finalidad (los datos solo se usan para control de acceso) y seguridad. Las imágenes no se guardan como archivos JPG accesibles públicamente, sino que se procesan y almacenan de forma segura, respetando la privacidad de los residentes.

2.5.2 Nueva Ley de Copropiedad Inmobiliaria (Ley N° 21.442)

Esta ley moderniza la regulación de condominios, permitiendo explícitamente el uso de plataformas digitales para la participación y comunicación.

La ley faculta a los comités de administración para tomar decisiones sobre seguridad. La funcionalidad “Módulos Flexibles” de la aplicación (activar/desactivar LPR o Biometría) responde directamente a esta realidad, permitiendo que la tecnología se adapte al reglamento de copropiedad específico de cada comunidad, y no al revés.

2.5.3 Normativa de Seguridad Privada (OS10 de Carabineros)

El decreto Ley N° 3.607 regula las actividades de vigilancia privada.

Esta normativa establece que los guardias son componentes de un sistema de seguridad, no la única medida. La aplicación se diseña como una herramienta de apoyo (Bitácora Digital) que profesionaliza la labor del guardia, permitiéndole cumplir con su obligación de registrar y controlar accesos de manera más eficiente y fidedigna, sin reemplazar su criterio ni responsabilidad legal.

CAPÍTULO 3: PROPUESTA DE SOLUCIÓN

3.1 Modelado y Arquitectura del Sistema

Esta sección presenta la abstracción técnica de la solución propuesta. Se utiliza diagramas estandarizados (UML) para representar la estructura, el comportamiento y la interacción de los componentes del sistema, facilitando la comprensión del flujo de información entre la aplicación móvil y los servicios en la nube.

3.1.1 Diagramas de Caso de Uso

Los siguientes diagramas modelan el comportamiento funcional del sistema, desglosando las interacciones permitidas para cada uno de los tres actores principales. Se ha utilizado el estándar UML para representar no solo las acciones directas, sino también las dependencias lógicas entre procesos.

A. Casos de Uso del Perfil Administrador

El administrador es el actor encargado de la configuración estratégica y la gestión de la comunidad.

Como se observa en la Figura 3.x, todos los casos de uso de gestión crítica (como "Gestionar Guardias" o "Configurar Módulos") tienen una relación de inclusión con el caso base "Autenticarse", lo que indica que la seguridad es un pre-requisito obligatorio que no puede ser eludido. Adicionalmente, el caso de uso "Gestionar Residentes" se extiende mediante la acción "Enviar Invitación", representando un flujo que permite el enrolamiento a nuevos usuarios.

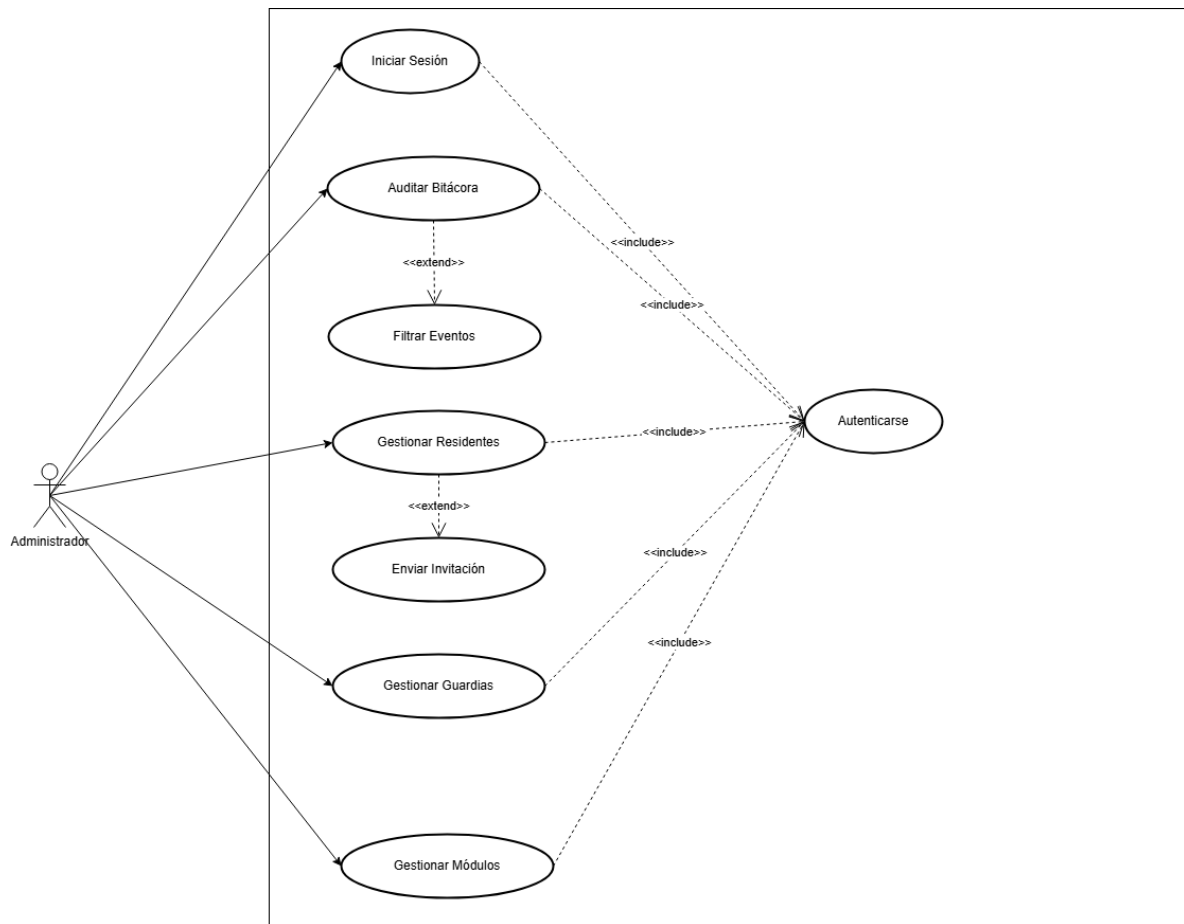


Figura 7: Diagrama de Casos de Uso del Administrador
Fuente: Elaboración Propia.

B. Casos de Uso del Perfil Guardia

El guardia es el operador del sistema en tiempo real. Sus casos de uso están diseñados para la eficiencia operativa y la trazabilidad forense.

En la figura 3.x se detalla que las tres acciones principales de validación comparten una relación de inclusión con el caso de uso "Registrar en Bitácora". Esto implica que el sistema está diseñado para que sea imposible realizar una validación sin que se quede un registro inmutable de la misma, garantizando la auditoría. Por otro lado, estas validaciones pueden extenderse hacia una "Alerta de Rechazo" si las reglas así lo determinan.

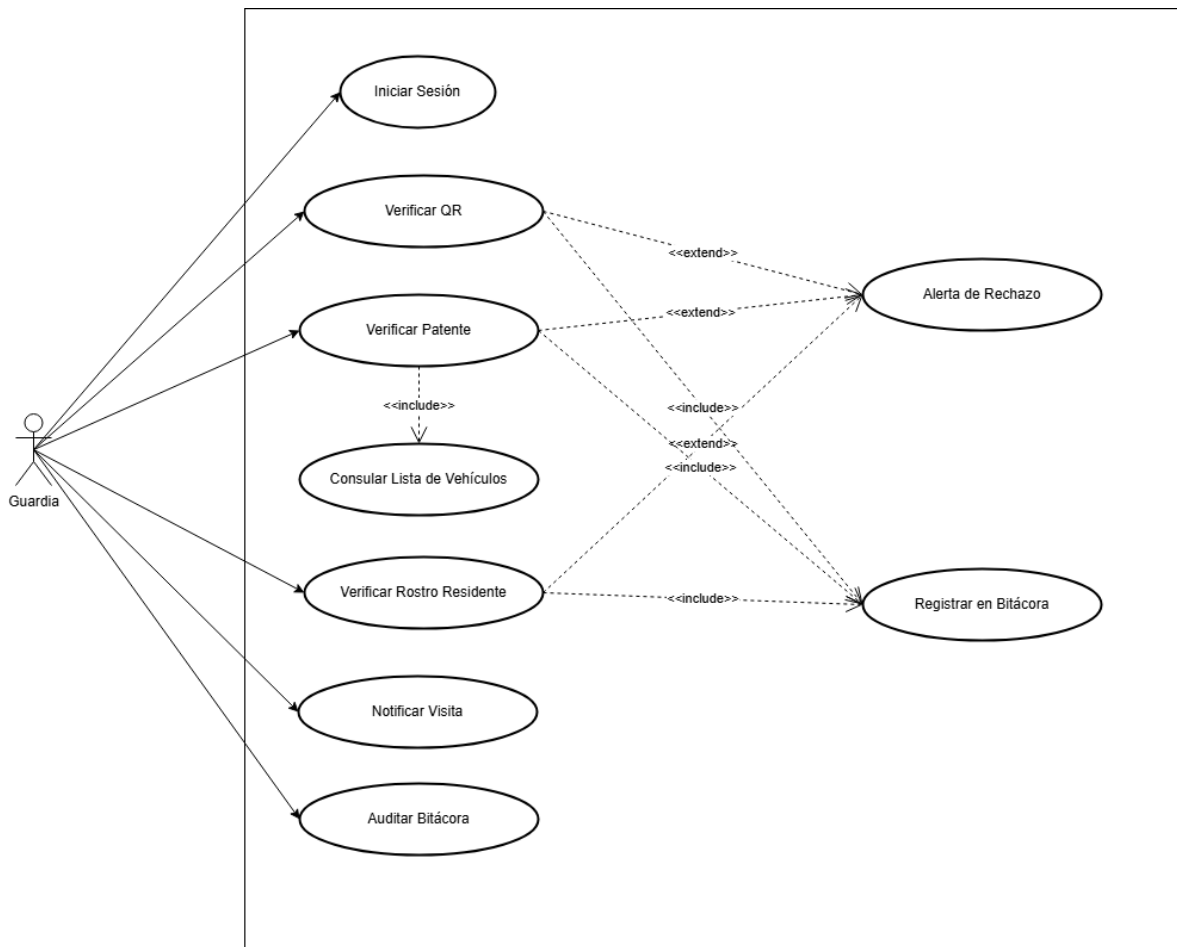


Figura 8: Diagrama de Casos de Uso del Guardia
Fuente: Elaboración Propia

C. Casos de Uso del Perfil Residente

El Residente es el usuario final que interactúa con los servicios de autogestión. Su diagrama modela la autonomía en la gestión de su seguridad personal.

La figura 3.X ilustra cómo el caso de uso "Crear Pase de Visita" incluye necesariamente la "Generación QR". Este proceso extiende opcionalmente con "Compartir Pase", permitiendo al usuario enviar el QR vía correo. Finalmente, el caso de uso "Recibir Notificaciones" presenta dos extensiones críticas de decisión "Aprobar Acceso" o "Rechazar Acceso", la cuales disparan actualizaciones inmediatas en la terminal del guardia.

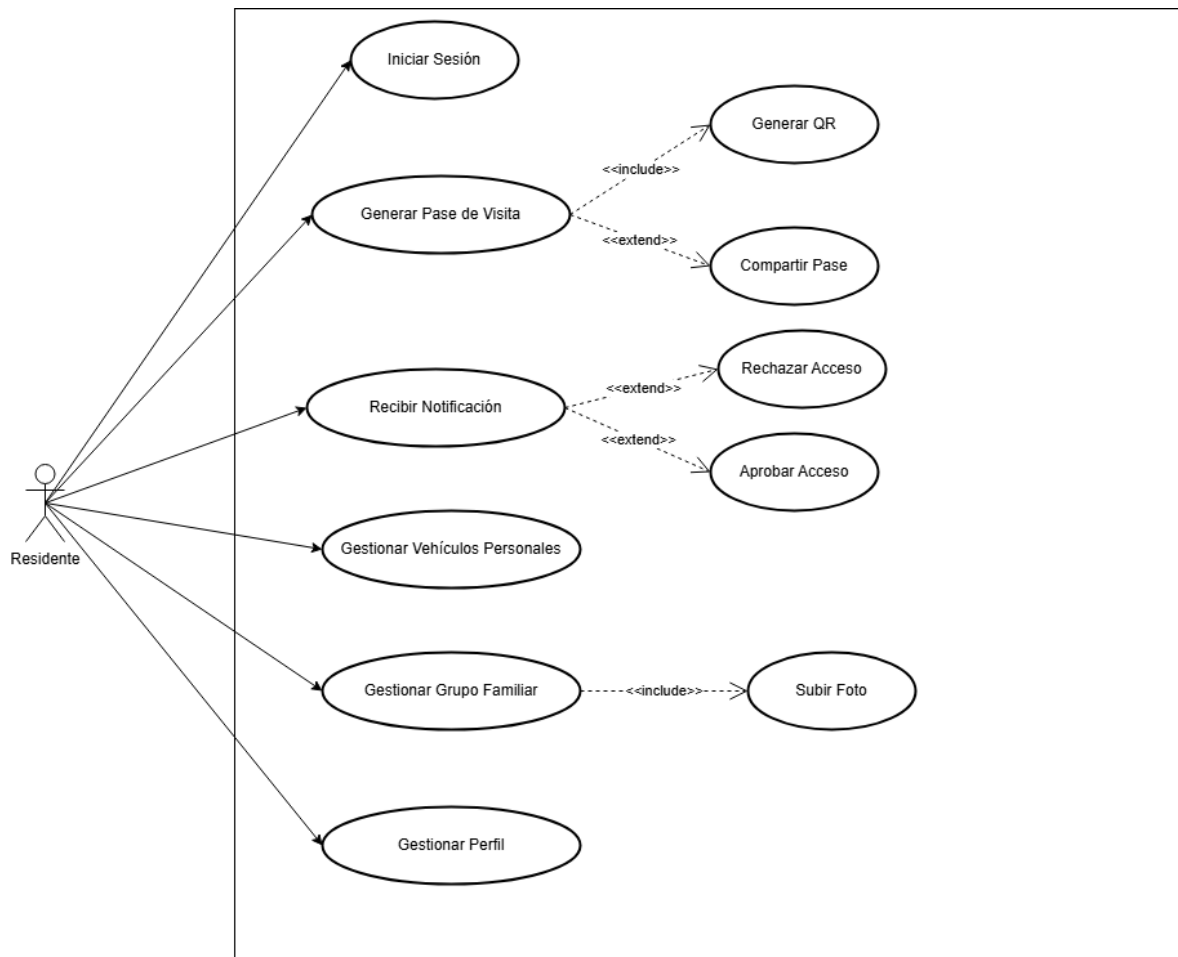


Figura 9: Diagrama de Casos de Uso del Residente
Fuente: Elaboración Propia

3.1.2 Proceso de Gestión de identidad y Enrolamiento

La seguridad del sistema depende de un control estricto sobre quién tiene acceso a la plataforma. A diferencia de aplicaciones abiertas, en este sistema los usuarios (Residentes y Guardias) no pueden auto registrarse libremente; deben ser invitados y validados previamente por el Administrador. A continuación, se detallan los flujos de invitación y activación.

A. Flujo de Invitación a Residente (Rol: Administrador)

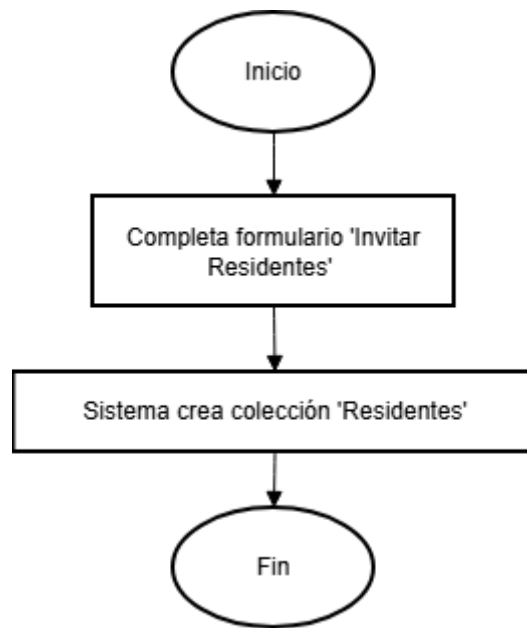


Figura 10: Diagrama de Flujo Invitación a Residente como Administrador
Fuente: Elaboración Propia

Este proceso describe cómo el administrador da de alta a un nuevo residente en el sistema, asegurando que solo personas autorizadas por la comunidad puedan acceder a la aplicación.

Lo primero que se realiza dentro de este proceso es que el Administrador accede a la vista de gestión de Residentes, luego debe completar el formulario con los datos del residente (Nombre, Apellido, Torre en el caso que sea edificio, Numero de residencia y correo).

En el caso de que el correo este registrado, debe mostrar mensaje que ya se encuentra en la base de datos.

Luego de enviar la invitación, se crea un registro en la colección "Residentes" con el estado "Pendiente" y el sistema confirma al administrador que la invitación fue enviada exitosamente.

B. Flujo de Activación de Cuenta Residente (Rol: Residente)

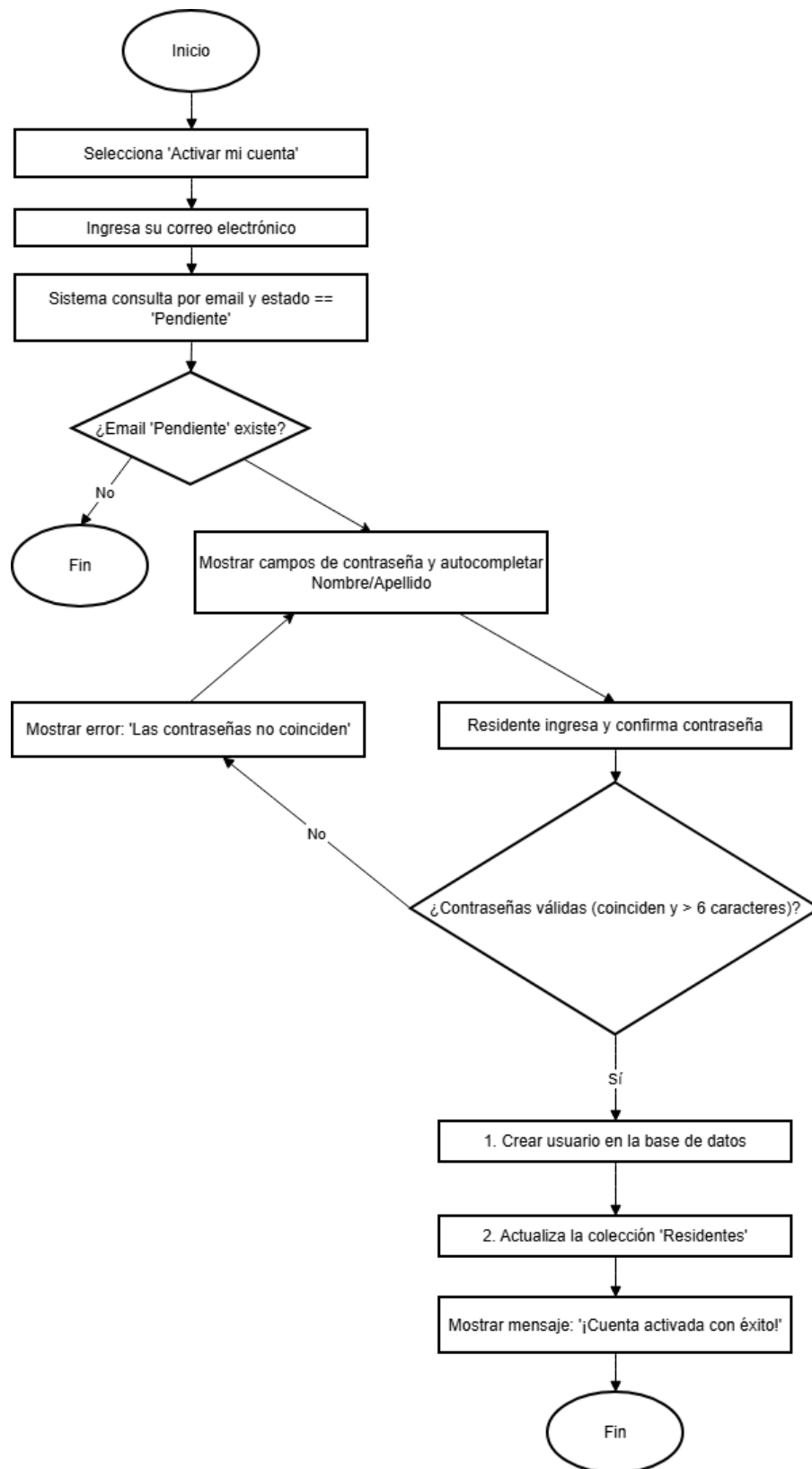


Figura 11: Diagrama de Flujo Activación de cuenta del Residente
Fuente: Elaboración Propia

Una vez que se crea la invitación para el residente, este debe completar su registro para activar su cuenta y definir su contraseña persona.

El residente abre la aplicación móvil y selecciona la opción "Activar Cuenta de Residente", ingresa el correo electrónico al cuál se envió la invitación.

El sistema verifica que exista en la base de datos y consulta el estado en el que se encuentra. En el caso de que el correo no existe o ya se encuentra activo, mostrar un mensaje de error y detener el proceso.

Si la validación es correcta, el usuario define una contraseña segura y el sistema crea el usuario en el servicio de autenticación (Firebase Auth) y actualiza el estado del residente a "Registrado".

C. Flujo de Invitación a Guardia (Rol: Administrador)

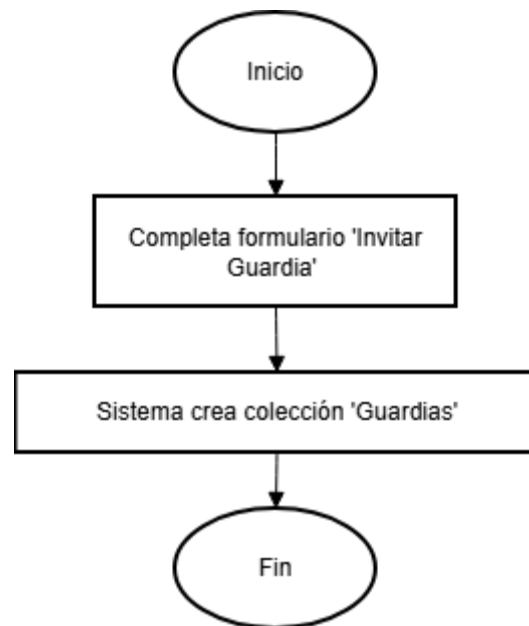


Figura 12: Diagrama de Flujo Invitación a Guardia como Administrador

Fuente: Elaboración Propia

Similar al proceso de residentes, este flujo permite al administrador gestionar la dotación de seguridad, vinculando al guardia con el condominio específico.

El administrador accede al módulo de gestión de Guardias, se registra los datos personales (Nombre, Apellido, Correo) y se asigna el guardia al condominio actual (Se vincula al condominio del Administrador que crea la invitación).

Se guarda al usuario en la colección "Guardias" con el estado de "Pendiente" y queda habilitado para activar su cuenta.

D. Flujo de Activación de Cuenta Guardia (Rol: Guardia)

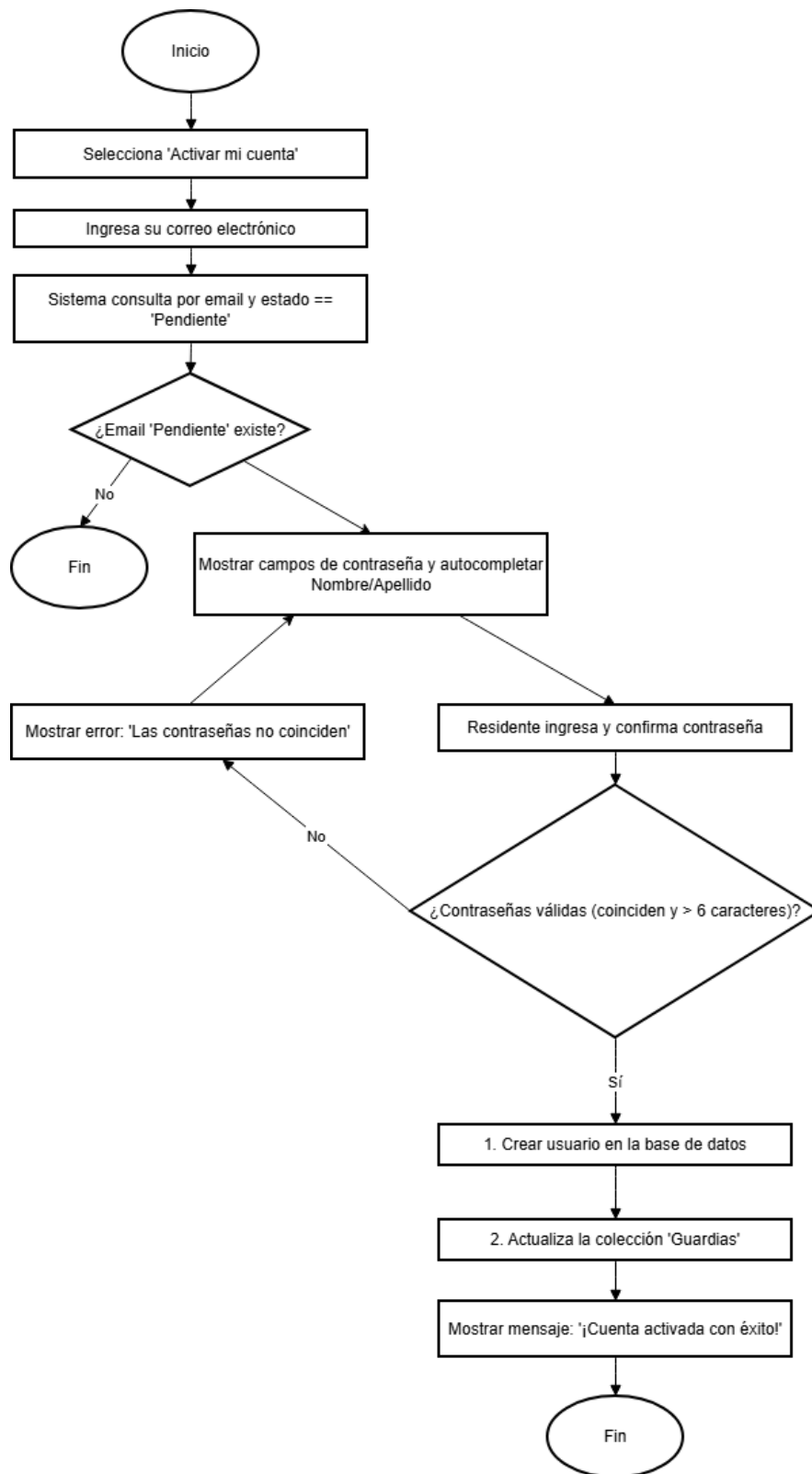


Figura 13: Diagrama de Flujo Activación Cuenta de Guardia
Fuente: Elaboración Propia

Este proceso asegura que el guardia configure su acceso personal, garantizando que las acciones registradas en la bitácora sean trazables a su identidad única.

El guardia abre la app y selecciona “Activar Cuenta de Guardia”, ingresa el correo para verificar que exista una invitación al correo ingresado, en el caso de no existe o ya este activa se le notifica al usuario.

Si el correo es válido y tiene una invitación, el guardia debe crear su contraseña de acceso. El sistema registra a este usuario en el Firebase Auth.

Luego de esto el usuario puede ingresar a las funcionalidades del guardia y comenzar a trabajar con la aplicación.

3.1.3 Diagramas de Flujo Operativos

Los siguientes diagramas modelan los procesos de negocio críticos del sistema, detallando la secuencia lógica de decisiones y acciones tecnológicas para cada funcionalidad.

A. Flujo de Control de Acceso Vehicular (LPR)

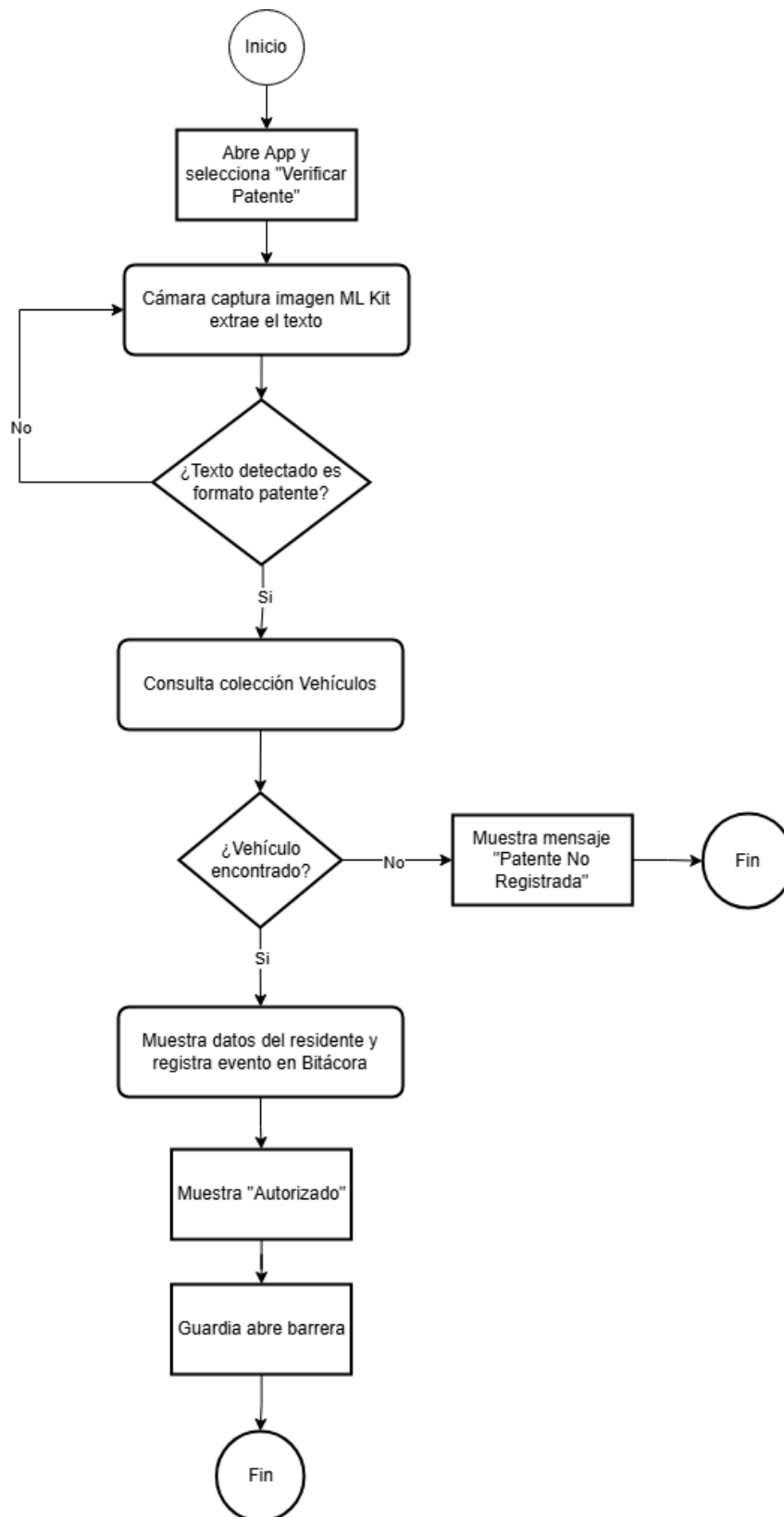


Figura 14: Diagrama de Flujo Control de Acceso Vehicular
Fuente: Elaboración Propia

Este diagrama ilustra el proceso de validación automática de patentes utilizando reconocimiento de caracteres (OCR) directamente en el dispositivo móvil del guardia.

Para comenzar este proceso un residente debe querer ingresar con su vehículo en el punto de control. El guardia dentro de la aplicación debe seleccionar la opción "Verificar Patente" en la aplicación, activando la cámara.

Para analizar la patente se ocupa la librería Google ML Kit, lo que a través de la imagen busca patrones alfanuméricos compatibles con matrículas chilenas, así detectando si la patente es válida y extraer la cadena de texto para así, consultar en la base de datos si el vehículo esta registrado en el condominio actual.

A través de esta verificación, el guardia accionará la barrera de ingreso al vehículo que desea ingresar.

B. Flujo de Control de Acceso Residente (Biometría Facial)

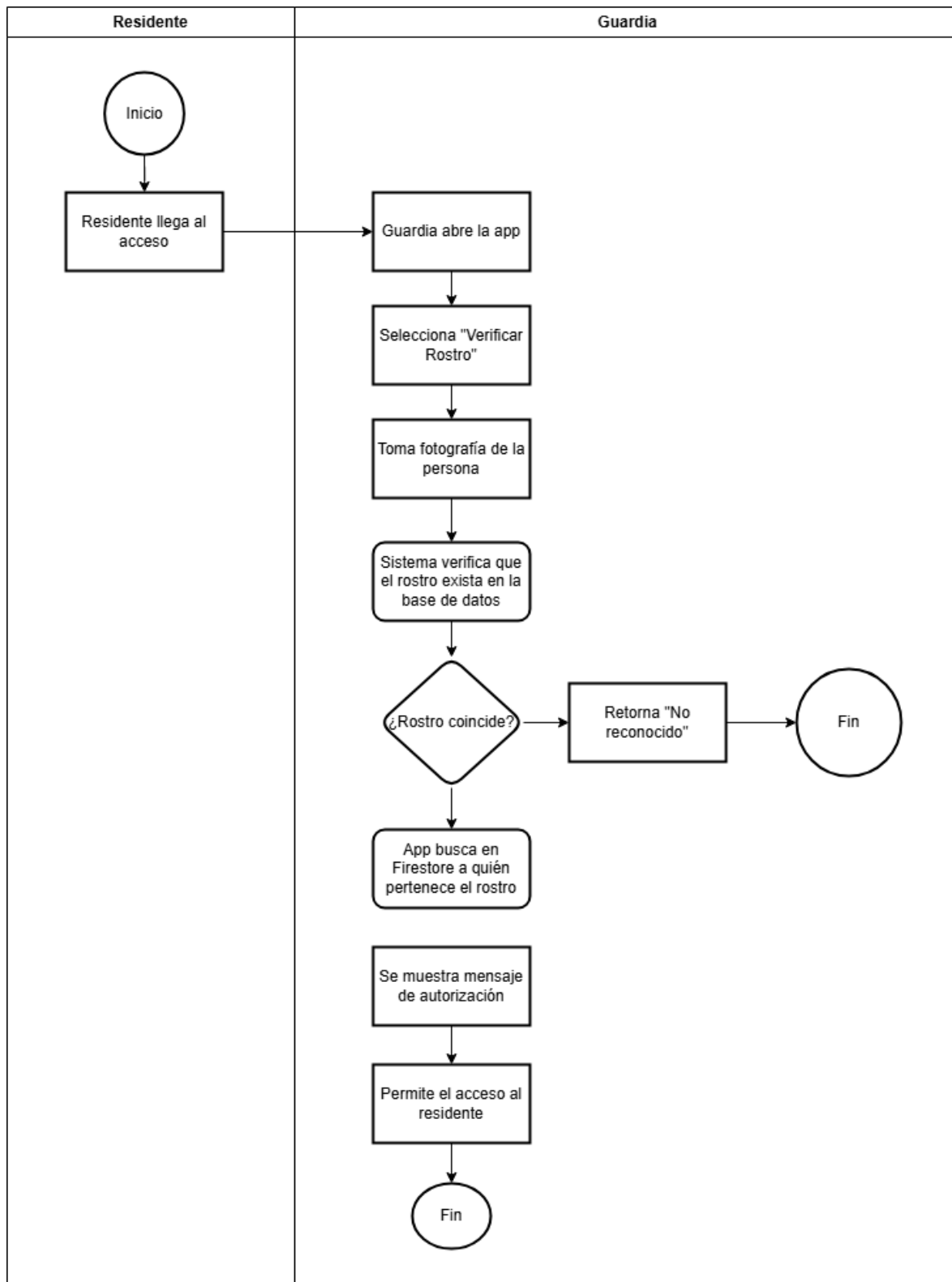


Figura 15: Diagrama de Flujo Control de Acceso Residente
Fuente: Elaboración Propia

Representa la interacción con servicios en la nube para la validación de identidad sin contacto físico.

Para poder realizar la validación, un residente se debe presentar en la portería para que luego el guardia seleccione "Verificar Rostro" y tome una fotografía de la persona.

Esta imagen es enviada al servicio de AWS Rekognition para comparar la imagen con la colección de rostros guardados del condominio, si encuentra una coincidencia superior al umbral de confianza (90%) retorna el FaceID para buscar en Firestore los datos del residente asociado.

Para finalizar se muestra un mensaje de "Acceso Autorizado" con los datos del residente y se guarda el evento en bitácora para luego permitir el acceso al Residente.

C. Flujo de Generación y Verificación de Pase de Visita (QR)

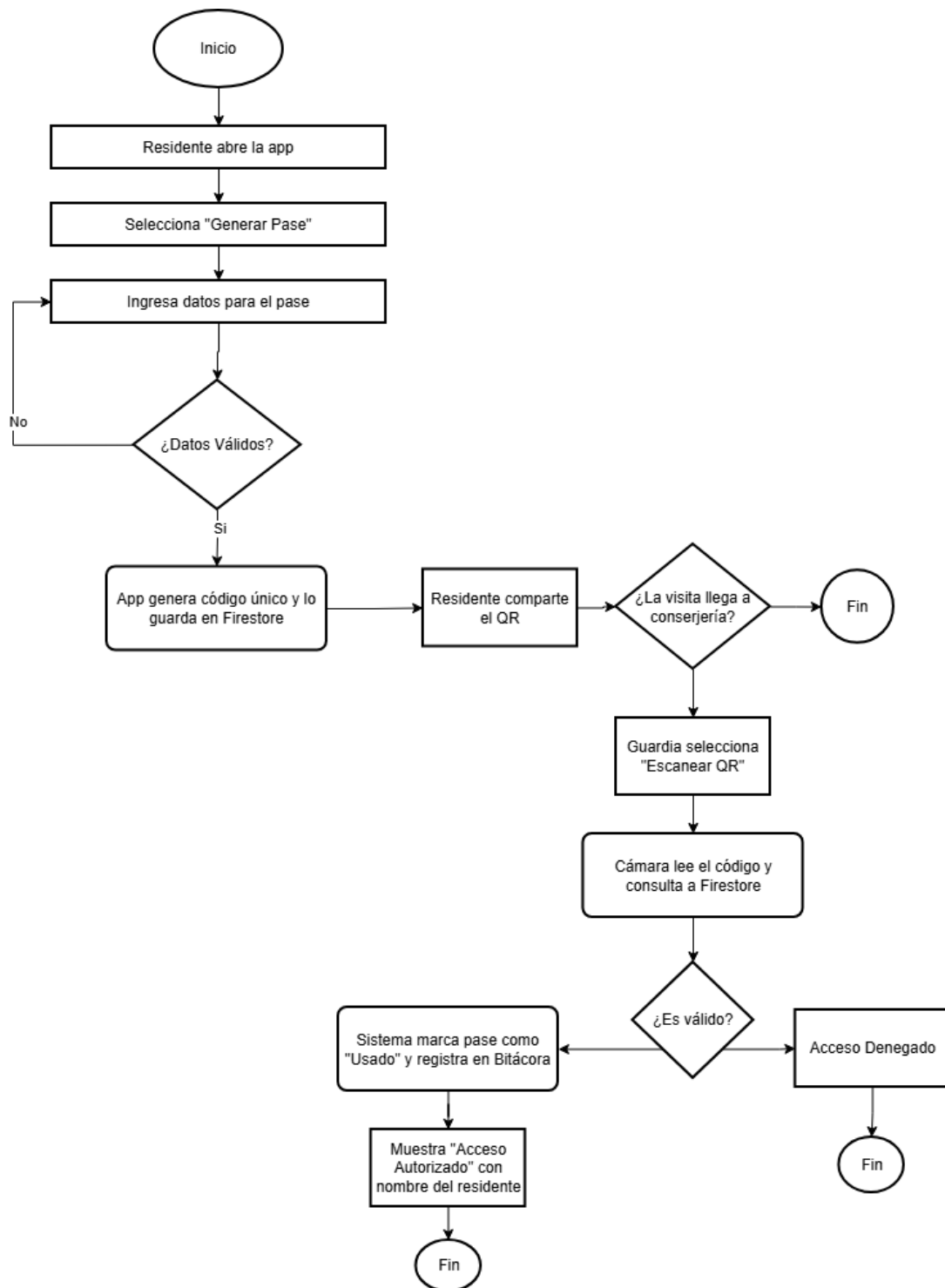


Figura 16: Diagrama de Flujo de Generación código QR y Verificación
Fuente: Elaboración Propia

Describe el ciclo completo de una invitación digital, desde su creación por el residente hasta su validación en portería.

Para poder generar un código QR el residente debe ingresar los datos de la visita en su aplicación. El sistema genera un código único y lo almacena en la base de datos con su estado ("Programada"). El residente comparte este código QR vía correo.

Al llegar la visita al punto de control, el guardia escanea el código QR presentado, el sistema verifica el estado del código QR.

- ¿El código existe en la base de datos?
- ¿La fecha actual corresponde a la programada?
- ¿El estado del pase está vigente?

La aplicación al ya validar el código QR, muestra los datos de la Visita y del Residente que invita y cambia el estado del pase para evitar reingresos.

D. Flujo de Notificación de Visita No Anunciada

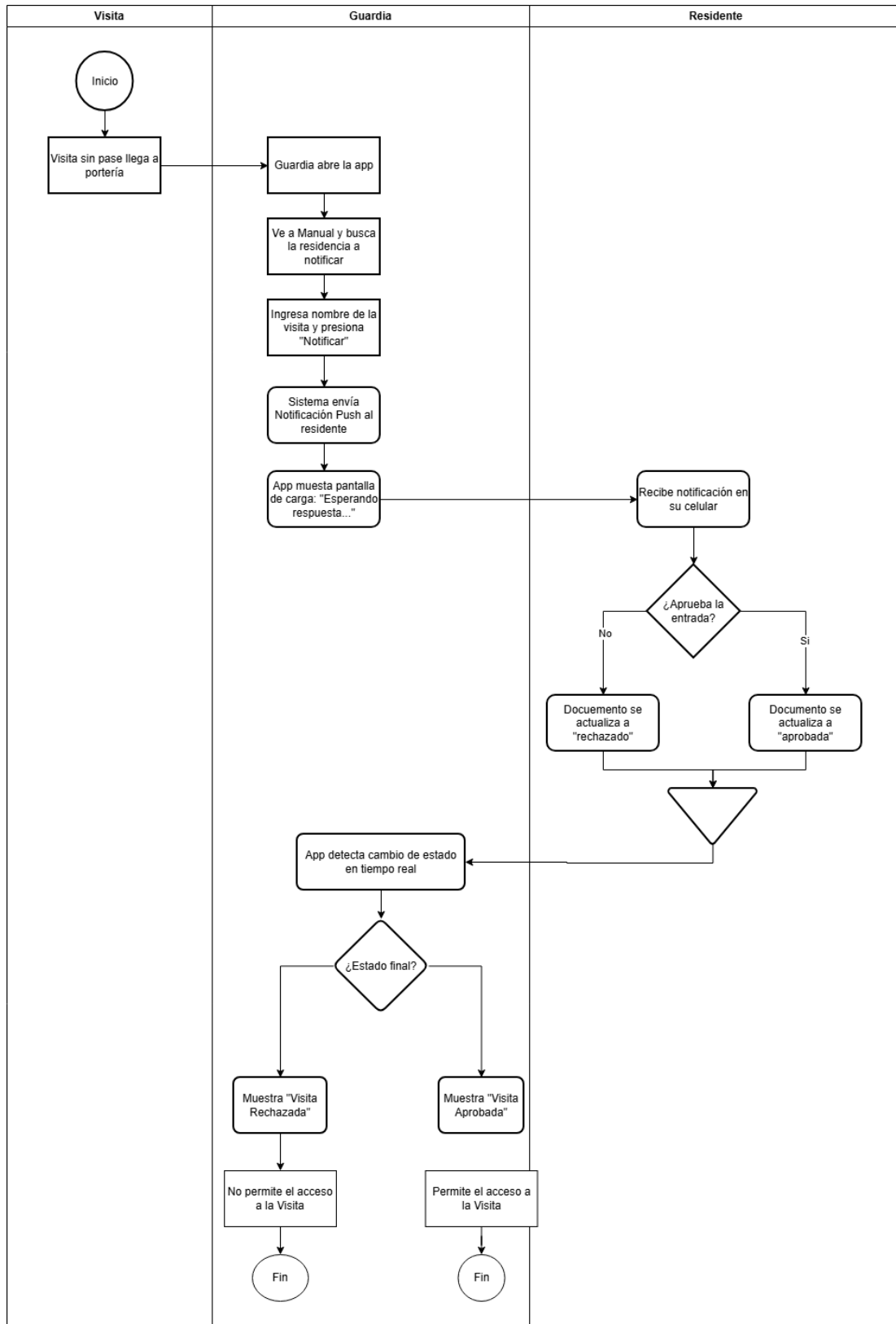


Figura 17: Diagrama de Flujo de Visita no Anunciada
Fuente: Elaboración Propia

Detalla el proceso de comunicación asíncrona entre la portería y la vivienda para autorizar ingresos imprevistos.

El guardia para notificar una visita al cual no han generado un código QR, debe seleccionar la residencia de destino en la aplicación e ingresar sus datos para luego enviar una notificación al Residente.

Se crea un registro de solicitud en la base de datos, lo que activa una Cloud Function que envía una notificación push al dispositivo móvil del residente.

La interfaz del guardia entra en estado de espera hasta que se autorice o rechace la notificación, lo cual después de esto muestra el resultado final para permitir o denegar el acceso.

E. Flujo de Configuración de Módulos (Administrador)

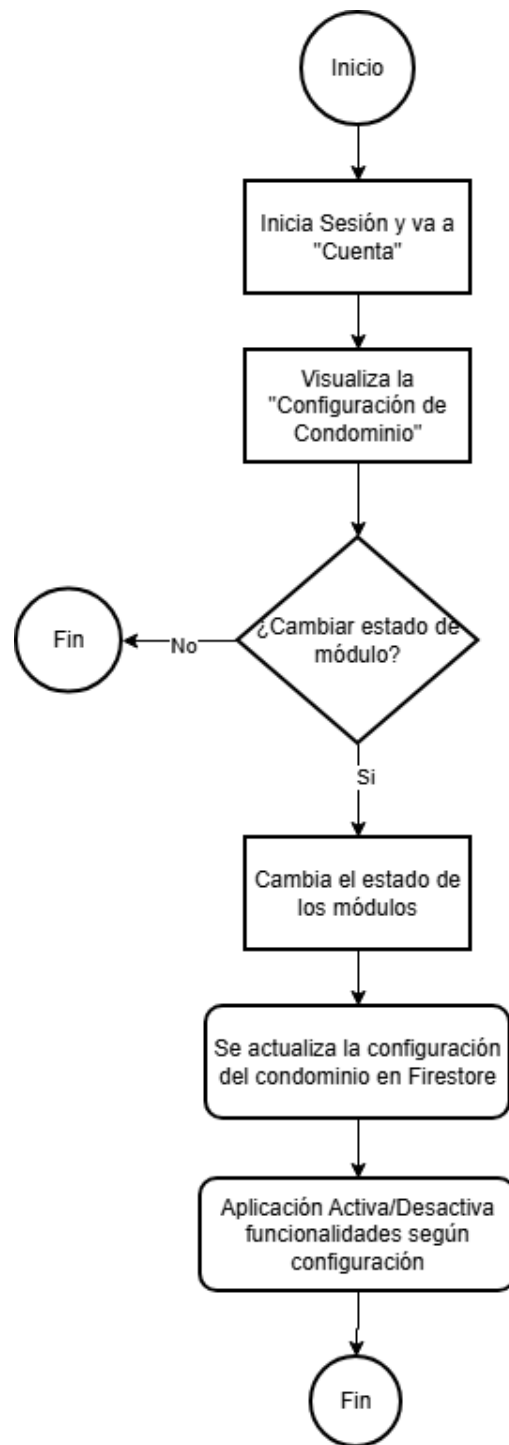


Figura 18: Diagrama de Flujo Configuración Modular
Fuente: Elaboración Propia

Explica la capacidad del sistema para adaptar su funcionamiento a las políticas del recinto.

El administrador ingresa al panel de configuración del condominio, visualiza los switches disponibles para cada módulo y toma la decisión de activar o desactivar una funcionalidad específica (Biometría, LPR, Notificación de Visita no anunciada)

El cambio se guarda en la configuración del condominio y las vistas de cada rol de la aplicación se actualizan según esta configuración.

3.2 Modelo de Datos (Diseño de Base de Datos)

3.2.1 Modelo Conceptual Relacional

Para la persistencia de datos se seleccionó Cloud Firestore, una base de datos NoSQL orientada a documentos. Esta elección permite una estructura flexible y escalable, capaz de manejar la sincronización en tiempo real requerida por los múltiples roles de la aplicación.

El modelo se diseñó situando a la entidad Condominio como el nodo central que orquesta las relaciones entre los distintos actores, asegurando la integridad referencial y la seguridad de los datos en un entorno *multi-tenant*. A continuación, se describen las colecciones principales y sus relaciones lógicas.

1. Colección Condominios

Condominios	
PK	<u>uid</u>
	nombreCondominio
	configuracion
	createdAt
FK	tipoCondominioID

Figura 19: Colección Condominios
Fuente: Elaboración Propia

Esta es la columna vertebral del sistema. Aquí es donde se almacena la identidad del entorno residencial (nombreCondominio) y, lo más importante la configuración Modular dentro del 'configuracion'.

Su 'uid' actúa como la llave primaria. Las entidades operativas utilizan este ID como llave foránea para asegurar la pertenencia de los datos.

2. Colección Administradores

Administradores	
PK	<u>uid</u>
	rut
	nombre
	apellido
	email
	condominiosIds

Figura 20: Colección Administradores
Fuente: Elaboración Propia

Se utiliza el UID de autenticación como identificador principal e incluye un el campo rut para cumplir con los requisitos de identificación formal.

A través del campo condominiosIds, un mismo administrador puede gestionar múltiples comunidades simultáneamente desde una única cuenta, permitiendo escalabilidad operativa.

3. Colección condo_types

condo_types	
PK	<u>id</u>
	name
	order

Figura 21: Colección condo_types
Fuente: Elaboración Propia

Actúa como un catálogo maestro o tabla de referencia estática.

Define los tipos de entornos residenciales soportados por el sistema (ej. "Edificio", "Condominio" o "Parcelas").

Su ID se guarda en el campo 'tipoCondominioID' de la colección Administradores y Residentes. Lo que permite a la aplicación adaptar la interfaz: por ejemplo si el tipo es "Edificio", se solicitará el dato "Torre", mientras que el condominio, solo se pedirá el "Numero" de domicilio.

4. Colección Guardias

Guardias	
PK	<u>uid</u>
FK	condominioId
	nombre
	apellido
	rut
	correo
	rol
FK	estado
	createdAt

Figura 22: Colección Guardias
Fuente: Elaboración Propia

Contiene los perfiles del personal de seguridad autorizado para operar en la aplicación.

Almacena datos personales (nombre, correo), el estado de la cuenta ("Registrado" o "Pendiente") y el condominioId al que pertenece este usuario.

El campo uid de este documento es referenciado posteriormente en la colección Eventos y en Visitas para dejar constancias de qué funcionario autorizo un ingreso específico.

5. Colección Residentes

Residentes	
PK	<u>uid</u>
FK	condominioid
	nombre
	apellido
	rut
	correo
	rol
	torre
	numero
	estado
	fcmToken
	hasFaceId
	rekognitionFaceId
	lastTokenUpdate
	createdAt

Figura 23: Colección Residentes
Fuente: Elaboración Propia

Esta colección guarda la información de contacto, la ubicación dentro del recinto y el fcmToken, lo cual es necesario para el envío de notificaciones push al dispositivo del usuario. También es importante el rekognitionFaceId, que vincula al usuario con su vector biométrico en AWS.

Esta colección actúa como “padre” de dos sub-colecciones críticas: “Vehículos” y “GrupoFamiliar”, manteniendo los datos organizados lógicamente bajo cada usuario.

6. Sub-Colecciones de Residente

Para mantener la integridad de los datos, los vehículos y familiares se modelan como sub-colecciones dentro de cada documento de residente.

A. Sub-Colección GrupoFamiliar

GrupoFamiliar	
PK	<u>id</u>
FK	condominioid
	nombre
	apellido
	nombreCondominio
	rut
	hasFaceld
	rekognitionFaceld
	createdAt

Figura 24: Sub-Colección GrupoFamiliar

Fuente: Elaboración Propia

Esta sub-colección almacena los datos de las personas que residen con el residente principal de la cuenta, guarda su nombre, Rut y su propio "RekognitionFaceId".

Esta colección permite que el sistema de biometría reconozca no solo al residente dueño de la cuenta, si no que a cualquier miembro de su familia que viva dentro del entorno residencial, vinculando el ingreso.

B. Sub-Colección Vehiculos.

Vehiculos	
PK	<u>id</u>
FK	condominioid
	plate
	description
	createdAt

Figura 25: Sub-Colección Vehiculos
Fuente: Elaboración Propia

Esta registra las patentes autorizadas para el ingreso automático.

El módulo LPR del guardia consulta esta colección para validar si una patente leída por la cámara corresponda a un residente activo.

7. Colección Visitas

Visitas	
PK	<u>id</u>
FK	condominioid
FK	residentUid
	visitorName
	visitorLastName
	visitorId
	code
	phone
	plate
	status
FK	checkedByGuardUid
	createdAt
	scheduledAt

Figura 26: Colección Visitas
Fuente: Elaboración Propia

Esta colección gestiona el ciclo de las invitaciones digitales (Pases QR).

Almacena el código, el nombre del visitante junto con el estado del pase ('programada', 'autorizada', 'expirada').

Actúa como un registro transaccional que vincula tres partes: el Residente que creo la invitación ('residentUid'), el Guardia que la validó ('checkedByGuardUid') y el condominio donde ocurrió el evento ('condominioId').

8. Colección notificaciones_visita

notificaciones_visita	
PK	<u>id</u>
FK	condominioId
FK	residentUid
FK	guardUid
	guardName
	residentName
	visitorName
	torre
	numero
	status
	createdAt
	respondedAt

Figura 27: Colección notificaciones_visita

Fuente: Elaboración Propia

Esta colección cumple una función técnica específica: actúa como una "cola de mensajes" para la comunicación en tiempo real.

Es una colección efímera, que cuando el Guardia crea un documento aquí, se dispara automáticamente una Cloud Function.

Sirve de puente temporal entre el Guardia y el Residente. Contiene el estado de la solicitud ('pendiente', 'aprobada', 'rechazada'), el cual es escuchado en tiempo real por la app del Guardia para saber cuando permitir el acceso.

9. Colección Eventos

Eventos	
PK	id
FK	condominioId
FK	guardUid
FK	residentUid
	residentName
	residentTower
	residentUnit
	description
	status
	timestamp

Figura 28: Colección Eventos

Fuente: Elaboración Propia

Constituye la Bitácora Digital del sistema. Es un registro histórico e inmutable.

Esta colección almacena una descripción textual del suceso, el tipo de evento, el estado final y la fecha exacta (timestamp).

Es la colección más interconectada, diseñada para auditorias. Relaciona cada evento con el Condominio (condominioId), el responsable (guardUid) y el afectado (residentUid), permitiendo generar reportes de seguridad cruzados y detallados.

3.3 Diseño de la Interfaz de Usuario (UI)

3.3.1 Vistas por Rol de Usuario

La aplicación adapta su interfaz dinámicamente según el rol de usuario autenticado. A continuación, se detallan las vistas principales para cada perfil:

A. Perfil Residente

El diseño de la interfaz para el residente se centra en la autogestión y la inmediatez. La navegación se estructura mediante una barra inferior con cinco secciones clave, permitiendo al usuario acceder a las funciones críticas con un solo toque.

1. **Visita de Inicio:** Es el centro de control de la aplicación. Su objetivo es ofrecer un resumen rápido del estado de la vivienda y accesos directos a las tareas más frecuentes.
 - **Estado General:** En la parte superior, se visualizan métricas clave como la cantidad de vehículos registrados, número de visitas programadas para el día en curso y cantidad de pases que se encuentran activos.
 - **Acciones Rápidas:** Botones prominentes para “Generar Pase” y “Mis Visitas”, diseñados para ser accesibles en un solo clic.
 - **Próximas Llegadas:** Una lista cronológica que muestre las visitas autorizadas próximas a ingresar, permitiendo al residente estar atento sin necesidad de navegar a otra pantalla.



Figura 29: Vista de Inicio en la aplicación del Residente.
Fuente: Elaboración Propia

2. Vista Generar Pase: Esta sección permite la creación de autorizaciones temporales para invitados. Se diseñó un formulario simplificado para minimizar el tiempo de interacción.

- Ingreso de Datos: El residente completa campos básicos de la visita (nombre, Rut, fecha y hora de la visita).
- Generación: Al apretar el botón, el sistema genera automáticamente un código QR único.
- Compartir: La interfaz incluye un botón para poder compartir el pase directamente al invitado.

The screenshot shows the 'Mi Condominio - Residente' app interface. At the top, there's a title bar with the text 'Mi Condominio - Residente' and a bell icon. Below this, the section is titled 'Nuevo pase de visita'. It contains several input fields: 'Nombre del visitante', 'Apellido del visitante', 'RUT (opcional)', and 'Teléfono (opcional)'. There is a toggle switch for '¿Ingresa con vehículo?' which is currently turned off. Below the toggle, it shows 'Llegada: 21/11 17:50' and a 'Cambiar' button with a calendar icon. A large blue button labeled 'Generar pase' with a QR code icon is positioned below the arrival information. At the bottom, there is a navigation bar with five icons: 'Inicio' (house), 'Generar' (QR code), 'Visitas' (calendar), 'Vehículos' (car), and 'Cuenta' (person).

Figura 30: Vista para generar un pase de Visita en la interfaz del Residente.
Fuente: Elaboración Propia

3. Vista Mis Visitas: Funciona como una bitácora personal para el residente, permitiéndole gestionar y auditar los ingresos a su propiedad.
- Listado Cronológico: Muestra todas las invitaciones creadas, ordenadas por fecha.
 - Indicadores de Estado: Cada tarjeta incluye una etiqueta visual que cambia de color según el estado del pase: "Programada" (Azul), "Autorizada" (Verde) o "Expirada" (Gris). Esto otorga feedback inmediato sobre quién ha llegado.

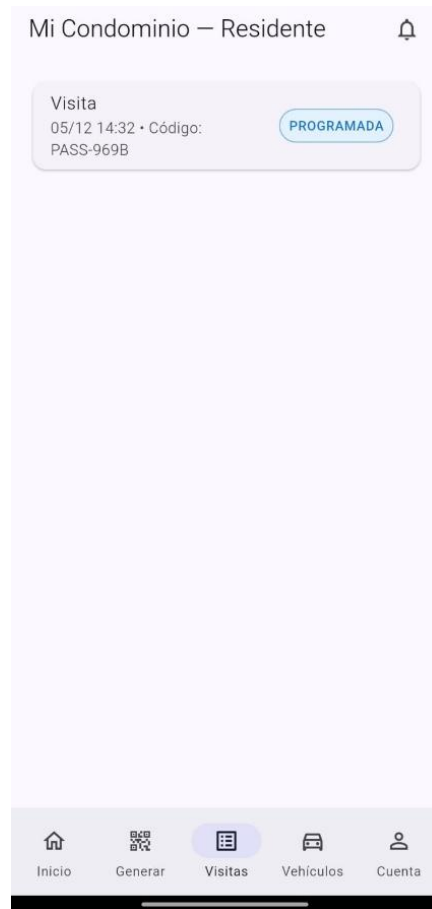


Figura 31: Vista para visualizar las próximas visitas en la interfaz del Residente
Fuente: Elaboración Propia

4. Visita Vehículos: Módulo dedicado a la gestión del acceso vehicular automatizado (LPR).
- Registro de Patentes: Permite al residente ingresar la patente del vehículo y descripción del vehículo (opcional).
 - Al guardar un vehículo, la información se actualiza instantáneamente en la base de datos del condominio, habilitando para que se pueda reconocer la patente para el ingreso.
 - Gestión: El usuario puede eliminar vehículos antiguos o agregar nuevos de forma autónoma.

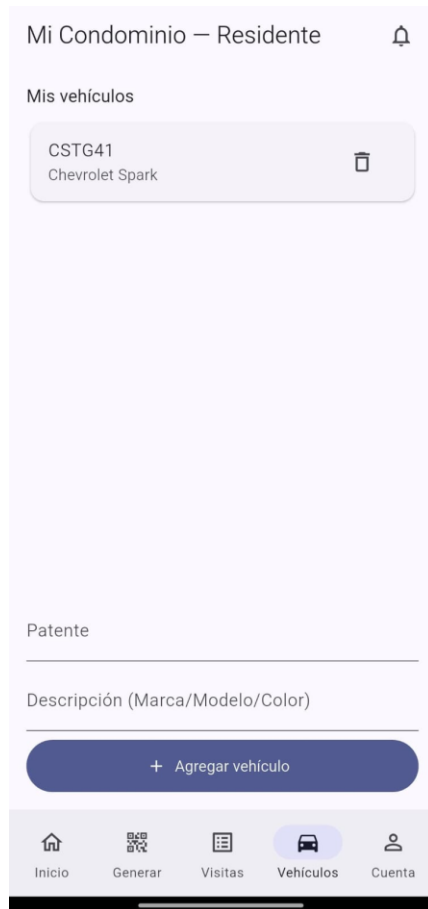


Figura 32: Vista para agregar/eliminar mis vehículos como Residente
Fuente: Elaboración Propia

5. Vista Cuenta: Es el panel de la administración del perfil, donde convergen las funcionalidades más avanzadas del sistema.
- Datos personales: Visualización de la información del residente y su unidad asignada.
 - Grupo Familiar: Sub-módulo crítico que permite agregar a otros habitantes de la vivienda. Cada miembro listado cuenta con un indicador de estado para su registro biométrico.
 - Biometría Facial: Desde aquí, el residente puede registrar su propio rostro utilizando la cámara del celular. El sistema valida la calidad de la imagen antes de enviarla al motor de reconocimiento (AWS).
 - Notificaciones: Interruptores (Switches) para activar o desactivar alertas por correo electrónico o notificaciones push al celular.
 - En esta vista también se va a poder cerrar sesión de forma segura.

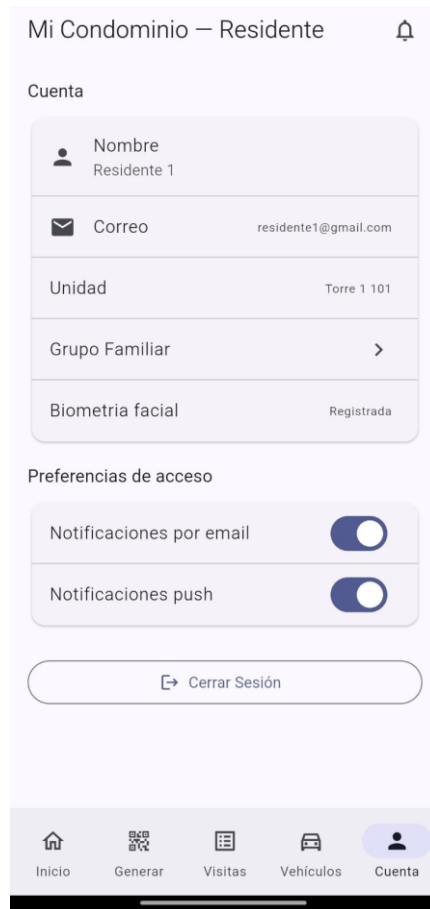


Figura 33: Vista de Cuenta en la interfaz del Residente
Fuente: Elaboración Propia

B. Perfil Guardia

La interfaz diseñada para el perfil de Guardia o Conserje prioriza la operatividad y la rapidez de respuesta. Dado que el usuario puede estar de pie o en movimiento, la navegación se simplificó en una barra inferior con cuatro módulos esenciales, eliminando menús complejos.

1. Vista Verificar: Esta es la pantalla principal de operación. Su diseño es minimalista y presenta tres botones de gran tamaño, claramente diferenciados por íconos, que activan los distintos mecanismos de validación tecnológica:
 - Escanear QR Visita: Activa la cámara para leer los códigos digitales presentados por las visitas. Luego escanear el QR se mostrará un mensaje si es válido o si ha expirado/es inválido.
 - Verificar Patente: Botón enfocado en el acceso vehicular. Al seleccionarla, el guardia debe apuntar con la cámara a la placa del vehículo; el sistema extrae el texto mediante OCR y consulta

a la base de datos para autorizar el ingreso si el vehículo está registrado.

- **Verificar Rostro:** Utilizada para el acceso peatonal de residentes o familiares sin llaves. Captura una imagen facial y, tras el análisis biométrico en la nube, devuelve la identidad de la persona y su unidad de residencia.

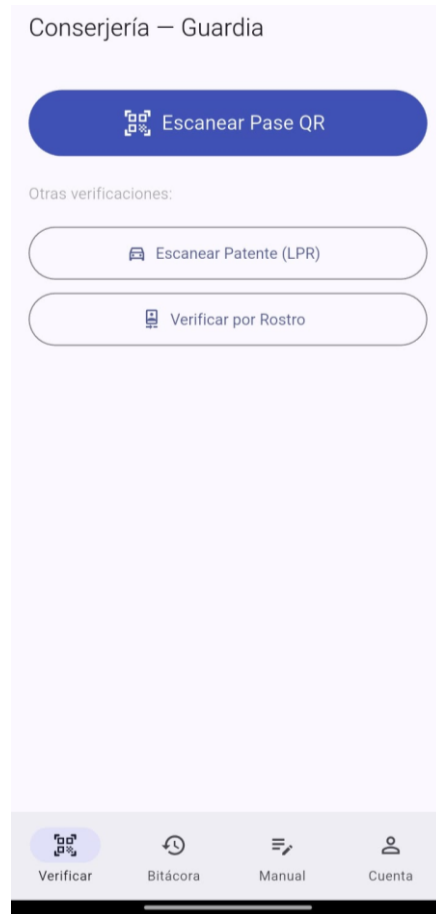


Figura 34: Vista de verificaciones en la interfaz del Guardia.

Fuente: Elaboración Propia

2. **Vista Bitácora:** Este módulo reemplaza el tradicional libro de actas físico. Funciona como un registro de auditoría en tiempo real que aumenta la transparencia de la operación.

- **Historial de Eventos:** Muestra una lista cronológica de todas las acciones realizadas (ingresos autorizados, rechazos, notificaciones enviadas). Cada evento incluye la hora exacta, el tipo de validación y el nombre del residente asociado.
- **Filtros Inteligentes:** Para facilitar la búsqueda de información, se incorporó un filtro por "Residente". Esto permite al guardia

revisar rápidamente el historial de accesos de una unidad específica en caso de reclamos o dudas, sin tener que revisar todo el listado general.



Figura 35: Vista de Bitácora Digital en la interfaz del Guardia
Fuente: Elaboración Propia.

3. Vista Manual: Diseñada para resolver si es que hay una “visita no anunciada” o proveedores sin pase QR.
 - Búsqueda de Unidad: Mediante listas desplegables de Torres y Departamentos, el guardia selecciona la unidad de destino, evitando errores de escritura manual.
 - Sistema de notificación: Al ingresar el nombre del visitante y presionar “Notificar Visita”, la interfaz entra en un estado de “Esperando Respuesta...”. Durante ese lapso, el sistema bloquea nuevas acciones hasta recibir la aprobación o rechazo del residente en tiempo real, eliminado la necesidad de llamar por citófono.

Conserjería – Guardia

Búsqueda de Residente

Seleccionar Torre ▼

Seleccionar Unidad/Residente

Busca por número... ▼

Nombre del Visitante

Notificar Visita

✓ Registrar Acceso Manual (Sin aviso)

Verificar Bitácora Manual Cuenta

Figura 36: Vista para notificar Visita en la interfaz del Guardia.
Fuente: Elaboración Propia

4. Vista Cuenta: Módulo administrativo personal para el guardia.

- Información del Guardia: Muestra los datos del usuario autenticado.
- Cierre de Sesión: Botón para cerrar sesión de forma segura y para prevenir que otro guardia ocupe esta cuenta para quitar responsabilidad en eventos que ocurran.

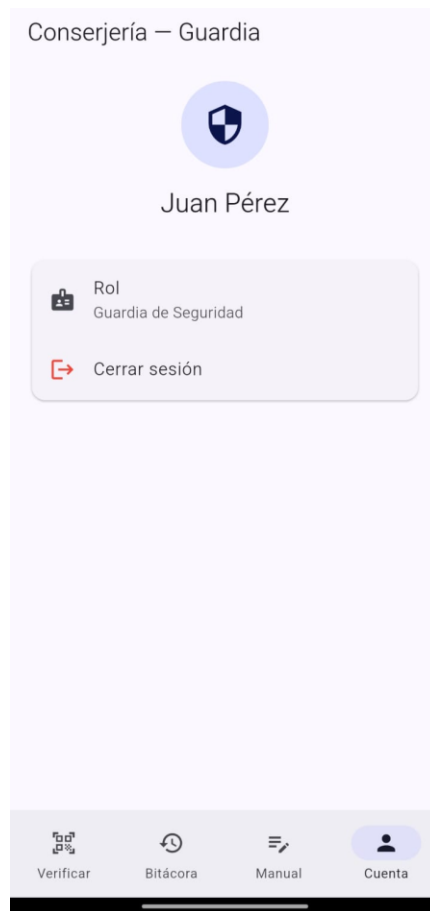


Figura 37: Vista de cuenta en la interfaz del Guardia
Fuente: Elaboración Propia

C. Perfil Administrador

Este perfil actúa como el panel de control del sistema. Su interfaz está diseñada para la gestión estratégica, la supervisión de la seguridad y la configuración global del condominio. La navegación se organiza en cinco módulos clave a través de la barra inferior.

1. Vista Dashboard: Es la pantalla de aterrizaje del administrador, diseñada para ofrecer una vista instantánea del estado de la comunidad.
 - Métricas en Tiempo Real: Se presentan tarjetas que resumen los datos operativos más relevantes: Cantidad total de Residentes Activos, Cantidad de Guardias Registrados, Total de Vehículos registrados para el acceso LPR y Visitas programadas activas para el día.

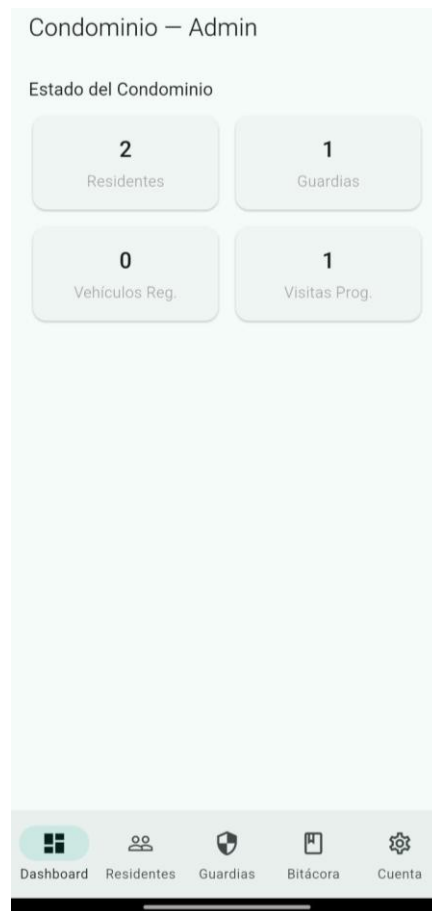


Figura 38: Vista de Dashboard en la interfaz del Administrador
Fuente: Elaboración Propia.

2. Vista Gestión de Residentes: Este módulo centraliza el directorio digital de la comunidad.
 - Listado de Usuarios: Muestra una lista de todos los residentes asociados al condominio, diferenciando entre aquellos que ya completaron su registro y aquellos que tienen una "Invitación Pendiente"
 - Sistema de Invitaciones: En la parte inferior, un botón flotante que permite "Invitar Residente". Al ingresar los datos básicos (Nombre, Correo, Numero de Residencia), el sistema guarda esta invitación dentro de la colección "Residentes" con un estado "Pendiente" para que este usuario luego active su cuenta dentro de la aplicación

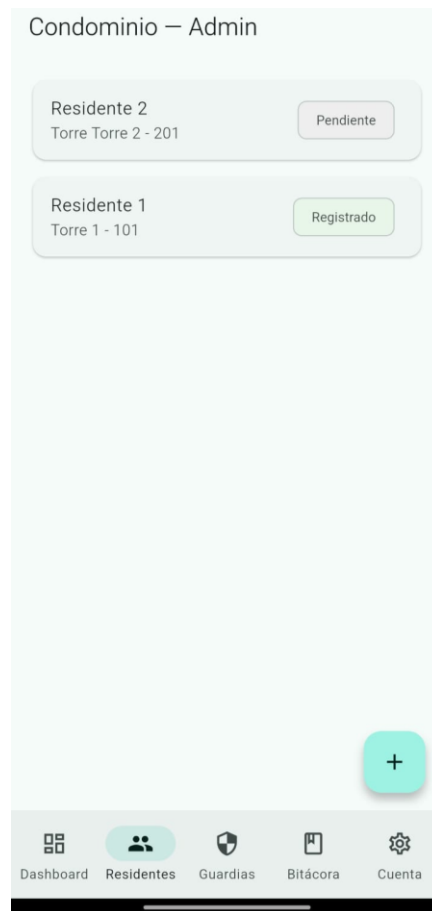


Figura 39: Vista para invitar y visualizar residente en la interfaz del Administrador
Fuente: Elaboración Propia

3. Vista Gestión de Guardias: Funciona de manera análoga a la gestión de residentes, pero enfocada en el personal de seguridad.
 - Control de dotación: Permitir al administrador dar de alta o baja a los guardias. Esto es crítico para la seguridad en el caso de que un guardia sea despedido, el administrador puede revocar su acceso inmediatamente desde esta vista, impidiendo que siga operando dentro de la aplicación
 - Invitación de Personal: Se repite el mismo paso que la invitación al residente, pero esta se guarda dentro de la colección "Guardias", para que, a posterior, este active su cuenta.

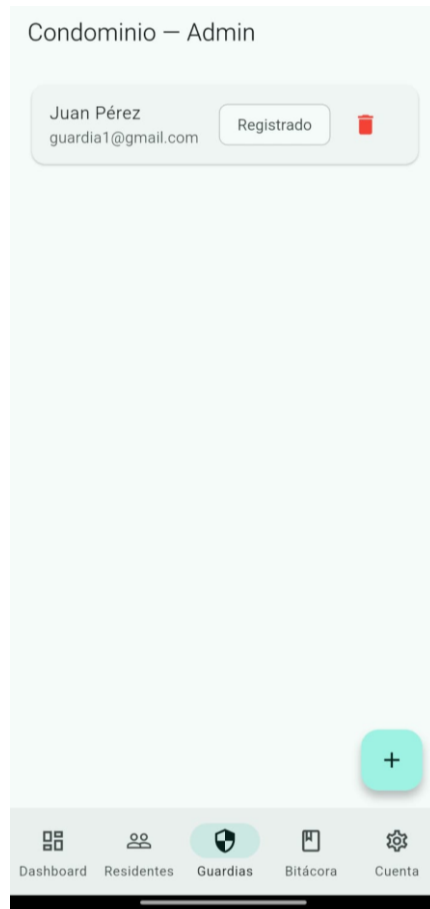


Figura 40: Vista para invitar, visualizar y eliminar guardias en la interfaz del Administrador

Fuente: Elaboración Propia.

4. Vista Bitácora: Es la herramienta para poder visualizar y poder auditar los eventos que ocurran dentro del entorno residencial.
 - Registro Inmutable: Muestra la totalidad de los eventos generados en el sistema.
 - Filtros Avanzados: Incluye un selector de "Residente" que permite filtrar los eventos a este residente en específico.



Figura 41: Vista de Bitácora Digital en la interfaz del Administrador
Fuente: Elaboración Propia

5. Vista Cuenta: Más allá de mostrar la información básica del administrador y del condominio, esta vista alberga la funcionalidad de Configuración Modular lo cual es importante para modificar según las políticas del condominio.
 - Panel de Módulos: Una sección dedicada llamada "Configuración del Condominio" presenta interruptores (Switches) para cada tecnología de validación: Biometría Facial, Acceso vehicular, Notificaciones para Visitas no Anunciadas.
 - Al modificar cualquiera de estos interruptores, la interfaz de las aplicaciones de todos los residentes y guardias se reconfiguran automáticamente, ocultando o mostrando los botones correspondientes. Esto otorga al administrador el control total sobre la política de seguridad del recinto.

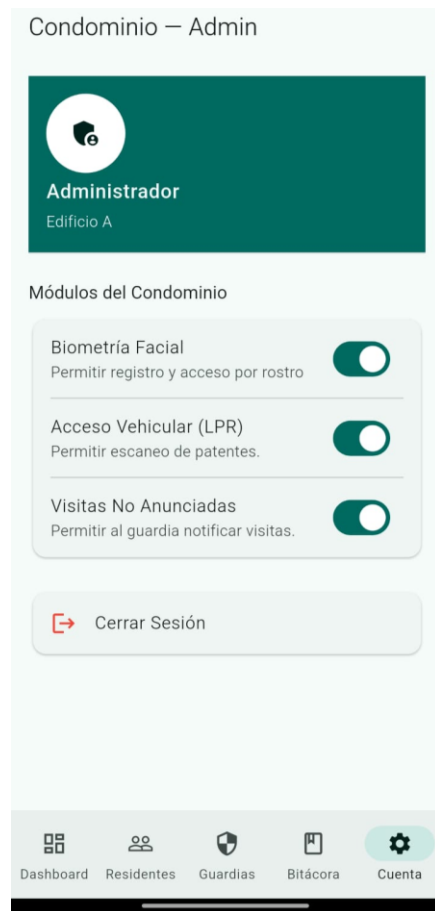


Figura 42: Vista de Cuenta y Configuración de módulos en la interfaz del Administrador
Fuente: Elaboración Propia.

3.4 Modelo de Seguridad y Privacidad de Datos

La seguridad de la información es un pilar fundamental en un sistema de control de acceso, residencial, dado que se gestionan datos altamente sensibles como patrones de movimiento, identidades familiares y registros biométricos.

3.4.1 Autenticación y Control de Acceso

El sistema no almacena credenciales de usuario (contraseña) en su propia base de datos, delegando esta responsabilidad a Firebase Authentication, un proveedor de identidad federada certificado.

Para la gestión de sesiones, se utilizan *JSON Web Tokens* (JWT) de corta duración (1 hora) que se renuevan automáticamente mediante *refresh tokens*. Esto asegura que, si un dispositivo es comprometido, el acceso pueda ser revocado remotamente invalidando el token.

La aplicación implementa un control de acceso estricto basado en el rol de usuario (Guardia, Residente, Administrador). Esta lógica se refuerza tanto en la interfaz de usuario (ocultando botones) como en el backend (reglas de base de datos), impidiendo, por ejemplo, que un residente acceda a la bitácora general del condominio.



Figura 43: Servicio de autenticación y gestión de usuarios Firebase Authentication
Fuente: LibreríasJS

3.4.2 Seguridad en la Base de Datos

A diferencia de las bases de datos tradicionales protegidas por un firewall perimetral, *Firestore* es accesible directamente desde el cliente móvil. Por

ello, la seguridad se implementa Reglas de Seguridad (*Security Rules*) que evalúan cada solicitud de lectura o escritura antes de procesarla.

Se implementarán las siguientes políticas de acceso:

1. Se implementa una regla lógica donde ``resource.data.adminUid == request.auth.token.adminUid'`. Esto garantiza que un guardia o residente solo pueda leer documentos que pertenezcan a su propio condominio, haciendo que sea imposible acceder a datos de otras comunidades.
2. Los documentos de la colección 'Residentes' tienen permisos de lectura restringidos. Un residente solo puede leer y escribir en su propio perfil (``uid == auth.uid'`), protegiendo su información personal y la de su grupo familiar frente a otros vecinos.
3. La colección 'Eventos' permite la creación de documentos (*create*) por parte de los guardias autenticados, pero deniega explícitamente cualquier intento de modificación (*update*) o eliminación (*delete*). Esto asegura que la bitácora sea un registro inmutable y fidedigno para auditorías.

3.4.3 Protección de Datos Sensibles y Biometría

El tratamiento de datos biométricos faciales cumple con los estándares de privacidad mediante una arquitectura de "Mínimo Privilegio" y almacenamiento efímero.

Todas las comunicaciones entre la aplicación móvil, Firebase y AWS se realizan a través de canales cifrados con TLS 1.2+ (*Transport Layer Security*), protegiendo las imágenes y datos contra ataques de interceptación (*Man-in-the-Middle*).

Las fotografías capturadas por el guardia para la verificación facial no se almacenan permanentemente en el dispositivo móvil ni en la base de datos del condominio. La imagen se envía como un flujo de bytes de *AWS Rekognition*, el cual devuelve un vector matemático (FaceID). La imagen original es descartada de la memoria inmediatamente después del procesamiento, cumpliendo con el principio de minimización de datos.

Los datos almacenados en los servidores de *Google Cloud (Firestore)* y *Amazon (AWS)* se encuentran cifrados en reposo utilizando el estándar AES-256, protegiendo la información física en los centros de datos.

CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN

4.1 Validación Funcional (Matriz de Pruebas)

Para validar el correcto funcionamiento del sistema en un entorno operativo real, se ejecutó un plan de pruebas integral en Condominio Peumayen Sur.

El proceso conto con la participación de actores del entorno residencial: un trabajador con el rol de conserje/guardia para las pruebas de operación y un residente de la comunidad, quién validó los flujos de autogestión y acceso. A continuación, se presenta la matriz de resultados obtenidos tras la ejecución de las pruebas.

Tabla 1: Matriz de Pruebas
Fuente: Elaboración Propia

ID	Módulo	Descripción del Caso de Prueba	Pasos Realizados	Resultado Esperado	Resultado Obtenido	Estado
CP-01	Acceso Vehicular	Verificación de Patente (LPR)	1. El guardia selecciona la opción "Escanear Patente". 2. Apunta la cámara a vehículo para capturar la patente	El sistema debe reconocer los caracteres, consultar la colección "Vehículos" y mostrar "Acceso Autorizado" junto a los datos del residente.	El sistema identifico la patente correctamente y desplegó el mensaje de autorización con el nombre y unidad del residente.	Aprobado
CP-02	Acceso Vehicular	Rechazo de Patente No Registrada	1. Guardia escanea un vehículo cuya patente no existe en la base de datos.	El sistema debe denegar el acceso e indicar el mensaje "Patente No Registrada".	Al verificar la patente desconocida, la aplicación mostró la alerta visual de "PATENTE NO REGISTRADA".	Aprobado
CP-03	Biometría	Verificación Facial de Residente	1. El guardia selecciona "Verificar Rostro" 2. Captura una fotografía del residente.	La imagen debe procesarse en AWS y retornar la identidad del usuario en un tiempo inferior a 3 segundos.	Se obtuvo el mensaje "ACCESO AUTORIZADO" desplegando los datos del residente en menos de 3 segundos.	Aprobado
CP-04	Biometría	Verificación de Grupo Familiar	1. Guardia selecciona "Verificar Rostro" 2. Captura una fotografía de una familiar previamente registrado.	El sistema debe identificar a la persona, clasificándola con el rol de "Familiar" vinculado a la unidad del residente.	El sistema mostró "ACCESO AUTORIZADO" indicando correctamente los datos del familiar asociado.	Aprobado.
CP-05	Visitas	Generación y Lectura de Pase QR	1. Residente genera y envía QR a la visita. 2. Guardia escanea el código QR presentado en portería.	El pase debe ser validado, cambiando su estado de "Programado" a "Autorizado" en la base de datos.	Al escanear se validó el código, mostró el nombre del visitante y actualizo a "Autorizado" exitosamente.	Aprobado
CP-06	Visitas	Notificación de Visita No Anunciada	1. Guardia envía notificación al Residente. 2. Residente presiona "Aprobar" en su dispositivo.	El residente debe recibir una Push Notification. La pantalla del guardia debe actualizarse sola.	La notificación fue recibida en el dispositivo móvil. Al seleccionar la opción "Aprobar", la interfaz del guardia cambia	Aprobado

					automáticamente su estado.	
CP-07	Configuración	Gestión de Módulos	1. El Administrador desactiva "Biometría Facial" en su panel. 2. Se verifica la interfaz en los perfiles Guardia y Residente.	El botón "Verificar Rostro" debe desaparecer de la interfaz del guardia y el residente no podrá registrar nuevos rostros.	La opción de biometría se ocultó inmediatamente en ambas interfaces tras el cambio de configuración.	Aprobado
CP-08	Bitácora	Registro de Eventos y Filtros	1. Se realizan ingresos LPR, Facial y QR. 2. Se filtra la bitácora por un residente específico.	La bitácora debe registrar todos los eventos y el filtro debe mostrar solo los registros vinculados a la unidad seleccionada.	Los eventos se registraron cronológicamente y el filtro aisló correctamente la información del residente.	Aprobado.

4.1.1 Análisis de Resultado de las Pruebas Funcionales

A partir de la ejecución de la matriz de pruebas presentada en la tabla 1, es posible concluir que la primera versión desarrollada cumple satisfactoriamente con los requerimientos críticos definidos en el alcance del proyecto.

Se destacan los siguientes hallazgos técnicos:

1. El sistema demostró una interoperabilidad robusta entre el procesamiento local (*On-Device*) utilizado para lectura de patentes (LPR) y los servicios en la nube para la biometría facial (AWS). Ambos módulos arrojaron resultados positivos con tiempos de respuesta adecuados para la operación en portería.
2. Las pruebas de gestión de visitas (CP-05 y CP-06) validaron la arquitectura basada en eventos de Firestore. La capacidad del sistema para actualizar la interfaz del guardia instantáneamente cuando un residente aprueba una visita remota elimina la necesidad de llamadas telefónicas, cumpliendo con el objetivo de eficiencia operativa.
3. Las pruebas de rechazo (CP-02) y configuración (CP-07) confirmaron que el sistema prioriza la seguridad, bloqueando accesos no autorizados y permitiendo al administrador restringir funcionalidades (como la biometría) en tiempo real sin necesidad de reinstalar la aplicación.

4.2 Validación Comparativa: Eficiencia Operativa

El estudio comparativo de eficiencia se llevó a cabo en el acceso principal del Condominio Peumayen Sur. Las mediciones se realizaron contrastando el procedimiento manual actual del recinto frente al uso del prototipo propuesto, bajo condiciones normales de operación.

El objetivo de esta validación es cuantificar la reducción de tiempos de espera y la eliminación de pasos burocráticos en los accesos.

4.2.1 Metodología de la Prueba

Se definieron dos escenarios de uso frecuentes en una portería. Para cada escenario, se cronometra el tiempo total del proceso, desde que el vehículo/peatón se detiene frente al guardia hasta que se autoriza su ingreso.

1. Primer escenario: Ingreso de Visita (QR)

Tabla 2: Comparación de pasos para el ingreso de visita (Manual vs Sistema QR)

Fuente: Elaboración Propia

Pasos	Modelo Manual	Modelo Propuesto (App con QR)
1	Visita se detiene e indica edificio/casa a visitar.	Visita se detiene y muestra código QR.
2	Guardia se contacta con el residente a través de mensaje de Whatsapp.	Guardia escanea el QR con la App.
3	Guardia recibe la respuesta del residente para autorizar el ingreso.	Sistema valida y registra evento en bitácora.
4	Guardia abre puerta de acceso.	Guardia abre puerta de acceso.

2. Segundo escenario: Ingreso de Visita (No anunciada).

Tabla 3: Comparación de pasos para el ingreso visita (Manual vs Notificación en App)

Fuente: Elaboración Propia

Pasos	Modelo Manual	Modelo Propuesto (Notificación en la App)
1	Visita se detiene e indica edificio/casa a visitar.	Visita se detiene y le entrega información de donde desea visitar.

2	Guardia se contacta con el residente a través de mensaje de Whatsapp.	Guardia ingrese los datos y presiona "Notificar".
3	Guardia recibe la respuesta del residente para autorizar el ingreso.	Sistema envía notificación al residente y este la aprueba.
4	Guardia abre puerta de acceso.	Sistema registra evento en bitácora.
5		Guardia abre puerta de acceso.

3. Tercer escenario: Ingreso de Residente Vehicular

Tabla 4: Comparación de pasos ingreso vehicular (Manual vs App con LPR)

Fuente: Elaboración Propia

Pasos	Modelo Manual	Modelo Propuesto (App con LPR)
1	Vehículo se detiene y guardia observa el conductor.	Vehículo se aproxima y Guardia apunta con la cámara.
2	Guardia intenta reconocer al residente o vehículo	Sistema lee la patente y busca en la base de datos.
3	Si hay duda, Guardia solicita bajar el vidrio.	Sistema valida el vehículo y se registra en bitácora.
4	Guardia abre barrera de acceso.	Guardia abre barrera de acceso.

4.2.2 Resultados Cuantitativos

A partir de las mediciones realizadas en terreno, se obtuvieron los tiempos promedios de operación para cada escenario. A continuación, se presenta la tabla comparativa entre el método manual actual y el uso de la aplicación propuesta.

Tabla 5: Comparativa de Tiempos de Operación (Manual vs App)

Fuente: Elaboración Propia

Escenario	Tiempo Promedio Manual	Tiempo Promedio App	Reducción de Tiempo	Observaciones
Ingreso Visita (QR)	2:10 min (130 segundos)	9,64 segundos	92,5%	El proceso se reduce a un solo escaneo.
Visita No Anunciada	2:10 (130 segundos)	80,0 segundos	38,4%	Elimina la espera de respuesta por WhatsApp/Citófono, además queda

				registro de quién entra
Ingreso Vehicular (LPR)	24,45 seg	19,0 segundos	22,2%	Diferencia crítica: El tiempo manual no incluye registro en bitácora, mientras que la App si registra el evento.

4.2.3 Análisis de Resultados

Los datos obtenidos demuestran una optimización significativa en los tres flujos operativos, destacando las siguientes conclusiones técnicas y funcionales:

- El escenario con mayor impacto es el ingreso mediante Código QR, logrando una reducción de tiempo del 92,5%. El cambio de un proceso asíncrono (esperar respuesta mediante WhatsApp o citófono) a uno síncrono (validación inmediata), permitiendo un flujo continuo sin la necesidad de necesitar una validación del residente.
- En el caso de visitas no anunciadas, aunque el tiempo es mayor que con QR (80 segundos), sigue siendo un 38,4 más rápido que el método manual. La notificación Push directa al residente resulta más efectiva que la coordinación telefónica o por mensajería informal, permitiendo también mantener un registro en bitácora al realizar el evento.
- En el ingreso vehicular, la diferencia de tiempo parece menor en comparación a los otros escenarios. Sin embargo, este dato esconde una mejora fundamental.
En el método manual el guardia solo realizar una validación visual y abre la barrera, al realizar esto no queda un registro del ingreso, lo que genera un “punto ciego” de seguridad. En cambio, con la validación vía app, el sistema no solo valida la patente, sino que crea automáticamente un registro inmutable en bitácora digital. Por lo tanto, la aplicación es más rápida y, a la vez, genera trazabilidad de seguridad que el método manual no posee.

4.2.4 Conclusión de la Validación Operativa

La solución propuesta valida la hipótesis de eficiencia operativa. La implementación del sistema no solo reduce los tiempos de espera promedio, mitigando el riesgo de seguridad en el acceso, sino que garantiza la integridad de los datos al registrar el 100% de las interacciones en la nube, algo que el procedimiento manual actual sacrifica en favor de la velocidad.

4.3 Validación de Usabilidad (Experiencia de Usuario)

La usabilidad de la primera versión fue evaluada utilizando el cuestionario estandarizado *System Usability Scale (SUS)*. Este método permite obtener una medida rápida y robusta de la satisfacción del usuario respecto a la interfaz y funcionalidad del sistema. El puntaje final oscila entre 0 y 100 donde puntajes sobre 70 son considerados aceptables.

4.3.1 Metodología y Participantes

Para la evaluación de usabilidad, se utilizó un muestreo por conveniencia seleccionado a un total de 10 participantes, divididos en dos grupos representativos para cubrir los roles críticos del sistema:

1. Grupo Guarda: Compuesto por personas con experiencia laboral en servicios de conserjería. Este criterio aseguró que la validación operativa fuera realizada por usuarios que estén familiarizados con la dinámica real de una portería.
2. Grupo Residente: Compuesto por habitantes actuales de condominios o edificios, quienes evaluaron las funcionalidades de autogestión desde la perspectiva del usuario final.

El instrumento de evaluación se aplicó de manera digital a través de la plataforma Google Forms inmediatamente después de que los usuarios interactuaron con el prototipo funcional, garantizando que las respuestas reflejaran su experiencia directa con la interfaz.

Tabla 6: Tareas asignadas para encuesta SUS
Fuente: Elaboración Propia

Rol Evaluado	Participantes	Tareas Asignadas
Guardia	5	Escanear QR, usar escáner LPR, validar rostro, enviar notificación de visita, revisar historial de bitácora.
Residente	5	Registrar vehículo, generar pase de visita (QR), compartir código QR, registrar rostro.

Los participantes fueron instruidos para calificar diez afirmaciones en una escala de *Likert* de 5 puntos (1: Totalmente en Desacuerdo a 5: Totalmente de Acuerdo) después de completar las tareas asignadas a su rol.

4.3.2 Cálculo y Resultados del Cuestionario SUS

El puntaje individual de cada encuestado se calcula mediante una fórmula que normaliza las respuestas a las 10 preguntas. Las preguntas impares (positivas) se puntúan como $P-1$, y las preguntas pares (negativas) como $5-P$ (donde P es la puntuación dada por el usuario). El resultado de la suma de estos valores se multiplica por 2.5 para obtener el puntaje final sobre 100.

A continuación, se presentan los ítemas evaluados en la escala SUS. Las respuestas se encuentran tabuladas posteriormente utilizando la referencia numérica.

Cuestionario Aplicado:

- **P1:** Creo que me gustaría usar este sistema con frecuencia.
- **P2:** Encontré el sistema innecesariamente complejo.
- **P3:** Me pareció que el sistema fue fácil de usar.
- **P4:** Creo que necesitaría del apoyo de un técnico para usar este sistema.
- **P5:** Encontré que las diversas funciones del sistema estaban bien integradas.
- **P6:** Me pareció que había demasiada inconsistencia en el sistema.
- **P7:** Imagino que la mayoría de la gente aprendería a usar este sistema muy rápidamente.
- **P8:** Encontré el sistema muy engorroso (torpe/incómodo) de usar.
- **P9:** Me sentí muy confiado al usar el sistema.
- **P10:** Necesité aprender muchas cosas antes de poder empezar a usar este sistema.

A. Puntaje SUS para el Rol Guardia

Tabla 7: Puntaje SUS Guardia
Fuente: Elaboración Propia

Participante	G1	G2	G3	G4	G5	Puntaje promedio del Rol
P1	5	5	5	5	4	4.8
P2	1	1	1	1	1	1
P3	5	5	5	5	5	5
P4	1	1	1	1	2	1.2
P5	4	4	5	4	4	4.2
P6	1	1	1	1	1	1

P7	4	4	5	5	5	4.6
P8	1	1	1	1	1	1
P9	5	5	5	4	4	4.6
P10	2	1	1	1	1	1.2
Puntaje Total	37	38	40	38	36	37.8
Puntaje SUS	92.5	95	100	95	90	94.5

B. Puntaje SUS para el Rol Residente

Tabla 8: Puntaje SUS Residente
Fuente: Elaboración Propia

Participante	R1	R2	R3	R4	R5	Puntaje promedio del Rol
P1	5	5	5	4	5	4.8
P2	1	1	1	2	1	1.2
P3	4	5	5	5	4	4.6
P4	1	1	1	1	1	1
P5	4	4	5	4	4	4.2
P6	1	1	1	1	2	1.2
P7	4	3	5	4	5	4.2
P8	1	1	1	1	1	1
P9	5	5	5	4	4	4.6
P10	1	1	1	2	1	1.2
Puntaje Total	37	37	40	34	35	36.6
Puntaje SUS	92.5	92.5	100	85	87.5	91.5

4.3.3 Análisis e Interpretación de Resultados

El resultado global del sistema es de 93.0 puntos SUS, lo que sitúa a la primera versión de la aplicación en la categoría de usabilidad “Excelente”. Este puntaje supera con creces el umbral de aceptabilidad de 70.

Para el rol del Guardia, el puntaje SUS es de 94.5, lo que quiere decir que la usabilidad percibida por los guardias fue extremadamente alta. Esto se debe, en gran medida, a la simplicidad del flujo de trabajo, que se centra en tareas críticas y claras (escanear, verificar). Las respuestas a las preguntas negativas como por ejemplo "Encontré el sistema innecesariamente complejo, fueron consistentemente bajas, indicando que la interfaz para escanear y realizar las validaciones es intuitiva y rápida de aprender.

En el caso del rol de Residente, su puntaje (91.5 puntos SUS), aunque fue ligeramente inferior al rol del Guardia, el puntaje de usabilidad es excelente. Esto valida que las funciones de autogestión, como el registro de un vehículo y la generación de pases QR, son fáciles de completar. El puntaje en la pregunta 7 ("Imagino que la mayoría de la gente aprendería a usar este sistema rápidamente") fue alto, lo que confirma el diseño minimalista de la aplicación para el usuario.

El resultado demuestra que la aplicación es altamente usable y que los usuarios de ambos perfiles pueden interactuar con las funciones de seguridad avanzada (LPR y Biometría) sin necesidad de un apoyo constante, cumpliendo así con uno de los objetivos de diseño de ser una solución intuitiva y fácil de adaptar en un entorno operativo real.

CAPÍTULO 5: CONCLUSIONES

Este proyecto se concibe como una solución tecnológica integral para enfrentar uno de los desafíos más apremiantes en la realidad nacional: la inseguridad en los accesos residenciales y la vulnerabilidad frente a delitos violentos como “portonazos”. La aplicación propuesta integra tecnologías de vanguardia en un diseño centralizado en la usabilidad, atendiendo las necesidades de seguridad y eficiencia de las comunidades de manera simple y efectiva.

La propuesta nació a causa del aumento en la percepción de inseguridad y la obsolescencia de los métodos manuales de control en condominios y edificios. De ahí, la idea creció buscando aumentar la eficiencia operativa y la tranquilidad de los residentes frente a situaciones de ingreso y salida. La aplicación sugiere una respuesta inmediata mediante la automatización, reemplazando la subjetividad humana con validaciones biométricas y lectura de patentes en tiempo real, asegurando que solo las personas autorizadas puedan acceder al recinto.

La investigación y desarrollo se centró en gran medida en la integración de servicios cognitivos de Inteligencia Artificial (LPR y Reconocimiento Facial) en dispositivos móviles estándar. Esto es una parte esencial del proyecto, ya que se busca democratizar la seguridad avanzada sin obligar a las comunidades a invertir en costosa infraestructura industrial, garantizando un control robusto desde el teléfono del guardia.

Se ha dedicado un gran esfuerzo en crear una apariencia de la aplicación simple, intuitiva y amigable. El diseño se enfoca principalmente en la facilidad y accesibilidad para el usuario, asegurando que tanto guardias como residentes de todas las edades puedan utilizarla sin mayores problemas. Se pensó bastante en que los flujos de “Generar Pase” y “Validar Acceso” fueran directos, eliminando pasos innecesarios que pudieran generar congestión o fricción en la portería.

La creación de una arquitectura híbrida y escalable, que combina el procesamiento local (*on-device*) para la rapidez con la potencia de la nube para la precisión, ha sido el punto clave de este proyecto. Esta infraestructura no solo soporta la operación actual, sino que permite una futura implementación de nuevas tecnologías más avanzadas.

La protección y confidencialidad de la información es esencial para esta aplicación, debido a que se manipulan datos sensibles como rostros y patentes. Esto se consiguió haciendo uso de técnicas de encriptación y arquitecturas de “mínimo privilegio” en la nube, proporcionando una base

sólida para garantizar que la privacidad de los residentes esté resguardada bajo estándares modernos.

En el futuro, sería valioso investigar tecnologías nuevas que complementen la funcionalidad de la aplicación. La implementación de dispositivos IoT (Internet de las Cosas) para la apertura automática de barreras al momento de la validación sería un plus enorme para la automatización total. Asimismo, se podría enriquecer aún más la aplicación integrando cámaras externas de vigilancia que alimenten al sistema de reconocimiento y validación, o módulo de gestión comunitaria, transformando la herramienta en un ecosistema integral de vida en comunidad.

El progreso de esta investigación ha conseguido satisfacer los objetivos declarados, demostrando que es posible reducir drásticamente los tiempos de espera y aumentar la seguridad mediante software. Se busca aportar tranquilidad y evitar situaciones de riesgos en entornos residenciales, lo que esto será la base para llevar a cabo un cambio en la modernización de la seguridad residencial.

REFERENCIAS BIBLIOGRAFICAS

Amazon Web Services. (2025). ¿Qué es el reconocimiento facial? Recuperado de <https://aws.amazon.com/es/what-is/facial-recognition/>

Asana. (2025). ¿Qué es un diagrama de flujo? Recuperado de <https://asana.com/es/resources/what-is-a-flowchart>

Biblioteca del Congreso Nacional de Chile. (2025). DFL 1: Fija texto refundido, coordinado y sistematizado del Código Civil. Recuperado de <https://www.bcn.cl/leychile/navegar?idNorma=7193>

Biblioteca del Congreso Nacional de Chile. (2022). Ley Núm. 19.628: Sobre protección de la vida privada. Recuperado de <https://www.bcn.cl/leychile/navegar?idNorma=141599>

Biblioteca del Congreso Nacional de Chile. (2024). Ley Núm. 21.442: Aprueba nueva ley de copropiedad inmobiliaria. Recuperado de <https://www.bcn.cl/leychile/navegar?idNorma=1174663>

Cloudflare. (s.f). ¿Qué es el backend como servicio (BaaS)? Recuperado de <https://www.cloudflare.com/es-es/learning/serverless/glossary/backend-as-a-service-baas/>

Creately. (2023). Tutorial de diagrama de caso de uso. Recuperado de <https://creately.com/blog/es/diagramas/tutorial-diagrama-caso-de-uso/>

CyberHoot. (2019). Access Control (Physical and Logical). Recuperado de <https://cyberhoot.com/es/cybrary/access-control-physical-and-logical/>

IBM. (s.f.). ¿Qué es el reconocimiento óptico de caracteres (OCR)? Recuperado de <https://www.ibm.com/es-es/think/topics/optical-character-recognition>

Instituto Nacional de Estadísticas. (2024). Seguridad Ciudadana. Recuperado de <https://www.ine.gob.cl/estadisticas/sociales/seguridad-publica-y-justicia/seguridad-ciudadana>

TicNow. (s.f.). Autenticación digital: Cómo funciona y cuáles métodos existen. Recuperado de <https://ticnow.cl/autenticacion-digital-como-functiona-y-cuales-metodos-existen/>

UFM. (2024). Seguridad en Condominios: Guía Completa según la Ley 21.442. Recuperado de <https://ufm.cl/seguridad-en-condominios-guia-completa-segun-la-ley-21442/>

ANEXO

ANEXO A: Primera Versión App

Contiene la primera versión funcional de la aplicación móvil desarrollada en Flutter, incluyendo la estructura de carpetas, lógica de negocio y configuración de vistas.

1. GitHub con el código de la aplicación.

<https://github.com/benja14slq/AccessControlApp/tree/App>

Anexo B: Diagramas de Arquitectura y Diseño

Este anexo incluye el acceso a diagramas UML, flujos de proceso y esquemas de base de datos en formato digital.

1. Draw.io con los diagramas.

https://viewer.diagrams.net/?tags=%7B%7D&lightbox=1&highlight=0000ff&edit=blank&layers=1&nav=1&title=Diagrama%20sin%20t%C3%ADtulo.drawio&dark=0#Uhttps%3A%2F%2Fdrive.google.com%2Fuc%3Fid%3D1FtKOc2D_HvrNS0hsaZ4d5-pqKSNk-7vj%26export%3Ddownload