

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

APLICACIÓN MÓVIL UTILIZANDO FLUTTER PARA EL CONTROL DE INGRESO Y SALIDA DE ESTACIONES DE TRABAJO EN LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la Información

ÁREA: Base de datos y Sistemas informáticos.

LÍNEA DE INVESTIGACIÓN: Software, Tecnologías de la Información y Ciencia de Datos

AUTOR: Kevin Gabriel Pico Garzón

TUTOR: Ing. Franklin Oswaldo Mayorga Mayorga Mg.

Ambato – Ecuador

enero - 2026

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: APLICACIÓN MÓVIL UTILIZANDO FLUTTER PARA EL CONTROL DE INGRESO Y SALIDA DE ESTACIONES DE TRABAJO EN LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA, desarrollado bajo la modalidad Proyecto de Investigación por el señor Kevin Gabriel Pico Garzón, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, enero 2026



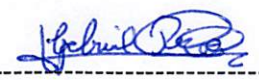
Ing. Franklin Oswaldo Mayorga Mayorga, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: APLICACIÓN MÓVIL UTILIZANDO FLUTTER PARA EL CONTROL DE INGRESO Y SALIDA DE ESTACIONES DE TRABAJO EN LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, enero 2026.



Kevin Gabriel Pico Garzón
C.C. 1803587987
AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, enero 2026.



Kevin Gabriel Pico Garzón

C.C. 1803587987

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Kevin Gabriel Pico Garzón, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado APLICACIÓN MÓVIL UTILIZANDO FLUTTER PARA EL CONTROL DE INGRESO Y SALIDA DE ESTACIONES DE TRABAJO EN LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con el señor Presidente del Tribunal.

Ambato, enero 2026.

Firmado electrónicamente por:
FRANKLIN OSWALDO MAYORGA MAYORGA
Validar únicamente con FirmaEC

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
OSCAR FERNANDO IBARRA TORRES
Validar únicamente con FirmaEC

Ing. Oscar Fernando Ibarra Torres, Mg.
PROFESOR CALIFICADOR

Firmado electrónicamente por:
MARCOS RAPHAEL BENITEZ ALDAS
Validar únicamente con FirmaEC

Ing. Marcos Raphael Benítez Aldás, MSc.
PROFESOR CALIFICADOR

DEDICATORIA

Dedico este trabajo a Dios, porque, a pesar de los tropiezos que tuve en el camino, siempre me dio la fortaleza necesaria para seguir adelante y nunca rendirme.

A mi madre, Janeth Amparo Garzón Ojeda, porque a pesar de mis errores siempre me dio su apoyo incondicional y ha estado conmigo en todo este proceso en las buenas y en las malas. Ha sido mi pilar fundamental para conseguir este logro.

A mi abuelita, María Zulay Ojeda Cifuentes, quien, a pesar de la distancia, nunca ha dejado de acompañarme con su cariño, sus palabras de ánimo y su apoyo constante, que han sido una motivación especial para mí.

A mi tío, Juan Miguel Garzón Ojeda, quien ha sido una presencia importante en mi vida, apoyándome con sus consejos, su confianza y su respaldo.

A mi papá, a quien agradezco profundamente por el apoyo que me ha brindado en toda esta etapa, por creer en mí y por acompañarme en cada paso hacia este objetivo.

AGRADECIMIENTO

A mis amigos Mateo, Munir, Daniel y Frank, por su apoyo constante durante todo este tiempo y por estar conmigo en cada momento importante. Gracias por cada experiencia compartida, por las risas, los consejos y la compañía que hicieron este camino más divertido y me siento agradecido de haberla vivido junto a ustedes.

Al Ing. Mg. Franklin Mayorga, mi tutor, por su guía profesional, su orientación clara y su disposición constante para compartir sus conocimientos. Su compromiso académico fue esencial para el desarrollo adecuado de este proyecto.

Al Ing. José Acán, por confiar en mi trabajo y brindarme el apoyo necesario para llevar a cabo esta investigación. Su disposición, apertura y acompañamiento no solo facilitaron el desarrollo del proyecto, sino que también me motivaron a dar lo mejor de mí en este proceso.

A la Universidad Técnica de Ambato, por ser el espacio donde consolidé mi formación profesional, brindándome una educación integral, recursos académicos de calidad y la oportunidad de crecer en lo personal y lo tecnológico.

ÍNDICE GENERAL DE CONTENIDOS

PORTADA ..... **i**

APROBACIÓN DEL TUTOR ..... **ii**

AUTORÍA ..... **iii**

DERECHOS DE AUTOR ..... **iv**

APROBACIÓN DEL TRIBUNAL DE GRADO ..... **v**

DEDICATORIA ..... **vi**

AGRADECIMIENTO ..... **vii**

ÍNDICE GENERAL DE CONTENIDOS ..... **viii**

ÍNDICE DE TABLAS ..... **xii**

ÍNDICE DE FIGURAS ..... **xvi**

ÍNDICE DE ANEXOS ..... **xx**

RESUMEN EJECUTIVO ..... **xxi**

ABSTRACT ..... **xxii**

CAPÍTULO I. MARCO TEÓRICO **1**

1.1 Tema de investigación 1

1.1.1 Planteamiento del problema 1

1.2 Antecedentes investigativos 2

1.3 Fundamentación teórica 5

1.3.1 Tecnologías de la información 6

1.3.2 Desarrollo de aplicaciones móviles 6

1.3.3 Flutter… 6

1.3.4 Patrón Modelo-Vista-Controlador 7

1.3.5 Aplicación móvil para control de acceso 7

1.3.6 Gestión Empresarial 8

1.3.7 Seguridad en aplicativos móviles 8

1.3.8 Privacidad y Cumplimiento Normativo 9

1.3.9 Arquitectura de Backend Seguro 10

1.4 Objetivos 10

1.4.1 Objetivo general 10

1.4.2 Objetivos específicos 10

CAPÍTULO II. METODOLOGÍA 11

2.1 Materiales 11

2.2 Métodos 16

2.2.1 Modalidad de la investigación 16

2.2.2 Población y muestra 17

2.2.3 Recolección de información 17

2.2.4 Procesamiento y análisis de datos 35

CAPÍTULO III. RESULTADOS Y DISCUSIÓN 38

3.1 Análisis de procesos 38

3.1.1 Modelado de procesos 38

3.1.2 Modelado de procesos optimizados 40

3.2 Framework Flutter para desarrollo móvil multiplataforma. 43

3.2.1 Ventajas y desventajas de Flutter 45

3.2.2 Casos de éxito utilizando Flutter 46

3.2.3 Comparativa de versiones 47

3.3 Gestor de Base de Datos 48

3.4 Metodología de Desarrollo Móvil 49

3.5 Desarrollo de la Propuesta 51

3.5.1 Exploración 52

3.5.2 Inicialización 57

3.5.3 Diseño de la aplicación móvil 60

3.5.4 Diagrama de Endpoints (API REST) 84

3.5.5 Producción 85

3.5.6 Estabilización 97

3.5.7 Pruebas. 98

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 120

4.1 Conclusiones 120

4.2 Recomendaciones 121

REFERENCIAS BIBLIOGRÁFICAS 122

ANEXOS 125

ÍNDICE DE TABLAS

Tabla 1. Cadenas de búsqueda en base de datos académicas y científicas. 3

Tabla 2. Búsqueda en el repositorio institucional UTA. 3

Tabla 3. Criterios de inclusión y exclusión. 4

Tabla 4. Guía de entrevista. 14

Tabla 5. Ficha de Observación. 15

Tabla 6. Población de estudio. 17

Tabla 7. Coeficiente alfa de Cronbach en la encuesta. 18

Tabla 8. Criterios de la escala de consistencia del alfa de Cronbach. 18

Tabla 9. Resultados de la pregunta 1. 19

Tabla 10. Resultados de la pregunta 2. 20

Tabla 11. Resultados de la pregunta 3. 21

Tabla 12. Resultados de la pregunta 4. 23

Tabla 13. Resultados de la pregunta 5. 24

Tabla 14. Resultados de la pregunta 6. 25

Tabla 15. Resultados de la pregunta 7. 26

Tabla 16. Resultados de la pregunta 8. 28

Tabla 17. Resultados de la pregunta 9. 29

Tabla 18. Resultados de la pregunta 10. 30

Tabla 19. Entrevista completa con el Gerente General. 31

Tabla 20. Ficha de Observación rellenada. 33

Tabla 21. Características de Flutter. 44

Tabla 22. Ventajas y desventajas de Flutter. 46

Tabla 23. Casos de éxito utilizando Flutter. 46

Tabla 24. Comparativa de versiones que constituye Flutter. 47

Tabla 25. Metodologías para desarrollo móvil. 50

Tabla 26. Interesados “stakeholders”. 52

Tabla 27. Requisitos funcionales de la aplicación móvil. 54

Tabla 28. Requisitos no funcionales. 55

Tabla 29. Planificación de fases de la metodología empleada. 59

Tabla 30. Esquemas y controladores. 86

Tabla 31. Endpoints establecidos en el backend. 88

Tabla 32. Diseño Storycards. 89

Tabla 33. Storycard Interfaz de Inicio de Sesión. 91

Tabla 34. Storycard panel rol Administrador. 91

Tabla 35. Storycard gestión de usuarios. 92

Tabla 36. Storycard asignación de dispositivos a usuario. 92

Tabla 37. Storycard dispositivos asignados y envío de solicitud. 93

Tabla 38. Storycard estado de las solicitudes, envío de notificación y reporte de estado de dispositivos. 94

Tabla 39. Storycard verificar salida o ingreso del equipo por escaneo de QR. 94

Tabla 40. Storycard visualización de reportes según rol. 95

Tabla 41. Storycard cambio de contraseña para todos los roles. 96

Tabla 42. Storycard integración del sistema de notificaciones push. 96

Tabla 43. Modificaciones en el desarrollo de la aplicación. 97

Tabla 44. Prueba de funcionalidad 1. 98

Tabla 45. Prueba de funcionalidad 2. 99

Tabla 46. Prueba de funcionalidad 3. 101

Tabla 47. Prueba de funcionalidad 4. 102

Tabla 48. Prueba de funcionalidad 5. 103

Tabla 49. Prueba de funcionalidad 6. 104

Tabla 50. Prueba de funcionalidad 7. 105

Tabla 51. Prueba de funcionalidad 8. 106

Tabla 52. Prueba de funcionalidad 9. 107

Tabla 53. Prueba de funcionalidad 10. 108

Tabla 54. Prueba de funcionalidad 11. 110

Tabla 55. Formato para pruebas de aceptación. 112

Tabla 56. Prueba de aceptación Storycard 1. 112

Tabla 57. Prueba de aceptación Storycard 2. 113

Tabla 58. Prueba de aceptación Storycard 3 – 4. 113

Tabla 59. Prueba de aceptación Storycard 5. 114

Tabla 60. Prueba de aceptación Storycard 6. 114

Tabla 61. Prueba de aceptación Storycard 7. 115

Tabla 62. Prueba de aceptación Storycard 8. 115

Tabla 63. Prueba de aceptación Storycard 9. 116

Tabla 64. Prueba de aceptación Storycard 10. 117

Tabla 65. Tabla de rendimiento..... 118

ÍNDICE DE FIGURAS

Gráfico 1. Resultados pregunta 1. 19

Gráfico 2. Resultados pregunta 2. 20

Gráfico 3. Resultados pregunta 3. 22

Gráfico 4. Resultados pregunta 4. 23

Gráfico 5. Resultados pregunta 5. 24

Gráfico 6. Resultados pregunta 6. 26

Gráfico 7. Resultados pregunta 7. 27

Gráfico 8. Resultados pregunta 8. 28

Gráfico 9. Resultados pregunta 9. 29

Gráfico 10. Resultados pregunta 10. 30

Figura 11. Diagrama del proceso actual de control de ingreso y salida de estaciones de trabajo. 40

Figura 12. Diagrama optimizado para el proceso de control de ingreso y salida de estaciones de trabajo. 42

Figura 13. Versión de MongoDB. 49

Figura 14. Fases de la metodología MOBILE-D. 52

Figura 15. Diagrama de Clases BD. 61

Figura 16. Pantalla Inicio de Sesión. 63

Figura 17. Pantalla Menú Principal. 64

Figura 18. Pantalla Gestión de Usuarios. 65

Figura 19. Pantalla Generación de Código QR. 66

Figura 20. Pantalla Registro de Usuario Nuevo. 67

Figura 21. Pantalla Asignación de Dispositivo. 68

Figura 22. Pantalla Visualización de Dispositivo. 69

Figura 23. Pantalla Formulario Solicitud de Salida. 70

Figura 24. Pantalla Autorización de Solicitud. 71

Figura 25. Pantalla Escaneo de Código QR. 72

Figura 26. Scaffold. 73

Figura 27. Column. 73

Figura 28. Row. 73

Figura 29. Container. 74

Figura 30. Expanded. 74

Figura 31. Margin. 74

Figura 32. Padding. 75

Figura 33. SingleChildScrollView. 76

Figura 34. SafeArea. 77

Figura 35. ListView 78

Figura 36. TextField y TextFormField. 79

Figura 37. ElevatedButton. 79

Figura 38. IconButton. 80

Figura 39. FloatingActionButton. 80

Figura 40. GestureDetector. 81

Figura 41. DropdownButton. 81

Figura 42. Text. 82

Figura 43. Card. 82

Figura 44. Image.asset. 83

Figura 45. Divider. 83

Figura 46. Navigator.push. 83

Figura 47. Diagrama de Endpoints. 85

Figura 48. Pantalla de Inicio de Sesión. 99

Figura 49. Pantalla de Registro de Usuarios. 100

Figura 50. Pantalla de Lista de Usuarios. 101

Figura 51. Pantalla de Asignación de Dispositivos. 102

Figura 52. Pantalla de Generación de Código QR. 103

Figura 53. Pantalla de Envío de Solicitud de Salida. 105

Figura 54. Notificación al Oficial de Seguridad. 106

Figura 55. Pantalla de Revisión de Solicitudes. 107

Figura 56. Notificación al Funcionario. 108

Figura 57. Pantalla de verificación de salida y notificación push de aprobación de salida. 109

Figura 58. Pantalla de registro de ingreso y notificación push de aprobación. 110

Figura 59. Pantalla de Control de Dispositivos. 111

ÍNDICE DE ANEXOS

Anexo A. ISO 9001:2015 125

Anexo B. ISO/IEC 27001:2022 126

Anexo C. Ley de Protección de Datos 127

Anexo D. Manual de Usuario 128

RESUMEN EJECUTIVO

Para dar cumplimiento al objetivo de identificar los procesos actuales de control en la Cooperativa de Ahorro y Crédito Credi Ya Ltda., se realizó un diagnóstico que evidenció deficiencias significativas en el registro de ingreso y salida de estaciones de trabajo. Se constató la ausencia de mecanismos formales que aseguren trazabilidad, seguridad y un seguimiento de los activos tecnológicos, lo que generaba riesgos como pérdida de equipos, accesos no autorizados y dificultad para verificar movimientos, afectando la productividad y el cumplimiento de políticas de seguridad.

Ante esta situación, el proyecto se enfocó en desarrollar una aplicación móvil multiplataforma capaz de automatizar el proceso mediante registros digitales, flujos de aprobación y validación por códigos QR. Esta solución permite gestionar solicitudes de salida, autorizar movimientos y verificar retornos en tiempo real.

Para su implementación se utilizó Flutter 3.27 en el desarrollo móvil, mientras que el backend fue construido en Node.js con Express.js 4.16.4 para la creación de servicios RESTful. La gestión de datos se realizó con MongoDB 6.0.22, apoyado en Mongoose 5.11.4 para la estructuración de modelos. Además, se integró Firebase Cloud Messaging mediante la librería firebase-admin 13.3.0 para el envío de notificaciones.

Como resultado, la aplicación aporta un avance en la modernización del proceso, optimiza tiempos de registro y autorización, mejora la transparencia en la administración de activos y fortalece la seguridad organizacional alineándose con los estándares ISO 9001:2015 e ISO/IEC 27001:2022.

Palabras clave: Framework Flutter, aplicación móvil multiplataforma, control de activos tecnológicos, Metodología Mobile-D, sistema de notificaciones push, cooperativa de ahorro y crédito.

ABSTRACT

To achieve the objective of identifying current control processes at the Credi Ya Ltda. Savings and Credit Cooperative, a diagnostic assessment was conducted that revealed significant deficiencies in the recording of workstation entry and exit. The assessment confirmed the absence of formal mechanisms to ensure traceability, security, and monitoring of technological assets, generating risks such as equipment loss, unauthorized access, and difficulty in verifying movements, thus impacting productivity and compliance with security policies.

In response to this situation, the project focused on developing a cross-platform mobile application capable of automating the process through digital records, approval workflows, and QR code validation. This solution allows for managing exit requests, authorizing movements, and verifying returns in real time.

For its implementation, Flutter 3.27 was used for mobile development, while the backend was built in Node.js with Express.js 4.16.4 for creating RESTful services. Data management was performed using MongoDB 6.0.22, supported by Mongoose 5.11.4 for model structuring. Additionally, Firebase Cloud Messaging was integrated using the firebase-admin 13.3.0 library for sending notifications.

As a result, the application represents an advance in process modernization, optimizes registration and authorization times, improves transparency in asset management, and strengthens organizational security by aligning with ISO 9001:2015 and ISO/IEC 27001:2022 standards.

Keywords: Flutter Framework, Multi-platform mobile application, technology asset management, Mobile-D methodology, push notification system, savings and credit cooperative.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

APLICACIÓN MÓVIL UTILIZANDO FLUTTER PARA EL CONTROL DE INGRESO Y SALIDA DE ESTACIONES DE TRABAJO EN LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.

1.1.1 Planteamiento del problema

Durante la última década, América Latina y el Caribe se ha evidenciado importantes avances en términos de digitalización en el sector financiero cooperativo, la inversión tecnológica en este sector ha experimentado un incremento del 65% entre 2020 y 2023 [1].

Según un estudio realizado por la Superintendencia de Economía Popular y Solidaria, el sistema financiero popular y solidario en Ecuador, (SEPS), ha tenido un crecimiento significativo en la última década, hasta 2023 existían más de 600 cooperativas de ahorro y crédito activas, con más de 8 millones de socios registrados. Esto refleja una presencia significativa, especialmente en sectores rurales y populares, donde estas entidades cumplen un rol fundamental al ofrecer una alternativa basado en el Informe de Inclusión Financiera Digital de Ecuador accesible al sistema financiero tradicional [2].

Según el Informe de Inclusión Financiera Digital de Ecuador (2023), el 78% de las cooperativas del segmento 1 y 2 han implementado algún tipo de solución tecnológica para mejorar sus procesos internos.

En la provincia de Tungurahua, un epicentro clave en el desarrollo del cooperativismo, se evidencia el creciente compromiso con la innovación tecnológica en el sector. Según el reporte "Tecnología e Innovación en Cooperativas de Ahorro y Crédito 2023", publicado por la Red de Instituciones Financieras de Desarrollo (RFD), las cooperativas de Tungurahua muestran indicadores de eficiencia operativa superiores a

la media nacional, con una relación de gastos operativos sobre activos totales de 4.2% frente al 5.1% del promedio nacional [3].

Según la Ley Orgánica sobre Información Personal (LODP), se impone especial responsabilidad a todas las organizaciones que recopilan y procesan datos personales, incluidas las cooperativas de ahorro y crédito, al administrar información confidencial sobre sus socios, como datos financieros, personales y laborales, estas organizaciones deben garantizar su comportamiento apropiado y garantizar su confidencialidad, integridad y uso legítimo [4].

La Cooperativa de Ahorro y Crédito Credi Ya Ltda., con una significativa presencia en el sistema financiero popular y solidario, es consciente de la relevancia de implementar sistemas avanzados de registro y control para el ingreso y salida de sus colaboradores en las estaciones de trabajo, alineándose con las tendencias de transformación digital que caracterizan al sector.

1.2 Antecedentes investigativos

Se ha realizado la revisión bibliográfica mediante la búsqueda en diferentes fuentes de información científica y académica. Además, se han llevado a cabo las cadenas de búsqueda de forma específica, con las palabras clave mencionadas, es decir, "Flutter", "mobile application", "attendance control", "financial", escogiendo para ello tres de las bases de datos académicas las fuentes principales incluyeron, Springer Link, ScienceDirect y IEEE Xplore. Estas búsquedas se realizaron abarcando publicaciones desde 2020 hasta 2024. Los resultados obtenidos de esta búsqueda se presentan de manera sintetizada en la Tabla 1, proporcionando una visión general de las publicaciones más importantes para el estudio.

Tabla 1. Cadenas de búsqueda en base de datos académicas y científicas.

Base de datos	Cadenas de búsqueda	Núm. de artículos
Springer Link	(TITLE-ABS-KEY ("Mobile Application Development") (Using "Flutter"), AND PUBYEAR 2024.	2
ScienceDirect	(GTITLE-ABS-KEY "Flutter" AND (All: "workstation access") AND PUBYEAR "financial" within 2020-2023.	2
IEEE Xplore	(All: "mobile application") AND ([All: "credit cooperative") AND (All: "access management") PUBYEAR 2021-2024	2
	Total	6

Asimismo, se amplió la búsqueda explorando repositorios académicos de instituciones en Ecuador, incluyendo la Universidad Técnica de Ambato (UTA) y Universidad Israel (ISRAEL), en el periodo comprendido desde el año 2020 al 2024. Obteniendo los siguientes resultados, comprendidos en la Tabla 2.

Tabla 2. Búsqueda en el repositorio institucional UTA.

Universidad	Filtro de búsqueda	Núm. de artículos
Universidad de Israel	Aplicación móvil utilizando Flutter para el control de ingreso y salida.	3
Universidad Técnica de Ambato	Aplicación móvil usando Flutter para el seguimiento y control.	4
Total		7

El objetivo de esta revisión bibliográfica fue abordar la búsqueda, análisis y síntesis de los antecedentes más relevantes que tuvieron que ver con el proceso de desarrollar aplicaciones móviles con Flutter, orientadas a controlar el ingreso y salida en la 6 actividad laboral en el sector financiero cooperativo. Para ello se definieron criterios de inclusión y exclusión detallados en la Tabla 3, permitieron la selección de estudios que resultaron pertinentes y que fueron publicados entre los años 2020 y 2024. Finalmente, como resultado se seleccionaron cinco artículos fundamentales que

aportan aspectos técnicos y conceptuales relevantes para enriquecer el marco teórico a partir del cual se aborda esta investigación.

Tabla 3. Criterios de inclusión y exclusión.

Inclusión	Exclusión
• Artículos que aborden el desarrollo de aplicaciones móviles con Flutter. • Investigaciones que traten el control de ingreso y salida de estaciones de trabajo mediante tecnología. • Publicaciones que analicen tecnologías como Firebase y QR.	• Artículos que no utilicen Flutter ni se enfoquen en tecnologías móviles. • Artículos de pago • Artículos que no estén relacionados con el desarrollo de aplicaciones móviles.

En el proyecto de investigación, Argila Lorente [5] explica la creación mediante Flutter y a Firebase, una aplicación multiplataforma que permite escanear códigos Quick Response (QR) para registrar entradas y salidas de ítems de forma casi instantánea. La arquitectura construida, con un front-end muy liviano en Flutter más un back-end definido por la Firebase Realtime Database, ofrece garantía de alta disponibilidad, baja latencia en la captura de eventos y trazabilidad de cada uno de los movimientos. Los mismos principios de diseño escáner QR, registro inmediato y almacenamiento sin desconexión, pueden ser aplicados directamente al control de ingreso y salida en estaciones de trabajo, garantizando exactitud, seguridad y escalabilidad.

Según Chutas Ramos [6] a través del planteamiento y puesta en marcha de una aplicación móvil en Flutter para llevar el control de inventario de los productos que más movimiento tienen dentro de una cadena de suministro, se implantó Firebase Firestore como sistema de base de datos en tiempo real y se dispuso el modo offline con SQLite consiguiendo que los registros de entrada y salida queden siempre sincronizados, incluso si la aplicación pudiera recuperar conectividad. El trabajo describe la arquitectura Modelo-Vista-Controlador (MVC) que se utilizó, el manejo de formularios dinámicos y la validación de datos, que podrían trasladarse al control de ingreso y salida en estaciones de trabajo, siendo robusta, escalable y permitiendo la continuidad de la actividad en entornos de conectividad intermitente.

Toledo Orozco et al. [7], presenta una aplicación en Flutter que crea y verifica códigos QR dinámicos, autentica los usuarios mediante Firebase Authentication y registra cada acceso en Firestore. Envía alertas automáticas a Recursos Humanos en caso de acceso fuera de horarios. Con un diseño ágil y multiplataforma, esta solución convierte al smartphone en un lector de acceso inteligente, mejorando la seguridad y la eficiencia en cualquier lugar de trabajo.

Aldás Montesdeoca [8] con este proyecto se desarrolló una aplicación que permite mejorar la accesibilidad en las estaciones de trabajo mediante la fusión de Firebase Firestore y SQLite la interfaz, diseñada para ser fácil de usar, ayuda al usuario para alcanzar su propósito en pocos toques, mientras que la arquitectura MVC permite que cualquier evento quede almacenado de manera segura y trazable. El resultado es un proceso rápido, fiable y completamente auditable.

El estudio de StrongDM (2024) [9] demuestra que el 52% de equipos de desarrollo pierden fechas límite por problemas de acceso a sistemas, mientras que el 73% de empleados necesita más de 15 minutos diarios para obtener accesos necesarios. Además, Argila Lorente en su investigación establece una correlación directa entre la eficiencia de los sistemas de control de acceso y tres variables dependientes clave como la productividad laboral, cumplimiento de cronogramas y optimización de tiempos operacionales los problemas de acceso generan cuellos de botella que se traducen en pérdidas acumulativas de productividad organizacional.

1.3 Fundamentación teórica

Este apartado presenta un análisis comprehensivo de las tecnologías, plataformas y herramientas metodológicas implementadas en las investigaciones que constituyen el marco referencial de este estudio. Se examinarán los componentes tecnológicos adoptados por cada investigación, evaluando su pertinencia metodológica y la manera en que estos recursos fueron integrados estratégicamente para dar respuesta a los objetivos específicos planteados en cada trabajo referenciado.

1.3.1 Tecnologías de la información

Las Tecnologías de la Información TI representan un conjunto de recursos, procesos y técnicas utilizadas en el almacenamiento y difusión de datos. En el ámbito corporativo se han transformado en un componente estratégico que posibilita a las empresas perfeccionar sus procesos, potenciar la toma de decisiones y su competitividad de acuerdo a lo expuesto por Avendaño Castro et al. [10], las Tecnologías de la Información incluyen hardware, software, tecnologías de almacenamiento y comunicación lo que simplifican la administración de datos en las instituciones. De igual modo, para entidades financieras las TI son un recurso esencial para la administración eficaz de sus operaciones y para la protección de la información.

1.3.2 Desarrollo de aplicaciones móviles

El desarrollo de aplicaciones móviles es un procedimiento a través del cual se crean programas destinados a funcionar en dispositivos móviles como smartphones y tablets de acuerdo con Molina Ríos et al. [11], dicha área ha visto un aumento significativo debido a la popularidad de los dispositivos móviles y la demanda de información accesible en todo momento y lugar. Las aplicaciones móviles orientadas a negocios están específicamente elaboradas para atender requerimientos de las organizaciones, como la automatización de tareas, el manejo de recursos o la supervisión de accesos por otra parte, en el ámbito financiero, estas aplicaciones hacen posible establecer medidas de seguridad, simplificar transacciones y optimizar la eficiencia operativa.

1.3.3 Flutter

Flutter es un framework creado por Google que permite el desarrollo de aplicaciones nativas multiplataforma a partir de un solo código base para Quisaguano Collaguazo et al. [12], Flutter emplea el lenguaje de programación Dart y se distingue por su alto desempeño, su adaptable interfaz de usuario y su habilidad para crear aplicaciones visualmente atractivas, además incluye widgets a medida que facilitan la implementación de los fundamentos de Material Design (para Android) y Cupertino (para iOS), proporcionando una experiencia de usuario consistente con la plataforma.

Las características lo convierten en la opción perfecta para la creación de aplicaciones corporativas que necesitan interfaces fácilmente comprensibles y un desempeño óptimo, como las aplicaciones de control de acceso.

1.3.4 Patrón Modelo-Vista-Controlador

La arquitectura Model-View-Controller (MVC) constituye un patrón arquitectónico fundamental en el desarrollo de software moderno, ampliamente adoptado en 2024 y 2025 para la construcción de aplicaciones web y móviles. Este patrón divide la aplicación en tres componentes interdependientes: el Modelo, encargado de gestionar los datos y la lógica de negocio; la Vista, responsable de la presentación de la interfaz de usuario; y el Controlador, que actúa como intermediario coordinando las interacciones entre el Modelo y la Vista.

Esta separación de responsabilidades proporciona ventajas significativas como la mejora en la mantenibilidad del código, la facilitación del trabajo colaborativo entre equipos de desarrollo mediante el desarrollo en paralelo, la reutilización de componentes entre diferentes interfaces, y la simplificación en la implementación de pruebas unitarias [13].

1.3.5 Aplicación móvil para control de acceso

Las aplicaciones móviles para el control de acceso son programas diseñados específicamente para administrar y supervisar el ingreso y salida de estaciones de trabajo y recursos tecnológicos en contextos organizacionales. Sin embargo, estas aplicaciones incorporan tecnologías como códigos QR, identificación biométrica o geolocalización para comprobar y documentar accesos. Dentro del marco de una entidad financiera, una aplicación de control de acceso creada con Flutter tiene la capacidad de ofrecer características como autenticación segura, registro de tiempos de utilización de equipos, generación de reportes sobre el uso de recursos tecnológicos y alertas en tiempo real sobre accesos no autorizados, favoreciendo la protección de los activos tecnológicos y el cumplimiento de normativas del sector [14].

1.3.6 Gestión Empresarial

De acuerdo con [15], la administración organizacional constituye un sistema integrado de actividades, enfoques metodológicos y estrategias institucionales dirigidas hacia la maximización del aprovechamiento de recursos y la consecución de las metas empresariales. Dicho sistema se distingue por adoptar una perspectiva sistemática que engloba la formulación de planes estratégicos, la estructuración organizacional eficaz, el liderazgo directivo y la supervisión metódica de las actividades operacionales.

En complemento, [16] señala que dentro de los elementos esenciales se encuentran la administración del capital humano, el manejo de recursos financieros, la mejora continua de procedimientos y la formulación de tácticas para el posicionamiento competitivo. Paralelamente, en el panorama empresarial contemporáneo, la administración organizacional integra componentes cruciales como el fomento de la innovación permanente, la viabilidad operacional a largo plazo y la flexibilidad para responder a contextos variables.

Adicionalmente, su relevancia se fundamenta en que facilita a las empresas el perfeccionamiento de su rendimiento operativo, el fortalecimiento de su posición competitiva y la capacidad de respuesta ágil ante las demandas del entorno comercial. Sin embargo, también confronta retos considerables, destacando la transformación digital acelerada, la demanda de liderazgo adaptativo en contextos evolutivos y el manejo de la volatilidad en un ambiente internacionalizado [17]. En última instancia, los enfoques metodológicos actuales enfatizan la formulación de decisiones fundamentadas en información analítica, la administración del conocimiento organizacional y la implementación de estándares de excelencia sectorial, elementos que favorecen una gestión más efectiva y enfocada hacia el desarrollo sustentable.

1.3.7 Seguridad en aplicativos móviles

La protección de los registros de ingreso, salida e información personal operativa de los afiliados junto con los empleados de la cooperativa requiere la implementación de una estrategia de seguridad multicapa. Esta estrategia debe abarcar la aplicación móvil

(cliente), los servicios backend, así como toda la infraestructura tecnológica subyacente.

a. Autenticación y Control de Accesos

La implementación de mecanismos de autenticación robustos constituye el primer pilar de la estrategia de seguridad. El sistema debe incorporar autenticación multifactor (MFA) como requisito obligatorio para roles con privilegios elevados, incluyendo administradores, supervisores o personal con acceso a funciones críticas. La arquitectura recomendada contempla el uso de proveedores de identidad consolidados como Firebase Auth o servidores OAuth2, los cuales ofrecen funcionalidades probadas para la gestión segura de tokens de acceso junto con tokens de renovación [18].

b. Confidencialidad en Tránsito y en Reposo

La protección de la información durante su transmisión además de almacenamiento requiere la implementación de protocolos de cifrado robustos. Todas las comunicaciones entre la aplicación móvil, las APIs intermedias hasta los servicios backend deben forzar el uso exclusivo de TLS (HTTPS). Para la información almacenada, el sistema debe emplear algoritmos de cifrados modernos como AES-256 tanto en servidores como en dispositivos móviles, utilizando mecanismos nativos seguros como Keychain en iOS o Android Keystore para el almacenamiento local de credenciales [19].

1.3.8 Privacidad y Cumplimiento Normativo

El diseño del sistema debe contemplar el cumplimiento estricto de la normativa aplicable tanto a nivel nacional como sectorial. En Ecuador, las cooperativas de ahorro están sujetas a la supervisión de la Superintendencia de Economía Popular y Solidaria (SEPS), lo cual implica obligaciones específicas de confidencialidad, reporte además de conservación de información. La solución debe incorporar controles para el tratamiento de datos personales conforme a la normativa local, considerando también la aplicabilidad de regulaciones internacionales como el GDPR en caso de procesamiento de datos de ciudadanos europeos [20].

1.3.9 Arquitectura de Backend Seguro

El diseño de servicios backend debe seguir principios de separación de responsabilidades, estableciendo APIs diferenciadas para autenticación, registro de eventos además de servicios de reporting. Los endpoints que manejan información sensible deben requerir scopes o roles específicos, mientras que las operaciones críticas como correcciones manuales de registros deben generar trazas de auditoría además de requerir autorizaciones de nivel superior. La estrategia debe incluir políticas robustas de backup, planes de recuperación ante desastres junto con procedimientos de continuidad operativa [21] [22].

1.4 Objetivos

1.4.1 Objetivo general

Desarrollar una aplicación móvil utilizando Flutter para el control de ingreso y salida de estaciones de trabajo en la Cooperativa de Ahorro y Crédito Credi Ya Ltda.

1.4.2 Objetivos específicos

- Determinar los procesos actuales de registro de ingreso y salida de estaciones de trabajo en la Cooperativa de Ahorro y Crédito Credi Ya Ltda.
- Investigar la tecnología Flutter en el desarrollo de soluciones móviles multiplataforma.
- Diseñar una aplicación móvil utilizando Flutter para el control de ingreso y salida de estaciones de trabajo en la Cooperativa de Ahorro y Crédito Credi Ya Ltda.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Para la recolección de información de la investigación se emplearon tres técnicas: encuesta, entrevista y ficha de observación. En primera instancia, se aplicó una encuesta conformada por 10 preguntas cerradas, dirigida a los administradores, personal de seguridad y funcionarios de la Cooperativa de Ahorro y Crédito Credi Ya Ltda. Esta herramienta tuvo como propósito explorar el sistema actual de registro de ingreso y salida del personal, evaluar el grado de automatización en el control de asistencia a las estaciones de trabajo y detectar las principales dificultades que enfrenta el personal con los mecanismos de registro utilizados. Asimismo, permitió conocer la percepción del equipo respecto a la necesidad de incorporar una solución tecnológica móvil que optimice el control de acceso y permanencia en sus puestos laborales.

Posteriormente, se realizó una entrevista estructurada al Gerente general de la empresa, la cual incluyó 5 preguntas enfocadas en analizar el funcionamiento del sistema de control de asistencia actual, identificar los puntos críticos que afectan la supervisión y gestión de los operarios de la empresa, y justificar la pertinencia de implementar una aplicación móvil desarrollada en Flutter para el seguimiento de ingreso y salida de las estaciones de trabajo. Esta entrevista ofreció una perspectiva estratégica que complementó la visión operativa obtenida a través de la encuesta.

Finalmente, se ejecutó una observación directa mediante una ficha de observación diseñada previamente, con el objetivo de evidenciar de manera práctica cómo se desarrollan los procesos de control de permanencia del personal dentro de la empresa. A través de esta técnica se pudo comprobar, entre otros aspectos, la dependencia de procedimientos manuales para el registro de entrada y salida del personal, la inexistencia de un sistema automatizado que centralice la información de asistencia, y la limitada trazabilidad en actividades claves como el monitoreo en tiempo real y la generación de reportes de permanencia. Estas observaciones revelan una serie de ineficiencias que afectan la supervisión adecuada y la gestión efectiva del personal en la organización.

Modelo de Encuesta

Objetivo: Recopilar información sobre el proceso actual de control de ingreso y salida de equipos institucionales, con el fin de identificar riesgos, limitaciones y oportunidades de mejora. La información recabada se empleará como soporte principal para el diseño e implementación de una aplicación móvil que permita optimizar los registros, mejorar la seguridad y agilizar los procesos.

1. **¿Con qué frecuencia los equipos institucionales salen de la institución?**

a) Nunca
b) Ocasionalmente
c) Frecuentemente
d) Siempre

2. **¿Con qué frecuencia necesita registrar ingreso o salida de equipos en su área de trabajo?**

a) Nunca
b) Ocasionalmente
c) Frecuentemente
d) Siempre

3. **¿Cómo se realiza actualmente el registro de ingreso y salida de equipos?**

a) Manual (en hojas o cuadernos)
b) Digital (Excel u otro sistema básico)
c) Mixto (manual y digital)
d) No se lleva un registro formal

4. **¿Qué tan confiable considera el método actual de registro de equipos?**

a) Nada confiable
b) Medianamente confiable
c) Confiable
d) Muy confiable

5. **¿Con qué frecuencia se presentan errores o inconsistencias en los registros actuales?**

a) Nunca
b) Ocasionalmente
c) Frecuentemente

d) Siempre

6. ¿Qué riesgos identifica con mayor frecuencia en el control de ingreso y salida de equipos?

a) Pérdida de equipos
b) Accesos no autorizados
c) Errores en el registro manual
d) Demora en los procesos

7. ¿Qué nivel de seguridad percibe en el proceso actual de control de equipos?

a) Baja
b) Media
c) Alta
d) Muy alta

8. ¿Qué tan adecuado considera el proceso actual de autorización para cumplir con las políticas internas de la institución?

a) En desacuerdo
b) Neutral
c) De acuerdo
d) Muy de acuerdo

9. ¿Considera que una aplicación móvil mejoraría el control de ingreso y salida de equipos?

a) En desacuerdo
b) Neutral
c) De acuerdo
d) Muy de acuerdo

10. ¿Qué beneficio considera más importante que debería ofrecer una aplicación móvil para el control de equipos?

a) Mayor seguridad en la salida/ingreso
b) Ahorro de tiempo en los registros
c) Reducción de errores humanos
d) Acceso a la información en tiempo real

Entrevista

Tabla 4. Guía de entrevista.

Lugar y Fecha: Entrevistado: Cargo: Objetivo:			
N°	**PREGUNTA**	**RESPUESTA**	**OBSERVACIÓN**
1	¿Desde su experiencia, ¿cuáles son las principales dificultades que ha observado en el control actual de ingreso y salida de equipos?		
2	¿Qué procedimientos se siguen actualmente cuando un equipo sale de la institución y quiénes participan en ese proceso?		
3	¿Qué riesgos considera más relevantes al no contar con un sistema automatizado de control?		
4	¿Qué tan efectivo considera el método actual para garantizar seguridad y trazabilidad de los equipos?		
5	¿Qué situaciones recuerda en las que se hayan presentado errores o inconvenientes con el registro de equipos?		
6	¿En su opinión, ¿cómo influye la participación de los guardias de seguridad en la confiabilidad del proceso?		
7	¿De qué manera el tiempo que toma autorizar la salida de un equipo afecta el trabajo diario en la institución?		
8	¿Qué tipo de controles adicionales considera necesarios para reducir riesgos en el manejo de los equipos?		
9	¿Qué expectativas tendría usted sobre una aplicación móvil que ayude en el control de equipos?		
10	¿Qué sugerencias daría para que el nuevo sistema sea sostenible en el tiempo y no quede en desuso?		
CONCLUSIONES			

Ficha de Observación

Tabla 5. Ficha de Observación.

Fecha:								
Hora de inicio:								
Hora de fin:								
Ubicación:								
Aspectos para observar	Indicador	Cumplimiento					Comentario
		1	2	3	4	5	
Procedimiento de control	Se observa la existencia de un protocolo formal para registrar y autorizar el ingreso y salida de equipos institucionales.						
Participación del personal responsable	El personal administrativo, técnico y de seguridad participa activamente en el control y verificación de los equipos.						
Registro y trazabilidad de equipos	Cada equipo cuenta con un registro que detalla responsable, destino, fechas de salida y retorno, y estado del activo.						
Uso de herramientas tecnológicas	Se utilizan herramientas tecnológicas (códigos QR, sistemas digitales, bases de datos, etc.) para controlar los equipos.						
Seguridad en los puntos de control	Se aplican medidas de seguridad efectivas en el ingreso y salida, verificando los datos del equipo y del responsable.						
Respaldo y conservación de registros	Se mantiene respaldo físico o digital actualizado de los equipos ingresados y salidos, con acceso restringido.						
CONCLUSIONES								

Criterio:

- 1= Muy bajo
- 2= Bajo
- 3= Moderado
- 4= Alto
- 5= Muy Alto

2.2 Métodos

La presente investigación empleo una metodología con enfoque mixto, dado que se llevó a cabo un tratamiento estadístico de la información recopilada mediante un instrumento de encuesta dirigido al grupo de estudio definido, lo que facilitó enriquecer los resultados de manera cuantitativa.

2.2.1 Modalidad de la investigación

El proyecto de investigación se enmarca dentro de la modalidad de campo y bibliográfica - documental, debido a que combina la recolección de datos primarios a través de encuestas, entrevistas y observaciones directas con la revisión de fuentes secundarias para respaldar y enriquecer los resultados obtenidos.

Investigación bibliográfica – documental

Esta investigación adoptará un enfoque Bibliográfico-Documental, fundamentándose en el análisis minucioso de artículos científicos, revistas especializadas, tesis de grado y posgrado, manuales técnicos y otras fuentes académicas de reconocida confiabilidad. El propósito será recopilar y analizar información pertinente sobre el desarrollo de aplicaciones móviles utilizando el framework Flutter, así como los sistemas de control de acceso a estaciones.

Esta revisión permitirá obtener una comprensión profunda de la problemática planteada, proporcionar el sustento teórico-técnico necesario para justificar la solución tecnológica propuesta, y establecer las directrices metodológicas que guiarán el proceso de desarrollo e implementación de la aplicación móvil.

Investigación de campo

Esta investigación también será de campo, puesto que se obtendrá información directamente en las instalaciones de la Cooperativa, se recopilarán datos específicos sobre los procedimientos actuales para el control de acceso a las estaciones de trabajo, identificando los métodos, herramientas y tecnologías que se emplean en la actualidad. Esta aproximación directa al entorno laboral permitirá comprender de manera integral

la situación real de la Cooperativa, identificando las necesidades específicas y los desafíos operativos existentes.

Los hallazgos obtenidos servirán como base fundamental para desarrollar la aplicación móvil que se ajuste efectivamente a los requerimientos particulares de la Cooperativa y optimice sus procesos de control de estaciones de trabajo.

2.2.2 Población y muestra

El presente proyecto de investigación dirige su análisis hacia el personal operativo de la Cooperativa de Ahorro y Crédito Credi Ya Ltda., constituyendo la población objetivo del estudio. La Tabla 4 presenta la caracterización detallada de los diversos roles organizacionales desempeñados por el equipo de trabajo, proporcionando una descripción exhaustiva de las funciones específicas, responsabilidades asignadas, además de competencias requeridas para cada posición dentro de la estructura operacional de la institución.

Tabla 6. Población de estudio.

Población	N° de personas	Porcentaje %
Gerencia	1	2.27%
Coordinador de TI	1	2.27%
Desarrolladores	3	6.82%
Guardias de Seguridad	2	4.45%
Oficial de Seguridad Física	1	2.27%
Seguridad de la Información	1	2.27%
Colaboradores	35	79.55%
Total	44	100%

2.2.3 Recolección de información

Validación de instrumento

Alfa de Cronbach en la encuesta dirigida a los administradores, personal de seguridad y funcionarios de la Cooperativa de Ahorro y Crédito Credi Ya Ltda.

El índice alfa de Cronbach representa un indicador de fiabilidad que permite valorar la coherencia interna entre los elementos que conforman un instrumento de evaluación o escala de medida.

Este coeficiente se emplea para verificar si los componentes del instrumento evalúan de forma homogénea una misma dimensión o variable. En la investigación, se implementó Alfa de Cronbach con el propósito de analizar la consistencia entre los reactivos correspondientes a 5 preguntas, las cuales fueron seleccionadas del cuestionario aplicado las siguientes: 4, 5, 7, 8 y 9.

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum \boldsymbol{\sigma_i^2}}{\sigma_{total}^2}\right)$$

Donde:

k = número de ítems en la escala.

$\sum \boldsymbol{\sigma_i^2} = Sumatoria\ de\ la\ varianza\ de\ los\ ítems.$

$\sigma_{total}^2 = Varianza\ total\ del\ instrumento.$

Los resultados se tabularon en Excel y se comprobó utilizando el software estadístico SPSS (Statistical Package for the Social Sciences), obteniendo los siguientes valores:

Tabla 7. Coeficiente alfa de Cronbach en la encuesta.

Simbología	Valor
$\propto$	0,70
$\boldsymbol{k}$	5
$\sum \boldsymbol{\sigma_i^2}$	4,338
$\boldsymbol{\sigma_{total}^2}$	9,724

El coeficiente obtenido fue de 0,70, tal como se muestra en la Tabla 7, el resultado muestra que el instrumento utilizado tiene un nivel aceptable de confiabilidad, según los criterios establecidos en la Tabla 8.

Tabla 8. Criterios de la escala de consistencia del alfa de Cronbach.

Rango	Interpretación
0,9	Excelente
0,9 – 0,8	Buena
0,8 – 0,7	Aceptable
0,7 – 0,6	Cuestionable
0,6 – 0,5	Pobre
< 0,5	Inaceptable

Resultados de la Encuesta

Pregunta 1. ¿Con qué frecuencia los equipos institucionales salen de la institución?

Tabla 9. Resultados de la pregunta 1.

Indicador	Frecuencia	Porcentaje
Nunca	4	9%
Ocasionalmente	9	21%
Frecuentemente	16	36%
Siempre	15	34%
Total	**44**	**100%**

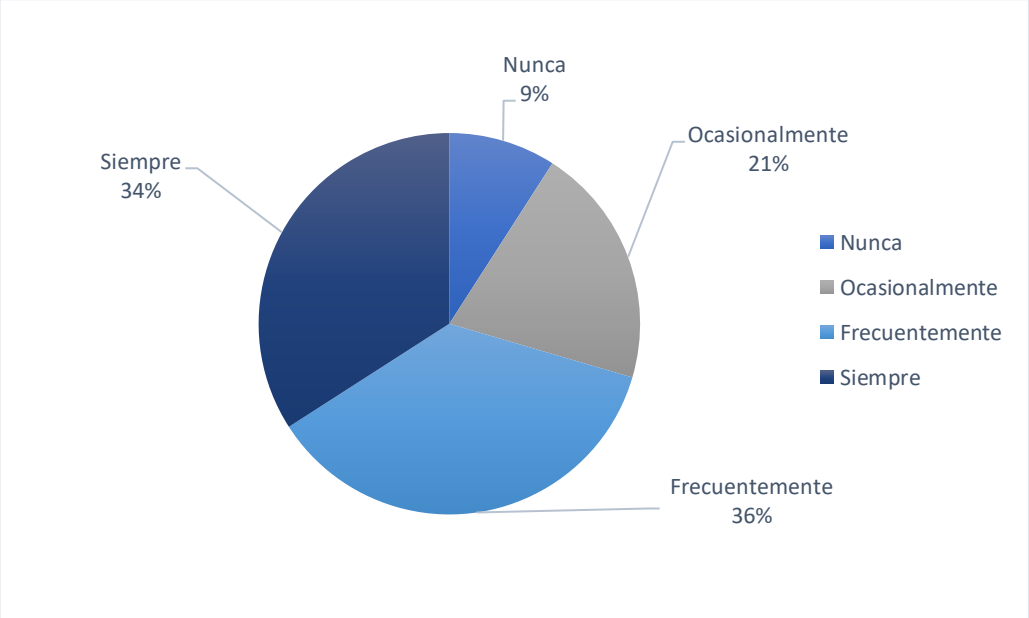


Gráfico 1. Resultados pregunta 1.

Análisis e Interpretación de resultados

De acuerdo con los resultados presentados en el Gráfico 1, se evidencia lo siguiente: El 36% de los encuestados manifestó que los equipos de la organización son trasladados fuera de las instalaciones de manera frecuente, en tanto que el 34% afirmó que esto ocurre siempre. Por su parte, el 21% indicó que dichos movimientos se presentan ocasionalmente, y el 9% señala que estos desplazamientos no se registran en ningún momento.

Al analizar estos datos, resulta evidente que una proporción significativa de los participantes (70% sumando las categorías "frecuentemente" y "siempre") identifica una movilización recurrente de los equipos tecnológicos. Este resultado resalta la importancia de disponer de una herramienta que facilite la administración y el monitoreo efectivo de los movimientos de entrada y salida, asegurando así una mayor trazabilidad sobre los recursos patrimoniales de la institución.

En cuanto a los porcentajes inferiores (30% considerando "ocasionalmente" y "nunca"), estos evidencian que, aunque ciertos equipos se mantienen al interior de las instalaciones durante períodos prolongados, esto no disminuye la pertinencia de establecer soluciones tecnológicas que garanticen un control documentado y verificable.

Pregunta 2. ¿Con qué frecuencia necesita registrar ingreso o salida de equipos en su área de trabajo?

Tabla 10. Resultados de la pregunta 2.

Indicador	Frecuencia	Porcentaje
Nunca	10	23%
Ocasionalmente	8	18%
Frecuentemente	11	25%
Siempre	15	34%
Total	**44**	**100%**

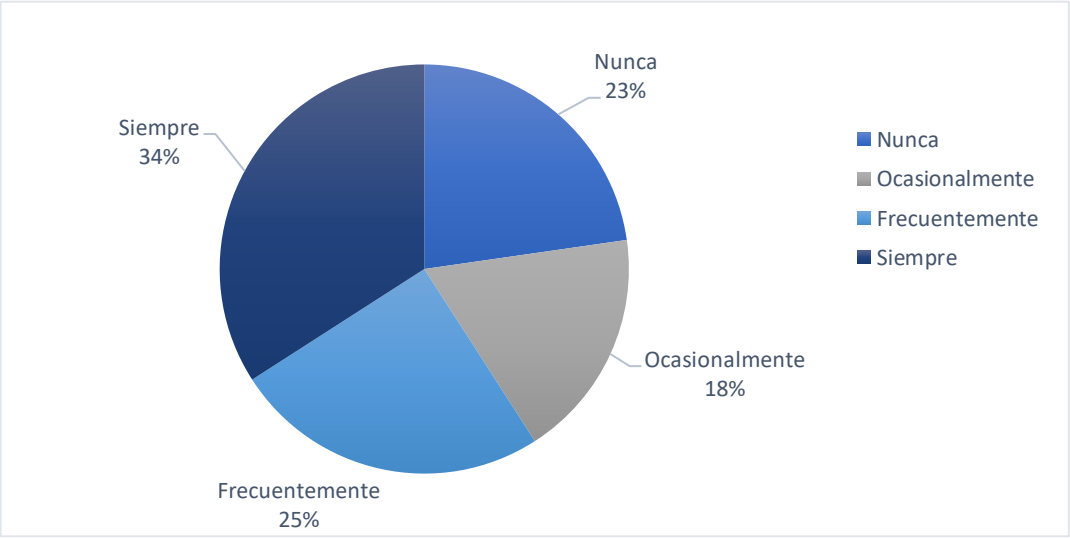


Gráfico 2. Resultados pregunta 2.

Análisis e Interpretación de resultados

De acuerdo con los datos presentados en el Gráfico 2, el 34% de los encuestados indicó que siempre necesita registrar el ingreso o salida de equipos en su área de trabajo. Por otra parte, un 25% señaló que esta actividad se realiza de manera frecuente. Además, un 23% mencionó que nunca requiere llevar a cabo este registro, mientras que un 18% afirmó que lo hace solo de forma ocasional.

Al observar estas cifras, se destaca que los procesos más relevantes se concentran en dos categorías principales: "siempre" (34%) y "frecuentemente" (25%). En conjunto, estas respuestas representan un 59% del total, lo que evidencia que la mayoría de los encuestados reconoce la necesidad de registrar de forma constante los movimientos de los equipos en su área laboral.

Sin embargo, las opciones "nunca" (23%) y "ocasionalmente" (18%) suman un 41%. Aunque menores en comparación con las primeras, reflejan que todavía existe un número significativo de personas para quienes esta práctica no es prioritaria o se da en circunstancias limitadas, lo que sugiere una diversidad en la frecuencia de uso y la importancia del registro de equipos dentro de la institución.

Pregunta 3. ¿Cómo se realiza actualmente el registro de ingreso y salida de equipos?

Tabla 11. Resultados de la pregunta 3.

Indicador	Frecuencia	Porcentaje
Manual (en hojas o cuadernos)	0	0%
Digital (Excel u otro sistema básico)	0	0%
Mixto (manual y digital)	0	0%
No se lleva un registro formal	44	100%
Total	**44**	**100%**

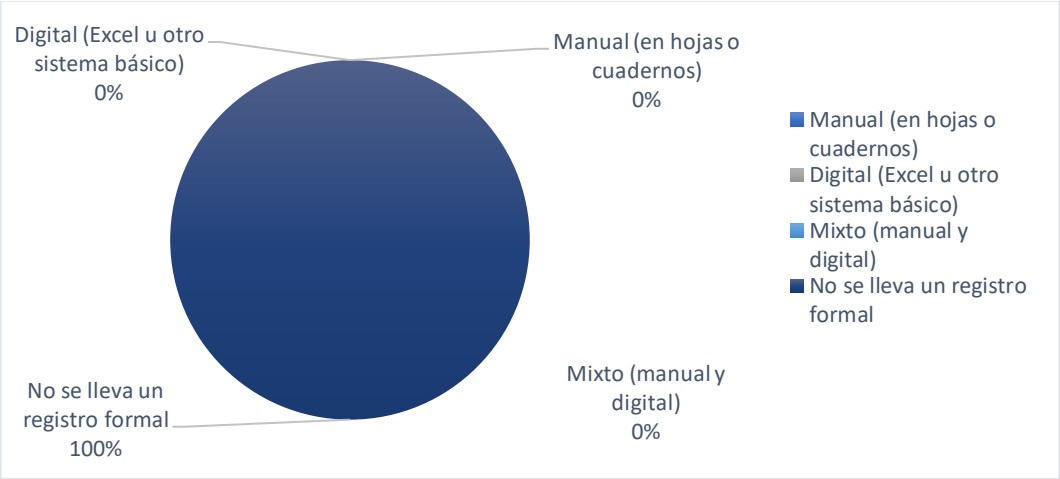


Gráfico 3. Resultados pregunta 3.

Análisis e Interpretación de resultados

Los resultados dentro del Gráfico 3 reflejan un panorama concreto: el 100% de los encuestados señaló que actualmente no se lleva un registro formal del ingreso y salida de equipos en la institución. Ninguno de los operarios indicó que este control se realice de manera manual, digital o mediante un sistema mixto, lo cual evidencia una ausencia total de procedimientos estructurados para este tipo de actividad.

Este resultado es relevante porque marca una diferencia notable frente a las preguntas anteriores, donde se evidenciaba una movilidad constante de los equipos y la necesidad de registrar dichos movimientos. La falta absoluta de registros formales, pese a la existencia de esa necesidad, revela un vacío organizacional que puede influir directamente en la trazabilidad, seguridad y control de los bienes institucionales.

Finalmente, la unanimidad de las respuestas muestra que existe una práctica inexistente en cuanto a control documental, lo que pone en evidencia una dependencia únicamente de la confianza y del manejo empírico dentro de la institución. Esta situación genera una brecha entre la realidad operativa y las necesidades de gestión, aspecto que se vuelve central al analizar la eficiencia y la transparencia en los procesos internos.

Pregunta 4. ¿Qué tan confiable considera el método actual de registro de equipos?

Tabla 12. Resultados de la pregunta 4.

Indicador	Frecuencia	Porcentaje
Nada confiable	29	66%
Medianamente confiable	10	23%
Confiable	5	11%
Muy Confiable	0	0%
Total	**44**	**100%**

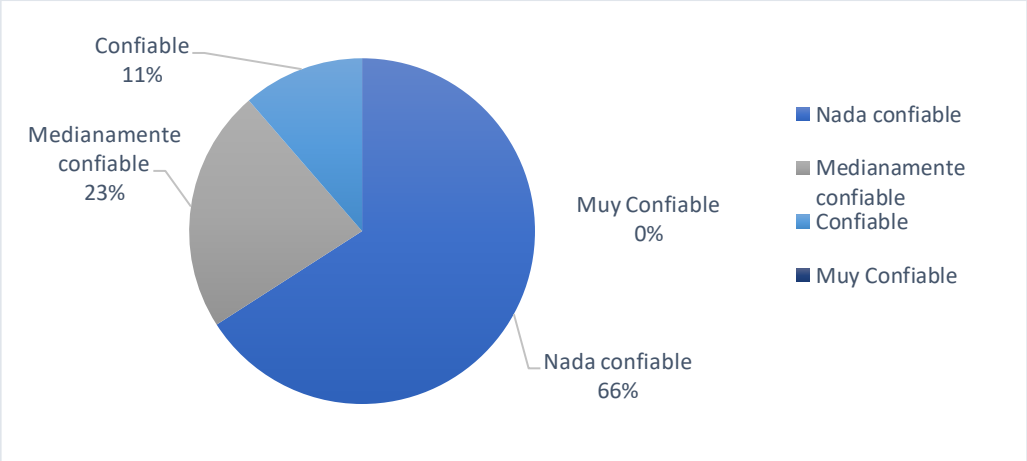


Gráfico 4. Resultados pregunta 4.

Análisis e Interpretación de resultados

Los resultados en el Gráfico 4 evidencian una percepción realmente negativa sobre la confiabilidad del método actual de registro de equipos. El 66% de los encuestados lo calificó como nada confiable, mientras que un 23% lo consideró medianamente confiable. Sin embargo, solo un 11% señaló que el registro es confiable, y ningún participante lo catalogó como muy confiable.

Este escenario revela que más de dos tercios de los encuestados no confían en el procedimiento actual, lo que pone de manifiesto un déficit importante en cuanto a la credibilidad y seguridad de los registros. El hecho de que la valoración “muy confiable” no haya recibido ninguna respuesta confirma que, dentro de la percepción general, el método carece de solidez y no responde a las expectativas de control requeridas.

Del mismo modo, la presencia de un 23% que lo califica como medianamente confiable y un 11% que lo considera confiable, aunque minoritarios, refleja que en ciertos casos los usuarios perciben algún grado de utilidad en los mecanismos actuales. Además, estos porcentajes son insuficientes para contrarrestar la tendencia general de desconfianza, consolidando la idea de que el sistema vigente no garantiza la transparencia ni la fiabilidad que se espera en los procesos de registro.

Pregunta 5. ¿Con qué frecuencia se presentan errores o inconsistencias en los registros actuales?

Tabla 13. Resultados de la pregunta 5.

Indicador	Frecuencia	Porcentaje
Nunca	5	11%
Ocasionalmente	10	23%
Frecuentemente	14	32%
Siempre	15	34%
Total	**44**	**100%**

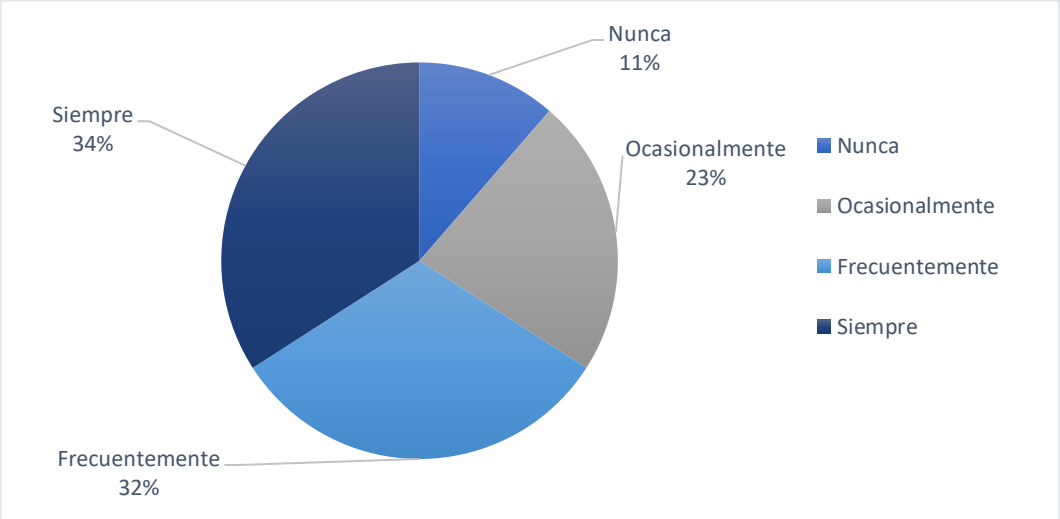


Gráfico 5. Resultados pregunta 5.

Análisis e Interpretación de resultados

Dentro del Gráfico 5, se demuestra una tendencia clara hacia la presencia constante de errores en los registros actuales. El 34% de los encuestados señalo que las inconsistencias ocurren siempre, mientras que un 32% consideró que se presentan

frecuentemente. Esto significa que dos tercios de los participantes (66%) identifican que los registros están expuestos a fallas de manera continua.

Por otro lado, un 23% indicó que los errores se dan ocasionalmente, lo cual sugiere que incluso en contextos donde los registros son menos frecuentes, persisten debilidades en el control. Solo un 11% manifestó que los errores nunca se presentan, porcentaje que resulta significativamente menor en comparación con las percepciones mayoritarias.

Estos resultados evidencian un panorama en el que la falta de confiabilidad, ya detectada en la pregunta anterior, se confirma ahora con la alta frecuencia de errores. La combinación de respuestas refleja que las inconsistencias forman parte de la dinámica habitual de los registros, lo que afecta tanto la precisión de la información como la confianza en los procedimientos actuales.

Pregunta 6. ¿Qué riesgos identifica con mayor frecuencia en el control de ingreso y salida de equipos?

Tabla 14. Resultados de la pregunta 6.

Indicador	Frecuencia	Porcentaje
Pérdida de equipos	14	32%
Accesos no autorizados	20	45%
Errores en el registro manual	4	9%
Demora en los procesos	6	14%
Total	**44**	**100%**

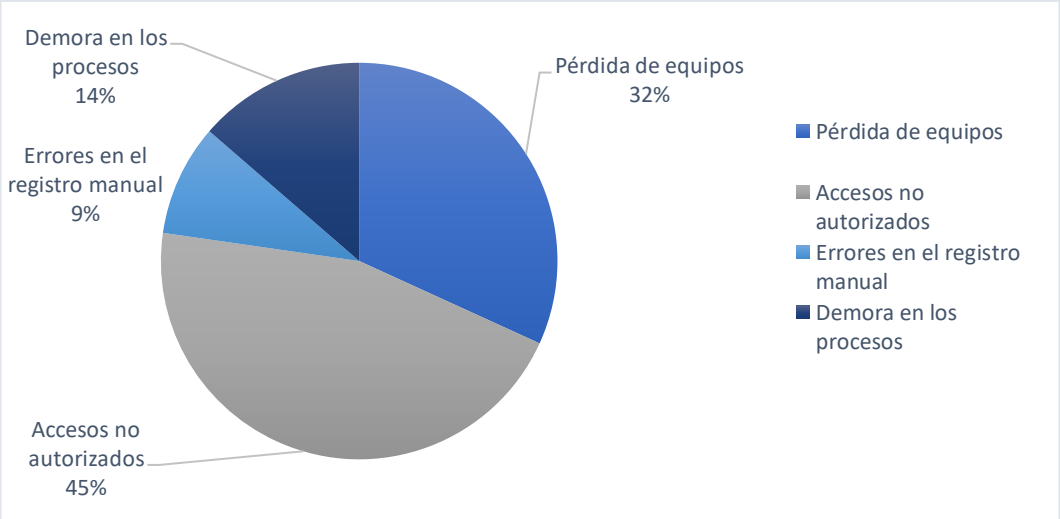


Gráfico 6. Resultados pregunta 6.

Análisis e Interpretación de resultados

El Gráfico 6 establece que los encuestados demostraron como principales riesgos en el control de ingreso y salida de equipos los accesos no autorizados (45%) y la pérdida de equipos (32%). Estos dos indicadores concentran más de las tres cuartas partes de las respuestas (77%), lo que refleja una preocupación prioritaria por la seguridad y la integridad de los equipos.

Además, el 14% de los participantes identificó como riesgo la demora en los procesos, lo que señala ineficiencias operativas que afectan la agilidad de las actividades cotidianas. Finalmente, un 9% destacó los errores en el registro manual, aspecto que, aunque menos frecuente, confirma las limitaciones de los procedimientos actuales para garantizar precisión y confiabilidad en los datos.

Los resultados revelan que los riesgos están vinculados con la vulnerabilidad de los equipos frente a pérdidas o usos indebidos, mientras que los factores relacionados con la gestión administrativa errores y demoras, ocupan un lugar complementario. Sin embargo, los mismos muestran una percepción crítica hacia el control vigente, donde la seguridad física y el acceso regulado son los aspectos más sensibles y de mayor impacto en la operatividad institucional.

Pregunta 7. ¿Qué nivel de seguridad percibe en el proceso actual de control de equipos?

Tabla 15. Resultados de la pregunta 7.

Indicador	Frecuencia	Porcentaje
Baja	31	71%
Media	8	18%
Alta	5	11%
Muy alta	0	0%
Total	**44**	**100%**

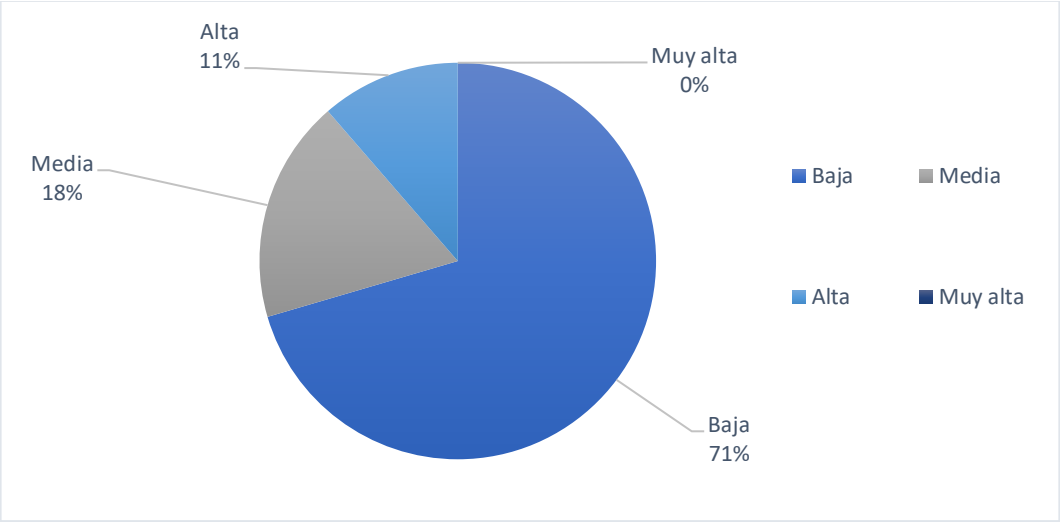


Gráfico 7. Resultados pregunta 7.

Análisis e Interpretación de resultados

El Gráfico 7 evidencia que la mayoría de los encuestados señalo un nivel de seguridad bajo en el proceso actual de control de equipos, con un 71% de respuestas en esta categoría. Le siguen un 18% que considera que la seguridad es media y apenas un 11% que la califica como alta. Ningún encuestado la valoró como muy alta, lo cual resalta la ausencia de confianza plena en los mecanismos vigentes.

Este hecho refleja una percepción crítica hacia el control existente, ya que más de dos tercios de los encuestados opinan que el proceso carece de medidas suficientes para garantizar la protección de los equipos. El hecho de que las valoraciones positivas (“alta” y “muy alta”) apenas representen el 11% muestra una tendencia clara hacia la desconfianza generalizada.

Finalmente, los datos revelan que el proceso actual no es visto como una herramienta robusta ni segura, sino como un sistema débil que expone a la institución a riesgos de pérdida, acceso indebido o fallas en el manejo de la información.

Pregunta 8. ¿Qué tan adecuado considera el proceso actual de autorización para cumplir con las políticas internas de la institución?

Tabla 16. Resultados de la pregunta 8.

Indicador	Frecuencia	Porcentaje
En desacuerdo	23	52%
Neutral	11	25%
De acuerdo	10	23%
Muy de acuerdo	0	0%
Total	**44**	**100%**

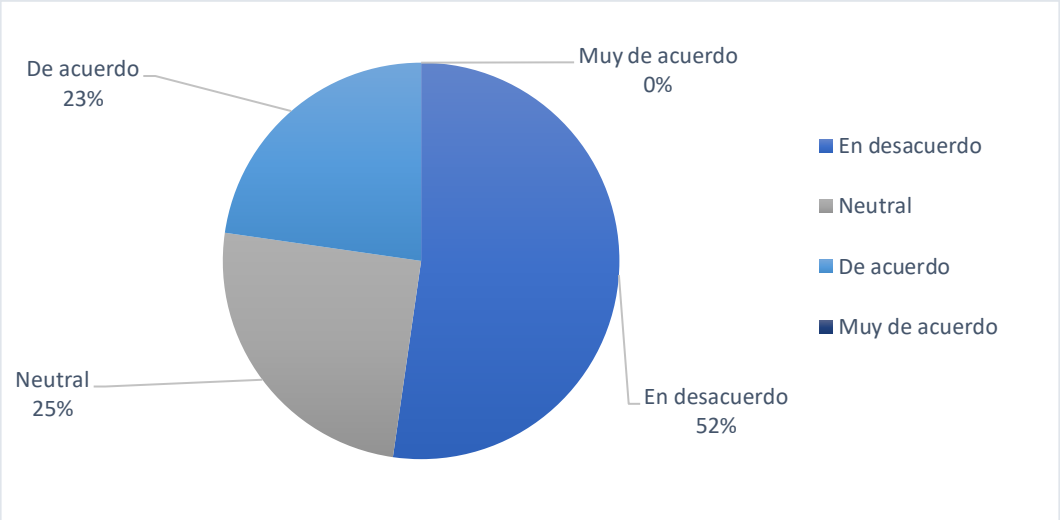


Gráfico 8. Resultados pregunta 8.

Análisis e Interpretación de resultados

Los resultados del Gráfico 8 muestran que más de la mitad de los encuestados (52%) está en desacuerdo con la adecuación del proceso actual de autorización para cumplir con las políticas internas de la institución. Un 25% adoptó una postura neutral, lo que indica cierta indecisión o falta de claridad respecto al funcionamiento del procedimiento. Por otro lado, un 23% señaló estar de acuerdo, mientras que ninguna persona se ubicó en la categoría de muy de acuerdo.

Este hecho refleja una valoración predominantemente negativa hacia el proceso de autorización, ya que solo una minoría lo percibe como adecuado para responder a las políticas internas. La ausencia total de respuestas en el nivel más alto de aprobación evidencia que, dentro de la percepción general, el procedimiento no cumple con la solidez suficiente para garantizar el cumplimiento institucional.

Del mismo modo, la presencia de un cuarto de los encuestados en la categoría neutral muestra que existe un sector que no logra identificar con certeza si el proceso realmente se ajusta a las políticas, lo cual puede estar relacionado con una falta de comunicación o de estandarización en su aplicación.

Pregunta 9. ¿Considera que una aplicación móvil mejoraría el control de ingreso y salida de equipos?

Tabla 17. Resultados de la pregunta 9.

Indicador	Frecuencia	Porcentaje
En desacuerdo	6	14%
Neutral	7	16%
De acuerdo	17	38%
Muy de acuerdo	14	32%
Total	**44**	**100%**

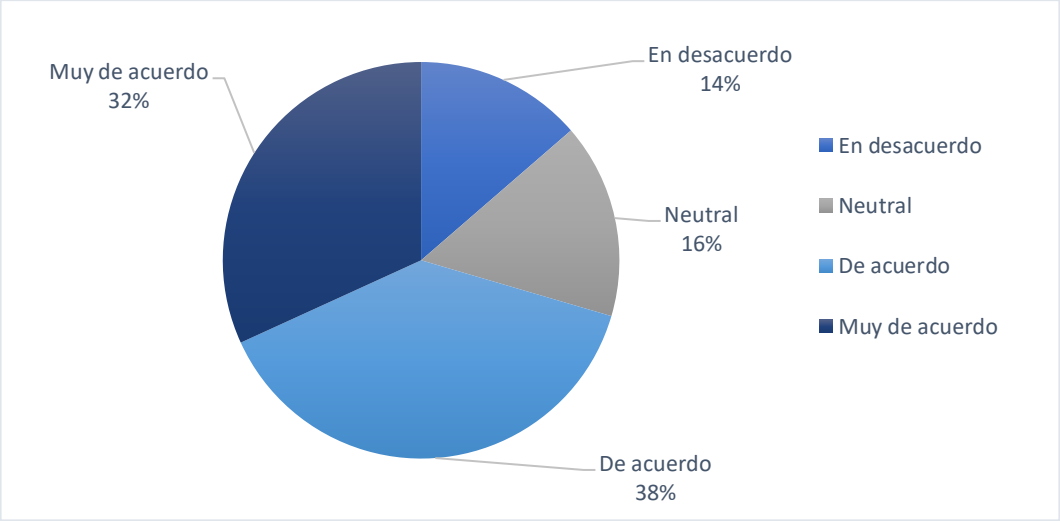


Gráfico 9. Resultados pregunta 9.

Análisis e Interpretación de resultados

Los porcentajes del Gráfico 9 muestran una percepción favorable hacia la posibilidad de implementar una aplicación móvil para el control de ingreso y salida de equipos. El 38% de los encuestados indicó estar de acuerdo con que esta herramienta mejoraría el proceso, y un 32% se manifestó muy de acuerdo. En conjunto, estas dos categorías representan un 70%, lo que evidencia un amplio respaldo a la idea de incorporar un recurso tecnológico en este ámbito.

Por otra parte, un 16% adoptó una posición neutral, lo que sugiere que un sector de los encuestados no logra visualizar con claridad el impacto que podría tener la aplicación en el fortalecimiento de los controles. Finalmente, un 14% expresó estar en desacuerdo, porcentaje minoritario que refleja cierta resistencia o escepticismo frente a la adopción de nuevas herramientas digitales.

Pregunta 10. ¿Qué beneficio considera más importante que debería ofrecer una aplicación móvil para el control de equipos?

Tabla 18. Resultados de la pregunta 10.

Indicador	Frecuencia	Porcentaje
Mayor seguridad en la salida/ingreso	19	43%
Ahorro de tiempo en los registros	13	29%
Reducción de errores humanos	6	14%
Acceso a la información en tiempo real	6	14%
Total	**44**	**100%**

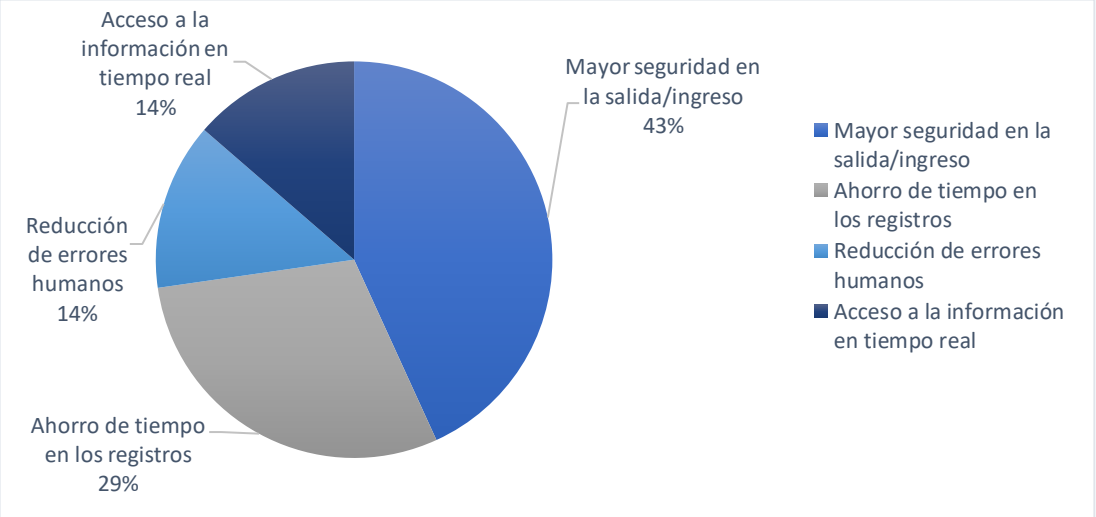


Gráfico 10. Resultados pregunta 10.

Análisis e Interpretación de resultados

Los resultados del Gráfico 10 muestran que un alto porcentaje de los encuestados (43%) considera que el beneficio más importante que debería ofrecer una aplicación móvil para el control de equipos es garantizar mayor seguridad en el ingreso y salida.

Este hallazgo coincide con las percepciones expresadas en preguntas anteriores, donde la seguridad fue identificada como el principal problema en los procesos actuales.

Por consiguiente, un 29% resaltó el ahorro de tiempo en los registros, lo que evidencia que la agilidad y eficiencia operativa son también aspectos valorados por los usuarios en la gestión de los equipos. Además, un 14% señaló como prioridad el acceso a la información en tiempo real, mientras que un 14% destacó la reducción de errores humanos.

En conjunto, los resultados reflejan que los beneficios esperados se concentran principalmente en dos dimensiones: seguridad y eficiencia. La primera aparece como la más relevante y prioritaria, mientras que la segunda se orienta a optimizar la gestión diaria de los registros y la disponibilidad de información confiable.

Resultados de la entrevista

ENTREVISTA 1

Tabla 19. Entrevista completa con el Gerente General.

Lugar y Fecha: Ambato, Tungurahua, 22 de Septiembre de 2025 Entrevistado: Ing. José Luis Acán Bonilla Cargo: Coordinador de TI Objetivo: Recopilar información sobre el proceso actual de control de ingreso y salida de equipos institucionales, con el fin de identificar riesgos, limitaciones y oportunidades de mejora. La información recabada se empleará como soporte principal para el diseño e implementación de una aplicación móvil que permita optimizar los registros, mejorar la seguridad y agilizar los procesos.			
N°	**PREGUNTA**	**RESPUESTA**	**OBSERVACIÓN**
1	¿Desde su experiencia, ¿cuáles son las principales dificultades que ha observado en el control actual de ingreso y salida de equipos?	Una de las principales dificultades que he notado es el tiempo de espera que se genera para aprobar la salida de un equipo. Este proceso suele ser lento y afecta directamente al trabajo de los funcionarios. Además, en varias ocasiones se ha evidenciado la pérdida de activos fijos de la cooperativa debido a la falta de un control más riguroso.	
2	¿Qué procedimientos se siguen actualmente cuando un equipo sale de la institución y quiénes participan en ese proceso?	Actualmente no existe un procedimiento formal establecido para la salida de los equipos. Generalmente, es el personal administrativo quien	

		interviene en este proceso, pero no se cuenta con un protocolo estandarizado que garantice seguridad o trazabilidad.	
3	¿Qué riesgos considera más relevantes al no contar con un sistema automatizado de control?	Los riesgos son varios. Entre los más importantes puedo mencionar la pérdida de equipos, la dificultad para darles un seguimiento adecuado, posibles daños a los mismos y, en el peor de los casos, la suplantación de equipos para sacar uno distinto al autorizado.	
4	¿Qué tan efectivo considera el método actual para garantizar seguridad y trazabilidad de los equipos?	En mi criterio, el método actual resulta deficiente e inseguro, ya que no se lleva un registro claro de las salidas ni un monitoreo de los activos. Esto genera vacíos importantes en el control.	
5	¿Qué situaciones recuerda en las que se hayan presentado errores o inconvenientes con el registro de equipos?	Recuerdo casos en los que se ha producido la suplantación de un equipo al momento de la salida, así como pérdidas o incluso robos de equipos por la falta de registros claros.	
6	¿En su opinión, ¿cómo influye la participación de los guardias de seguridad en la confiabilidad del proceso?	Los guardias de seguridad cumplen con generar una bitácora de las salidas, pero esta información no incluye las características específicas de cada activo. Eso hace que su participación, aunque importante, resulte limitada y con poca incidencia real en la confiabilidad del proceso.	
7	¿De qué manera el tiempo que toma autorizar la salida de un equipo afecta el trabajo diario en la institución?	El tiempo que demora la autorización repercute directamente en el trabajo diario, porque retrasa las actividades de los departamentos de control y afecta la productividad de las áreas que requieren los equipos.	
8	¿Qué tipo de controles adicionales considera necesarios para reducir riesgos en el manejo de los equipos?	Considero fundamental implementar códigos QR en todos los activos que ingresan y salen de la institución. Cada código debería contener la información detallada de las características del equipo y	

		del funcionario responsable, lo que permitiría un control más ágil y seguro.	
9	¿Qué expectativas tendría usted sobre una aplicación móvil que ayude en el control de equipos?	Esperaría que una aplicación de este tipo facilite y agilite todo el proceso de control, permitiendo monitorear en tiempo real y generar registros confiables en el momento en que se autoriza la salida de los equipos.	
10	¿Qué sugerencias daría para que el nuevo sistema sea sostenible en el tiempo y no quede en desuso?	Considero que para que el sistema se mantenga vigente y no quede en desuso es necesario garantizar un mantenimiento constante de la plataforma, realizar actualizaciones periódicas del software y capacitar al personal en su uso. Además, es importante establecer políticas internas que promuevan su aplicación en todos los procesos relacionados con el control de equipos.	
CONCLUSIONES De la entrevista realizada se concluye que el proceso actual de control de ingreso y salida de equipos presenta limitaciones significativas que afectan la seguridad y la eficiencia institucional, debido a la falta de procedimientos formales, registros poco confiables, demoras en las autorizaciones y una participación limitada del personal de seguridad, lo que incrementa los riesgos de pérdida, robo, suplantación y daños en los activos. El entrevistado señaló como indispensables la implementación de herramientas tecnológicas, como códigos QR y aplicaciones móviles, que agilicen los procesos, garanticen la trazabilidad y fortalezcan la productividad, destacando además que la sostenibilidad del sistema dependerá del mantenimiento constante, actualizaciones periódicas, capacitación del personal y políticas institucionales que aseguren su aplicación permanente; en definitiva, se evidencia la necesidad urgente de modernizar y automatizar el control de activos para reducir riesgos y optimizar la gestión administrativa y de seguridad de la institución.			

FICHA DE OBSERVACIÓN

Tabla 20. Ficha de Observación rellenada.

Fecha: Ambato, Tungurahua, 22 de Septiembre de 2025							
Hora de inicio: 08:00H AM							
Hora de fin: 10:00H AM							
Ubicación: Ambato - Simón Bolivar 7-22 y Joaquín Ayllon							
Aspectos para observar	Indicador	Cumplimiento					Comentario
		1	2	3	4	5	
Procedimiento de control	Se observa la existencia de un protocolo formal para registrar y autorizar	X					No existe un protocolo formal establecido para registrar y

	el ingreso y salida de equipos institucionales.						autorizar la salida e ingreso de equipos. Las acciones se realizan de manera manual y dependen del criterio del personal, lo cual genera demoras, poca trazabilidad y riesgo de pérdida o sustitución de activos.
Participación del personal responsable	El personal administrativo, técnico y de seguridad participa activamente en el control y verificación de los equipos.		X				La participación del personal administrativo y de seguridad es limitada, ya que no existe una distribución clara de responsabilidades ni un seguimiento coordinado entre áreas, lo que afecta el control integral de los equipos.
Registro y trazabilidad de equipos	Cada equipo cuenta con un registro que detalla responsable, destino, fechas de salida y retorno, y estado del activo.	X					No se lleva ningún tipo de registro que permita identificar la salida, destino o responsable de los equipos. Esta ausencia total de control impide realizar seguimiento, verificar retornos o determinar la ubicación actual de los activos, generando un alto riesgo de pérdida o suplantación.
Uso de herramientas tecnológicas	Se utilizan herramientas tecnológicas (sistemas digitales, bases de datos, etc.) para controlar los equipos.	X					Los registros se realizan de forma manual en documentos físicos o planillas sin estandarización, dificultando el seguimiento del estado, destino y responsable de

							cada equipo, así como la verificación posterior.
Seguridad en los puntos de control	Se aplican medidas de seguridad efectivas en el ingreso y salida, verificando los datos del equipo y del responsable.	X					Los controles de seguridad son básicos y se limitan a la revisión visual o verbal. No se aplican mecanismos formales de validación como códigos, autorizaciones digitales o escaneo de datos, lo que debilita la seguridad del proceso.
CONCLUSIONES A partir de la observación realizada, se evidencia que el proceso actual de control de ingreso y salida de equipos en la cooperativa presenta un nivel de cumplimiento muy bajo, reflejando la ausencia de procedimientos formales y herramientas tecnológicas que garanticen la trazabilidad y seguridad de los activos. No se lleva un registro de los equipos ni existe un protocolo definido para su ingreso o salida, lo que genera desorganización y dificulta el seguimiento. Además, la participación del personal responsable es limitada y los controles de seguridad se realizan de manera básica, sin mecanismos de validación o respaldo digital. En conjunto, estas deficiencias incrementan el riesgo de pérdida, sustitución o uso indebido de los equipos institucionales, evidenciando la necesidad urgente de implementar un sistema automatizado que permita un control eficiente, seguro y verificable de los activos tecnológicos.							

Criterio:

1= Muy bajo

2= Bajo

3= Moderado

4= Alto

5= Muy Alto

2.2.4 Procesamiento y análisis de datos

En base a la recolección de datos obtenidos a través de la encuesta, entrevista y ficha de observación se han extraído conclusiones significativas que respaldan la necesidad

de implementar mejoras en los procesos de control de ingreso y salida de equipos institucionales en la Cooperativa de Ahorro y Crédito Credi Ya Ltda.

- La gestión actual del control de equipos presenta deficiencias críticas, evidenciadas por la ausencia total (100%) de un registro formal para el ingreso y salida de activos. Esta situación se agrava considerablemente al considerar que el 70% de los movimientos de equipos ocurren de manera frecuente o constante, generando una brecha operativa que expone a la institución a riesgos significativos de pérdida, robo o suplantación de equipos.

- Existe un resultado general de baja confiabilidad en el método actual, donde el 66% de los encuestados lo señala como "nada confiable" y solo el 11% lo considera confiable. Esta valoración negativa se correlaciona directamente con la alta frecuencia de errores e inconsistencias reportadas, donde el 66% de los participantes indica que estos ocurren frecuentemente o siempre, confirmando las debilidades sistémicas del proceso actual.

- El 59% del personal necesita registrar movimientos de equipos de manera frecuente o constante en sus áreas de trabajo, lo que refleja significativamente con la ausencia de herramientas formales para realizar esta actividad. Esta discrepancia entre necesidad operativa y recursos disponibles genera ineficiencias que afectan directamente la productividad institucional.

- Los riesgos más relevantes identificados se centran en dos categorías principales: accesos no autorizados (45%) y pérdida de equipos (32%), que en conjunto representan el 77% de las preocupaciones del personal. Estos hallazgos coinciden plenamente con las situaciones reportadas en la entrevista gerencial, donde se mencionaron casos específicos de suplantación, pérdidas y robos de equipos.

- La percepción de seguridad en el proceso actual es significativamente baja, con un 71% que la califica como baja y ningún encuestado que la considere muy alta. Esta valoración se complementa con el 52% que está en desacuerdo con la adecuación del proceso de autorización para cumplir con las políticas

internas, evidenciando una falta de alineación entre las prácticas operativas y los estándares institucionales.

- Las demoras en los procesos de autorización impactan negativamente la productividad institucional, aspecto señalado por el 16% de los encuestados como un riesgo relevante y confirmado en la entrevista gerencial, donde se indicó que estos retrasos afectan directamente el trabajo diario de los departamentos y áreas que requieren los equipos.

- Existe una amplia aceptación hacia soluciones tecnológicas, con un 71% de los encuestados que está de acuerdo o muy de acuerdo con que una aplicación móvil mejoraría el control de equipos. Los beneficios más valorados son: mayor seguridad en la salida/ingreso (43%), ahorro de tiempo en los registros (29%), acceso a la información en tiempo real (14%) y reducción de errores humanos (14%).

- La implementación de códigos QR en todos los activos fue identificada como un control adicional fundamental por el Coordinador de TI, quien sugirió que cada código contenga información detallada de las características del equipo y del funcionario responsable, permitiendo un control más ágil y seguro.

- La adaptación de una aplicación móvil desarrollada en Flutter, integrada con tecnología de códigos QR para identificación de activos, sistemas de autenticación segura para autorización de salidas, registro en tiempo real con trazabilidad completa, generación automática de reportes y respaldos en la nube, fortalecería la seguridad, eficiencia y confiabilidad integral de las operaciones de control de equipos en la Cooperativa de Ahorro y Crédito Credi Ya Ltda., disminuyendo los riesgos identificados y optimizando los tiempos de respuesta en los procesos operativos.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Análisis de procesos

En este apartado se analiza el proceso de ingreso y salida de estaciones de trabajo en la Cooperativa de Ahorro y Crédito Credi Ya Ltda. El análisis contempla dos escenarios: el procedimiento actual basado en gestión manual con limitaciones en el registro y seguimiento de equipos, frente al proceso mejorado mediante la implementación de la aplicación móvil. Esta comparación permite identificar las mejoras operativas que otorga la solución tecnológica propuesta, demostrando cómo se automatiza el control de activos y se reducen los riesgos de seguridad detectados en la fase de diagnóstico.

3.1.1 Modelado de procesos

Se presenta el detalle correspondiente al proceso de control de ingreso y salida de estaciones de trabajo, el cual será implementado mediante el desarrollo de la aplicación móvil.

a. Proceso actual para el control de ingreso y salida de estaciones de trabajo.

El control de ingreso y salida de estaciones de trabajo en una cooperativa de ahorro y crédito tiene como propósito registrar, monitorear y gestionar el acceso del personal a los equipos informáticos asignados, garantizando la seguridad de la información, la trazabilidad de las operaciones y el uso adecuado de los recursos tecnológicos. Este proceso es fundamental para mantener la integridad de los datos, prevenir accesos no autorizados y optimizar la disponibilidad de los recursos informáticos dentro del marco operativo de la institución financiera.

Actualmente, la Cooperativa de Ahorro y Crédito Credi Ya Ltda. no cuenta con un sistema automatizado para el registro y control de ingreso y salida de estaciones de trabajo, por ende, el acceso a los equipos se realiza de manera libre y sin ningún tipo de registro formal, lo que genera las siguientes problemáticas:

- Falta de trazabilidad.
- Riesgos de seguridad.
- Dificultad en la gestión de recursos.
- Incumplimiento de normativas.
- Ausencia de auditoría.

La falta de procesos tal como se demuestra en la Figura 11, resalta la necesidad de implementar una solución tecnológica que permita automatizar y sistematizar el proceso, garantizando el cumplimiento de las políticas internas de seguridad y las normativas vigentes establecidas por organismos de control como la Superintendencia de Economía Popular y Solidaria (SEPS), así como estándares internacionales de calidad y seguridad de la información como ISO 9001:2015 e ISO/IEC 27001:2022 (Ver Anexo A y Anexo B, respectivamente).



Figura 11. Diagrama del proceso actual de control de ingreso y salida de estaciones de trabajo.

3.1.2 Modelado de procesos optimizados

a. Proceso optimizado para el control de ingreso y salida de estaciones de trabajo.

El control de ingreso y salida de estaciones de trabajo ha sido optimizado mediante un flujo sistemático que se visualiza en la Figura 12, que garantiza trazabilidad, seguridad y eficiencia en la gestión de dispositivos corporativos. El proceso está diseñado para

registrar en tiempo real el movimiento de equipos mediante un sistema de validación por código QR y notificaciones automatizadas.

El proceso inicia con la asignación de dispositivos a los funcionarios autorizados y la generación de códigos QR únicos para cada estación de trabajo. Cuando un colaborador requiere retirar un equipo, envía una solicitud de salida indicando el motivo y el horario estimado de uso. Esta solicitud es notificada inmediatamente al Oficial de Seguridad para su evaluación.

En el punto de decisión, el Oficial de Seguridad puede aprobar o rechazar la solicitud. Si la solicitud es rechazada, el sistema registra automáticamente el motivo del rechazo y notifica tanto al funcionario solicitante como al personal de seguridad, finalizando el proceso en ese punto.

Cuando la solicitud es aprobada, el flujo continúa con la notificación simultánea al guardia de seguridad y al funcionario autorizado. El guardia procede entonces a verificar la identidad del funcionario mediante el escaneo del código QR asociado al equipo, registrando formalmente la salida del dispositivo en el sistema. Esta acción genera una notificación de salida tanto al funcionario como al oficial de seguridad.

Al momento del retorno, el sistema evalúa si el equipo regresa dentro del horario previamente establecido. Si el funcionario se presenta después de la hora prevista, el sistema genera alertas automáticas dirigidas al oficial de seguridad, al funcionario y al guardia, asegurando que todos los involucrados estén informados de la irregularidad. Independientemente de si hay retraso o no, el guardia verifica nuevamente el código QR del equipo y registra el ingreso en el sistema, completando así el ciclo de control.

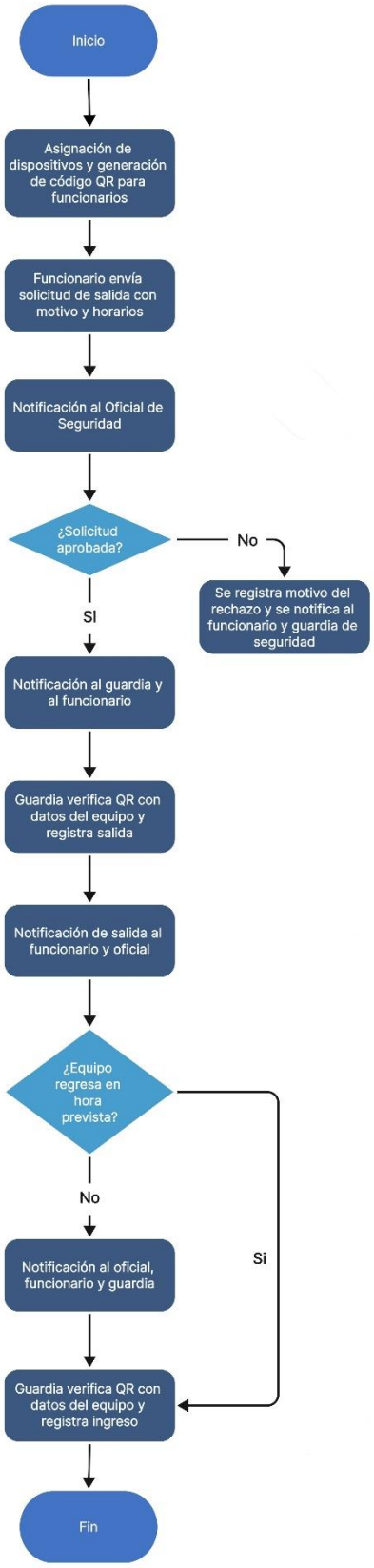


Figura 12. Diagrama optimizado para el proceso de control de ingreso y salida de estaciones de trabajo.

3.2 Framework Flutter para desarrollo móvil multiplataforma.

Flutter fue seleccionado como tecnología de desarrollo con el objetivo de implementar una aplicación móvil que funcione en dispositivos iOS y Android del personal de seguridad y funcionarios de la organización, manteniendo una única base de código que reduzca tiempos de desarrollo y costos de mantenimiento.

La implementación de Flutter en el sistema de control de acceso permite integrar funcionalidades específicas requeridas por el proyecto: escaneo de códigos QR para verificación de equipos, envío de notificaciones push instantáneas entre roles, y sincronización en tiempo real con la base de datos centralizada. Estas capacidades técnicas son esenciales para cumplir con los requerimientos operativos del proceso de control de ingreso y salida de estaciones de trabajo.

El framework facilita la construcción de interfaces diferenciadas según el rol del usuario: pantallas de solicitud y consulta para funcionarios, interfaces de escaneo y registro para guardias de seguridad, y paneles de aprobación y monitoreo para oficiales de seguridad. Esta adaptabilidad permite que cada actor del proceso cuente con herramientas específicas para sus responsabilidades dentro del flujo de control de dispositivos.

La arquitectura modular del mismo permite organizar el código por funcionalidades independientes, lo que simplifica la implementación de actualizaciones, corrección de errores y adición de nuevas características al sistema sin comprometer la estabilidad de los módulos existentes.

A continuación, se exponen las características principales de Flutter en la Tabla 21, proporcionando una visión más amplia de sus capacidades y ventajas en el desarrollo de aplicaciones móviles.

Tabla 21. Características de Flutter.

Característica	Descripción
Multiplataforma / un solo código	Permite crear aplicaciones para móviles (iOS/Android), web, escritorio y dispositivos embebidos desde una única base de código, reduciendo duplicación de trabajo al desplegar en múltiples plataformas.
Hot reload / desarrollo rápido	"Hot reload" y "hot restart" permiten ver cambios de UI y lógica casi al instante sin perder el estado de la app, acelerando la iteración y depuración durante el desarrollo.
Sistema de widgets y UI personalizable	Flutter ofrece una amplia biblioteca de widgets (Material y Cupertino) y un modelo de composición que permite controlar cada píxel para construir interfaces altamente personalizadas y adaptativas.
Rendimiento y compilación nativa (motor de renderizado)	Las apps Flutter se compilan de forma nativa; además, el proyecto ha introducido mejoras en el motor (p. ej. Impeller) para mejorar rendimiento y consistencia gráfica en distintas plataformas.
Soporte de plataformas (móvil, web, escritorio, embebido)	Flutter mantiene soporte estable y en evolución para Android/iOS, web, macOS, Windows, Linux y targets embebidos, con actualizaciones periódicas que ajustan qué versiones de plataformas están soportadas.
Ecosistema de paquetes y plugins	Existe un ecosistema amplio de paquetes (pub.dev) y plugins oficiales/comunitarios (p. ej. integraciones con Firebase) que aceleran la integración de servicios y funcionalidades comunes.
Herramientas y soporte de IDEs	Flutter incluye CLI y extensiones/plug-ins para VS Code y Android Studio/IntelliJ, además de herramientas para depuración, profiling y previews de widgets.
Lenguaje Dart y null safety	Flutter se programa en Dart; Dart provee características modernas (tipado fuerte, null safety, herramientas de compilación) que mejoran la seguridad y el rendimiento del código.
Documentación, roadmap y actualizaciones activas	La documentación oficial y las notas de lanzamiento son activas y frecuentes; el proyecto publica guías "What's new" y un historial de releases para seguir cambios y nuevas capacidades.
Comunidad y casos de uso en producción	Amplia adopción en la industria, repositorios y ejemplos de apps reales; la comunidad mantiene recursos, paquetes y artículos que complementan la documentación oficial.

En concordancia con la tabla 21, Flutter se ha establecido como uno de los frameworks más prácticos para el desarrollo de aplicaciones multiplataforma en la actualidad. Su principal característica se enfoca en la capacidad de generar aplicaciones móviles, web y de escritorio a partir de una sola base de código, lo que optimiza los recursos de desarrollo y reduce significativamente el tiempo de implementación [19].

Por otro lado, una de las características más destacadas es su función de "hot reload", la cual permite visualizar los cambios realizados en el código de forma simultánea sin reiniciar la aplicación, incrementando la eficiencia en la etapa de pruebas y diseño. A ello se suma su amplio sistema de widgets personalizables, que ofrece componentes adaptados tanto al estilo Material Design como a Cupertino, posibilitando interfaces visualmente consistentes y de alta calidad [23].

El rendimiento nativo constituye otro de sus pilares fundamentales, pues Flutter compila directamente a código de máquina mediante el motor Impeller, garantizando una ejecución fluida y estable en diferentes plataformas. Además, el lenguaje Dart brinda seguridad en tiempo de compilación y soporte para null safety, reforzando la confiabilidad del código.

La amplia comunidad de desarrolladores y el ecosistema de paquetes en pub.dev facilitan la integración con servicios como Firebase y herramientas de terceros, potenciando la versatilidad del framework. Finalmente, su documentación actualizada y el soporte continuo de Google reflejan un compromiso con la mejora constante y la innovación tecnológica en el desarrollo de software multiplataforma.

3.2.1 Ventajas y desventajas de Flutter

A continuación, se presenta un análisis basado en investigaciones recientes [24], [25], [26], [27] en base a las ventajas y desventajas de Flutter.

Tabla 22. Ventajas y desventajas de Flutter.

VENTAJAS	DESVENTAJAS
Una sola base de código para múltiples plataformas (iOS, Android, web, escritorio).	Desconocimiento generalizado por ser framework reciente.
Hot Reload: Los cambios se ven instantáneamente sin reiniciar la aplicación.	Tamaño de archivo mayor por incluir motor Skia.
Alto rendimiento: Compila a código nativo con tiempos de carga rápidos.	Comunidad más pequeña comparada con otros frameworks.
Desarrollo más rápido y económico.	Dart es un lenguaje poco usado (posición 46 en popularidad).
Dart es fácil de aprender para desarrolladores con poca experiencia.	Dificultad para integrar librerías de terceros nativas.
Líder multiplataforma: Usado por 46% de desarrolladores en 2023.	Curva de aprendizaje inicial con sintaxis de Flutter.
Interfaz personalizable con amplia colección de widgets.	Menor cantidad de librerías disponibles.
Tiempo de comercialización rápido (TTM ágil).	Retrasos en actualizaciones cuando salen nuevas versiones de SO.

3.2.2 Casos de éxito utilizando Flutter

El framework Flutter ha sido adoptado por empresas líderes a nivel mundial, demostrando su capacidad para crear aplicaciones de alto rendimiento y experiencia de usuario excepcional. La siguiente tabla presenta casos representativos de organizaciones que han implementado Flutter con resultados sobresalientes, según fuentes consultadas [28], [29], [30], [31]. Estos ejemplos evidencian la efectividad de Flutter como solución multiplataforma en diversos sectores.

Tabla 23. Casos de éxito utilizando Flutter.

EMPRESA	INDUSTRIA	IMPLEMENTACIÓN
Alibaba (Xianyu)	Comercio electrónico	La aplicación Xianyu, el mercado de segunda mano más grande de China con 200 millones de usuarios registrados, fue desarrollada íntegramente en Flutter para mejorar significativamente la experiencia de usuario.
Google Pay	Servicios financieros digitales	Con más de 100 millones de usuarios en decenas de países, migró a Flutter reduciendo el código en un 35% y ahorrando entre 60-70% del tiempo de los desarrolladores.
Nubank	Banca digital	El banco digital más grande de América Latina con 48+ millones de usuarios implementó Flutter, reduciendo el tiempo de publicación de aplicaciones en un 30% y lanzando soluciones de seguros de vida en solo tres meses.
BMW (My BMW)	Automotriz	Lanzó la aplicación My BMW en 47 países en menos de un año con Flutter, desplegando más de 10,000 versiones de 96 variantes diferentes de la aplicación en tiempo record.
Google Ads	Publicidad digital	Desarrolló su aplicación de gestión de campañas publicitarias en Flutter, permitiendo mantener el funcionamiento de Google Ads desde dispositivos móviles.

EMPRESA	INDUSTRIA	IMPLEMENTACIÓN
MGM Resorts	Hospitalidad y entretenimiento	La nueva aplicación MGM Rewards fue rediseñada en solo 4 meses con Flutter, reduciendo el código a la mitad y cuadruplicando la velocidad de entrega para más de 400 restaurantes.
LG Electronics	Electrónica de consumo	Planea usar Flutter para aplicaciones clave en televisores con webOS a nivel mundial a partir de 2025, combinando velocidad de desarrollo rápida con rendimiento excelente.
Toyota	Automotriz	Incluye Flutter en las pantallas de sus automóviles para crear y desarrollar sistemas vehiculares.
Tencent	Tecnología y redes sociales	Una de las compañías tecnológicas más grandes del mundo utiliza Flutter para varias de sus aplicaciones, incluyendo redes sociales, juegos y servicios financieros.
Reflectly	Salud y bienestar	Herramienta de bienestar personal potenciada por inteligencia artificial que utiliza Flutter, logrando gran adopción gracias a su diseño atractivo y facilidad de uso.

3.2.3 Comparativa de versiones

Las versiones del framework Flutter [32] han experimentado una evolución considerable desde su lanzamiento. A continuación, se detallan las iteraciones más significativas del framework junto con sus mejoras y funcionalidades más destacadas:

Tabla 24. Comparativa de versiones que constituye Flutter.

Año	Versión	Lanzamiento	Características destacadas
2024	3.27	Diciembre 2024	• Introducción del motor Impeller como predeterminado en Android, mejorando notablemente el rendimiento gráfico. • Actualización de widgets Cupertino (iOS) con nuevos estilos y personalización. • Cambios en la gestión de recursos: eliminación del archivo AssetManifest.json tradicional para optimizar carga. • Mejoras en rendimiento, tiempo de compilación y menor uso de memoria.
2025	3.28	Enero 2025	• Versión de transición enfocada en estabilidad y pruebas previas de nuevas APIs. • Ajustes en el sistema de internacionalización (i18n) y generación de recursos. • Mejoras en Material 3, especialmente en componentes de navegación y formularios. • Cambios en la estructura de plugins (*flutter_plugins* y DSL de Gradle).
2025	3.29	Febrero 2025	• Rendimiento y fidelidad gráfica mejorados en todas las plataformas (Android, iOS, Web, macOS, Linux). • Actualizaciones de Material 3 (sliders, chips, y tooltips renovados). • DevTools rediseñado con nuevo inspector visual y trazas de rendimiento más claras. • Impeller optimizado y más estable.

Año	Versión	Lanzamiento	Características destacadas
			• Enfoque en rendimiento multiplataforma y accesibilidad.

Se ha seleccionado la versión 3.27 de Flutter para el desarrollo de la aplicación móvil, ya que proporciona un equilibrio óptimo entre innovación tecnológica y estabilidad, lo que es esencial para el proyecto de control de ingreso y salida de estaciones de trabajo. Esta versión, lanzada en diciembre de 2024, introduce el motor Impeller como predeterminado en Android, lo cual mejora el rendimiento gráfico y la fluidez de la interfaz de usuario, aspectos críticos para garantizar una experiencia responsiva en las operaciones diarias de registro de personal. Además, incorpora actualizaciones significativas en los widgets Cupertino para iOS, optimizaciones en la gestión de recursos mediante la eliminación del archivo AssetManifest.json tradicional, y mejoras sustanciales en el tiempo de compilación y uso de memoria.

La decisión de no optar por versiones más recientes como la 3.28 (enero 2025) o la 3.29 (febrero 2025) se fundamenta en consideraciones prácticas de desarrollo. Si bien estas versiones posteriores ofrecen mejoras adicionales en Material 3, DevTools rediseñado y optimizaciones continuas en Impeller, representan versiones de transición con cambios estructurales importantes en la gestión de plugins, internacionalización y arquitectura interna que aún se encuentran en fase de adopción y ajuste por parte de la comunidad de desarrolladores. Por lo tanto, la versión 3.27 ha demostrado ser suficientemente practica y estable, con un ecosistema de paquetes consolidado y amplia documentación disponible, lo que minimiza el riesgo de enfrentar problemas de compatibilidad o errores inesperados durante el desarrollo.

3.3 Gestor de Base de Datos

Para el desarrollo del presente proyecto, se ha decidido emplear MongoDB versión 6.0.22 como sistema de gestión de bases de datos para la aplicación móvil, dado que esta versión ofrece alto rendimiento, flexibilidad y escalabilidad, lo que resulta esencial para el correcto funcionamiento de un sistema de control de ingreso y salida de estaciones de trabajo en tiempo real.

Esta elección responde no solo a las capacidades avanzadas de MongoDB 6.0.22, como su arquitectura orientada a documentos que facilita el almacenamiento de datos semiestructurados y su rendimiento optimizado en operaciones de lectura/escrituras concurrentes, sino también a su robustez en entornos móviles mediante MongoDB Realm, ampliamente utilizado en aplicaciones empresariales por su capacidad de sincronización offline y modelo de licencia flexible.

Al tratarse de una base de datos NoSQL, se garantiza la agilidad en el desarrollo y la capacidad de adaptarse a cambios en la estructura de datos sin afectar el funcionamiento del sistema, aprovechando al máximo las funcionalidades requeridas para el registro dinámico de eventos de acceso.

```
admin@MacBook-Pro-de-admin ~ % mongod --version
db version v6.0.22
Build Info: {
    "version": "6.0.22",
    "gitVersion": "ee527360b84c6798535ee0895de3c7186b3522f9",
    "modules": [],
    "allocator": "system",
    "environment": {
        "distarch": "x86_64",
        "target_arch": "x86_64"
    }
}
admin@MacBook-Pro-de-admin ~ %
```

Figura 13. Versión de MongoDB.

3.4 Metodología de Desarrollo Móvil

En base a las fuentes revisadas, se ha elaborado una tabla comparativa que analiza dos metodologías ágiles: Extreme Programming (XP) y Mobile-D. La Tabla 25 presenta las características más representativas, fortalezas, limitaciones y ámbitos de aplicación de cada enfoque, ofreciendo una visión precisa de sus principios y prácticas fundamentales. La información expuesta permite comprender cómo XP promueve la calidad técnica y la respuesta rápida ante los cambios mediante iteraciones cortas y colaboración continua, mientras que Mobile-D se orienta al desarrollo ágil de aplicaciones móviles, priorizando la adaptabilidad a diferentes dispositivos, plataformas y entornos tecnológicos dinámicos.

Tabla 25. Metodologías para desarrollo móvil.

Característica	XP (eXtreme Programming)	Mobile-D
Enfoque característico	Enfoque ágil que enfatiza calidad técnica, simplicidad, feedback rápido, adaptabilidad al cambio.	Enfoque ágil especializado para desarrollo de aplicaciones móviles, con fases adaptadas al entorno móvil y alta adaptación a dispositivos, plataformas y entrega rápida.
Tamaño de equipo / contexto típico	Equipos pequeños a medianos, típicamente hasta 10-20 personas, altamente colaborativos.	Equipos pequeños, focalizados en desarrollo móvil donde se necesitan velocidad, adaptabilidad y recursos técnicos móviles especializados.
Iteraciones / ciclo de trabajo	Ciclos muy cortos (por ejemplo 1-2 semanas), liberaciones frecuentes e integración continua.	Fases estructuradas para móvil: • Exploración • Iniciación • Producción • Estabilización Pruebas del sistema, con iteraciones dentro de estas fases.
Principales prácticas técnicas o distintivas	• Programación en pareja (pair programming) • Desarrollo orientado a pruebas (TDD) • Refactorización frecuente • Integración continua • Cliente "in situ" (Onsite customer)	Adaptación al entorno móvil: • Manejo de restricciones móviles (dispositivos, red, plataforma). • Historia de usuario + tarjetas de tarea propias del móvil. • Entregas frecuentes y adaptadas al móvil.
Flexibilidad ante cambios	Alta: acepta cambios incluso en etapas avanzadas, gracias a iteraciones cortas y feedback constante.	Muy alta también, pero con enfoque específico en el entorno móvil, adaptarse a nuevos dispositivos, plataformas, requerimientos de usuario móvil.
Fortaleza clave	Entrega de software de alta calidad con capacidad de respuesta rápida ante los cambios, fomentando buenas prácticas técnicas y equipo colaborativo.	Adaptación rápida y eficiente al entorno móvil, con entrega enfocada en dispositivos, plataformas y usuarios móviles, y con estructura de fases para mitigar riesgos móviles.
Cuando es más adecuado usarlo	Proyectos de software donde los requisitos pueden cambiar a menudo, se busca alta calidad técnica, equipo pequeño-mediano, entrega rápida.	Proyectos de desarrollo de apps móviles (o soluciones móviles) que requieren velocidad, adaptación a múltiples dispositivos/plataformas, equipos pequeños y respuesta rápida al usuario móvil.

De acuerdo a las características comparativas de las metodologías de desarrollo móvil presentadas en la Tabla 25, se ha seleccionado MOBILE-D como la metodología más adecuada para el desarrollo de la aplicación móvil de control de ingreso y salida de estaciones de trabajo. Esta selección se fundamenta en que MOBILE-D está específicamente diseñada para el desarrollo de aplicaciones móviles, incorporando fases estructuradas (Exploración, Iniciación, Producción, Estabilización y Pruebas del sistema) que se adaptan perfectamente a las particularidades del entorno móvil, tales

como las restricciones de dispositivos, conectividad de red variable y compatibilidad multiplataforma entre Android e iOS. Además, esta metodología está optimizada para equipos pequeños y focalizados, permitiendo una respuesta rápida ante los requerimientos específicos de usuarios móviles y facilitando entregas frecuentes adaptadas al contexto de dispositivos móviles, aspectos cruciales considerando el cronograma ajustado del proyecto y la necesidad de implementar un sistema funcional.

Aunque XP (eXtreme Programming) es una metodología ágil reconocida que enfatiza la calidad técnica mediante prácticas como programación en pareja, desarrollo orientado a pruebas "Test-Driven Development (TDD)" y refactorización frecuente, su enfoque está orientado al desarrollo de software en general sin considerar las particularidades inherentes al ecosistema móvil. Si bien XP ofrece alta flexibilidad ante cambios y es efectiva para equipos pequeños a medianos de hasta 10-20 personas, sus prácticas técnicas distintivas como la integración continua y el cliente "in situ" resultan más apropiadas para proyectos de software tradicional donde los requisitos cambian frecuentemente, pero no abordan específicamente desafíos móviles como la optimización para múltiples dispositivos, gestión de recursos limitados, sincronización offline o adaptación a diferentes tamaños de pantalla y sistemas operativos.

Por estas razones, MOBILE-D es la opción más adecuada al proporcionar un marco metodológico que mitiga los riesgos propios del desarrollo móvil, permitiendo manejar eficientemente las restricciones técnicas de los dispositivos móviles, adaptarse rápidamente a las diferentes plataformas requeridas (Android e iOS), y entregar una solución funcional que responda a las necesidades específicas del personal de la empresa, garantizando al mismo tiempo una estructura de trabajo clara mediante sus fases definidas que facilita la planificación, seguimiento y control del proyecto.

3.5 Desarrollo de la Propuesta

En la presente sección se describe de manera detallada el desarrollo de la propuesta, abarcando las distintas fases de la metodología MOBILE-D empleada en la Figura 14 para abordar el sistema de control de ingreso y salida de estaciones de trabajo en la Cooperativa de Ahorro y Crédito Credi Ya Ltda. Cada fase comprende diversas tareas y prácticas metodológicas específicas, estructuradas con el propósito de garantizar una

implementación sistemática y coherente que se alinee con los objetivos establecidos para el proyecto.

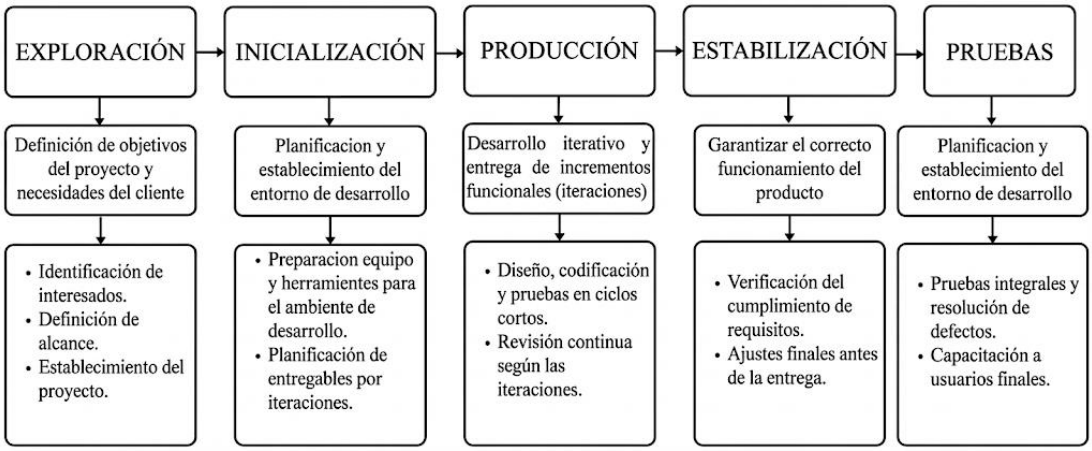


Figura 14. Fases de la metodología MOBILE-D.

3.5.1 Exploración

Durante la exploración, se llevan a cabo una serie de actividades fundamentales orientadas a garantizar una comprensión integral del proyecto y facilitar una planificación apropiada del mismo.

a. Definición de los Interesados

En la Tabla 26 se detallan los distintos interesados (stakeholders) del proyecto, sus roles específicos y el tipo de vinculación que mantienen con el desarrollo de la aplicación móvil. Esta información permite visualizar de manera clara a los actores principales involucrados y el nivel de participación que cada uno desempeña en el proceso de implementación del sistema.

Tabla 26. Interesados "stakeholders".

Interesados	Descripción
Cooperativa de Ahorro y Crédito Credi Ya Ltda	Entidad orientada a la administración de productos y servicios financieros.
Personal Administrativo	Empleados de Cooperativa de Ahorro y Crédito Credi Ya Ltda que forman parte del proceso de entrada y salida.
Desarrollador	Persona autora del proyecto, encargada de diseñar, programar, y probar el software para que cumpla con los requisitos del cliente: Cooperativa de Ahorro y Crédito Credi Ya Ltda

b. Definición de Alcance

La aplicación móvil estará orientada al control de ingreso y salida de las estaciones de trabajo de empresa, con el fin de garantizar la trazabilidad de los activos tecnológicos y fortalecer los procesos de seguridad física y administrativa dentro de la institución.

El sistema se enfocará en la gestión integral de los dispositivos asignados a cada funcionario, permitiendo el registro, seguimiento y control mediante códigos QR, así como la autorización digital por parte del personal de seguridad y supervisión.

Las principales funcionalidades que contempla la aplicación son las siguientes:

- Registro y administración de usuarios con diferentes niveles de acceso (Administrador, funcionario, Oficial de Seguridad y Guardia).
- Asignación de dispositivos a usuarios con generación automática de códigos QR.
- Envío de solicitudes de salida de dispositivos con registro de motivo, fecha y hora de salida e ingreso.
- Notificación automática al Oficial de Seguridad para la autorización o denegación de solicitudes.
- Comunicación en tiempo real mediante notificaciones push hacia los distintos roles.
- Registro digital de la salida e ingreso de equipos mediante escaneo de código QR.
- Generación de reportes automáticos sobre movimientos, solicitudes y estados de los dispositivos.
- Validación automática de horarios y estados de solicitudes (pendiente, aprobada, denegada o finalizada).

- ***Requisitos Funcionales***

En base a la investigación de campo aplicada a la población, se definieron las siguientes funcionalidades principales para la aplicación móvil:

Tabla 27. Requisitos funcionales de la aplicación móvil.

Identificador	Requerimiento	Descripción
RF-1	Inicio de Sesión	Permite que los usuarios ingresen al sistema mediante credenciales válidas. Se valida el rol (administrador, funcionario, oficial o guardia) para redirigir al panel correspondiente.
RF-2	Registro de Usuarios	Permite la creación de nuevos usuarios con datos personales, cargo y rol asignado, generando credenciales únicas y notificando por correo electrónico.
RF-3	Asignación de Dispositivos	Permite registrar los dispositivos institucionales, asignarlos a usuarios y generar un código QR con la información completa del activo.
RF-4	Escaneo de Códigos QR	Permite escanear el código QR del dispositivo para verificar su información, estado y permisos de salida o ingreso.
RF-5	Envío de Solicitudes de Salida	El funcionario puede registrar una solicitud de salida indicando el motivo, destino, fechas y descripción del traslado.
RF-6	Autorización o Denegación de Solicitudes	El Oficial de Seguridad puede aprobar o rechazar solicitudes, indicando una justificación.
RF-7	Registro de Salida e Ingreso	El Guardia registra digitalmente la salida y el retorno del equipo, escaneando el código QR y registrando fecha y hora reales.
RF-8	Notificaciones Push	El sistema envía notificaciones automáticas a los usuarios involucrados en cada proceso (funcionario, oficial, guardia).
RF-9	Reportes de Movimientos	Permite generar reportes en formato digital sobre los dispositivos en uso, fuera de la institución, ingresados o retrasados.
RF-10	Gestión de Roles y Permisos	Permite definir los accesos y restricciones de cada rol dentro del sistema para garantizar la seguridad de la información.

- ***Requisitos No Funcionales***

Los requisitos no funcionales establecen las características técnicas y de calidad que la aplicación debe cumplir para garantizar su correcto funcionamiento. En la Tabla 28 se identifica y describe los principales requisitos no funcionales establecidos:

Tabla 28. Requisitos no funcionales.

Identificador	Requerimiento	Descripción
RN-1	Compatibilidad con Dispositivos	La aplicación debe funcionar correctamente en dispositivos móviles con sistemas operativos Android e iOS.
RN-2	Seguridad	El sistema debe garantizar la protección de los datos de los usuarios, incluyendo el uso de cifrado para contraseñas y datos sensibles.
RN-3	Autenticación	Se debe asegurar que solo los usuarios autorizados puedan acceder a la aplicación mediante validación de credenciales.
RN-4	Interfaz Intuitiva	La interfaz debe ser clara, moderna y fácil de usar, permitiendo la interacción fluida entre los distintos módulos.
RN-5	Rendimiento	La aplicación debe responder de manera eficiente, gestionando múltiples solicitudes y notificaciones sin afectar el rendimiento.
RN-6	Conectividad	La aplicación debe sincronizar los datos en tiempo real mediante conexión a internet y garantizar la actualización automática de estados.
RN-7	Escalabilidad	El sistema debe permitir la ampliación de funcionalidades y módulos sin afectar la estructura principal ni el rendimiento general.

- ***Limitaciones***

- La aplicación no contempla la integración con sistemas externos o plataformas de terceros.
- El alcance del sistema se limita exclusivamente al control de ingreso y salida de estaciones de trabajo dentro de la Cooperativa Credi Ya Ltda.
- El funcionamiento requiere conexión a internet para el envío de notificaciones y sincronización de datos en tiempo real.
- No se incluye el control de otros activos ajenos al proceso tecnológico.
- Los dispositivos deben contar con Android 6.0 o superior, o iOS 15 o superior, para asegurar la compatibilidad con las versiones actuales de Flutter.
- La gestión de reportes se limita al entorno interno de la institución y no contempla exportaciones a sistemas de terceros.

c. Establecimiento del proyecto

Esta fase establece las tecnologías y recursos que se utilizan en el desarrollo de la aplicación móvil.

- ***Flutter***

Framework de desarrollo multiplataforma de código abierto creado por Google. Permite desarrollar desde una única base de código aplicaciones nativas para iOS (actualmente el entorno principal del proyecto) y Android, garantizando una interfaz moderna, responsiva y adaptable a diferentes dispositivos.

- ***Dart***

Lenguaje de programación optimizado que permite desarrollar aplicaciones móviles y web, caracterizado por su alto rendimiento y su integración nativa con el framework Flutter. Dart permite implementar la lógica de negocio, la comunicación con el backend, el manejo de controladores GetX, la validación de formularios, la autenticación biométrica (Face ID / huella digital) y la integración con Firebase Messaging para las notificaciones push.

- ***Visual Studio Code***

Editor de código fuente multiplataforma y de alto rendimiento que proporciona un entorno de desarrollo integrado con soporte extensivo para depuración, autocompletado inteligente y gestión de extensiones. Ofrece compatibilidad nativa con el lenguaje Dart mediante plugins especializados, facilitando el desarrollo de aplicaciones Flutter con herramientas como hot reload, análisis de código en tiempo real y gestión eficiente de dependencias.

- ***Node.js y Express.js***

Entorno de ejecución de JavaScript del lado del servidor que permite construir aplicaciones escalables y APIs RESTful. Express.js actúa como framework minimalista que facilita la creación de rutas, middleware y gestión de solicitudes HTTP de manera eficiente.

- ***MongoDB***

Sistema de gestión de bases de datos NoSQL orientado a documentos que almacena información en formato JSON (BSON), ofreciendo flexibilidad en el esquema de datos, escalabilidad horizontal y alto rendimiento en operaciones de lectura y escritura.

- ***Firebase Cloud Messaging (FCM)***

Plataforma de mensajería multiplataforma desarrollada por Google que permite enviar notificaciones push y mensajes de datos a dispositivos Android, iOS y web de forma gratuita, confiable y escalable.

- ***Xcode***

Entorno de desarrollo integrado (IDE) oficial de Apple para crear aplicaciones destinadas a iOS, macOS, watchOS y tvOS, que incluye simuladores, herramientas de depuración, compiladores y gestión de certificados de desarrollo.

3.5.2 Inicialización

La inicialización se orienta a definir los fundamentos técnicos y la estructura organizacional requeridos para la ejecución del proyecto. Dicha preparación garantiza que el proceso de desarrollo se lleve a cabo de forma ordenada y con un enfoque definido hacia los objetivos del producto final.

a. Configuración del ambiente de desarrollo

- **Tipo de aplicación:** Aplicación móvil multiplataforma.
- **Lenguaje de programación:** Dart.
- **Framework de desarrollo:** Flutter.
- **Backend:** Node.js con Express.js para la implementación de servicios RESTful.
- **Servicio de Autenticación:** Autenticación biométrica (Face ID/Touch ID).

- **Sistema gestor de base de datos:** MongoDB (NoSQL orientado a documentos).
- **Servicio de mensajería**: Firebase Cloud Messaging (FCM) para notificaciones push.
- **Formato de intercambio de datos:** JSON (JavaScript Object Notation).
- ***Preparación del Ambiente de desarrollo***

Se detallan las herramientas y tecnologías instaladas-configuradas para el correcto desarrollo de la aplicación móvil:

- Flutter:
    - Lenguaje de programación Dart.
    - Visual Studio Code.
    - Android Studio.
    - Xcode.
- Node.js y Express.js.
- MongoDB.
- Firebase Cloud Messaging (FCM).
- Postman.

b. Planificación de Fases

Tabla 29. Planificación de fases de la metodología empleada.

Fase	Iteración	Descripción
Exploración	Iteración 0	• Identificación de los actores del sistema: Administrador, funcionario, Oficial de Seguridad y Guardia de Seguridad. • Definición de objetivos, alcance y limitaciones del Sistema. • Selección de herramientas tecnológicas: Flutter para el frontend, Node.js + Express para el backend y MongoDB como base de datos principal. • Establecimiento del entorno de desarrollo en Visual Studio Code, Xcode y Android Studio.
Inicialización	Iteración 1	• Levantamiento de requerimientos funcionales y de diseño según los procesos institucionales de control de activos. • Diseño de la arquitectura cliente–servidor y definición de la estructura de colecciones. • Configuración de entorno backend con dependencias.
	Iteración 2	• Diseño del modelo de base de datos en MongoDB y definición de relaciones entre usuarios, roles y dispositivos. • Creación de endpoints para registro, autenticación y manejo de solicitudes. • Pruebas iniciales de conexión entre Flutter y Node.js.
Producción	Iteración 3	• Implementación del módulo de Inicio de Sesión. • Validación de credenciales desde la base de datos y redirección dinámica según el rol detectado (Administrador, Funcionario, Oficial o Guardia). • Pruebas de login, autenticación Face ID y huella dactilar.
	Iteración 4	• Desarrollo del panel principal del Administrador.
	Iteración 5	• Implementación de la gestión de usuarios
	Iteración 6	• Implementación del módulo Asignar Dispositivo y generación de código QR. • Guardado automático del QR generado en la base de datos.
	Iteración 7	• Pantalla de Dispositivos asignados mostrando información de cada uno según el usuario. • Envío de solicitud para iniciar el proceso de salida del equipo.
	Iteración 8	• Implementación del rol Oficial de Seguridad. • Listado de Solicitudes Pendientes, Aprobadas y Denegadas, con opción para autorizar o rechazar.
	Iteración 9	• Desarrollo del rol Guardia de Seguridad. • Implementación del escáner de código QR para verificar la validez del permiso, mostrando los datos completos del dispositivo y del funcionario. • Habilitación de acciones de Registrar Salida e Ingreso del Equipo según el estado actual.
	Iteración 10	• Implementación del módulo de Reportes accesible por roles 3 (Oficial de Seguridad) y 4 (Guardia de Seguridad).
	Iteración 11	• Implementación del módulo Cambio de Contraseña para todos los roles. • Encriptación con bcrypt y actualización del campo contraseña en MongoDB.

Fase	Iteración	Descripción
	Iteración 12	• Integración completa del sistema de Notificaciones Push con Firebase Cloud Messaging (FCM). • Asignación de tokens únicos por usuario. • Validación de comunicación entre los tres roles operativos.
Estabilización	Iteración 13	• Pruebas de integración general entre módulos (usuarios, dispositivos, solicitudes, notificaciones, QR). • Corrección de errores visuales, validación de flujo de navegación y consistencia de datos entre Flutter y Node.js. • Ajuste de diseño UI/UX.
Pruebas	Iteración 14	• Ejecución de pruebas de aceptación con todos los roles en entorno real. • Validación de los flujos: Login → Solicitud → Aprobación → Escaneo → Ingreso/Salida → Reporte. • Comprobación de la trazabilidad completa del proceso y del funcionamiento de notificaciones push.

3.5.3 Diseño de la aplicación móvil

a. Estructura y planificación de la arquitectura de la aplicación móvil.

La arquitectura de la aplicación móvil se ha estructurado para garantizar una interacción eficiente entre los usuarios y el sistema. El personal de la Cooperativa de Ahorro y Crédito Credi Ya Ltda. interactúan con la aplicación mediante un cliente móvil desarrollado en Flutter, el cual proporciona una interfaz de usuario moderna, intuitiva y responsiva. Este cliente móvil establece comunicación con una API RESTful desarrollada en Node.js con Express.js, mediante conexiones seguras a través de Internet. La base de datos, gestionada por MongoDB, almacena toda la información relacionada con usuarios, dispositivos, solicitudes, códigos QR y notificaciones, asegurando la flexibilidad, integridad y disponibilidad de los datos. Adicionalmente, Firebase Cloud Messaging (FCM) se integra al sistema para el envío de notificaciones en tiempo real entre los diferentes roles (funcionarios, oficiales de seguridad y guardias). Esta arquitectura modular facilita la escalabilidad, el mantenimiento y la evolución continua de la aplicación.

b. Diseño de la base de datos.

MongoDB, como sistema de gestión de bases de datos NoSQL orientado a documentos, proporciona una plataforma flexible y escalable para el almacenamiento y manejo eficiente de la información. Se emplea para gestionar los datos relacionados con el control de ingreso y salida de estaciones de trabajo en la Cooperativa de Ahorro

y Crédito Credi Ya Ltda. La versión utilizada es MongoDB 6.0.22, la cual se integra con el backend a través de Mongoose 5.11.4, una librería ODM (Object Data Modeling) que facilita el modelado de esquemas y la conexión con la base de datos.

Dentro de este entorno, se han definido colecciones específicas para organizar y estructurar la información de manera óptima, tales como la colección userIngSal almacena los datos de los usuarios y los dispositivos asignados, integrando además el token FCM para el envío de notificaciones y campos de control como visible. La colección solicitud gestiona las solicitudes de salida e ingreso de equipos, incorporando fechas planificadas y reales, estado del proceso, y banderas específicas para controlar las notificaciones y el registro efectivo de salida e ingreso. Por su parte, la colección RespuestaSolicitud mantiene un historial de aprobaciones y denegaciones, asociando cada acción con la solicitud original e incluyendo la razón y fecha de la decisión. La estructura basada en documentos JSON permite una comunicación directa entre la app Flutter y el backend Node.js/Express, lo que facilita la sincronización, trazabilidad y manejo eficiente de la información. Además, la conexión con la base de datos se establece mediante la variable de entorno MONGO_URL configurada en el archivo ".env", asegurando la centralización de credenciales y la seguridad del sistema.

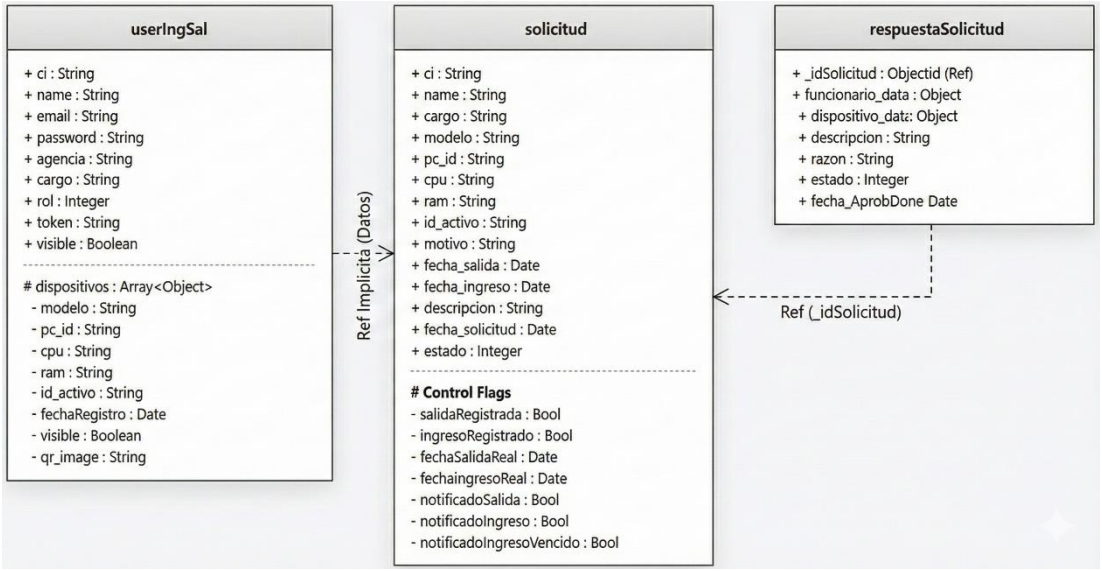


Figura 15. Diagrama de Clases BD.

c. Prototipo

En la presente investigación se desarrollará un prototipo funcional, el cual representará una versión preliminar que definirá las funcionalidades principales y la estructura de la interfaz de usuario del sistema móvil. El diseño se llevará a cabo mediante la herramienta Balsamiq Wireframes, que facilitará la definición de la arquitectura visual, la distribución de componentes interactivos como botones, menús y formularios, así como los flujos de navegación entre pantallas.

El prototipo se caracterizará por ser una etapa fundamental para validar la usabilidad, coherencia del diseño y eficiencia de los procesos antes de proceder con la implementación en Flutter, asegurando una interfaz clara, intuitiva y alineada con los objetivos funcionales del sistema.

- ***Inicio de sesión***

La pantalla de inicio de sesión será el punto de acceso principal al sistema. Esta interfaz presentará dos campos de entrada de texto destinados a las credenciales del usuario: nombre de usuario y contraseña. Se incluirá un botón denominado "Ingresar" posicionado de manera prominente en la zona central de la pantalla.

Adicionalmente, se incorporará la opción "¿Olvidaste tu contraseña?" ubicada debajo de los campos de autenticación. El diseño de esta pantalla mantendrá coherencia con la identidad visual institucional de Credi Ya Ltda., integrando los colores corporativos, tipografía oficial y el logotipo de la entidad en la parte superior de la interfaz.

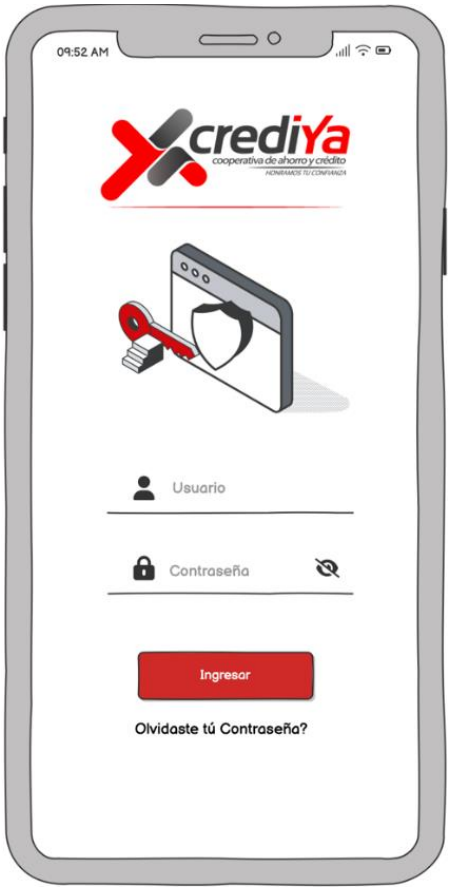


Figura 16. Pantalla Inicio de Sesión.

- ***Menú Principal***

El menú principal presentará una estructura organizada que mostrará las funcionalidades centrales del sistema. En la zona superior se ubicará el logotipo de Credi Ya Ltda. alineado a la izquierda, mientras que en el extremo derecho se posicionará el botón "Cerrar Sesión".

La sección central de la interfaz contendrá un mensaje de bienvenida personalizado con la frase "¡Qué gusto tenerte aquí!" seguido del nombre o rol del usuario autenticado. Debajo de este mensaje se dispondrán tres tarjetas o botones de acceso organizados visualmente: dos elementos ubicados en la fila superior correspondientes a "Usuarios/Dispositivos" y "Dispositivos/QR", y un tercer elemento centrado en la fila inferior identificado como "Cambiar Contraseña". Cada tarjeta incluirá un ícono representativo de su funcionalidad acompañado de su etiqueta descriptiva.



Figura 17. Pantalla Menú Principal.

- ***Gestión de Usuarios***

Gestión de usuarios mostrará un encabezado con el título "Lista de Usuarios". En la zona superior de la interfaz se incluirán filtros desplegables organizados por tipo de usuario: Funcionarios, Oficial de Seguridad, Administrador y Guardia de Seguridad, junto con un campo de búsqueda textual y un botón "Agregar" (+) posicionado en la esquina derecha del campo de búsqueda.

El apartado central mostrará un listado vertical de usuarios registrados en el sistema. Cada registro se presentará en formato de tarjeta o fila que contendrá la información del usuario acompañada de tres íconos de acción alineados horizontalmente: un ícono para visualizar dispositivos asignados, otro para realizar asignaciones de equipos, y un tercero para eliminación de usuarios.

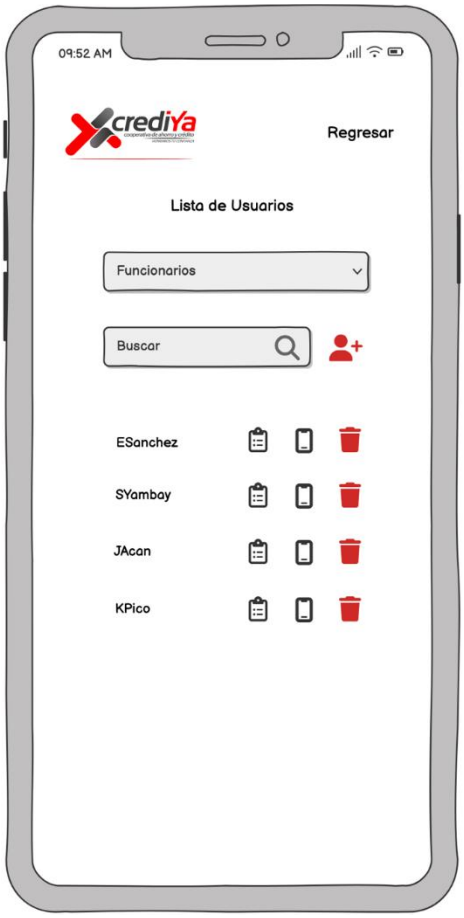


Figura 18. Pantalla Gestión de Usuarios.

- ***Generación de Código QR***

La interfaz de generación de código QR enfocara una estructura dividida en secciones informativas. En la zona superior se mostrará el título "Dispositivo (QR bajo el nombre)" junto con opciones de navegación o retorno.

En el centro de la pantalla se posicionará dos bloques principales de información: el primero dedicado a los datos del funcionario, incluyendo campos para nombre completo, agencia de adscripción y cargo; el segundo bloque presentará las especificaciones técnicas del dispositivo asignado, mostrando campos para modelo, PC_ID, CPU, RAM, ID_ACTIVO y fecha de registro.

En la parte inferior de la pantalla se ubicará el código QR generado, visualizado de manera prominente y centrada. Debajo del código QR se dispondrán dos botones de acción: uno para imprimir y otro para eliminar el código generado.

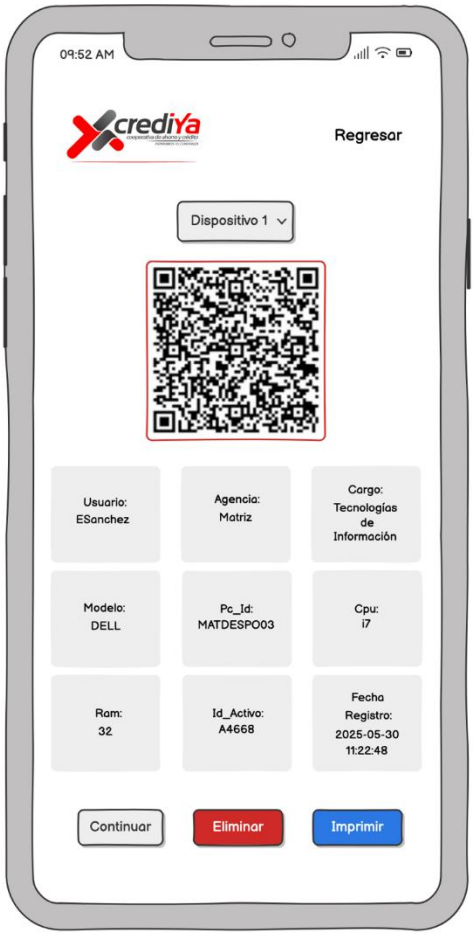


Figura 19. Pantalla Generación de Código QR.

- ***Registro de Usuario Nuevo***

El registro de usuario nuevo tendrá un formulario estructurado con campos de entrada organizados verticalmente. En la zona superior se mostrará el título "Agregar Usuario".

El formulario contendrá los siguientes campos de entrada: Cédula, Usuario, Correo Electrónico, Contraseña, Agencia (como menú desplegable), Área (como menú desplegable) y Rol (como menú desplegable o selector de opciones). Cada campo estará claramente identificado con su etiqueta correspondiente. En la parte inferior del formulario se ubicará un botón prominente denominado "Guardar", centrado o alineado según el diseño establecido.



Figura 20. Pantalla Registro de Usuario Nuevo.

- ***Asignación de Dispositivo***

El apartado de asignación de dispositivo reflejara un formulario estructurado con campos de entrada específicos para información técnica del equipo. En la zona superior se expondrá el título "Asignar Dispositivo"

El formulario contendrá los siguientes campos de entrada organizados verticalmente: Modelo, Pc_Id, Cpu, Ram e Id_Activo. Cada campo estará identificado con su etiqueta correspondiente y mostrará un cuadro de texto para el ingreso de datos.

En la parte superior o inicio del formulario se incluirá información del usuario al cual se asignará el dispositivo, mostrando datos como nombre, cédula o identificador del funcionario seleccionado. En la zona inferior del formulario se colocará un botón denominado "Guardar", posicionado en el centro del bloque.



Figura 21. Pantalla Asignación de Dispositivo.

- ***Visualización de Dispositivo***

Visualización de dispositivo expondrá una estructura organizada que mostrará los datos técnicos del equipo asignado. En la zona superior se ubicará el nombre del equipo.

La sección central contendrá la información técnica del dispositivo distribuida en tarjetas o bloques visuales, cada uno acompañado de un ícono representativo. Se revelarán los siguientes campos: Modelo, PC_ID, CPU, RAM e ID_ACTIVO, organizados de manera vertical u horizontal según el diseño establecido.

En la parte superior de la interfaz se incluirá información del usuario propietario del dispositivo, presentando datos como nombre y cargo del funcionario asignado. En la zona inferior de la pantalla se posicionará de manera notoria el botón "Solicitar Salida del Activo", centrado y con un diseño destacado.

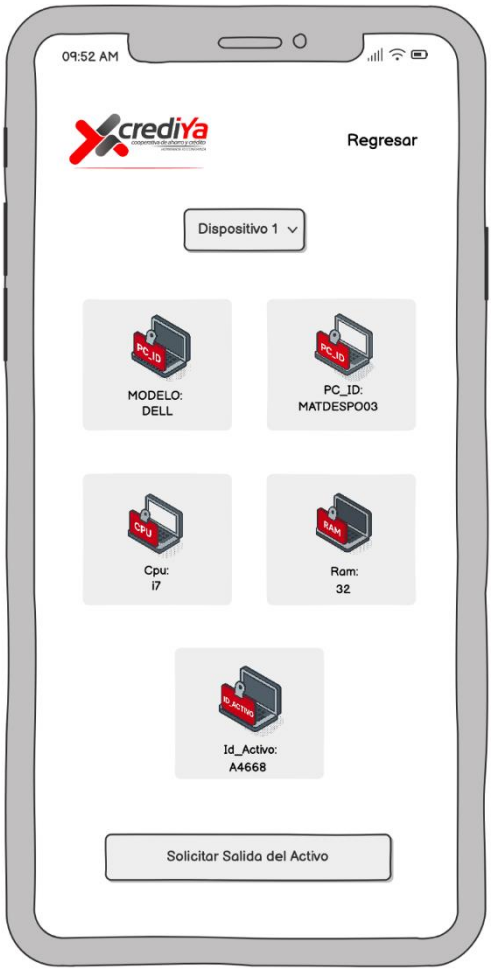


Figura 22. Pantalla Visualización de Dispositivo.

- ***Formulario Solicitud de Salida***

El formulario de solicitud de salida lucirá campos de entrada específicos para tramitar el permiso de traslado temporal de un dispositivo. En la zona superior se mostrará el nombre del dispositivo que solicitará su salida.

La interfaz contendrá un selector o menú desplegable para la selección del dispositivo, seguido de los campos obligatorios organizados verticalmente: Motivo (como menú desplegable o campo de texto), Fecha de Salida (con selector de calendario), Fecha de Ingreso (con selector de calendario) y Descripción (como área de texto expandida para comentarios detallados). Cada campo estará claramente identificado con su etiqueta correspondiente.

En la parte superior del formulario se visualizará información del funcionario solicitante, incluyendo nombre y datos relevantes de identificación, en la zona inferior se ubicará el botón "Enviar Solicitud", centrado.

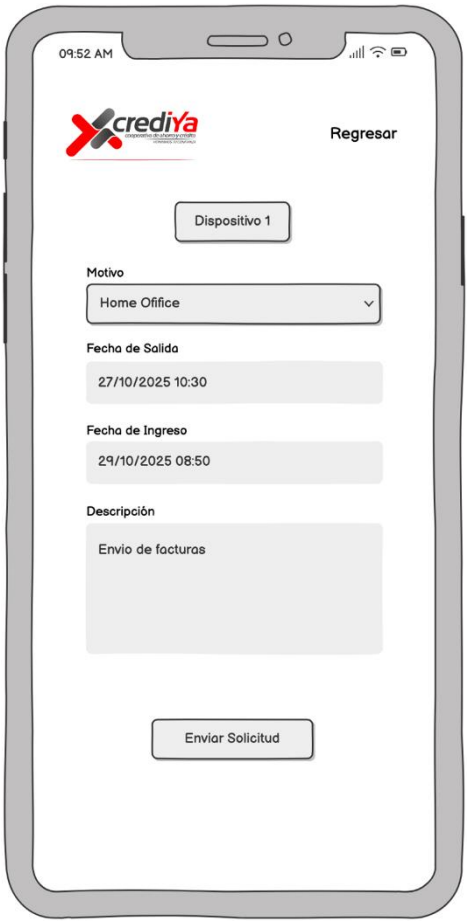


Figura 23. Pantalla Formulario Solicitud de Salida.

- ***Autorización de Solicitud***

La opción de autorización de solicitud mostrará secciones informativas. La zona central contendrá un bloque organizado con la información detallada de la solicitud: fecha de solicitud, datos del funcionario solicitante (nombre, cédula, cargo, agencia), especificaciones técnicas del dispositivo (modelo, PC_ID, características), descripción de la salida y el rango de fechas planificado (fecha de salida y fecha de ingreso). En la parte inferior se ubicarán dos botones de acción posicionados horizontalmente centrados: "Autorizar" y "Denegar". Sobre estos botones se incluirá un campo de texto o área expandida etiquetada como "Razón", destinada al registro obligatorio de la decisión tomada.



Figura 24. Pantalla Autorización de Solicitud.

- ***Escaneo de Código QR***

En la interfaz escaneo de código QR, dentro de su bloque central mostrará la información recuperada del escaneo distribuida en tarjetas organizadas en dos columnas. La columna izquierda contendrá los campos: Cédula, Agencia, Modelo, CPU e ID Activo. La columna derecha presentará: Funcionario, Cargo, PC_ID, RAM y Fecha de Registro. Cada campo estará acompañado de un ícono identificativo y su valor correspondiente.

En la zona inferior se mostrará el estado del permiso con la etiqueta "Permiso:" seguida del estado correspondiente (Aprobado, Pendiente o Rechazado) y la fecha programada de salida con su horario. Debajo de esta información se posicionará de manera prominente un botón de acción denominado "Salida" o "Ingreso" según corresponda, destacado con color corporativo rojo.



Figura 25. Pantalla Escaneo de Código QR.

d. Diseño con Flutter

Para el diseño de las interfaces se emplearon los principales layouts, widgets estructurales, widgets interactivos y widgets visuales, cumpliendo así con el objetivo de estructurar la aplicación dentro del entorno Flutter de manera coherente y funcional.

Widgets de estructura y composición (Layouts)

Los widgets de estructura y composición como Scaffold, Column, Row, Container, Expanded, Padding, SingleChildScrollView, SafeArea y ListView permiten organizar y distribuir los elementos visuales en la pantalla de manera jerárquica y responsive.

- **Scaffold**

Proporciona la estructura visual básica de una pantalla en Flutter, incluyendo áreas como appBar, body, drawer y floatingActionButton, permitiendo construir interfaces completas de forma organizada.

```
return Scaffold(
  backgroundColor: Colors.white,
  body: cargando
      ? const Center(
          child: CircularProgressIndicator(color: Colors.red),
        ) // Center
      : solicitud == null
          ? const Center(child: Text("No se encontró la solicitud."))
          : DetalleSolicitudPage(solicitud: solicitud!),
); // Scaffold
```

Figura 26. Scaffold.

- **Column y Row**

Widgets que organizan elementos de forma vertical (Column) u horizontal (Row), permitiendo alinear y distribuir varios widgets dentro de la pantalla.

```
return Column(
  children: [
    _buildHeader(context),
    const SizedBox(height: 300),
    const Center(child: Text("No hay dispositivos disponibles.")),
  ],
); // Column
```

Figura 27. Column.

```
Row(
  mainAxisAlignment: MainAxisAlignment.spaceBetween,
  children: [
    Image.asset('assets/images/logo1.png', width: 120),
    TextButton(
      onPressed: () => _goHomeByRole(context),
      child: const Text(
        "Regresar",
        style: TextStyle(fontSize: 16, color: Colors.black),
      ), // Text
    ), // TextButton
  ],
), // Row
```

Figura 28. Row.

- **Container**

Widget versátil que permite aplicar márgenes, padding, bordes, tamaños y colores a un elemento, funcionando como un contenedor personalizable.

```
Container(
  width: double.infinity,
  padding: const EdgeInsets.all(20),
  decoration: BoxDecoration(
    color: Colors.grey.shade200,
    borderRadius: BorderRadius.circular(30),
  ), // BoxDecoration
  child: _buildInfo("Razón:", solicitud["razon"] ?? "-"),
), // Container
```

Figura 29. Container.

- **Expanded**

Permite que un widget hijo dentro de un Row, Column o Flex ocupe el espacio disponible restante, distribuyendo el área de manera flexible.

```
Expanded(
  child: const Text(
    'Desea salir de la Aplicación?',
    maxLines: 22,
    style: TextStyle(color: Colors.black, fontSize: 18),
    textAlign: TextAlign.center,
  ), // Text
  //  ),
), // Expanded
```

Figura 30. Expanded.

- **Padding y Margin (dentro de Container)**

Espacios interiores (padding) (Figura 32) o exteriores (margin) (Figura 31) que se aplican a los widgets para mejorar la separación y distribución visual dentro de la interfaz.

```
child: Container(
  margin: const EdgeInsets.only(right: 10),
  child: const Text("Cerrar Sesión",
      style: TextStyle(fontSize: 16, color: Colors.black, fontWeight: FontWeight.w500)),
), // Container
```

Figura 31. Margin.

```
Container(
  padding:
      const EdgeInsets.symmetric(horizontal: 20, vertical: 4),
  decoration: BoxDecoration(
    color: Colors.grey.shade200,
    borderRadius: BorderRadius.circular(30),
  ), // BoxDecoration
  child: DropdownButtonHideUnderline(
    child: DropdownButton<String>(
      dropdownColor: Colors.white,
      value: rolSeleccionado,
      isExpanded: true,
      icon: const Icon(Icons.arrow_drop_down,
          color: Colors.black), // Icon
      items: <String>[
        'Funcionarios',
        'Administradores',
        'Oficial de Seguridad',
        'Guardias de Seguridad',
        'Todos'
      ].map((String value) { // <String>[]
        return DropdownMenuItem<String>(
          value: value,
          child: Text(value,
              style: const TextStyle(color: Colors.black)),
        ); // DropdownMenuItem
      }).toList(),
      onChanged: (valor) {
        if (valor != null) _filtrarPorRol(valor);
      },
      menuMaxHeight: 300,
    ), // DropdownButton
  ), // DropdownButtonHideUnderline
), // Container
```

Figura 32. Padding.

- **SingleChildScrollView**

Permite que el contenido del body sea desplazable cuando excede el tamaño de la pantalla, útil para formularios y vistas largas.

```
child: SingleChildScrollView(
  padding: const EdgeInsets.all(20),
  child: Column(
    children: [
      Container(
        width: double.infinity,
        padding: const EdgeInsets.all(20),
        decoration: BoxDecoration(
          color: Colors.grey.shade200,
          borderRadius: BorderRadius.circular(30),
        ), // BoxDecoration
        child: Column(
          crossAxisAlignment: CrossAxisAlignment.start,
          children: [
            _buildInfo(
              "Fecha de Solicitud:",
              solicitud["fecha_solicitud"] != null
                  ? _formatearFechaHora(
                      solicitud["fecha_solicitud"])
                  : "-"),
            _buildInfo("Cédula:", solicitud["ci"] ?? "-"),
            _buildInfo("Nombre:", solicitud["name"] ?? "-"),
            _buildInfo("Cargo:", solicitud["cargo"] ?? "-"),
            _buildInfo("Modelo:", solicitud["modelo"] ?? "-"),
            _buildInfo("Pc_Id:", solicitud["pc_id"] ?? "-"),
            _buildInfo("Motivo:", solicitud["motivo"] ?? "-"),
            _buildInfo(
              "Fecha de Salida:",
              solicitud["fecha_salida"] != null
                  ? _formatearFechaHora(solicitud["fecha_salida"])
                  : "-",
            ),
```

Figura 33. SingleChildScrollView.

- **SafeArea**

Asegura que el contenido no se superponga con zonas inseguras del dispositivo, como la barra superior, bordes curvos o notch.

```
body: SafeArea(
  child: Column(
    children: [
      Padding(
        padding: const EdgeInsets.symmetric(horizontal: 16, vertical: 10),
        child: Row(
          mainAxisAlignment: MainAxisAlignment.spaceBetween,
          children: [
            Image.asset('assets/images/logo1.png', width: 120),
            TextButton(
              onPressed: () {
                Get.offAll(() => const listaSolicitudesPage());
              },
              child: const Text("Regresar",
                  style: TextStyle(color: Colors.black, fontSize: 16)),
            ), // TextButton
          ],
        ), // Row
      ), // Padding
      const SizedBox(height: 20),
      Expanded(
        child: SingleChildScrollView(
          padding: const EdgeInsets.all(20),
          child: Column(
            children: [
              Container(
                width: double.infinity,
                padding: const EdgeInsets.all(20),
                decoration: BoxDecoration(
                  color: Colors.grey.shade200,
                  borderRadius: BorderRadius.circular(30),
                ), // BoxDecoration
                child: Column(
                  crossAxisAlignment: CrossAxisAlignment.start,
                  children: [
                    _buildInfo(
```

Figura 34. SafeArea.

- **ListView**

Widget que muestra una lista de elementos desplazable, ideal para mostrar datos dinámicos o colecciones de widgets repetitivos.

```
child: ListView(
  padding: const EdgeInsets.symmetric(horizontal: 20, vertical: 12),
  children: [
    Row(
      mainAxisAlignment: MainAxisAlignment.spaceBetween,
      children: [
        Image.asset('assets/images/logo1.png', width: 120),
        TextButton(
          onPressed: () => _goHomeByRole(context),
          child: const Text(
            "Regresar",
            style: TextStyle(fontSize: 16, color: □Colors.black),
          ), // Text
        ), // TextButton
      ],
    ), // Row
    const SizedBox(height: 20),
    const Center(
      child: Text(
        'Cambiar Contraseña',
        style: TextStyle(fontSize: 16, fontWeight: FontWeight.w500),
      ), // Text
    ), // Center
    const SizedBox(height: 20),
    _buildPasswordField(
      label: "Contraseña Actual",
      controller: actualController,
      visible: verActual,
      onToggle: () => setState(() => verActual = !verActual),
      errorText: errorActual,
    ),
```

Figura 35. ListView

Widgets interactivos

Los widgets interactivos como TextField, TextFormField, ElevatedButton, IconButton, FloatingActionButton, GestureDetector y DropdownButton definen cómo el usuario interactúa con la aplicación, capturando entradas de texto, toques, gestos y selecciones.

- **TextFormField**

Campos de entrada que permiten al usuario escribir texto; TextFormField incluye validaciones y funciona mejor dentro de formularios.

```
TextFormField(
  controller: controller,
  keyboardType: keyboardType,
  maxLength: maxLength,
  decoration: InputDecoration(
    counterText: '',
    isDense: true,
    filled: true,
    fillColor: Colors.grey.shade200,
    contentPadding: const EdgeInsets.symmetric(
      horizontal: 20,
      vertical: 14,
    ), // EdgeInsets.symmetric
    border: OutlineInputBorder(
      borderRadius: BorderRadius.circular(30),
      borderSide: BorderSide.none,
    ), // OutlineInputBorder
  ), // InputDecoration
), // TextFormField
```

Figura 36. TextField y TextFormField.

- **ElevatedButton**

Botón con elevación y relleno que ejecuta una acción al ser presionado, usado comúnmente para interacciones principales.

```
ElevatedButton(
  onPressed: cambiarContrasena,
  style: ElevatedButton.styleFrom(
    backgroundColor: Colors.red.shade700,
    shape: RoundedRectangleBorder(
        borderRadius: BorderRadius.circular(30)), // RoundedRectan
    padding:
        const EdgeInsets.symmetric(horizontal: 40, vertical: 15),
  ),
  child: const Text("Actualizar",
      style: TextStyle(color: Colors.white)), // Text
) // ElevatedButton
```

Figura 37. ElevatedButton.

- **IconButton**

Botón que muestra únicamente un ícono y permite ejecutar acciones rápidas o secundarias al tocarse.

```
IconButton(
  icon: const Icon(Icons.assignment_outlined,
      color: Colors.black, size: 22), // Icon
  onPressed: () => mostrarQRParaUsuario(usuario),
), // IconButton
```

Figura 38. IconButton.

- **FloatingActionButton**

Botón circular flotante usado para acciones principales dentro de una pantalla, típicamente ubicado en la esquina inferior derecha.

```
FloatingActionButton(
  onPressed: () {
    Navigator.push(
      context,
      PageRouteBuilder(
        pageBuilder: (_, __, ___) =>
            const AgregarUsuarioPage(),
        transitionsBuilder: (_, animation, __, child) {
          return FadeTransition(
              opacity: animation, child: child); // FadeT
        },
        transitionDuration:
            const Duration(milliseconds: 100),
        reverseTransitionDuration:
            const Duration(milliseconds: 100),
      ), // PageRouteBuilder
    );
  },
  backgroundColor: Colors.transparent,
  elevation: 0,
  child: const Icon(Icons.person_add,
      color: Colors.red, size: 35), // Icon
), // FloatingActionButton
```

Figura 39. FloatingActionButton.

- **GestureDetector**

Widget que detecta gestos del usuario como toques, arrastres o doble toques, permitiendo personalizar interacciones avanzadas.

```
GestureDetector(
  onTap: () =>
      _seleccionarFecha(context: context, esSalida: true),
  child: Container(
    width: double.infinity,
    padding: const EdgeInsets.symmetric(
        horizontal: 15, vertical: 12), // EdgeInsets.symme
    decoration: BoxDecoration(
      color: Colors.grey.shade200,
      borderRadius: BorderRadius.circular(20),
    ), // BoxDecoration
    child: Text(fechaSalida == null
        ? "Selecciona la fecha"
        : DateFormat('dd/MM/yyyy HH:mm')
            .format(fechaSalida!)), // Text
  ), // Container
), // GestureDetector
```

Figura 40. GestureDetector.

- **DropdownButton**

Desplegable que permite seleccionar una opción de una lista de valores visibles al abrir el menú.

```
child: DropdownButton<String>(
  isExpanded: true,
  dropdownColor: Colors.white,
  value: estadoSeleccionado,
  underline: Container(),
  onChanged: _cambiarEstado,
  items: const [
    DropdownMenuItem(value: "0", child: Text("Pendientes")),
    DropdownMenuItem(value: "1", child: Text("Aprobadas")),
    DropdownMenuItem(value: "2", child: Text("Denegadas")),
  ],
), // DropdownButton
```

Figura 41. DropdownButton.

Widgets visuales (UI / Branding)

Los widgets visuales como Text, Card, Image.asset y Divider se encargan de la presentación del contenido y la identidad visual de la aplicación, permitiendo personalizar colores, tipografías, imágenes y estilos.

- **Text**

Muestra texto en pantalla con opciones de estilo, tamaño, color y alineación, siendo uno de los widgets más utilizados.

```
Text(
  "Acción no permitida",
  style: TextStyle(fontWeight: FontWeight.w700, fontSize: 20),
), // Text
```

Figura 42. Text.

- **Card**

Contenedor con bordes redondeados y sombra ligera, ideal para mostrar información agrupada de forma elegante y destacada.

```
return Card(
  color: Colors.white,
  shape: RoundedRectangleBorder(
    borderRadius: BorderRadius.circular(15),
  ), // RoundedRectangleBorder
  elevation: 3,
  child: Padding(
    padding: const EdgeInsets.all(12),
    child: Column(
      crossAxisAlignment: CrossAxisAlignment.start,
      children: [
        Row(
          children: [
            const Icon(Icons.info_outline,
                size: 18, color: Colors.blueGrey),
            const SizedBox(width: 6),
            Expanded(
              child: Text(
                nombreCampo,
                style: const TextStyle(
                  fontSize: 12,
                  fontWeight: FontWeight.w600,
                  color: Colors.black54,
                ), // TextStyle
              ), // Text
            ), // Expanded
          ],
        ), // Row
        const SizedBox(height: 6),
        Text(
          valor.toString(),
          style: const TextStyle(
            fontSize: 14,
            fontWeight: FontWeight.bold,
          ), // TextStyle
          maxLines: 2,
          overflow: TextOverflow.ellipsis,
```

Figura 43. Card.

- **Image.asset**

Permite mostrar imágenes almacenadas localmente dentro de los assets de la aplicación.

```
children: [
  Image.asset('assets/images/logo1.png', width: 120),
  TextButton(
    onPressed: () => _goMenuDispositivos(context),
    child: const Text("Regresar",
        style: TextStyle(fontSize: 16, color: Colors.black)),
  ), // TextButton
],
```

Figura 44. Image.asset.

- **Divider**

Línea horizontal usada para separar secciones o elementos dentro de una lista o interfaz.

```
const Divider(),
```

Figura 45. Divider.

Navegación de la aplicación

- **Navigator.push**

Método que permite navegar hacia una nueva pantalla agregándola a la pila de navegación, con la posibilidad moverse entre diferentes vistas de la app.

```
Navigator.push(
  context,
  MaterialPageRoute(
    builder: (context) => SolicitudSalidaPage(dispositivo: dispositivo),
  ), // MaterialPageRoute
);
```

Figura 46. Navigator.push.

3.5.4 Diagrama de Endpoints (API REST)

El diagrama de endpoints (Figura 47) de la API REST representa la arquitectura de comunicación del sistema de control de activos, estructurada mediante el framework Node.js con Express. Esta representación visual muestra la distribución lógica de los servicios backend organizados en cuatro módulos funcionales principales: Gestión de Usuarios, Solicitudes de Salida, Aprobación y Denegación, Notificaciones Push FCM, y Gestión de Tokens. Cada módulo expone endpoints HTTP específicos (POST, GET) que facilitan operaciones como el registro y autenticación de usuarios, la solicitud y autorización de salida de equipos, el envío de notificaciones en tiempo real, y la administración de tokens de seguridad. Esto permite una comunicación eficiente entre la aplicación móvil desarrollada en Flutter y el servidor backend, garantizando la interoperabilidad, escalabilidad y mantenibilidad del sistema de control de activos tecnológicos.

3.5.5 Producción

Durante esta etapa, se llevó a cabo el desarrollo de la aplicación móvil a través de las iteraciones especificadas en la Tabla 29, en conformidad con lo establecido en las fases de Exploración e Inicialización del proceso metodológico MOBILE-D.

a. Backend

El backend fue desarrollado utilizando Node.js con el framework Express.js, y MongoDB como base de datos principal. Este backend actúo como intermediario entre la aplicación móvil desarrollada en Flutter y la base de datos, permitiendo realizar operaciones de autenticación, gestión de usuarios, control de dispositivos, generación de códigos QR, manejo de solicitudes de salida y envío de notificaciones push mediante Firebase Cloud Messaging (FCM).

Para optimizar la interacción y garantizar la integridad de los datos, se definieron esquemas y controladores específicos en la Tabla 30, encargados de administrar las principales entidades del sistema.

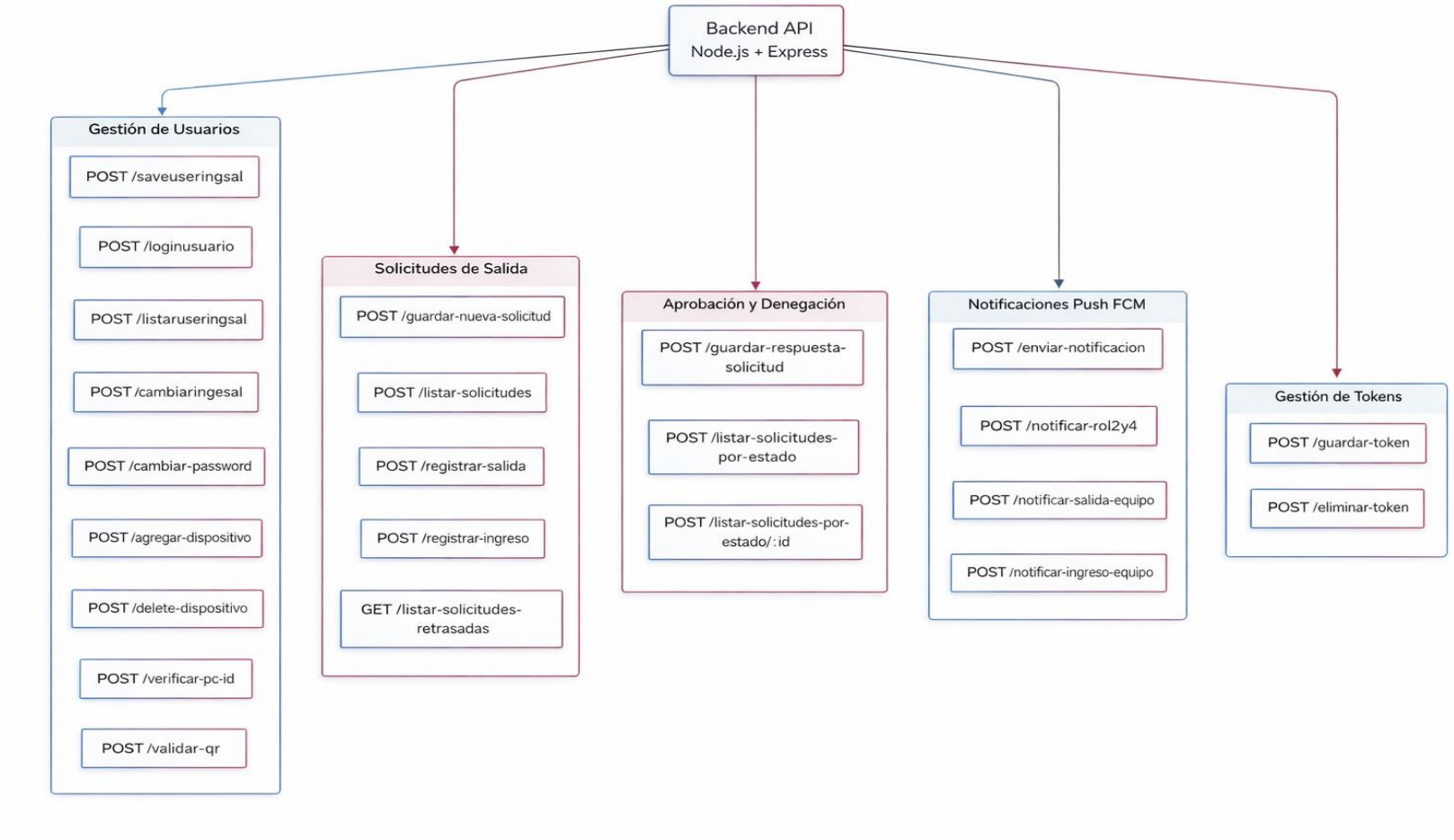


Figura 47. Diagrama de Endpoints.

Tabla 30. Esquemas y controladores.

Modelo	Descripción
userIngSal	Administra la información de los usuarios del sistema, incluyendo campos como ci, name, email, password, agencia, cargo, rol y el token utilizado para notificaciones push. Permite almacenar múltiples dispositivos asociados a un mismo usuario, cada uno con sus datos técnicos (modelo, pc_id, cpu, ram, id_activo), la fechaRegistro, el estado de visibilidad (visible) y la imagen del código QR generado (qr_image).
solicitud	Registra las solicitudes de salida e ingreso de dispositivos. Contiene información del funcionario (ci, name, cargo), datos del equipo (modelo, pc_id, cpu, ram, id_activo), motivo de la solicitud, fechas planificadas (fecha_salida y fecha_ingreso), descripción, fecha de creación (fecha_solicitud) y el estado de la solicitud (pendiente, aprobada, denegada o finalizada). Incluye además campos de control para el flujo operativo, como salidaRegistrada, ingresoRegistrado, fechaSalidaReal, fechaIngresoReal, notificadoSalida, notificadoIngreso y notificadoIngresoVencido.
respuestaSolicitud	Almacena las respuestas emitidas por el oficial de seguridad al aprobar o denegar una solicitud. Registra la referencia a la solicitud original (_idSolicitud), los datos del funcionario involucrado, la información del dispositivo, la descripción, la justificación ingresada (razon), el estado asignado (aprobada o denegada) y la fecha en que se generó la respuesta (fecha_AproDene). Este modelo permite mantener un historial completo y auditable de todas las decisiones tomadas.
FirebaseConfig	Maneja la configuración del servicio de notificaciones push mediante Firebase Admin SDK, permitiendo enviar alertas según los roles definidos (funcionario, oficial de seguridad, guardia).

- ***Dependencias Utilizadas***

Se emplearon diversas dependencias que permitieron establecer la conexión con la base de datos MongoDB y gestionar las funcionalidades del sistema. Entre estas dependencias se incluyeron librerías especializadas para la comunicación con la base de datos, herramientas de autenticación, gestión de notificaciones, envío de correos electrónicos y otros componentes esenciales para el backend:

- express@4.16.4.
- mongoose@5.11.4.
- firebase-admin@13.3.0.
- bcrypt@5.0.1.
- nodemailer@6.7.5.
- dotenv@10.0.0.

- cors@2.8.5.
- axios@1.3.5.
- moment@2.29.1 y moment-timezone@0.5.33.
- cookie-parser@1.4.6.
- morgan@1.10.0.
- ***Arquitectura Modelo-Vista-Controlador (MVC)***

La arquitectura del backend se estructuró siguiendo el patrón de diseño Modelo-Vista-Controlador (MVC) adaptado para APIs RESTful, lo que permitió una clara separación de responsabilidades y modularidad del código.

- En la carpeta **models/** se definieron los esquemas y modelos de datos mediante Mongoose 5.11.4, representando las entidades principales del sistema como usuarios, dispositivos, solicitudes, respuestas históricas y notificaciones.
- En la carpeta **controllers/** se implementaron los controladores encargados de gestionar las peticiones HTTP provenientes de la aplicación móvil Flutter, procesar la lógica de negocio, interactuar con los modelos correspondientes y retornar respuestas estructuradas en formato JSON.
- En la carpeta **routes/** se establecieron los endpoints HTTP que exponen la API hacia los clientes (Flutter y aplicaciones web), definiendo las rutas de acceso y asociándolas con los controladores correspondientes.

- ***Endpoints***

El backend implemento una estructura modular basada en rutas RESTful. Cada endpoint cumplió una función específica para gestionar los diferentes procesos del sistema (Tabla 31).

Tabla 31. Endpoints establecidos en el backend.

Módulo	Método	Endpoint	Descripción
Gestión de Usuarios	POST	/consultas-ingresosalida/saveuseriingsal	Crea un nuevo usuario con contraseña encriptada y rol asignado (1–4).
	POST	/consultas-ingresosalida/loginusuario	Autentica usuarios verificando credenciales cifradas en MongoDB y asigna token FCM.
	POST	/consultas-ingresosalida/listuseriingsal	Lista todos los usuarios visibles en el sistema.
	POST	/consultas-ingresosalida/deleteingresal	Realiza eliminación lógica del usuario y sus dispositivos, previa verificación de solicitudes activas.
	POST	/consultas-ingresosalida/cambiar-password	Permite cambiar la contraseña del usuario validando la actual y encriptando la nueva.
Gestión de Dispositivos	POST	/consultas-ingresosalida/agregar-dispositivo	Asigna un dispositivo a un usuario, evitando duplicados de `pc_id`.
	POST	/consultas-ingresosalida/delete-dispositivo	Realiza eliminación lógica del dispositivo solo si no tiene solicitudes activas.
	POST	/consultas-ingresosalida/verificar-pc-id	Verifica si un `pc_id` ya existe en la base de datos.
	POST	/consultas-ingresosalida/validar-qr	Valida el código QR escaneado para confirmar la pertenencia del equipo a un usuario activo.
Solicitudes de Salida	POST	/enviarsolicitud/guardar-nueva-solicitud	Registra una nueva solicitud de salida de dispositivo. Valida horario laboral y solicitudes previas.
	POST	/enviarsolicitud/listar-solicitudes	Lista todas las solicitudes pendientes de aprobación (estado 0).
	POST	/enviarsolicitud/registrar-salida	Registra la salida real del dispositivo aprobada, almacenando fecha y hora actuales.
	POST	/enviarsolicitud/registrar-ingreso	Registra el ingreso del equipo, cambiando el estado a 3 (finalizado).
	GET	/enviarsolicitud/listar-solicitudes-retrasadas	Devuelve las solicitudes cuyo ingreso no fue registrado en el tiempo establecido.
Aprobación y Denegación	POST	/autoDenega/guardar-respuesta-solicitud	Guarda la respuesta del oficial de seguridad (aprobado o denegado) con justificación.
	POST	/autoDenega/listar-solicitudes-por-estado	Lista solicitudes aprobadas o denegadas según el estado.
	POST	/autoDenega/listar-solicitudes-por-estado-ci	Filtra solicitudes aprobadas o denegadas por número de cédula.
Notificaciones Push (FCM)	POST	/notificaciones/enviar-notificacion	Envía notificación general a todos los usuarios con rol 3 (oficiales de seguridad).

Módulo	Método	Endpoint	Descripción
	POST	/notificaciones/notificar-rol2y4	Envía notificaciones de aprobación o denegación a funcionarios (rol 2) y guardias (rol 4).
	POST	/notificaciones/notificar-salida-equipo	Envía notificación cuando el dispositivo ha salido de la institución.
	POST	/notificaciones/notificar-ingreso-equipo	Envía notificación cuando el equipo ha sido ingresado.
	POST	/token-envio/guardar-token	Guarda el token FCM del usuario según su rol al iniciar sesión.
	POST	/token-envio/eliminar-token	Elimina el token FCM al cerrar sesión.

b. Storycards

Los Storycards son herramientas importantes en la gestión ágil de proyectos, diseñadas para representar, planificar y organizar las tareas o funcionalidades que deben desarrollarse durante el proceso. Cada Storycard actúa como un registro estructurado que permite descomponer las actividades en unidades más pequeñas y manejables, brindando una visión clara de los objetivos específicos a alcanzar. Además, los Storycards favorecen la priorización de tareas, la estimación del esfuerzo requerido y la evaluación del impacto que cada funcionalidad tiene en el desarrollo global del proyecto.

El formato propuesto en la Tabla 32 para los Storycards, fue diseñado con el propósito de estructurar de forma clara, ordenada y precisa la información esencial correspondiente a cada iteración, integrando los campos necesarios para su adecuada gestión y seguimiento.

Tabla 32. Diseño Storycards.

Nº	**Tipo**	**Dificultad**		**Esfuerzo/Horas**		**Importancia**
		Antes	**Después**	**Antes**	**Después**	
#	**Nuevo Corrección Mejora**	**Simple Regular Complicado**	**Simple Regular Complicado**	#	#	**Baja Intermedia Alta**
Descripción						
Fecha		**Estado**		**Comentario**		

Descripción de los campos:

- **Número:** Código identificador único que se asigna a cada Storycard.
- **Tipo:** Es el campo que clasifica la actividad indicando si se trata de una nueva funcionalidad, mejora o corrección.
- **Dificultad:** Medición que estima el grado de dificultad de la tarea, antes o después de su ejecución, valorado como simple, moderado o complejo.
- **Esfuerzo/Horas:** Incluye la estimación inicial de tiempo que se requería hasta esta última asignada y la total de horas de las realmente utilizadas.
- **Importancia:** Reflejo del impacto que tiene una tarea dentro del propio sistema, por ejemplo, bajo, medio o alto.
- **Descripción:** Muestra un resumen lo más claro y detallado de la tarea o funcionalidad a desarrollar.
- **Fecha:** Define los hitos temporales correspondientes a la tarea, fechas de comienzo y actualizaciones, así como de finalización.
- **Estado:** Establece cual es el estado de avance actual, siendo pendiente, en proceso o finalizado.
- **Comentario**: Espacio abierto para registrar información relevante relacionada con la tarea.

A continuación, se presentan las Storycards correspondientes a la planificación establecida en la Tabla 29, desarrolladas durante la Fase de Producción de la metodología MOBILE-D:

- ***Storycard 1***

Iteración 3: Implementación de la interfaz de inicio de sesión.

Tabla 33. Storycard Interfaz de Inicio de Sesión.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
1	Nuevo	Moderado	Moderado	4	6	Alta
Descripción: Creación, diseño y validación de la interfaz de inicio de sesión						
Fecha		Estado		Comentario		
23/09/2025		Definición		Sin comentarios		
24/09/2025		Implementación		Sin comentarios		
24/09/2025		Ejecución		Sin comentarios		
24/09/2025		Verificación		Sin comentarios		

La pantalla de inicio de sesión cuenta con campos para ingresar usuario y contraseña, además del botón "Ingresar". Las credenciales ingresadas se validan directamente en el backend y, si son correctas, el sistema redirige automáticamente al usuario al módulo correspondiente según su rol asignado. Adicionalmente, el sistema verifica si existe una sesión activa en otro dispositivo. En caso afirmativo, muestra una alerta que solicita cerrar primero la sesión existente antes de permitir el acceso desde el nuevo dispositivo. Esta funcionalidad garantiza el control efectivo de sesiones concurrentes y refuerza la seguridad del sistema.

- ***Storycard 2***

Iteración 4: Implementación de la pantalla principal Administrador

Tabla 34. Storycard panel rol Administrador.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
2	Nuevo	Moderado	Moderado	5	8	Alta
Descripción: Panel rol Administrador						
Fecha		Estado		Comentario		
25/09/2025		Definición		Sin comentarios		
25/09/2025		Implementación		Sin comentarios		
26/09/2025		Ejecución		Sin comentarios		
27/09/2025		Verificación		Sin comentarios		

En esta iteración se implementa el panel del rol Administrador, que funciona como centro de control para las funciones críticas del sistema. Este panel integra, de manera organizada y accesible, los módulos de gestión de usuarios, asignación de dispositivos y administración de códigos QR. Con ello se consolida la operatividad inicial del

sistema al establecer las herramientas fundamentales para el control y administración de usuarios y dispositivos dentro de la plataforma.

- ***Storycard 3***

Iteración 5: Implementación de la interfaz de gestión de usuarios

Tabla 35. Storycard gestión de usuarios.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
3	Nuevo	Moderado	Moderado	6	9	Alta
Descripción: Gestión de usuarios						
Fecha		Estado		Comentario		
28/09/2025		Definición		Sin comentarios		
29/09/2025		Implementación		Sin comentarios		
30/09/2025		Ejecución		Sin comentarios		
01/10/2025		Verificación		Sin comentarios		

La pantalla de Gestión de Usuarios centraliza todas las acciones relacionadas con la administración del personal en el sistema. Desde esta interfaz es posible registrar nuevos usuarios mediante un formulario validado, visualizar el listado completo de funcionarios a través de un buscador dinámico y ejecutar eliminaciones lógicas de registros cuando sea necesario. Su diseño unificado permite realizar todas las operaciones esenciales de forma rápida y ordenada dentro de una misma vista.

- ***Storycard 4***

Iteración 6: Implementación de la interfaz asignar dispositivo a un usuario

Tabla 36. Storycard asignación de dispositivos a usuario.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
4	Nuevo	Moderado	Moderado	5	8	Alta
Descripción: Asignación de dispositivos a usuario						
Fecha		Estado		Comentario		
02/10/2025		Definición		Sin comentarios		
03/10/2025		Implementación		Sin comentarios		
05/10/2025		Ejecución		Sin comentarios		
06/10/2025		Verificación		Sin comentarios		

En esta iteración se desarrolla el módulo de asignación de dispositivos, que permite registrar los datos técnicos de cada equipo: modelo, PC_ID, CPU, RAM, ID_ACTIVO y fecha de registro. Una vez completado el formulario, el sistema genera

automáticamente el código QR correspondiente, el cual contiene tanto la información técnica del dispositivo como los datos del funcionario asignado.

Posteriormente, se despliega una segunda interfaz que muestra el código QR generado, acompañado de tarjetas resumen con los datos del usuario, la agencia, el cargo y la información técnica completa del equipo. Esta pantalla incluye las opciones para continuar, eliminar el dispositivo mediante eliminación lógica y exportar el código QR para su impresión. Finalmente, el código QR se almacena de forma automática en la base de datos, garantizando su disponibilidad para procesos posteriores como verificación, escaneo y generación de reportes.

- ***Storycard 5***

Iteración 7: Implementación de la interfaz rol funcionario

Tabla 37. Storycard dispositivos asignados y envío de solicitud.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
5	Nuevo	Moderado	Moderado	4	7	Alta
Descripción: Dispositivos asignados y envío de solicitud						
Fecha		Estado		Comentario		
07/10/2025		Definición		Sin comentarios		
09/10/2025		Implementación		Sin comentarios		
13/10/2025		Ejecución		Sin comentarios		
14/10/2025		Verificación		Sin comentarios		

En esta iteración se incorpora la pantalla Dispositivos Asignados, que permite al funcionario visualizar todos los equipos asociados a su cuenta mediante un menú desplegable. Cada selección despliega la información completa del dispositivo: modelo, agencia, cargo, PC_ID, CPU, RAM, ID_ACTIVO y fecha de registro.

Asimismo, se implementa el módulo de Solicitud de Salida, donde el usuario selecciona uno de sus dispositivos asignados, especifica el motivo, las fechas de salida e ingreso, y agrega una descripción. Al confirmar el envío, el sistema registra la solicitud en el backend y genera automáticamente una notificación push mediante FCM dirigida al Oficial de Seguridad, quien recibe un resumen de la petición para su posterior aprobación o rechazo.

- ***Storycard 6***

Iteración 8: Implementación de la interfaz rol oficial de seguridad

Tabla 38. Storycard estado de las solicitudes, envío de notificación y reporte de estado de dispositivos.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
6	Nuevo	Moderado	Moderado	5	8	Alta
Descripción: Estado de las solicitudes, envío de notificación y reporte de estado de dispositivos						
Fecha		Estado		Comentario		
15/10/2025		Definición		Sin comentarios		
16/10/2025		Implementación		Sin comentarios		
20/10/2025		Ejecución		Sin comentarios		
22/10/2025		Verificación		Sin comentarios		

En esta iteración se implementa el módulo del rol Oficial de Seguridad, que incorpora un menú con las opciones Dispositivos, Reporte de Dispositivos y Cambiar Contraseña. Dentro de este módulo se desarrolla la gestión de solicitudes, permitiendo visualizar listados separados según su estado: Pendientes, Aprobadas y Denegadas, cada uno con los datos fundamentales del funcionario y del dispositivo.

La pantalla Detalle de Solicitud muestra la información de la cédula, nombre, cargo, modelo del equipo, PC_ID, motivo, fechas y descripción y habilita las acciones de Autorizar o Denegar, incluyendo un campo para registrar la justificación de la decisión.

Al emitir una respuesta, el sistema envía automáticamente notificaciones push al funcionario y al Guardia, informando el resultado de la autorización. Finalmente, se incorpora una vista de reportes por estado, que facilita el seguimiento de las solicitudes procesadas en el sistema.

- ***Storycard 7***

Iteración 9: Implementación de la interfaz rol guardia de seguridad

Tabla 39. Storycard verificar salida o ingreso del equipo por escaneo de QR.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
7	Nuevo	Moderado	Moderado	5	9	Alta
Descripción: Verificar salida o ingreso del equipo por escaneo de QR						

Fecha	Estado	Comentario
23/10/2025	Definición	Sin comentarios
25/10/2025	Implementación	Sin comentarios
29/10/2025	Ejecución	Sin comentarios
01/11/2025	Verificación	Sin comentarios

En esta iteración se desarrolla por completo el rol Guardia de Seguridad, incorporando un menú dedicado con las opciones Dispositivos Aprobados y Verificar Salida/Entrada. Se implementa el escáner de código QR, que permite validar la autenticidad del permiso y visualizar la información completa del funcionario y del dispositivo asociado. A partir de esta verificación, el sistema habilita las acciones de Registrar Salida o Registrar Ingreso según el estado actual del equipo.

Una vez registrada la acción, se actualiza la base de datos y se envía automáticamente una notificación push al funcionario, confirmando si la salida o el ingreso ha sido registrado correctamente. Asimismo, se implementan listados visuales para el guardia que distinguen claramente los dispositivos según su estado: Fuera o Ingresados, cada uno con sus marcas de tiempo para asegurar la trazabilidad.

- ***Storycard 8***

Iteración 10: Implementación de la interfaz de reportes

Tabla 40. Storycard visualización de reportes según rol.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
8	Nuevo	Moderado	Moderado	4	7	Alta
Descripción: Visualización de reportes según rol						
Fecha		Estado		Comentario		
02/11/2025		Definición		Sin comentarios		
05/11/2025		Implementación		Sin comentarios		
07/11/2025		Ejecución		Sin comentarios		
08/11/2025		Verificación		Sin comentarios		

En esta iteración se implementa el módulo de Reportes, accesible tanto para el Oficial de Seguridad como para el Guardia. Este módulo permite consultar información consolidada sobre dispositivos y solicitudes mediante filtros por rango de fechas y estado: Pendiente, Aprobado, Denegado, Fuera e Ingresado. Además, se integran mecanismos de actualización automática los cambios generados al registrar una salida o ingreso.

- ***Storycard 9***

Iteración 11: Implementación de la interfaz cambio de contraseña

Tabla 41. Storycard cambio de contraseña para todos los roles.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
9	Nuevo	Moderado	Moderado	5	9	Alta
Descripción: Cambio de contraseña para todos los roles						
Fecha		Estado		Comentario		
09/11/2025		Definición		Sin comentarios		
11/11/2025		Implementación		Sin comentarios		
14/11/2025		Ejecución		Sin comentarios		
16/11/2025		Verificación		Sin comentarios		

En esta iteración se implementa el módulo de Cambio de Contraseña para todos los roles del sistema, permitiendo que cada usuario actualice sus credenciales de forma segura. La pantalla incluye un formulario con validaciones que verifican requisitos como longitud mínima, uso de caracteres especiales y coincidencia entre la nueva contraseña y su confirmación. Una vez confirmado el cambio, la solicitud se envía al backend, donde la nueva contraseña se encripta mediante bcrypt antes de almacenarse en la base de datos.

- ***Storycard 10***

Iteración 12: Implementación de Firebase Cloud Messaging (FCM)

Tabla 42. Storycard integración del sistema de notificaciones push.

Nº	Tipo	Dificultad		Esfuerzo/Horas		Importancia
		Antes	Después	Antes	Después	
10	Nuevo	Moderado	Moderado	4	7	Alta
Descripción: Integración del sistema de notificaciones push						
Fecha		Estado		Comentario		
17/11/2025		Definición		Sin comentarios		
19/11/2025		Implementación		Sin comentarios		
21/11/2025		Ejecución		Sin comentarios		
23/11/2025		Verificación		Sin comentarios		

En esta iteración se completó la integración del sistema de notificaciones push utilizando Firebase Cloud Messaging (FCM), garantizando que cada usuario cuente con un token único para la recepción de notificaciones. Además, se validó la comunicación entre los tres roles operativos del sistema, asegurando que las notificaciones se envíen correctamente en los eventos clave: creación de solicitudes

(dirigidas al Oficial de Seguridad), aprobación o denegación de solicitudes (dirigidas al Funcionario), y registros de salida e ingreso realizados por el Guardia de Seguridad (dirigidos al Funcionario).

3.5.6 Estabilización

En esta fase se ejecutaron ajustes finales sobre el sistema con el propósito de garantizar su funcionamiento óptimo, estabilidad operativa y conformidad con los requerimientos funcionales y no funcionales establecidos durante las etapas previas del desarrollo (Ver Tabla 34). Las modificaciones implementadas se centraron en optimizar la usabilidad de la interfaz de usuario, mejorar la experiencia de interacción y perfeccionar la comunicación con la base de datos MongoDB, asegurando la integridad y consistencia de los datos.

Tabla 43. Modificaciones en el desarrollo de la aplicación.

Modificación	Descripción
Interfaz de Usuario	▪ Se optimizó el diseño de la pantalla de inicio de sesión para garantizar una experiencia más intuitiva y segura, validando el rol del usuario (administrador, funcionario, oficial o guardia) y redirigiéndolo automáticamente a su respectivo panel. ▪ Se implementó una interfaz moderna y adaptable a diferentes dispositivos móviles, con iconografía clara y botones de acceso rápido. ▪ Se añadió un módulo de registro de usuarios con formularios validados y un sistema de notificación por correo electrónico que comunica la creación de nuevas credenciales.
Base de Datos	▪ Se estructuró una base de datos no relacional para gestionar usuarios, dispositivos, solicitudes y movimientos de activos institucionales. ▪ Se integraron tablas relacionadas con los roles, permisos y estados de los dispositivos, garantizando la trazabilidad completa de las operaciones. ▪ Se incorporó el almacenamiento seguro de contraseñas mediante cifrado y la sincronización automática de datos en tiempo real, asegurando la integridad de la información ante posibles desconexiones.
Notificaciones y Reportes	▪ Se implementó un sistema de notificaciones push que alerta a los usuarios involucrados sobre el estado de las solicitudes, aprobaciones y registros de salida o ingreso. ▪ Las notificaciones se diseñaron para operar en tiempo real y adaptarse tanto a Android como a iOS, optimizando la conectividad del sistema.
Código y Seguridad	▪ Se realizaron ajustes en la arquitectura del código para mejorar su rendimiento y legibilidad, aplicando principios de refactorización. ▪ Se implementaron validaciones adicionales para el control de errores y la protección de datos sensibles. ▪ Se garantizó la autenticación segura de los usuarios mediante el cifrado de credenciales y la restricción de accesos según los roles definidos.

3.5.7 Pruebas

En la siguiente fase se ejecutaron las pruebas correspondientes con el objetivo de verificar el correcto funcionamiento de la aplicación y validar el cumplimiento de los requerimientos funcionales y no funcionales establecidos por los interesados del proyecto. Como resultado de esta etapa de validación, se obtuvo la versión final y estable de la aplicación móvil, lista para su implementación en el entorno productivo.

a. Pruebas de funcionalidad

Las pruebas de funcionalidad se ejecutaron bajo la supervisión y validación del responsable del área administrativa de la Cooperativa de Ahorro y Crédito Credi Ya Ltda. Estas pruebas tuvieron como propósito verificar que la aplicación cumpliera con las funcionalidades especificadas en los requerimientos del sistema y que respondiera adecuadamente a las interacciones del usuario. Se evaluaron exhaustivamente los distintos módulos implementados al fin de garantizar que el sistema operara de manera correcta, estable y alineada con las necesidades operativas y de seguridad de la institución financiera.

- **Pantalla de Inicio de Sesión**

Tabla 44. Prueba de funcionalidad 1.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
El usuario accede a la aplicación móvil	**1.** Ingresa nombre de usuario y contraseña **2.** El sistema valida que no existan caracteres especiales en el campo usuario **3.** Se validan las credenciales contra la base de datos **4.** Si son correctas, se genera token de autenticación **5.** Los datos de sesión se almacenan en SharedPreferences. **6.** El sistema redirige a la pantalla	10-15 segundos	- Ingreso de credenciales incorrectas - Uso de caracteres especiales en usuario - Campos vacíos	• Funcionario • Oficial de Seguridad • Administrador • Guardia de Seguridad

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
	principal según el rol asignado			



Figura 48. Pantalla de Inicio de Sesión.

- **Pantalla de Registro de Usuarios**

Tabla 45. Prueba de funcionalidad 2.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
El administrador accede al módulo de registro	1. Ingresa datos obligatorios: Cédula, Usuario, Correo Electrónico, Contraseña, Agencia, Área y Rol 2. El sistema valida formatos y campos obligatorios 3. Verifica que la cédula no esté duplicada en MongoDB 4. Al presionar "Guardar", envía	20-40 segundos	• Campos vacíos • Formato inválido de correo electrónico • Cédula duplicada	Administrador

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
	solicitud HTTP POST al backend 5. Los datos se almacenan en la colección de usuarios de MongoDB 6. La interfaz se actualiza automáticamente mostrando el nuevo usuario			



Figura 49. Pantalla de Registro de Usuarios.

- **Pantalla de Lista de Usuarios**

Tabla 46. Prueba de funcionalidad 3.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
El administrador accede a la lista de usuarios	**1.** El sistema despliega todos los usuarios registrados **2.** Permite filtrar por tipo de rol (Funcionario, Oficial, Administrador, Guardia) **3.** Permite búsqueda por nombre de usuario **4.** Cada acción (editar/eliminar) se ejecuta de forma independiente **5.** La eliminación se realiza mediante soft delete (campo "visible" cambia de 1 a 0) **6.** Se preserva la integridad de datos históricos	5-10 segundos por operación	-	Administrador



Figura 50. Pantalla de Lista de Usuarios.

- **Pantalla de Asignación de Dispositivos**

Tabla 47. Prueba de funcionalidad 4.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
El administrador accede al módulo de asignación	**1.** Selecciona un usuario del sistema **2.** Ingresa datos obligatorios: Modelo, Pc_id, Cpu, Ram, Id_Activo **3.** El sistema valida formatos y restricciones establecidas **4.** Al presionar "Guardar", envía solicitud HTTP POST al backend **5.** Se vincula el dispositivo con el usuario en la colección de usuarios de MongoDB **6.** La asignación queda registrada y activa	20-40 segundos	• Campos obligatorios vacíos • Formatos incorrectos en campos técnicos	Administrador



Figura 51. Pantalla de Asignación de Dispositivos.

- **Pantalla de Generación de Código QR**

Tabla 48. Prueba de funcionalidad 5.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
Tras asignar un dispositivo, el sistema genera automáticamente el código QR	**1.** El sistema genera código QR con: usuario, agencia, cargo, modelo, CPU, RAM, ID Activo, fecha de registro **2.** Los datos coinciden exactamente con MongoDB **3.** Botón "Continuar" regresa al menú principal **4.** Botón "Eliminar" ejecuta soft delete del dispositivo **5.** Botón "Imprimir" permite la impresión del QR	3-10 segundos	-	Administrador



Figura 52. Pantalla de Generación de Código QR.

- **Pantalla de Envío de Solicitud de Salida**

Tabla 49. Prueba de funcionalidad 6.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
El funcionario accede al formulario de solicitud	**1.** Selecciona el dispositivo asignado **2.** Ingresa: Motivo, Fecha de Salida, Fecha de Ingreso, Descripción **3.** El sistema valida campos obligatorios y lógica de fechas **4.** Verifica que el dispositivo no tenga solicitud activa pendiente **5.** Al presionar "Enviar Solicitud", envía HTTP POST al backend **6.** Se almacena en MongoDB con estado "Pendiente" **7.** Se envía notificación push vía FCM al oficial de seguridad **8.** Mensaje de confirmación al usuario **9.** La solicitud aparece en listas de pendientes	25-40 segundos	• Campos vacíos • Fecha de ingreso anterior a fecha de salida • Dispositivo con solicitud activa pendiente	Funcionario



Figura 53. Pantalla de Envío de Solicitud de Salida.

- **Notificación al Oficial de Seguridad**

Tabla 50. Prueba de funcionalidad 7.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
Se envía automáticamente tras registrar solicitud	1. Firebase Cloud Messaging envía notificación push 2. Contiene: nombre del funcionario, cargo, agencia, modelo del dispositivo, motivo 3. Notificación se recibe en tiempo real 4. Al interactuar con ella, redirige a pantalla de autenticación biométrica 5. Se valida Face ID o Touch ID 6. Tras validación exitosa, accede a detalles de la solicitud	Inmediato (1-5 segundos)	Fallo en autenticación biométrica	Oficial de Seguridad

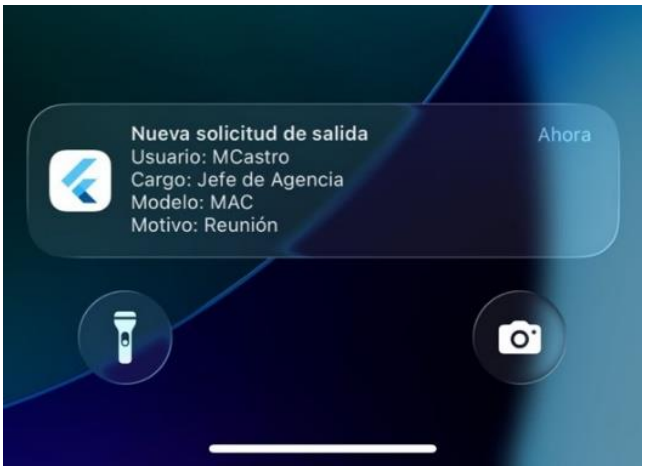


Figura 54. Notificación al Oficial de Seguridad.

- **Pantalla de Revisión de Solicitudes**

Tabla 51. Prueba de funcionalidad 8.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
El oficial accede a la solicitud pendiente	**1.** Visualiza detalles completos: fecha de solicitud, cédula, nombre, cargo, modelo, pc_id, motivo, fechas programadas, descripción **2.** Ingresa observaciones en campo "Razón" **3.** Presiona "Autorizar" o "Denegar" **4.** Si autoriza: estado cambia a 1 (aprobada) vía HTTP al backend **5.** Si deniega: estado cambia a 2 (rechazada) **6.** La razón se almacena en colección de respuestas históricas en MongoDB **7.** Se envía notificación automática al funcionario	15-30 segundos	-	Oficial de Seguridad

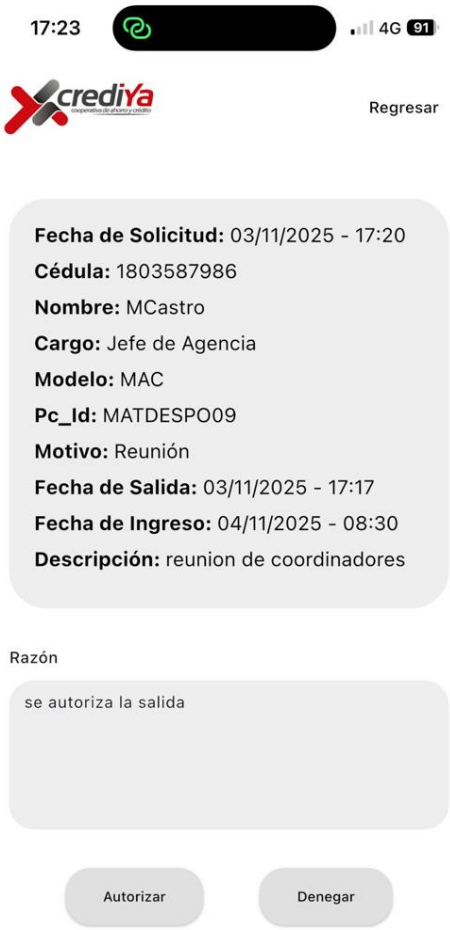


Figura 55. Pantalla de Revisión de Solicitudes.

- **Notificación al funcionario**

Tabla 52. Prueba de funcionalidad 9.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
Se genera automáticamente tras decisión del oficial	1. Firebase Cloud Messaging envía notificación push 2. Informa decisión tomada (aprobada/denegada) 3. Incluye mensaje descriptivo visible en pantalla de bloqueo/banner 4. Al interactuar, redirige a pantalla de detalle de solicitud	Inmediato (1-5 segundos)	-	Funcionario

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
	5. Refleja estado actualizado y observaciones del oficial			

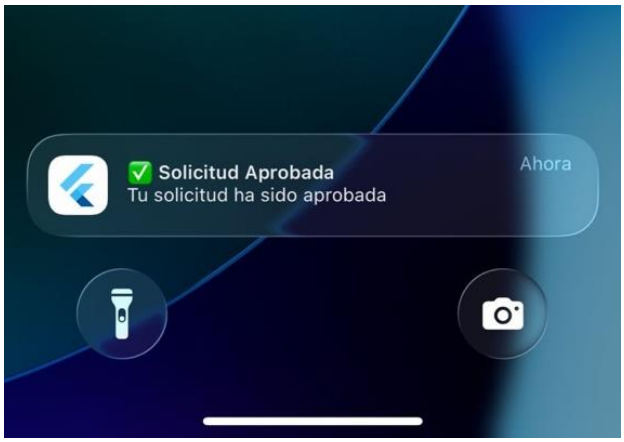


Figura 56. Notificación al Funcionario.

- **Pantalla de Verificación de Salida**

Tabla 53. Prueba de funcionalidad 10.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
El guardia escanea código QR del dispositivo	1. Escanea código QR 2. El sistema muestra: cédula, nombre, cargo, agencia, modelo, PC_ID, CPU, RAM, ID_ACTIVO, fecha de registro, estado del permiso 3. Verifica que el estado sea "Aprobado" 4. Verifica que la fecha actual coincida con fecha de salida programada 5. Si cumple las condiciones, el	15-45 segundos	• Permiso no aprobado • Fecha actual no coincide con fecha programada	• Guardia de Seguridad • Funcionario (recibe notificación)

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
	botón "Salida" se habilita **6.** Al presionar, registra fecha y hora exactas de salida en MongoDB **7.** Actualiza estado a "Fuera de la institución" **8.** Envía notificación push al funcionario			

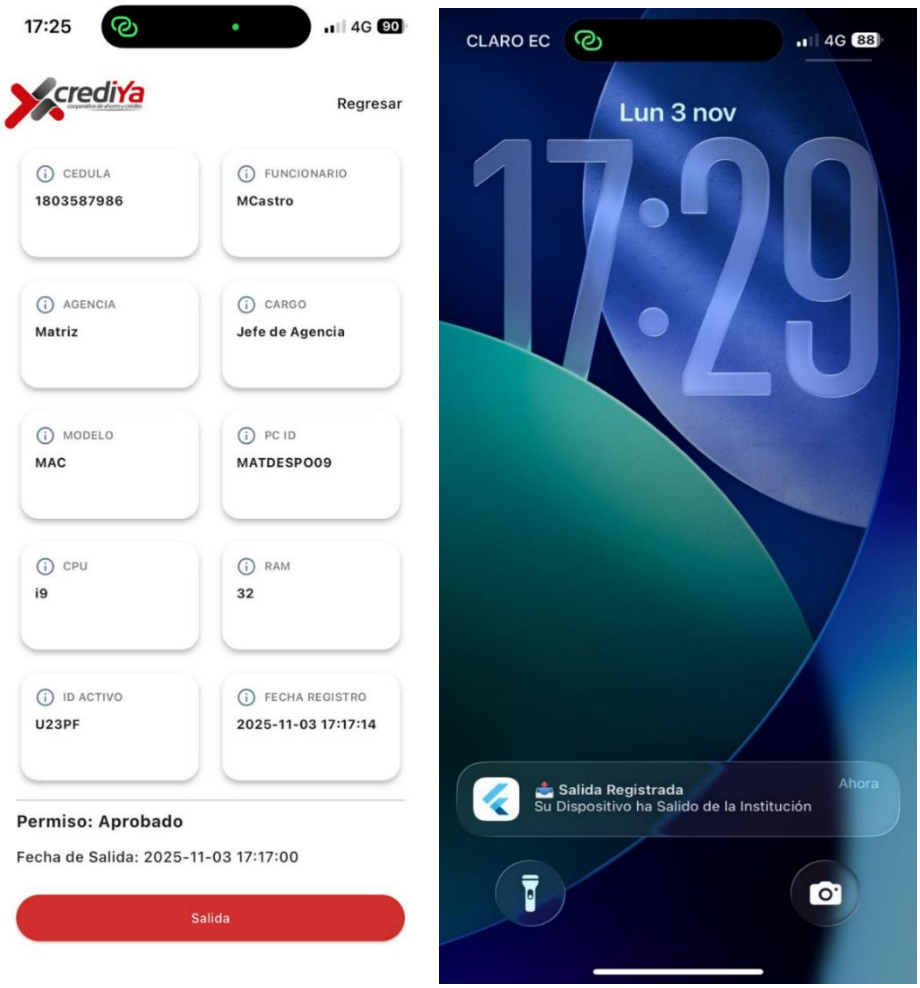


Figura 57. Pantalla de verificación de salida y notificación push de aprobación de salida.

- **Pantalla de Registro de Ingreso**

Tabla 54. Prueba de funcionalidad 11.

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
El guardia escanea código QR cuando el dispositivo retorna	1. Escanea código QR del dispositivo 2. Sistema muestra datos técnicos del dispositivo y funcionario 3. Muestra fecha y hora de salida previamente registrada 4. Verifica que el estado sea "Fuera de la institución" 5. Si cumple, botón "Ingreso" se habilita 6. Al presionar, registra fecha y hora de ingreso en MongoDB 7. Actualiza campo ingresoRegistrado 8. Cambia estado a "Completada" 9. Envía notificación push al funcionario y oficial de seguridad	15-45 segundos	Dispositivo no está en estado "Fuera de la institución"	• Guardia de Seguridad • Funcionario (recibe notificación) • Oficial de Seguridad (recibe notificación)

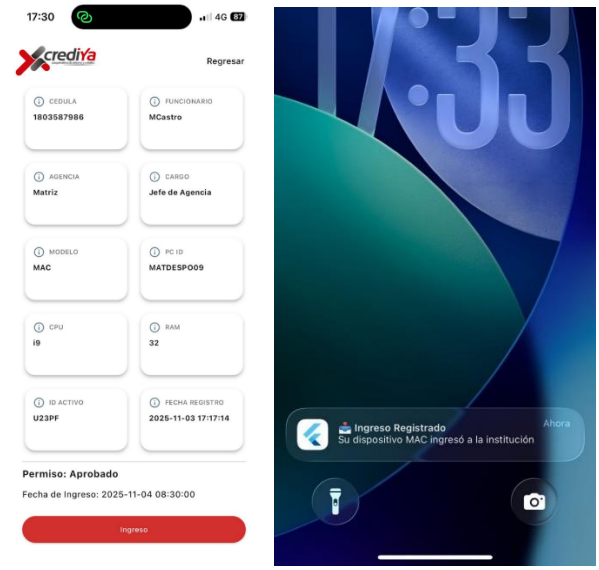


Figura 58. Pantalla de registro de ingreso y notificación push de aprobación.

- **Pantalla de Control de Dispositivos**

Inicio	Acciones Realizadas	Tiempo Estimado	Errores Cometidos	Usuarios Involucrados
El guardia accede al panel de control	1. Visualiza estado centralizado de todos los dispositivos 2. Diferencia entre "Fuera de la institución" e "Ingresados" 3. Los cambios se reflejan automáticamente en tiempo real 4. Ícono de flecha indica dispositivos en salida 5. Check verde indica dispositivos reingresados 6. Actualización automática tras cada escaneo	Consulta instantánea (1-3 segundos)	-	Guardia de Seguridad



Figura 59. Pantalla de Control de Dispositivos.

b. Pruebas de aceptación

A continuación, se presentan las pruebas de aceptación ejecutadas con el objetivo de validar el cumplimiento de los requisitos funcionales establecidos para cada módulo y pantalla del sistema, siguiendo el formato estandarizado definido en la Tabla 35. Cada prueba se realizó bajo condiciones controladas, reproduciendo los escenarios de uso y verificando que los resultados obtenidos coincidan con el comportamiento esperado del sistema, garantizando así la conformidad con los criterios de aceptación establecidos por los interesados del proyecto.

Tabla 55. Formato para pruebas de aceptación.

Prueba de Aceptación	**Número: #**
Nº de StoryCard: #	
Nombre:	
Descripción de la actividad:	
Condiciones de ejecución e interfaz:	
Resultado Esperado:	
Resultado de la Prueba:	

Tabla 56. Prueba de aceptación Storycard 1.

Prueba de Aceptación	**Número: 1**
Nº de StoryCard: 1	
Nombre: Validación y funcionamiento de la interfaz de inicio de sesión	
Descripción de la actividad: Se verifica que la pantalla de inicio de sesión valide correctamente las credenciales ingresadas, permitiendo el acceso únicamente a usuarios autorizados. Se comprueba que el sistema muestre mensajes de error apropiados ante credenciales incorrectas o campos vacíos. Adicionalmente, se valida que el campo de usuario rechace caracteres especiales y que las credenciales se contrasten adecuadamente con el backend para redirigir al usuario al módulo correspondiente según su rol asignado.	
Condiciones de ejecución e interfaz: Se ejecuta en un entorno controlado utilizando usuarios previamente registrados en el sistema. Se ingresan diversas combinaciones de credenciales, tanto válidas como inválidas, para evaluar el comportamiento del formulario y la gestión de errores. También se verifica la restricción de sesiones concurrentes, comprobando que el sistema detecte y notifique cuando existe una sesión activa en otro dispositivo.	
Resultado Esperado: El sistema debe permitir el acceso únicamente cuando las credenciales sean correctas y pertenezcan a un usuario registrado. Se espera que el formulario: • Gestione adecuadamente los mensajes de error ante campos vacíos o credenciales incorrectas • Rechace caracteres especiales en el campo de nombre de usuario • Muestre una alerta cuando se detecte una sesión activa en otro dispositivo • Redirija exitosamente al usuario al módulo correspondiente según su rol una vez autenticado	
Resultado de la Prueba: Satisfactorio	

Tabla 57. Prueba de aceptación Storycard 2.

Prueba de Aceptación	**Número: 2**
Nº de StoryCard: 2	
Nombre: Validación del panel principal del rol Administrador	
Descripción de la actividad: Se verifica que el panel principal del Administrador cargue correctamente todos los módulos esenciales del sistema, incluyendo: gestión de usuarios, asignación de dispositivos y administración de códigos QR. Se comprueba que los accesos funcionen sin errores, que la navegación sea coherente con los permisos del rol y que no se muestren funcionalidades no autorizadas. Adicionalmente, se valida que todos los botones y enlaces redirijan correctamente a las pantallas correspondientes.	
Condiciones de ejecución e interfaz: Se ejecuta en un entorno controlado utilizando un usuario con rol de Administrador previamente registrado en el sistema. Tras iniciar sesión, se accede al panel principal y se interactúa sistemáticamente con cada uno de los módulos disponibles (Usuarios, Dispositivos, QR). Se evalúa el comportamiento de la interfaz, la visibilidad de los elementos, la funcionalidad de los controles y la fluidez de la navegación entre módulos.	
Resultado Esperado: El sistema debe presentar el panel principal del Administrador con todos los módulos correspondientes visibles, activos y completamente funcionales. Se espera que: • Cada módulo se abra correctamente sin errores de navegación ni fallos visuales • No se muestren módulos o funcionalidades ajenas al rol de Administrador • Los botones y enlaces redirijan adecuadamente a sus respectivas pantallas • Se mantenga la continuidad del flujo de trabajo administrativo sin interrupciones	
Resultado de la Prueba: Satisfactorio	

Tabla 58. Prueba de aceptación Storycard 3 – 4.

Prueba de Aceptación	**Número: 3**
Nº de StoryCard: 3 - 4	
Nombre: Validación del módulo de Gestión de Usuarios y Asignación de Dispositivos	
Descripción de la actividad: Se evalúa que la interfaz facilite el registro de nuevos usuarios mediante un formulario con validaciones integradas, visualice el listado de funcionarios a través de un buscador con filtrado dinámico y ejecute la baja lógica de registros. Asimismo, se comprueba que el proceso de asignación de equipos capture correctamente la información técnica (modelo, PC_ID, CPU, RAM, ID_ACTIVO y fecha de registro) y que, al completar el formulario, el sistema genere de forma automática el código QR vinculado, presentando en pantalla la información consolidada tanto del funcionario como del equipo asignado. Se verifica que no se acepten campos sin completar, formatos no válidos o caracteres inapropiados en ninguno de los formularios.	
Condiciones de ejecución e interfaz: Se desarrolla incorporando usuarios y equipos en el sistema. Se introducen combinaciones correctas e incorrectas en los formularios de alta de usuario y asignación de equipo para analizar la gestión de validaciones y errores. Se constata que el buscador filtre información de manera instantánea, que las operaciones de eliminación de usuario o equipo ejecuten una baja lógica, y que la pantalla de visualización del QR despliegue las tarjetas resumen junto con las opciones para continuar, imprimir o eliminar el registro.	
Resultado Esperado: El sistema debe habilitar el registro de usuarios y la asignación de equipos exclusivamente cuando los formularios se encuentren completos y debidamente validados. Se espera que: • Presente mensajes de error claros ante campos incompletos, información no válida o formatos inadecuados • Actualice el listado de usuarios de forma inmediata y aplique filtros según el criterio especificado • El módulo de equipos genere el código QR con la información precisa del funcionario y del dispositivo asignado • Almacene automáticamente el QR en la base de datos y active las acciones disponibles para el usuario • Todas las operaciones se ejecuten sin fallos técnicos y manteniendo la coherencia e integridad de los datos	
Resultado de la Prueba: Satisfactorio	

Tabla 59. Prueba de aceptación Storycard 5.

Prueba de Aceptación	**Número: 4**
Nº de StoryCard: 5	
Nombre: Validación del módulo de Dispositivos Asignados y Solicitud de Salida	
Descripción de la actividad: Se evalúa la capacidad del funcionario para tramitar la salida de equipos asignados a su cargo. Desde el módulo de Dispositivos, el usuario selecciona un equipo y completa el formulario de Solicitud de Salida con la información requerida. Adicionalmente, desde la sección Solicitudes Enviadas, puede consultar el estado de sus peticiones (pendiente, aprobada o rechazada). Se verifican las restricciones del sistema que impiden registrar solicitudes duplicadas cuando existe una activa, aprobada en curso o con salida ya registrada para el mismo equipo. También se validan los límites de horario establecidos (hasta las 17:30 horas) y la disponibilidad exclusiva en días hábiles.	
Condiciones de ejecución e interfaz: Se ejecuta desde el panel correspondiente al rol de funcionario. Se accede al menú de Dispositivos para seleccionar un equipo y completar una solicitud incluyendo motivo, rango de fechas y descripción del traslado. Posteriormente, se navega por la sección Solicitudes Enviadas para verificar que los listados reflejen correctamente la información según cada estado.	
Resultado Esperado: El sistema debe permitir el registro de la Solicitud de Salida únicamente cuando no exista otra solicitud activa o en curso vinculada al mismo dispositivo. Se espera que: • El formulario habilite el envío solo si todos los campos están completos, se encuentra dentro del horario permitido y corresponde a un día hábil • La solicitud se registre correctamente en la base de datos • El estado de la solicitud se refleje de inmediato en la sección Solicitudes Enviadas • El sistema bloqueé solicitudes duplicadas o fuera de las condiciones establecidas, mostrando mensajes informativos apropiados • La navegación entre estados y el acceso a la información histórica funcione de manera fluida y precisa	
Resultado de la Prueba: Satisfactorio	

Tabla 60. Prueba de aceptación Storycard 6.

Prueba de Aceptación	**Número: 5**
Nº de StoryCard: 6	
Nombre: Validación del módulo del Oficial de Seguridad	
Descripción de la actividad: Se verifica el funcionamiento del módulo correspondiente al Oficial de Seguridad, el cual permite visualizar y gestionar solicitudes clasificadas en estados: Pendientes, Aprobadas y Denegadas. Se evalúa la capacidad de consultar la información detallada de cada solicitud y ejecutar las acciones de Autorizar o Denegar, requiriendo una justificación obligatoria.	
Condiciones de ejecución e interfaz: Se ejecuta desde la interfaz del rol Oficial de Seguridad, accediendo al módulo de Dispositivos donde se visualizan las solicitudes organizadas por estado. Se seleccionan registros individuales para acceder a la vista de Detalle, verificando que se despliegue correctamente la información completa del funcionario solicitante y del equipo involucrado. Se prueban las opciones de Autorizar y Denegar, validando que el sistema solicite y registre la justificación correspondiente en cada caso.	
Resultado Esperado: El Oficial de Seguridad debe poder visualizar de manera clara y organizada todas las solicitudes agrupadas según su estado actual. Se espera que: • El acceso al detalle de cada solicitud presente la información completa y actualizada del funcionario y del dispositivo • Las acciones de Autorizar o Denegar se ejecuten correctamente, requiriendo una justificación obligatoria antes de confirmar la operación • La decisión tomada se registre inmediatamente en el sistema, actualizando el estado de la solicitud • Los cambios se reflejen de forma instantánea en los listados correspondientes • El sistema mantenga un registro auditable de cada acción realizada, incluyendo la justificación proporcionada	
Resultado de la Prueba: Satisfactorio	

Tabla 61. Prueba de aceptación Storycard 7.

Prueba de Aceptación	**Número: 6**
Nº de StoryCard: 7	
Nombre: Validación del módulo del Guardia de Seguridad	
Descripción de la actividad: La prueba valida el correcto funcionamiento del módulo correspondiente al Guardia de Seguridad, verificando el proceso de escaneo del código QR para autenticar y validar permisos de tránsito. Se comprueba que el sistema despliegue la totalidad de la información asociada al funcionario y al equipo, y que permita registrar adecuadamente la salida o el ingreso únicamente cuando la solicitud correspondiente haya sido previamente aprobada por el Oficial de Seguridad.	
Condiciones de ejecución e interfaz: Se ejecuta desde la interfaz del rol Guardia, accediendo a la opción "Verificar Salida/Entrada". Se procede a escanear códigos QR reales generados previamente por el sistema, validando que se despliegue la información completa del funcionario y del dispositivo. Se verifica que las acciones disponibles se habiliten exclusivamente según el estado actual del equipo (disponible para salida o pendiente de ingreso). Se registran operaciones de salida e ingreso, confirmando la correcta actualización en la base de datos y la captura automática de las marcas temporales (timestamp) correspondientes a cada evento.	
Resultado Esperado: El sistema debe permitir la visualización completa y precisa de la información al escanear un código QR válido. Se espera que: • La lectura del QR despliegue de forma inmediata los datos del funcionario y del equipo asociado • Las opciones de registrar salida o ingreso se habiliten únicamente cuando exista una solicitud con estado aprobado • El registro de cada evento (salida/ingreso) se almacene correctamente en la base de datos con su marca temporal exacta • El sistema actualice automáticamente el estado del dispositivo tras cada operación • Se bloqueen acciones no autorizadas mostrando mensajes claros cuando la solicitud no esté aprobada o el QR sea inválido • La interfaz permanezca estable y responsiva durante todo el proceso de verificación y registro	
Resultado de la Prueba: Satisfactorio	

Tabla 62. Prueba de aceptación Storycard 8.

Prueba de Aceptación	**Número: 7**
Nº de StoryCard: 8	
Nombre: Validación del módulo de reportes según el rol	
Descripción de la actividad: Validar el funcionamiento de la interfaz de Reportes, accesible tanto para el Oficial de Seguridad como para el Guardia. Esta pantalla permite consultar información consolidada sobre solicitudes y dispositivos mediante la aplicación de filtros por estado (Pendiente, Aprobado, Denegado, Fuera e Ingresado). Se evalúa la capacidad del sistema para presentar datos organizados y actualizados que faciliten la supervisión y el seguimiento de las operaciones de control de equipos.	
Condiciones de ejecución e interfaz: Se ejecuta accediendo al módulo de Reportes desde ambos roles (Oficial de Seguridad y Guardia). Se aplican diferentes combinaciones de filtros por estado, verificando que el sistema recupere y presente correctamente los dispositivos y solicitudes que correspondan a cada criterio seleccionado. Se valida la funcionalidad de búsqueda, la actualización dinámica de los listados y la consistencia de la información mostrada respecto a los registros almacenados en la base de datos.	
Resultado Esperado: El sistema debe generar reportes precisos, actualizados y correctamente organizados según el filtro aplicado. Se espera que: • Los listados reflejen únicamente los registros que cumplan con el estado seleccionado • Cada solicitud y dispositivo muestre información completa y coherente con su estado actual • Los cambios generados por operaciones de salida o ingreso se reflejen de manera inmediata en los reportes	

• La interfaz permita una navegación fluida entre diferentes filtros sin pérdida de datos ni errores de visualización • El sistema garantice la trazabilidad completa de cada equipo, mostrando el historial de estados cuando corresponda • No existan inconsistencias entre la información presentada y los datos almacenados en la base de datos • Ambos roles accedan a la información pertinente según sus permisos, manteniendo la integridad y seguridad de los datos
Resultado de la Prueba: Satisfactorio

Tabla 63. Prueba de aceptación Storycard 9.

Prueba de Aceptación	**Número: 8**
Nº de StoryCard: 9	
Nombre: Validación del módulo cambio de contraseña	
Descripción de la actividad: La prueba verifica el correcto funcionamiento del módulo de Cambio de Contraseña implementado para todos los roles del sistema. Se valida la funcionalidad de los campos de nueva contraseña y su confirmación, comprobando el cumplimiento de requisitos de seguridad tales como longitud mínima, inclusión de caracteres especiales, combinación de mayúsculas, minúsculas y números, así como la coincidencia exacta entre ambas entradas. Asimismo, se evalúa que, al confirmar la operación, la contraseña sea transmitida de forma segura al backend para su encriptación mediante el algoritmo bcrypt y posterior almacenamiento protegido en la base de datos.	
Condiciones de ejecución e interfaz: Se ejecuta desde la pantalla de Cambio de Contraseña, accesible para cualquier usuario autenticado independientemente de su rol. Se introducen diversas combinaciones de contraseñas, tanto válidas como inválidas, para evaluar el comportamiento de las validaciones en tiempo real. Se verifica que los mensajes de error y advertencia se desplieguen de manera dinámica conforme el usuario completa los campos, que el botón de confirmación permanezca deshabilitado mientras no se cumplan todos los requisitos establecidos, y que la solicitud se envíe correctamente al backend una vez validada toda la información.	
Resultado Esperado: El sistema debe permitir la actualización de la contraseña exclusivamente cuando esta cumpla con la totalidad de los criterios de seguridad establecidos, mostrando validaciones claras, precisas y en tiempo real. Se espera que: • Las validaciones se ejecuten de forma dinámica mientras el usuario ingresa la información • Los mensajes de error sean específicos y orienten al usuario sobre los requisitos faltantes • El botón de confirmación se habilite únicamente cuando ambos campos sean válidos y coincidan • La contraseña sea transmitida de manera segura al backend y encriptada correctamente mediante bcrypt antes de su almacenamiento • La nueva contraseña se guarde de forma protegida en la base de datos, reemplazando la anterior • El usuario reciba una alerta clara y visible confirmando el cambio exitoso de su contraseña • El sistema permita la autenticación posterior utilizando las nuevas credenciales sin inconvenientes • No se produzcan vulnerabilidades de seguridad durante todo el proceso de actualización	
Resultado de la Prueba: Satisfactorio	

Tabla 64. Prueba de aceptación Storycard 10.

Prueba de Aceptación	**Número: 9**
Nº de StoryCard: 10	
Nombre: Validación del Firebase Cloud Messaging	
Descripción de la actividad: Se implementa y valida el sistema de notificaciones push mediante Firebase Cloud Messaging (FCM), asignando un token único e individual por cada usuario registrado en el sistema. Se habilitó la comunicación bidireccional entre los roles de Funcionario, Oficial de Seguridad y Guardia, estableciendo flujos de notificación automatizados para mantener informados a los usuarios sobre el estado de sus operaciones. Se verifica el envío correcto y oportuno de notificaciones durante los eventos clave del sistema: creación de solicitud de salida, aprobación de solicitud, denegación de solicitud y registro de salida o ingreso de dispositivos.	
Condiciones de ejecución e interfaz: Se realiza desde las interfaces correspondientes a los tres roles operativos del sistema, utilizando cuentas de usuarios con tokens FCM activos previamente registrados y almacenados en la base de datos. Se ejecuta operaciones reales que desencadenan notificaciones: envío de solicitudes por parte del Funcionario, autorización o denegación por parte del Oficial de Seguridad, y registro de salida o ingreso por parte del Guardia. Se comprueba la recepción inmediata y correcta de las notificaciones en los dispositivos correspondientes, tanto en primer plano como en segundo plano. Adicionalmente, se valida el funcionamiento del sistema de navegación profunda (deep linking), verificando que, al interactuar con una notificación, la aplicación se abra y dirija automáticamente al usuario hacia la pantalla específica relacionada con el evento notificado.	
Resultado Esperado: El sistema debe enviar notificaciones push de manera instantánea en cada uno de los eventos clave definidos, asociándolas correctamente al usuario destinatario mediante su token único registrado. Se espera que: • Las notificaciones se entreguen sin demoras significativas tanto cuando la aplicación está activa como cerrada • Cada notificación contenga información clara y relevante sobre el evento que la originó • Al interactuar con una notificación, la aplicación navegue automáticamente hacia la pantalla correspondiente según el tipo de evento (detalle de solicitud, lista de pendientes, registro de salida/ingreso) • La comunicación entre los diferentes roles se mantenga estable, consistente y sin pérdida de mensajes • Los tokens se actualicen correctamente cuando sea necesario, garantizando la continuidad del servicio de notificaciones • El sistema gestione adecuadamente casos excepcionales como tokens inválidos o dispositivos sin conexión • La experiencia del usuario sea fluida, informativa y contribuya a la eficiencia operativa del sistema	
Resultado de la Prueba: Satisfactorio	

c. Pruebas de rendimiento

A continuación, se presentan las pruebas de rendimiento ejecutadas con el objetivo de validar el cumplimiento de los requisitos funcionales establecidos para cada módulo y pantalla del sistema. Cada prueba se realizó bajo condiciones controladas, reproduciendo los escenarios de uso reales y verificando que los tiempos de respuesta, las acciones ejecutadas y los resultados obtenidos coincidieran con el comportamiento esperado del sistema, garantizando así la conformidad con los criterios de aceptación establecidos por los interesados del proyecto. Las métricas utilizadas son las siguientes:

- **Proceso:** Nombre de la funcionalidad o flujo evaluado en el sistema.
- **Tiempo Promedio**: Tiempo medio calculado de todas las ejecuciones.
- **Tiempo P95 (percentil 95):** Tiempo que el 95% de las ejecuciones no supera. Este valor indica el tiempo máximo que tarda el proceso en el 95% de los casos, excluyendo los casos atípicos o más lentos (el 5% restante).
- **Tasa de éxito:** Porcentaje de ejecuciones exitosas del proceso sobre el total de intentos realizados, expresado en formato decimal.
- **Estado:** Indica si cumplió con los criterios de aceptación establecidos.
- **Observaciones:** Notas adicionales relevantes sobre el comportamiento del proceso durante las pruebas.

Tabla 65. Tabla de rendimiento.

Proceso	Tiempo Promedio	Tiempo P95	Tasa de Éxito	Estado	Observaciones
Inicio de Sesión	7.2 s	10 s	100%	Exitoso	Credenciales validadas y sesión guardada correctamente en SharedPreferences.
Registro de Usuarios	22.4 s	29.1 s	98%	Exitoso	Validaciones correctas y registro en MongoDB sin fallas relevantes.
Gestión de Lista de Usuarios	9.3 s por operación	10 s	100%	Exitoso	Búsqueda, filtrado y soft delete operaron independientemente.
Asignación de Dispositivos	31.6 s	39.4 s	97%	Exitoso	Asignación del dispositivo al usuario almacenada correctamente.
Generación de Código QR	5.1 s	8.3 s	100%	Exitoso	QR generado con datos exactos consultados en la base de datos.
Envío de Solicitud de Salida	24.8 s	39 s	96%	Exitoso	Validaciones, registro en BD y notificación push completadas correctamente.
Notificación al Oficial de Seguridad	2.3 s	3.8 s	100%	Exitoso	Notificación recibida casi en tiempo real vía FCM.
Revisión de Solicitudes	16 s	22 s	98%	Exitoso	Aprobación o rechazo guardados correctamente en el historial.
Notificación al Funcionario	2.6 s	4.1 s	100%	Exitoso	Notificación con estado actualizado entregada inmediatamente.
Verificación de Salida	31.2 s	44.5 s	99%	Exitoso	Validación, registro de timestamp y notificación ejecutados sin errores.

Proceso	Tiempo Promedio	Tiempo P95	Tasa de Éxito	Estado	Observaciones
Registro de Ingreso	29.7 s	43.2 s	99%	Exitoso	Actualización del estado y notificaciones múltiples funcionando correctamente.
Control de Dispositivos	2.1 s	3.0 s	100%	Exitoso	Actualización instantánea reflejada en pantalla y base de datos.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se determinó que el proceso de control de ingreso y salida de estaciones de trabajo en la Cooperativa de Ahorro y Crédito Credi Ya Ltda. presentaba deficiencias críticas de seguridad y gestión. El diagnóstico reveló que el 100% de los encuestados confirmó la inexistencia de un registro formal, lo que derivaba en una falta total de trazabilidad.

- La investigación y aplicación de la tecnología Flutter demostró ser efectiva para el desarrollo de la solución móvil multiplataforma. La elección de la versión 3.27 permitió aprovechar el motor de renderizado Impeller, garantizando un rendimiento nativo óptimo desde una única base de código. Además, priorizó la estabilidad operativa frente a versiones posteriores de transición, permitiendo que, mediante el lenguaje Dart se implementaran eficientemente interfaces diferenciadas por roles y funcionalidades críticas como el escaneo de códigos QR y las notificaciones push, optimizando así los recursos y tiempos de desarrollo.

- El diseño integral de la solución se fundamentó en el modelado de prototipos mediante Balsamiq Wireframes, lo cual permitió validar la arquitectura visual y la usabilidad de los flujos operativos antes de la codificación. Esta fase preliminar facilitó una implementación precisa en el framework Flutter, resultando en una aplicación móvil con interfaz moderna, intuitiva y funcional que automatizó el control de activos, alcanzando una tasa de éxito promedio del 99% en la ejecución de procesos durante las pruebas de rendimiento. Las pruebas de funcionalidad y aceptación confirmaron que el sistema mitiga los riesgos detectados inicialmente, reduciendo los tiempos de registro y autorización mediante el uso de escaneo QR y flujos de aprobación digitales, respondiendo eficazmente a la necesidad de seguridad manifestada por el 71% del personal operativo.

4.2 Recomendaciones

- Extender la aplicación de la metodología Mobile-D a otros proyectos de desarrollo móvil dentro de la organización, aprovechando las lecciones aprendidas y las buenas prácticas identificadas durante la implementación del sistema de control de activos. El enfoque iterativo y ágil de Mobile-D ha demostrado ser efectivo para validar funcionalidades en contextos reales y mantener ciclos constantes de retroalimentación con los usuarios finales, lo cual puede replicarse en futuras soluciones tecnológicas que requieran respuestas rápidas a necesidades operativas cambiantes. Esta expansión metodológica mejoraría la capacidad institucional para desarrollar aplicaciones móviles robustas y alineadas con los requerimientos del personal, consolidando un marco de trabajo estandarizado que facilite la gestión de proyectos tecnológicos de manera eficiente.

- Establecer un cronograma periódico de mantenimiento que incluya la actualización de librerías y dependencias del framework Flutter y el backend Node.js para mitigar vulnerabilidades emergentes. Asimismo, realizar controles de seguridad regulares sobre los registros de la base de datos y los tokens de acceso, fortaleciendo los protocolos de protección de datos personales conforme a la normativa legal vigente.

- Evaluar la expansión del sistema para abarcar no solo las estaciones de trabajo informáticas, sino otros activos fijos de la institución (mobiliario, vehículos, documentación sensible). La estructura flexible de la base de datos NoSQL implementada permite la adición de nuevas categorías de activos sin alterar significativamente la arquitectura existente, lo que potenciaría el retorno de inversión del desarrollo realizado.

REFERENCIAS BIBLIOGRÁFICAS

[1] O. Laurido Santos, «Transformación Digital En Las Cooperativas De Ahorro Y Crédito,» Osvaldo Laurido & Company, 2022.

[2] Superintendencia de Economía Popular y Solidaria, «Informe de Rendición de Cuentas 2023,» Quito, 2023.

[3] D. F. Villacís Sánchez , Artist, *Aplicación móvil usando Flutter para el seguimiento y control de formulaciones en órdenes de producción para la empresa Curtiduría Tungurahua S.A. [Tesis de Grado].* [Art]. Universidad Técnica de Ambato, 2025.

[4] Ecuador, Precidencia de la República del, «Reglamento de la Ley Orgánica de Protección de Datos Personales,» Lexis, Quito, Ecuador, 2023.

[5] C. M. Argila Lorente, Artist, *Transformación digital en la restauración : de los códigos QR con plataforma de pago, a la gestión de comandas en tiempo real [Tesis de Grado].* [Art]. Comillas Universidad Pontificia, 2024.

[6] R. Chutas Ramos, Artist, *Aplicación móvil realizado con Flutter para el control de inventario usando la metodología Mobile-D en la empresa Baenz Constructora & Servicios Generales S.A.C., Lima 2022 [Tesis de Grado].* [Art]. Universidad César Vallejo, 2022.

[7] E. F. Toledo Orozco, D. P. Cisneros Quintanilla y G. M. Ramon Poma, «Innovación Tecnológica y Eficiencia Operativa en la Cooperativa de Ahorro y Crédito Señor de Girón, 2025,» *Religación,* vol. 10, nº 45, 2025.

[8] A. S. Aldás Montesdeoca, Artist, *Aplicación móvil de geolocalización para gestión y control de vendedores de la empresa "Skandinar S.A" [Tesis de Grado].* [Art]. Universidad Técnica de Ambato, 2021.

[9] StrongDM, «Access Productivity Report | StrongDM,» 2024. [En línea]. Available: https://www.strongdm.com/report/access-productivity.

[10] W. R. Avendaño Castro, C. . A. Hernández Suarez y A. A. Gamboa Suárez, «Tecnologías de la información y crecimiento empresarial,» *Revista Boletín Redipe,* vol. 11, nº 1, 2022.

[11] J. R. Molina Ríos, J. A. Honores Tapia, N. Pedreira Souto y H. P. Pardo León, «Estado del arte: metodologías de desarrollo de aplicaciones móviles,» *3C Tecnología. Glosas de innovación aplicadas a la pyme,* vol. 10, nº 2, 2021.

[12] L. R. Quisaguano Collaguazo, M. S. Pallasco Venegas, A. A. Andaluz Guerrero, M. N. Martínez Freire y S. H. Corrales Beltrán, «Desarrollo Hibrido con Flutter,» *Ciencia Latina Revista Científica Multidisciplinar,* vol. 6, nº 4, 2022.

[13] Great Learning Editorial Team, «A guide to MVC Architecture in 2025,» 06 Enero 2025. [En línea]. Available: https://www.mygreatlearning.com/blog/a-guide-to-mvc-architecture/. [Último acceso: 03 Noviembre 2025].

[14] J. L. Acosta Espinoza, A. R. León Yacelga y W. G. Sanafria Michilena, «Las aplicaciones móviles y su impacto en la sociedad,» *Revista Universidad y Sociedad,* vol. 14, nº 2, 2022.

[15] X. Zhein y L. Zhein, «Accounting Information Systems and Strategic Performance: The Interplay of Digital Technology and Edge Computing Devices,» *Journal Grid Computing,* vol. 22, nº 5, 2024.

[16] Y. Pino era y A. d. L. Torralbas Blazquez, «Resiliencia en la gestión empresarial. Una revisión teórica,» *Revista Transdiciplinaria De Estudios Sociales Y Tecnológicos,* vol. 4, nº 1, 2024.

[17] R. M. Torres Briones, M. E. García Bravo, . K. d. R. Hurtado García y R. A. Reyes Armas, «Rentabilidad del sector comercial del Ecuador un análisis del efecto financiero de la gestión empresarial,» *Revista Religación,* vol. 9, nº 39, 2024.

[18] Firebase, «Agrega la autenticación de varios factores a una app para Flutter,» [En línea]. Available: https://firebase.google.com/docs/auth/flutter/multi-factor?hl=es-419. [Último acceso: 25 Septiembre 2025].

[19] Flutter Docs, «Build and release an Android app,» [En línea]. Available: https://docs.flutter.dev/deployment/. [Último acceso: 25 Septiembre 2025].

[20] General Data Protection Regulation (GDPR), «General Data Protection Regulation (GDPR) – legal text,,» 22 Abril 2024. [En línea]. Available: https://gdpr-info.eu/.

[21] OWASP Foundation, «Secure Cloud Architecture - OWASP Cheat Sheet Series.,» 2024. [En línea]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Secure_Cloud_Architecture_Cheat_Sheet.html. [Último acceso: 25 Septiembre 2025].

[22] M. Trojanowski, «API Security Best Practices,» 03 Diciembre 2024. [En línea]. Available: https://curity.io/resources/learn/api-security-best-practices/. [Último acceso: 25 Septiembre 2025].

[23] Google Codelabs, «Tu primera app de Flutter,» Google Codelabs, [En línea]. Available: https://codelabs.developers.google.com/codelabs/flutter-codelab-first?hl=es-419. [Último acceso: 16 Octubre 2025].

[24] D. Yerygin, «¿Por qué usar Flutter en 2025? Ventajas y desventajas del desarrollo de aplicaciones con Flutter,» Redwerk, 18 Septiembre 2025. [En línea]. Available: https://redwerk.es/blog/ventajas-y-desventajas-del-desarrollo-de-aplicaciones-con-flutter/. [Último acceso: 29 Octubre 2025].

[25] ABAMobile, «¿Por qué el desarrollo de aplicaciones corporativas con Flutter?,» ABAMobile, 17 Febrero 2021. [En línea]. Available: https://abamobile.com/web/desarrollo-aplicaciones-flutter-caracteristicas-ventajas/. [Último acceso: 29 Octubre 2025].

[26] R. Vilanou, «Flutter: ventajas y desventajas del desarrollo en 2025,» Doonamis, 23 Noviembre 2023. [En línea]. Available: https://www.doonamis.com/descubre-ventajas-desventajas-flutter/. [Último acceso: 29 Octubre 2025].

[27] M. Pulido, «Pros y contras de Flutter.,» SlashMobility, 11 Junio 2019. [En línea]. Available: https://slashmobility.com/blog/2019/06/pros-y-contras-de-flutter/. [Último acceso: 29 Octubre 2025].

[28] Fuioaga y Developer, «Apps exitosas con Flutter,» Blog Abalit Technologies, 9 Enero 2023. [En línea]. Available: http://abalit.org/blog/post/casos-de-exito-flutter/es. [Último acceso: 30 Octubre 2025].

[29] O. Manek, «10 top apps made with Flutter redefining tech in 2024,» Developernation.net, 24 Julio 2024. [En línea]. Available: http://developernation.net/blog/10-top-apps-made-with-flutter-redefining-tech-in-2024/. [Último acceso: 30 Octubre 2025].

[30] M. Pastorini, «The best Apps built with Flutter,» Somniosoftware.com, 27 Octubre 2022. [En línea]. Available: https://somniosoftware.com/blog/the-best-apps-built-with-flutter. [Último acceso: 30 Octubre 2025].

[31] M. Nowak, «Companies using Flutter to build their products in 2024,» Nomtek.com, 2 Enero 2024. [En línea]. Available: https://www.nomtek.com/blog/flutter-app-examples. [Último acceso: 30 Octubre 2025].

[32] Flutter release notes, «Flutter release notes,» Flutter.dev, [En línea]. Available: https://docs.flutter.dev/release/release-notes. [Último acceso: 30 Octubre 2025].

[33] Very Good Ventures, «10 reasons to choose Flutter for your mobile app,» Verygood.Ventures, 04 Febrero 2025. [En línea]. Available: https://verygood.ventures/blog/10-reasons-why-to-choose-flutter-for-your-mobile-app. [Último acceso: 16 Octubre 2025].

[34] Flutter, «layout,» Flutter, 2025. [En línea]. Available: https://docs.flutter.dev/ui/layout/tutorial. [Último acceso: 23 Noviembre 2025].

ANEXOS

Anexo A. ISO 9001:2015

La adopción de un sistema de gestión de la calidad es una decisión estratégica para una organización que le puede ayudar a mejorar su desempeño global y proporcionar una base sólida para las iniciativas de desarrollo sostenible. Los beneficios potenciales para una organización de implementar un sistema de gestión de la calidad basado en esta Norma Internacional son:

La capacidad para proporcionar regularmente productos y servicios que satisfagan los requisitos del cliente y los legales y reglamentarios aplicables.

Facilitar oportunidades de aumentar la satisfacción del cliente.

Abordar los riesgos y oportunidades asociadas con su contexto y objetivos.

La capacidad de demostrar la conformidad con requisitos del sistema de gestión de la calidad especificados.

Esta Norma Internacional emplea el enfoque a procesos, que incorpora el ciclo Planificar-Hacer-Verificar-Actuar (PHVA) y el pensamiento basado en riesgos. El enfoque a procesos permite a una organización planificar sus procesos y sus interacciones.

Anexo B. ISO/IEC 27001:2022

La adopción de un sistema de gestión de la seguridad de la información es una decisión estratégica para una organización que le puede ayudar a proteger y preservar la información mediante la aplicación de un proceso de gestión de riesgos, y proporciona confianza a las partes interesadas de que los riesgos se gestionan de manera adecuada. Los beneficios potenciales para una organización de implementar un sistema de gestión de la seguridad de la información basado en esta Norma Internacional son:

Demostrar conformidad con los requisitos legales, estatutarios, regulatorios y contractuales.

Proporcionar confianza a las partes interesadas en el enfoque de la organización para la gestión de la seguridad de la información.

Mejorar la gestión de riesgos de seguridad de la información dentro del contexto del negocio global de la organización.

Permitir a la organización preservar la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos.

Esta Norma Internacional emplea un enfoque basado en procesos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información.

Anexo C. Ley de Protección de Datos

La implementación de la Ley Orgánica de Protección de Datos Personales representa una decisión estratégica fundamental para las instituciones del sistema financiero ecuatoriano, estableciendo un marco jurídico robusto para la protección de datos personales de clientes y usuarios. Los beneficios y obligaciones principales para las entidades financieras de implementar las disposiciones de esta normativa son:

Garantizar el derecho fundamental de protección de datos personales consagrado en el artículo 66 numeral 19 de la Constitución de la República.

Establecer mecanismos de consentimiento expreso y específico para el tratamiento de datos financieros sensibles.

Implementar medidas técnicas y organizativas apropiadas que aseguren la confidencialidad, integridad y disponibilidad de los datos personales.

Designar un delegado de Protección de Datos (DPO) cuando el tratamiento de datos constituya una actividad principal de la entidad.

Realizar Evaluaciones de Impacto de Protección de Datos (DPIA) para tratamientos de alto riesgo.

Mantener un registro detallado de actividades de tratamiento de datos personales.

Notificar violaciones de seguridad a la autoridad competente y a los titulares afectados dentro de los plazos establecidos.

Esta Ley emplea principios de licitud, finalidad, minimización, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva, aplicando el enfoque de privacidad desde el diseño y por defecto.

Anexo D. Manual de Usuario

APLICACIÓN MÓVIL UTILIZANDO FLUTTER PARA EL CONTROL DE INGRESO Y SALIDA DE ESTACIONES DE TRABAJO EN LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.

MANUAL DE USUARIO

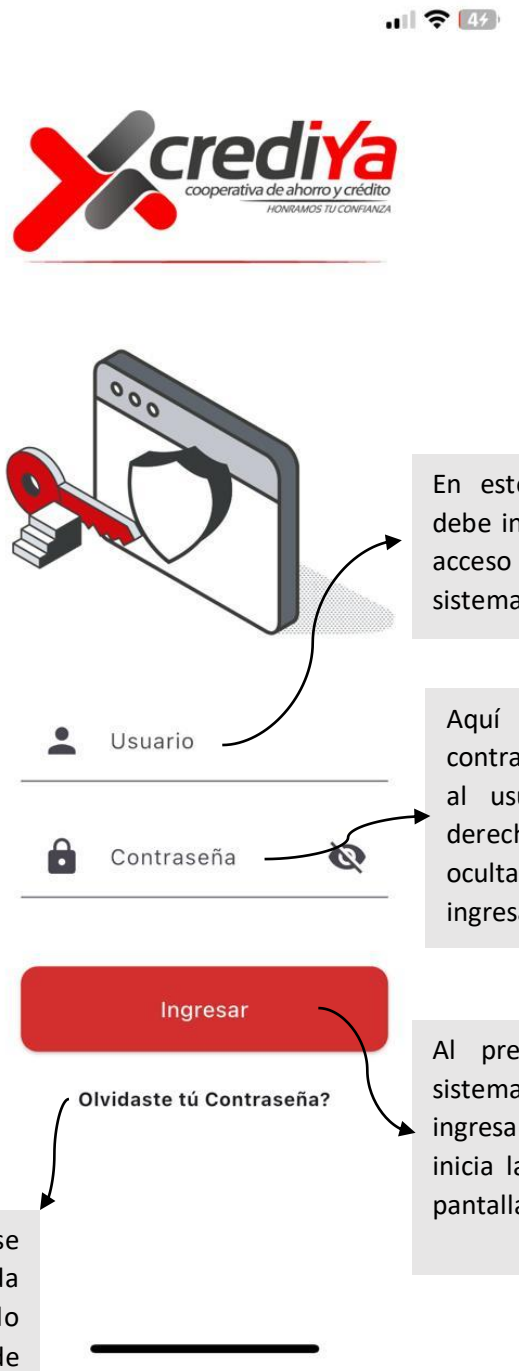
El objetivo de este manual es proporcionar una guía completa que permita a los usuarios utilizar eficazmente la aplicación de Control de Ingreso y Salida de equipos desarrollada para la Cooperativa Credi Ya. Este documento está diseñado para atender las necesidades específicas de los diferentes roles dentro del sistema (administradores, funcionarios, oficiales de seguridad y guardias), asegurando que cada usuario pueda desempeñar sus funciones de manera correcta y eficiente. A través de este manual, los usuarios aprenderán a navegar por la interfaz de la aplicación, registrar y consultar dispositivos, generar y gestionar solicitudes de salida, aprobar o denegar movimientos de equipos, verificar salidas y retornos mediante códigos QR, visualizar reportes del estado de los dispositivos y administrar sus credenciales de acceso. El contenido ha sido estructurado para facilitar una interacción intuitiva con la plataforma, garantizando que cada rol pueda acceder de manera clara y sencilla a las herramientas y funcionalidades que le competen, contribuyendo así al control seguro y ordenado de los equipos institucionales.

Inicio de Sesión

La pantalla de Inicio de Sesión permite al usuario acceder de forma segura al sistema ingresando sus credenciales.

Desde esta interfaz se ingresa el nombre de usuario y la contraseña, se valida la información y se inicia la sesión en la aplicación.

Además, ofrece la opción de recuperar la contraseña en caso de olvido.



En este campo el usuario debe ingresar su nombre de acceso registrado en el sistema.

Aquí se debe digitar la contraseña correspondiente al usuario. El ícono a la derecha permite visualizar u ocultar los caracteres ingresados.

Al presionar este botón, el sistema verifica las credenciales ingresadas. Si son correctas, se inicia la sesión y se muestra la pantalla principal.

Esta opción debe seleccionarse cuando el usuario no recuerda su contraseña. El sistema lo guiará al proceso de recuperación.

Panel del Administrador

El Panel del Administrador es la pantalla principal para los usuarios con rol administrativo.

Desde esta interfaz se accede a la gestión de usuarios, dispositivos, códigos QR y al módulo para cambiar la contraseña.

Además, se muestra un saludo personalizado y la opción para cerrar sesión de forma segura.



Permite finalizar la sesión activa y regresar a la pantalla de inicio de sesión.

Al seleccionar esta opción, se muestra la lista completa de usuarios registrados en el sistema, independientemente de su rol, junto con la información de los dispositivos asignados.



Esta opción permite visualizar a todos los funcionarios junto con sus equipos asignados y el código QR correspondiente a cada dispositivo.

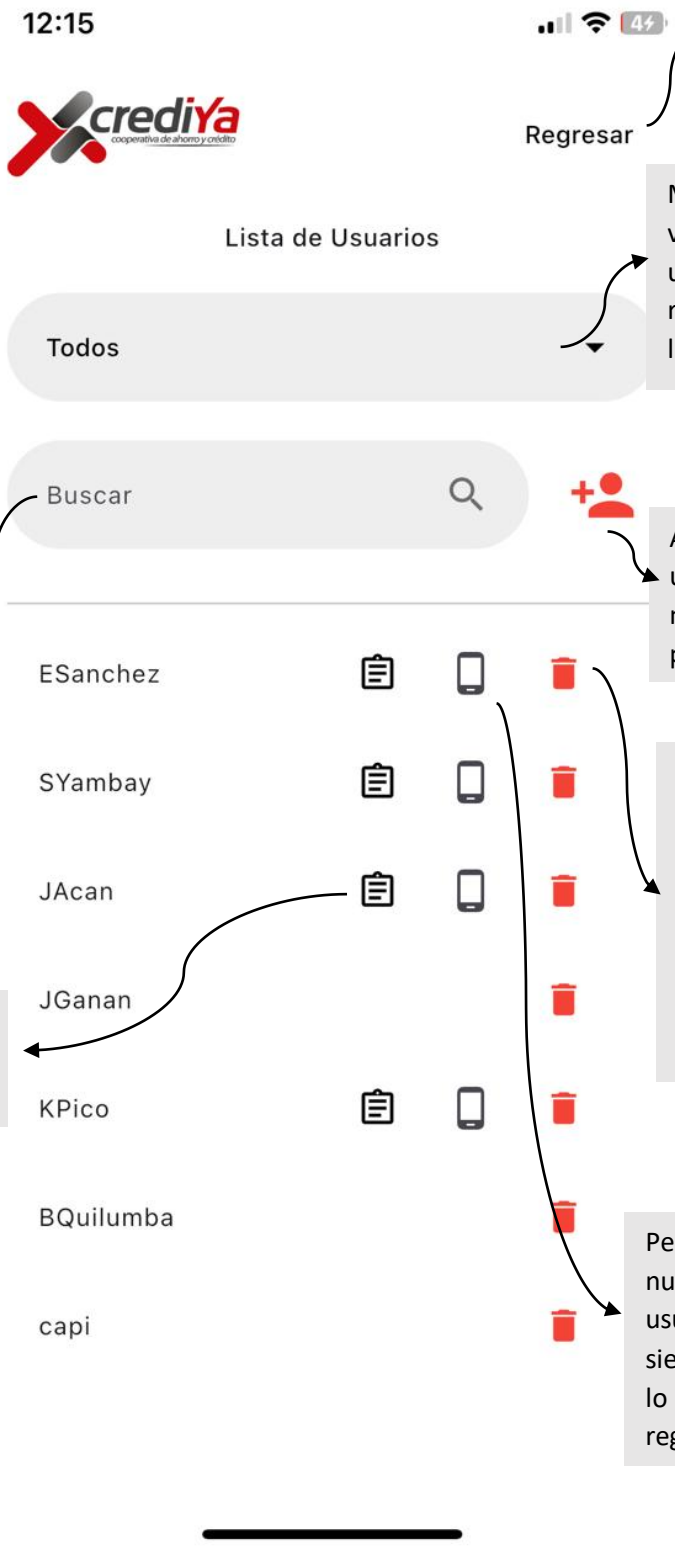


Al presionar este módulo, el sistema dirige a una pantalla donde el administrador puede actualizar su contraseña de manera segura.

Lista de Usuarios

La pantalla Lista de Usuarios permite al administrador visualizar, buscar y gestionar a todos los usuarios registrados en el sistema.

Desde esta interfaz se pueden agregar nuevos usuarios, consultar los dispositivos asignados y realizar acciones administrativas como asignación o eliminación, según las reglas del sistema.



Permite volver a la pantalla anterior del módulo Usuarios/Dispositivos.

Muestra un filtro que permite visualizar únicamente a los usuarios pertenecientes a un rol específico o presentar la lista completa.

Permite localizar rápidamente a un usuario ingresando su nombre o identificación dentro de la lista.

Al presionarlo, el sistema abre una pantalla para registrar un nuevo usuario dentro de la plataforma.

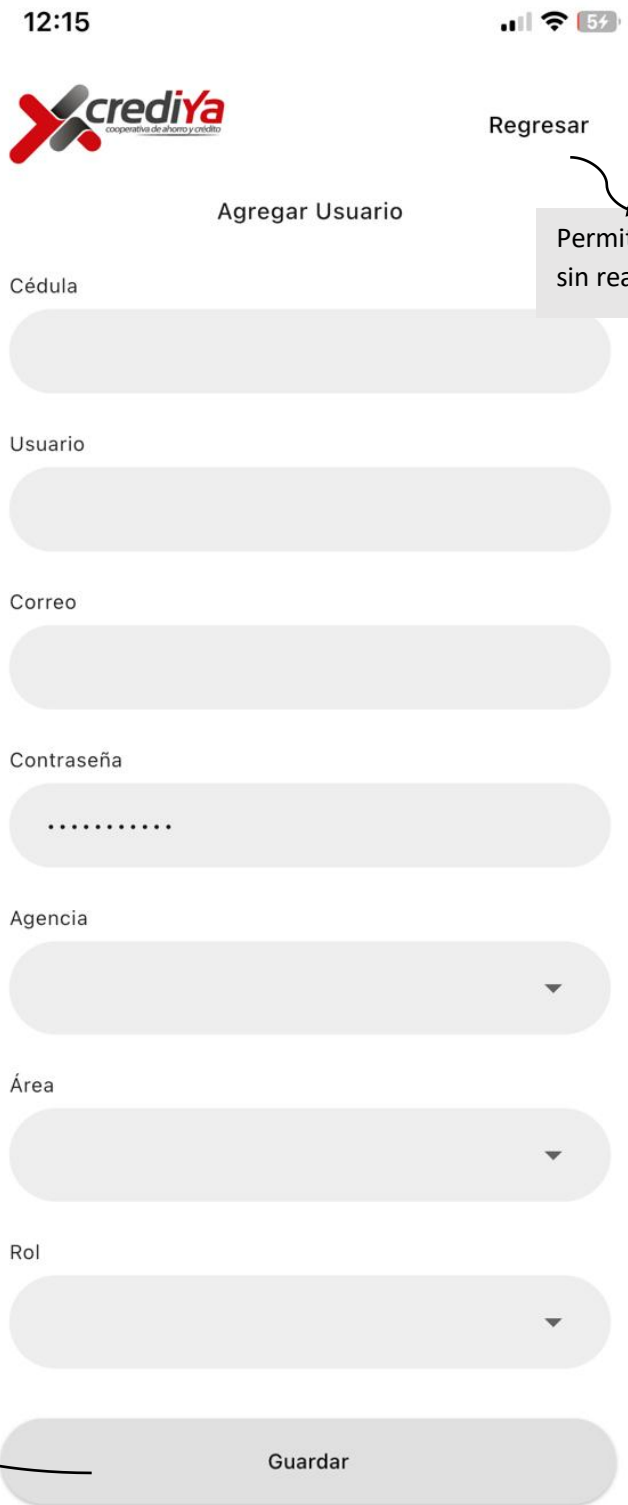
Esta opción elimina al usuario únicamente si no mantiene solicitudes activas o dispositivos fuera de la institución. El sistema valida automáticamente estas condiciones antes de permitir la eliminación.

Muestra los dispositivos asignados al usuario y su respectivo código QR.

Permite asignar un nuevo dispositivo al usuario seleccionado, siempre que el sistema lo permita según sus reglas de asignación.

Agregar Usuario

La pantalla Agregar Usuario permite registrar un nuevo usuario dentro del sistema. Desde esta interfaz, el administrador puede completar el formulario con la información requerida para crear una nueva cuenta y asignar los datos correspondientes a su perfil.



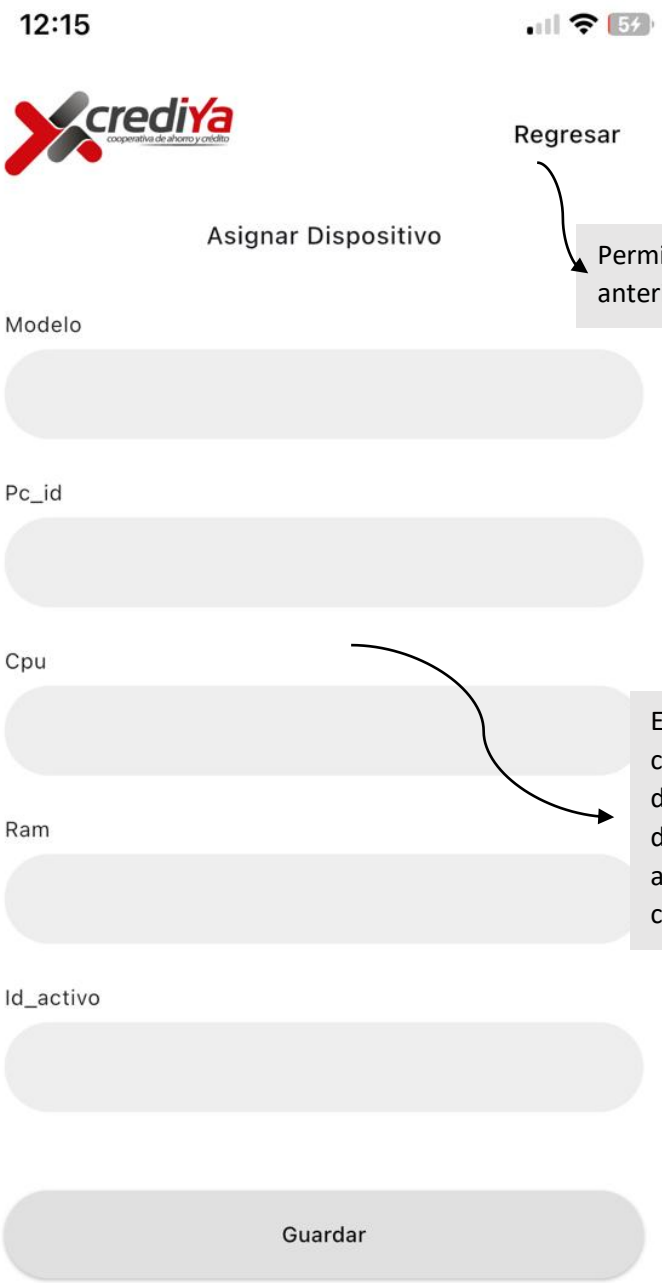
Permite volver a la pantalla anterior sin realizar cambios.

El administrador debe completar todos los campos solicitados, ingresando la información personal, institucional y el rol correspondiente del usuario que se desea incorporar al sistema.

Una vez llenados todos los campos, se debe presionar este botón para registrar al nuevo usuario. El sistema validará la información y confirmará el registro exitoso.

Asignar Dispositivo

La pantalla Asignar Dispositivo permite registrar un nuevo equipo y asociarlo a un usuario específico dentro del sistema. Desde esta interfaz, el administrador puede completar la información técnica del dispositivo para dejarlo correctamente vinculado al perfil del funcionario correspondiente.



Permite volver a la pantalla anterior sin realizar cambios.

El administrador debe completar todos los campos del formulario ingresando los datos del equipo que se asignará al usuario, tales como modelo, identificadores

Una vez completada la información, se debe presionar este botón para confirmar la asignación del dispositivo. El sistema registrará la información y vinculará el equipo al usuario seleccionado.

Código QR del Dispositivo

La pantalla Código QR del Dispositivo permite visualizar la información completa del equipo asignado a un usuario, junto con el código QR generado automáticamente durante su registro. Esta interfaz facilita la consulta, gestión y exportación de los datos del dispositivo, además de ofrecer opciones para eliminarlo o continuar con otras acciones administrativas.



Si el usuario tiene más de un equipo asignado, este menú permite seleccionar el dispositivo cuyo código QR e información se desea visualizar.

Representa los datos del equipo registrados en el sistema. Puede ser escaneado para obtener la información de manera inmediata.

En la parte inferior se muestran los datos asociados al equipo, tales como modelo, identificadores, características técnicas, agencia y fecha de registro.

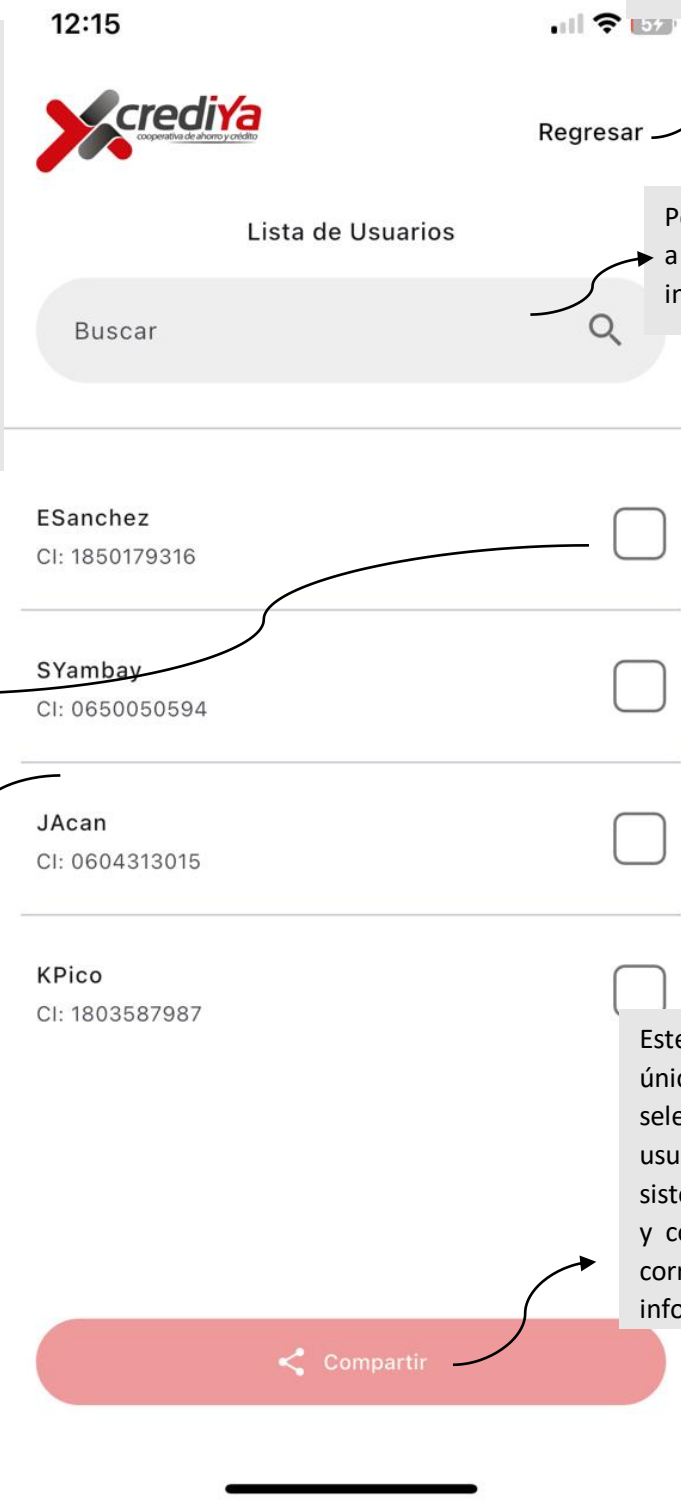
Elimina el dispositivo seleccionado, siempre que cumpla con las condiciones establecidas por el sistema.

Genera un documento con toda la información del dispositivo y su código QR para fines de archivo o control institucional.

Permite regresar a la pantalla de lista de usuarios para realizar nuevas gestiones.

Selección de Usuarios para Compartir

La pantalla Selección de Usuarios para Compartir permite elegir uno o varios usuarios con rol funcionario para generar y compartir un documento que contiene su información y el código QR asociado. Desde esta interfaz se puede filtrar la lista, seleccionar múltiples usuarios y proceder con la acción de compartir.



Permite volver a la pantalla anterior sin realizar cambios.

Permite localizar rápidamente a un usuario específico ingresando su nombre.

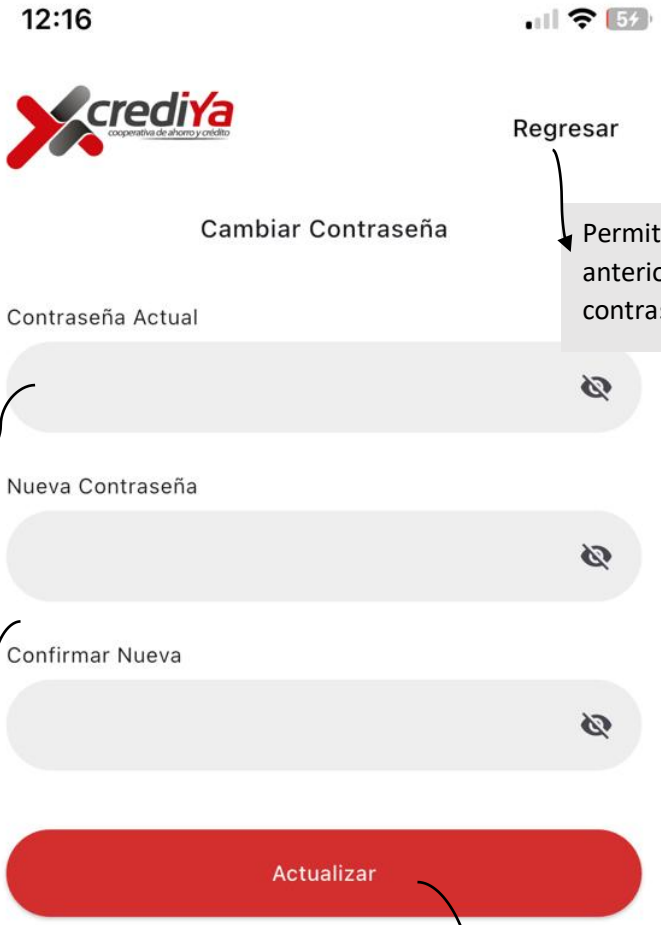
El administrador puede marcar una o varias casillas según los usuarios que desea incluir en el documento a compartir.

Se muestran únicamente los usuarios con rol funcionario. Cada registro incluye el nombre y la cédula, junto con una casilla de selección que permite elegir uno o varios usuarios al mismo tiempo.

Este botón se habilita únicamente cuando se ha seleccionado al menos un usuario. Al presionarlo, el sistema procede a generar y compartir el documento correspondiente con la información seleccionada.

Cambiar Contraseña

La pantalla Cambiar Contraseña permite al usuario actualizar su clave de acceso de manera segura. Para completar el proceso, el sistema solicita verificar la contraseña actual e ingresar y confirmar una nueva.



Permite volver a la pantalla anterior sin modificar la contraseña.

El usuario debe ingresar su contraseña vigente para validar su identidad antes de realizar cualquier cambio.

Se debe ingresar una nueva contraseña y repetirla en el campo de confirmación para asegurar que coinciden.

Una vez completados los campos correctamente, se debe presionar este botón para guardar la nueva contraseña.

Si toda la información es válida, el sistema actualizará la clave de acceso y mostrará un mensaje de confirmación.

Panel del usuario funcionario

La pantalla Panel del Usuario funcionario es el punto de inicio para los usuarios con rol funcionario. Desde esta interfaz pueden acceder a la información de su dispositivo, gestionar solicitudes de salida de activos, revisar el estado de sus solicitudes y actualizar su contraseña. También se ofrece la opción de cerrar sesión de forma segura.



Permite finalizar la sesión del usuario y regresar a la pantalla de inicio de sesión.

Al seleccionarlo, el sistema muestra la información del dispositivo asignado y habilita el botón para solicitar la salida del activo en caso de requerirlo.

Permite visualizar todas las solicitudes registradas por el usuario, organizadas en pendientes, aprobadas y denegadas.

Dirige a la pantalla donde el usuario puede actualizar su contraseña de manera segura.

Información del dispositivo

La pantalla Información del Dispositivo permite al usuario funcionario visualizar los datos técnicos del equipo que tiene asignado.

Si el usuario posee más de un dispositivo, puede seleccionar cuál desea consultar mediante el menú desplegable.

Desde esta interfaz también se habilita la opción para solicitar la salida del activo, conforme a los procedimientos establecidos por la institución.



Permite volver al panel principal del usuario sin realizar

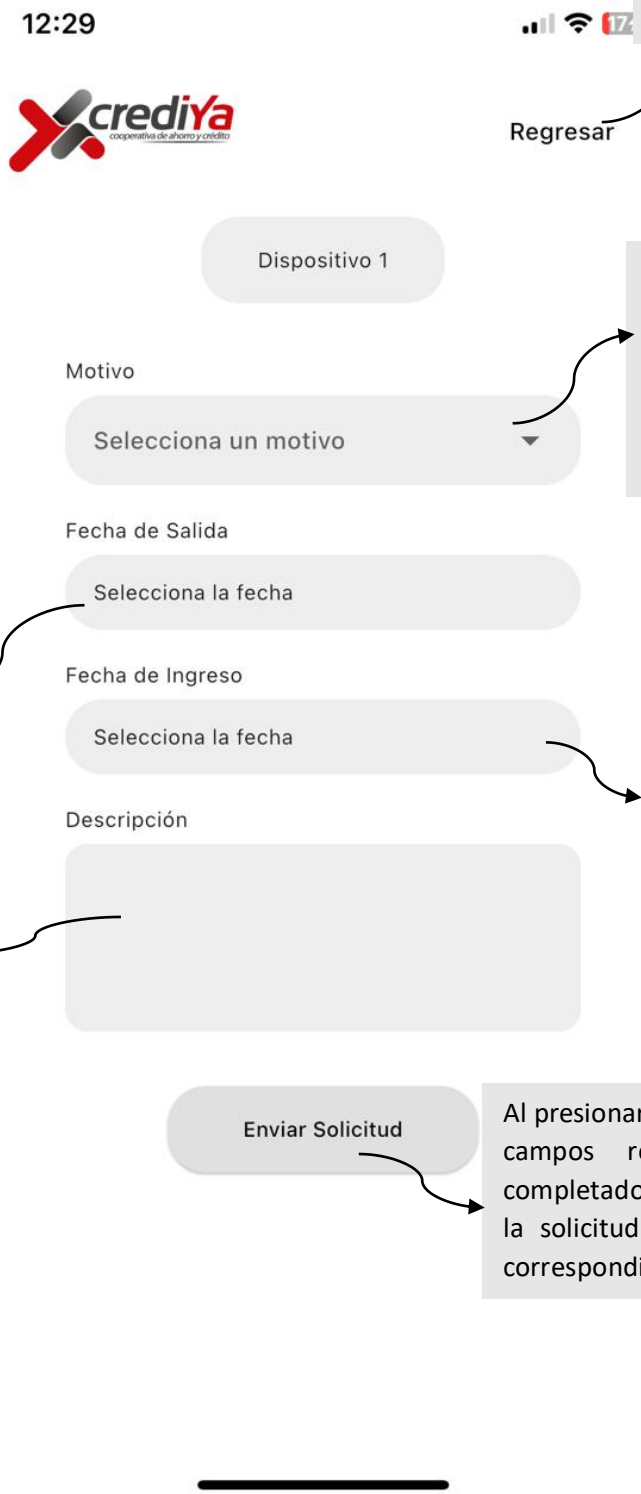
Muestra los dispositivos asignados al usuario. Si tiene más de uno, puede cambiar entre ellos para visualizar la información correspondiente.

Se presenta la información completa del equipo, incluyendo modelo, identificación, CPU, memoria RAM e ID del activo. Los datos se muestran de forma visual mediante tarjetas informativas.

Permite iniciar una solicitud de salida del dispositivo. El usuario debe presionar este botón para continuar con el registro de la solicitud y completar el formulario correspondiente.

Solicitar salida del Equipo

La pantalla Solicitar Salida del Activo permite al usuario funcionario registrar una solicitud formal para retirar temporalmente un dispositivo de la institución. En esta interfaz se selecciona el dispositivo, se indica el motivo, se establecen las fechas de salida e ingreso y se describe la razón de la solicitud. El sistema validará la información antes de permitir el envío.



Permite volver a la pantalla anterior sin enviar la solicitud.

Al seleccionarlo, se despliega un listado con los motivos disponibles para justificar la salida del activo. El usuario debe elegir uno antes de continuar.

Se debe seleccionar una fecha y hora de salida.

La fecha y hora de ingreso no pueden ser menores a las de salida. El sistema validará que las fechas cumplan estos criterios.

Permite ingresar una explicación adicional sobre el motivo de la salida del dispositivo.

Al presionarlo, el sistema valida todos los campos requeridos que han sido completados correctamente y registrará la solicitud y notificará al responsable correspondiente.

Historial de Solicitudes Enviadas

La pantalla Historial de Solicitudes Enviadas permite al usuario funcionario visualizar todas las solicitudes realizadas para la salida de activos. Esta interfaz cuenta con un filtro que organiza las solicitudes en categorías: pendientes, aprobadas y denegadas. Además, ofrece acceso al detalle completo de cada solicitud registrada.



Permite filtrar las solicitudes según su estado actual.

- Pendientes: solicitudes aún sin respuesta.
- Aprobadas: solicitudes autorizadas.
- Denegadas: solicitudes rechazadas.

Se muestran todas las solicitudes correspondientes al estado seleccionado.

Cada elemento incluye información relevante como el modelo del dispositivo, motivo, fecha de solicitud y fecha de aprobación o rechazo.

Al presionar sobre cualquier solicitud del listado, el sistema mostrará la información completa de dicha solicitud, incluyendo fechas, motivo, detalles del dispositivo y estado actual.

Detalle de Solicitud

La pantalla Detalle de Solicitud muestra la información completa de una solicitud seleccionada desde el historial. Aquí el usuario puede revisar todos los datos ingresados al momento de solicitar la salida del dispositivo, así como el estado final de la solicitud y la razón proporcionada por el responsable que la aprobó o rechazó.



Se presenta un resumen detallado del funcionario y el equipo seleccionado.

Razón o comentario final del responsable (por ejemplo: aprobado o denegado)

Permite regresar a la pantalla del historial de solicitudes para seguir consultando o realizar otras acciones dentro del sistema.

Panel del Oficial de Seguridad

La pantalla Panel del Oficial de Seguridad es el punto de acceso principal para los usuarios responsables de revisar, aprobar o denegar solicitudes de salida de activos.

Desde esta interfaz, el oficial puede visualizar el estado general de los dispositivos de la institución, acceder al historial completo de solicitudes

enviadas por los funcionarios y administrar su contraseña de acceso al sistema.



Permite finalizar la sesión y regresar a la pantalla de inicio de sesión.

Permite visualizar el estado actual de todos los dispositivos

Muestra el listado completo de solicitudes realizadas por los funcionarios, organizadas en pendientes, aprobadas y denegadas.

Desde esta sección, el oficial puede revisar la información de cada solicitud y tomar decisiones de aprobación o rechazo.

Dirige a la pantalla correspondiente para actualizar la contraseña del oficial de seguridad de manera segura.

Enviar solicitud salida de equipo

La pantalla Historial de Solicitudes del Oficial de Seguridad permite al responsable visualizar todas las solicitudes enviadas por los funcionarios, clasificadas según su estado actual. Desde esta interfaz se pueden consultar solicitudes pendientes para revisión, así como solicitudes aprobadas y denegadas en fechas anteriores.

Cada elemento del listado ofrece acceso al detalle completo de la solicitud seleccionada.



Permite filtrar las solicitudes según su situación actual:

- Pendientes: solicitudes que requieren ser aprobadas o denegadas por el oficial.
- Aprobadas: solicitudes autorizadas previamente.
- Denegadas: solicitudes rechazadas, con motivo visible.

Muestra la información relevante de cada solicitud.

Al presionar sobre cualquier solicitud del listado, el sistema mostrará la información completa, permitiendo su revisión y, en el caso de las solicitudes pendientes, la toma de decisión correspondiente.

Reporte de estado de Dispositivos

La pantalla Reporte de Estado de Dispositivos permite al oficial de seguridad visualizar el estado actual de todos los equipos asignados a los funcionarios.

Desde esta interfaz se puede identificar si un dispositivo se encuentra fuera de la institución, si ya fue ingresado o si presenta retraso en su retorno.

Además, cada elemento del listado ofrece acceso al detalle completo de la solicitud asociada.



Permite volver a la pantalla principal del oficial de seguridad.

Permite filtrar los dispositivos según su situación actual:

- Todos: muestra todos los dispositivos registrados.
- Fuera: dispositivos cuya salida ha sido registrada y aún no han retornado.
- Ingresados: equipos que ya han sido devueltos dentro del plazo establecido.
- Retrasados: dispositivos que no han ingresado en la fecha y hora previstas.

Cada elemento muestra la información relevante del equipo y su situación

Panel del Guardia de Seguridad

La pantalla Panel del Guardia de Seguridad constituye el punto de acceso principal para los usuarios encargados de verificar y registrar la salida e ingreso de los dispositivos mediante códigos QR.

Desde esta interfaz, el guardia puede consultar el estado general de los equipos, escanear códigos QR para validar movimientos y actualizar su contraseña cuando sea necesario.



Permite finalizar la sesión del guardia y regresar a la pantalla de inicio de sesión.

Al seleccionarlo, el sistema muestra el listado de solicitudes aprobadas, denegadas y retrasadas de todos los funcionarios.

Desde esta vista, el guardia puede consultar el estado actual de los equipos y acceder al detalle de cada solicitud.

Abre la pantalla de escaneo de código QR.

Una vez escaneado el código del dispositivo, el sistema dirige automáticamente a la pantalla donde se registra la salida o el ingreso correspondiente.

Dirige a la pantalla en la que el guardia puede actualizar su contraseña de manera segura.

Solicitudes de Verificación

La pantalla Solicitudes para Verificación permite al guardia de seguridad consultar las solicitudes aprobadas, denegadas y retrasadas enviadas por los funcionarios.

Esta vista facilita el monitoreo del estado de los dispositivos y ofrece acceso directo al detalle de cada solicitud para su revisión.

Además, desde esta interfaz el guardia puede dirigirse al módulo de cambio de contraseña cuando sea necesario.



Permite volver al panel principal del guardia de seguridad.

Permite filtrar las solicitudes según su estado actual:

- Aprobadas: solicitudes autorizadas y listas para ser procesadas en la salida o ingreso del activo.
- Denegadas: solicitudes rechazadas por el oficial de seguridad.
- Retrasadas: solicitudes cuyo dispositivo no ha retornado dentro del tiempo previsto.

Muestra la información esencial de cada solicitud.

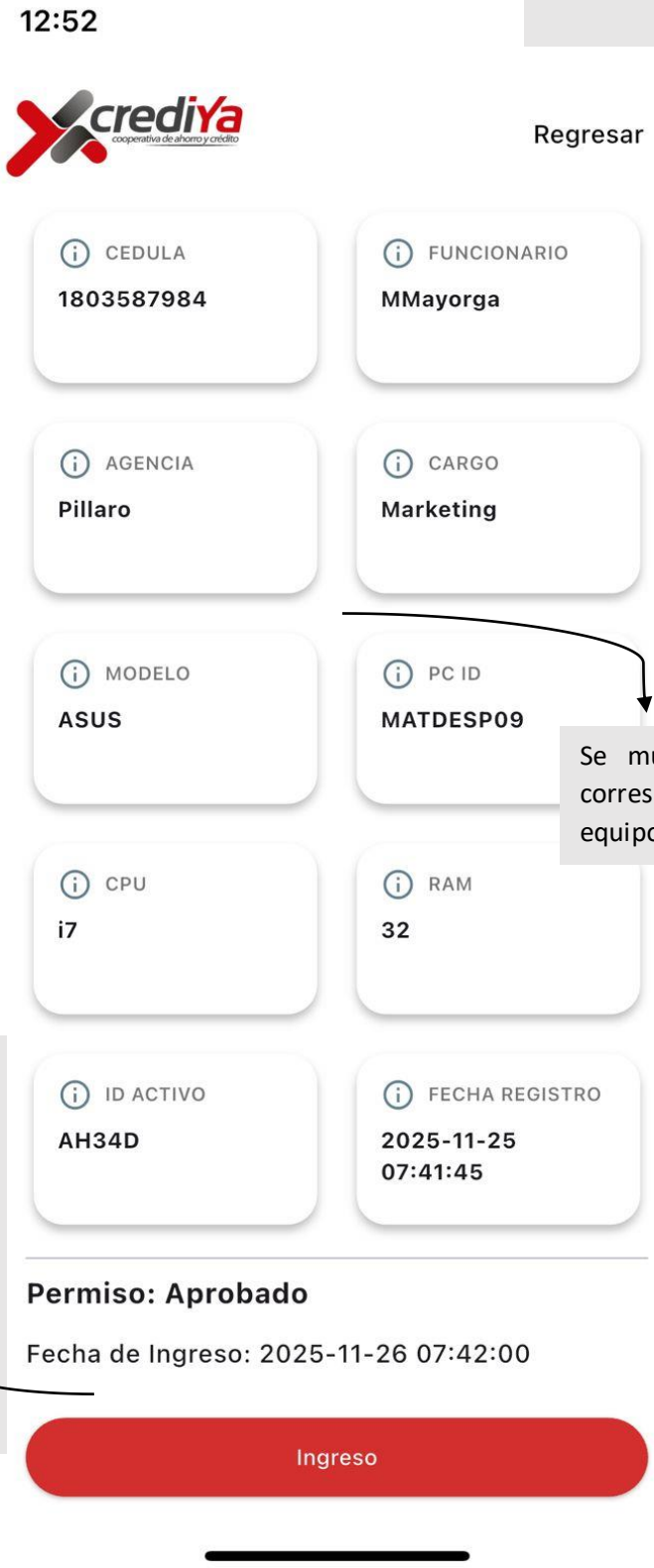
Al presionar sobre cualquier solicitud del listado, el sistema mostrará la información completa, permitiendo al guardia confirmar los datos antes de registrar la salida o el ingreso.

Registro de Salida/Ingreso Dispositivo

La pantalla Registro de Ingreso del Dispositivo permite al guardia de seguridad visualizar la información completa del funcionario y del equipo cuya salida fue aprobada previamente.

Desde esta interfaz, el guardia verifica los datos del activo y registra su ingreso una vez que el dispositivo retorna a la institución.

Permite volver a la pantalla anterior sin realizar ningún registro adicional.



Se muestra toda la información correspondiente al usuario y al equipo.

Se indica si la solicitud fue aprobada y se muestra la fecha prevista para la salida del dispositivo y se registra la salida del equipo, y el mismo proceso para el ingreso. El sistema registra la salida y el ingreso del dispositivo, completando el proceso de control de equipos.

.