

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA PARA EL CONTROL DE INGRESO DEL PERSONAL EN LAS INSTALACIONES DE LA COORDINACIÓN ZONAL 3 DEL SERVICIO INTEGRADO DE SEGURIDAD ECU 911

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

ÁREA: Seguridad y Redes

LÍNEA DE INVESTIGACIÓN: Software, Tecnologías de la información y Ciencia de datos.

AUTOR: Karina Mishell Cunuhay Quirco

TUTOR: Ing. David Omar Guevara Aulestia, MSc.

Ambato - Ecuador

enero – 2026

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA PARA EL CONTROL DE INGRESO DEL PERSONAL EN LAS INSTALACIONES DE LA COORDINACIÓN ZONAL 3 DEL SERVICIO INTEGRADO DE SEGURIDAD ECU 911, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Karina Mishell Cunuhay Quirco, estudiante de la Carrera de Ingeniería en Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada 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.

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA
Validar únicamente con FirmaEC

Ing. David Omar Guevara Aulestia, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA PARA EL CONTROL DE INGRESO DEL PERSONAL EN LAS INSTALACIONES DE LA COORDINACIÓN ZONAL 3 DEL SERVICIO INTEGRADO DE SEGURIDAD ECU 911 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.

Firmado electrónicamente por:
KARINA MISHELL CUNUHAY QUIRCO
Validar únicamente con FirmaEC

Karina Mishell Cunuhay Quirco

C.C. 0550154157

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.

Firmado electrónicamente por:
KARINA MISHELL CUNUHAY QUIRCO
Validar únicamente con FirmaEC

Karina Mishell Cunuhay Quirco

C.C. 0550154157

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por la señorita Karina Mishell Cunuhay Quirco 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 SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA PARA EL CONTROL DE INGRESO DEL PERSONAL EN LAS INSTALACIONES DE LA COORDINACIÓN ZONAL 3 DEL SERVICIO INTEGRADO DE SEGURIDAD ECU 911, 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, juntamente 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:
FRANKLIN OSWALDO MAYORGA MAYORGA
Validar únicamente con FirmaEC

Ing. Franklin Mayorga Mayorga, Mg.
PROFESOR CALIFICADOR

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

Ing. Marcos Benitez Aldas, Mg.
PROFESOR CALIFICADOR

DEDICATORIA

A mi madre, Sofía; mujer luchadora que, con manos vacías, me entregó el universo y nadó contra la corriente para que yo pudiera llegar a la orilla. Gracias por su amor incondicional, aquel que trasciende dimensiones.

A mis hermanos, pilares de mi alma: Jhon, mi compañero anhelado, quien con su llegada desterró para siempre mi soledad; y Amy, cuya ternura fue el bálsamo dulce que apaciguó mis dolores más profundos. Ellos son mi refugio; su existencia es la brújula que orienta mi camino.

AGRADECIMIENTO

A Dios, por ser la fuerza que me sostuvo en este mundo frente a toda adversidad, por haberme bendecido con el regalo invaluable de mi madre y por haber tejido en mi destino el encuentro con personas maravillosas que iluminaron mi camino.

A Bryan por ser apoyo constante en mis momentos de duda, eres el matiz más dulce de esta historia.

A mis amigos, Jairo y Martín que se convirtieron en hermanos, gracias por ser refugio en las batallas y risa en las victorias.

Gratitud infinita a toda mi familia materna, mi raíz y mi amparo. Gracias por estar presente en cada etapa de mi vida, brindándome siempre el calor de un hogar y los valores que hoy definen mi ser. Gracias por no soltarme nunca, por ser mi compañía constante y el amoroso cimiento sobre el cual he construido mis sueños.

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 ..... **xiv**

ÍNDICE DE ANEXOS ..... **xviii**

RESUMEN EJECUTIVO ..... **xix**

ABSTRACT ..... **xx**

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 6

1.3.1 Tecnologías de la información 6

1.3.2 Seguridad física informática 6

1.3.3 Identificación biométrica 7

1.3.4 Sistema de reconocimiento facial 7

1.3.5 Validación de identidad personal 7

1.3.6 Supervisión y control de acceso 8

1.3.7 Gestión de talento humano 8

1.3.8 Control de ingreso del personal 9

1.4 Objetivos 9

1.4.1 Objetivo general 9

1.4.2 Objetivos específicos 9

CAPÍTULO II. METODOLOGÍA 11

2.1 Materiales 11

2.2 Métodos 15

2.2.1 Modalidad de la investigación 15

2.2.2 Población y muestra 16

2.2.3 Recolección de información 17

2.2.4 Procesamiento y análisis de datos 31

CAPÍTULO III. RESULTADOS Y DISCUSIÓN 33

3.1 Análisis y discusión de los resultados 33

3.1.1 Requisitos técnicos del reconocimiento facial 35

3.1.1.1 Modelos de detección y alineación del rostro 35

3.1.1.2 Hardware requerido 39

3.1.1.3 Dispositivo biométrico 40

3.1.1.4 Servidor 40

3.1.1.5 Software y frameworks 41

3.1.2 Requisitos operativos del reconocimiento facial 42

3.1.2.1 Captura inicial de fotos – creación de plantilla 42

3.1.2.2 Uso diario del sistema 42

3.1.2.3 Procedimientos operativos 43

3.1.2.4 Seguridad operativa 43

3.1.2.5 Protocolos de contingencia 43

3.1.3 Metodologías ágiles de desarrollo 43

3.2 Desarrollo de la propuesta 45

3.3 Aplicación de la metodología de trabajo 45

3.3.1 Planificación 45

3.3.2 Desarrollo 49

3.3.3 Integración y pruebas 69

3.3.4 Validación y entrega 74

3.3.4.1 Precisión y tasa de error: 74

3.3.4.2 Equidad 77

3.3.4.3 Suplantación 78

3.3.4.4 Cumplimiento legal 78

3.3.4.5 Entrega 79

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 89

4.1 Conclusiones 89

4.2 Recomendaciones 90

REFERENCIAS BIBLIOGRÁFICAS 92

ANEXOS 96

ÍNDICE DE TABLAS

Tabla 1. Cadenas de búsqueda en bases de datos de investigación científica. 2

Tabla 2. Filtros de búsqueda en repositorios de universidades del Ecuador. 3

Tabla 3. Criterios de inclusión y exclusión. 4

Tabla 4. Formato de entrevista. 14

Tabla 5. Formato de ficha de observación. 15

Tabla 6. Población de estudio. 16

Tabla 7. Escala de interpretación de Cronbach. 26

Tabla 8. Entrevista. 27

Tabla 9. Ficha de observación. 30

Tabla 10. Comparación modelos de reconocimiento facial. 38

Tabla 11. Comparación entre metodologías ágiles. 44

Tabla 12. Requerimientos funcionales. 46

Tabla 13. Requerimientos no funcionales. 47

Tabla 14. Fases del proyecto. 49

Tabla 15. Medición de tiempo de reconocimiento facial. 72

Tabla 16. Verificación de equidad. 78

Tabla 17. Verificación de suplantación. 78

Tabla 18. Verificación de cumplimiento legal. 78

Tabla 19. Cumplimiento normativo. 79

Tabla 20. Verificación de requisitos funcionales. 79

Tabla 21. Prueba de aceptación 1. 81

Tabla 22. Prueba de aceptación 2. 82

Tabla 23. Prueba de aceptación 3. 83

Tabla 24. Prueba de aceptación 4. 84

Tabla 25. Prueba de aceptación 5. 85

Tabla 26. Validación de pruebas de cada iteración. 86

ÍNDICE DE FIGURAS

Figura 1. Resultado pregunta 1. 17

Figura 2. Resultados pregunta 2. 18

Figura 3. Resultados pregunta 3. 19

Figura 4. Resultados pregunta 4. 20

Figura 5. Resultados pregunta 5. 21

Figura 6. Resultados pregunta 6. 22

Figura 7. Resultados pregunta 7. 23

Figura 8. Resultados pregunta 8. 24

Figura 9. Resultados pregunta 9. 24

Figura 10. Resultados pregunta 10. 25

Figura 11. Diagrama de proceso tradicional de control de ingreso. 33

Figura 12. Diagrama de procesos optimizados. 34

Figura 13. Fases de la metodología hibrida Kanban – Scrum. 45

Figura 14. Arquitectura del sistema de reconocimiento facial. 50

Figura 15. Diagrama de flujo del reconocimiento facial. 51

Figura 16. Fase1: Detección facial. 52

Figura 17. Fase 2: Análisis de atributos. 52

Figura 18. Fase 3: Extracción de características. 53

Figura 19. Fase 4: Verificación. 54

Figura 20. Diagrama entidad - relación de la base de datos. 55

Figura 21. Prototipo de inicio de sesión móvil. 56

Figura 22. Prototipo de modo de uso. 57

Figura 23. Motivo de registro. 58

Figura 24. Escaneo y verificación. 59

Figura 25. Registro mediante PIN. 60

Figura 26. Prototipo web de inicio de sesión. 61

Figura 27. Prototipo web, panel dashboard – Administrador. 61

Figura 28. Prototipo módulo web usuarios – Administrador. 62

Figura 29. Prototipo módulo web empleados – Administrador. 62

Figura 30. Prototipo ventana creación empleado – Administrador. 63

Figura 31. Prototipo ventana creación empleado externo – Administrador. 63

Figura 32. Prototipo página de usuarios de recursos humanos. 64

Figura 33. Prototipo formulario web – Guardias. 64

Figura 34. Diagrama de caso de uso de administradores. 65

Figura 35. Diagrama de caso de uso de recursos humanos y guardias. 65

Figura 36. Diagrama de caso de uso de acceso a las instalaciones–empleados. 66

Figura 37. Verificación de instalación de InsightFace. 66

Figura 38. Inicialización del detector y extractor de características faciales. 67

Figura 39. Detección facial y preparación del vector. 67

Figura 40. Cálculo de coincidencias. 67

Figura 41. Conexión PostgreSQL. 68

Figura 42. Guardado de embeddings en la base de datos. 68

Figura 43. Validación ESP32. 68

Figura 44. Pantalla modo de uso. 69

Figura 45. Pantalla elección motivo de registro. 70

Figura 46. Reconocimiento facial. 70

Figura 47. Registro a través de PIN. 71

Figura 48. Salida de motivos solicita usuario y clave de administrador. 71

Figura 49. Ingreso de un nuevo empleado-administrador. 72

Figura 50. Registro facial. 73

Figura 51. Carga de imágenes exitosa. 73

Figura 52. Verificación de ingreso, listado general. 74

Figura 53. Resultados de la matriz de confusión. 75

Figura 54. Matriz de confusión con métricas. 75

Figura 55. Resultado matriz de confusión. 76

Figura 56. Matriz de confusión. 77

Figura 57. Ingreso de un nuevo empleado. 80

Figura 58. Carga de plantillas faciales iniciales. 81

Figura 59. Ingreso de datos del visitante. 82

Figura 60. Verificación de ingreso de datos del visitante. 82

Figura 61. Visualización de dashboard. 83

Figura 62. Generación de reportes descargables. 84

Figura 63. Usuarios registrados a través del dispositivo biométrico. 85

Figura 64. Código de emparejamiento. 87

Figura 65. Selección modo de uso del dispositivo. 87

Figura 66. Pantalla de acceso para instalación. 88

Figura 67. Fin de instalación. 88

ÍNDICE DE ANEXOS

Anexo A. Manual de usuario. 96

Anexo B. Instalación de dispositivos biométricos 103

RESUMEN EJECUTIVO

El presente proyecto aborda la falta de un sistema oficial para el control de ingreso del personal en la Coordinación Zonal 3 del SIS ECU 911. Para dar respuesta a esta problemática se aplicó una metodología mixta que incluyó encuestas, entrevistas, fichas de observación y revisión bibliográfica en repositorios académicos como SCOPUS, IEEE Xplore y ScienceDirect.

Se investigaron los requisitos técnicos y condiciones operativas del reconocimiento facial para su aplicación en el control biométrico. La revisión comparativa de tres modelos permitió analizar aspectos esenciales como embeddings, robustez, dificultad de entrenamiento y limitaciones, posicionando a InsightFace como la opción más adecuada por su precisión y eficiencia. Se definió el uso de hardware basado en teléfonos móviles reutilizados por su versatilidad al integrar cámara y pantalla en un solo dispositivo, complementado con software y frameworks libres y de código abierto.

Los requisitos operativos incluyeron la captura inicial de fotografías para la plantilla, protocolos para garantizar el uso diario, resguardo seguro de la información, cumplimiento legal y protección de datos personales, además de mecanismos de contingencia para asegurar la continuidad del sistema.

Los resultados evidenciaron una aceptación institucional del 89% y un desempeño del modelo con un 90% de precisión, reduciendo errores humanos y asegurando confiabilidad. Se concluye que la propuesta mejora la eficiencia del control de acceso, cumple normativas y promueve la sostenibilidad mediante la reutilización tecnológica, contribuyendo a la transformación digital de procesos estratégicos.

Palabras claves: Control de ingreso, Seguridad Institucional, InsightFace, Reconocimiento facial, ECU 911.

ABSTRACT

This project addresses the lack of an official system for controlling staff access to Zone 3 Coordination of SIS ECU 911. To respond to this problem, a mixed methodology was applied that included surveys, interviews, observation sheets, and a literature review in academic repositories such as SCOPUS, IEEE Xplore, and ScienceDirect.

The technical requirements and operating conditions of facial recognition for use in biometric control were investigated. A comparative review of three models allowed for the analysis of essential aspects such as embeddings, robustness, training difficulty, and limitations, positioning InsightFace as the most suitable option due to its accuracy and efficiency. The use of hardware based on reused mobile phones was defined due to its versatility in integrating a camera and screen into a single device, complemented by free and open-source software and frameworks.

Operational requirements included the initial capture of photographs for the template, protocols to ensure daily use, secure storage of information, legal compliance, and personal data protection, as well as contingency mechanisms to ensure system continuity.

The results showed 89% institutional acceptance and 90% model accuracy, reducing human error and ensuring reliability. It is concluded that the proposal improves access control efficiency, complies with regulations, and promotes sustainability through technological reuse, contributing to the digital transformation of strategic processes.

Keywords: Access control, Institutional Security, InsightFace, Facial recognition, ECU 911.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA PARA EL CONTROL DE INGRESO DEL PERSONAL EN LAS INSTALACIONES DE LA COORDINACIÓN ZONAL 3 DEL SERVICIO INTEGRADO DE SEGURIDAD ECU 911.

1.1.1 Planteamiento del problema

En la era digital, los sistemas de control de acceso son herramientas esenciales para garantizar la seguridad del personal y de las instalaciones de cualquier institución, ya que permiten gestionar y restringir el acceso a áreas específicas de personas o vehículos. Estos sistemas se basan en procesos sistemáticos que aseguran que únicamente el personal autorizado pueda ingresar o salir de un espacio físico, llevando un registro y monitoreo constante que fortalece la seguridad y la eficiencia operativa. Entre los principales beneficios de la implementación de un sistema de control de acceso se destacan la prevención de amenazas externas, reducción de riesgos internos y la generación de registros que facilitan auditorias en caso de ser necesarias. También, posibilitan la integración con cámaras, alarmas y sistemas de monitoreo en tiempo real para una respuesta oportuna ante emergencias. De esta manera, los sistemas de control de acceso contribuyen a la recepción integral del personal y los activo, al mismo tiempo que apoyan el cumplimiento normativo vigente [1].

Dado el rol fundamental de la seguridad física para una institución, varias empresas u organizaciones han optado por implementar estándares internacionales que manejan las normas de la International Organization for Standardization (ISO, en español Organización Internacional de Normalización), como la norma ISO 27001 que establece requisitos para un sistema de Gestión de Seguridad de la Información (SGSI), A pesar de que la adopción de estas normas suele ser voluntarias tiene gran impacto en las prácticas empresariales latinoamericanas y a nivel mundial [2].

Organismos internacionales incluyendo la Organización Internacional de Policía Criminal (INTERPOL) resaltan la relevancia de los sistemas biométricos en la seguridad interna como componente esencial para la protección física, seguridad de la información y continuidad operativa [3].

Según la revista Innovación la integración de soluciones biométricas como estrategia de identificación se encuentra dentro de las diez primeras tendencias que marcan el rumbo de la biometría en América Latina [4].

En Ecuador, diversas entidades que han incorporado soluciones biométricas para la gestión del tiempo, control de acceso, seguridad y la administración del personal. En este contexto, la coordinación zonal 3 del Servicio Integrado de Seguridad ECU 911, como sede regional encargada de brinda respuesta inmediata ante emergencias en conjunto con organismos de seguridad pública, enfrenta la necesidad de fortalecer sus mecanismos de control de ingreso[5].

El control de acceso al personal constituye un factor crítico para salvaguardar la información sensible y garantizar un registro preciso de quienes ingresan a la institución, alineándose con las mejores prácticas internacionales de seguridad física, especialmente en instituciones estratégicas de esta naturaleza.

1.2 Antecedentes investigativos

Se realizó una revisión bibliográfica a través de la búsqueda de fuentes de información científica y académica, en las bases de datos certificadas como SCOPUS, IEEE Xplore y ScienceDirect para lo cual se aplicaron cadenas de búsqueda con palabras clave como “biometric control”, “facial recognition” y “Access control systems”, tomando en cuenta información a partir del año 2020 como se encuentran detalladas en la Tabla 1.

Tabla 1. Cadenas de búsqueda en bases de datos de investigación científica.

Base de datos	Cadena de búsqueda	Número de artículos

Scopus	(TITLE-ABS-KEY (biometric control) AND (LIMIT-TO (SUBJAREA,"COMP") OR LIMIT-TO (SUBJAREA,"ENGI")) AND (LIMIT-TO (DOCTYPE,"ar") OR LIMIT-TO (DOCTYPE,"cp")) AND (LIMIT-TO (EXACTKEYWORD, "Biometrics") OR LIMIT-TO (EXACTKEYWORD,"Article") OR LIMIT-TO (EXACTKEYWORD,"Authentication") OR LIMIT-TO (EXACT KEYWORD,"Access Control")) AND (LIMIT-TO (LANGUAGE,"English") OR LIMIT-TO (LANGUAGE,"Spanish")))	28
	(TITLE-ABS-KEY (facial recognition) AND PUBYEAR >2020 AND PUBYEAR <2025 AND (LIMIT-TO (DOCTYPE, "re")) OR LIIT-TO (DOCTYPE, "ar")))	30
IEEE Xplore	("All Metadata":"facial recognition") AND (("All Metadata":"biometrics") OR ("All Metadata":"access control") OR ("All Metadata":"identity verification")) Filters Applied: 202-2025 Language: English – Spanish Document type: Article, Conference paper	45
ScienceDirect	TITLE ("Access control system") AND ("access control" OR "security") AND ("authentication" OR "authorization") Date: from 2023 to 2025 Language: English Access type: Open Aceess	12
Total		115

La Tabla 2 respalda la búsqueda de información académica en repositorios como la Escuela Politécnica Nacional y la Universidad Técnica de Ambato a partir del año 2021 hasta el 2024.

Tabla 2. Filtros de búsqueda en repositorios de universidades del Ecuador.

Universidad	**Filtro de búsqueda**	**Número de artículos**
Escuela Politécnica Nacional	Ingeniería en Electricidad y Computación.	120
Universidad Técnica de Ambato	Ingeniería en Sistemas, Electrónica e Industrial	125
Total		245

Además, se efectuó una búsqueda de información en repositorios académicos aplicando criterios de inclusión y exclusión relacionados principalmente con las fechas de publicación como muestra la Tabla 3. Se seleccionó únicamente

investigaciones vinculadas a tecnologías biométricas, aplicaciones en entornos reales o simulados, documentos de acceso abierto y artículos centrados en el reconocimiento facial.

Tabla 3. Criterios de inclusión y exclusión.

Criterios de inclusión	Criterios de exclusión
Artículos enfocados a tecnologías biométricas (reconocimiento facial).	Investigaciones que no aborden tecnologías biométricas.
Estudios acerca de sistemas de control de acceso mediante identificación biométrica.	Investigaciones que no aborden sistemas de control de acceso
Investigaciones entre los años 2020-2025	Investigaciones antes del año 2020
Aplicaciones o estudios en entornos reales o simulados.	Trabajos que no cuenten con respaldo académico.
Documentos de investigaciones de acceso libre.	Artículos de paga

Un artículo emitido por la compañía Karspersky [6] destaca la importancia de la lectura de la geometría del rostro, identificando de factores clave como la distancia entre los ojos, profundidad de las cuencas, distancia entre frente y mentón, forma de pómulos y contorno de labios, con el objetivo de identificar puntos referenciales para distinguir un rostro. El reconocimiento facial es considerado la medición biométrica más natural, y se aplica en múltiples ámbitos, como el desbloqueo de dispositivos, control en aeropuertos y fronteras, operaciones bancarias, publicidad, salud e incluso la sustitución de llaves de automóviles. A nivel global, empresas como Amazon, Apple, Coca-Cola y Google utilizan esta tecnología con fines diversos, ñp qie demuestra su utilidad en la identificación, la protección y la seguridad, junto con otras modalidades biométricas como la voz, huellas dactilares o reconocimiento del iris y la retina.

Según J. Reyes, C. Castañeda, L. Alva y A. Mendoza [7], en su investigación presenta el diseño de un sistema de reconocimiento facial basado en Inteligencia Artificial (IA) mediante redes neuronales convolucionales. Desarrollado en Python con OpenCV e Imutils, registró 450 imágenes faciales en un dataset mediante scripts personalizados. El modelo fue entrenado con el algoritmo Local Binary Pattern Histogram (LBPH), generando un archivo Extensible Markup Language (XML) con los factores de ponderación. Al

evaluar rostros en tiempo real, el sistema maximizó la precisión y redujo la intervención humana. Se emplearon herramientas como Visual Studio Code y bibliotecas numéricas como NumPy. Los resultados demuestran la viabilidad de integrar IA y aprendizaje profundo en sistemas de control de acceso. Además, al limitar el ingreso solo a personal autorizado, se refuerza la seguridad de la información. Esto evidencia el potencial de la visión artificial en entornos de autenticación biométrica.

M. I. Ouloul, Z. Moutakki, A. Amghar, y K. Afdel [8] sugieren la implementación de sistemas de reconocimiento facial en hardware embebido pero presentar un reto por sus limitaciones de operación y memoria. Sin embargo, estas plataformas ofrecen ventajas como bajo costo, portabilidad y autonomía. Como solución, se propone el uso de descriptores Local Binary Pattern (LBP), organizados en tres etapas: detección, extracción de rasgos y clasificación. Esta metodología se adapta a las capacidades del hardware, logrando equilibrio entre precisión y tiempo de respuesta.

Autores como H. L. Gururaj, B. C. Soundarya, S. Priya, J. Shreyas, y F. Flammini [9] exponen que las técnicas de reconocimiento facial (RF) presentan limitaciones en tres categorías principales: apariencia, características e híbridos, afectadas por factores como envejecimiento, oclusiones, postura, emociones y variaciones de iluminación. Los avances recientes clasifican los métodos según el tipo de entrada (imagen o video) y destacan la identificación y verificación como funciones clave en aplicaciones como pagos electrónicos y vigilancia. Aunque los primeros enfoques, como los Modelos de Procesamiento Paralelo Masivo (MPP), eran versátiles, pero dependían de anotaciones manuales, el desarrollo de técnicas como la destilación de autoatención y el aprendizaje profundo ha mejorado significativamente la precisión y velocidad del RF. Arquitecturas modernas como CNN-LSTM-ELM y MM-DFR integran información multimodal para generar firmas faciales más compactas, mientras que el aprendizaje por transferencia permite estimaciones faciales 3D en tiempo real, aumentando la eficacia y resiliencia de estos sistemas.

Por otro lado, C. Morocho [10] en su proyecto de titulación resalta que el control de asistencia es fundamental para garantizar la productividad y puntualidad de los empleados, ya que la falta de este puede generar ausentismo, tardanzas y baja calidad en el servicio. Como solución, se desarrolló un prototipo de sistema para el Centro de Desarrollo Infantil Temprano (CDI-CI) "Cielo Infantil", capaz de registrar entradas, salidas y temperatura corporal del personal. El proyecto se estructuró en tres etapas: diseño, implementación y análisis teórico, aplicando el Modelo Vista Controlador (MVC) e integrando tecnologías como ESP-32, Angular, Ionic y Firebase. El sistema, basado en huellas dactilares, permite además registrar horas extras y sus motivos, diferenciando roles entre administradores y empleados. Las pruebas confirmaron su eficacia, con una rápida adaptación de los usuarios, lo que evidencia su valor y aporte a la gestión organizacional.

1.3 Fundamentación teórica

1.3.1 Tecnologías de la información

Es el uso de ordenadores en conjunto con softwares, aplicaciones en la nube y redes para el desarrollo de infraestructuras organizativas basadas en la creación, almacenamiento e intercambio de información, misma que será gestionada y procesada de manera fácil, eficiente y eficaz. Las Tecnologías de la Información (TI) desempeñan la mayoría de las funciones esenciales en la continuidad operativa de una empresa por lo que su futuro depende de la transformación digital y la infraestructura de TI [11].

1.3.2 Seguridad física informática

La seguridad física protege a empleados, redes, hardware, software, edificios y datos contra eventos y actividades físicas que podrían dañar gravemente o destruir una empresa, organización o agencia. Esto abarca la protección contra desastres naturales, robos o vandalismo que podrían tener acceso a datos confidenciales poniendo en riesgo la seguridad informática. Si bien la mayoría las pérdidas físicas están cubiertas por el seguro, se puede ahorrar tiempo,

dinero y recursos priorizando la seguridad física sobre la prevención de daños y protección de la información garantizando la confidencialidad, integridad y disponibilidad de cualquier tipo de datos [12].

1.3.3 Identificación biométrica

Es un sistema de validación personal basado en rasgos físicos distintivos únicos y exclusivos de cada individuo que pueden ser conductuales o fisiológicos. La medición de rasgos como las huellas dactilares, iris, rostro y retina forman parte del proceso de identificación personal. Dado que estas características sin difíciles de descifrar se convierten en una opción segura a comparación de métodos tradicionales. Este tipo de procedimiento agiliza y reduce gastos administrativos en diversos sectores, además de ser seguro resulta eficiente para su implementación en el ámbito bancario, administración pública y empresas [13].

1.3.4 Sistema de reconocimiento facial

Utiliza una imagen del rostro de una persona para identificarla o verificar su identidad. Funciona en tres pasos: detección, en la que se encuentran rostros en imágenes o vídeos mediante visión artificial. Análisis, en el que se mide la geometría facial y se reconocen puntos de referencia importantes, como la separación entre la boca, la nariz y los ojos, creando una "huella facial numérica" distintiva. Reconocimiento, en el que la huella facial se compara con otras imágenes para confirmar la identidad. Entre sus ventajas se encuentran una seguridad rápida y eficaz, una mayor precisión de reconocimiento que las técnicas convencionales y una interacción sencilla con diversas aplicaciones y dispositivos, incluidos los smartphones [14].

1.3.5 Validación de identidad personal

El proceso de validación que la información de una persona tiene como fin reflejar con precisión su identidad. El objetivo es verificar que la persona es quien dice ser mediante documentos oficiales e información biométrica. La

validación crea una correspondencia en tiempo real entre los datos y la persona, empleando funciones como la detección de vida y la biometría facial para prevenir la suplantación de identidad, proteger los procesos de alta de clientes y cumplir con estrictas normas de autenticación, especialmente en entornos digitales, a diferencia de la verificación simple, que verifica la autenticidad de un documento o información [15].

1.3.6 Supervisión y control de acceso

El control de acceso es un sistema que regula y supervisa la entrada de personas a instalaciones, asegurando que solo individuos autorizados ingresen a áreas específicas. Su implementación permite un monitoreo constante, previene intrusiones y optimiza la gestión de proveedores, contratistas y empleados en entornos comerciales. Además, el registro automatizado facilita la detección de patrones e irregularidades, contribuye al cumplimiento normativo y fortalece la confianza institucional. Al centralizar la información mediante soluciones tecnológicas, se logra un control más preciso, eficiente y seguro de los recursos y operaciones [16].

1.3.7 Gestión de talento humano

Definida como el conjunto de procesos estratégicos para atraer, seleccionar, formar, motivar y retener a los empleados, destacando su importancia como activo fundamental para el rendimiento y la competitividad organizacional. Colocando al personal como base fundamental de una empresa, controlando el tiempo y la asistencia ya que es un proceso clave para garantizar la productividad y eficiencia organizacional. Mediante sistemas especializados, es posible registrar y administrar de forma automatizada las horas de entrada, salida y permanencia del personal. Estas herramientas permiten optimizar la puntualidad, reducir el ausentismo, facilitar la gestión de nómina y asegurar un seguimiento transparente del cumplimiento laboral, integrándose al conjunto de procesos estratégicos de recursos humanos [17].

1.3.8 Control de ingreso del personal

El control de ingreso de empleados es un mecanismo clave para garantizar la seguridad de las instalaciones y la eficiencia en la gestión laboral. Su finalidad es permitir el acceso únicamente a personal autorizado, reduciendo riesgos de intrusión y protegiendo información y activos sensibles. Estos sistemas, que combinan hardware como torniquetes, cerraduras electrónicas o dispositivos biométricos con software de gestión, permiten monitorear en tiempo real, asignar permisos y generar registros precisos de entradas y salidas. Además, facilitan el control de asistencia, simplifican la nómina, reducen fraudes y respaldan el cumplimiento normativo. Su aplicación en sectores estratégicos como oficinas, industrias, hospitales y centros de datos evidencia su papel fundamental como herramienta de seguridad y eficiencia organizacional [18].

1.4 Objetivos

1.4.1 Objetivo general

Implantar un sistema de identificación biométrica para el control de ingreso del personal en las instalaciones de la coordinación zonal 3 del servicio integrado de seguridad ECU 911.

1.4.2 Objetivos específicos

- Analizar el estado actual del control de ingreso del personal en las instalaciones de la coordinación zonal 3 del servicio integrado de seguridad ECU 911.
- Investigar los requisitos técnicos y condiciones operativas del reconocimiento facial para su aplicación en el control de ingreso biométrico.

- Desarrollar un sistema de reconocimiento facial para el control de ingreso del personal en las instalaciones de la coordinación zonal 3 del servicio integrado de seguridad ECU 911.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Los materiales utilizados en la investigación para la recolección de información se detallan a continuación: Encuesta dirigida a las diferentes direcciones de la institución, entrevista hacia el director de tecnología y soporte y una ficha de observación para el control de ingreso actual.

Encuesta dirigida al personal de la coordinación zonal 3 del sistema integrado de seguridad ECU 911.

¿Considera que actualmente la institución cuenta con un sistema formal de control de ingreso del personal?

- Sí
- No

¿Qué tan eficiente considera el control manual realizado por los guardias de seguridad en el ingreso del personal?

- Muy eficiente
- Eficiente
- Poco eficiente
- Nada eficiente

¿Qué tan importante cree que es modernizar el sistema de control de ingreso del personal en la institución?

- Muy importante
- Importante
- Poco importante
- Nada importante

¿Ha tenido experiencias con sistemas de identificación biométrica (huella, iris, rostro) en otras instituciones o lugares?

- Sí, con reconocimiento facial
- Sí, con huella dactilar
- Sí, con otro tipo
- No, nunca

¿Qué nivel de confianza le genera el reconocimiento facial como método de control de ingreso?

- Muy confiable
- Confiable
- Poco confiable
- Nada confiable

¿Qué aspecto considera más importante en un sistema de control de ingreso biométrico?

- Seguridad
- Rapidez en el acceso
- Facilidad de uso
- Reducción de errores

¿Qué tan efectivo cree que sería un sistema de reconocimiento facial para mejorar el control de ingreso en la institución?

- Muy efectivo
- Efectivo
- Poco efectivo
- Nada efectivo

¿Considera que la implementación de un sistema biométrico agilizará el ingreso del personal?

- Sí, mucho

- Sí, algo
- Poco
- Nada

En caso de fallas técnicas de un sistema de reconocimiento facial, ¿qué tan necesario considera que exista un procedimiento alternativo de ingreso?

- Muy necesario
- Necesario
- Poco necesario
- Nada necesario

¿Está de acuerdo con que se implemente un sistema de reconocimiento facial para el control de ingreso en la institución?

- Muy de acuerdo
- De acuerdo
- En desacuerdo
- Muy en desacuerdo

Entrevista al director general de tecnología y soporte

Tabla 4. Formato de entrevista.

Entrevista			
Entrevistado: **Cargo:** **Fecha:**			
N°	**Pregunta**	**Respuesta**	**Observación**
1	¿Cuál es el sistema actual de control de ingreso del personal que utiliza la institución y cuáles son sus principales limitaciones?		
2	Desde la perspectiva tecnológica, ¿qué tan seguro considera el sistema de control de ingreso que se emplea actualmente?		
3	¿Qué incidentes o riesgos relacionados con el ingreso no autorizado se han identificado en la institución en los últimos años?		
4	¿Existen políticas o lineamientos institucionales que orienten la modernización de los sistemas de control de acceso?		
5	¿Qué tan viable considera la incorporación de tecnologías biométricas, como el reconocimiento facial, en comparación con otros métodos de identificación?		
6	En términos de mantenimiento y soporte, ¿qué aspectos considera más críticos al implementar un sistema de reconocimiento facial?		
7	¿Cuáles son las medidas de seguridad informática que la institución tiene implementadas para proteger los datos biométricos del personal?		
8	¿Qué procedimientos de respaldo y contingencia tiene la institución establecidos en caso de fallas del sistema biométrico?		
Conclusiones:			

Ficha de observación: Control de ingreso del personal

Tabla 5. Formato de ficha de observación.

Ficha de observación			
Datos generales			
Observador: **Fecha/Hora:** **Lugar de observación:**			
Categoría	**Pregunta de observación**	**Escala / Tipo de respuesta**	**Observaciones**
Procedimiento de ingreso	¿Existe un protocolo o control definido para el ingreso del personal?	☐ Sí ☐ No	
Registro de ingreso	¿Cómo se registra el ingreso del personal?	☐ Manual ☐ Digital ☐ No se registra	
Verificación de identidad	¿Se verifica la identidad del personal al ingresar?	☐ Siempre ☐ A veces ☐ Nunca	
Personal de control	¿Hay guardias u otro personal encargado del control de ingreso?	☐ Sí ☐ No	
Infraestructura y equipos	¿El punto de acceso cuenta con señalización y equipos en buen estado (puerta, cámara, lector, etc.)?	☐ Sí ☐ Parcialmente ☐ No	
Fluidez del ingreso	¿El ingreso se realiza de forma rápida y ordenada?	☐ Sí ☐ Parcialmente ☐ No	
Puntualidad del personal	¿El personal llega dentro del horario establecido?	☐ Sí ☐ A veces ☐ No	
Incidentes observados	¿Se observaron irregularidades o inconvenientes durante el ingreso?	☐ Sí ☐ No	(Especifique)
Conclusiones			

2.2 Métodos

Esta investigación se realizó utilizando un estudio de campo y de revisión bibliográfica-documental.

2.2.1 Modalidad de la investigación

a. Investigación de campo

La modalidad de investigación de campo se cumplió a través de la encuesta, entrevista y la ficha de observación, que se realizaron en las instalaciones de la coordinación zonal 3, lo cual permitió recopilar información relevante.

b. Investigación bibliográfica-documental

Para este proyecto de investigación fue necesario e importante la revisión literaria de artículos, trabajos y proyectos con énfasis en identificación biométrica, la modalidad bibliográfica documental sustenta con información válida y verificada los métodos y procesos alineados a los objetivos establecidos.

2.2.2 Población y muestra

La población partícipe de la presente investigación corresponde a los empleados de la coordinación zonal 3 de la provincial de Tungurahua, a continuación, se detalla el total de empleados por dirección.

Tabla 6. Población de estudio.

Población	Número	Porcentaje
Coordinador	1	0.52%
Administración financiera y administración de recursos humanos	17	8.85%
Comunicación social	1	0.52%
Estadística	1	0.52%
Operaciones	166	86.46%
Planificación y gestión estratégica	1	0.52%
Tecnología y soporte	5	2.60%
Total	192	100%

Dado que los empleados de la coordinación zonal son superiores a 100 elementos, se realizó el cálculo de muestra significativa aplicando la fórmula correspondiente para poblaciones finitas. Asegurando que el grupo de estudio sea del tamaño justo y así obtener resultados precisos y representativos.

Fórmula de muestra para población finita:

$$n = \frac{NZ^2PQ}{Ne^2 + Z^2PQ}$$

Donde:

$N = Tamaño\ de\ la\ población\ total$

$e = Error\ estándar\ (9\%\ o\ 0.09)$

$Z = Nivel\ de\ confianza\ (95\%\ lo\ que\ corresponde\ a\ 1.96)$

$P = Probabilidad\ de\ éxito\ (0.5, para\ máxima\ variabilidad)$

$Q = Probabilidad\ de\ fracaso\ (0.5, para\ máxima\ variabilidad)$

$n = Tamaño\ de\ la\ muestra$

Aplicación de la fórmula:

$$n = \frac{192 * (1.96)^2 * (0.5) * (0.5)}{192 * (0.09)^2 + (1.96)^2 * (0.5) * (0.5)} = 73.3$$

$$n = 73$$

Por lo tanto, el tamaño de muestra es de 73 personas.

2.2.3 Recolección de información

Resultados de la encuesta

Pregunta 1:

¿Considera que actualmente la institución cuenta con un sistema formal de control de ingreso del personal?

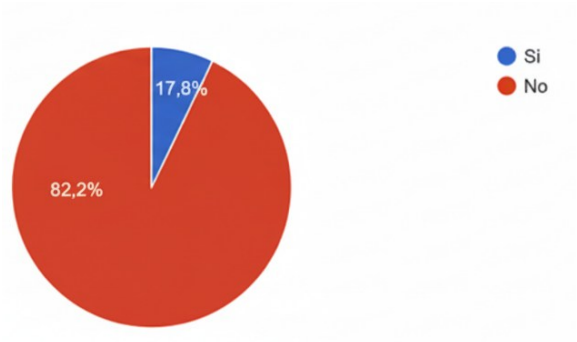


Figura 1. Resultado pregunta 1.

Análisis e interpretación de resultados

Los resultados reflejan que más del 80% percibe la ausencia de un sistema formal de control de acceso a las instalaciones, mientras que solo el 17,8% considera que sí existe uno. Estos resultados evidencian una percepción generalizada de falta de un sistema estructurado o automatizado para el registro y control de ingreso de los empleados. Los procesos manuales o informales dependientes de los guardias de seguridad o registros en papel pueden ser considerados una forma de control de ingreso, lo cual genera ineficiencias, errores o vulnerabilidades en la institución.

Pregunta 2:

¿Qué tan eficiente considera el control manual realizado por los guardias de seguridad en el ingreso del personal?

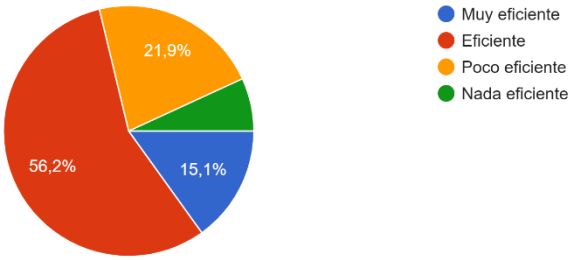


Figura 2. Resultados pregunta 2.

Análisis e interpretación de resultados

Estos resultados muestran que el 56,2% de los trabajadores encuestados consideran que el control manual realizado por los guardias de seguridad en el ingreso del personal es eficiente, mientras que un porcentaje del 21,9 lo califica como poco eficiente, un 15,1% como muy eficiente y solo un 6,8 lo percibe como nada eficiente, Esto refleja que a pesar de que la mayoría del personal reconoce cierta eficiencia en el trabajo del personal de seguridad, existe una porción significativa que logra identificar limitaciones en el método manual.

Depender en gran medida del criterio humano puede generar errores, demoras o falta de precisión en la información registrada, el sistema manual no garantiza un control óptimo ni seguro.

Pregunta 3:

¿Qué tan importante cree que es modernizar el sistema de control de ingreso del personal en la institución?

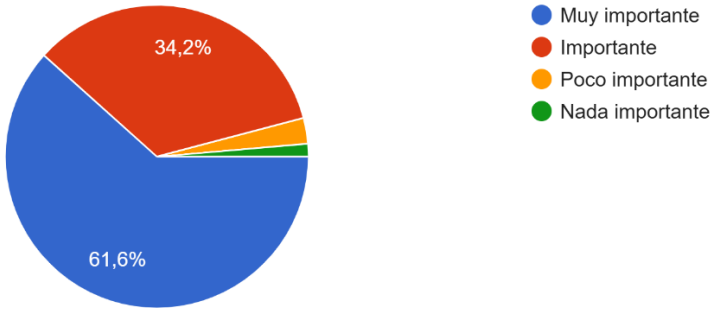


Figura 3. Resultados pregunta 3.

Análisis e interpretación de resultados

Como se muestra en la gráfica el 61,6% considera que es muy importante modernizar el sistema de control de ingreso del personal, mientras que un 34,2% lo califica como importante y solo un 2,7% cree que es poco importante y un 1,4% que no tiene importancia, por lo cual la mayor parte del personal están de acuerdo sobre la necesidad de modernizar el sistema actual, evidenciando que la mayoría tiene como prioridad institucional la actualización y modernización. Por otro lado, la minoría se mantiene en los procesos tradicionales lo cual se puede atribuir a desconocimiento de nuevas opciones o a la comodidad con métodos modernos.

Pregunta 4:

¿Ha tenido experiencias con sistemas de identificación biométrica (huella, iris, rostro) en otras instituciones o lugares?

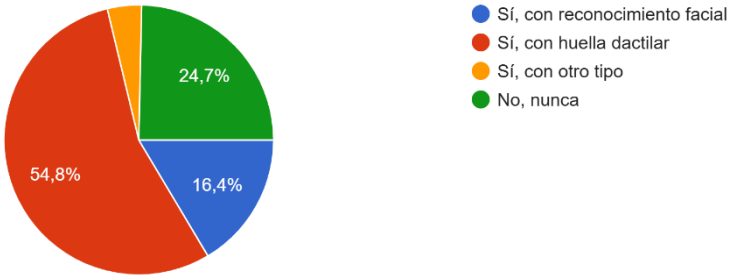


Figura 4. Resultados pregunta 4.

Análisis e interpretación de resultados

Como se puede apreciar el 54,8% de personas encuestadas indicó haber tenido experiencia con sistemas de identificación basados en huella dactilar, mientras que el 16,4% ha utilizado reconocimiento facial y el 4,1% ha tenido contacto con otro tipo de sistema. Es necesario hacer énfasis en que los resultados obtenidos muestran que el 24,7% menciona no haber tenido ninguna experiencia con algún tipo de tecnología de control de ingreso.

Más de la mitad del personal ya ha tenido interacción con mecanismos biométricos, esto refleja un nivel de familiaridad previo con este tipo de tecnologías. El uso de la huella dactilar para la identificación es el método más empleado en otros entornos institucionales pero el reconocimiento facial es un método poco implementado, indicando que es una tecnología no difundida o aplicada en el entorno laboral de los encuestados.

El porcentaje de personas sin experiencia en el uso de este tipo de tecnologías revela la necesidad de capacitaciones para asegurar la aceptación, adaptación y constante actualización del personal ante este tipo de innovaciones.

Pregunta 5:

¿Qué nivel de confianza le genera el reconocimiento facial como método de control de ingreso?

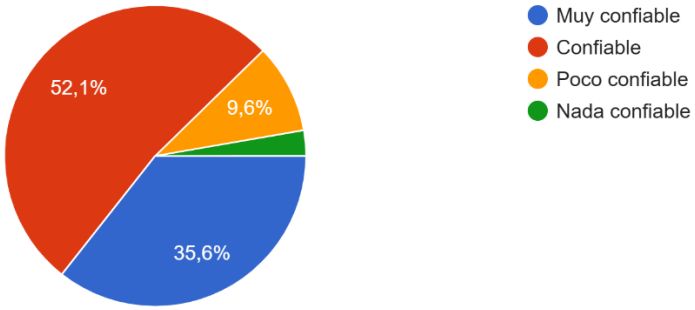


Figura 5. Resultados pregunta 5.

Análisis e interpretación de resultados

El 52,1% califica al reconocimiento fácil como un método confiable para el control de ingreso, mientras que el 35,6% considera que es muy confiable, un 9.6% lo percibe como poco confiable y solo un 2,7% cree que no es confiable en absoluto.

Estos resultados muestran una alta aceptación y confianza generalizada hacia el reconocimiento facial como herramienta tecnológica para identificación y control de acceso del personal. El personal que muestra desconfianza podría estar relacionada con falta de conocimiento técnico sobre el funcionamiento del sistema.

Pregunta 6:

¿Qué aspecto considera más importante en un sistema de control de ingreso biométrico?

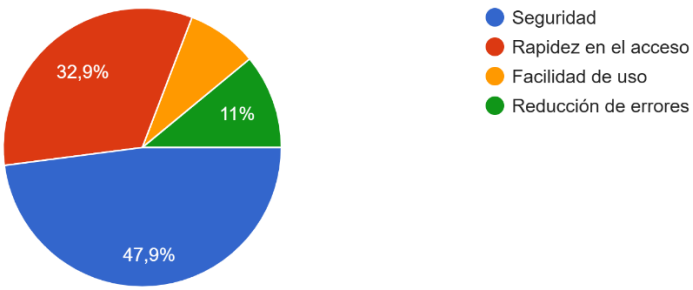


Figura 6. Resultados pregunta 6.

Análisis e interpretación de resultados

Los resultados muestran que el 47,9% considera que la seguridad es el aspecto más importante en un sistema de control de ingreso biométrico, seguida por la rapidez en el acceso con un 32,9%, el 11% valora la reducción de errores y un 8,2% destaca la facilidad de uso como el factor más importante en este tipo de tecnología.

Se puede deducir que la mayoría del personal enfatiza la seguridad y rapidez del sistema sobre otros factores operativos, la protección y confiabilidad garantiza un control seguro y preciso de la identidad de los trabajadores. La preocupación por la agilidad en los procesos de ingreso se ven reflejados por el porcentaje que muestra la encuesta en cuanto a rapidez en el acceso.

Pregunta 7:

¿Qué tan efectivo cree que sería un sistema de reconocimiento facial para mejorar el control de ingreso en la institución?

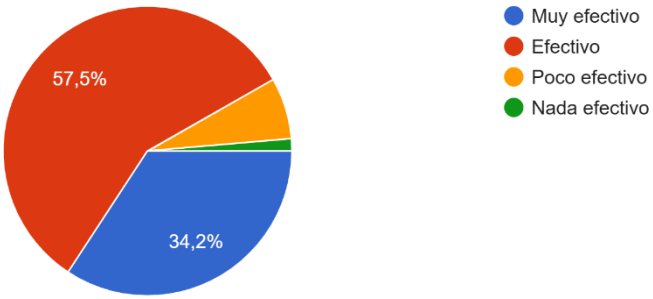


Figura 7. Resultados pregunta 7.

Análisis e interpretación de resultados

De las 73 personas encuestadas, la mayoría con un 57,5% cree que un sistema de reconocimiento facial sería efectivo en la mejora del proceso de control de ingreso a la institución, mientras que el 34,2% lo califica como muy efectivo, por otro lado, en menor medida el 6,8% lo percibe como poco efectivo y solo el 1,5% opina que no sería efectivo.

Estas cifras reflejan una amplia aceptación y confianza en la efectividad del reconocimiento facial como herramienta tecnológica para simplificar los procedimientos de entrada y salida. La baja proporción de respuestas negativas evidencian actitudes positivas hacia la adopción de tecnologías biométricas lo cual constituye una ventaja para futuras implementaciones.

Pregunta 8:

¿Considera que la implementación de un sistema biométrico agilizará el ingreso del personal?

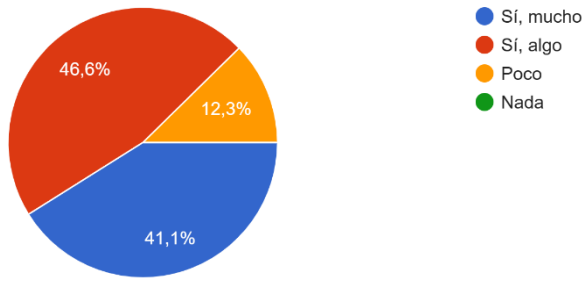


Figura 8. Resultados pregunta 8.

Análisis e interpretación de resultados

El gráfico refleja que el 46,6% contempla algo de agilidad en el ingreso de personal al implementar un sistema biométrico, mientras que el 41,1% opina que lo agilizará mucho, en menor proporción, el 12,3% considera que contribuirá poco en la mejora de la rapidez y ningún encuestado cree que no habrá efectos al optar el uso de este tipo de sistema biométrico.

Se logra una percepción positiva respecto al impacto de la incorporación de un sistema biométrico, la mayor parte del personal reconoce que este tipo de tecnología permitiría reducir los tiempos de espera y los procedimientos manuales, logrando un control más ágil.

Pregunta 9:

En caso de fallas técnicas de un sistema de reconocimiento facial, ¿qué tan necesario considera que exista un procedimiento alternativo de ingreso?

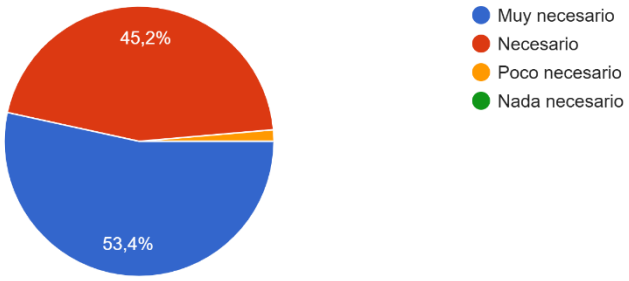


Figura 9. Resultados pregunta 9.

Análisis e interpretación de resultados

Estos resultados muestran preocupación por la continuidad operativa y confiabilidad del sistema ya que el 53,4% cree muy necesario un procedimiento alternativo de ingreso en caso de fallas técnicas del sistema de reconocimiento facial, mientras que el 45,2% lo califica como necesario, solo el 1,4% opina que sería poco necesario. El alto porcentaje de respuestas que destacan la necesidad de un método alternativo demuestra que todo sistema tiene posibilidades de fallo tecnológico y el personal es consciente de ello ya que valoran la importancia de contar con un plan de contingencia para evitar retrasos.

Pregunta 10:

¿Está de acuerdo con que se implemente un sistema de reconocimiento facial para el control de ingreso en la institución?

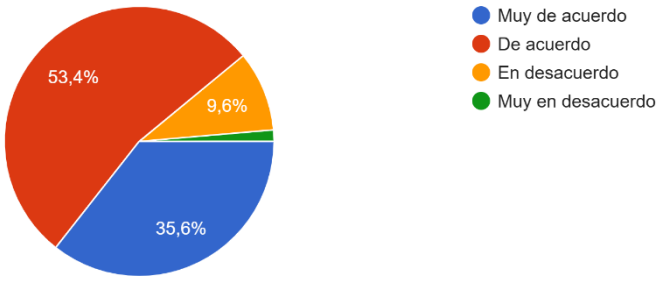


Figura 10. Resultados pregunta 10.

Análisis e interpretación de resultados

Estos resultados califican con una alta aceptación y disposición positiva del personal para la adopción de tecnologías de reconocimiento facial ya que el 53,4% manifestó estar de acuerdo con la implementación de un sistema de reconocimiento facial para el control de ingreso a la institución, mientras que el 35,6% indicó estar muy de acuerdo, en contraste con el 9,6% que expresa estar en desacuerdo y solo el 1,4% se mostró muy en desacuerdo.

La mayoría de los empleados percibe esta medida como una solución moderna, eficiente y segura que contribuirá a mejorar el control de acceso y optimizar el registro de asistencia.

Validación del instrumento

La uniformidad y fiabilidad de los datos recopilados garantizan la veracidad de los datos recopilados a través de los instrumentos, por ello se aplicó el coeficiente alfa de Cronbach. Este índice mide la consistencia interna de los ítems de un cuestionario.

La Tabla 7 define el rango de confiablidad tomando valores numéricos entre 0 y 1, en donde el valor que más se acerca a 1 será considerado el de mayor consistencia.

Tabla 7. Escala de interpretación de Cronbach.

Rango de α	**Nivel de confiabilidad**
0.90 – 1.00	Excelente
0.80 – 0.89	Buena
0.70 – 0.79	Aceptable
0.60 – 0.69	Cuestionable
<0.60	Baja

Para determinar cuál es el nivel de confianza de la herramienta utilizada, se requieren variables que de describen a continuación:

Fórmula alfa de Cronbach:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum {S_i}^2}{{S_t}^2}\right]$$

Donde:

$\alpha = Coeficiente\ de\ confiabilidad\ del\ cuestionario$

$K = Número\ de\ ítems\ del\ instrumento$

$\sum {S_i}^2 = sumatoria\ de\ las\ varianzas\ de\ los\ ítems$

${S_t}^2 = Varianza\ total\ del\ instrumento$

Aplicación de la fórmula:

$$\alpha = \frac{10}{110-1}\left[1 - \frac{1.9237}{5.5719}\right] = 0.7276$$

$$\alpha = 0.73$$

El coeficiente de Alpha de Cronbach que se obtuvo en la encuesta dirigida al personal del sistema integrado de seguridad refleja un 0.73, valor que refleja una confiabilidad aceptable.

Resultados de la entrevista

Tabla 8. Entrevista.

Entrevista			
Entrevistado: Ing. Iván Chulde **Cargo:** Director general de la dirección de tecnología y soporte **Fecha:** 09/09/2025			
N°	**Pregunta**	**Respuesta**	**Observación**
1	¿Cuál es el sistema actual de control de ingreso del personal que utiliza la institución y cuáles son sus principales limitaciones?	Actualmente la Coordinación Zonal 3 del SIS ECU 911 no posee un sistema de control de ingreso de personal a la institución. El control lo realizan los guardias de seguridad solicitando identificaciones de las personas, se utiliza la comprobación humana que es propensa a errores. Además, se cuenta con un receptor biométrico de picadas por parte de RRHH que regula el control de ingreso a jornada laboral el cual solo registra al personal perteneciente al SIS ECU 911 e instituciones articuladas, pero no a invitados.	
2	Desde la perspectiva tecnológica, ¿qué tan seguro considera el sistema de control de ingreso que se emplea actualmente?	Centrándose en el control de ingreso que se realiza mediante los guardias de seguridad, este no es seguro, debido a que el error humano en llenar bitácoras manualmente no es confiable, además del aspecto ético de las personas que llenan la información. No se tiene seguridad al momento de identificar a las personas y a la	

		vez en el registro de entrada y salida.	
3	¿Qué incidentes o riesgos relacionados con el ingreso no autorizado se han identificado en la institución en los últimos años?	En los últimos años se ha identificado que personal del ECU 911 a instituciones articuladas al mismo salen de la institución sin un justificativo lo cual ha sido comprobado mediante el sistema de CCTV interno de la institución, pero sus salidas no existen en los registros de bitácoras de los guardias de seguridad, lo que provoca inconsistencia en los datos almacenados por la parte humana. Adicionalmente cuando existe cambio de personal de guardias de seguridad no conocen al personal que labora en la institución y han permitido el ingreso sin medidas de seguridad extras.	
4	¿Existen políticas o lineamientos institucionales que orienten la modernización de los sistemas de control de acceso?	Si. Anualmente se realiza un proyecto tecnológico en cada centro de acuerdo con el PROCEDIMIENTO DE GESTIÓN DE PROYECTOS TECNOLÓGICOS documento oficial de la Institución el cual menciona que se debe identificar una mejora en la institución para realizar un proyecto. En este caso este proyecto podría considerarse para aplicar.	
5	¿Qué tan viable considera la incorporación de tecnologías biométricas, como el reconocimiento facial, en comparación con otros métodos de identificación?	Considero que es una gran innovación dentro de la institución debido a que no se ha realizado aun, siendo el reconocimiento facial una tecnología en auge actual lo que brindará a la institución de una innovación tecnológica.	
6	En términos de mantenimiento y soporte, ¿qué aspectos considera más críticos al implementar un sistema de reconocimiento facial?	Podría considerarse el apartado de software debido a la instalación de los sistemas con sus bases de datos. Adicionalmente considero que la parte electrónica sería un aspecto critico a considerar. Esto debido a la experiencia ya que el SIS ECU 911 tiene un	

		sistema biométrico de reconocimiento de huella que fue implementado más de 10 años atrás pero su sistema fue descontinuado y en muchos aspectos el hardware y software no se puede reparar o actualizar.	
7	¿Cuáles son las medidas de seguridad informática que la institución tiene implementadas para proteger los datos biométricos del personal?	Para proteger la información no solamente de los datos del personal sino también de toda la información confidencial que almacena el SIS ECU 911 tenemos políticas de seguridad informática que están aplicadas a la institución una de las cuales es la seguridad de redes a través de firewalls, el uso de software legal, capacitación del personal sobre posibles ataques cibernéticos, antivirus, etc.	
8	¿Qué procedimientos de respaldo y contingencia tiene la institución establecidos en caso de fallas del sistema biométrico?	En caso de fallo del sistema la institución tiene como respaldo el ingreso manual de los registros de ingresos. Si el sistema a implementarse fallara los guardias de seguridad tendrán la responsabilidad de volver al sistema actual de llenado manual de los ingresos a la institución.	
Conclusiones: La entrevista sintetiza que la incorporación de tecnologías biométricas, como el reconocimiento facial fortalecerá significativamente la confiabilidad y eficiencia institucional, contribuyendo a la innovación tecnológica y a la mejora continua de los procesos operativos de la institución. Además, el director general de tecnología resalta una necesidad urgente de modernización tecnológica en el proceso de control de ingreso del personal, al carecer de un mecanismo formal y autorizado, dependiendo del control manual realizado por los guardias de seguridad y de un dispositivo biométrico limitado al registro a ciertos departamentos y dejando fuera el resto del personal genera riesgo de seguridad y errores humanos que afectan la confiabilidad de los registros.			

Resultado de la ficha de observación

Tabla 9. Ficha de observación.

Ficha de observación			
Datos generales			
Observador: Karina Cunuhay - Investigador **Fecha/Hora:** 10/09/2025 -12h00 **Lugar de observación:** Garita 2 de las instalaciones del ECU 911			
Categoría	Pregunta de observación	Escala / Tipo de respuesta	Observaciones
Procedimiento de ingreso	¿Existe un protocolo o control definido para el ingreso del personal?	☒ Si ☐ No	Si, existe, pero algunos trabajadores de instituciones articuladas no registran ingresos ni salidas.
Registro de ingreso	¿Cómo se registra el ingreso del personal?	☒Manual ☐ Digital ☐ No se registra	Existe un biométrico para registro de ingresos para cierto personal, pero suele fallar por deterioro de tiempo y los guardias se encargan de llevar un registro en bitácora de algunos trabajadores.
Verificación de identidad	¿Se verifica la identidad del personal al ingresar?	☒Siempre ☐ A veces ☐ Nunca	Los guardias verifican de manera visual.
Personal de control	¿Hay guardias u otro personal encargado del control de ingreso?	☒Sí ☐ No	
Infraestructura y equipos	¿El punto de acceso cuenta con señalización y equipos en buen estado (puerta, cámara, lector, entre otros)?	☐ Sí ☒ Parcialmente ☐ No	Cuenta con señalización, los equipos otorgados por el gobierno hacen más de 10 años se encuentran obsoletos y fuera de uso.
Fluidez del ingreso	¿El ingreso se realiza de forma rápida y ordenada?	☐ Sí ☒ Parcialmente ☐ No	En horas de ingreso por jornada laboral a veces el personal no lo hace de manera ordenada.
Puntualidad del personal	¿El personal llega dentro del horario establecido?	☐Sí ☒ A veces ☐No	En el ingreso de jornada laboral las puertas permanecen abiertas hasta minutos posteriores a la hora máxima de llegada.
Incidentes observados	¿Se observaron irregularidades o	☒ Sí ☐No	A pesar de existir señalización de

	inconvenientes durante el ingreso?		ingreso y salida algunos trabajadores entran y salen por cualquier puerta.
Conclusiones: La observación realizada evidencia que, a pesar de existir un protocolo básico de control de ingreso, este presenta deficiencias en su aplicación y ejecución. El registro se realiza principalmente de manera manual, complementando por un sistema biométrico deteriorado y con fallas frecuentes, lo cual obliga al personal de seguridad a mantener bitácoras escritas que son susceptibles a errores y omisiones. La verificación visual de identidad y el uso de equipos obsoletos limitan la seguridad del proceso. Además, se observó desorden y faltas de puntualidad en los ingresos, así como incumplimiento en las rutas establecidas.			

2.2.4 Procesamiento y análisis de datos

A partir de la entrevista realizada al personal de las instalaciones de la coordinación zonal 3 del servicio integrado de seguridad ECU 911, la ficha de observación y la entrevista al director general de tecnología revelan información importante sobre los procesos de control:

- El análisis correspondiente a la pregunta 1, que obtuvo un 82.2%, evidencia que la mayoría del personal reconoce la ausencia de un sistema formal y automatizado de control de ingreso. En su lugar, depende principalmente de procedimientos manuales realizados por los guardias de seguridad, lo que genera ineficiencias, errores y vulnerabilidades que comprometen la confiabilidad y la seguridad institucional.

- De acuerdo con los resultados obtenidos en la pregunta 10, se evidencia una amplia aceptación y predisposición del personal hacia la implementación de un sistema biométrico con reconocimiento facial. El 53.4% manifestó estar de acuerdo y el 35.6% muy de acuerdo con su adopción. Estos valores reflejan que la mayoría percibe esta tecnología como una alternativa moderna, confiable y necesaria para optimizar el control de ingreso, valorando principalmente su seguridad, rapidez y eficiencia operativa.

- La entrevista confirma que el sistema con el cual se trabaja no garantiza un control seguro ni eficiente, además resalta que la vialidad técnica y estratégica de incorporar un sistema de reconocimiento facial

representa la innovación alineada con los lineamientos tecnológicos del sistema integrado de seguridad ECU 911 y subraya la importancia del mantenimiento, seguridad y olanes de contingencia del sistema para mantener su sostenibilidad.

- La ficha de observación evidenció que el control de ingreso es manual, desactualizado, poco riguroso, con fallas en equipos biométricos, desorden en los horarios de acceso y una verificación del personal visual que incita a la modernización de la infraestructura y fortalecer los protocolos de control, implementando tecnologías biométricas que garanticen un ingreso más seguro, ágil y confiable.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

El análisis de las herramientas usadas para la recolección mediante la encuesta y entrevista muestran hallazgos que se pueden visualizar en la siguiente figura.

a. Proceso tradicional de control de ingreso y salida del personal en las instalaciones de la coordinación zonal 3 del Servicio Integrado de Seguridad ECU 911.

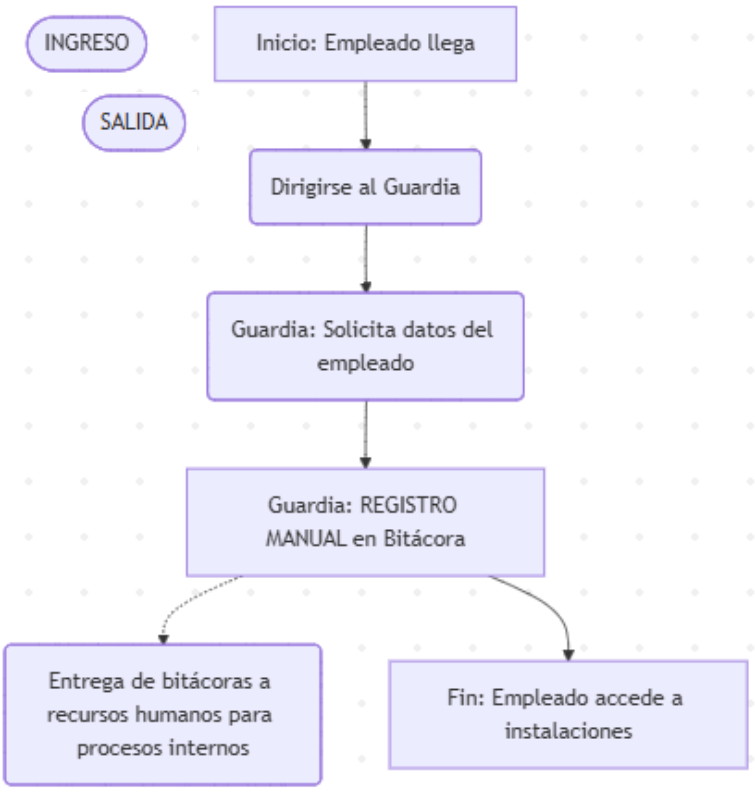


Figura 11. Diagrama de proceso tradicional de control de ingreso.

La Figura 11 muestra la manera tradicional de control de ingreso y salida del personal de las instalaciones de la coordinación zonal 3 del sistema integrado de seguridad ECU 911, en donde:

El empleado llega a la institución, luego se dirige al guardia de seguridad de turno, el cual le solicita sus datos y los registra en una bitácora de manera manual y el empleado queda registrado y pude acceder.

El procedimiento es similar a la salida del personal, sea cual sea el motivo el registro se realiza manualmente y el único encargado es el guardia de seguridad.

b. Diagrama de procesos optimizado.

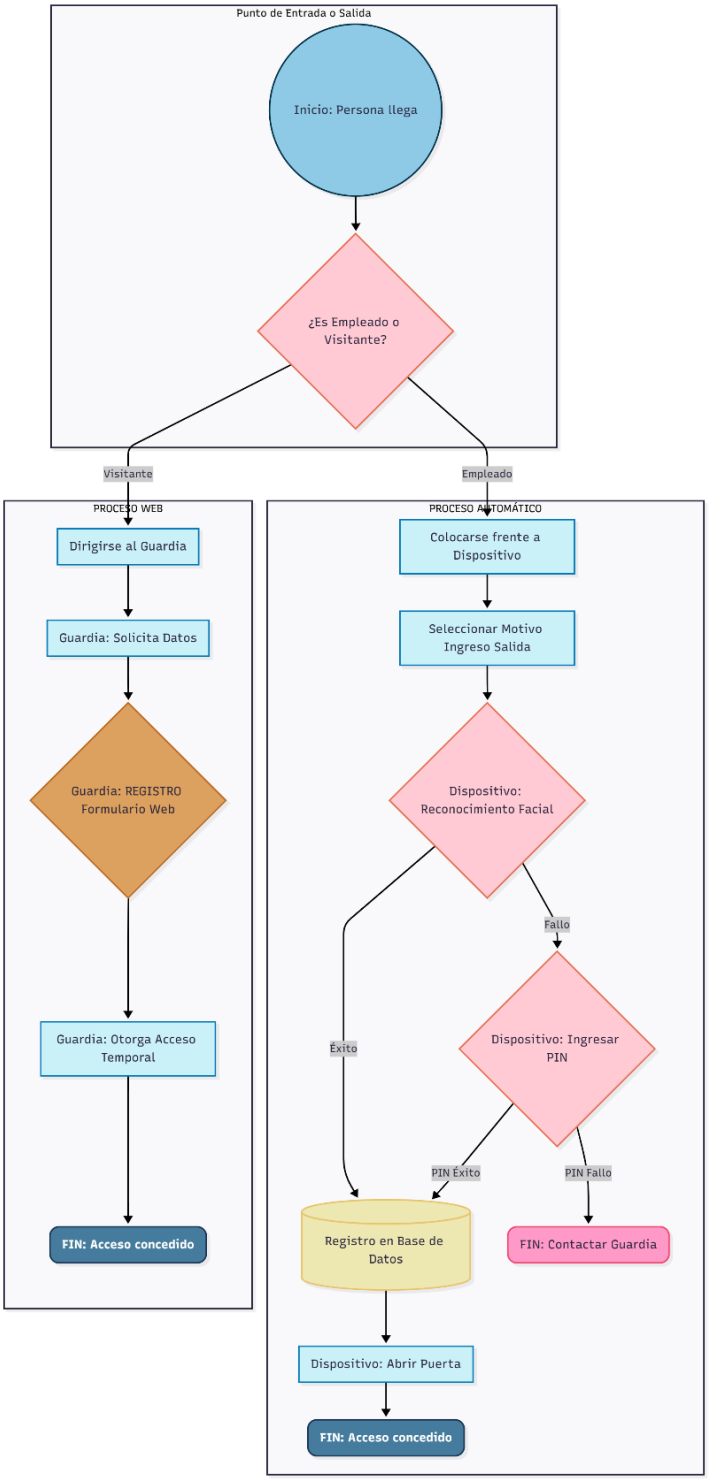


Figura 12. Diagrama de procesos optimizados.

Como muestra la Figura 12 el proceso de optimización para empleados se da en el siguiente orden a través de un dispositivo móvil:

- Acercamiento del empleado al dispositivo de acceso/salida.
- Selección de motivo de ingreso/salida.
- El dispositivo abre la cámara y el empleado clica el botón de captura.
- Si el dispositivo registra de manera exitosa se registra internamente la fecha y hora de acceso o salida.
- Si el reconocimiento facial falla después de tres intentos se activa automáticamente el registro alternativo.
- El empleado registra con su código personal (método alternativo) para completa el registro de manera correcta.

Por otro lado, en el proceso de ingreso de un visitante interviene el personal de seguridad y la autorización de un empleado superior, de la siguiente manera:

- El visitante se acerca al guardia de seguridad.
- El guardia solicita una identificación y realiza el registro de los datos, mediante un formulario web.
- Notifica a un superior para aceptar o denegar el ingreso.
- Se la orden es aceptada el visitante puede ingresar, caso contrario el visitante no accede.

3.1.1 Requisitos técnicos del reconocimiento facial

3.1.1.1 Modelos de detección y alineación del rostro

Se realizó el análisis de tres frameworks más conocidos en el área del reconocimiento facial que describen a continuación:

*a. **InSightFace***

Es una biblioteca de código abierto para Python que ofrece realizar análisis facial en 2D y 3D de forma precisa y eficiente. Su propósito es integrar en una sola herramienta los métodos más avanzados de

detección, alineación y reconocimiento facial, haciendo uso de algoritmos de aprendizaje profundo de última generación.

Su tecnología de vanguardia, versatilidad para distintos tipos de análisis facial y su reconocimiento internacional son algunas de sus principales características por las cuales se destaca, además de ser usada en áreas como la seguridad biométrica, identificación de usuarios, vigilancia inteligente y medios interactivos la posicionan como una solución integral, confiable y moderna [19].

R. Stewart, K. Kralev, y D. Stoyanov en su artículo exponen que este framework para reconocimiento facial es de código abierto y proporciona soluciones basadas en Redes Neuronales Profundas con metodología basa en Redes Neuronales Convolucionales Profundas. El flujo de trabajo de InsightFace se desglosan en: Detección y alineación facial, análisis y localización de puntos clave, extracción de características faciales y finalmente reconocimiento y verificación facial [20].

De igual manera el sistema propuesto por N. Anjeana y K. Anusudha en el cual integra el detector YOLO-V7 en el framework InsightFace para lograr originar embeddings faciales discriminativos, determinando un proceso secuencial de detección, extracción de características y verificación [21].

b. *DeepFace*

Desarrollada por Facebook AI Research, es una arquitectura de reconocimiento facial aplicada al aprendizaje profundo y redes convolucionales al análisis visual.

Su capacidad de alcanzar una precisión singular en la identificación facial superando sistemas de visión por computadora al generalizar eficazmente bajo variaciones de postura, ángulo de visión y condiciones de iluminación, han colocado a esta tecnología en una de las más usadas en los últimos años.

La secuencia de su funcionamiento se basa en: detección de rostro en una imagen. Posteriormente, realiza una alineación facial mediante

normalización tridimensional de la posición y orientación del rostro. Después la extracción de características distintivas a través de la red neuronal profunda permite obtener una representación vectorial única del rostro. Finalmente, estas características se someten a una comparación de similitud con una base de datos preexistente, culminando en una decisión de reconocimiento justificándola con el umbral de coincidencia [22].

c. FaceNet

FaceNet es un modelo de aprendizaje profundo desarrollado por Google que revolucionó el reconocimiento facial al introducir una forma más precisa y eficiente de representar los rostros, el funcionamiento se basa en la conversión de cada rostro en un vector numérico de 128 dimensiones, conocido como "embedding", el cual resume las características únicas del rostro de una persona permitiendo compara y verificar identidades faciales con gran exactitud, convirtiéndola en una herramienta fundamental en el ámbito del análisis y verificación de rostros aplicada en sistemas de seguridad y autenticación de usuarios [23].

Como explican A. K. Jain, A. A. Ross, K. Nandakumar, y T. Swearingen este sistema de vanguardia enfocado en análisis facial a gran escala verifica, agrupa y mapea las imágenes faciales hasta un espacio euclidiano compacto en el cual las distancias entre embeddings corresponden a la medida de similitud facial; por ende, una distancia más corta corresponde la similitud del rostro de la misma persona; caso contrario las caras de personas distintas tienen distancias mucho más grandes. Al igual que otros modelos, FaceNet tiene sus etapas las cuales verifican, reconocen y agrupan para encontrar personas comunes dentro de un conjunto de rostros [24].

Tabla 10. Comparación modelos de reconocimiento facial.

Aspecto	InsightFace	DeepFace	FaceNet
Embeddings	512 dimensiones discriminativas.	4096 dimensiones	128 dimensiones.
Robustez	Alta	Media-baja	Media
Dificultad de entrenamiento	Moderada	Alta	Alta
Dependencia de alineamiento	Moderada	Muy alta	Media
Aplicaciones ideales	Seguridad biométrica, autenticación, sistemas de acceso.	Análisis de atributos.	Autenticación.
Limitaciones	Requiere hardware adecuado.	Embeddings enormes.	Menos robusto en condiciones extremas.

La Tabla 10 muestra el posicionamiento de InsightFace como el modelo más adecuado para el proyecto ya que la perdida angular que usa basada en ArcFace permite una separación discriminativa entre identidades, además tiene un alto rendimiento en condiciones extremas de variación de iluminación y pose, también gracias a su detección basada en RetinaFace, alineación, puntos clave, embeddings y verificación generan un pipeline completo. Este modelo muestra una gran capacidad para tareas de vigilancia, control de acceso y seguridad biométrica ya que tiene mayor precisión que DeepFace y FaceNe por su arquitectura es moderna.

InisghtFace es reconocido y especializado en el alto rendimiento del reconocimiento facial, así como las tareas a gran escala, por otro lado DeepFace es aprovechado en el análisis multifuncional de atributos, como emociones, edad o género [20].

FaceNet es un modelo de transición que introdujo los embeddings modernos pero su entrenamiento es difícil, no usa márgenes angulares explícitos, además su precisión es menor en condiciones adversas a comparación de los modelos actuales, por otro lado, DeepFace es un

modelo histórico que usa redes neuronales clásicas, pero que se encuentra desactualizado, usa embeddings muy grandes y depende fuertemente del alineamiento 3D. Mientras que InsightFace que es un modelo de última generación que está basado en pérdidas angulares, tiene mejor estabilidad y mayor desempeño real [24].

3.1.1.2 Hardware requerido

El proceso de captura y procesamiento de imágenes para un sistema de reconocimiento facial requiere dispositivos con cámara e interfaz para control físico, ya que el sistema permite al usuario elegir el motivo de ingreso o salida. Existen opciones que se detallan a continuación:

- **Terminales de control de acceso biométrico:** Estos dispositivos combinan tecnologías biométricas y no biométricas en una sola terminal y ofrecen autenticación multifuncional segura y flexible.
  Estas terminales usan lectores biométricos que comparan los rasgos del usuario con plantillas almacenadas, si existe una coincidencia existe una respuesta positiva y el sistema desbloquea el acceso, caso contrario lo deniega [25].
- **Cámaras IP en conjunto con interfaz gráfica:** Esta solución requiere de dos componentes; la cámara que realiza el reconocimiento y una pantalla para el manejo de la interfaz del usuario. Empresas con una amplia trayectoria en la implementación de estos sistemas de control de acceso reconocen sus beneficios y compatibilidad para fortalecer la seguridad, es esencial contar con tipos de cámaras específicas, softwares de gestión aptos y su integración electrónica profesional.
- **Smartphones:** Los teléfonos celulares incluyen funciones de reconocimiento facial como parte de sus características de seguridad biométrica ya que cuentan con sensores específicos. Más allá del uso especifico en aplicaciones los smartphones cuentan con una cámara que detecta y permite verificar la identidad de una persona, además cuenta con una pantalla táctil a través de la cual se puede interactuar con el sistema de control de acceso.

La elección del teléfono celular como dispositivo biométrico ofrece ventajas prominentes frente a otras soluciones convencionales que se utiliza actualmente, el teléfono móvil integra factores de autenticación e interacción con la plataforma de registro de asistencia ofreciendo ventajas operacionales. El móvil facilita el uso de la cámara para la toma de fotografías en tiempo real y realizar la comparación con las plantillas existentes, permitiendo tener un biométrico completo en un solo dispositivo [26].

La reutilización de teléfonos móviles clasificados como residuos electrónicos aporta a la tecnología sostenible extendiendo el ciclo de vida de los dispositivos para reducir la acumulación de residuos electrónicos y contribuir con prácticas más sostenibles, los dispositivos informáticos modernos tienen una vida útil típica de 2 a 3 años antes de volverse obsoletos y desechados por múltiples razones, lo cual representa acumulación de residuos electrónicos. Los dispositivos pueden ser reutilizados con un enfoque de sostenibilidad del hardware o enfocada en el uso de sus partes y componentes; ambas formas promueven una economía circular y presentan una solución complementaria al reciclaje reduciendo la acumulación de residuos electrónicos [27].

3.1.1.3 Dispositivo biométrico

Los dispositivos biométricos son teléfonos celulares en desuso reutilizados, los cuales deben contar con características mínimas que se detallan a continuación:

- Sistema Operativo: Android
- Versión mínima de Android: 11
- Memoria RAM: 4 G
- Almacenamiento: 32 G

3.1.1.4 Servidor

- Sistema Operativo: Ubuntu 24.04.3 LTS (64-bit)
- Modelo/Fabricante: LENOVO ThinkServer RD350

- Procesador (CPU): Intel(R) Xeon(R) CPU E5-2609v3 @ 1.90GHz (6 núcleos)
- Memoria (RAM): 8192MB (8GB) RAM

3.1.1.5 Software y frameworks

El sistema de reconocimiento facial se desarrolla con software libre y open source que se detallan a continuación:

Backend:

- Python >= 3.11
- OpenCV (instalable vía pip y dependencias del sistema)
- InsightFace (instalable vía pip)
- Docker

Frontend:

- Node.js LTS (18+ o 20+)
- npm (gestor de paquetes)
- Angular CLI (instalable vía npm)
- Navegador moderno compatible con ES2020+
- Para desarrollo: ejecutar npm install y ng serve
- Para producción: ejecutar npm run build y servir los archivos estáticos

Desarrollo móvil:

- Lenguaje: Kotlin.
- Tipo de App: Android Nativo.
- Librerías y Tecnologías Clave:
    1. UI Moderna: Jetpack Compose (Material 3) + Navigation Compose.
    2. Visión: CameraX (Manejo nativo de cámara).
    3. Conectividad Híbrida:
        - Retrofit + OkHttp: Para conectar con el servidor central (Backend Web).
        - Integración IoT: Comunicación directa con microcontroladores (ESP32) vía HTTP.

4. Persistencia de Datos:

   DataStore: Para configuración crítica (Token, IP del ESP32, ID de dispositivo).

Base de Datos

- PostgreSQL >= 13
- Puerto: 5432
- Host: db (en Docker) o localhost (instalación local)
-

Conectividad y red

- Servidor backend: IP interna fija
- Dispositivos móviles: red interna

3.1.2 Requisitos operativos del reconocimiento facial

El sistema de reconocimiento facial cuenta con requisitos operativos determinados a través de la recolección de datos, los cuales se detallan a continuación:

3.1.2.1 Captura inicial de fotos – creación de plantilla

La plantilla inicial de los rostros de los usuarios se debe capturar las fotografías con un fondo neutro y luz adecuada para que el modelo pueda identificar todas las características del rostro de cada usuario, el registro debe darse con el rostro descubierto y fotos en diferentes ángulos.

3.1.2.2 Uso diario del sistema

La interacción entre el dispositivo de reconocimiento facial y los usuarios finales se da diariamente ya que el control del personal se da a cualquier hora del día, por ello el dispositivo permite elegir el motivo de ingreso o salida de la institución.

3.1.2.3 Procedimientos operativos

Un mantenimiento operativo es crucial para el correcto funcionamiento a corto y largo plazo, la revisión de cámaras, elementos electrónicos e iluminación evita fallos por factores de suciedad, manipulación o escasez de luz. Además, para mantener el nivel de precisión del sistema es necesario actualizar fotos si existen cambios físicos en los rostros de los empleados.

3.1.2.4 Seguridad operativa

El resguardo de información como el control de acceso a la base de datos, la encriptación de fotografías permite cumplir con el reglamento legal y protección de la información del personal institucional.

3.1.2.5 Protocolos de contingencia

Ante cualquier fallo o deterioro del sistema una solución ante fallos detectados y el resguardo de un Backup son cruciales para garantizar la continuidad operativa.

3.1.3 Metodologías ágiles de desarrollo

La selección de una metodología ágil adecuada permite el desarrollo del proyecto de manera flexible y alineada con sus objetivos, facilitando la adaptación a los cambios, la optimización de recursos y el aseguramiento de la calidad del producto final. En proyectos que integran sistemas de identificación biométrica, se emplean comúnmente metodologías como Cascada, Kanban y Scrum, motivo por el cual se realizó una comparativa considerando el alcance, el enfoque y los objetivos del proyecto.

La metodología Cascada sigue un enfoque secuencial, en el que cada fase debe completarse antes de avanzar a la siguiente; Kanban prioriza la visualización y gestión continua del trabajo sin plazos rígidos; mientras que Scrum estructura el desarrollo en iteraciones temporales definidas (Sprints), con roles claramente establecidos dentro del equipo.

La investigación realizada por H. Vega-Huerta, M. Pillaca Pullo, R. Velásquez Quiroz, G. L. E. Maquen-Niño, A. Camara-Figueroa, J. Pantoja-Collantes y R. Gil-Calvo [28] muestra el uso de una combinación de metodologías ágiles, tomando a Scrum y Kanban por la flexibilidad que ofrece al planificar tareas durante el desarrollo del sistema.

Estas metodologías pueden ser combinadas y adaptadas para alinearlas al ritmo de trabajo con la naturaleza del proyecto, por ello en la Tabla 11 se muestra una comparación de metodologías ágiles más usadas en proyectos similares.

Tabla 11. Comparación entre metodologías ágiles.

Criterio	**SCRUM**	**HÍBRIDO SCRUM-KANBAN**	**CASCADA**
Flujo de trabajo	Iterativo en ciclos fijos (Sprints).	Continuo y flexible.	Lineal y fijo.
Flexibilidad	Los grandes cambios se incorporan al inicio del siguiente sprint.	Permite ajustar la dirección del desarrollo o entrenamiento de modelos en momentos requeridos.	Los cambios requieren volver a fases previas provocando retraso.
Fases	El trabajo se planifica y ejecuta en sprints repetitivos que tocan todas las fases (diseño, codificación, pruebas).	Definidas por el flujo (entrenamiento, validación, despliegue), el investigador las define sin esperar que todas las tareas en una fase se completen.	No es posible avanzar a la siguiente sin terminar la actual ya que son fases secuenciales y rígidas (requisitos, diseño, implementación, prueba despliegue).
Carga administrativa	Requiere de 4 roles participantes por sprint.	Requiere mantener un tablero visual, maximizando el tiempo de desarrollo.	Requiere la entrega de gran documentación en cada fase.
Foco principal	Énfasis en el compromiso y ritmo fijo.	Énfasis en el flujo y la finalización de tareas.	Énfasis en la planificación inicial.

Una vez analizadas las características de las metodologías que se detallan en la Tabla 11 se determina que una metodología Hibrida entre Kanban y SCRUM también conocida como scrumban, es la más adecuada para este proyecto, ya que maximiza la eficiencia del desarrollo individual con supervisión académica y empresarial al combinar visibilidad continua,

flexibilidad adaptativa ante cambios de requerimientos y facilita la autogestión efectiva, Además, esta metodología permite priorizar tareas en el momento deseado y tomar tareas sin necesidad de esperar a que la anterior se finalice, las reuniones son mínimas y efectivas ya que se planifican los próximos pasos, se informa lo realizado y se realiza un análisis en retrospectiva de la semana de desarrollo tanto académica como empresarialmente.

3.2 Desarrollo de la propuesta

3.3 Aplicación de la metodología de trabajo

Para el desarrollo del proyecto se examinaron y definieron las fases de la metodología Scrumban, que se ha adaptado para el enfoque en este proyecto de identificación biométrica con el fin de cumplir la propuesta. Las fases se describen en la Figura 13.

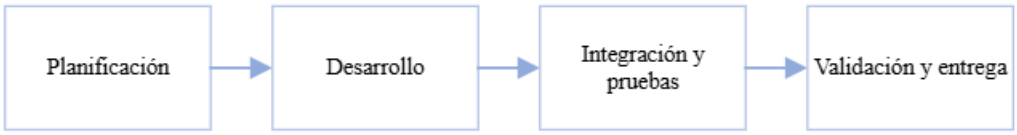


Figura 13. Fases de la metodología hibrida Kanban – Scrum.

3.3.1 Planificación

a) Especificación de los grupos de interés

Las personas involucradas en el proyecto fueron:

- **Desarrollador**
  Encargado de la creación, codificación y configuración del sistema biométrico, así como la estructuración de la funcionalidad técnica y la integración del hardware con la base de datos y el cumplimiento de los requerimientos establecidos.

- **Personal**

  Son los usuarios finales directos del sistema; los empleados de la Coordinación Zonal 3 del ECU 911, encargados de experimentar la experiencia de usuario, la facilidad y rapidez de uso para el registro de ingreso y salida del sistema.

- **Director de tecnología y soporte**

  Responsable ejecutivo del área que se encarga de la viabilidad estratégica, seguridad lógica y física del sistema, supervisión de la infraestructura y cumplimiento normativo, además es el único personal autorizado para dar información que el desarrollador necesita.

b) Recolección de requisitos iniciales

Mediante el análisis de las entrevistas realizadas y de la información recopilada en las fichas de observación, se logró establecer las características fundamentales y adicionales requeridas para crear el sistema de control de ingreso del personal basado en identificación facial.

c) Requisitos funcionales

Tabla 12. Requerimientos funcionales.

Código	Requerimiento	Descripción
RF1	Registro biométrico	El sistema debe proporcionar una funcionalidad en el módulo web administrativo que permita al personal autorizado registrar la plantilla facial biométrica inicial de un nuevo empleado.
RF2	Identificación y verificación	El sistema debe ser capaz de capturar, comparar e identificar al empleado en tiempo real utilizando el modelo InsightFace al escanear su rostro con el smartphone.
RF3	Control de acceso	El sistema otorga o deniega el ingreso a las instalaciones tras una identificación biométrica fallida o exitosa.
RF4	Selección de motivo de ingreso	El móvil debe presentar una interfaz donde el empleado pueda seleccionar la razón de ingreso o salida.
RF5	Registro de transacciones	El sistema debe almacenar de manera segura cada transacción de ingreso o egreso.
RF6	Gestión administrativa del personal	El módulo web debe permitir al personal administrativo consultar, añadir,

		modificar y dar de baja a los empleados y sus plantillas biométricas.
RF7	Generación de reportes	El módulo administrativo debe generar reportes detallados con filtros por fecha y empleado.

d) Requisitos no funcionales

Tabla 13. Requerimientos no funcionales.

Código	Requerimiento	Descripción
RNF1	Protección de datos biométricos	El sistema debe garantizar que las plantillas faciales almacenadas estén cifradas para cumplir con la legislación de datos y prevenir fuga de información sensible.
RNF2	Detección de Spoofing	El sistema debe distinguir un rostro real de una foto o video.
RNF3	Tiempo de respuesta	El proceso de escaneo, identificación y respuesta de acceso debe ser rápido para evitar la formación de filas y frustración del personal durante las horas pico.
RNF4	Precisión del modelo	El sistema debe mostrar un alto porcentaje de acierto y bajo porcentaje de errores de falsa aceptación o rechazo.
RNF5	Compatibilidad de hardware	La compatibilidad total y el rendimiento del modelo con los dispositivos elegidos.

e) Definición y alcance del sistema

Para definir un alcance del proyecto es necesario conocer sus limitaciones:

Limitaciones:

- El sistema de reconocimiento facial será única y exclusivamente para el control y registro de ingreso y salida de los empleados de la coordinación zonal 3 del sistema integrado de seguridad ECU 911, aquellas personas ajenas al establecimiento son registradas por el personal de seguridad en el módulo web correspondiente.
- El dispositivo para el reconocimiento facial es un smartphone, el mismo que es de uso exclusivo para este proceso, ya que se encuentra en modo quiosco.
- La aplicación está disponible solo para dispositivos con sistema operativo Android 10 o superior.

Establecimiento de categoría

- El sistema de reconocimiento facial utiliza características únicas del rostro para asegurar que solo la persona indicada pueda registrar su ingreso o egreso.
- Emplea modelos con un alto grado de fiabilidad, haciéndolo superior a tarjetas o contraseñas.
- Provee una solución para el control de horario y autorización de la recolección de datos de asistencia del personal.

Establecimiento del proyecto

Herramientas usadas para el sistema de reconocimiento facial:

- **InsightFace:** Biblioteca de análisis profundo de rostros en 2D y 3D de código abierto para la detección, alineación y reconocimiento de rostros con alta precisión.
- **Visual Studio Code:** Editor de código gratuito para el desarrollo del sistema.
- **Python:** Lenguaje de programación de código abierto versátil para la creación de API's.
- **Angular:** Framework de desarrollo web que proporciona herramientas para construir aplicaciones web de manera eficiente.
- **PostgreSQL:** Gestor de base de datos relacionales, gratuito, escalable y adecuada para manejar grandes volúmenes de datos y usuarios simultáneos.
- **Docker:** Plataforma de código abierto para crear contenedores y ejecutar aplicaciones de manera eficiente.
- **Kotlin:** Lenguaje específico para desarrollo de aplicaciones para sistema operativo Android.
- **Linux Server:** Ordenador con sistema operativo de código abierto diseñado para almacenar y distribuir servicios a través de la red.

f) Definición de las fases

El proyecto se estructura en iteraciones establecidas en las diferentes fases de la metodología delimitada, el cual permitió avanzar y detectar fallos, así como áreas de progreso adecuadas, en la Tabla 14 se muestra la estructura general del proyecto:

Tabla 14. Fases del proyecto.

Fase	Iteración	Descripción
Planificación	Iteración 0	Identificación del proceso inicial de control de ingreso y salida del personal a través de la recolección de datos.
	Iteración 1	Especificación de los grupos de interés.
	Iteración 2	Definición de requerimientos funcionales y no funcionales.
	Iteración 3	Establecer las fases del proyecto.
Desarrollo	Iteración 4	Diseño de la arquitectura del sistema.
	Iteración 5	Fases del reconocimiento facial en InsightFace.
	Iteración 6	Diseño de la base de datos.
	Iteración 7	Prototipo pantallas del dispositivo.
	Iteración 8	Prototipo pantallas del servicio web.
	Iteración 9	Diagramas de casos de uso.
Integración y pruebas	Iteración 10	Codificación
	Iteración 11	Integración dispositivo móvil
	Iteración 12	Registro nuevo empleado
	Iteración 13	Verificación
Validación y entrega	Iteración 14	Precisión y tasa de error
	Iteración 15	Entrega

3.3.2 Desarrollo

a) Diseño de la arquitectura del sistema

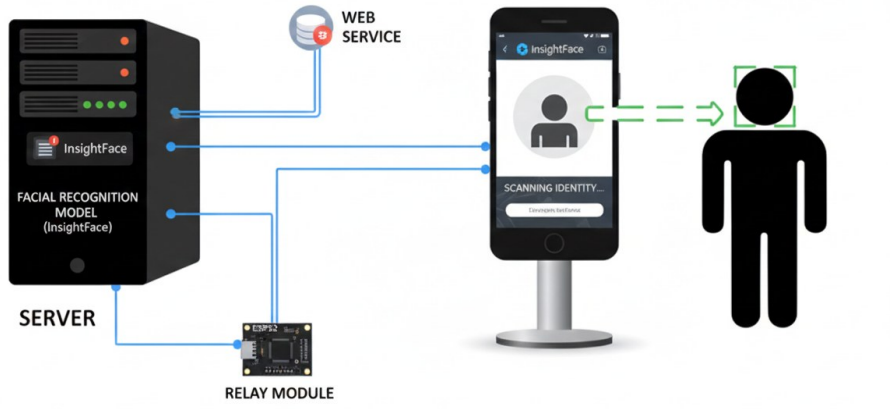


Figura 14. Arquitectura del sistema de reconocimiento facial.

El diseño del sistema que muestra la Figura 14 corresponde a un patrón cliente-servidor, con una variación de arquitectura distribuida por la implementación de diversos componentes. El patrón define roles en el sistema en donde:

El servidor es el componente central que almacena el modelo de reconocimiento facial y lo proporciona a los clientes, también maloja el servicio web para la comunicación con el cliente móvil.

El Cliente corresponde al dispositivo móvil que ejecuta la aplicación de reconocimiento facial y es el punto en donde se escanea la identidad de la persona y se comunica con el servidor para obtener el resultado de la verificación.

Los componentes adicionales pertenecen a una arquitectura distribuida ya que contribuye a la integración de los servicios; el módulo ESP32 en conjunto con el relé reciben la señal de control del servidor de acceso concedido o denegado y realiza una acción física de abrir la puerta.

b) Fases del reconocimiento facial en InisghtFace

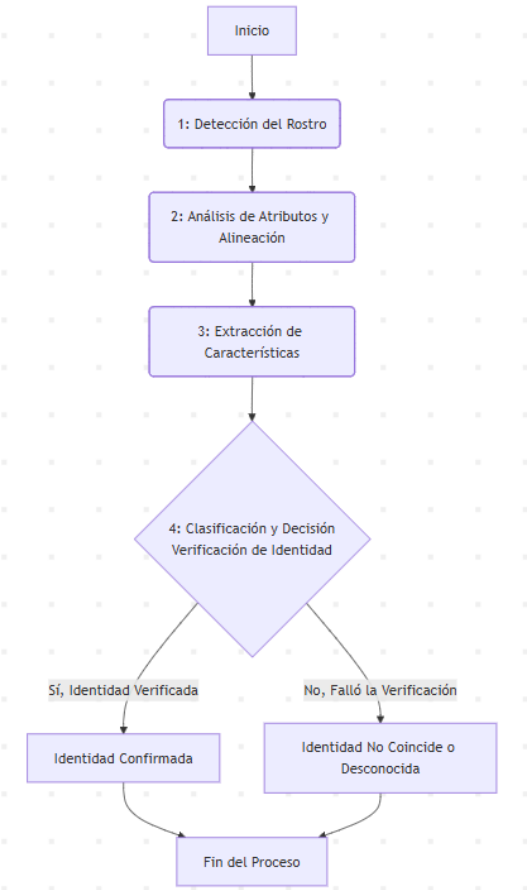


Figura 15. Diagrama de flujo del reconocimiento facial.

El proceso de reconocimiento facial se muestra en la Figura 15, en donde el dispositivo identifica la existencia de un rostro, lo escanea y localiza su posición aislándolo, después lo normaliza para que identifique las características claves del rostro como ojos, nariz y boca los cuales InsightFace realiza una transformación geométrica y genera un vector numérico de alta dimensión correspondientes a las características únicas de la persona, Finalmente la decisión depende de la distancia entre vectores, en donde se compara embeddings nuevos con las plantillas existentes y se confirma la identidad o se deniega.

1. **Detección del rostro**

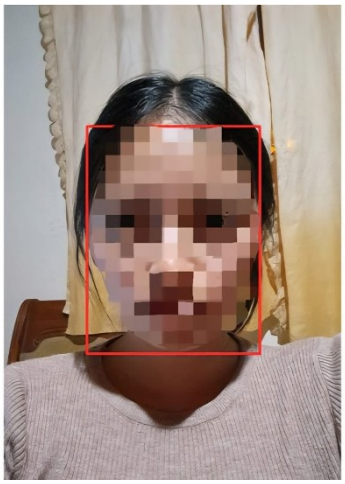


Figura 16. Fase1: Detección facial.

En la Figura 16 se evidencia la primera fase del reconocimiento facial con el modelo InsightFace en cual escanea la imagen y localiza los rostros presentes y dibuja un recuadro delimitando la cara detectada.

2. **Análisis de atributos faciales y alineación del rostro**



Figura 17. Fase 2: Análisis de atributos.

Una vez detectado el rostro se alinea y se realiza un análisis de atributos como tarea complementaria ya que el modelo se centra en identificar quien es la persona que intenta identificarse.

3. Extracción de Características (*Embedding)*

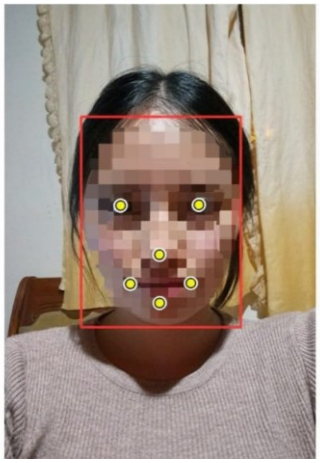


Figura 18. Fase 3: Extracción de características.

En la fase 3 el modelo identifica puntos de referencia faciales enfocados en los ojos, nariz y boca como se puede observar en la Figura 18 para transformarla geométricamente y que los ojos y boca se posicionen de manera consistente sin importar la pose o ángulo de la cabeza.

Ya alineado el rostro, la red neuronal con la cual trabaja el modelo la transforma en un vector numérico de alta dimensión conocido como embeddings.

El modelo está entrenado para garantizar que los embeddings de la misma persona estén más cerca del espacio vectorial y de quienes son diferentes personas se encuentren lejos.

4. Clasificación y Decisión



Figura 19. Fase 4: Verificación.

En la última fase de clasificación y decisión se procede a compararlo con la base de datos que contiene los rostros conocidos, se calcula la distancia coseno entre la cara escaneada y todos los embeddings almacenados. Se establece un umbral de similitud, se determina la coincidencia. Y se clasifica como persona conocida o desconocida. Las verificaciones de varias pruebas se pueden identificar en la fase de validación y entrega.

c) Diseño de la base de datos

La Figura 20 muestra el modelo entidad-relación de la base de datos diseñada para el sistema de identificación biométrica para el control de acceso.

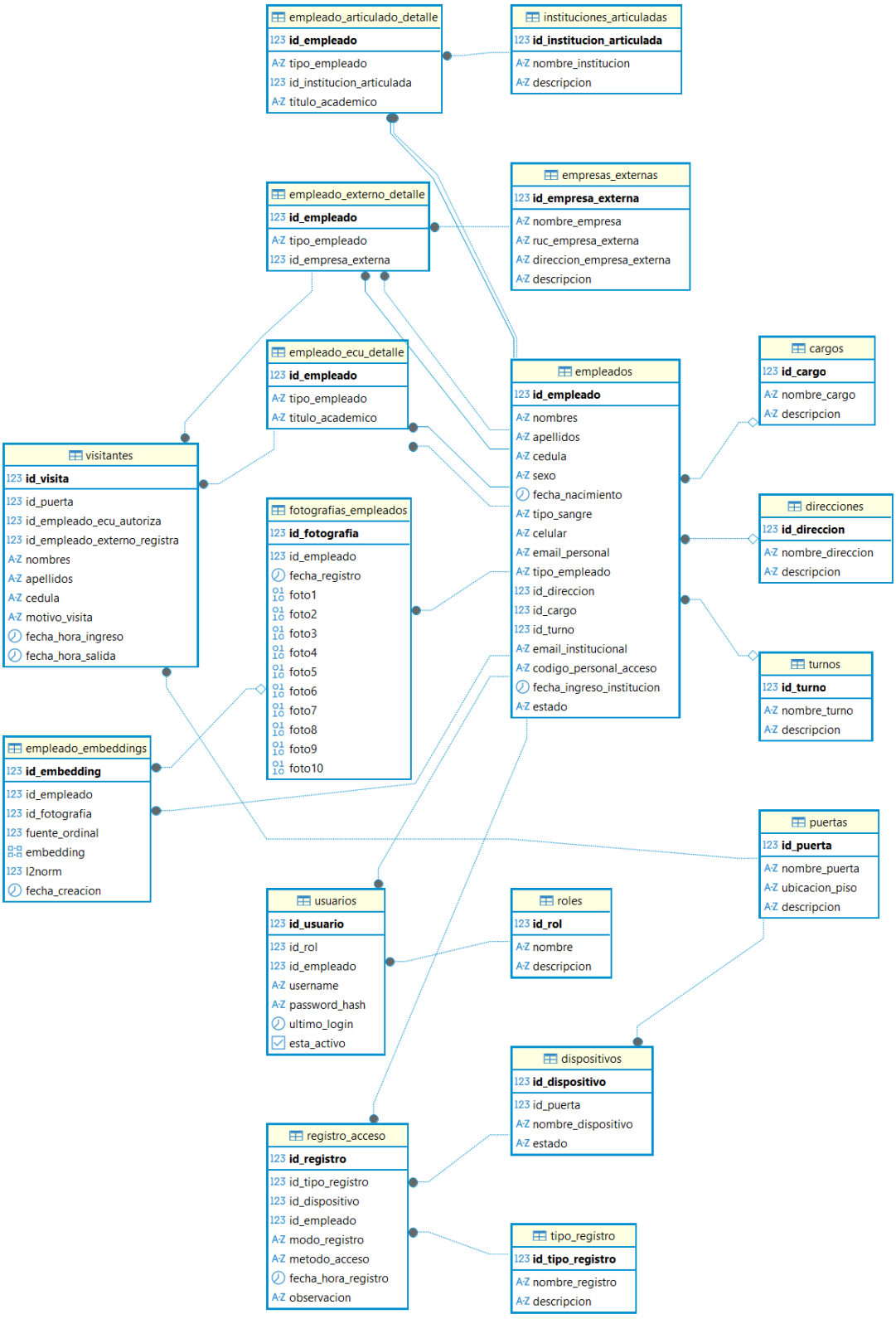


Figura 20. Diagrama entidad - relación de la base de datos.

d) Prototipo pantallas del dispositivo

Se desarrollaron prototipos basados en la interacción que tendrá el usuario con el móvil que servirá como dispositivo de registro de asistencia a través del reconocimiento facial.

Inicio de sesión

La Figura 21 muestra el prototipo de pantalla de inicio de sesión única y exclusivamente para el administrador encargado del dispositivo de reconocimiento facial. Los datos ingresados deben ser validados para un acceso seguro y correcto.

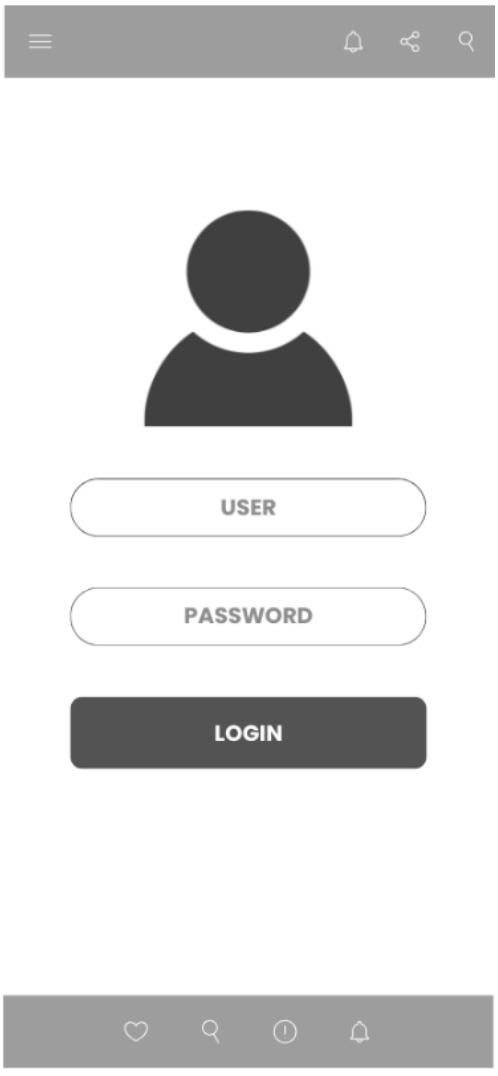


Figura 21. Prototipo de inicio de sesión móvil.

Modo de uso

La pantalla que muestra la Figura 22 corresponde a la selección de modo de uso del dispositivo, el modo “Ingreso” o “Salida” determina el tipo de registro que se realizará y el lugar de posicionamiento del dispositivo.



Figura 22. Prototipo de modo de uso.

Motivo

La Figura 23 muestra el prototipo de pantalla en el cual el usuario elige el motivo de ingreso o salida a la institución, se puede visualizar que esta pantalla cuanta con un texto que muestra la fecha y hora exacta con la cual se registrará su ingreso o salida.



Figura 23. Motivo de registro.

Verificación

Se realiza el escaneo de rostro y verificación facial mediante el uso de la cámara frontal como se muestra en el prototipo de la Figura 24, también cuenta con un botón de registro mediante un PIN personal en caso de que el primer método resulte fallido.

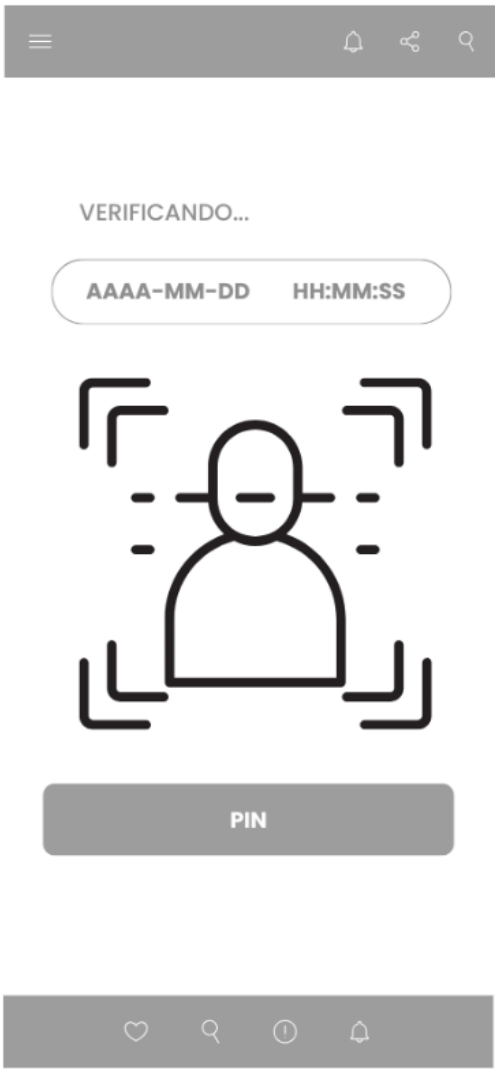


Figura 24. Escaneo y verificación.

Registro por PIN

El método alternativo en caso de falla del reconocimiento facial se habilita únicamente si el primero falla y se muestra en la Figura 25 el prototipo de uso de la clave personal para el registro de ingreso o salida.



Figura 25. Registro mediante PIN.

e) Prototipo pantallas del servicio web

Los prototipos del servicio web se desarrollaron para los usuarios administrativos, recursos humanos y guardias de seguridad. A continuación, se muestran las pantallas correspondientes:

Inicio de sesión

La Figura 26 muestra el inicio de sesión en el servicio web, el acceso se da a través del usuario y contraseña correctos.



Figura 26. Prototipo web de inicio de sesión.

Panel dashboard: Permite visualizar de manera dinámica los registros de ingreso/salida diarios, semanales y mensuales, permitiendo obtener un descargable para usos posteriores como muestra la Figura 27.

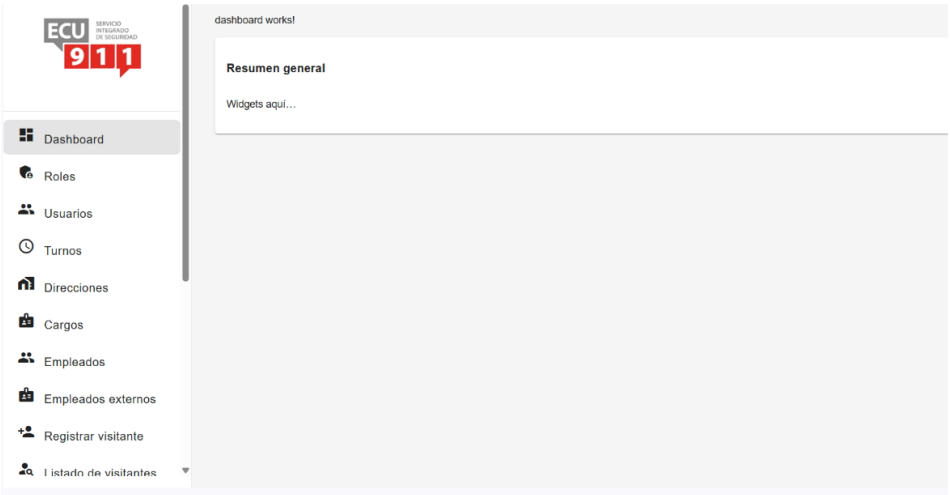


Figura 27. Prototipo web, panel dashboard – Administrador.

Módulo de usuarios: La Figura 28 refleja como el administrador puede listar, editar y crear usuarios que tendrán acceso al sistema web por los roles definidos.

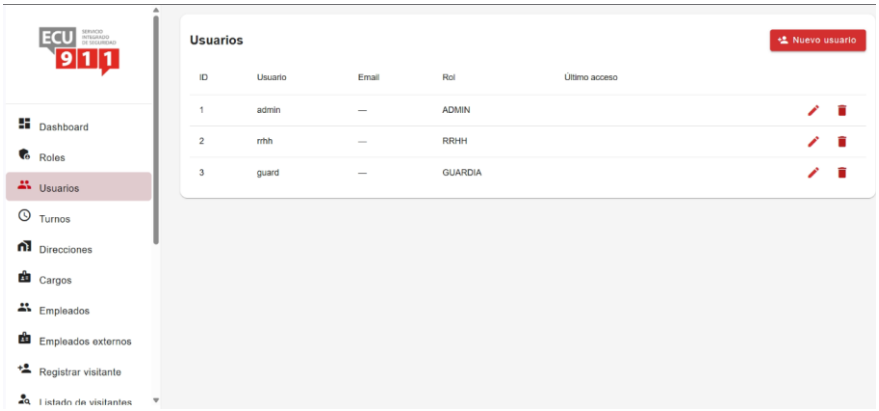


Figura 28. Prototipo módulo web usuarios – Administrador.

Modulo empleados: Presenta el listado de los empleados pertenecientes a la coordinación zonal 3 del SIS ECU911, permitiendo agregar, editar y desactivar a sus participantes como se muestra en la Figura 29.

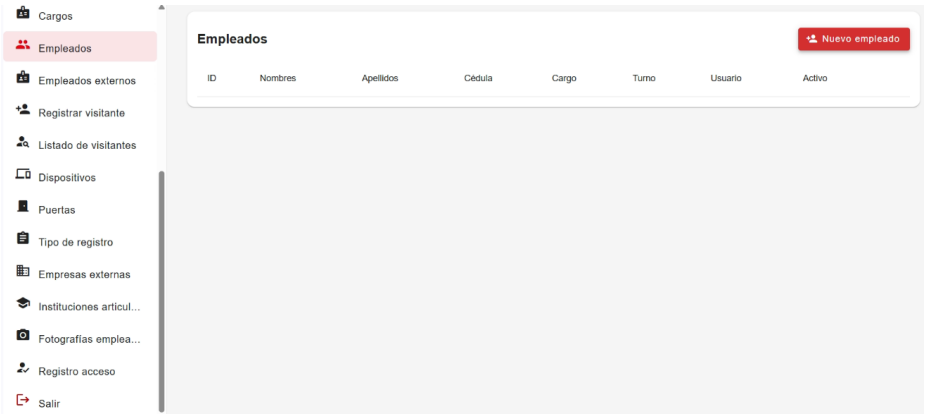


Figura 29. Prototipo módulo web empleados – Administrador.

Ventana creación empleado: La Figura 30 muestra los campos requeridos para la creación de un nuevo empleado interno especificados por la infraestructura interna de la coordinación zonal 3.

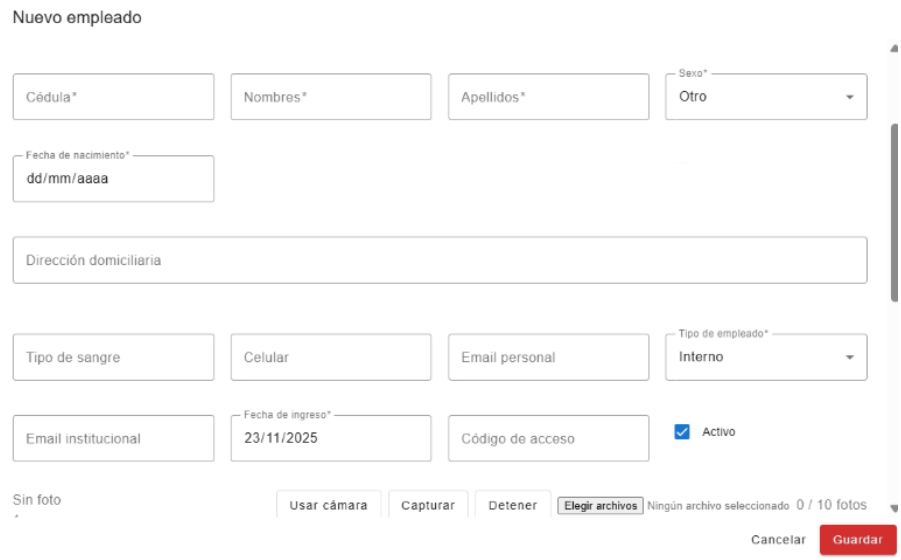


Figura 30. Prototipo ventana creación empleado – Administrador.

Ventana creación empleado externo: La Figura 31 muestra la solicitud de datos de empleados externos según la estructura organizacional del personal del SIS ECU 911.

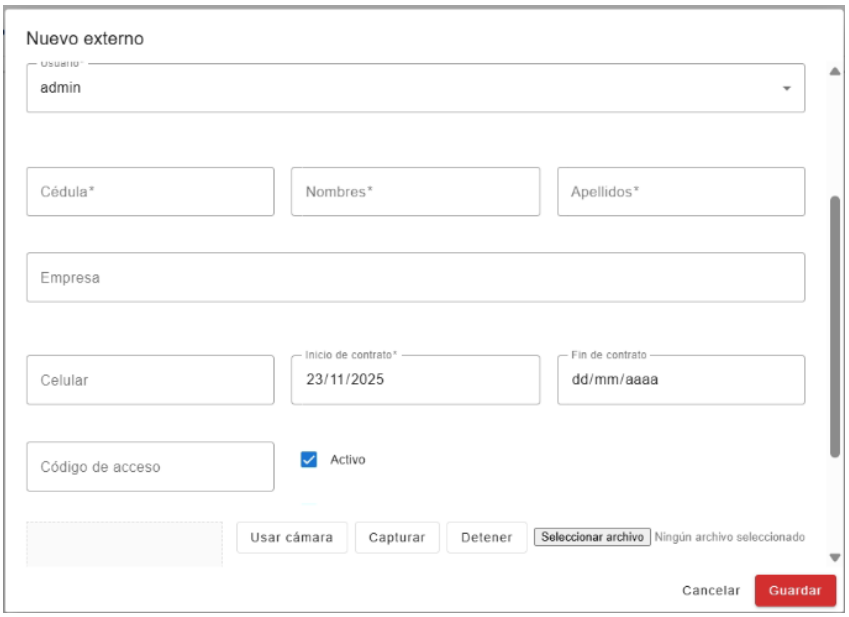


Figura 31. Prototipo ventana creación empleado externo – Administrador.

Página de usuarios de recursos humanos: Muestra los gráficos dinámicos que representan los registros de ingreso/salida, además permite la descarga de estos resultados para usos internos de esta área como se muestra en la Figura 32.

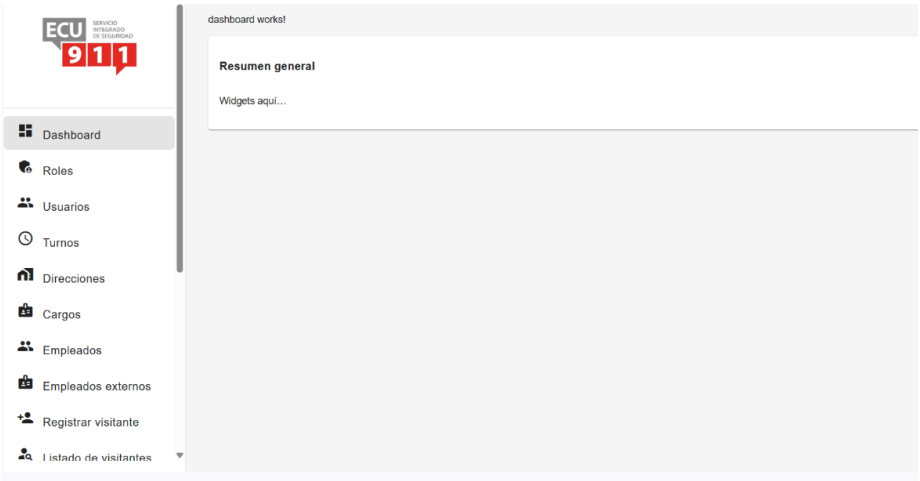


Figura 32. Prototipo página de usuarios de recursos humanos.

Página de usuarios de guardias: Permite al personal de seguridad registrar a los visitantes, como refleja la Figura 33. en donde se ingresan datos personales del visitante, el guardia de seguridad que dio acceso y el empleado superior que autoriza posterior a la notificación permitiendo o denegando el acceso.

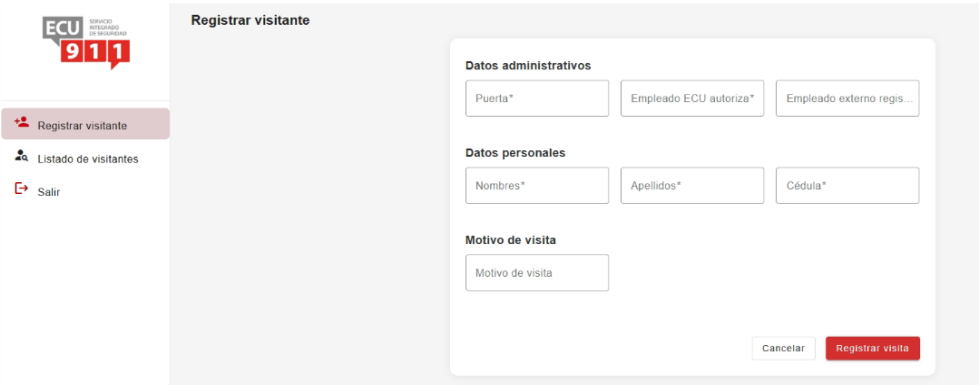


Figura 33. Prototipo formulario web – Guardias.

f) Diagramas de casos de uso

La Figura 34 muestra la interacción que tiene el usuario administrador con el sistema, el servicio web le permite creación, edición y eliminación lógica de todas las tablas que contienen la base de datos.

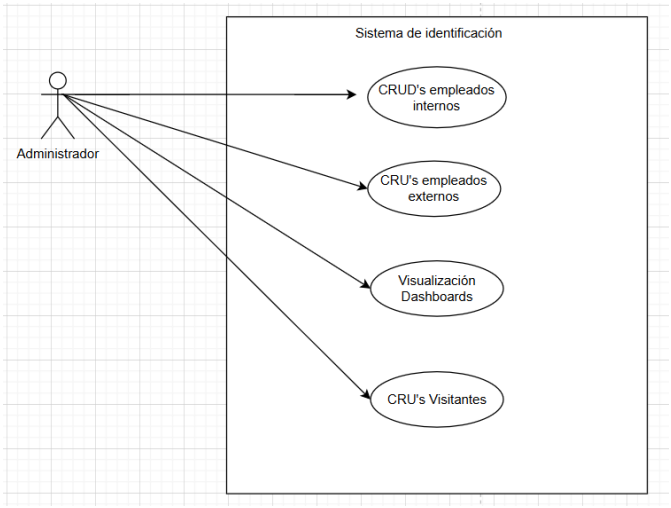


Figura 34. Diagrama de caso de uso de administradores.

El servicio web registros y visualizaciones de visitantes para guardias de seguridad y visualizaciones de acceso o salida para recursos humanos, como se evidencia en la Figura 34.

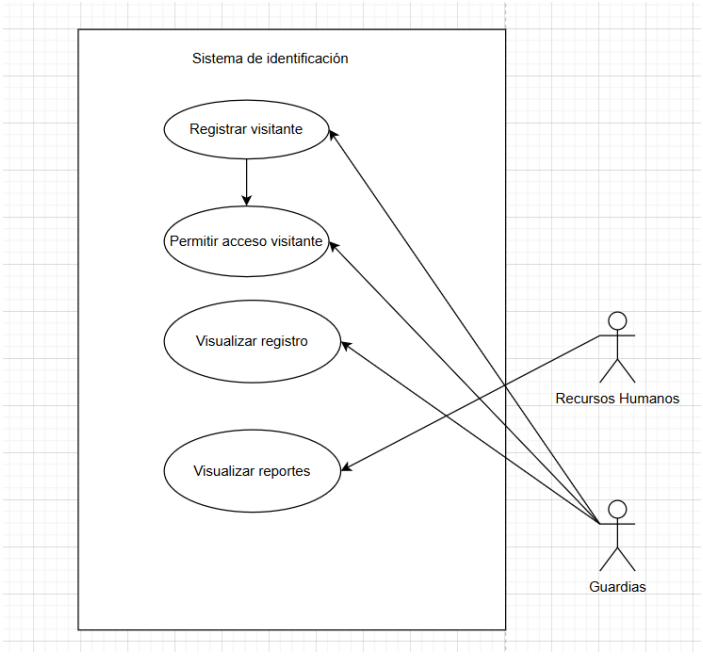


Figura 35. Diagrama de caso de uso de recursos humanos y guardias.

La Figura 36 refleja el uso del dispositivo biométrico por parte de los empleados.

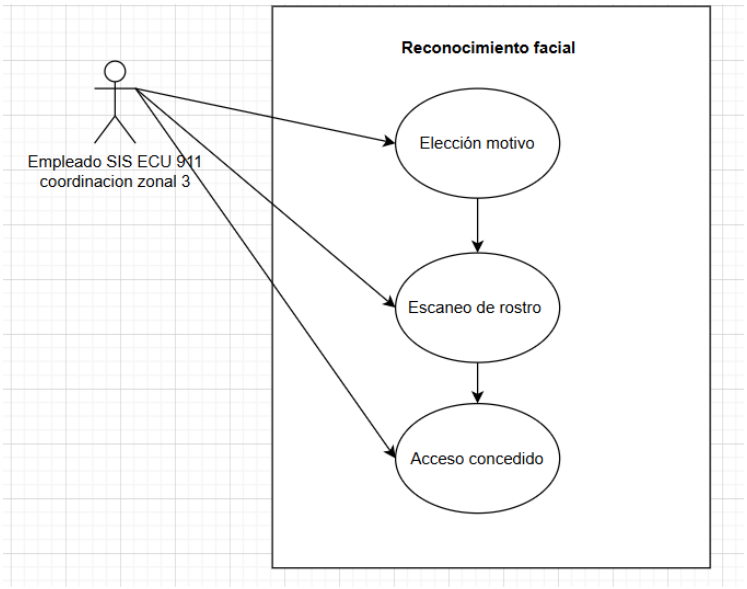


Figura 36. Diagrama de caso de uso de acceso a las instalaciones–empleados.

g) Codificación

Procesamiento del framework InsightFace.

Se verifica si la librería InsightFace se encuentra instalada y se importan las herramientas necesarias, si no está instalada se maneja la excepción y muestra un mensaje de advertencia, como muestra el código de la Figura 37.

```
try:
    import insightface
    import cv2
    from insightface.utils import face_align
    INSIGHTFACE_AVAILABLE = True
except ImportError as e:
    INSIGHTFACE_AVAILABLE = False
    logging.warning(f"InsightFace not available: {e}")
    try:
        import traceback
        tb = traceback.format_exc()
        logging.warning(tb)
        print(tb)
```

Figura 37. Verificación de instalación de InsightFace.

El código de la Figura 38 muestra la inicialización del detector y extracción de características faciales y lo configura para que sea ligero y compatible al cargar los módulos de detección y reconocimiento.

```
try:
        os.environ['INSIGHTFACE_ONNX_PROVIDERS'] = 'CPUExecutionProvider'

        self.model = insightface.app.FaceAnalysis(
            providers=['CPUExecutionProvider'],
            allowed_modules=['detection', 'recognition']
        )
```

Figura 38. Inicialización del detector y extractor de características faciales.

La Figura 39 muestra las líneas de código encargadas de la detección facial y preparación del vector de características del rostro para su uso en verificación o identificación.

```
det_score = float(getattr(face, 'det_score', 0.0))
            if det_score < self.det_thresh:
                logger.info(f"Confianza de detección baja: {det_score:.3f} < {self.det_thresh}")
                return None

            # Embedding base (InsightFace ya alinea internamente antes de reconocimiento)
            emb = face.normed_embedding.astype(np.float32)
```

Figura 39. Detección facial y preparación del vector.

Finalmente, la Figura 40 el código calcula las posibles coincidencias, identifica la más posible a ser correcta y decide si es la mejor coincidencia.

```
try:
            similarities = [self.cosine_similarity(probe_embedding, emb) for emb in gallery_embeddings]
            logger.info(f"Similitudes calculadas: {similarities}")
            best_idx = int(np.argmax(similarities))
            best_score = similarities[best_idx]
            logger.info(f"Mejor score: {best_score} (umbral: {threshold})")
            if best_score >= threshold:
                logger.info(f"Match encontrado en indice {best_idx} con score {best_score}")
                return best_idx, best_score
            logger.info(f"No se alcanzó el umbral de m
```

Figura 40. Cálculo de coincidencias.

- ***Conexión a la base de datos.***

  La configuración de la conexión a la base de datos se evidencia en el código que contiene la Figura 41.



Figura 41. Conexión PostgreSQL.

El análisis de la imagen y creación de la huella digital facial que persiste en la base de datos se detalla en el código de la Figura 42.



Figura 42. Guardado de embeddings en la base de datos.

- ***Dispositivo de biometría***

  Modulo ESP32 - relé:

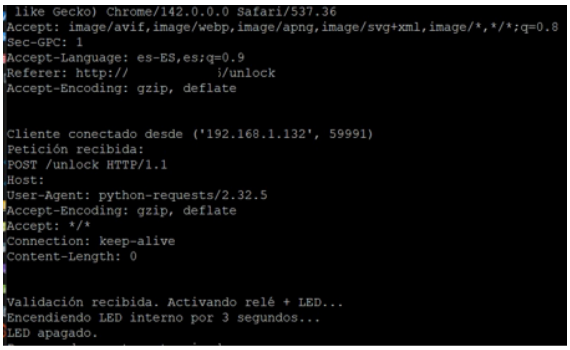


Figura 43. Validación ESP32.

La Figura 43 muestra la recepción de una verificación acertada y envía una señal al relé activándolo y haciendo apertura de la puerta para el ingreso o salida del empleado reconocido.

3.3.3 Integración y pruebas

Integración dispositivo móvil

Para una adecuada verificación del sistema del reconocimiento facial se realizaron pruebas de integración que se detallan a continuación:

El dispositivo permite la selección del modo de uso (Entrada/Salida) como muestra la Figura 44.

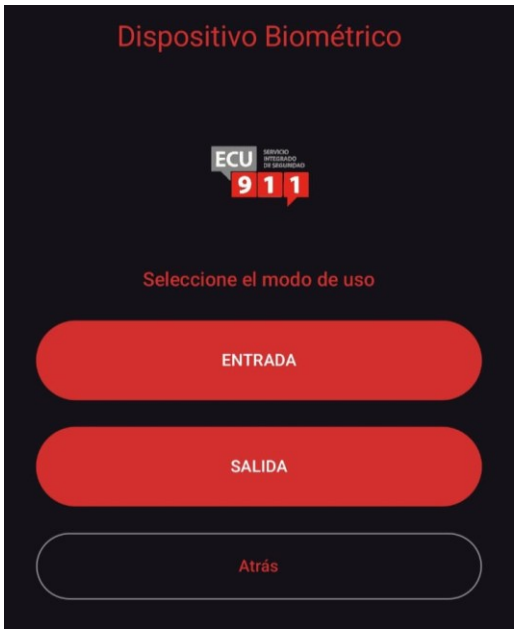


Figura 44. Pantalla modo de uso.

Con el modo seleccionado se muestra la pantalla de elección de motivo de ingreso o salida, la pantalla muestra la fecha y hora real que se registra la acción como muestra la Figura 45.

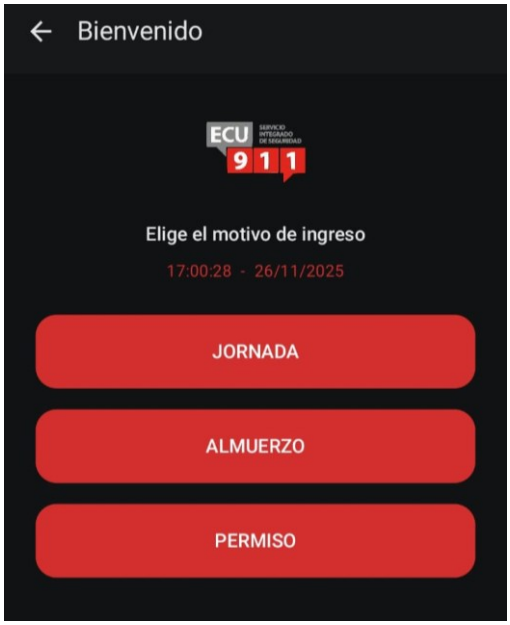


Figura 45. Pantalla elección motivo de registro.

La Figura 46 ilustra como una vez seleccionado el motivo, el proceso de reconocimiento facial inicia una vez clicado el botón “Capturar y verificar” y el dispositivo efectúa la verificación biométrica.

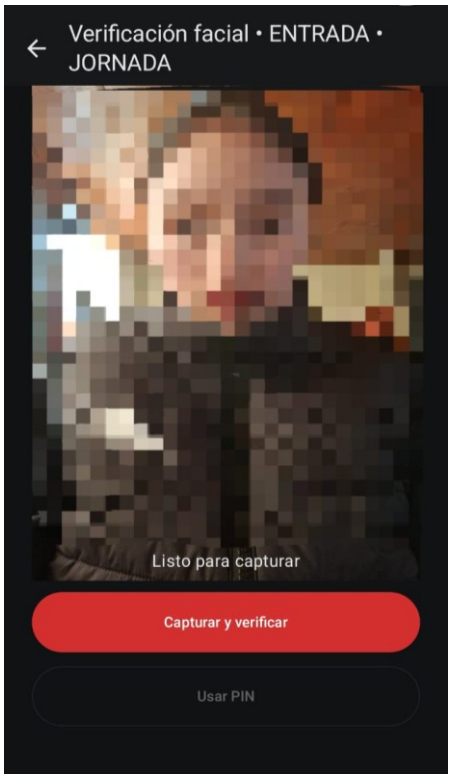


Figura 46. Reconocimiento facial.

Si el primer método de registro falla después de tres intentos se activa el registro por PIN automáticamente y el usuario debe ingresar su clave personal y registrar su acceso o egreso de la institución en la pantalla como muestra la Figura 47.

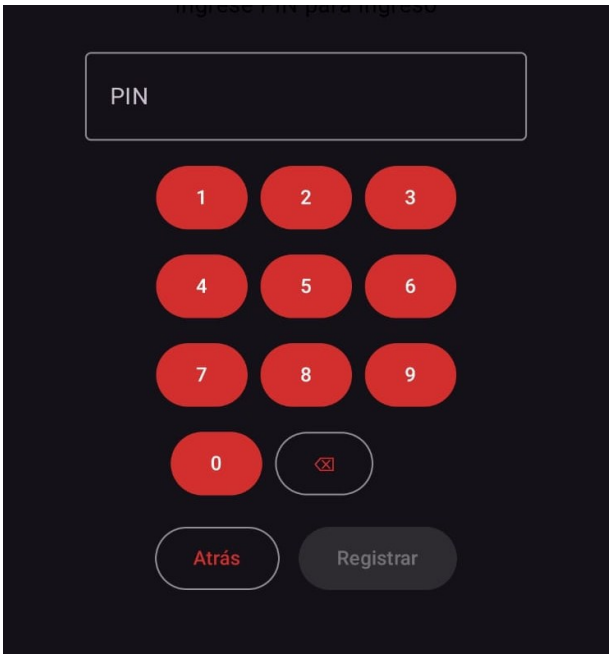


Figura 47. Registro a través de PIN.

La pantalla principal de los usuarios que desean registrar su ingreso/salida será por defecto, para regresar a la pantalla de modos o salir de la aplicación es obligatorio el uso de credenciales de administrador especificas destinadas para esta acción como se muestra en la Figura 48.

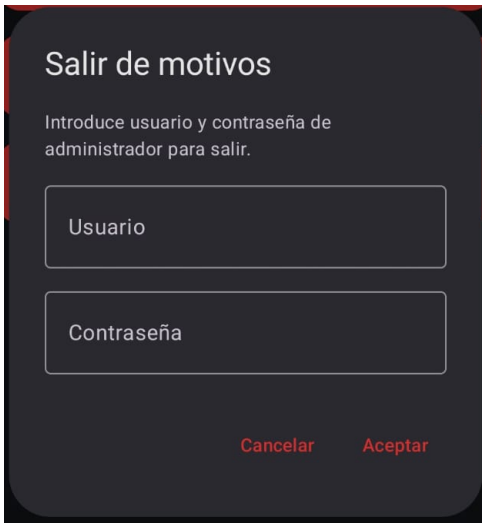


Figura 48. Salida de motivos solicita usuario y clave de administrador.

Dentro del proceso de reconocimiento facial cada una de sus fases cuenta con una duración temporal que se especifica en la Tabla 15.

Tabla 15. Medición de tiempo de reconocimiento facial.

Proceso	Métrica	Tiempo milisegundos (ms)
Detección	Tiempo de Detección	1000
Preprocesamiento	Tiempo de alineación	500
Extracción	Tiempo de inferencia	2000
Búsqueda y comparación	Tiempo de búsqueda	1000
Latencia total	Tiempo de decisión	4500

El tiempo total que toma el proceso de reconocimiento facial en el ingreso o salida y en cualquiera de los motivos de registro es de 4500 milisegundos, es decir, la latencia total de este proceso es de 4 a 5 segundos.

Registros nuevos empelados:

El usuario administrador ingresa todos los datos del empleado en la ventana de registro que solicita la información del usuario como los que se especifican en la Figura 49.



Figura 49. Ingreso de un nuevo empleado-administrador.

El registro del empleado incluye la carga de platillas faciales que requiere de diez fotografías del rostro del empleado de diferente ángulo y de ser posible en las mismas condiciones lumínicas a las que el dispositivo será ubicado, estas imágenes pueden obtenerse directamente desde el equipo o a través de la carga de imágenes previamente guardada como se puede evidenciar en la Figura 50.

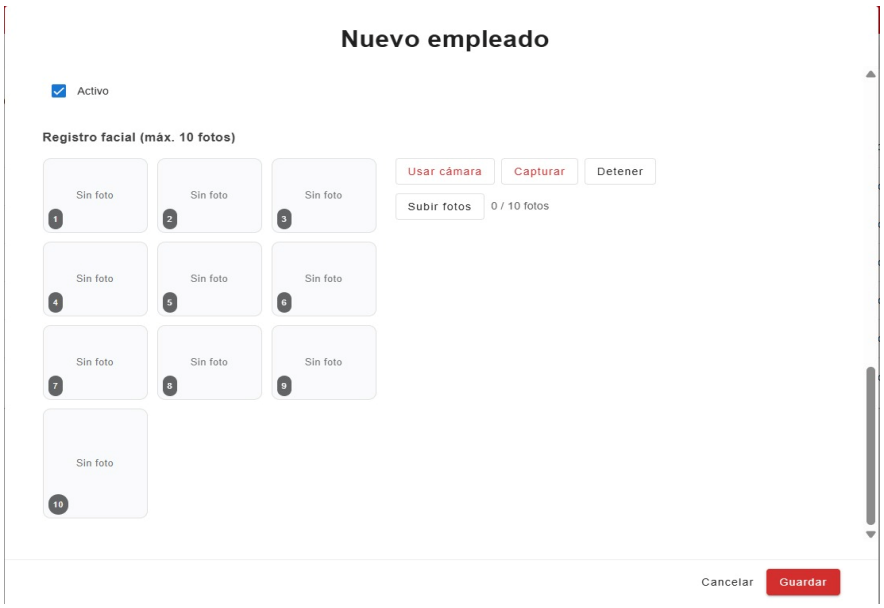


Figura 50. Registro facial.

Las fotos subidas pueden ser visualizadas antes de ser guardadas en este proceso como muestra la Figura 51.



Figura 51. Carga de imágenes exitosa.

Una vez registrado el empleado se puede visualizar en el listado general y realizar ediciones de ciertos datos del empleado registrado como muestra la Figura 52.



Figura 52. Verificación de ingreso, listado general.

3.3.4 Validación y entrega

En el proceso de validación del sistema de reconocimiento facial se consideran los siguientes puntos para asegurar que su funcionamiento sea legítimo.

3.3.4.1 Precisión y tasa de error:

Las métricas de evaluación de sistemas de reconocimiento facial se basan en dos métodos; verificación e identificación, en donde el proceso de identificación compara la imagen de entrada con todas las plantillas registradas y determina a cual identidad pertenece, siguiendo el flujo estándar que describe InsightFace que se comprende en la detección, alineación, extracción de embeddings, comparación e identificación de similitud [29].

Matriz de confusión, verificación 1:1

Se realizaron 40 comparaciones en las que 20 intentos fueron realizados por la misma persona y 20 intentos por personas diferentes, creando un dataset con un umbral de 0.6 en donde si es mayor a este valor es aceptado y si es inferior es rechazado dando como resultado la Figura 53:

```
MATRIZ DE CONFUSIÓN (verificación 1:1)
--------------------------------------
TN (impostor rechazado): 18
FP (impostor aceptado) : 2
FN (genuino rechazado) : 2
TP (genuino aceptado)  : 18
```

Figura 53. Resultados de la matriz de confusión.

Para una mejor visualización se colocan las métricas correspondientes en cada recuadro de la matriz como la que se visualiza en la Figura 54:

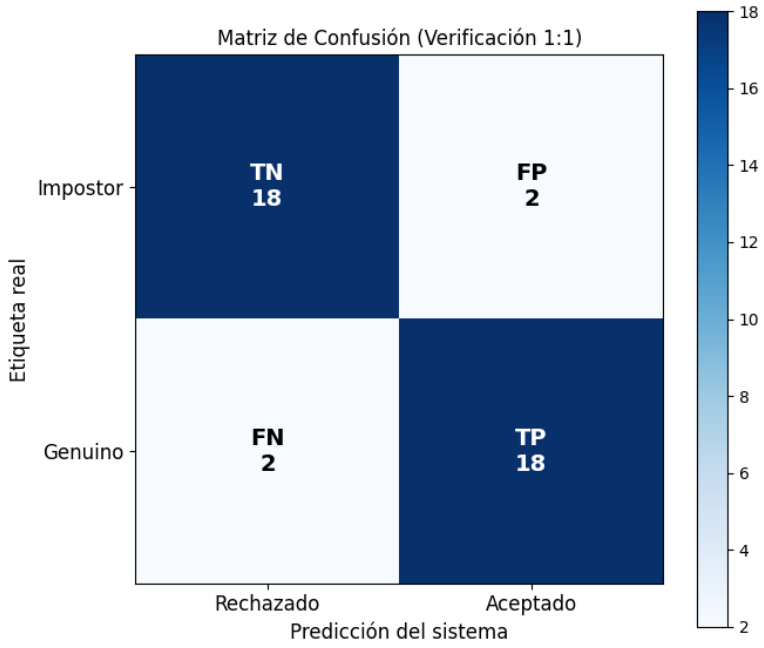


Figura 54. Matriz de confusión con métricas.

Los resultados de la matriz de confusión permiten el cálculo de las métricas de fiabilidad de los sistemas de identificación como se detallan a continuación:

FAR: *False Acceptance Rate (Falsa aceptación)*

$$FAR = \frac{FP}{FP + TN} = \frac{2}{2 + 18} = \frac{2}{20} = 0.10 = 10\%$$

FRR: *False Rejection Rate (Falsos rechazos)*

$$FRR = \frac{FN}{TP + FN} = \frac{2}{2 + 18} = \frac{2}{20} = 0.10 = 10\%$$

TAR: *True Acceptance Rate (Verdadera aceptación)*

$$TAR = \frac{TP}{TP + FN} = \frac{18}{18 + 2} = \frac{18}{20} = 0.90 = 90\%$$

Accuracy global: *Precisión global*

$$Acc = \frac{TP + TN}{Total} = \frac{18 + 18}{40} = \frac{36}{40} = 0.90 = 90\%$$

El sistema presenta un 90% de precisión global, su tasa de aceptación verdadera con un 90% y tasas de error en 10% indican que la aceptación de una persona diferente o el rechazo de una persona genuina es escaza, estos resultados son adecuados para un sistema de control de asistencia y verificación del personal.

Matriz de confusión, identificación 1:N

Esta validación asigna una muestra biométrica de entrada a una previamente registrada en el sistema, mientras que la verificación 1:1 el sistema decide si confirma o rechaza la existencia del empleado, la identificación 1:N determina quien es la persona, para esta validación se construyó un dataset con 10 identidades. Cada identidad se compara con las plantillas existentes y decide la similitud correspondiente mediante InsightFace a partir de los cuales se obtuvo la matriz que se muestra en la Figura 55 y para una mejor interpretación la Figura 56 muestra una representación más detallada.

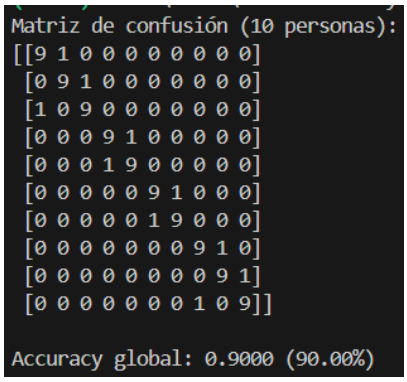


Figura 55. Resultado matriz de confusión.

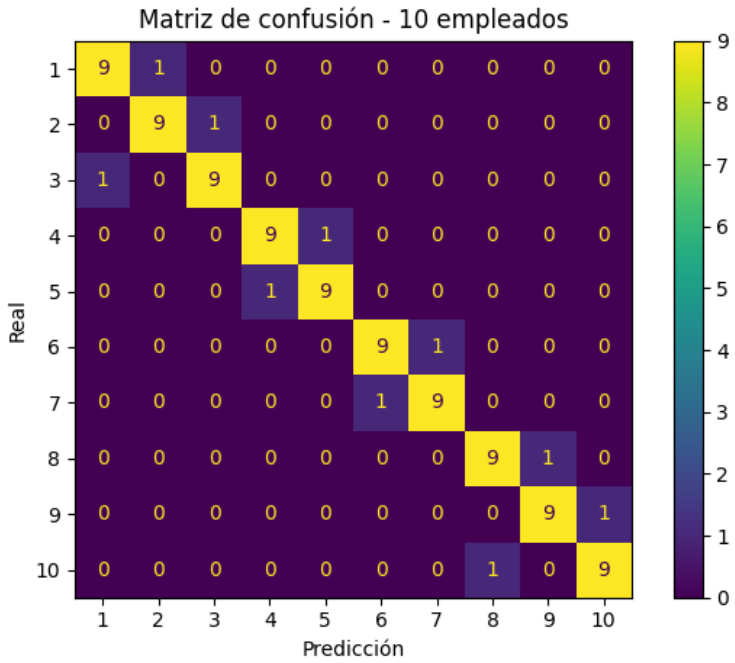


Figura 56. Matriz de confusión.

La matriz obtenida con un conjunto específico de 10 identidades en modo de identificación muestra el comportamiento de InsightFace, mostrando a cada fila como la identidad real y cada columna como una identidad predicha por el modelo.

La Figura 56 muestra de manera clara la diagonal principal que concentra 90 aciertos correspondientes al 90% de reconocimiento correcto y el resto de las celdas fuera de la diagonal representan casos de confusión de identidad dando como predicción errónea 1 de cada 10 pruebas.

3.3.4.2 Equidad

La coordinación zonal 3 cuenta con un personal diverso por ello, el sistema permite el registro y reconocimiento de todos los trabajadores, pero no identifica los factores mencionados en la Tabla 16:

Tabla 16. Verificación de equidad.

Interseccionalidad	Identificación
Etnias	No
Géneros	No
Edades	No

3.3.4.3 Suplantación

Existes diversas formas de suplantar la identidad de una persona, por lo que el modelo debe ser capaz de diferenciar y rechazar estos procedimientos, asegurar que la persona es quien dice ser, en la Tabla 17 se muestra los cumplimientos que tiene el sistema de reconocimiento facial.

Tabla 17. Verificación de suplantación.

Funcionalidad	Cumplimiento
Diferencia fotografías o videos de persona real	Si
Diferencia máscaras o modelos 3D de persona real	No
Implementa livess detection	Si

3.3.4.4 Cumplimiento legal

El organismo interno del Sistema Integrado de Seguridad ECU 911, exige que se cumpla con el reglamento de cumplimiento legal que se detalla en la Tabla 18.

Tabla 18. Verificación de cumplimiento legal.

Consideración	Cumplimiento
Protección de datos biométricos	Si
Consentimiento informado	Si
Documentación del propósito de uso	Si

El sistema debe cumplir con las reglas de las normas ISO enfocadas en el reconocimiento facial y control de asistencia, las mismas que se detallan en la Tabla 19:

Tabla 19. Cumplimiento normativo.

Norma ISO	Descripción	Cumplimiento
ISO 197945	Calidad y formato de imágenes faciales	100%
ISO 301073	Detección de suplantaciones	100%
ISO 24745	Seguridad y protección de plantillas biométricas	100%
ISO 27001	Seguridad de la información del sistema	100%
ISO 27001	Privacidad y manejo de datos biométricos	100%

3.3.4.5 Entrega

- ***Pruebas de requisitos funcionales***

La entrega del sistema requiere validación del cumplimiento total de los requisitos funcionales que se demostraron mediante pruebas previas, la Tabla 20 detalla el estado de cumplimiento de estos requisitos.

Tabla 20. Verificación de requisitos funcionales.

Código	Requerimiento	Cumplimiento
RF1	Registro biométrico	100%
RF2	Identificación y verificación	100%
RF3	Control de acceso	100%
RF4	Selección de motivo de ingreso	100%
RF5	Registro de transacciones	100%
RF6	Gestión administrativa del personal	100%
RF7	Generación de reportes	100%

- ***Pruebas de aceptación***

Las pruebas de aceptación permiten determinar si el sistema cumple con las especificaciones esenciales para satisfacer al usuario final. Con este fin se han realizado evaluaciones por usuario usando como referencia el Manual de usuarios detallados en el Anexo A, se tomaron las funciones más usadas que se detalla a continuación:

a. Usuario administrador:

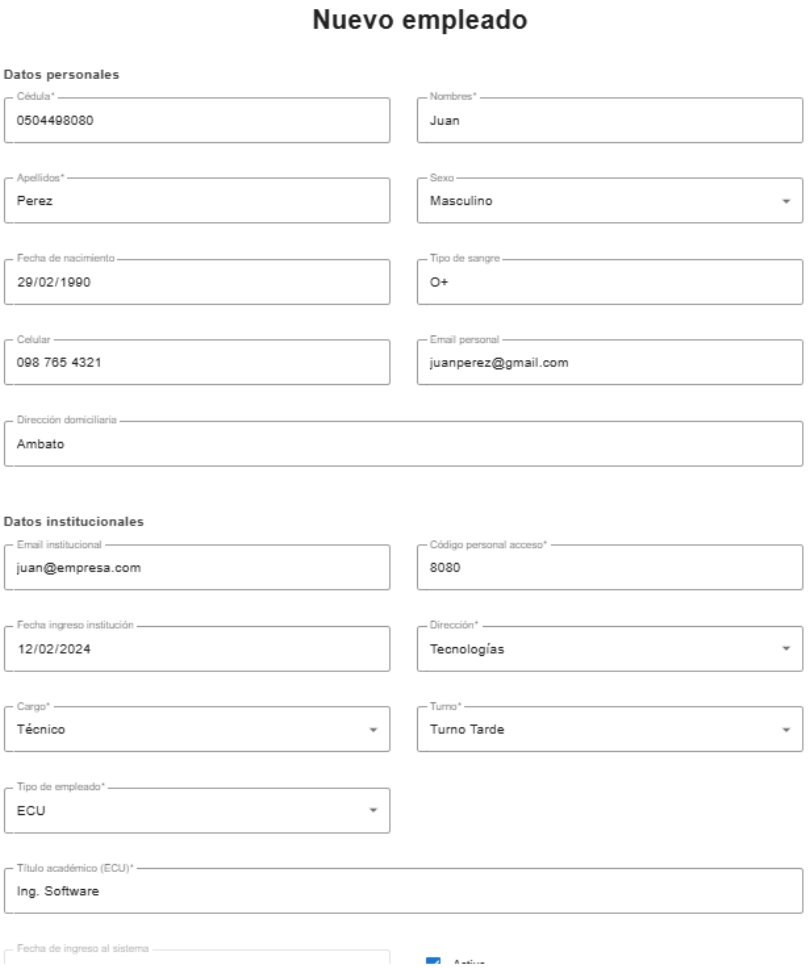


Figura 57. Ingreso de un nuevo empleado.

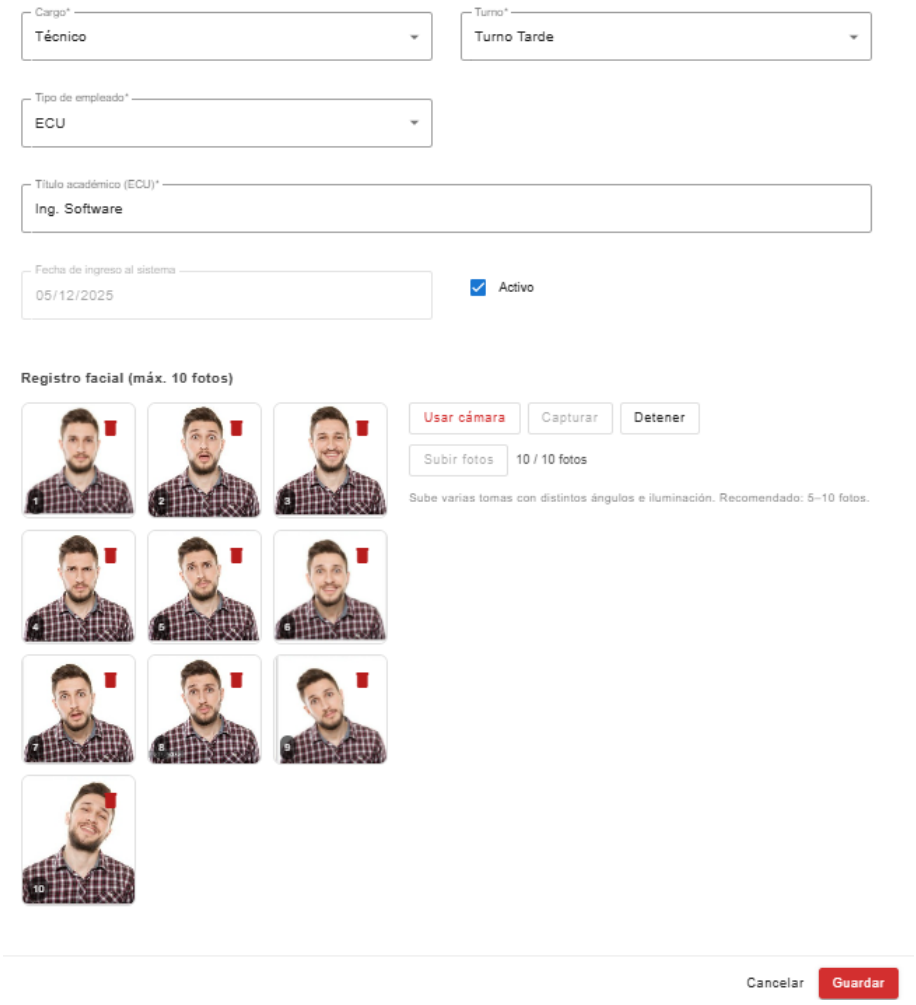


Figura 58. Carga de plantillas faciales iniciales.

Tabla 21. Prueba de aceptación 1.

Prueba de aceptación	
Código: 01	**Historia de usuario:** Registro de empleado
Nombre: Registro de un nuevo empleado al sistema	
Descripción: Validar que el administrador logre registrar un nuevo empleado y cargar las plantillas faciales iniciales	
Condiciones de ejecución: El usuario administrador debe contar con el consentimiento del empleado para uso de los datos personales y biométricos, además debe contar con 10 fotos del empleado.	
Ejecución: Iniciar sesión con el rol “Administrador” Acceder al módulo Empleado interno /empleado articulado/empleado externo Clicar en el botón “Agregar nuevo empleado” Ingresar todos los datos requeridos Subir las 10 fotos necesarias y obligatorias Clicar en “Guardar”	
Resultado esperado:	

El sistema registra al nuevo empleado de manera exitosa y se verificar en el listado general la creación del nuevo empleado.
Evaluación de la prueba: Satisfactoria

b. Usuario guardia:

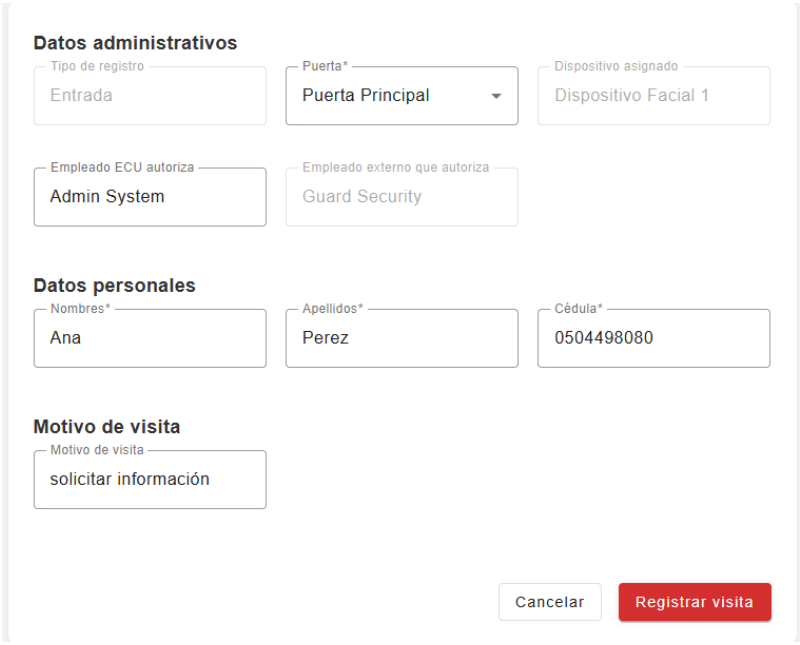


Figura 59. Ingreso de datos del visitante.

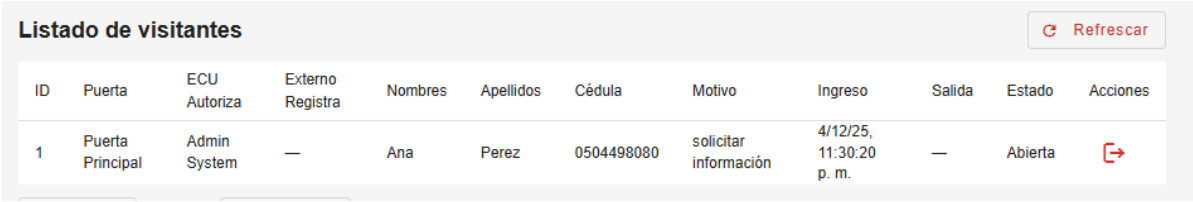


Figura 60. Verificación de ingreso de datos del visitante.

Tabla 22. Prueba de aceptación 2.

Prueba de aceptación	
Código: 02	**Historia de usuario:** Registro de visitantes
Nombre: Registro de visitantes	
Descripción: Validar que el guardia de seguridad a través de su usuario logre registrar un nuevo visitante	
Condiciones de ejecución: El usuario guardia debe contar con una identificación de los visitantes y aprobar o denegar el ingreso.	
Ejecución: Iniciar sesión con el rol “Guardia”	

Acceder al módulo Registrar visitante Clicar en el botón “Agregar nuevo visitante” Ingresar todos los datos requeridos Clicar en el botón “Guardar” Notificar mediante llamada telefónica a un superior Conceder o denegar el ingreso
Resultado esperado: El sistema registra al nuevo visitante a través del formulario de registro y concede o deniega el acceso previo a la solicitud de la petición a un elemento superior
Evaluación de la prueba: Satisfactoria

c. Usuario recursos humanos:

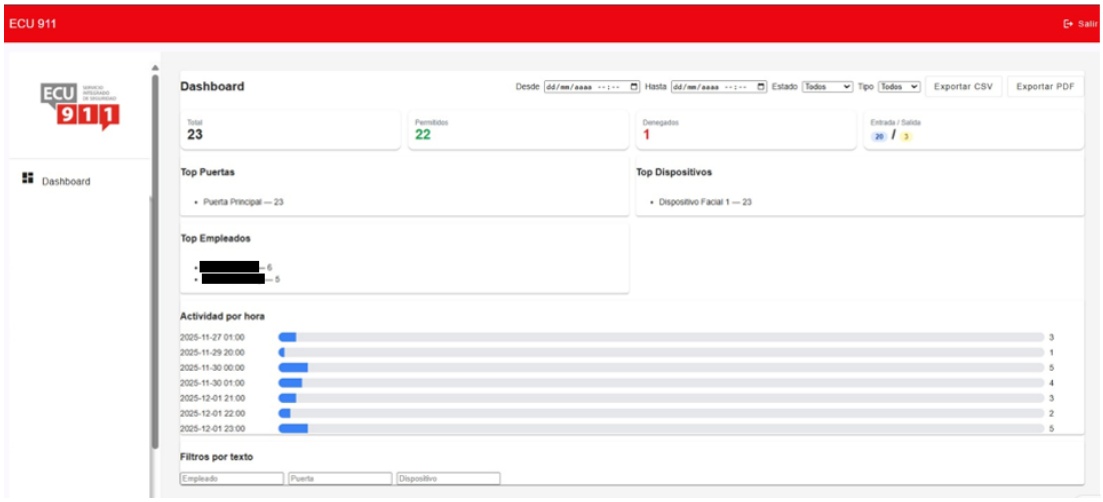


Figura 61. Visualización de dashboard.

Tabla 23. Prueba de aceptación 3.

Prueba de aceptación	
Código: 03	**Historia de usuario:** Visualización de registros de ingreso y salida del personal
Nombre: Visualización de gráficos de reporte de asistencia	
Descripción: Validar que el usuario de recursos humanos pueda visualizar gráficamente los registros de ingreso y salida del personal	
Condiciones de ejecución: El usuario de recursos humanos debe iniciar sesión con las credenciales correctas	
Ejecución: Iniciar sesión con el rol “Recursos Humanos” Acceder al módulo Registros Clicar en el botón “Filtros” Elegir el filtro que desea Visualizar las gráficas con los filtros aplicados	
Resultado esperado: El sistema permite visualiza los registros de acceso o egreso a la institución aplicando filtros requeridos sin inconvenientes	

Evaluación de la prueba: Satisfactoria

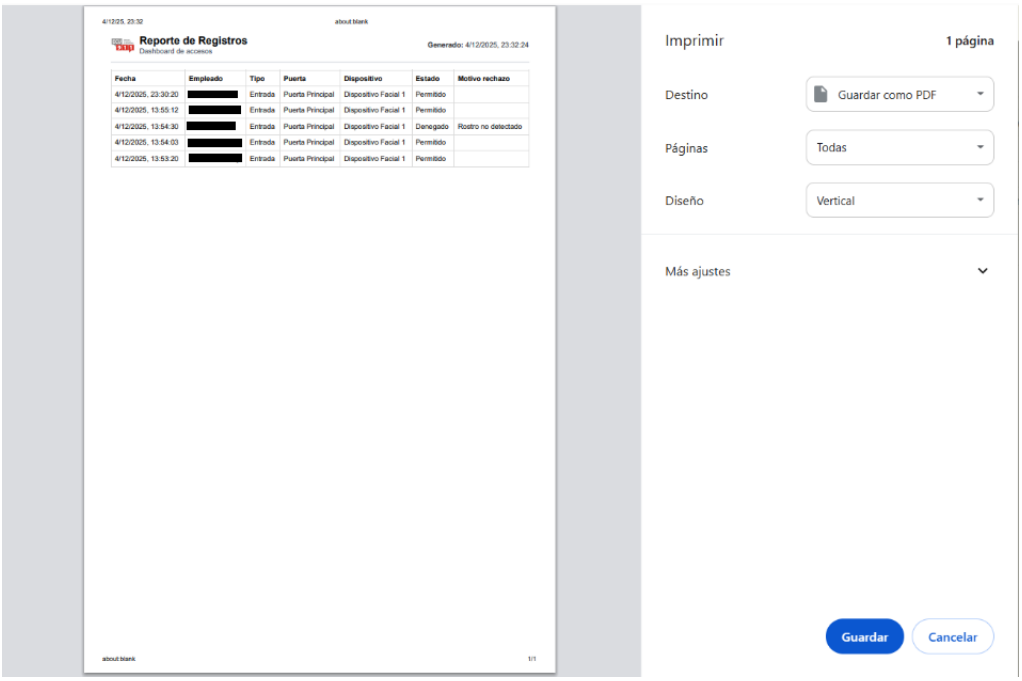


Figura 62. Generación de reportes descargables.

Tabla 24. Prueba de aceptación 4.

Prueba de aceptación	
Código: 04	**Historia de usuario:** Generación de reportes de asistencias
Nombre: Generación y obtención de reportes de asistencia	
Descripción: Validar que el usuario de recursos humanos pueda generar reportes de asistencia descargables.	
Condiciones de ejecución: El usuario de recursos humanos debe iniciar sesión con las credenciales correctas	
Ejecución: Iniciar sesión con el rol “Recursos Humanos” Acceder al módulo Registros Clicar en el botón “Filtros” Elegir el filtro que desea Visualizar las gráficas con los filtros aplicados Clicar en el botón “Descargar reporte” Verificar en el explorador de archivos la descarga correcta del reporte	
Resultado esperado: El sistema permite generar reportes de asistencia generales, o específicos del personal en archivos descargables	
Evaluación de la prueba: Satisfactoria	

d. Usuarios que usan el dispositivo biométrico:

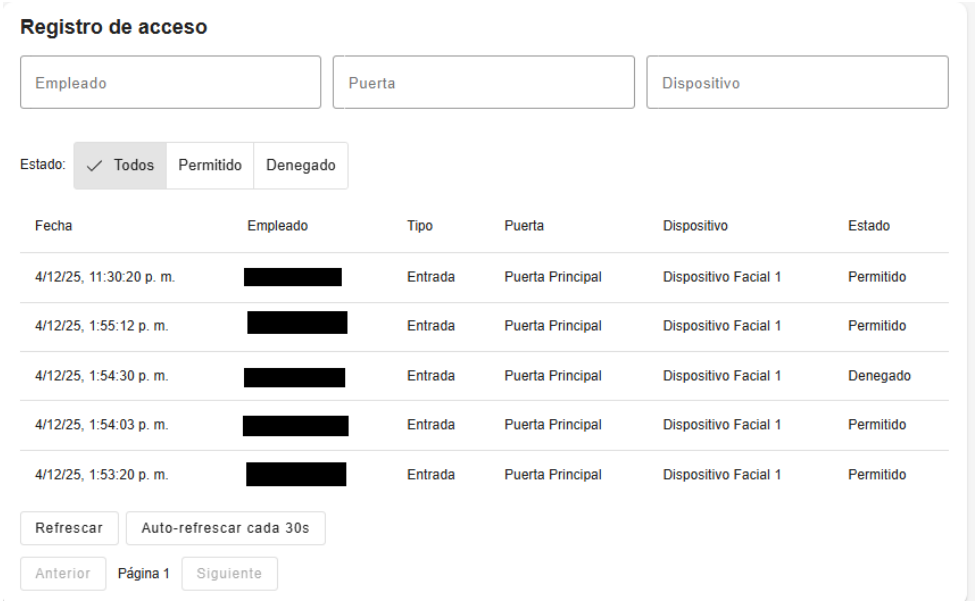


Figura 63. Usuarios registrados a través del dispositivo biométrico.

Tabla 25. Prueba de aceptación 5.

Prueba de aceptación	
Código: 05	**Historia de usuario:** Registro de ingreso/salida
Nombre: Registro de ingreso/salida	
Descripción: Validar que el usuario de recursos humanos pueda generar reportes de asistencia descargables.	
Condiciones de ejecución: El empleado que desea realizar su registro de ingreso/salida por reconocimiento facial debe estar registrado en el sistema	
Ejecución: Acercamiento al dispositivo Seleccionar el motivo de ingreso/salida Clicar en el botón “Capturar y verificar” Puerta abierta Ingreso/salida con éxito Visualización en la ventana de registro de acceso	
Resultado esperado: El sistema permite la selección de motivos de ingreso/salida para la verificación del empleado y registro con fecha y hora exactos.	
Evaluación de la prueba: Satisfactoria	

- ***Pruebas de iteración***

Tabla 26. Validación de pruebas de cada iteración.

Fase	Iteración	Descripción	Cumplimiento
Planificación	Iteración 0	Identificación del proceso inicial de control de ingreso y salida del personal a través de la recolección de datos.	Aprobado
	Iteración 1	Especificación de los grupos de interés.	Aprobado
	Iteración 2	Definición de requerimientos funcionales y no funcionales.	Aprobado
	Iteración 3	Establecer las fases del proyecto.	Aprobado
Desarrollo	Iteración 4	Diseño de la arquitectura del sistema.	Aprobado
	Iteración 5	Fases del reconocimiento facial en InsightFace.	Aprobado
	Iteración 6	Diseño de la base de datos.	Aprobado
	Iteración 7	Prototipo pantallas del dispositivo.	Aprobado
	Iteración 8	Prototipo pantallas del servicio web.	Aprobado
	Iteración 9	Diagramas de casos de uso.	Aprobado
Integración y pruebas	Iteración 10	Codificación	Aprobado
	Iteración 11	Integración dispositivo móvil	Aprobado
	Iteración 12	Registro nuevo empleado	Aprobado
	Iteración 13	Verificación	Aprobado
Validación y entrega	Iteración 14	Precisión y tasa de error	Aprobado
	Iteración 15	Entrega	Aprobado

- ***Guía de implantación:***

Servidor

Preparación del entorno

Instalación de Docker

```
sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin -y
```

Verificación del estado de docker

```
sudo systemctl status docker
```

Despliegue

Acceder a la raíz del proyecto e inicializar contenedor

```
docker-compose build
```

```
docker-compose up
```

Dispositivo móvil:

La configuración administrativa inicial solo la realizar el usuario administrador de dispositivos, el cual ingresa el código de emparejamiento para registrar el móvil como se puede evidenciar en la Figura 64.

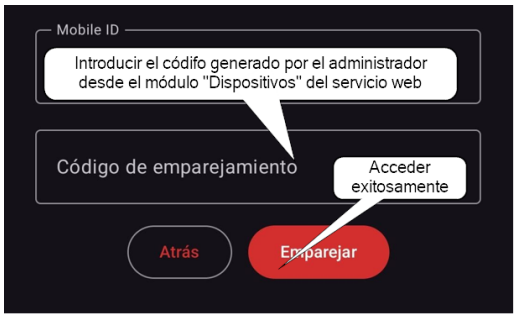


Figura 64. Código de emparejamiento.

El administrador de dispositivos selecciona el motivo con el cual trabajará el móvil, el cual estará fijo en el lugar de ingreso o salida. La Figura 65 muestra el modo entrada y salida como las dos únicas opciones de selección.



Figura 65. Selección modo de uso del dispositivo.

Para finalizar con la instalación es necesario el ingreso de usuario y contraseña del administrador de dispositivos como muestra la Figura 66.

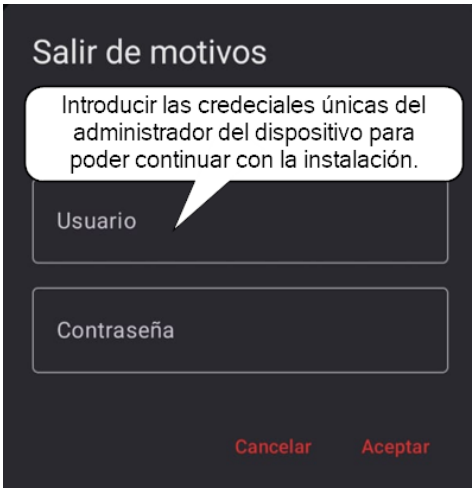


Figura 66. Pantalla de acceso para instalación.

La instalación finaliza dejando la interfaz lista para el registro de ingreso o salida con los motivos de jornada, almuerzo y permisos, la Figura 67 muestra la primera interfaz que se visualizará para los empleados.



Figura 67. Fin de instalación.

Una vez configurado y desplegado el servicio y el dispositivo se procede a la instalación física de los biométricos como se evidencia en el Anexo B.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se determinó que las instalaciones de la coordinación zonal 3 del servicio integrado de seguridad ECU 911 carece de un sistema formal y automatizado de control de ingreso, a través de la recopilación de información mediante la entrevista al director de tecnología, encuesta y ficha de observación se evidenciaron limitaciones críticas del sistema tradicional, se comprobó la existencia de equipos biométricos obsoletos, verificación humana del personal y desorden del personal en horas pico, que a través de procesos manuales con el personal de seguridad y bitácoras en papel destacaban riesgos por errores humanos, pérdida de información, ingresos no verificados, valores inexactos e información errónea lo cual permitió reforzar la necesidad de modernizar y automatizar la infraestructura y protocolos de control de ingreso/salida.

- A través de la investigación se logró establecer los requisitos técnicos y operativos necesarios para el desarrollo e implementación de un sistema de reconocimiento facial en la coordinación zonal 3 del sistema integrado de seguridad ECU 911, el análisis contempló la elección del framework InsightFace, la especificación de los componentes de hardware y software apropiados, protocolos de seguridad y mantenimiento aseguran la vialidad técnica y funcional del sistema. Además, se añadió un enfoque sostenible mediante la reutilización de dispositivos móviles en desuso, optimizando recursos, disminuyendo la basura electrónica y reduciendo costos, para alinear el proyecto a prácticas responsables de gestión de tecnología.

- Se desarrolló un sistema de reconocimiento facial que contempla un flujo de detección, alineación, extracción de características y verificación mediante el framework InsightFace, el proceso de diseño implicó una arquitectura con módulos móviles, web y hardware de control físico que a través de las pruebas de rendimiento confirmaron

una alta precisión en entornos reales, también se incorporó mecanismos alternativos de registro como el uso de un PIN para garantizar la continuidad operativa frente a fallos logrando así mostrar confiabilidad frente a los usuarios.

- Se logró implantar el sistema biométrico integral de verificación y control de acceso en la coordinación zonal 3 del sistema integrado de seguridad ECU 911, dejando atrás mecanismos manuales vulnerables para optimizar procesos que aseguren mecanismos seguros y eficientes, además de cumplir con los estándares técnicos normativos, el sistema incorpora un enfoque sostenible mediante la reutilización de dispositivos móviles en desuso como terminales biométricos, lo cual contribuye a prácticas responsables alineadas con la transformación digital y optimización del control de personal de la institución.

- La metodología híbrida Scrum-Kanban permitió combinar la estructura de Scrum con la flexibilidad de Kanban, logrando un desarrollo ágil, adaptable y con visibilidad continua del progreso. Este enfoque redujo la carga administrativa, facilitó la priorización dinámica de tareas y aseguró entregas incrementales alineadas con los objetivos del proyecto, demostrando ser ideal para proyectos tecnológicos que requieren rapidez y control.

4.2 Recomendaciones

- Es importante considerar la implementación del sistema de reconocimiento facial con medidas de seguridad continua como cifrado de plantillas faciales, umbrales de precisión y tiempos de respuesta junto con respaldos frecuentes y protocolos de contingencia ante fallas adaptados a la infraestructura del sistema, además mantener un plan operativo para el mantenimiento preventivo de dispositivos, actualizaciones de plantillas faciales y capacitación constante del personal en el uso del sistema, sin dejar de lado el enfoque sostenible para la reducción de costos y disminución de residuos electrónicos.

- Fomentar la investigación continua sobre tecnologías biométricas emergentes y su difusión de manera responsable a través de repositorios académicos, congresos y libros especializados permitirá actualizaciones en conocimiento fortaleciendo la formación profesional en áreas de seguridad y transformación digital.

- El uso de metodologías ágiles híbridas en futuros proyectos tecnológicos permitirá flexibilidad frente a cambios rigurosos gracias a la gestión eficiente del tiempo, recursos y la adaptabilidad de la metodología que investigador deseé darle a su proyecto, asegurando iteraciones rápidas, validaciones tempranas y mejora continua en todos los procesos que lo requiera en conjunto con la infraestructura existente.

REFERENCIAS BIBLIOGRÁFICAS

[1] «10 beneficios de usar un control de accesos | Scati». Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://www.scati.com/2024/05/29/10-beneficios-de-usar-un-control-de-accesos/

[2] «Controles ISO 27001: cuáles son y qué debes saber para implementarlos». Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://innevo.com/blog/controles-iso27001

[3] «Centro de Biometría». Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Centro-de-Biometria

[4] «Las 10 tendencias que están marcando el rumbo de la biometría en América Latina», Revista Innovación Seguridad. Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: http://revistainnovacion.com/nota/12574/las_10_tendencias_que_estan_marcando_el_rumbo_de_la_biometria_en_america_latina/

[5] «Servicio Integrado de Seguridad ECU 911 – Servicio Integrado de Seguridad ECU 911». Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://www.ecu911.gob.ec/servicio-integrado-de-seguridad-ecu-911/

[6] «¿Qué es el reconocimiento facial y cómo funciona?», /. Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-facial-recognition

[7] J. E. M. R. Campos, C. S. C. Rodríguez, L. D. A. Luján, y A. C. M. de los Santos, «Sistema de reconocimiento facial para el control de accesos mediante Inteligencia Artificial», *Innov. Softw.*, vol. 4, n.º 1, 2023, Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://www.redalyc.org/journal/6738/673874721016/html/

[8] M. Ouloul, Z. Moutakki, A. Amghar, y K. Afdel, «Low-cost embedded facial recognition system based on overlapped local binary pattern», *E-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 11, p. 100924, mar. 2025, doi: 10.1016/j.prime.2025.100924.

[9] H. L. Gururaj, B. C. Soundarya, S. Priya, J. Shreyas, y F. Flammini, «A Comprehensive Review of Face Recognition Techniques, Trends, and Challenges», *IEEE Access*, vol. 12, pp. 107903-107926, 2024, doi: 10.1109/ACCESS.2024.3424933.

[10] C. X. Morocho Vallejo, «Desarrollo de un prototipo de sistema de control de asistencia y de horario laboral de un centro de desarrollo inicial.», bachelorThesis, Quito : EPN, 2022., 2022. Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://bibdigital.epn.edu.ec/handle/15000/23431

[11] «TI (tecnología de la información): conceptos básicos». Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://www.ninjaone.com/es/blog/conceptos-basicos-ti/

[12] «What is Physical Security and How Does it Work? | Definition from TechTarget», Search Security. Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://www.techtarget.com/searchsecurity/definition/physical-security

[13] E. Estudio, «¿Qué es la identificación biométrica?», Ecdisis Estudio. Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://ecdisis.com/que-es-la-identificacion-biometrica/

[14] «¿Qué es el reconocimiento facial? - Explicación del software de reconocimiento facial y análisis facial - AWS», Amazon Web Services, Inc. Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://aws.amazon.com/es/what-is/facial-recognition/

[15] J. M. Sánchez, «¿Qué es la validación de identidad y para qué sirve?», Veridas. Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://veridas.com/es/validacion-identidad/

[16] «Control de Acceso: Clave para la Seguridad de Instalaciones», https://www.aimmanager.com/. Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://www.aimmanager.com/blog/control-de-acceso/

[17] «¿Qué es la gestión del talento humano? | UNIR Colombia», Universidad Virtual. | UNIR Colombia - Maestrías y Grados virtuales.

Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://colombia.unir.net/actualidad-unir/gestion-del-talento-humano/

[18] proware, «Importancia Del Control De Ingreso De Empleados En La Gestión Laboral - Proware HS S.A.S». Accedido: 24 de septiembre de 2025. [En línea]. Disponible en: https://www.proware.com.co/blog/importancia-del-control-de-ingreso-de-empleados-en-la-gestion-laboral/

[19] «InsightFace Tarificación, Reseñas, Alternativas - AI Image Editing». Accedido: 24 de octubre de 2025. [En línea]. Disponible en: https://aitools.fyi/es/insightface

[20] R. Stewart, K. Kralev, y D. Stoyanov, «Deep Learning-based Face Recognition in Help of Historical Data and Event Analyses», *Digit. Present. Preserv. Cult. Sci. Herit.*, vol. 15, pp. 107-116, sep. 2025, doi: 10.55630/dipp.2025.15.10.

[21] A. N y K. Anusudha, «Real time face recognition system based on YOLO and InsightFace», *Multimed. Tools Appl.*, vol. 83, n.º 11, pp. 31893-31910, mar. 2024, doi: 10.1007/s11042-023-16831-7.

[22] «DeepFace: avances en el reconocimiento facial con IA». Accedido: 7 de noviembre de 2025. [En línea]. Disponible en: https://www.innovatiana.com/es/post/deepface-101

[23] «How to Build a Face Recognition System Using FaceNet in Python», DEV Community. Accedido: 24 de octubre de 2025. [En línea]. Disponible en: https://dev.to/abhinowww/how-to-build-a-face-recognition-system-using-facenet-in-python-27kh

[24] A. K. Jain, A. A. Ross, K. Nandakumar, y T. Swearingen, «Face Recognition», en *Introduction to Biometrics*, A. K. Jain, A. A. Ross, K. Nandakumar, y T. Swearingen, Eds., Cham: Springer International Publishing, 2025, pp. 119-173. doi: 10.1007/978-3-031-61675-4_4.

[25] «Guía de control de acceso biométrico y cerraduras seguras», Avigilon. Accedido: 19 de noviembre de 2025. [En línea]. Disponible en: https://www.avigilon.com/es/blog/biometric-access-control

[26] Y. D. Romero Carrión y F. J. Vásquez Fajardo, «Desarrollo de una aplicación para registro de asistencia mediante técnicas inteligentes como

reconocimiento facial, reconocimiento del hablante y geolocalización», bachelorThesis, 2022. Accedido: 3 de diciembre de 2025. [En línea]. Disponible en: http://dspace.ups.edu.ec/handle/123456789/22011

[27] P. Ngoy *et al.*, «Supporting Sustainable Computing by Repurposing E-Waste Smartphones as Tiny Data Centers», *IEEE Pervasive Comput.*, vol. 24, n.º 1, pp. 53-60, ene. 2025, doi: 10.1109/MPRV.2025.3541558.

[28] H. Vega *et al.*, «Reconocimiento facial mediante aprendizaje por transferencia para el control de acceso a áreas restringidas», *RISTI - Rev. Ibérica Sist. E Tecnol. Informação*, pp. 261-273, may 2024.

[29] V. L. B. De Mel, *Survey of Evaluation Metrics in Facial Recognition Systems*. 2023. doi: 10.13140/RG.2.2.10974.20805.

ANEXOS

Anexo A. Manual de usuario.





USUARIO:
ADMINISTRADOR



1 El panel administrativo muestra todos los módulos del sitio web, el módulo **Dashboard** contiene:

2 -3 Filtro para visualización de ingresos y salidas en un intervalo de fechas.

4 Filtro para visualización por estado y tipo.

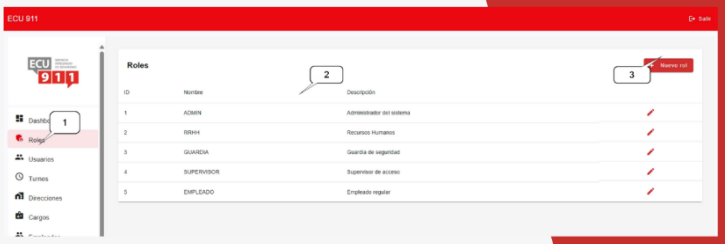
5 Botones de exportación en formatos CSV y PDF

6 Muestra el top 5 de empleados más registrados.

7 Visualización gráfica de actividad por horas.

8 Lista de dispositivos

USUARIO:
ADMINISTRADOR



1 Seleccionar el módulo "Roles"

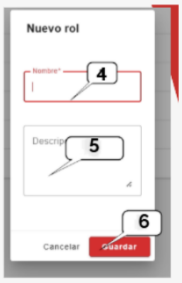
2 Visualizar listado de roles

3 Botón para creación de nuevos roles

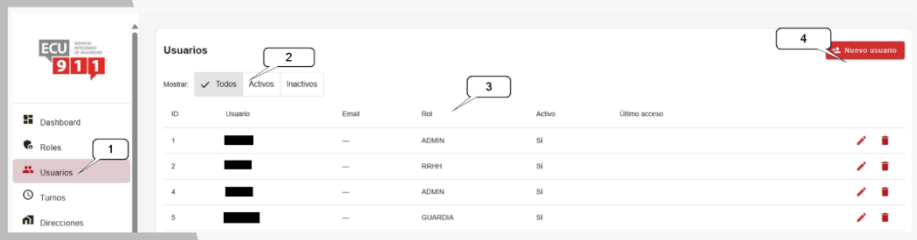
4 Ingresar el nombre del rol

5 Ingresar la descripción del rol

6 Guardar el rol y visualizar en el paso 2.



USUARIO:
ADMINISTRADOR



1 El panel administrativo muestra todos los modulos del sitio web el módulo **Usuarios** contiene:

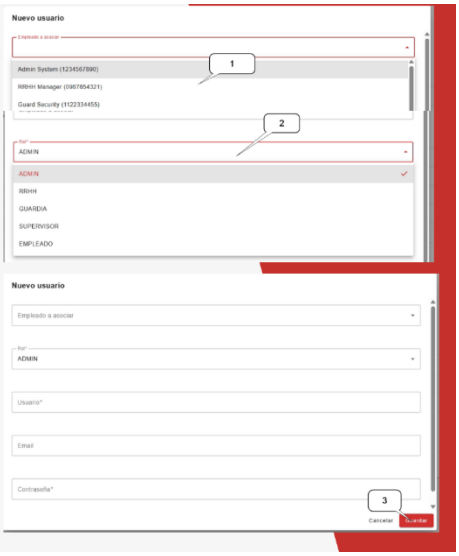
2 Filtros para visualizar el listado

3 Listado de usuarios

4 Creación nuevo usuario

USUARIO:
ADMINISTRADOR

CREACIÓN
NUEVO USUARIO

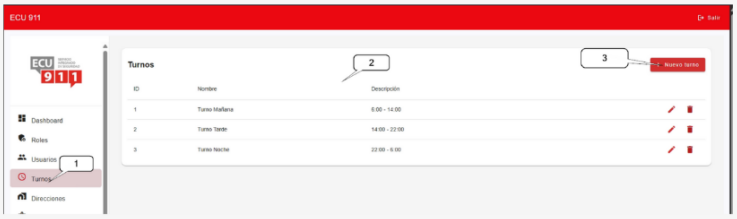


1 Seleccionar el empleado al cual se le va asignar un usuario

2 Seleccionar el rol que tendrá este usuario

3 Llenar todos los campos y clicar en "Guardar"

USUARIO:
ADMINISTRADOR



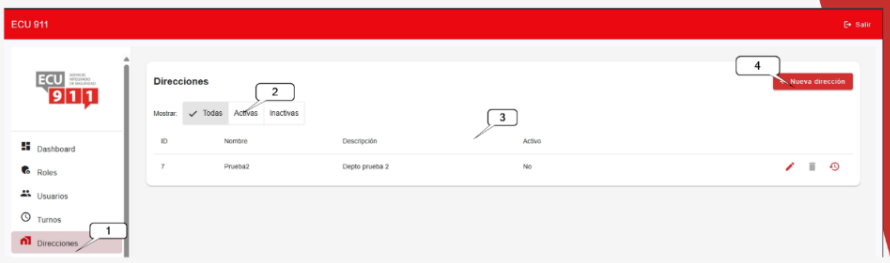
1 El panel administrativo muestra todos los modulos del sitio web el módulo **Turnos** contiene:

2 Listado de turnos

3 Botón para creación de nuevo turno

4 Creación nuevo usuario

USUARIO:
ADMINISTRADOR



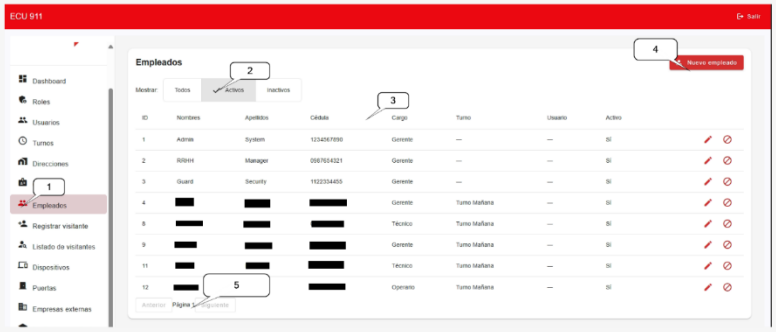
1 El panel administrativo muestra todos los módulos del sitio web, el módulo **Direcciones** contiene:

2 Filtros para visualizacion del listado

3 Listado de direcciones

4 Botón creacion nueva dirección de la institución

USUARIO: ADMINISTRADOR



1 El panel administrativo muestra todos los modulos del sitio web, el módulo **Empleados** contiene:

2 Filtros para visualización el listado

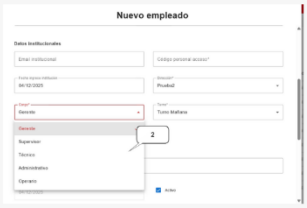
3 Listado de los empleados registrados

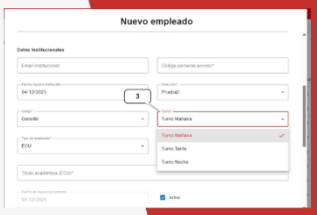
4 Botón para creación de nuevo empleado

5 Botones de paginación

USUARIO: ADMINISTRADOR **CREACIÓN NUEVO EMPLEADO**





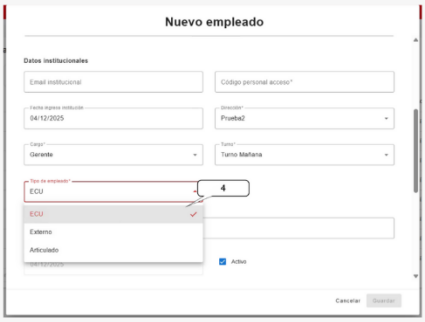


1 La ventana de creación de nuevo empleado solicita datos personales

2 Elección del cargo que mantiene en la institución

3 Elección del turno en el cual labora

USUARIO: ADMINISTRADOR **CREACIÓN NUEVO EMPLEADO**





4 Elección del tipo de empleado

5 Carga de imágenes a través de la cámara

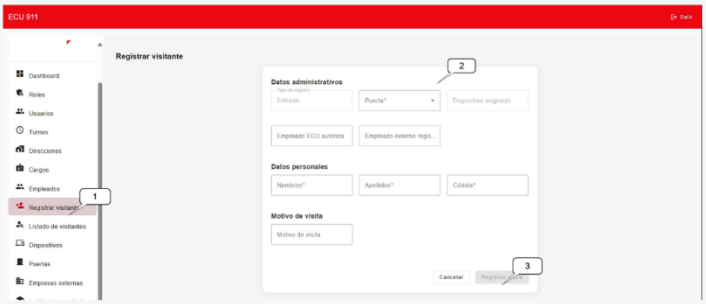
6 Capturar imágenes

7 Botón para subir fotos desde el ordenador

8 Visualización de imágenes cargadas

9 Botón Guardar empleado

USUARIO:
ADMINISTRADOR

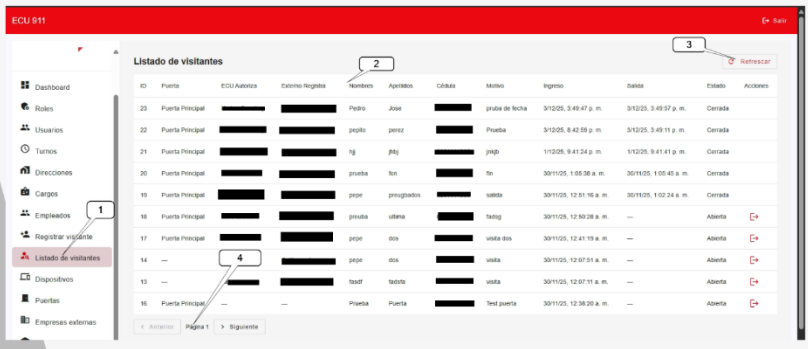


1 El panel administrativo muestra todos los módulos del sitio web, el módulo **Registrar visitantes** contiene:

2 Ingreso de datos del visitante

3 Botón de registro del visitante

USUARIO:
ADMINISTRADOR



1 El panel administrativo muestra todos los modulos del sitio web el módulo **Listado de visitantes** contiene:

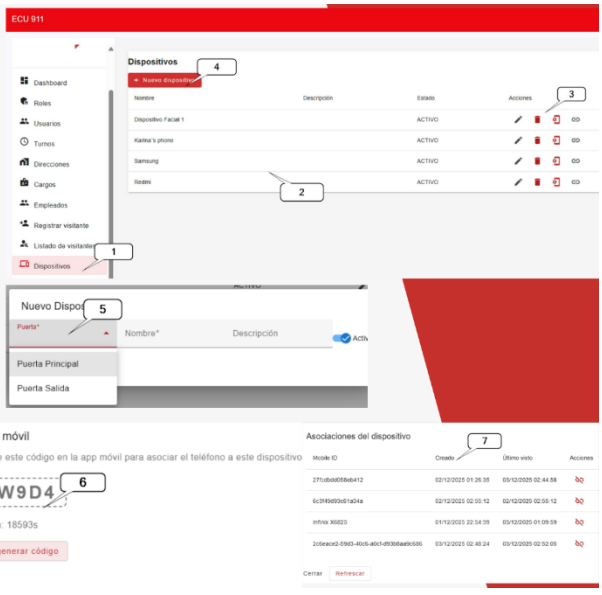
2 Visualización del listado de visitantes

3 Botón para recargar el listado

4 Botones de paginación

USUARIO:
ADMINISTRADOR DISPOSITIVOS

1. El panel administrativo muestra todos los módulos del sitio web, el módulo **Dispositivos** contiene:
2. Listado de dispositivos registrados
3. Acciones para dispositivos registrados
4. Botón de creación de nuevo dispositivo
5. Al crear un nuevo dispositivo se debe vincular a la puerta en la que se ubicará el dispositivo
6. Una vez creado el dispositivo se lo asocia con el código generado.
7. La acción del paso 3 permite visualizar las asociaciones del dispositivo

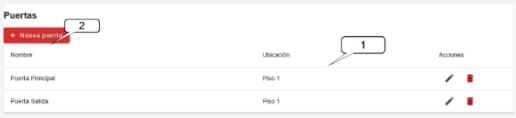


USUARIO: ADMINISTRADOR



El panel administrativo muestra todos los módulos del sitio web, el módulo **Instituciones articuladas** contiene:

1. Visualización del listado de Instituciones articuladas
2. Acciones para instituciones creadas
3. Botón para registrar una nueva institución articulada



El panel administrativo muestra todos los módulos del sitio web, el módulo **Puertas** contiene:

1. Visualización del listado de puertas
2. Botón para crear una nueva puerta



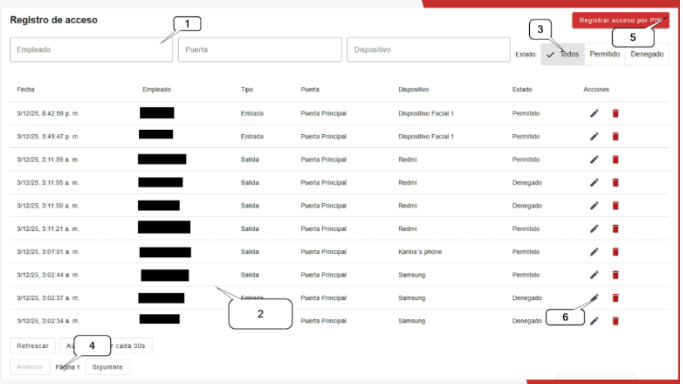
El panel administrativo muestra todos los módulos del sitio web, el módulo **Empresas externas** contiene:

1. Visualización del listado de empresas externas
2. Botón para registrar una nueva empresa externa

USUARIO: ADMINISTRADOR DISPOSITIVOS

El panel administrativo muestra todos los módulos del sitio web, el módulo **Registro de acceso** contiene:

1. Barras de búsqueda de empleados
2. Visualización del listado de empleados registrados
3. Filtros de visualización
4. Botones de paginación
5. Botón de registrar acceso por PIN
6. Acciones de empleados registrados



ECU 911 SERVICIO INTEGRADO DE SEGURIDAD

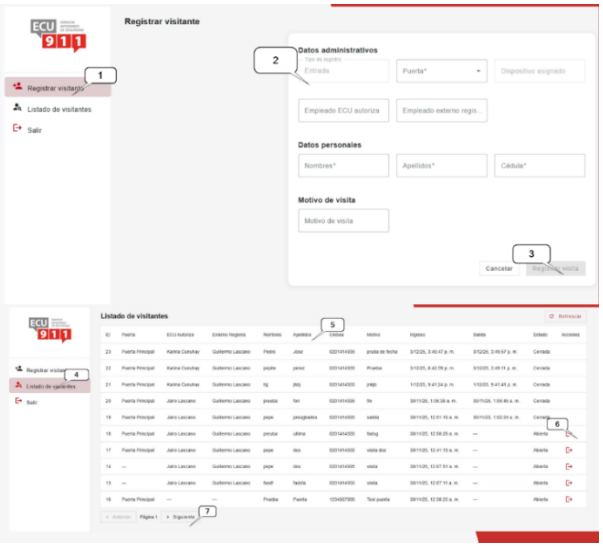
SISTEMA DE IDENTIFICACION BIOMÉTRICA PARA EL CONTROL DE INGRESO DEL PERSONAL EN LAS INSTALACIONES DE LA COORDINACION ZONAL 3 DEL SERVICIO INTEGRADO DE SEGURIDAD ECU911

MANUAL DE USUARIOS

USUARIO: GUARDIA

USUARIO: GUARDIA

1. El módulo **Registrar visitantes** contiene:
2. Formulario de ingreso de datos del visitante
3. Botón "Guardar" visitante
4. El módulo **Listado de visitantes** contiene:
5. Visualización del listado de visitantes registrados
6. Registrar salida del viisitante
7. Botones de paginación



ECU 911 SERVICIO INTEGRADO DE SEGURIDAD

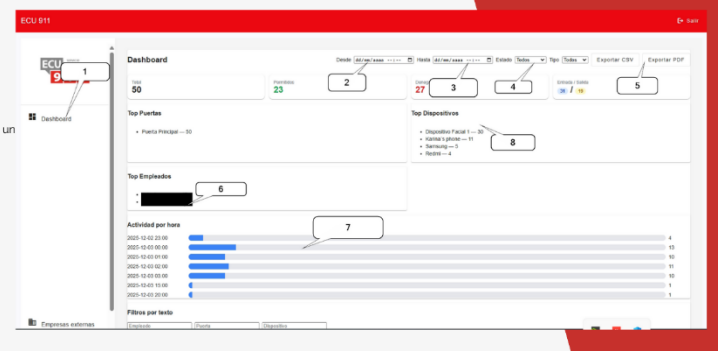
SISTEMA DE IDENTIFICACION BIOMÉTRICA PARA EL CONTROL DE INGRESO DEL PERSONAL EN LAS INSTALACIONES DE LA COORDINACION ZONAL 3 DEL SERVICIO INTEGRADO DE SEGURIDAD ECU911

MANUAL DE USUARIOS

USUARIO: RECURSOS HUMANOS

USUARIO: RECURSOS HUMANOS

1. El módulo **Dashboard** contiene:
2. Filtro para visualización de ingresos y salidas en un intervalo de fechas.
3. Filtro para visualización de ingresos y salidas en un intervalo de fechas.
4. Filtro para visualización por estado y tipo.
5. Botones de exportación en formatos CSV y PDF
6. Muestra el top 5 de empleados mas registrados.
7. Visualización gráfica de actividad por horas.



Anexo B. Instalación de dispositivos biométricos.



