DISEÑO Y DESARROLLO DE UN PROTOTIPO FUNCIONAL DE SISTEMA DE IDENTIFICACIÓN Y CONTROL DE ACCESO PEATONAL A LAS INSTALACIONES EN LA UNIVERSIDAD INTERNACIONAL DEL TRÓPICO AMERICANO

HAROLD STIVEN GUTIERREZ ORDUZ
DIDIER ANTONIO NIÑO GONZALEZ

UNIVERSIDAD INTERNACIONAL DEL TRÓPICO AMERICANO - UNITRÓPICO

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA DE SISTEMAS

YOPAL

2026

DISEÑO Y DESARROLLO DE UN PROTOTIPO FUNCIONAL DE SISTEMA DE IDENTIFICACIÓN Y CONTROL DE ACCESO PEATONAL A LAS INSTALACIONES EN LA UNIVERSIDAD INTERNACIONAL DEL TRÓPICO AMERICANO

HAROLD STIVEN GUTIERREZ ORDUZ
DIDIER ANTONIO NIÑO GONZALEZ

Proyecto presentado para optar por el título de

INGENIERO DE SISTEMAS

Tutor

ING. JUAN CARLOS FONSECA

UNIVERSIDAD INTERNACIONAL DEL TRÓPICO AMERICANO - UNITRÓPICO

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA DE SISTEMAS

YOPAL

2026

Dedicatoria

Dedicamos este proyecto de grado a nuestras familias y amigos, quienes han sido un pilar fundamental en nuestro proceso de formación profesional. Su apoyo incondicional, confianza y motivación constante nos permitieron afrontar cada desafío y perseverar hasta alcanzar esta meta. De igual manera, este logro está dedicado a todas las personas que, con sus enseñanzas, consejos y palabras de aliento, contribuyeron a nuestro crecimiento personal y académico, dejando huellas significativas en este camino. Este trabajo representa no solo el resultado de nuestro esfuerzo, dedicación y compromiso, sino también el reflejo del respaldo y la confianza de quienes creyeron en nosotros y nos acompañaron durante esta importante etapa de nuestras vidas.

Agradecimientos

Expresamos nuestro más sincero agradecimiento a Dios, a nuestras familias por su apoyo incondicional, a nuestro director de proyecto por su orientación y acompañamiento, y a la Universidad Internacional del Trópico Americano, por brindarnos los conocimientos y herramientas necesarias para nuestra formación profesional y agradecemos a todas las personas que contribuyeron directa o indirectamente al desarrollo de este proyecto de grado.

CONTENIDO

GLOSARIO 13
RESUMEN 18
ABSTRACT 19
1 INTRODUCCIÓN 20
2 PLANTEAMIENTO DEL PROBLEMA 21
2.1 FORMULACIÓN 25
3 JUSTIFICACIÓN 26
3.1 Justificación Social 26
3.2 Justificación Tecnológica 26
3.3 Justificación Académica 27
3.4 Justificación institucional 27
4 DELIMITACIÓN 29
4.1 Delimitación espacial 29
4.2 Delimitación cronológica 29
4.3 Delimitación de recursos 30
4.3.1 Recursos Tecnológicos Hardware. 30
4.3.2 Recursos Tecnológicos Software. 30
4.4 Delimitación de alcance 31
5 ESTADO DEL ARTE 36
5.1 Sistemas de Reconocimiento Facial con Inteligencia Artificial 38
6 OBJETIVOS 43
6.1 OBJETIVO GENERAL 43
6.2 OBJETIVOS ESPECÍFICOS 43
7 MARCO REFERENCIAL 44
7.1 Marco teórico o conceptual 44
7.1.1 Inteligencia Artificial 44
7.1.2 Reconocimiento Facial 44
7.1.3 Redes Neuronales Convolucionales y Embeddings Faciales 44
7.1.4 Arquitectura MVC y API REST 45
7.1.5 Código QR 45
7.1.6 Base de datos 46

7.1.7 Control de asistencia 46
7.1.8 Autenticación. 47
7.1.9 Token de acceso. 48
7.1.10 Sistemas de Información. 48
7.1.11 API 49
7.1.12 Frontend 50
7.1.13 Backend 50
7.1.14 Liveness Detection 51
7.1.15 Anti-Spoofing 51
7.1.16 InsightFace y Modelo Buffalo_L 51
7.1.17 MediaPipe y FaceLandmarker 53
7.1.18 Eye Aspect Ratio (EAR) y detección de parpadeo 53
7.1.19 Métricas de evaluación biométrica 54
7.2 Marco Demográfico 55
7.3 Marco Geográfico 55
7.4 Marco Histórico 56
7.5 Marco legal 56
7.6 Marco Institucional 58
8 METODOLOGÍA 59
8.1 Metodología de investigación 59
8.2 Metodología de desarrollo 60
8.3 Diseño de la Investigación 61
8.4 Población y Muestra 62
8.5 Selección de la muestra 62
8.6 Técnica e instrumentos de recolección de datos 64
8.6.1 Observación Directa: 64
8.6.2 Entrevistas: 69
8.6.3 Revisión documental: 72
8.6.4 Encuesta 73
8.7 Evaluación del sistema mediante Evaluation Harness 82
8.7.1 Dataset utilizado: Labeled Faces in the Wild (LFW) 83
8.7.2 Tratamiento y preprocesamiento de las imágenes del dataset 83
8.7.3 Configuración y ejecución del harness 89
8.8 Dispositivos utilizados en las pruebas de reconocimiento facial 90

8.9 Planificación y gestión de requerimientos ágiles 95
8.9.1 Historias de Usuario XP 95
8.9.2 Criterios de Aceptación 95
8.9.3 Pruebas de Aceptación 96
8.9.4 Estructura de Historias de Usuario, Criterios y Backlog 96
8.10 Diseño de mockups. 113
8.10.1 Herramientas y metodología 114
8.10.2 Mockups del proyecto 114
8.10.3 Pantalla de inicio de sesión 114
8.10.4 Mockup de la pantalla de inicio de sesión. 114
8.10.5 Pantalla Crear Usuario 115
8.10.6 Mockup Crear Usuario 115
8.10.7 Pantalla Eliminar Cuenta 116
8.10.8 Mockup de la pantalla Eliminar Cuenta. 116
8.10.9 Pantalla Escanear QR 116
8.10.10 Mockup de la pantalla Escanear QR. 117
8.10.11 Pantalla Estado de Usuario (Activo/Inactivo) 117
8.10.12 Mockup de pantalla Estado de Usuario 117
8.10.13 Pantalla Actualizar Información 118
8.10.14 Mockup de la pantalla Actualizar Información. 118
8.10.15 Pantalla Lista de Usuarios 118
8.10.16 Mockup de la pantalla Lista de Usuarios. 119
8.10.17 Pantalla Dashboard Estadísticas y Datos 119
8.10.18 Mockup de la pantalla Dashboard. 120
8.10.19 Pantalla de escaneo facial 120
8.10.20 Mockup escaneo facial 120
8.10.21 Pantalla de resultado Acceso concedido / Acceso denegado 121
8.10.22 Mockup acceso concedido 121
8.10.23 Mockup acceso denegado 122
8.10.24 Pantalla de registro 123
8.10.25 Mockup crear nuevo usuario 123
8.11 Diseño del sistema 130
9 RESULTADOS 132
9.1 Introducción 132

9.2 Descripción del prototipo 132
9.3 Resultados de la evaluación del reconocimiento facial .....**¡Error! Marcador no definido.**
9.3.1 Resumen de métricas por threshold .....**¡Error! Marcador no definido.**
9.4 Análisis e interpretación de resultados.....**¡Error! Marcador no definido.**
9.4.1 Threshold recomendado y justificación técnica .....**¡Error! Marcador no definido.**
9.5 Pruebas de alcance del reconocimiento facial por dispositivo 155
10 IMPACTOS 158
10.1 Impacto institucional 158
10.2 Impacto académico 158
10.3 Impacto tecnológico 159
10.4 Impacto organizacional y en la gestión de la información 159
10.5 Alcance del impacto 159
11 CRONOGRAMA DE ACTIVIDADES 161
12 PRESUPUESTO 161
13 BIBLIOGRAFÍA 164
14 ANEXOS 168

LISTA DE TABLAS

Pág.

Tabla 1. Matriz de riesgos..... 32
Tabla 2. Comparativo de trabajos relacionados IA. 41
Tabla 3. Comparativo de trabajos relacionados QR. 42
Tabla 4. Promedio de los dos días de observación directa..... 65
Tabla 5. Backlog de tareas, Inicio de sesión..... 97
Tabla 6. Backlog de tareas, Ver información general. 98
Tabla 7. Backlog de tareas, Crear y gestionar vigilantes. 100
Tabla 8. Backlog de tareas, Registro de usuario. 101
Tabla 9. Backlog de tareas, Dashboard de estadísticas. 102
Tabla 10. Backlog de tareas, Ver datos de ingreso y salida. 104
Tabla 11. Backlog de tareas – Editar datos de usuario y rol. 105
Tabla 12. Backlog de tareas, Comparativo histórico de acceso. 106
Tabla 13. Backlog de tareas, Reporte de personas vs afuera. 107
Tabla 14. Backlog de tareas, Ver personas dentro actualmente. 108
Tabla 15. Backlog de tareas, Registrar salida. 109
Tabla 16. Backlog de tareas, Escanear QR. 110
Tabla 17. Backlog de tareas, Verificar acceso mediante reconocimiento facial..... 111
Tabla 18. Backlog de tareas, Registrar rostro biométrico de un usuario..... 113

Tabla 19. Requisitos Funcionales. 123
Tabla 20. Requisitos No Funcionales. 125
Tabla 21. Diagrama de Fases. 126
Tabla 22. Resumen de métricas por threshold Fase 2 149
Tabla 23. Presupuesto. 162

LISTA DE FIGURAS

Pág.

Figura 1. Entrada peatonal campus universitario 21
Figura 2. Campus Universitario 29
Figura 3. Proceso de desarrollo de la metodología XP 60
Figura 4. Minuta de registro de la entrada peatonal 65
Figura 5. Usuarios en fila en el punto de acceso peatonal durante registro manual. ... 66
Figura 6. Estudiante registrándose en la minuta de ingreso. 67
Figura 7. Registro manual en el punto de acceso. 67
Figura 8. Puesto de control de salida sin recursos tecnológicos de apoyo. 68
Figura 9. Flujo de personas en el corredor principal de acceso durante hora pico. 68
Figura 10. Diagrama de Secuencias. 130
Figura 11. Modelo Entidad Relación 131
Figura 12. Login 133
Figura 13. Panel del celador 133
Figura 14. Escaneo del Reconocimiento Facial 134
Figura 15. Confirmación del Escaneo del Reconocimiento Facial 135
Figura 16. Manejo de error en el reconocimiento facial 135
Figura 17. Confirmación exitosa del reconocimiento facial con gafas 136
Figura 18. Reconocimiento facial exitoso con gafas oscuras 137
Figura 19. Reconocimiento facial exitoso con gorra 138
Figura 20. Clasificación de permisos usuario. 138
Figura 21. Clasificación de permisos administrador. 138
Figura 22. Clasificación de permisos celador. 139
Figura 23. Consulta de usuario de Administrador. 139
Figura 24. Consulta de usuario de Celador. 139
Figura 25. Visualización de tarjeta usuario. 140
Figura 26. Módulo de escaneo QR 140
Figura 27. Módulo de Confirmación 141
Figura 28. Historial de registros de usuarios. 142
Figura 29. Directorio de usuarios 142
Figura 30. Comportamiento del sistema de reconocimiento facial por umbral 145
Figura 31. Proyección bidimensional de los embeddings faciales 146
Figura 32. Visualización del embedding facial del Usuario 1 148
Figura 33. Mapa PCA 2D con su interpretación 154
Figura 34. Cronograma de actividades 161

LISTA DE CUADROS

pág.

Cuadro 1. Historia de Usuario Inicio de sesión. 96
Cuadro 2. Historia de usuario, Ver información general. 98
Cuadro 3. Historia de usuario, Crear y gestionar vigilante. 99
Cuadro 4. Historia de usuario, Registro usuario. 100
Cuadro 5. Historia de usuario, Dashboard de estadísticas. 101
Cuadro 6. Historia de usuario, ver datos de ingreso y salida. 103
Cuadro 7. Historia de usuario, Editar datos de usuario y rol. 104
Cuadro 8. Historia de usuario, Comparativo histórico de acceso 105
Cuadro 9. Historia de usuario, Reporte de personas dentro vs afuera. 106
Cuadro 10. Historia de usuario, Ver personas dentro actualmente. 107
Cuadro 11. Historia de usuario, Registrar salida. 108
Cuadro 12. Historia de usuario, Escanear QR 109
Cuadro 13. Historia de usuario, Verificar acceso mediante reconocimiento facial 110
Cuadro 14. Historia de usuario, Registrar rostro biométrico de un usuario 112

LISTA DE ANEXOS

pág.

Anexo A. Guía de entrevista semiestructurada 168
Anexo B. Cuestionario de encuesta. 169
Anexo C. Formato consentimiento informado para tratamiento de datos biométricos 171
Anexo D. Entrevista a Jefe del Departamento de Sistemas 175
Anexo E. Entrevista Vigilante No. 01 178
Anexo F. Entrevista Vigilante No. 02 179
Anexo G. Entrevista Vigilante No. 03 181

GLOSARIO

A

API: Conjunto de reglas y definiciones que permiten que diferentes sistemas o aplicaciones se comuniquen entre sí.

Aplicativo web: Herramienta desarrollada en un lenguaje de programación que permite acceder a un servidor web mediante internet, que está soportado por los navegadores en donde se ejecute.

ArcFace: Algoritmo de reconocimiento facial basado en redes neuronales profundas que utiliza una función de pérdida de margen angular aditivo para mejorar la discriminación entre identidades. Es el modelo de reconocimiento utilizado por el paquete Buffalo_L de InsightFace.

B

Base de Datos: Sistema organizado de almacenamiento de información que permite la gestión eficiente de datos estructurados para su consulta y análisis.

Biometría: Conjunto de técnicas que utilizan características físicas o de comportamiento para identificar a una persona.

C

Cámara web: Es un dispositivo digital que permite tomar fotografías o imágenes en tiempo real. Estas se usan para diferentes situaciones, desde vigilar un establecimiento hasta videollamadas.

Código QR: Código de barras bidimensional que almacena información y puede ser escaneado por dispositivos móviles o lectores especializados.

Control de Acceso: Mecanismo de seguridad que regula la entrada y salida de personas en instalaciones mediante credenciales de identificación.

D

Desarrollo Ágil: Metodología de programación que prioriza la entrega rápida de software funcional y la mejora basada en la retroalimentación del usuario.

E

Encriptación: Técnica utilizada para proteger datos mediante algoritmos que convierten la información en un formato ilegible sin la clave de descifrado.

Escaneo Biométrico: Tecnología que permite la autenticación de identidad mediante características físicas únicas, como huellas dactilares o reconocimiento facial.

Embedding: Vector numérico de alta dimensionalidad que representa matemáticamente las características únicas de un rostro. En el presente sistema, cada rostro enrolado genera un embedding de 512 dimensiones que es almacenado en la base de datos para su posterior comparación.

F

Frontend: Parte visible de una aplicación web o móvil con la que interactúan los usuarios, generalmente desarrollada con tecnologías como HTML, CSS y JavaScript.

FMR (False Match Rate): Tasa de falsa coincidencia. Proporción de comparaciones entre personas diferentes que el sistema identifica incorrectamente como la misma persona. También conocida como FAR (False Acceptance Rate).

FNMR (False Non-Match Rate): Tasa de falsa no coincidencia. Proporción de comparaciones entre imágenes de la misma persona que el sistema no logra identificar correctamente como coincidentes. También conocida como FRR (False Rejection Rate).

I

Identificación Digital: Proceso mediante el cual se verifica la identidad de una persona utilizando medios electrónicos o digitales.

Interfaz de Usuario: Diseño gráfico y elementos visuales con los que interactúa un usuario en una aplicación o sistema.

InsightFace: Librería de código abierto especializada en análisis facial que integra detección, reconocimiento y extracción de atributos faciales. En el presente sistema se utilizó el modelo Buffalo_L de esta librería para la extracción de embeddings faciales.

L

Lector QR: Dispositivo o software capaz de interpretar códigos QR para acceder a la información almacenada en ellos.

M

Machine Learning: Rama de la inteligencia artificial que permite a los sistemas aprender y mejorar automáticamente a partir de datos sin ser programados explícitamente.

MongoDB: Base de datos NoSQL utilizada para el almacenamiento y gestión eficiente de grandes volúmenes de datos.

Middleware: Software que conecta aplicaciones y sistemas, facilitando la comunicación entre el sistema de control de acceso y la base de datos.

P

Python: Lenguaje de programación utilizado en el desarrollo de software, especialmente en análisis de datos, inteligencia artificial y backend de aplicaciones web.

Programación Extrema XP: Metodología de desarrollo ágil que se enfoca en la entrega continua de software de alta calidad mediante pruebas constantes y colaboración en equipo.

Prototipo: Es la puesta en marcha del primer diseño, construcción e implementación de un software. Generalmente el prototipo es la base donde se hacen gran número de pruebas para entregar un proyecto finalizado.

R

Reconocimiento Facial: Tecnología de identificación biométrica que analiza las características del rostro para autenticar a una persona.

S

Seguridad Informática: Conjunto de medidas y tecnologías destinadas a proteger sistemas y datos contra accesos no autorizados, fraudes o ataques cibernéticos.

Software de Gestión: Aplicación informática utilizada para administrar procesos, en este caso, el control de acceso y la identificación de usuarios.

Sistema de Control de Asistencia: Herramienta utilizada para registrar y gestionar la presencia de personas en una instalación mediante identificación digital.

T

Token de Seguridad: Clave digital generada para autenticar a un usuario en un sistema y garantizar transacciones seguras.

Threshold: Umbral numérico utilizado en sistemas de reconocimiento facial para determinar si dos embeddings corresponden a la misma persona. Si la similitud de coseno entre dos embeddings supera el threshold configurado, el sistema concede el acceso; de lo contrario, lo deniega.

U

Unitrópico: Universidad Internacional del Trópico Americano, institución en la que se implementará el sistema de identificación digital.

Usabilidad: Grado de facilidad y eficiencia con el que los usuarios pueden interactuar con una aplicación o sistema.

V

Validación de Datos: Proceso que verifica la exactitud y coherencia de la información ingresada en un sistema.

W

Wi-Fi: Tecnología inalámbrica que permite la conexión de dispositivos a internet y a redes locales sin necesidad de cables.

Z

Zonas de Acceso: Áreas delimitadas dentro de una institución que requieren credenciales específicas para ingresar, reforzando la seguridad.

RESUMEN

El presente documento describe el diseño y desarrollo de un prototipo funcional de un sistema integrado de identificación y control de acceso para la Universidad Internacional del Trópico Americano, orientado a fortalecer los procesos de ingreso y salida de la comunidad universitaria. El objetivo general es diseñar una solución tecnológica orientada a automatizar los métodos manuales tradicionales, como registros en papel y verificación visual de carnés, mediante una plataforma centralizada que busca automatizar el registro y mejorar la trazabilidad institucional. El proyecto contempla la incorporación de tecnologías de verificación orientadas a fortalecer la eficiencia y seguridad en el control de acceso. La solución se estructura bajo una arquitectura modelo vista controlador (MVC) y se desarrolla con la metodología ágil de Programación Extrema (XP), apoyada en un enfoque de investigación cuantitativo. Como resultado, se plantea un proceso de ingreso más seguro y organizado, alineado con las nuevas tecnologías y con capacidad, a nivel de prototipo, para generar estadísticas en tiempo real que, en una futura implementación, podrían facilitar la toma de decisiones y el seguimiento de usuarios dentro del campus.

Palabras clave: Control de acceso, inteligencia artificial, aplicativo web, programación extrema, tecnología.

ABSTRACT

This document describes the design and development of a functional prototype of an integrated identification and access control system for the Universidad Internacional del Trópico Americano, aimed at strengthening entry and exit processes for the university community. The overall objective is to design a technological solution focused on automating traditional manual methods, such as paper-based logs and visual ID card verification, through a centralized platform that seeks to automate record-keeping and improve institutional traceability. The project includes the incorporation of verification technologies aimed at strengthening efficiency and security in access control. The solution is structured under a model-view-controller (MVC) architecture and is developed using the Extreme Programming (XP) agile methodology, supported by a mixed research approach. As a result, a safer and more organized entry process is proposed, aligned with new technologies and capable, at the prototype level, of generating real-time statistics that, in a future implementation, could facilitate decision-making and user tracking within the campus.

Keywords: Access control, artificial intelligence, web application, extreme programming, technology.

1 INTRODUCCIÓN

La optimización de procesos y la mejora continua son elementos cruciales para proporcionar una experiencia educativa de calidad, uno de los desafíos identificados en la Universidad Internacional del Trópico Americano, a partir de la observación directa y el análisis del proceso actual, se relaciona con el proceso de ingreso y salida en sus instalaciones, donde actualmente se utiliza un sistema de control de acceso basado en carnets físicos y verificación manual por parte del personal de vigilancia.

El sistema de identificación actualmente implementado presenta diversas limitaciones, ya que es vulnerable, poco eficiente dependiendo de procesos manuales y no permite un registro automatizado de quién ingresa, a qué hora y por cuánto tiempo permanece en las instalaciones. La permanencia del sistema actual podría generar inconsistencias en el registro de accesos, al basarse en procesos manuales que limitan la trazabilidad de la información, incrementan el riesgo de pérdida de datos y dificultan su integración con tecnologías modernas.

El presente documento aborda esta problemática desarrollando un prototipo funcional de sistema que integra el reconocimiento facial con Inteligencia Artificial como mecanismo de identificación, complementado con el escaneo del código QR del carnet institucional como alternativa de verificación ante situaciones en las que las condiciones de captura no permitan completar el proceso de identificación biométrica. Esta combinación busca ofrecer una solución robusta y escalable, orientada a automatizar el registro de accesos y a proporcionar, en una futura implementación, datos estadísticos y de trazabilidad en tiempo real a la institución.

Investigaciones recientes demuestran que los sistemas de reconocimiento facial alcanzan precisiones superiores al 96% en condiciones reales (Chavez Vargas, 2025), y que la implementación de sistemas QR en instituciones educativas reduce el tiempo de registro hasta en un 85.5% (Palomino Sulca, 2023), estas tecnologías representan una solución integral para las necesidades identificadas en Unitrópico.

2 PLANTEAMIENTO DEL PROBLEMA

La comunidad universitaria presenta una dificultad relacionada con la identificación y el control de acceso a las instalaciones. El ingreso de los usuarios se ve comprometido por la falta de rigurosidad en los procedimientos de verificación de identidad al acceder al campus. A partir de un ejercicio de observación directa realizado entre el 15 y el 30 de abril de 2025, así como durante el inicio del periodo académico del año 2026 en el punto de acceso peatonal principal ubicado en la Carrera 19 No. 39 - 40, se evidenció que cualquier individuo podría ingresar proporcionando información falsa en el formulario de registro, sin que el personal de vigilancia realizara una verificación rigurosa de identidad, lo que representa un riesgo para la seguridad e integridad de la comunidad universitaria.

Figura 1. Entrada peatonal campus universitario



Nota: Imagen tomada de la página Unitropico (2025),

https://unitropico.edu.co/

Un caso reciente ocurrido en Yopal, Casanare, reportado por la prensa local, narra cómo un individuo, la mañana del 16 de julio de 2024, se identificó con credenciales falsas y logró sustraer tres dispositivos móviles de gama alta dentro de la Universidad Internacional del Trópico Americano mediante métodos convincentes de engaño. Este tipo de situaciones evidencia la vulnerabilidad de los actuales procesos de control de acceso y refuerza la necesidad de implementar soluciones tecnológicas que permitan validar la identidad de quienes ingresan a las instalaciones (John Navarrete, 2024).

El sistema de identificación actualmente implementado presenta diversas limitaciones confirmadas a través de entrevistas semiestructuradas realizadas al personal de vigilancia de la empresa Binarios, contratada por la institución. La principal dificultad identificada radica en que los estudiantes no portan el carnet como lo exige la norma, lo que obliga a recurrir a una minuta de registro manual como mecanismo alternativo de ingreso (**Anexo E.** Entrevista Vigilante No. 01 y **Anexo F.** Entrevista Vigilante No. 02). Este mecanismo resulta insuficiente para garantizar la trazabilidad de

los accesos, dado que registrar en un libro a miles de personas hace imposible contar con una hora precisa de ingreso (**Anexo F.** Entrevista Vigilante No. 02). Esta situación se ve agravada por la falta de consenso entre el mismo personal de seguridad respecto a las capacidades reales del sistema: mientras un vigilante considera que la minuta permite conocer con precisión quién ingresó y a qué hora, otro reconoce abiertamente que dicha precisión no es posible sin automatización (**Anexo F.** Entrevista Vigilante No. 02 y **Anexo G.** Entrevista Vigilante No. 03), lo que evidencia una falta de estandarización en los procedimientos de control de acceso.

Los métodos tradicionales de seguimiento de asistencia, como las hojas de registro manuales o los sistemas de código de barras y RFID, están plagados de diversas limitaciones que obstaculizan la eficiencia y precisión del proceso. Uno de los problemas clave es la inexactitud y la naturaleza propensa a errores de la toma manual de asistencia, donde errores humanos como registros omitidos, asistencia por terceros y errores de transcripción pueden llevar a registros de asistencia poco fiables. Además, la falta de accesibilidad a datos en tiempo real en los registros en papel y sistemas estáticos dificulta que los administradores obtengan visibilidad inmediata de los datos de asistencia y respondan rápidamente a los problemas (Shruthi et al., 2024). Esta realidad coincide con lo identificado en Unitrópico, donde el personal de vigilancia confirma que, ante la ausencia de un sistema automatizado, no es posible conocer en tiempo real cuántas personas se encuentran dentro de las instalaciones, lo que representa un riesgo crítico especialmente en situaciones de emergencia o evacuación (**Anexo F.** Entrevista Vigilante No. 02).

Los Sistemas de Información tienen una enorme importancia en el incremento de la capacidad organizacional frente al cambio del entorno, siendo una necesidad actual el tomar decisiones en poco tiempo para poder hacer frente a la agresividad de este, lo cual hace necesario la inmediatez de la información procesada con una gran dosis de veracidad (Alvarado et al., 2018). De acuerdo con los lineamientos del Ministerio de Educación, las universidades necesitan implementar un sistema de aseguramiento de la calidad en los servicios educativos ofrecidos. Para lograr esto, deben desarrollar un sistema de evaluación de la calidad de los programas respaldado por sistemas de información internos que permita generar datos de calidad (Jaramillo Alberto, 2018). En este contexto, el personal de seguridad entrevistado señala que la institución no provee ningún apoyo tecnológico y que el sistema actual responde únicamente a los requerimientos mínimos establecidos entre la universidad y la empresa de seguridad (**Anexo F.** Entrevista Vigilante No. 02 y **Anexo G.** Entrevista Vigilante No. 03).

Para llevar un control de acceso efectivo, se dificulta la identificación precisa de quienes se encuentran en el campus en un momento dado, por lo cual se requiere una solución que aproveche las nuevas tecnologías como una herramienta versátil que no solo identifique a los usuarios, sino que también brinde beneficios adicionales (Martinez Renteria & Florez Burgos, 2023).

Los métodos digitales de identificación ofrecen una serie de ventajas sobre el proceso manual actual, por lo que el presente proyecto, a través del prototipo desarrollado, aborda tres puntos clave. En primer lugar, integra tecnologías actuales como la inteligencia artificial para la validación y veracidad de la identidad del usuario en el momento del ingreso. En segundo lugar, centraliza la información del titular en un único

lugar, facilitando su gestión y actualización. En tercer lugar, contempla la capacidad de almacenar un mayor volumen de información, lo que posibilitaría un mayor nivel de verificación de identidad y trazabilidad institucional en una futura implementación.

2.1 FORMULACIÓN

¿Cómo diseñar y desarrollar un prototipo funcional de un sistema de identificación y control de acceso, basado en reconocimiento de personas, que permita automatizar y mejorar la trazabilidad del ingreso a las instalaciones de la Universidad Internacional del Trópico Americano?

3 JUSTIFICACIÓN

3.1 Justificación Social

En Colombia, algunas instituciones de educación superior no cuentan con sistemas automatizados de control de acceso a sus instalaciones, lo que impide conocer en tiempo real quién se encuentra dentro del campus, dificulta la trazabilidad de los ingresos y limita la capacidad institucional para tomar decisiones oportunas sobre la seguridad y la gestión del espacio universitario (Ortiz Cuadros, 2018) .

Las falencias expuestas anteriormente, podrían generar insatisfacción en la comunidad académica y una gestión inadecuada de los procesos de ingreso y salida de estudiantes, docentes, administrativos, egresados.

3.2 Justificación Tecnológica

La Universidad Internacional del Trópico Americano presenta un sistema de control de acceso basado en la verificación visual de la credencial del usuario y el registro manual de visitantes en una lista de papel, que presenta deficiencias relacionadas con la trazabilidad, la consulta de información histórica, la disponibilidad de datos en tiempo real y la generación de reportes institucionales.

De igual manera, la ausencia de un sistema digital y centralizado de control de acceso expone a la institución a riesgos continuos de personas no autorizadas y limita la disponibilidad de información confiable para la toma de decisiones, ya que al contar con un sistema que registre y supervise el ingreso de personas es una necesidad inmediata que permitirá mejorar la trazabilidad y contribuir a un entorno universitario más protegido y organizado.

Por esta razón, el desarrollo de una herramienta de control de acceso se plantea como una alternativa tecnológica que permitiría optimizar dichos procesos y aportar beneficios significativos a la institución. Entre estos beneficios se destaca la posibilidad de llevar un control de acceso más riguroso, en el cual se valide la identidad del usuario mediante herramientas digitales actuales como el reconocimiento facial basado en Inteligencia Artificial, complementado con el escaneo de código QR institucional como mecanismo de verificación.

3.3 Justificación Académica

El desarrollo de este proyecto permite aplicar de manera práctica los conocimientos adquiridos durante la formación en el programa de Ingeniería de Sistemas, especialmente en áreas como desarrollo de software, bases de datos, desarrollo web, inteligencia artificial y visión por computador. De igual manera, permite integrar conocimientos de ingeniería de software e inteligencia artificial en el desarrollo de una solución funcional orientada a la validación facial de usuarios. Su realización implica aplicar procesos de análisis de requerimientos, diseño de arquitectura, modelado del sistema, construcción de servicios, pruebas funcionales, fortaleciendo competencias técnicas y metodológicas propias del perfil profesional.

3.4 Justificación institucional

La alineación del proyecto con los objetivos estratégicos de la universidad podría contribuir al fortalecimiento de su reputación institucional. De igual manera, se relaciona con la visión y misión de Unitrópico, orientadas a generar un ambiente educativo excepcional, seguro y eficiente, promoviendo la investigación científica y el desarrollo tecnológico (*Misión Visión*, 2021). En este sentido, una futura implementación del

sistema podría respaldar la misión de proporcionar educación de calidad y contribuir a un ambiente de aprendizaje óptimo, además de reforzar la imagen de la universidad como una institución comprometida con la innovación, lo cual podría incrementar la satisfacción de la comunidad universitaria y su sentido de pertenencia.

4 DELIMITACIÓN

4.1 Delimitación espacial

El proyecto se desarrolla solamente en la sede principal de la Universidad Internacional del Trópico Americano, ubicada en la Carrera 19 No. 39 - 40 de la ciudad de Yopal, Casanare. El desarrollo se enfoca en el punto de acceso peatonal principal de dicha sede, abarcando a toda la comunidad universitaria: estudiantes, docentes, administrativos y egresados.

Figura 2. Campus Universitario



Nota: Imagen tomada de https://unitropico.edu.co/

4.2 Delimitación cronológica

En cuanto al tiempo, el proyecto tiene una duración aproximada de 4 meses, comprendida entre el 11 de mayo de 2026 y el 23 de agosto de 2026. Durante este período, se llevan a cabo todas las actividades de análisis, desarrollo, pruebas y entrega del sistema de control de acceso.

4.3 Delimitación de recursos

4.3.1 Recursos Tecnológicos Hardware.

El desarrollo del sistema se realiza utilizando equipos de cómputo personales, sin adquisición de hardware especializado. Se adquieren cámaras digitales, lector QR y escáner, además de contar con los equipos que administran el sistema de control de acceso. Para garantizar una conexión a internet, se cuenta con los dispositivos básicos de red como enrutadores, repetidores o puntos de acceso, el cableado correspondiente y un servicio de internet estable proporcionado por un operador.

4.3.2 Recursos Tecnológicos Software.

Se emplean herramientas de software de uso libre, tales como lenguajes y frameworks para el desarrollo web: JavaScript, Node.js y React. Así mismo, se utilizan sistemas gestores de bases de datos, principalmente MongoDB Atlas, y plataformas de control de versiones Git/GitHub. Para la creación del microservicio correspondiente al apartado de reconocimiento facial, se integran tecnologías basadas en inteligencia artificial orientadas al procesamiento y análisis de imágenes, con el fin de soportar procesos de verificación automatizada de identidad mediante reconocimiento de características faciales.

En la primera versión del desarrollo, la cual constituye el entregable del proyecto, se utilizan recursos internos disponibles, lo que implica el uso de una cámara como sensor principal en el módulo de inteligencia artificial del sistema de control de ingreso, además de material tecnológico propio.

4.4 Delimitación de alcance

El alcance del proyecto se enfoca en la creación de un prototipo funcional, el cual comprende el análisis, diseño y desarrollo de un aplicativo web para el sistema de control de acceso de personas para Unitrópico, incluyendo los siguientes módulos: módulo de captura facial mediante cámara web para el registro y validación de identidad; módulo de escaneo de código QR institucional como mecanismo complementario de autenticación.

No se incluye el despliegue del sistema en el entorno operativo de la universidad, ni la instalación física en porterías, ni la integración con infraestructura física como talanqueras o dispositivos de entrada, ni la migración de datos reales, ni la integración con plataformas académicas institucionales. Estas son consideradas etapas posteriores, que pueden ser desarrolladas por la institución si decide adoptar la solución tecnológica presentada en este trabajo de grado.

Durante la ejecución del proyecto pueden presentarse diversos riesgos técnicos y operativos asociados a la integración de las tecnologías empleadas. Uno de los principales riesgos corresponde a posibles fallos en el proceso de reconocimiento facial, los cuales pueden verse influenciados por condiciones como la iluminación, el ángulo de captura o la calidad de la imagen, afectando la precisión en la verificación de identidad.

De igual manera, puede existir riesgo de errores en la lectura o validación del código QR, especialmente en casos de baja calidad de impresión, daños en la imagen o fallas en la captura mediante dispositivos móviles. La integración entre los módulos de reconocimiento facial, el escaneo de código QR y la base de datos puede generar inconsistencias en el registro de información si no se gestiona adecuadamente la sincronización de los datos.

Otro riesgo identificado está relacionado con la disponibilidad del sistema, ya que posibles fallas de conectividad o del servidor pueden afectar el acceso en tiempo real a la plataforma y el registro oportuno de los ingresos.

El alcance de este trabajo no contempla la incorporación de mecanismos avanzados de liveness detection o anti-spoofing en el componente de reconocimiento facial. Esta decisión obedece a que el proyecto se orienta al desarrollo de un prototipo funcional enfocado en validar la viabilidad técnica de la solución e integrar los módulos principales de captura facial, autenticación por código QR y registro de accesos. La inclusión de técnicas de liveness detection y prevención de suplantación implica un mayor nivel de complejidad en términos de adquisición de datos, definición de escenarios de ataque, entrenamiento y validación de modelos especializados, así como mayores requerimientos de hardware, tiempo y recursos para su evaluación. Por ello, estas capacidades se consideran una línea de mejora futura que puede incorporarse en etapas posteriores de madurez del sistema, una vez validado el funcionamiento base de la solución.

Tabla 1. Matriz de riesgos

ID	Descripción del riesgo	Probabilidad	Impacto	Severidad (P×I)	Plan de mitigación	Responsable
R1	Iluminación adversa durante la captura facial que afecte la detección o validación del rostro	Alta	Medio	6 (Alta)	Realizar pruebas en diferentes franjas horarias y condiciones de luz; definir recomendaciones mínimas de iluminación para la captura	Equipo de desarrollo

R2	Baja calidad de la imagen capturada por cámara, generando errores en el procesamiento facial	Alta	Alto	9 (Crítica)	Establecer validaciones previas de calidad de imagen, resolución mínima y enfoque; mostrar mensaje de retroalimentación al usuario	Equipo de desarrollo
R3	Conjunto de datos insuficiente o poco representativo para entrenar y evaluar adecuadamente el componente inteligente	Media	Alto	6 (Alta)	Ampliar progresivamente el dataset, incluir variaciones de ángulo, iluminación y distancia; revisar calidad antes del entrenamiento	Equipo de desarrollo
R4	Desempeño del componente inteligente por debajo de las métricas esperadas de precisión y recall	Media	Alto	6 (Alta)	Ajustar parámetros, revisar preprocesamiento, mejorar etiquetado y realizar nuevas iteraciones de validación	Equipo de desarrollo
R5	Errores en el etiquetado del dataset que afecten el entrenamiento y la evaluación del modelo	Media	Medio	4 (Media)	Aplicar revisión manual del etiquetado, muestreo de control de calidad y corrección antes del entrenamiento	Equipo de desarrollo
R6	Indisponibilidad del servidor o fallos del	Baja	Alto	3 (Media)	Mantener copias locales del servicio,	Equipo de desarrollo

	microservicio durante las pruebas del sistema				definir mecanismo de reinicio y reintento, y ejecutar pruebas en entorno controlado	
R7	Fallos en la integración entre el componente inteligente y el microservicio/backend	Media	Alto	6 (Alta)	Realizar pruebas de integración tempranas, definir contratos API claros y validar formatos de entrada y salida	Equipo de desarrollo
R8	Pérdida, corrupción o inconsistencia de registros almacenados durante el desarrollo y las pruebas	Baja	Medio	2 (Baja)	Generar copias de respaldo periódicas, controlar versiones de archivos/datos y validar escritura/lectura de registros	Equipo de desarrollo
R9	Retrasos en el cronograma por subestimación del tiempo requerido para dataset, entrenamiento o integración	Media	Alto	6 (Alta)	Definir hitos semanales, priorizar entregables críticos y mantener seguimiento continuo con ajustes de alcance si es necesario	Estudiante investigador
R10	Uso inadecuado de datos biométricos o ausencia de consentimiento informado para	Baja	Alto	3 (Media)	Aplicar formato de consentimiento informado, limitar el uso a fines	Estudiante investigador / Director

	pruebas con rostros				académicos y restringir el acceso a los datos recolectados	

Nota. Elaboración propia (2026).

5 ESTADO DEL ARTE

La revisión desarrollada se organiza en dos ejes principales: los sistemas de control de acceso mediante códigos QR y los sistemas de reconocimiento facial con Inteligencia Artificial. Para su elaboración, se revisaron estudios en revistas indexadas, repositorios universitarios y conferencias internacionales, con el fin de identificar los avances actuales y las limitaciones que justifican el desarrollo de este proyecto.

En este contexto, el uso de códigos QR como mecanismo de identificación y control de acceso en instituciones educativas ha crecido significativamente, impulsado por la masificación de dispositivos móviles con cámara y la necesidad de reemplazar procesos manuales ineficientes. A continuación, se presentan los trabajos más relevantes en este eje:

Implementaron un sistema de control de asistencia estudiantil mediante carnet virtual con código QR integrado a una plataforma IoT en la Universidad Distrital Francisco José de Caldas de Bogotá. El estudio evidenció que la ausencia de sistemas digitales de control afecta directamente la certificación de calidad exigida por el Ministerio de Educación Nacional colombiano, y propuso la centralización de los registros de acceso como mecanismo de apoyo a los procesos de acreditación institucional. El trabajo validó la viabilidad técnica y operativa del QR como credencial estudiantil en el contexto universitario colombiano, siendo el antecedente nacional más cercano al presente proyecto por institución y normativa aplicable (Llanos Bermudez & Hurtado Pardo, 2021).

Desarrollaron un sistema de control de acceso mediante código QR sobre hardware Raspberry Pi. El sistema generaba códigos QR únicos por usuario, los almacenaba en una base de datos centralizada y los verifica mediante lectura óptica en los puntos de ingreso. El estudio validó la integración de plataformas de bajo costo con lectura QR, aunque identificó como limitación la necesidad de mantener el código a una distancia específica de la cámara por ausencia de autoenfoque en el hardware utilizado (Zertucha González et al., 2022).

Implementó un sistema de registro de usuarios temporales con código QR en una institución privada colombiana, obteniendo una reducción del 85.5% en el tiempo de registro y un aumento del 20.43% en la satisfacción de los usuarios. La investigación empleó una metodología experimental con grupos de control, validando estadísticamente el impacto positivo del QR frente a los métodos manuales (Palomino Sulca, 2023). Este es el trabajo que reporta la mayor reducción de tiempo en la literatura revisada para sistemas QR educativos, constituyendo un referente cuantitativo clave para los resultados esperados del presente proyecto.

El artículo publicado en la revista Ciencia Latina presentó el diseño y desarrollo de un sistema digital de toma de asistencia estudiantil mediante códigos QR para optimizar procesos de control académico en educación superior. La propuesta se fundamentó en la integración de tecnologías de información aplicadas al ámbito educativo, con énfasis en automatización, trazabilidad de registros y accesibilidad para docentes y estudiantes. El sistema fue prototipado mediante análisis de requerimientos, modelado UML y desarrollo de arquitectura funcional, mostrando que los QR reducen el

tiempo de lista y minimizan errores de transcripción en comparación con los métodos tradicionales (Cano Perfecto et al., 2026)

5.1 Sistemas de Reconocimiento Facial con Inteligencia Artificial

La evolución de los sistemas de reconocimiento facial ha transitado desde métodos clásicos como Eigenfaces y Haar Cascade, utilizados en trabajos como el de (Alfonso Sierra & Castaño Saavedra, 2021) hacia modelos de aprendizaje profundo como ArcFace y FaceNet, que han demostrado precisiones del 96.7% (Elnozahy Seifeldin Liang et al., 2025), 96.92% (Chavez Vargas, 2025) y superiores al 95% (Legarda Delgado & Loaiza Pabon, 2022) en condiciones reales de uso en entornos educativos e institucionales.

Desarrollaron un sistema de control de acceso residencial con Raspberry Pi 3B+ y el algoritmo Eigenfaces (PCA), realizando un análisis comparativo de cinco técnicas: PCA, Gabor Wavelet, SVM, redes neuronales y modelos ocultos de Markov. Sus resultados demostraron la viabilidad técnica del hardware embebido de bajo costo para reconocimiento facial, aunque evidenciaron limitaciones bajo iluminación adversa y en ángulos extremos que los trabajos posteriores buscaron superar. Es el primer antecedente colombiano identificado en control de acceso biométrico con hardware de bajo costo (Alfonso Sierra & Castaño Saavedra, 2021).

Publicaron en la revista indexada Paideia XXI (Redalyc) el artículo 'Sistema de reconocimiento facial para el control de accesos mediante Inteligencia Artificial', cuyo objetivo fue desarrollar un sistema que permitiera el reconocimiento facial para control de accesos usando Redes Neuronales Convolucionales como algoritmo principal. El

sistema fue implementado con Python y OpenCV, demostrando que las CNN superan a los clasificadores clásicos en entornos con variaciones de iluminación y expresión facial. Este trabajo es relevante porque es una publicación en revista científica indexada en Redalyc con enfoque específico en control de accesos, lo que lo convierte en una referencia de alto valor académico para el estado del arte (Reyes Campos et al., 2023).

Desarrollaron FR-ARCA, sistema piloto de registro automático de asistencia con arquitectura modular (Docker, FastAPI, Django, REST/MQTT). Evaluaron detectores MTCNN, RetinaFace y SCRFD, y modelos de reconocimiento ArcFace, FaceNet y VGG-Face mediante curvas ROC/AUC y matrices de confusión. Demostraron que las soluciones open source son técnicamente comparables a Amazon Rekognition y Azure Face. Es el antecedente colombiano universitario más completo en términos de arquitectura y evaluación de modelos de aprendizaje profundo aplicados a la asistencia académica (Legarda Delgado & Loaiza Pabon, 2022).

Presentaron en el V Congreso Internacional en Inteligencia Ambiental un sistema de registro de asistencia con Python, OpenCV y face-recognition, almacenando resultados automáticamente en Excel. Las pruebas con tres estudiantes mostraron reconocimiento del 100% en perspectiva frontal, con reconocimiento nulo en vistas laterales por ausencia de imágenes de entrenamiento en esos ángulos. El sistema reconoció usuarios con mascarilla parcial, gorras y lentes, validando robustez ante accesorios faciales (Paredes et al., 2023).

Publicaron en la revista IoT (MDPI, 2025) un sistema de cerradura inteligente con reconocimiento facial sobre Raspberry Pi con 96.7% de precisión global. Integró HOG

con DeepFace, aprendizaje adaptativo sin reentrenamiento y preprocesamiento CLAHE con corrección gamma. Los tiempos de detección promediaron 564 ms y las notificaciones vía TCP tuvieron una latencia de 200 ms. Precisión por condición: 98.5% con luz brillante, 92.8% con poca luz y 92.4% en ángulos estrechos. Es la publicación científica indexada más reciente y técnicamente afín al módulo de IA propuesto (Elnozahy Seifeldin Liang et al., 2025).

Desarrolló una aplicación web (React + FastAPI) para control de asistencia escolar. Evaluó VGG-Face (93.02%, 276.74 s), ArcFace (92.8%, 168.8 s), Dlib (90.83%, 310.12 s) y SFace (89.9%, 51.33 s) con la biblioteca DeepFace, seleccionando ArcFace por su balance óptimo. Logró una reducción del 50.81% en el tiempo del proceso (649.84 s a 319.66 s), con precisión global del 96.92%. La prueba t de Student (p=0.00018) confirmó la mejora estadísticamente significativa. Es el trabajo con mayor rigor metodológico en evaluación de impacto entre los revisados (Chavez Vargas, 2025).

Implementó un sistema de control de acceso educativo con terminal biométrico SenseFace 2A y plataforma web en Firebase. Aportó datos contextuales de UNESCO y BID: más del 60% de centros educativos en países en desarrollo usan métodos manuales y el 55% de instituciones públicas latinoamericanas carecen de plataformas centralizadas. El sistema demostró mejoras en trazabilidad, precisión del registro y eficiencia operativa, con administración por roles y generación de reportes institucionales (Reyes Alcivar, 2026).

Publicaron en esta revista científica un sistema de reconocimiento biométrico facial para control de asistencia de alumnos en centros educativos con visualización de

resultados en dispositivos móviles. El sistema permitió a los alumnos registrar sus marcaciones mediante reconocimiento facial desde sus dispositivos, optimizando el uso de recursos institucionales. Los resultados evidenciaron mejoras en la eficiencia del proceso y en la accesibilidad del sistema para docentes y estudiantes, consolidando la tendencia hacia soluciones móviles en el ámbito educativo latinoamericano (Cardozo Servian & Macen Rojas, 2023).

Desarrollaron un sistema de control de asistencia estudiantil basado en reconocimiento facial usando modelos preentrenados de Deep Learning: VGGFace, FaceNet y ArcFace, siendo FaceNet el que presentó los mejores resultados en su evaluación. Para identificar estudiantes con un mínimo de imágenes por persona emplearon Redes Siamesas, lo que permitió registrar nuevos usuarios sin reentrenamiento del modelo. El sistema fue desplegado como aplicación de escritorio con la librería QtDesigner de Python, validando la viabilidad de redes siamesas como alternativa al aprendizaje adaptativo en contextos con datasets reducidos (Silva, 2024).

Tabla 2. Comparativo de trabajos relacionados IA.

Referencia	**País / Año**	**Hardware**	**Algoritmo**	**Precisión**	**Aplicación**	***Delimitación***
(Alfonso Sierra & Castaño Saavedra, 2021)	Colombia 2019	Raspberry Pi 3 B+	Eigenfaces / PCA	~85-90%	Control acceso residencial	Iluminación y ángulos
(Elnozahy Seifeldin Liang et al., 2025)	Malasia 2025	Raspberry Pi 3B	HOG + DeepFace	96.7%	Cerradura inteligente	Sin módulo QR
(Legarda Delgado & Loaiza	Colombia 2022	Servidor / PC	ArcFace FaceNet VGG	>95%	Asistencia clases FR-ARCA	Solo asistencia

Pabon, 2022)						
(Paredes et al., 2023)	Panamá 2023	PC + Webcam	face-recognition	100% frontal	Asistencia aulas	Sin ángulos laterales
(Chavez Vargas, 2025)	Perú 2025	Servidor web	ArcFace (DeepFace)	96.92%	Asistencia escolar	Solo asistencia
(Reyes Alcivar, 2026)	Ecuador 2026	SenseFace 2A	Biométrico propietario	Alta	Control acceso educativo	Hardware propietario

Nota. Elaboración propia (2026).

Tabla 3. Comparativo de trabajos relacionados QR.

Referencia	País/Año	Tecnología	Precisión	Limitación
(Llanos Bermudez & Hurtado Pardo, 2021)	Col. 2021	QR / IoT	N/A	Sin reconocimiento facial
(Zertucha González Et Al., 2022)	Cuba 2022	QR / Rasp. Pi	N/A	Sin autoenfoque
(Palomino Sulca, 2023)	Perú 2023	QR / Web	N/A	Sin reconocimiento facial

Nota. Elaboración propia (2026).

6 OBJETIVOS

6.1 OBJETIVO GENERAL

Diseñar y desarrollar un prototipo funcional de un sistema de identificación y control de acceso para la entrada peatonal, que permita automatizar el registro de ingreso y salida de usuarios a las instalaciones de la Universidad Internacional del Trópico Americano.

6.2 OBJETIVOS ESPECÍFICOS

- Documentar los requerimientos funcionales y no funcionales del sistema, mediante observación directa, entrevistas semiestructuradas con actores relacionados.
- Diseñar la arquitectura técnica del sistema bajo el patrón Modelo – Vista - Controlador, incluyendo el modelo de datos, diagrama entidad - relación, la arquitectura de microservicios, módulo web y microservicio de IA y los diagramas UML de casos de uso.
- Integrar el prototipo funcional del sistema, aplicando la metodología ágil XP, mediante una aplicación web y componentes tecnológicos, incluyendo controladores y servicios para la gestión y validación de la información, integrados mediante API REST.
- Validar el prototipo mediante pruebas funcionales, pruebas de precisión del modelo de IA y pruebas de usabilidad con usuarios finales.

7 MARCO REFERENCIAL

7.1 Marco teórico o conceptual

7.1.1 Inteligencia Artificial

La Inteligencia Artificial es una tecnología que permite a las computadoras y máquinas simular capacidades humanas como el aprendizaje, la comprensión, la resolución de problemas y la toma de decisiones. Estos sistemas pueden analizar grandes volúmenes de datos, identificar patrones y mejorar su rendimiento a partir de la experiencia mediante técnicas como el aprendizaje automático (machine learning) y el aprendizaje profundo (deep learning). Además, la IA permite automatizar procesos, optimizar tareas y desarrollar soluciones inteligentes en diferentes ámbitos como la educación, la seguridad y la industria (IBM, 2024a)

7.1.2 Reconocimiento Facial

El reconocimiento facial es una aplicación de la Inteligencia Artificial y la visión por computador que permite identificar o verificar la identidad de una persona a partir de imágenes digitales o fotogramas de vídeo, analizando los patrones únicos de sus características faciales. El proceso involucra tres etapas fundamentales: la detección del rostro dentro de la imagen, la extracción de características mediante redes neuronales que generan un vector matemático denominado embedding, y el reconocimiento por comparación de dicho vector con una base de datos de entidades registradas (Alfonso Sierra & Castaño Saavedra, 2021).

7.1.3 Redes Neuronales Convolucionales y Embeddings Faciales

Las Redes Neuronales Convolucionales (CNN) son una subdisciplina del aprendizaje profundo que extrae características espaciales de las imágenes de manera

automática, superando significativamente a los métodos clásicos bajo condiciones variables de iluminación y expresión facial (Legarda Delgado & Loaiza Pabon, 2022). Un embedding facial es un vector de alta dimensionalidad (típicamente 128 o 512 dimensiones) que representa matemáticamente las características únicas de un rostro. Los embeddings permiten identificar usuarios sin reentrenar el modelo ante nuevos registros, haciendo el sistema escalable y adaptable a contextos donde el número de usuarios varía periódicamente.

7.1.4 Arquitectura MVC y API REST

El patrón Modelo-Vista-Controlador (MVC) separa la lógica de negocio (Modelo), la interfaz de usuario (Vista) y el control de flujo (Controlador), facilitando el mantenimiento, la escalabilidad y las pruebas del sistema. Una API REST (Interfaz de Programación de Aplicaciones) es un conjunto de reglas que permite la comunicación entre el frontend y el backend mediante protocolos HTTP. Las API simplifican el desarrollo al permitir que diferentes componentes del sistema intercambien datos de manera estructurada y segura (IBM, 2025). El sistema propuesto implementará esta arquitectura para garantizar la separación de responsabilidades entre el módulo web y el microservicio de IA (Microsoft, 2025).

7.1.5 Código QR

Un código QR (del inglés Quick Response code, "código de respuesta rápida") es un módulo para almacenar información en una matriz de puntos o en un código de barras bidimensional. Fue creado y desarrollado en 1994 por la compañía japonesa Denso Wave, subsidiaria de Toyota. Posee tres cuadrados en las esquinas que permiten detectar la posición del código al lector. El objetivo de los creadores y desarrolladores

(un equipo de dos personas en Denso Wave, dirigido por Masahiro Hara) es que el código permitiera que su contenido se leyera o descifrara a alta velocidad. Los códigos QR son muy comunes en Japón, donde es el código bidimensional más popular. Aunque inicialmente se usó para registrar repuestos en el área de la fabricación de vehículos, hoy los códigos QR se usan para administración de inventarios en una gran variedad de industrias. La inclusión de software que lee códigos QR en teléfonos móviles ha permitido nuevos usos orientados al consumidor y a los negocios en línea, que se manifiestan en comodidades como el dejar de tener que introducir datos de forma manual en los teléfonos. Las direcciones y los URLs se están volviendo cada vez más comunes en revistas y anuncios. El agregado de códigos QR en tarjetas de presentación también se está haciendo común, y permite simplificar en gran medida la tarea de introducir detalles individuales del nuevo cliente en la agenda de un teléfono móvil (Llanos Bermudez & Hurtado Pardo, 2021).

7.1.6 Base de datos

Una base de datos es un “almacén” que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente. Cada base de datos se compone de una o más tablas que guardan un conjunto de datos. Cada tabla tiene una o más columnas y filas. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla, cada fila de la tabla conforma un registro (Pérez Valdés, 2007).

7.1.7 Control de asistencia

La función de un control de asistencia es básica, saber cuándo una persona entra o sale de un lugar específico. Con un control de asistencia bien desarrollado se pueden

conocer con certeza las cantidades horarias en cada recinto por persona, además se tiene el número exacto de personas que se encuentran al interior del lugar a monitorear, con esta información se pueden detectar las fallas que pudieran existir y optimizar los procesos internos (Reyes Alcivar, 2026).

7.1.8 Autenticación.

En un sistema informático, la autenticación (“auth” para abreviar) es el proceso que verifica que un usuario sea quien dice ser. La mayoría de los sistemas de autenticación se basan en factores de autenticación, que son elementos (una tarjeta de deslizamiento), características (un escaneo de huellas dactilares) o bits de información que solo tiene el usuario. Considere un escenario de autenticación común: proporcionar un ID de usuario y una contraseña para iniciar sesión en una cuenta de email. Cuando el usuario ingresa su ID de usuario (que probablemente sea su dirección de email en esta situación), le está diciendo al sistema de email: "Esto es lo que soy". Pero eso no es suficiente para verificar la identidad del usuario final. Cualquiera puede ingresar el ID de usuario que desee, especialmente cuando el ID de un usuario es algo público, como una dirección de email. Para demostrar que realmente es la persona propietaria de esa dirección de email, el usuario ingresa su contraseña, un conocimiento secreto que (teóricamente) nadie más debería tener. Luego, el sistema de email identifica a este usuario como el verdadero titular de la cuenta y le permite ingresar. Los procesos de autenticación también pueden confirmar las identidades de usuarios no humanos, como servidores, aplicaciones sitio web y otras máquinas y cargas de trabajo. La autenticación es un componente fundamental de la estrategia de seguridad de la información. Es particularmente importante para la gestión de identidades y accesos, la disciplina de

ciberseguridad que se ocupa de cómo los usuarios acceden a los recursos digitales. La autenticación permite a las organizaciones limitar el acceso a la red a usuarios legítimos y es el primer paso para hacer cumplir las licencias de los usuarios individuales (IBM, 2025a).

7.1.9 Token de acceso.

Un token de autenticación transmite de manera segura información sobre las identidades de los usuarios entre aplicaciones y sitios web. Permiten a las organizaciones fortalecer sus procesos de autenticación para dichos servicios. Un token de autenticación permite a los usuarios de Internet acceder a aplicaciones, servicios, sitios web e interfaces de programación de aplicaciones (API) sin tener que ingresar sus credenciales de inicio de sesión cada vez que lo visitan. En cambio, el usuario inicia sesión una vez y se genera un token único y se comparte con aplicaciones o sitios web conectados para verificar su identidad. Estos tokens son la versión digital de un boleto sellado para un evento. Al usuario o portador del token se le proporciona un token de acceso a un sitio web hasta que cierran sesión o cierran el servicio. Un token de autenticación está formado por tres componentes clave: el encabezado, la carga útil y la firma (Fortinet, 2025).

7.1.10 Sistemas de Información.

Un sistema de información es un conjunto ordenado de personas, procesos y herramientas cuyo fin es administrar datos e información, de manera que puedan ser recuperados y procesados fácil y rápidamente. Todo sistema de información se compone de una serie de recursos interconectados y en interacción, bien organizados y dispuestos del modo más conveniente en relación con un propósito informativo determinado, que

puede ser recabar información personal, procesar estadísticas, organizar archivos, entre otros. Los sistemas de información pueden presentar diferencias, pero generalmente recolectan y clasifican datos, que son procesados por personas y/o con recursos informáticos, para que sean fáciles de comprender y recuperar. Así, esta información queda almacenada para ser consultada de manera sencilla o para ser divulgada cuando sea necesario. Estos sistemas se emplean en organizaciones empresariales y gubernamentales, pero también en otros sitios o estructuras, como bibliotecas, universidades, museos, redes sociales o aplicaciones (Vargas Encalada et al., 2019).

7.1.11 API

Una API, o interfaz de programación de aplicaciones, es un conjunto de reglas o protocolos que permite a las aplicaciones informáticas comunicarse entre sí para intercambiar datos, características y funcionalidades. Las API simplifican y aceleran el desarrollo de aplicaciones y software permitiendo a los desarrolladores integrar datos, servicios y capacidades de otras aplicaciones, en lugar de desarrollarlas desde cero. Las API también ofrecen a los propietarios de aplicaciones una forma sencilla y segura de poner los datos y las funciones de sus aplicaciones a disposición de los departamentos de su organización. Los propietarios de aplicaciones también pueden compartir o comercializar datos y funciones con Business Partners o terceros. Las API permiten compartir solo la información necesaria, manteniendo ocultos otros detalles internos del sistema, lo que ayuda a la seguridad del sistema. Los servidores o dispositivos no tienen que exponer completamente los datos: las API permiten compartir pequeños paquetes de datos, relevantes para la solicitud específica. La documentación de la API es como un manual de instrucciones técnicas que proporciona detalles sobre una API e

información para los desarrolladores sobre cómo trabajar con una API y sus servicios. Una documentación bien diseñada promueve una mejor experiencia de API para los usuarios y, en general, hace que las API sean más exitosas (IBM, 2024b)

7.1.12 Frontend

El frontend es la parte de una página web o aplicación que los usuarios ven y con la que interactúan. Se centra en presentar la información de manera atractiva y facilitar las interacciones del usuario. El diseño del frontend se adapta a las necesidades y expectativas de los usuarios, priorizando una experiencia de usuario positiva (user experience, UX). El frontend es una capa de software que se ejecuta en el cliente. Aunque parece estar realizando todo el trabajo, en realidad, se comunica constantemente con el backend, que se encarga del procesamiento de datos. Esta comunicación se realiza a través de interfaces de programación conocidas como API. Siguiendo el principio de “Separation of concerns”, en español “Separación de responsabilidades”, el backend y el frontend se desarrollan como capas independientes pero complementarias. Ambas capas siempre son necesarias para crear un software plenamente funcional. Un backend sin el frontend es como una fachada sin nada detrás (Perez Ibarra et al., 2021).

7.1.13 Backend

El backend es un término que utilizamos para referirnos a la arquitectura interna de un sitio web. Esta área lógica, que no es visible a los ojos del usuario y no incluye elementos de tipo gráfico, permite que todos los elementos de una web desarrollen la función correcta. La palabra, en inglés, se refiere a ‘lo que está detrás’, ‘lo que no se ve’. De ahí su término ‘back’. Cuando hablamos de backend, hablamos únicamente del

código interno de la página. Quien lo desarrolla, desarrolla la funcionalidad del sitio y la seguridad y la optimización de los recursos. Se trata de una rama del desarrollo web que se encarga de que toda la lógica de una web funcione. Se refiere a todo lo que ocurre dentro de una página, aunque no lo podamos ver (Perez Ibarra et al., 2021).

7.1.14 Liveness Detection

La detección de vida facial, o Face Liveness Detection, es una técnica de seguridad biométrica que permite verificar si el rostro capturado por una cámara corresponde a una persona real y físicamente presente, evitando que el sistema sea engañado mediante fotografías, videos, máscaras u otros ataques de suplantación. Según Khairnar, esta técnica busca proteger los sistemas de reconocimiento facial frente a ataques de spoofing, mediante el uso de métodos basados en inteligencia artificial, aprendizaje automático y aprendizaje profundo (Khairnar et al., 2023).

7.1.15 Anti-Spoofing

El Face Anti-Spoofing es una técnica de seguridad aplicada a los sistemas de reconocimiento facial, cuyo objetivo es determinar si el rostro capturado corresponde a una persona real o a un intento de suplantación mediante una fotografía, video, pantalla digital o máscara. Según (Yang et al., 2019)esta tarea es fundamental en aplicaciones de autenticación facial, controles de seguridad y control de acceso, ya que permite fortalecer la protección de los sistemas biométricos frente a ataques de presentación o spoofing (Yang et al., 2019).

7.1.16 InsightFace y Modelo Buffalo_L

InsightFace es una librería de código abierto especializada en análisis facial que integra en un solo paquete las funciones de detección, reconocimiento, alineación y

extracción de atributos como edad y género (Mukesh, 2024). Dentro de los distintos modelos que ofrece, el paquete Buffalo_L incluye un detector de rostros basado en RetinaFace, un modelo de reconocimiento ArcFace de 512 dimensiones, así como estimación de edad, género y predicción de puntos de referencia en 3D (Agentbus, 2026). Buffalo_L se considera el modelo de mayor precisión dentro del conjunto de modelos disponibles en InsightFace, lo cual justificó su elección para el desarrollo del presente proyecto (Mukesh, 2024).

El modelo Buffalo_L está fundamentado en la arquitectura ArcFace, la cual incorpora una función de pérdida de margen angular aditivo que mejora la separación entre identidades en el espacio de embeddings, logrando agrupaciones más compactas para una misma persona y una mayor distancia entre personas distintas (K, 2025). Dado que los embeddings generados por ArcFace se ubican sobre una hiperesfera, la similitud de coseno constituye la métrica de distancia adecuada para compararlos, donde dos embeddings correspondientes a una misma persona típicamente obtienen una puntuación superior a 0.4, mientras que los de personas distintas se ubican significativamente por debajo de dicho valor (Qasim, 2026).

El modelo Buffalo_L fue desarrollado sobre una arquitectura ResNet50 preentrenada con el dataset WebFace600K, que comprende 600.000 identidades únicas de personas de diferentes etnias, edades y condiciones de captura. En cuanto a su rendimiento, obtuvo los siguientes resultados en los benchmarks estándar: 99.83% en LFW, 98.74% en CFP-FP y 98.28% en AgeDB-30, posicionándose como el modelo de mayor precisión dentro de InsightFace (Mohamed Idabrahim, 2025). El modelo opera con una tasa de falsa coincidencia objetivo de 1×10^{-5}, equivalente a 1 falso positivo por cada

100.000 intentos de personas no registradas (Mukesh, 2024). Internamente normaliza las imágenes faciales a 112×112 píxeles antes de procesarlas, y en implementaciones prácticas el umbral de confianza recomendado es de 0.60 (Harish K, 2025).

7.1.17 MediaPipe y FaceLandmarker

MediaPipe es un framework de código abierto desarrollado por Google que proporciona soluciones de aprendizaje automático para el procesamiento de medios en tiempo real. Su solución FaceLandmarker es capaz de estimar 468 puntos de referencia faciales tridimensionales, denominados landmarks, en tiempo real utilizando únicamente la entrada de una cámara convencional, sin necesidad de sensores de profundidad especializados. El modelo emplea arquitecturas de redes neuronales convolucionales livianas con aceleración por GPU, lo que le permite operar en dispositivos móviles y navegadores web con alta eficiencia computacional (Anden, 2020)

Cada uno de los 468 landmarks corresponde a una ubicación específica del rostro, como los contornos de los ojos, cejas, nariz, labios y la superficie general de la cara. La densa red de puntos permite construir una malla facial, o face mesh, que representa geométricamente la superficie del rostro detectado y sirve como base para aplicaciones de análisis facial en tiempo real (Lugaresi Camillo, 2019).

7.1.18 Eye Aspect Ratio (EAR) y detección de parpadeo

El Eye Aspect Ratio (EAR), o Razón de Aspecto del Ojo, es una métrica escalar introducida por (Soukupová & Cech, 2016)

para cuantificar el grado de apertura del ojo en cada fotograma de video. Se calcula a partir de seis puntos de referencia facial ubicados alrededor del ojo mediante

la fórmula EAR = (|p2–p6| + |p3–p5|) / (2 × |p1–p4|), donde p1 y p4 son los cantos del ojo y los demás puntos corresponden a los párpados superior e inferior.

Cuando el ojo está abierto el EAR mantiene un valor constante; cuando se produce un parpadeo, el EAR cae abruptamente hacia cero. Un parpadeo se detecta cuando el valor EAR desciende por debajo de un umbral, típicamente 0.2, durante un número suficiente de fotogramas consecutivos. Esta técnica es ampliamente utilizada en sistemas de interacción humano-computador y detección de fatiga por su simplicidad y eficiencia computacional (Soukupová & Cech, 2016)

7.1.19 Métricas de evaluación biométrica

Las métricas de evaluación son indicadores cuantitativos utilizados para medir el rendimiento de un sistema de clasificación. En el contexto de sistemas de reconocimiento facial, los Verdaderos Positivos (TP) corresponden a usuarios registrados correctamente identificados; los Falsos Positivos (FP) a personas no registradas que el sistema identificó incorrectamente como válidas; los Verdaderos Negativos (TN) a impostores correctamente rechazados; y los Falsos Negativos (FN) a usuarios registrados que el sistema no reconoció.

A partir de estas categorías se derivan tres métricas compuestas: la Precisión, definida como TP / (TP + FP), mide qué proporción de los accesos concedidos correspondían a usuarios realmente registrados; el Recall, definido como TP / (TP + FN), mide qué proporción de los usuarios registrados fueron reconocidos exitosamente; y el F1-score, calculado como la media armónica de Precisión y Recall, representa el balance entre ambas métricas y constituye el indicador más completo para evaluar sistemas de identificación biométrica (Zhalgas et al., 2025a)

7.2 Marco Demográfico

El presente proyecto está dirigido a la comunidad académica de la Universidad Internacional del Trópico Americano, la cual está conformada principalmente por estudiantes, docentes y personal administrativo. Esta población presenta la necesidad de contar con mecanismos eficientes de control de acceso que permitan gestionar de manera adecuada el ingreso y salida dentro de la institución. El crecimiento de la población estudiantil y la dinámica diaria de ingreso a las instalaciones generan la necesidad de implementar soluciones tecnológicas que mejoren la organización, reduzcan tiempos de registro y aumenten la seguridad. En este contexto, el sistema propuesto busca beneficiar directamente a los estudiantes como principales usuarios, así como a la institución en términos de control y gestión de la información.

7.3 Marco Geográfico

El proyecto se desarrolla en la Universidad Internacional del Trópico Americano, ubicada en la ciudad de Yopal, departamento de Casanare, Colombia. Esta institución de educación superior se encuentra en una región caracterizada por su crecimiento académico y tecnológico, lo que demanda la implementación de soluciones innovadoras que fortalezcan sus procesos institucionales. Las condiciones del entorno, junto con la necesidad de modernizar los sistemas de control de acceso, hacen pertinente la implementación de tecnologías basadas en Inteligencia Artificial dentro del contexto universitario. De esta manera, el proyecto se adapta a las características del entorno local, lo cual podría contribuir, en una futura implementación, al fortalecimiento de la gestión institucional y al mejoramiento de los procesos de seguridad y control.

7.4 Marco Histórico

El control de acceso en instituciones ha experimentado una evolución significativa con el avance de las tecnologías de la información, ya que, en sus inicios, estos procesos se realizaban de forma manual mediante listas en papel, lo que generaba errores, pérdida de información y dificultades en la verificación de registros, con el tiempo, se incorporaron sistemas basados en tarjetas físicas y carnets institucionales, mejorando parcialmente la identificación de los usuarios.

Con la masificación de dispositivos móviles, surgieron soluciones digitales como los códigos QR, que permiten automatizar el registro de ingreso y salida. En la actualidad, el desarrollo de la Inteligencia Artificial ha dado lugar a tecnologías más avanzadas, como el reconocimiento facial, que permiten una identificación más precisa, rápida y segura. Esta evolución evidencia una transición hacia sistemas automatizados orientados a optimizar la gestión del acceso en entornos educativos.

7.5 Marco legal

Para el desarrollo del proyecto se deben tener en cuenta algunas normas o estándares estipulados:

- Ley 1581 de 2012 Protección de Datos Personales

Regula el tratamiento de datos personales incluyendo datos biométricos como imágenes faciales. Establece principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad.

- Resolución No. 014 de 2021 Reglamento Estudiantil UNITRÓPICO

Artículo 44 establece la obligatoriedad del porte del carnet para ingresar y permanecer en los predios universitarios.

- Resolución No. 025 de 2021 Código Comportamental UNITRÓPICO

Define los procedimientos de ingreso, los derechos y deberes de la comunidad universitaria en

relación con el acceso a las instalaciones, y los mecanismos de control institucional aplicables.

- ISO/IEC 25010:2011 Calidad del Software

Norma para evaluar la calidad de productos de software en términos de funcionalidad, confiabilidad, usabilidad, eficiencia, mantenibilidad y portabilidad.

- IEEE 802.3 / ISO/IEC 30141 Redes e IoT

Establecen lineamientos para la comunicación en redes y la interoperabilidad de sistemas conectados.

- ISO/IEC 27001

Norma internacional que establece los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de proteger la confidencialidad, integridad y disponibilidad de los datos.

- NIST SP 800-63

Conjunto de directrices para la gestión de identidad y autenticación digital, que define buenas prácticas para verificar de manera segura la identidad de los usuarios en sistemas electrónicos.

- ISO/IEC 19794-5:

Norma internacional que especifica el formato y los requisitos técnicos de las imágenes faciales utilizadas en sistemas biométricos, garantizando calidad e interoperabilidad para el reconocimiento facial.

- IEEE 830

Estándar que define la estructura y lineamientos para la especificación de requisitos de software, permitiendo documentar de forma clara las funcionalidades y restricciones de un sistema.

7.6 Marco Institucional

La Universidad Internacional del Trópico Americano es una institución de educación superior ubicada en Yopal, Casanare, en la Ciudadela Universitaria de la carrera 19 No. 39 - 40. Su origen se encuentra en una fundación universitaria creada para ampliar las oportunidades de acceso a la educación superior en la Orinoquía colombiana. Posteriormente, mediante la Ley 1937 de 2018 y la Ordenanza No. 014 de 2021, la institución fue oficializada como universidad pública del departamento de Casanare, adquiriendo autonomía académica, administrativa, financiera y presupuestal. Su Proyecto Educativo Institucional, actualizado mediante el Acuerdo CS No. 001 de 2026, define el horizonte ético, académico y territorial de la universidad, orientando sus políticas, planes, programas y acciones institucionales. Desde esta perspectiva, Unitrópico asume una misión regional orientada a cerrar brechas históricas, fortalecer la formación integral, promover la investigación, la innovación, la sostenibilidad y contribuir al desarrollo social, cultural y ambiental de la Orinoquía.

Este contexto institucional resulta relevante para el proyecto, dado que la propuesta de sistema de control de acceso se dirige específicamente a Unitrópico y busca responder a necesidades propias de su dinámica universitaria, como la trazabilidad del ingreso de estudiantes, docentes, administrativos y demás miembros de la comunidad académica (Unitropico, 2026).

8 METODOLOGÍA

8.1 Metodología de investigación

El proyecto se desarrolla bajo un enfoque metodológico cuantitativo, en el cual se utilizan métricas y datos numéricos para medir y evaluar el rendimiento del sistema, la calidad del software y el cumplimiento de los objetivos establecidos. Este enfoque permite tomar decisiones basadas en datos objetivos y realizar mejoras continuas en el proceso de desarrollo (Fidias G., 2012).

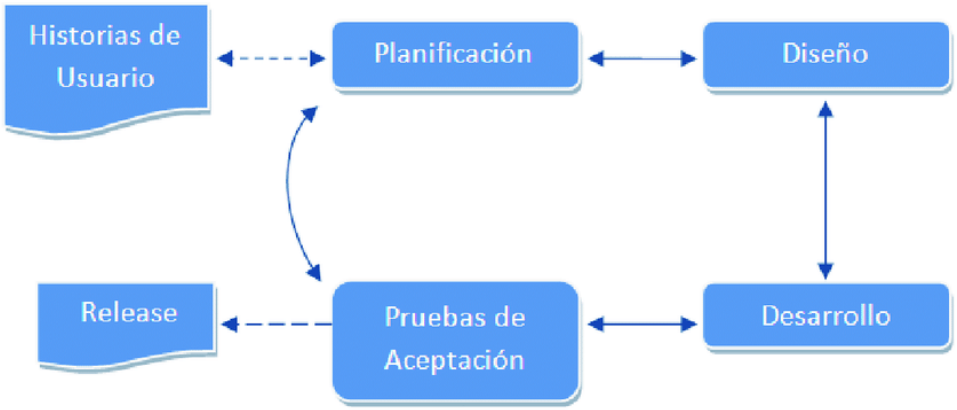
Debido a que se realizó el levantamiento de información para los requerimientos del sistema, se llevó a cabo una revisión exhaustiva de la documentación relacionada con sistemas de automatización de ingreso y salida en instituciones educativas. Al mismo tiempo, se identificaron las mejores prácticas, herramientas útiles y asequibles utilizadas en proyectos similares.

De igual manera, se realizaron entrevistas con expertos en el campus universitario, tales como el jefe del departamento de sistemas y los vigilantes de las entradas peatonales. Estas entrevistas permitieron obtener información valiosa sobre requerimientos, problemáticas y observaciones para llevar un desarrollo más adecuado de la aplicación. Adicionalmente, se utilizaron encuestas para recopilar información de los usuarios, como estudiantes, docentes y personal administrativo. Estas encuestas abordaron sus necesidades y expectativas en relación con el sistema de ingreso y salida automatizado.

8.2 Metodología de desarrollo

La metodología seleccionada para el desarrollo del proyecto fue Programación Extrema XP. La cual es una metodología ágil que se centra en la entrega continua de software funcional y en la colaboración estrecha entre los miembros del equipo de desarrollo. Se caracterizo por su enfoque en la simplicidad, la retroalimentación constante y la adaptabilidad a los cambios. (Villegas, 2022).

Figura 3. Proceso de desarrollo de la metodología XP



Nota. Elaboración propia (2026).

Dentro de la metodología XP, se siguieron los principios fundamentales, como la comunicación constante y efectiva entre los miembros del equipo, la simplicidad en el diseño y la implementación del software, la retroalimentación continua a través de pruebas y revisiones, y la capacidad de respuesta a los cambios en los requisitos del proyecto. Por otro lado, se utilizaron herramientas y tecnologías adecuadas para el desarrollo de software ágil, como sistemas de control de versiones, herramientas de seguimiento de tareas y pruebas. Estas herramientas facilitaron la creación y la gestión eficiente del proyecto (Villegas, 2022).

8.3 Diseño de la Investigación

El diseño de investigación corresponde al plan o estrategia global que el investigador asume para dar respuesta al problema formulado, de acuerdo con este autor, según el diseño, las investigaciones pueden ser de tipo documental, de campo o experimental (Fidias G., 2012).

En este caso, el estudio se enmarca en un diseño de campo, ya que se llevó a cabo directamente en el entorno donde se origina la problemática, como en este caso son las entradas de ingreso al campus, esto coincide con la definición de investigación de campo que plantea quien la describe como aquella que “Consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos” (Hernandez & R. Collado, 2018).

El diseño fue no experimental, debido a que los investigadores no modificaron deliberadamente las condiciones del proceso institucional de control de acceso para obtener la información (Hernandez & R. Collado, 2018). Por el contrario, observaron las prácticas existentes y analizaron las experiencias, dificultades y necesidades expresadas por los participantes en su contexto natural.

Las pruebas funcionales, de reconocimiento facial y de código QR se desarrollaron posteriormente como actividades de validación técnica del prototipo. Estas pruebas no hicieron parte de la recolección cualitativa de información sobre el proceso institucional, sino que permitieron verificar el funcionamiento de la solución desarrollada.

8.4 Población y Muestra

La población se entiende como el conjunto de casos que cumplen con las especificaciones del fenómeno estudiado, es decir, quienes participan directamente en el proceso de control de acceso (Hernandez & R. Collado, 2018).

Los actores vinculados con el proceso de control de acceso incluyen estudiantes, docentes, personal administrativo, personal de seguridad y visitantes. Sin embargo, para efectos de esta investigación, se seleccionaron como participantes a quienes contaban con experiencia directa o conocimiento relevante sobre el proceso: personal de seguridad, responsable del área de sistemas y estudiantes usuarios habituales de los puntos de ingreso.

La población objeto de estudio corresponde a los estudiantes matriculados en la Universidad Internacional del Trópico Americano durante el período académico 2026-A. Según las cifras oficiales publicadas por la Oficina Asesora de Planeación Estratégica de Unitrópico con corte al 30 de junio de 2026, la población estudiantil es de 4.534 estudiantes (*Planeacion estrategica*, 2026). Esta cifra se presenta como referencia del contexto institucional y de la magnitud potencial del proceso de control de acceso; no se utilizó para establecer una muestra estadística, dado que la investigación tuvo un enfoque cualitativo.

8.5 Selección de la muestra

La muestra que se utilizó en la investigación fue de tipo no probabilística, de tipo intencional y por conveniencia, ya que se seleccionaron participantes que, por sus funciones, pueden aportar información relevante sobre el proceso actual de control de acceso y sobre la factibilidad de la propuesta de sistema (Otzen & Manterola, 2017). El

responsable del área de sistemas y el personal de seguridad fueron seleccionados de manera intencional, debido a su conocimiento y participación directa en el proceso de control de ingreso y salida. Por su parte, los estudiantes fueron seleccionados mediante muestreo por conveniencia y participación voluntaria según su disponibilidad e interés en participar en la investigación. Según (Hernandez & R. Collado, 2018) este tipo de muestreo es válido en investigaciones donde el objetivo es comprender el comportamiento de un sistema en condiciones reales y donde las limitaciones de tiempo y recursos no permiten una selección aleatoria de la totalidad de la población.

8.5.1 Participación en las pruebas de usabilidad

Durante la aplicación de las pruebas se contactó un total de 201 estudiantes distribuidos en grupos académicos durante dos jornadas, sábado y martes. De estos, 60 participaron voluntariamente en las pruebas de usabilidad, representando el 29.85% del total contactado. Dado que no se obtuvo autorización formal para ingresar a los grupos por parte de los docentes debido a las limitaciones de tiempo que implicaba el proceso de registro por estudiante, las pruebas se realizaron mediante búsqueda voluntaria de participantes en las instalaciones del campus universitario. Los 141 estudiantes restantes no participaron por dos razones: 35 eran menores de edad, lo que implicaba la necesidad de consentimiento informado firmado por sus padres o acudientes, requisito que no pudo cumplirse en el momento; y 106 manifestaron su negativa al conocer que el proceso requería la captura de una fotografía de su rostro para el enrolamiento biométrico, de conformidad con lo establecido en la Ley 1581 de 2012 sobre protección de datos personales en Colombia.

8.6 Técnica e instrumentos de recolección de datos

Para dar cumplimiento a los objetivos del proyecto y obtener información suficiente sobre el proceso actual de control de acceso en la Universidad Internacional del Trópico Americano, así como sobre los requerimientos del sistema propuesto, se emplearon diversas técnicas de recolección de datos, cada una apoyada en instrumentos específicos.

8.6.1 Observación Directa:

Se realizó observación directa en el punto de acceso peatonal principal de la Universidad Internacional del Trópico Americano, ubicado en la Carrera 19 No. 39-40 de la ciudad de Yopal, Casanare, durante dos períodos: entre el 15 y el 30 de abril de 2025, y durante la tercera semana del período académico 2026-A, específicamente los días martes 12 y jueves 14 de mayo de 2026. Como instrumento, se utilizó una guía de observación que permitió registrar de manera sistemática los aspectos más relevantes del proceso (**Anexo *H***).

Durante la observación se identificaron tres franjas horarias de mayor afluencia de personas en el punto de acceso: 6:00 a.m. a 8:00 a.m., correspondiente al inicio de la jornada académica; 12:00 p.m. a 2:00 p.m., en el horario de mediodía; y 5:00 p.m. a 7:00 p.m., al cierre de actividades académicas del día. Este patrón de distribución del flujo de personas es consistente con el comportamiento documentado en otras instituciones de educación superior, donde se identifican momentos de alta afluencia asociados al inicio, mediodía y cierre de la jornada académica (Serna Herrera, 2010). Estudios sobre movilidad peatonal en campus universitarios confirman

además que las horas pico generan congestionamiento y demoras en los procesos de control de acceso (Nasareno et al., 2020).

En promedio, durante los dos días de observación, se registró el ingreso de 1.337 personas en las tres franjas monitoreadas. De estas, 96 no portaban el carnet institucional, lo que representó el 7.18% de los usuarios observados. Adicionalmente, 52 personas debieron registrarse en la minuta de ingreso. La franja de mayor incumplimiento en el porte del carnet fue la de 12:00 p.m. a 2:00 p.m., con un 9.85% de usuarios sin credencial, lo que evidenció que en el cambio de clases del mediodía se presenta la mayor vulnerabilidad en el proceso de verificación de identidad.

Los resultados detallados por día y franja horaria se presentan en la siguiente tabla.

Tabla 4. Promedio de los dos días de observación directa

Franja	Ingresos Mar.	Ingresos Jue.	Sin carnet Mar.	Sin carnet Jue.	% Promedio
6 - 8 a.m.	522	498	36 (6.90%)	34 (6.83%)	6.86%
12 - 2 p.m.	399	412	41 (10.28%)	38 (9.22%)	9.85%
5 - 7 p.m.	428	415	20 (4.67%)	22 (5.30%)	4.98%
Total	1.349	1.325	97 (7.19%)	94 (7.09%)	7.18%

Nota. Elaboración propia (2026).

Adicionalmente, durante la observación se identificó que ninguno de los puntos de acceso contaba con recursos tecnológicos de apoyo para el proceso de identificación.

Las figuras que se presentan a continuación ilustran el proceso de ingreso observado:

Figura 4. Minuta de registro de la entrada peatonal



Nota. Imagen tomada por los autores (2026).

Figura 5. Usuarios en fila en el punto de acceso peatonal durante registro manual.



Nota. Imagen tomada por los autores (2026).

Figura 6. Estudiante registrándose en la minuta de ingreso.



Nota. Imagen tomada por los autores (2026).

Figura 7. Registro manual en el punto de acceso.



Nota. Imagen tomada por los autores (2026).

Figura 8. Puesto de control de salida sin recursos tecnológicos de apoyo.



Nota. Imagen tomada por los autores (2026).

Figura 9. Flujo de personas en el corredor principal de acceso durante hora pico.



Nota. Imagen tomada por los autores (2026).

A partir de la observación realizada, se identificaron los siguientes hallazgos principales: el proceso de ingreso dependió en su totalidad de la verificación visual del carnet por parte del personal de vigilancia, sin apoyo de ningún recurso tecnológico. En los casos en que los usuarios no portaban su carnet, el procedimiento consistió en el registro manual en una minuta, lo que generó filas y demoras especialmente en las franjas horarias de mayor afluencia. Se evidenció además que ninguno de los puntos de acceso observados contaba con dispositivos digitales, lectores de código QR, cámaras de seguridad activas para control de acceso o cualquier otro sistema automatizado de identificación. La totalidad del proceso de verificación recayó sobre el criterio y la capacidad operativa del personal de vigilancia presente.

8.6.2 Entrevistas:

Se llevaron a cabo entrevistas semiestructuradas a participantes clave, entre ellos el personal de seguridad de la empresa Binarios y el Jefe del Departamento de Sistemas de la institución. Dichas entrevistas permitieron obtener información detallada sobre el funcionamiento actual del control de acceso, las problemáticas existentes y los requerimientos del sistema propuesto. Para ello, se utilizó una guía de preguntas previamente diseñada (**Anexo *A***), y la información recolectada fue registrada para su posterior análisis (**Anexo *D***, **Anexo *E***, **Anexo *F***, **Anexo *G***).

Jefe del Departamento de Sistemas (**Anexo *D***)

El Jefe del Departamento de Sistemas expresó interés en contar con un sistema que permitiera al vigilante verificar en tiempo real si una persona está

efectivamente registrada en la institución, señalando haber presenciado casos en los que personas ingresaron con carnets que no les pertenecían. Indicó que la universidad tenía prevista la adquisición de lectores QR para los puntos de acceso, con el propósito de no depender del celular del vigilante. Así mismo, manifestó la necesidad de contar con estadísticas de acceso por día, mes y franja horaria, y planteó la importancia de gestionar el ingreso de personas sin carnet mediante un mecanismo de usuario temporal que registre el motivo del ingreso y permita llevar un conteo de las veces que un estudiante ha ingresado sin su credencial institucional.



Vigilante No. 01 (**Anexo *E***)

El primer vigilante describió el procedimiento actual de ingreso: cuando un estudiante no porta su carnet, debe registrarse en una minuta con su nombre, número de documento, programa académico, firma y hora de ingreso. Para el caso de visitantes externos, se les solicita un documento de identidad y se les entrega un carnet temporal de visita. El vigilante no identificó mayores dificultades en el proceso actual, limitándose a describir el procedimiento sin señalar limitaciones específicas.



Vigilante No. 02 (**Anexo *F***)

El segundo vigilante confirmó que la minuta de registro se utiliza para toda la comunidad universitaria cuando no se porta el carnet, incluyendo docentes, administrativos y visitantes. Al ser consultado sobre la precisión del registro, indicó que sí era posible conocer quién ingresó y a qué hora, dado que la minuta incluye esa información. Sin embargo, reconoció que la principal dificultad del sistema radica en que los estudiantes no portan el carnet como lo exige la norma, y que la universidad no provee ningún tipo de apoyo tecnológico al personal de vigilancia. Señaló que sería útil implementar un sistema biométrico integrado con el carnet institucional.

Vigilante No. 03 (**Anexo *G***)

El tercer vigilante aportó una perspectiva más crítica frente al sistema actual. Indicó que si bien en la minuta queda una hora aproximada de ingreso, no es posible obtener una hora precisa sin automatización, dado que registrar manualmente a miles de personas hace inviable ese nivel de exactitud. Destacó que la ausencia de un registro automatizado impide conocer con certeza cuántas personas se encuentran dentro del campus en un momento dado, lo que representa un riesgo especialmente

en situaciones de emergencia o evacuación. También explicó el esquema contractual entre la universidad y la empresa de seguridad, señalando que el sistema actual responde únicamente a los requerimientos mínimos que la universidad le exige a la empresa. Finalmente, manifestó que un sistema con código QR que registre automáticamente entradas y salidas facilitaría significativamente el control de acceso y la generación de reportes.

8.6.3 Revisión documental:

Se revisaron documentos institucionales, normativos y académicos relacionados con el control de acceso y la identificación de usuarios en instituciones de educación superior.

Dentro de los documentos institucionales revisados, se encontró que la Resolución No. 014 de 2021 y la Resolución No. 025 de 2021 de Unitrópico establecen que el carné físico es el documento oficial de identificación del estudiante y su porte es obligatorio para ingresar y permanecer en el campus. A partir de esto, quedó claro que el sistema propuesto no busca reemplazar el carné institucional sino complementarlo, ofreciendo dos mecanismos tecnológicos de identificación: el escaneo del código QR del carné institucional como forma principal de validación, y el reconocimiento facial mediante inteligencia artificial como mecanismo de verificación biométrica, ambos orientados a automatizar el control de acceso sin modificar lo que ya establece la norma.

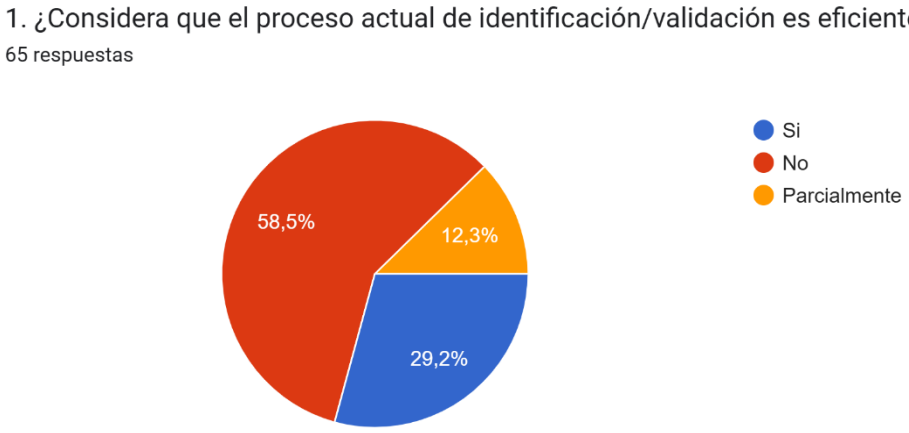
Durante esta revisión también se identificó la Circular Administrativa No. 024 del 22 de junio de 2026, emitida por la Vicerrectoría Administrativa y Financiera de

Unitrópico, en la que la institución le recuerda formalmente a toda la comunidad universitaria que el carné es personal e intransferible y que prestarlo o permitir su uso por parte de terceros está prohibido y puede acarrear sanciones disciplinarias. Esta circular confirmó que el uso indebido del carné y la suplantación de identidad en los puntos de acceso no es solo una percepción, sino una preocupación institucional activa y documentada.

8.6.4 Encuesta

Se aplicaron encuestas con preguntas de selección múltiple a usuarios del sistema, como estudiantes, con el fin de conocer sus percepciones, necesidades y expectativas frente al proceso actual y al sistema propuesto. Como instrumento, se diseñó un cuestionario estructurado con preguntas cerradas que facilitó la recolección de información cuantitativa.





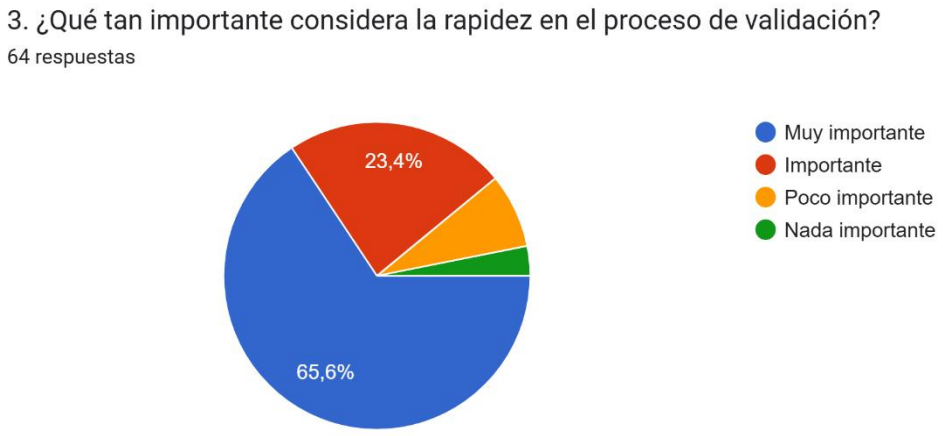
Los resultados obtenidos mostraron que el 58.5% de los encuestados, equivalente a 38 personas, consideró que el proceso actual de identificación y validación no es eficiente, el 29.2%, correspondiente a 19 personas, lo evaluó de forma positiva y el 12.3%, representado por 8 personas, indicó que funciona parcialmente.

La tendencia predominante reflejó una percepción negativa hacia el sistema vigente, dado que el 70.8% de los participantes, al sumar las respuestas negativas y parciales, identificó limitaciones en su funcionamiento.



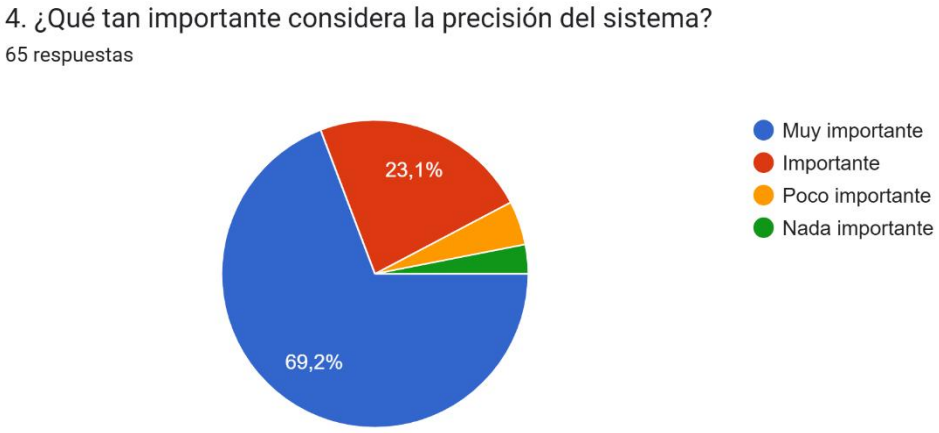
Los datos obtenidos indicaron que el 87.7% de los encuestados, equivalente a 57 personas, presentó inconvenientes con los métodos tradicionales de validación, el 7.7%, correspondiente a 5 personas, reportó haberlos experimentado ocasionalmente y el 4.6% restante, representado por 3 personas, manifestó no haber tenido dificultades.

La sumatoria entre quienes respondieron afirmativamente y quienes lo hicieron de forma ocasional representó el 95.4% de la población encuestada, lo que indicó que las fallas en los métodos tradicionales no constituyeron casos aislados sino una problemática recurrente y generalizada dentro de la comunidad universitaria.



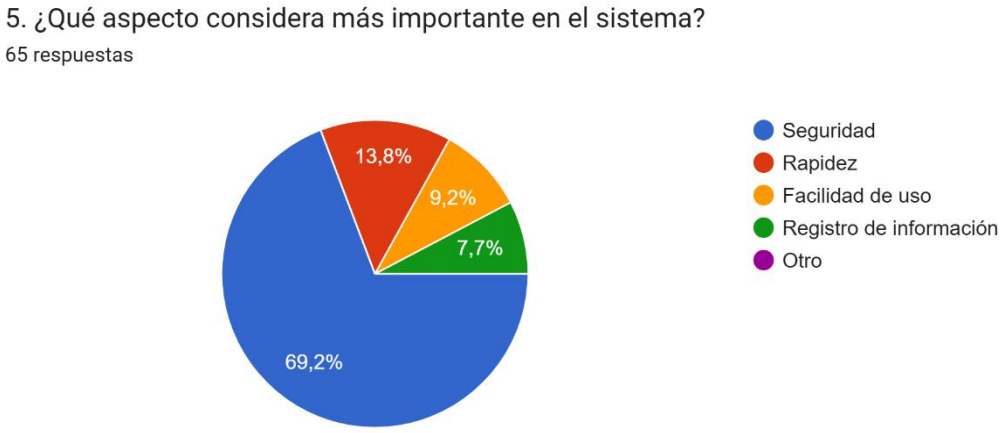
Los datos recolectados indicaron que el 65.6% de los encuestados, equivalente a 42 personas, consideró la rapidez en el proceso de validación como muy importante, seguido de un 23.4%, correspondiente a 15 personas, que la calificó como importante. En menor proporción, el 7.8%, representado por 5 personas, la percibió como poco importante y el 3.1%, equivalente a 2 personas, como nada importante.

La acumulación del 89% de las respuestas en las categorías de mayor valoración evidenció que la velocidad de respuesta del sistema constituyó un atributo crítico para la mayoría de los usuarios encuestados.



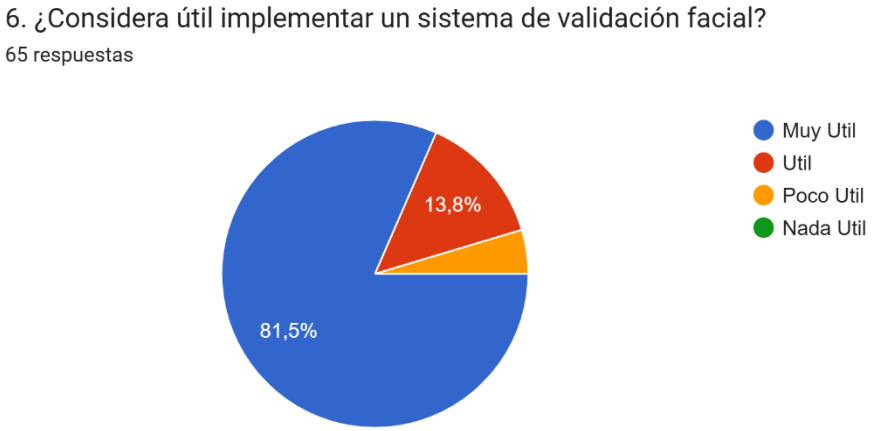
Los resultados evidenciaron que el 69.2% de los encuestados, equivalente a 45 personas, calificó la precisión del sistema como muy importante, mientras que el 23.1%, correspondiente a 15 personas, la consideró importante. El 4.6%, representado por 3 personas, la valoró como poco importante y el 3.1%, equivalente a 2 personas, como nada importante.

La precisión se posicionó como el atributo con mayor valoración dentro de la encuesta, dado que el 92.3% de los participantes la ubicó en las categorías más altas, reflejando que los usuarios no solo valoraron la rapidez en el proceso de validación, sino que otorgaron igual importancia a la exactitud del sistema.



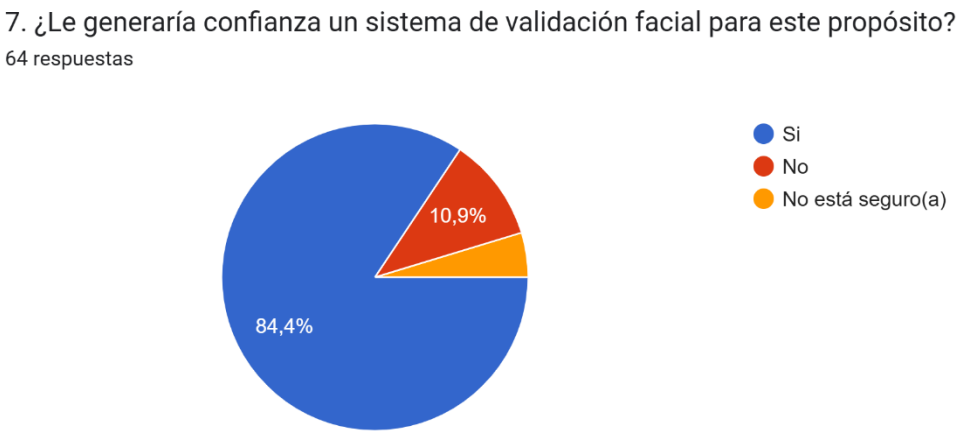
Los resultados mostraron que la seguridad fue el aspecto que la comunidad universitaria consideró más relevante en un sistema de validación, con un 69.2% de las respuestas, equivalente a 45 personas. A mayor distancia se ubicó la rapidez con un 13.8%, correspondiente a 9 personas, seguida de la facilidad de uso con un 9.2%, representado por 6 personas, y el registro de información con un 7.7%, equivalente a 5 personas.

Esta distribución indicó una clara diferencia en las prioridades de los usuarios, donde más de dos tercios de los encuestados concentró su preferencia en la seguridad, mientras que los demás aspectos evaluados obtuvieron porcentajes significativamente menores de manera uniforme.



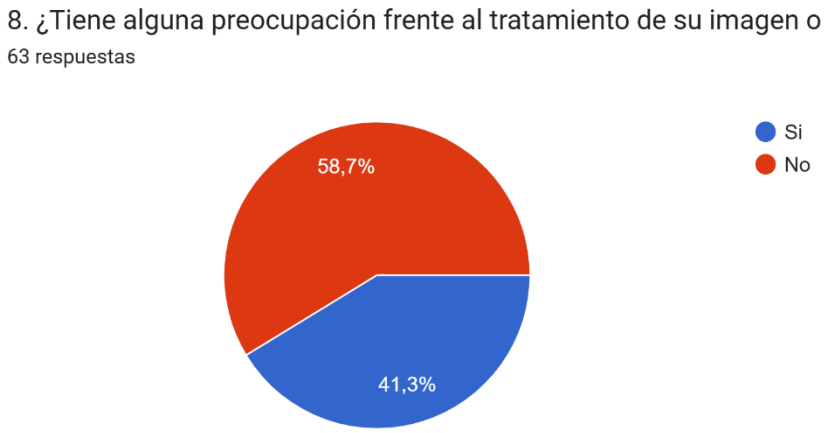
Los datos obtenidos indicaron que el 81.5% de los encuestados, equivalente a 53 personas, consideró muy útil la implementación de un sistema de validación facial, el 13.8%, correspondiente a 9 personas, lo evaluó como útil y únicamente el 4.6%, representado por 3 personas, lo percibió como poco útil.

La concentración del 95.3% de las respuestas en las categorías positivas reflejó una aceptación ampliamente favorable por parte de la comunidad universitaria frente a esta tecnología, constituyendo un indicador significativo sobre la disposición de los usuarios para adoptar este tipo de sistema en su entorno institucional.



Los resultados indicaron que el 84.4% de los encuestados, equivalente a 54 personas, manifestó que un sistema de validación facial le generaría confianza, mientras que el 10.9%, correspondiente a 7 personas, expresó lo contrario y el 4.7%, representado por 3 personas, no tuvo una posición definida al respecto.

La proporción mayoritaria de respuestas afirmativas señaló que la comunidad universitaria percibió esta tecnología como un mecanismo confiable para el propósito planteado. El porcentaje combinado de respuestas negativas e indecisas, equivalente al 15.6%, representó una fracción menor que pudo estar asociada a factores como el desconocimiento de la tecnología o preocupaciones relacionadas con la privacidad.



Los datos obtenidos mostraron que el 58.7% de los encuestados, equivalente a 37 personas, no manifestó preocupación frente al tratamiento de su imagen o datos biométricos, mientras que el 41.3% restante, correspondiente a 26 personas, expresó tener algún nivel de inquietud al respecto.

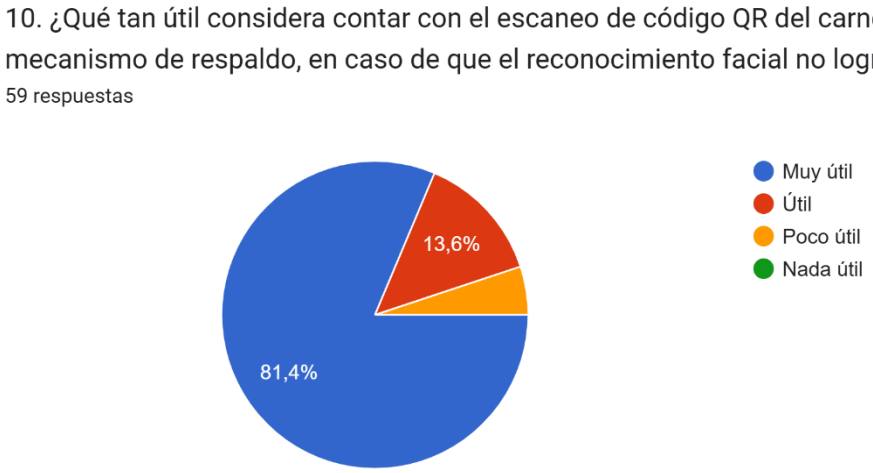
Si bien la mayoría de los participantes no presentó objeciones frente al manejo de sus datos biométricos, la proporción de quienes sí lo hicieron resultó significativa, al

representar más de un tercio de la muestra, reflejando que una parte considerable de la comunidad universitaria manifestó inquietud en cuanto a la privacidad y el tratamiento de su información biométrica.



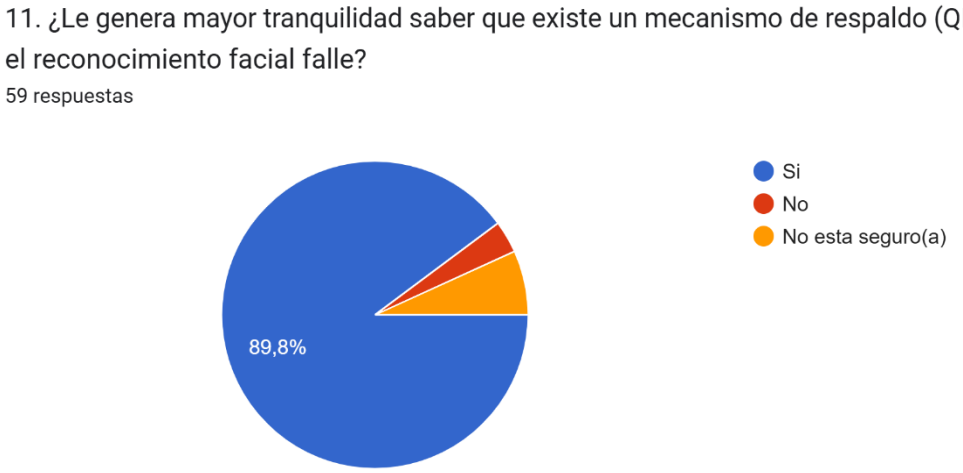
Los resultados evidenciaron que el 92.3% de los encuestados, equivalente a 60 personas, manifestó disposición para participar en pruebas del sistema, mientras que únicamente el 7.7%, correspondiente a 5 personas, indicó no estar dispuesto a hacerlo.

El alto nivel de respuestas afirmativas reflejó una actitud favorable y receptiva de la comunidad universitaria frente al proceso de validación y prueba del sistema, representando una proporción ampliamente mayoritaria respecto a quienes no expresaron dicha disposición.



Los datos obtenidos mostraron que el 81.4% de los encuestados, equivalente a 48 personas, consideró muy útil contar con el escaneo de código QR como mecanismo de respaldo, el 13.6%, correspondiente a 8 personas, lo evaluó como útil y el 5.1%, representado por 3 personas, lo percibió como poco útil.

La concentración del 94.9% de las respuestas en las categorías positivas indicó que los usuarios valoraron favorablemente la existencia de un mecanismo alternativo ante posibles fallas del reconocimiento facial, reflejando una preferencia generalizada por contar con opciones de contingencia.



Los resultados indicaron que el 89.8% de los encuestados, equivalente a 53 personas, expresó que contar con un mecanismo de respaldo mediante código QR le generó mayor tranquilidad, el 6.8%, correspondiente a 4 personas, no tuvo una posición definida al respecto y el 3.4%, representado por 2 personas, manifestó que no le generó dicha tranquilidad.

La amplia mayoría de respuestas afirmativas reflejó que los usuarios percibieron positivamente la existencia de una alternativa de contingencia, evidenciando que la posibilidad de contar con un sistema de respaldo incidió de manera favorable en la percepción general de seguridad y confiabilidad por parte de la comunidad encuestada.

8.7 Evaluación del sistema mediante Evaluation Harness

La evaluación del módulo de reconocimiento facial se realizó en dos fases complementarias con el propósito de validar el comportamiento del sistema en condiciones progresivamente más cercanas al entorno real de uso. En la primera fase se utilizó el dataset LFW con un número reducido de identidades para verificar el correcto funcionamiento del modelo en condiciones controladas. En la segunda fase se amplió el

dataset a 100 perfiles con el fin de evaluar el rendimiento del sistema ante una galería de mayor tamaño, lo que permitió además ajustar el threshold de similitud de coseno a un valor más apropiado para escenarios con múltiples identidades.

8.7.1 Dataset utilizado: Labeled Faces in the Wild (LFW)

Para la evaluación se utilizó el dataset Labeled Faces in the Wild (LFW), un conjunto de datos de referencia ampliamente empleado en la literatura científica para la evaluación de sistemas de reconocimiento facial en condiciones no controladas (Luckianto, 2026). El dataset fue estructurado en tres directorios funcionales dentro del entorno de evaluación:

El directorio enroll/ contenía una fotografía representativa por cada identidad a enrolar en el sistema, correspondiente a 13 personas públicas reconocidas. El directorio identify/ organizaba las imágenes de prueba (probes) en subcarpetas por identidad, con múltiples fotografías por persona para evaluar la capacidad de reconocimiento del sistema. Finalmente, el directorio impostors/ agrupaba imágenes de personas no enroladas, cuya función fue verificar la capacidad del sistema para rechazar correctamente identidades desconocidas.

8.7.2 Tratamiento y preprocesamiento de las imágenes del dataset

El preprocesamiento de las imágenes constituye una etapa determinante en el rendimiento de los sistemas de reconocimiento facial, dado que la calidad y uniformidad de las imágenes de entrada incide directamente en la precisión del proceso de extracción de embeddings. Según (Zhalgas et al., 2025b), un procesamiento previo adecuado que incluya normalización de iluminación, alineación geométrica y estandarización del

tamaño de la imagen mejora la estabilidad de la entrada y potencia los resultados del reconocimiento.

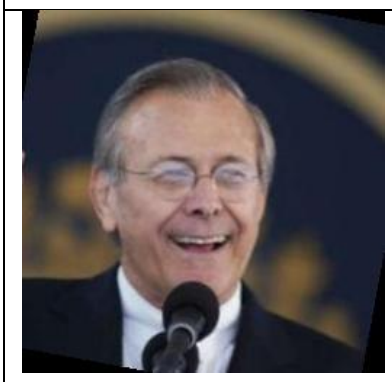
En el presente sistema, el harness impuso tres requisitos de calidad sobre cada imagen procesada. En primer lugar, cada imagen debía contener exactamente un rostro detectable; las imágenes con múltiples rostros fueron descartadas automáticamente, dado que la presencia de más de un rostro impide determinar con certeza cuál corresponde a la identidad evaluada. En segundo lugar, se estableció un tamaño mínimo de imagen para garantizar que el detector facial pudiera extraer características con suficiente resolución; las imágenes de tamaño insuficiente fueron rechazadas con la categoría imagen_pequeña. En tercer lugar, toda imagen en la que no se detectara ningún rostro fue descartada con la categoría sin_rostro. Este comportamiento es coherente con lo señalado por (Soekarta & Ku-Mahamud, 2025), quienes indican que la calidad de la imagen facial de entrada, en términos de resolución, nitidez y unicidad del rostro, es un factor crítico para la fiabilidad de los sistemas de identificación biométrica.

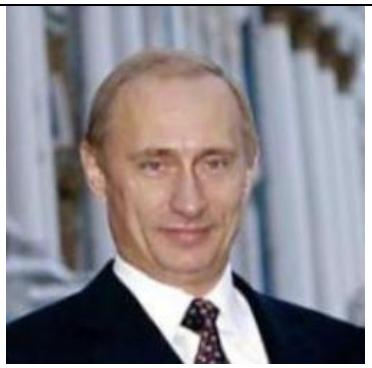
Como resultado de la aplicación de estos criterios de calidad sobre el dataset LFW, 135 imágenes fueron excluidas del proceso de evaluación: 125 por contener múltiples rostros, 7 por tamaño insuficiente y 3 por ausencia de rostro detectable. Las 588 imágenes restantes cumplieron los requisitos de preprocesamiento y fueron procesadas exitosamente por el sistema.

El dataset de evaluación comprendió en total 728 imágenes de prueba, distribuidas entre 13 identidades conocidas y un conjunto de impostores, lo que permitió medir tanto la tasa de aciertos sobre usuarios legítimos como la resistencia ante intentos

de acceso no autorizados. A continuación, se presenta una muestra representativa de las imágenes de cada directorio:

Directorio enroll/ — imágenes de enrolamiento:

Alvaro_Uribe	Ariel_Sharon	Arnold_Schwarzenegger
		
Bill_Clinton	**Colin_Powell**	**David_Beckham**
		
Donald_Rumsfeld	**George_W_Bush**	**Gerhard_Schroeder**
		

Hugo_Chavez	Junichiro_Koizumi	Tony_Blair
		
Vladimir_Putin		
		

Elaboración propia (2026).

Directorio identify/ — imágenes de prueba por identidad:

Alvaro_Uribe	Ariel_Sharon
	
Arnold_Schwarzenegger	**Bill_Clinton**

	
Colin_Powell	**David_Beckham**
	
Donald_Rumsfeld	**George_W_Bush**
	
Gerhard_Schroeder	**Hugo_Chavez**
	
Junichiro_Koizumi	**Tony_Blair**



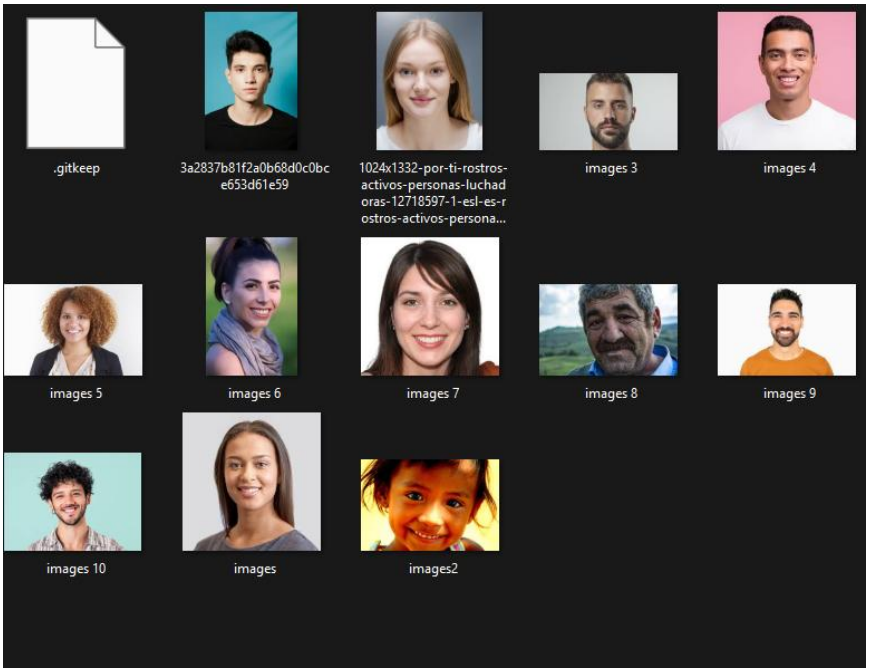


Vladimir_Putin



Elaboración propia (2026).

Directorio impostors/ — imágenes de personas no enroladas:



Elaboración propia (2026).

8.7.3 Configuración y ejecución del harness

El script fue ejecutado desde la terminal integrada de Visual Studio Code en el directorio backend/, configurando las variables de entorno requeridas para la autenticación y el acceso al sistema. La evaluación abarcó 13 valores de umbral (threshold) comprendidos entre 0.30 y 0.90 con incrementos de 0.05, lo que posibilitó un análisis comparativo del comportamiento del sistema ante diferentes niveles de exigencia en la similitud de coseno.

A continuación, se presenta la ejecución del harness desde la terminal:

```
Resumen por threshold
ThresholdTP    FP    TN    FN    Precision  Recall   F1       Errores
------------------------------------------------------------------------
0.30    588   0     5     0     100%       100%     100%     135
0.35    588   0     5     0     100%       100%     100%     135
0.40    587   0     5     1     100%       99.83%   99.91%   135
0.45    585   0     5     3     100%       99.49%   99.74%   135
0.50    582   0     5     6     100%       98.98%   99.49%   135
0.55    573   0     5     15    100%       97.45%   98.71%   135
0.60    543   0     5     45    100%       92.35%   96.02%   135
0.65    479   0     5     109   100%       81.46%   89.78%   135
0.70    334   0     5     254   100%       56.8%    72.45%   135
0.75    160   0     5     428   100%       27.21%   42.78%   135
0.80    36    0     5     552   100%       6.12%    11.54%   135
0.85    2     0     5     586   100%       0.34%    0.68%    135
0.90    0     0     5     588   0%         0%       0%       135

Threshold recomendado: 0.30
  Precision: 100%
  Recall:    100%
  F1-score:  100%

Rendimiento por identidad (threshold recomendado)
Identidad               TP    FP    FN    Prec.    Recall   F1       Usables  Errores
-----------------------------------------------------------------------------------------
Tony_Blair              124   0     0     100%     100%     100%     124      19
Gerhard_Schroeder       86    0     0     100%     100%     100%     86       21
Hugo_Chavez             48    0     0     100%     100%     100%     48       22
Colin_Powell            52    0     0     100%     100%     100%     52       7
Junichiro_Koizumi       52    0     0     100%     100%     100%     52       7
Ariel_Sharon            39    0     0     100%     100%     100%     39       9
Vladimir_Putin          39    0     0     100%     100%     100%     39       9
Arnold_Schwarzenegger   32    0     0     100%     100%     100%     32       9
Alvaro_Uribe            24    0     0     100%     100%     100%     24       10
George_W_Bush           26    0     0     100%     100%     100%     26       8
David_Beckham           29    0     0     100%     100%     100%     29       1
Bill_Clinton            24    0     0     100%     100%     100%     24       4
Donald_Rumsfeld         13    0     0     100%     100%     100%     13       2

Principales confusiones
  No se detectaron confusiones entre identidades en el threshold recomendado.

Distribucion de scores
  Aciertos
    count=588 mean=0.7065 min=0.3531 p25=0.6681 p50=0.7124 p75=0.7543 max=0.8678
  Confusiones
    count=0 mean=0 min=0 p25=0 p50=0 p75=0 max=0
  Conocidos rechazados
    count=0 mean=0 min=0 p25=0 p50=0 p75=0 max=0
  Impostores rechazados
    count=5 mean=0.0749 min=0.0427 p25=0.0664 p50=0.0724 p75=0.0939 max=0.0992

Errores de extraccion: 135
  Por categoria:
    - multiples_rostros: 125
    - imagen_pequena: 7
    - sin_rostro: 3
  Por identidad:
    - Hugo_Chavez: 22
    - Gerhard_Schroeder: 21
    - Tony_Blair: 19
    - Alvaro_Uribe: 10
    - Ariel_Sharon: 9
    - Arnold_Schwarzenegger: 9
    - Vladimir_Putin: 9
    - George_W_Bush: 8
    - Colin_Powell: 7
    - impostor: 7
```

Elaboración propia (2026).

Para cada valor de umbral evaluado, el harness calculó las siguientes métricas: Verdaderos Positivos (TP), Falsos Positivos (FP), Verdaderos Negativos (TN), Falsos Negativos (FN), Precisión, Recall y F1-score. Estas métricas son reconocidas en la literatura como los indicadores fundamentales para la evaluación de sistemas de identificación biométrica (Chavez Vargas, 2025).

8.7.4 Evaluación del sistema con perfiles reales enrolados

Para la segunda fase de evaluación se construyó un dataset ampliado conformado por 100 perfiles de identidades únicas, con el propósito de evaluar el comportamiento del sistema ante una galería de mayor tamaño y más representativa del entorno real de uso. A diferencia de la primera fase, en la cual se utilizaron identidades del dataset público LFW, los perfiles de esta segunda fase fueron registrados directamente en el sistema mediante el proceso de enrolamiento, generando embeddings de 512 dimensiones almacenados en la base de datos MongoDB.

El harness ejecutó un total de 12.603 pruebas sobre los 100 perfiles enrolados, realizando 1.018.700 comparaciones de similitud de coseno. Los thresholds evaluados abarcaron el rango de 0.30 a 0.90 con incrementos de 0.05, al igual que en la primera fase, permitiendo así una comparación directa entre ambas evaluaciones.

8.8 Dispositivos utilizados en las pruebas de reconocimiento facial

Para la realización de las pruebas internas de alcance del sistema de reconocimiento facial, se utilizaron dos dispositivos móviles: el Xiaomi 15T y el iPhone 17. La selección de smartphones en lugar de la webcam convencional integrada en el equipo de desarrollo se fundamentó en dos criterios técnicos y uno de representatividad del entorno real.

En cuanto a la calidad de imagen, la literatura académica establece que la resolución y nitidez de la imagen facial de entrada inciden directamente en la precisión del reconocimiento, siendo los sistemas basados en imágenes de baja resolución, como las provenientes de webcams integradas en equipos portátiles convencionales, especialmente susceptibles a errores de detección y extracción de características faciales (Zhalgas et al., 2025a). La webcam integrada del equipo de desarrollo HP Pavilion Gaming 15-dk1xxx cuenta con una resolución de 0.9 MP a 720p, mientras que el iPhone 17 dispone de una cámara frontal de 18 MP con sensor Sony IMX914 y estabilización óptica, y el Xiaomi 15T de una cámara frontal de 32 MP, lo que representa una diferencia significativa en la calidad de captura disponible para el procesamiento de imágenes faciales.

En cuanto a la representatividad del entorno real, el sistema fue desarrollado como una aplicación web compatible con cualquier dispositivo que disponga de cámara y navegador. El sistema puede operar desde una tableta o smartphone ubicado en el puesto de vigilancia, haciendo más representativas las pruebas realizadas con dispositivos móviles que las realizadas con una webcam de escritorio fija. Esta consideración es consistente con las tendencias actuales en sistemas de control de acceso biométrico, donde los dispositivos móviles con cámaras de alta resolución son cada vez más utilizados como sensores de captura (Zhalgas et al., 2025a).

A continuación, se presentan las especificaciones técnicas de los dispositivos utilizados:

Característica	HP Pavilion Gaming 15-dk1xxx	Xiaomi 15T	iPhone 17
Tipo	Laptop	Smartphone	Smartphone

Procesador	Intel Core i5-10300H 2.50 GHz	MediaTek Dimensity 8400-Ultra	Apple A19
RAM	16 GB DDR4	12 GB	8 GB
Sistema operativo	Windows 11 Pro	Android	iOS 26
Cámara frontal	0.9 MP, 720p	32 MP, f/2.2	18 MP Sony IMX914, f/1.9, OIS
Sensor cámara frontal	HD sensor integrado	Samsung KD1, 1/3.44"	Sony IMX914, 1.0µm
Resolución video frontal	720p	1080p / 4K	4K @ 60fps
Uso en el proyecto	Desarrollo y pruebas de reconocimiento facial	Pruebas de reconocimiento facial	Pruebas de reconocimiento facial

Nota. Elaboración propia (2026)

8.9 Procedimiento de las pruebas

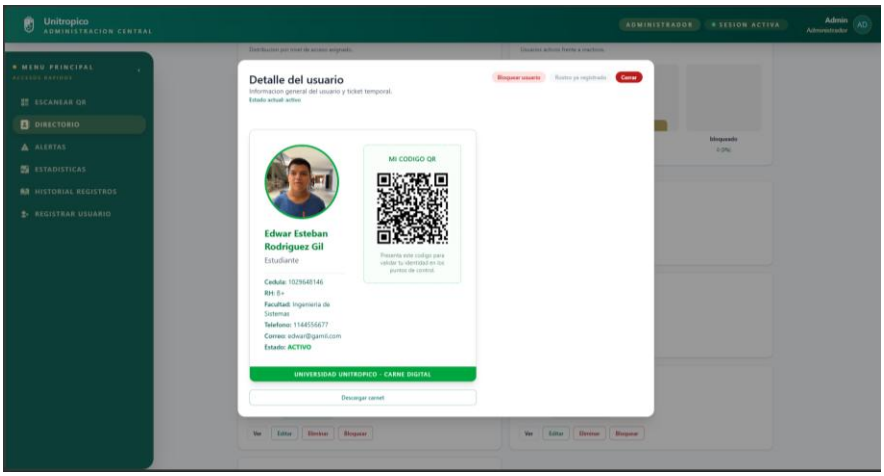
Antes del inicio de las pruebas, se informó a los participantes sobre los objetivos académicos del proyecto, las actividades a desarrollar y el tratamiento de los datos personales y biométricos requeridos para el funcionamiento del prototipo. La participación fue completamente voluntaria y estuvo respaldada por la firma de un consentimiento informado, mediante el cual los participantes autorizaron la captura y el tratamiento de su información biométrica exclusivamente para fines académicos y de investigación.

Se explicó la finalidad del tratamiento de los datos, el tiempo de conservación de la información, las medidas implementadas para su protección y el derecho de los participantes a retirar su consentimiento en cualquier momento, en cumplimiento de lo establecido en la Ley 1581 de 2012 sobre protección de datos personales.

Proceso de registro (enrolamiento)

Las pruebas de reconocimiento, cada estudiante participante fue registrado en el sistema. El estudiante se acercó al punto de prueba, proporcionó sus datos básicos de identificación y se capturó una fotografía de su rostro, la cual fue procesada por el módulo de reconocimiento facial para generar su embedding biométrico y almacenarlo en la base de datos. El registro pudo realizarse mediante dos métodos: asociación con el código QR del carnet institucional o registro manual de datos.

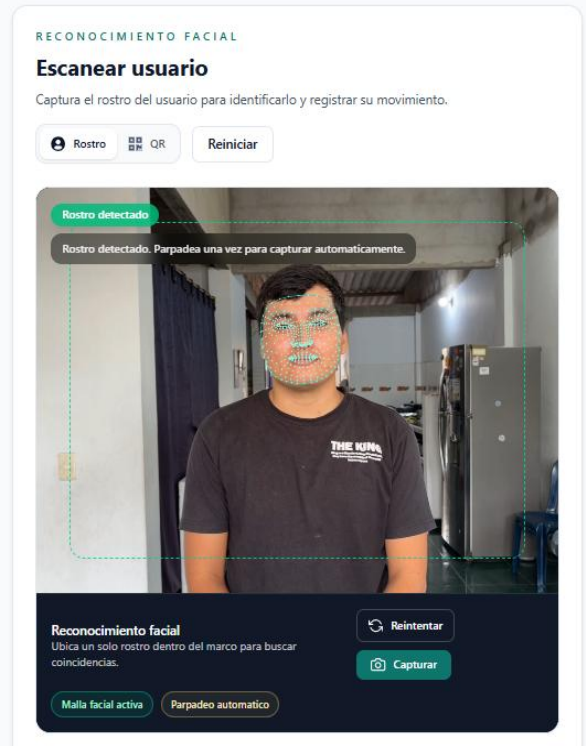


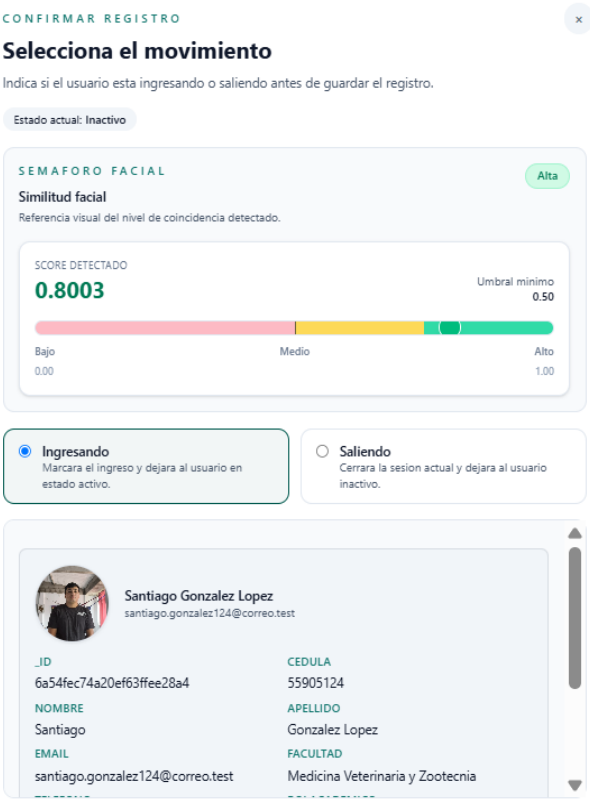


8.9.1 Proceso de reconocimiento facial

Una vez registrado el estudiante, se procedió a realizar la prueba de reconocimiento facial. El estudiante se posicionó frente a la cámara, el sistema activó la detección de rostro mediante MediaPipe FaceLandmarker y esperó el parpadeo automático para capturar la imagen. El sistema comparó el embedding generado con el embedding almacenado durante el registro, utilizando similitud de coseno con un threshold de 0.50, y mostró el resultado en pantalla: acceso concedido o acceso denegado. En caso de fallo, el sistema activó automáticamente el módulo de escaneo QR como mecanismo complementario.

El threshold de 0.50 fue definido con base en las pruebas internas realizadas previamente, donde se determinó que valores inferiores resultaban excesivamente permisivos. Con este umbral el sistema exige que la similitud entre el rostro capturado y el registrado supere el 50% para conceder el acceso,





8.10 Planificación y gestión de requerimientos ágiles

8.10.1 Historias de Usuario XP

Las historias de usuario son descripciones breves y simples de funcionalidades desde la perspectiva del usuario o cliente, que expresan lo que necesita y por qué en la metodología XP, las historias sirven para planificar y organizar el trabajo en iteraciones cortas. Se escriben de manera comprensible para todos los involucrados y deben ser lo suficientemente pequeñas para completarse dentro de una iteración, una historia no se considera finalizada hasta que pasa sus pruebas de aceptación (Max Rehkopf, 2025).

8.10.2 Criterios de Aceptación

Los criterios de aceptación son condiciones específicas y verificables que determinan cuándo una historia de usuario se considera cumplida y donde se definen

antes o al inicio de la implementación de la historia y permiten que el equipo y el cliente tengan claridad sobre lo que se espera, donde deben ser concretos, medibles y centrados en la perspectiva del usuario, evitando ambigüedades (Claudio, 2024).

8.10.3 Pruebas de Aceptación

Las pruebas de aceptación son procedimientos diseñados para verificar que una historia de usuario cumple con todos sus criterios de aceptación, en XP, estas pruebas confirman que la funcionalidad implementada satisface las necesidades del usuario o cliente e idealmente se automatizan y se ejecutan al finalizar la implementación de la historia para garantizar su correcto funcionamiento y servir también como pruebas de regresión en futuras iteraciones (Menzinsky et al., 2026).

8.10.4 Estructura de Historias de Usuario, Criterios y Backlog

Conforme a toda la información recolectada en la observación que nos ayudó a relacionar el uso del carnet en el proceso general de ingreso, así mismo como las entrevistas a los vigilante donde se identificaron puntos clave como el registro y no registro de aquellos que acceden al campus universitario, además de las funcionalidades que le gustaría ver el jefe del departamento de sistemas en el aplicativo web, se procedió a la elaboración y adaptación de las historias de usuario, criterios de aceptación y tareas específicas a modo de backlog según la metodología ágil utilizada, en este caso XP (Menzinsky et al., 2026).

Cuadro 1. Historia de Usuario Inicio de sesión.

Historia de Usuario	
Número: *1*	**Usuario:** *Usuario*
Nombre historia: *Inicio de sesión*	

Prioridad: *Alta*	**Riesgo en desarrollo:** *Bajo*
Puntos estimados: *3*	**Iteración asignada:** *1*
Programador responsable: *Didier Antonio Niño Gonzalez*	
Descripción: *Como usuario registrado quiero iniciar sesión con mis credenciales para acceder a mi cuenta.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El usuario debe poder iniciar sesión usando correo y contraseña válidos.
- Si el usuario ingresa datos incorrectos, debe mostrar un mensaje claro de error.
- Después de iniciar sesión, el usuario debe ser redirigido a su panel correspondiente según su rol.

Pruebas de Aceptación

- Iniciar sesión con un usuario registrado y confirmar que accede correctamente al panel.
- Ingresar credenciales incorrectas y validar que el sistema muestre un mensaje indicando que las credenciales son inválidas.
- Cerrar sesión y verificar que ya no se tenga acceso al panel sin iniciar sesión nuevamente.

Tabla 5. Backlog de tareas, Inicio de sesión.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Diseñar la interfaz del formulario de inicio de sesión (inputs, botones, estilos).	**2 h**
02	Implementar validación de campos (correo y contraseña) en el frontend.	**3 h**
03	Crear endpoint en el backend para autenticar usuarios registrados.	**4 h**
04	Conectar el frontend con el backend para enviar credenciales al servidor.	**3 h**

05	Implementar manejo de errores para credenciales incorrectas.	**2 h**

Nota. Elaboración propia (2026).

Cuadro 2. Historia de usuario, Ver información general.

Historia de Usuario	
Número: *2*	**Usuario:** *Usuario*
Nombre historia: *Ver información general*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Medio*
Puntos estimados: *3*	**Iteración asignada:** *1*
Programador responsable: *Harold Stiven Gutierrez Orduz*	
Descripción: *Como usuario quiero ver la información general y el estado de mi ingreso*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El sistema debe permitir al usuario visualizar su información general registrada en la base de datos.
- La información mostrada debe incluir datos básicos del usuario (nombre, identificación, tipo de usuario, entre otros).
- El usuario debe poder consultar el estado actual de su ingreso (activo o inactivo).

Pruebas de Aprobación

- La funcionalidad se considera aprobada cuando el usuario puede visualizar correctamente su información general y el estado de su ingreso sin errores.
- Los datos visualizados deben coincidir con la información almacenada en la base de datos.

Tabla 6. Backlog de tareas, Ver información general.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)

01	Diseñar la interfaz de visualización de información general utilizando Tailwind CSS, mostrando los datos del usuario y su estado de ingreso con estilos responsivos.	**3 h**
02	Crear el endpoint en el backend que obtenga la información del usuario desde la base de datos según su ID o token de sesión.	**4 h**
03	Conectar el frontend con el backend para mostrar los datos en la interfaz y validar que coincidan con los registros almacenados.	**3 h**

Nota. Elaboración propia (2025).

Cuadro 3. Historia de usuario, Crear y gestionar vigilante.

Historia de Usuario	
Número: 3	**Usuario:** *Administrador*
Nombre historia: Crear y gestionar vigilante	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Alta*
Puntos estimados: *3*	**Iteración asignada:** *1*
Programador responsable: *Didier Antonio Niño Gonzalez*	
Descripción: *Como administrador quiero crear usuarios tipo vigilante con permiso de la gestión de acceso*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El sistema debe permitir al administrador crear nuevos usuarios con el rol de vigilante.
- Durante la creación, el administrador debe poder asignar información básica (nombre, usuario, contraseña y correo).
- El sistema debe permitir asignar permisos específicos al rol de vigilante, especialmente los relacionados con la gestión de acceso.
- El administrador debe poder editar o eliminar usuarios tipo vigilante según sea necesario.

- Solo los usuarios con rol de administrador podrán acceder a esta funcionalidad.
- Al crear o modificar un vigilante, el sistema debe mostrar un mensaje de confirmación o error según el resultado de la acción.

Pruebas Aprobación

- El administrador puede crear, editar y eliminar usuarios tipo vigilante correctamente.
- Los permisos asignados deben permitir al vigilante gestionar accesos sin tener privilegios de administrador.

Tabla 7. Backlog de tareas, Crear y gestionar vigilantes.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Diseñar la interfaz para la creación, edición de usuarios tipo vigilante, con formulario de registro y lista de usuarios existentes.	**4 h**
02	Implementar el endpoint en el backend para crear, actualizar usuarios tipo vigilante con sus respectivos permisos.	**5 h**
03	Configurar el control de roles y permisos, asegurando que solo los administradores puedan acceder a esta funcionalidad.	**4 h**

Nota. Elaboración propia (2026).

Cuadro 4. Historia de usuario, Registro usuario.

	Historia de Usuario
Número: 4	**Usuario:** *Administrador*
Nombre historia: *Registro de usuario*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Bajo*
Puntos estimados: *1*	**Iteración asignada:** *1*
Programador responsable: *Harold Stiven Gutierrez Orduz*	
Descripción: *Como administrador quiero registrar usuarios en la plataforma.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El sistema debe solicitar nombre completo, identificación, correo y contraseña.
- El correo y la identificación no pueden estar registrados previamente.
- La contraseña debe tener mínimo 8 caracteres, una mayúscula y un número.
- Al completar el registro correctamente, el sistema debe mostrar un mensaje de confirmación.

Pruebas de Aceptación

- Registrar un usuario nuevo con datos correctos y verificar que el sistema muestra un mensaje de registro exitoso.
- Intentar registrar un usuario con un correo ya registrado y verificar que se muestre un mensaje indicando que el correo ya existe.
- Intentar utilizar una contraseña débil y verificar que el sistema no permite avanzar y muestre un mensaje explicando el requisito.

Tabla 8. Backlog de tareas, Registro de usuario.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Diseñar y desarrollar el formulario de registro con campos: nombre, identificación, correo y contraseña.	**2 h**
02	Implementar validaciones de formato, seguridad y verificación de duplicados en la base de datos.	**3 h**
03	Mostrar mensajes de confirmación o error según el resultado del registro.	**1 h**

Nota. Elaboración propia (2026).

Cuadro 5. Historia de usuario, Dashboard de estadísticas.

	Historia de Usuario
Número: 5	**Usuario:** *Administrador*

Nombre historia: *Dashboard de estadísticas*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Alto*
Puntos estimados: ***3***	**Iteración asignada:** *1*
Programador responsable: *Harold Stiven Gutierrez Orduz*	
Descripción: *Como administrador quiero visualizar estadísticas de acceso en gráficos para analizar patrones de ingreso y picos.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El administrador debe visualizar estadísticas gráficas sobre los accesos del sistema.
- Debe mostrar como mínimo:
    - Cantidad de entradas por día
    - Cantidad de accesos por hora
    - Accesos por rol de usuario
- Los datos deben actualizarse automáticamente o con botón de refrescar.

Pruebas de Aceptación

- Ingresar al dashboard y validar que se muestran las gráficas de acceso correspondientes.
- Validar que, al cambiar el rango de filtros, las estadísticas se actualicen correctamente.
- Simular accesos de diferentes roles y verificar que se reflejan en las estadísticas.

Tabla 9. Backlog de tareas, Dashboard de estadísticas.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Diseñar el Overview del dashboard con secciones para gráficos de accesos y filtros.	**3 h**
02	Implementar la obtención y procesamiento de datos estadísticos desde la base de datos.	**4 h**
03	Integrar gráficos dinámicos y funcionalidad de actualización automática o manual.	**3 h**

Nota. Elaboración propia (2026).

Cuadro 6. Historia de usuario, ver datos de ingreso y salida.

	Historia de Usuario
Número: 6	**Usuario:** *Administrador*
Nombre historia: *Ver datos de ingreso y salida*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Alto*
Puntos estimados: 3	**Iteración asignada:** *1*
Programador responsable: *Harold Stiven Gutierrez Orduz*	
Descripción: *Quiero ver un listado de los ingresos y salidas para monitorear y auditar el uso del sistema.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El sistema debe permitir al administrador visualizar un listado completo de los registros de ingreso y salida de los usuarios.
- Cada registro debe mostrar información como: nombre del usuario, hora de entrada, hora de salida y estado actual.
- El listado debe poder filtrar por fecha, tipo de ingreso y nombre del usuario.
- Solo los usuarios con rol de administrador podrán acceder a esta vista.

Aprobación

- El administrador puede visualizar correctamente los registros de ingreso y salida sin errores.
- Los datos deben coincidir con los almacenados en la base de datos.
- Los filtros y opciones de ordenamiento deben funcionar correctamente.
- La interfaz debe mostrar la información de manera clara y organizada, facilitando la auditoría del sistema.

Tabla 10. Backlog de tareas, Ver datos de ingreso y salida.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Maquetar y estilizar el componente React para listar los registros de acceso (entradas y salidas) con filtros	**3 h**
02	Conectar el componente al backend mediante un endpoint GET que recupere los registros desde MongoDB.	**4 h**
03	Añadir funciones de filtrado y ordenamiento dinámico por fecha, tipo de ingreso y usuario.	**3 h**

Nota. Elaboración propia (2026).

Cuadro 7. Historia de usuario, Editar datos de usuario y rol.

	Historia de Usuario
Número: *7*	**Usuario:** *Administrador*
Nombre historia: *Editar datos de usuario y rol*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Alta*
Puntos estimados: *3*	**Iteración asignada:** *2*
Programador responsable: *Harold Stiven Gutierrez Orduz*	
Descripción: *Como administrador quiero editar los datos, rol y estado de un usuario para mantener actualizada su información y permisos.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El administrador debe poder actualizar datos personales del usuario, rol y su estado (activo/inactivo).
- Debe solicitar confirmación para cambios sensibles (como cambio de rol).
- Debe registrarse qué administrador realizó la modificación.

Pruebas de Aceptación

- Editar los datos del usuario y verificar que se actualicen correctamente.
- Cambiar rol de usuario a guardia y confirmar acceso a funciones de guardia.

- Verificar que al editar se registre la acción.

Tabla 11. Backlog de tareas – Editar datos de usuario y rol.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Diseñar e implementar la interfaz de edición que muestre los datos del usuario, su rol actual y estado (activo/inactivo), con campos editables y confirmación de cambios.	**3 h**
02	Desarrollar la lógica en backend para actualizar los datos del usuario, el rol asignado y el estado, registrando la acción del administrador en la base de datos para auditoría.	**4 h**
03	Implementar validaciones y alertas de confirmación para modificaciones críticas (cambio de rol o desactivación), garantizando la consistencia de permisos en el sistema.	**3 h**

Nota. Elaboración propia (2026).

Cuadro 8. Historia de usuario, Comparativo histórico de acceso

Historia de Usuario	
Número: 8	**Usuario:** *Administrador*
Nombre historia: *Comparativo histórico de acceso*	
Prioridad: *Medio*	**Riesgo en desarrollo:** *Medio*
Puntos estimados: *3*	**Iteración asignada:** 2
Programador responsable: *Harold Stiven Gutierrez Orduz*	
Descripción: *Como administrador quiero consultar datos estadísticos de acceso entre días, semanas o meses para analizar tendencias.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El administrador debe poder comparar datos entre días, semanas y/o meses.
- Debe mostrar tendencia de aumento o disminución.
- Debe permitir seleccionar rango de fechas.

Pruebas de Aceptación

- Comparar dos períodos y verificar que los datos cambian correctamente según el rango.
- Confirmar que el gráfico refleje correctamente la diferencia entre períodos.
- Validar que el resumen muestre porcentaje de aumento o reducción.

Tabla 12. Backlog de tareas, Comparativo histórico de acceso.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Diseñar y programar el módulo de filtrado temporal en React, permitiendo seleccionar rangos (día, semana, mes) y enviarlos como parámetros a la API.	**4 h**
02	Crear endpoint que realice consultas agregadas en MongoDB con funciones para generar estadísticas comparativas entre períodos.	**5 h**
03	Renderizar gráficos dinámicos en el Dashboard con librerías como *Recharts* o *Chart.js*, mostrando tendencias y porcentajes de variación.	**4 h**

Nota. Elaboración propia (2026).

Cuadro 9. Historia de usuario, Reporte de personas dentro vs afuera.

Historia de Usuario	
Número: 9	**Usuario:** *Administrador*
Nombre historia: *Reporte de personas dentro vs fuera*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Alta*
Puntos estimados: *2*	**Iteración asignada:** *2*
Programador responsable: *Didier Antonio Niño Gonzalez*	
Descripción: *Como administrador quiero ver el número de personas dentro y fuera del campus en tiempo real para conocer el movimiento de acceso.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El administrador debe ver el número de personas dentro actualmente y total fuera.

- Debe permitir ver el listado de las personas dentro con hora de ingreso.

Pruebas de Aceptación

- Validar que el contador aumenta al ingresar personas y disminuye al salir.
- Visualizar listado y confirmar datos correctos.

Tabla 13. Backlog de tareas, Reporte de personas vs afuera.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Diseñar e implementar la interfaz de reporte en React para visualizar el número de personas dentro y fuera del campus en tiempo real.	**4 h**
02	Desarrollar el endpoint en Node.js y la consulta en MongoDB para calcular la cantidad de personas que se encuentran dentro y fuera del campus según su estado de ingreso y salida.	**5 h**
03	Implementar el listado de personas que se encuentran dentro del campus, mostrando nombre, identificación y hora de ingreso.	**3 h**
04	Integrar la información del backend con el frontend para actualizar automáticamente los contadores y el listado de personas.	**3 h**

Nota. Elaboración propia (2026).

Cuadro 10. Historia de usuario, Ver personas dentro actualmente.

Historia de Usuario	
Número: *10*	**Usuario:** Vigilante*/Administrador*
Nombre historia: *Ver personas dentro actualmente*	
Prioridad: *Medio*	**Riesgo en desarrollo:** *Medio*
Puntos estimados: *2*	**Iteración asignada:** *2*
Programador responsable: *Didier Antonio Niño Gonzalez*	
Descripción: *Como vigilante quiero ver cuántas y cuáles personas están actualmente dentro de la Universidad.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El vigilante y/o administrador debe ver un listado de personas que ingresaron y aún no han registrado salida.
- Listar nombre, rol y hora de entrada.
- Debe actualizarse automáticamente o con botón de refrescar.

Pruebas de Aceptación

- Verificar que usuarios con entrada sin salida aparezcan en el listado.
- Probar actualización automática/manual y confirmar que funciona.

Tabla 14. Backlog de tareas, Ver personas dentro actualmente.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Desarrollar la consulta para obtener los usuarios con registro de entrada sin salida desde la base de datos	**3 h**
02	Crear la vista que muestre el listado de personas dentro con nombre, rol y hora de ingreso	**2 h**
03	Configurar la actualización automática o manual del listado mediante botón de refrescar o recarga.	**2 h**

Nota. Elaboración propia (2026).

Cuadro 11. Historia de usuario, Registrar salida.

	Historia de Usuario
Número: *11*	**Usuario:** *Vigilante*
Nombre historia: *Registrar salida*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Medio*
Puntos estimados: 2	**Iteración asignada:** *2*
Programador responsable: *Didier Antonio Niño Gonzalez*	
Descripción: *Como vigilante quiero registrar la salida del usuario para llevar control de permanencia.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El vigilante debe poder registrar la salida del usuario escaneando el mismo QR.

- Si el usuario no tiene un ingreso registrado sin salida, el sistema debe mostrar un mensaje de advertencia.
- El sistema debe calcular la duración de la permanencia y guardarla en el registro.

Pruebas de Aceptación

- Registrar la salida de un usuario que tiene ingreso pendiente y verificar que el sistema guarde fecha, hora y duración.
- Intentar registrar la salida de un usuario que ya salió y verificar que se muestre un mensaje indicando que no hay ingreso activo.

Tabla 15. Backlog de tareas, Registrar salida.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Desarrollar la función que permita registrar la salida de usuarios mediante la lectura del código QR	**2 h**
02	Configurar validaciones para detectar si el usuario no tiene un ingreso activo antes de registrar la salida	**2 h**
03	Implementar el cálculo automático de la duración de permanencia y almacenamiento del registro actualizado en la base de datos	**3 h**

Nota. Elaboración propia (2026).

Cuadro 12. Historia de usuario, Escanear QR

	Historia de Usuario
Número: *12*	**Usuario:** *Vigilante*
Nombre historia: *Escanear QR*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Medio*
Puntos estimados: *2*	**Iteración asignada:** *2*
Programador responsable: *Didier Antonio Niño Gonzalez*	
Descripción: *Como vigilante quiero que el sistema al escanear el QR me muestre la información de la persona para validar su acceso*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El vigilante debe poder escanear el QR con su dispositivo.
- Al escanear, se deben mostrar: nombre, rol y estado.
- Si el QR no existe, el sistema debe mostrar un mensaje claro y negar el acceso.

Pruebas de Aceptación

- Escanear el QR de un usuario activo y verificar que se muestre su información y la opción de permitir acceso.
- Escanear el QR de un usuario no existente para verificar que se muestre mensaje de “No fue posible interpretar el contenido escaneado”.

Tabla 16. Backlog de tareas, Escanear QR.

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Implementar la funcionalidad de lectura QR utilizando la cámara del dispositivo del vigilante y asegurar compatibilidad con navegadores móviles.	**3 h**
02	Desarrollar la lógica para decodificar el contenido del QR y consultar los datos del usuario (nombre, rol y estado) desde la base de datos.	**2 h**
03	Programar el manejo de excepciones para mostrar mensajes claros ante códigos inválidos, caducados o inexistentes.	**2 h**

Nota. Elaboración propia (2026).

Cuadro 13. Historia de usuario, Verificar acceso mediante reconocimiento facial

	Historia de Usuario
Número: *13*	**Usuario:** *Vigilante*
Nombre historia: *Verificar acceso mediante reconocimiento facial*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Alto*
Puntos estimados: 5	**Iteración asignada:** *3*
Programador responsable: *Didier Antonio Niño Gonzalez*	

Descripción: *Como vigilante quiero que el sistema identifique automáticamente a una persona mediante reconocimiento facial para permitir o denegar su acceso a la universidad.*

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El sistema debe activar la cámara automáticamente al iniciar el módulo de verificación.
- La IA debe identificar el rostro del usuario y compararlo con los registros biométricos almacenados.
- Si la coincidencia supera el umbral de confianza definido, el sistema debe mostrar los datos del usuario y conceder el acceso.
- Si la coincidencia es inferior al umbral, el sistema debe denegar el acceso y registrar el intento fallido.

Pruebas de Aceptación

- Posicionar a un usuario registrado frente a la cámara y verificar que el sistema lo identifica correctamente y concede acceso en menos de 5 segundos.
- Posicionar a una persona no registrada y verificar que el sistema deniega el acceso y muestra un mensaje claro.
- Probar con baja iluminación y verificar que el sistema muestre advertencia de condiciones inadecuadas.

Tabla 17. Backlog de tareas, Verificar acceso mediante reconocimiento facial

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Integrar la librería de reconocimiento facial con el módulo de cámara del navegador	**3 h**

02	Desarrollar el flujo de captura, análisis y comparación del rostro contra los vectores biométricos almacenados en base de datos	**2 h**
03	Implementar la lógica de umbral de confianza y respuesta del sistema (acceso concedido / denegado) con registro del evento	**2 h**
04	Diseñar la interfaz de verificación con guía visual de posicionamiento del rostro y estados del proceso	**3 h**

Nota. Elaboración propia (2026).

Cuadro 14. Historia de usuario, Registrar rostro biométrico de un usuario

Historia de Usuario	
Número: *14*	**Usuario:** *Administrador*
Nombre historia: *Registrar rostro biométrico de un usuario*	
Prioridad: *Alta*	**Riesgo en desarrollo:** *Alto*
Puntos estimados: 4	**Iteración asignada:** *3*
Programador responsable: *Didier Antonio Niño Gonzalez*	
Descripción: *Como administrador quiero capturar y registrar el rostro biométrico de un usuario nuevo para que pueda ser identificado posteriormente por el sistema de reconocimiento facial con IA.*	

Nota. Elaboración propia (2026).

Criterios de Aceptación

- El administrador debe poder capturar el rostro desde la cámara del dispositivo o subir una foto desde el equipo.
- El sistema debe procesar la imagen y generar el vector biométrico facial del usuario para almacenarlo vinculado a su perfil.
- Si la imagen no tiene la calidad suficiente (mala iluminación, rostro parcial, múltiples rostros), el sistema debe rechazarla e indicar el motivo.
- El registro biométrico debe quedar asociado a los datos personales del usuario (cédula, nombre, rol, facultad).

- Solo el administrador puede realizar esta acción.

Pruebas de Aceptación

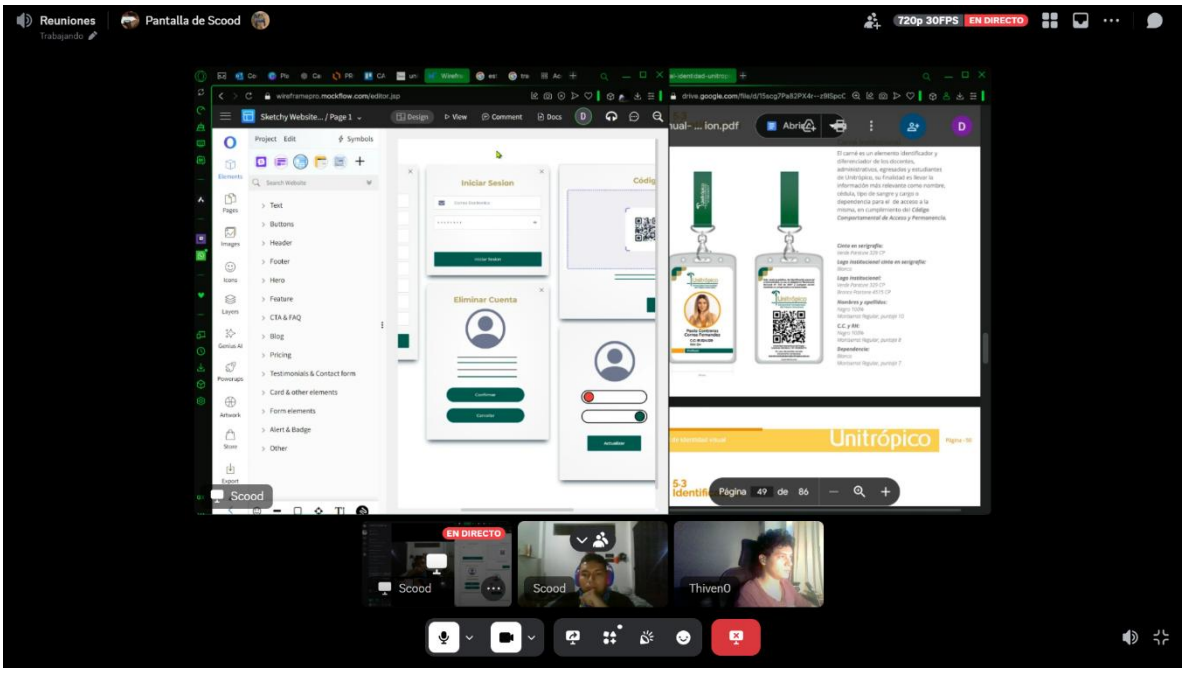
- Registrar el rostro de un usuario nuevo con buenas condiciones de captura y verificar que el vector biométrico se almacena correctamente y el usuario puede acceder por reconocimiento facial.
- Intentar registrar una foto borrosa o con múltiples rostros y verificar que el sistema la rechaza con un mensaje descriptivo.
- Intentar acceder al módulo de registro biométrico con perfil de vigilante y verificar que el acceso es denegado.

Tabla 18. Backlog de tareas, Registrar rostro biométrico de un usuario

ID Tarea	Descripción de la tarea o actividad	Estimación (horas)
01	Desarrollar el módulo de captura de imagen desde cámara en tiempo real y carga de archivo desde el dispositivo	**3 h**
02	Implementar validaciones de calidad de imagen: iluminación, número de rostros detectados y nitidez mínima requerida	**2 h**
03	Integrar la generación del vector biométrico facial a partir de la imagen capturada y almacenarlo en base de datos vinculado al usuario	**2 h**
04	Restringir el acceso al módulo exclusivamente al perfil administrador mediante control de roles	**3 h**

Nota. Elaboración propia (2026).

8.11 Diseño de mockups.



Nota. Imagen tomada por los autores (2026).

8.11.1 Herramientas y metodología

Los mockups fueron desarrollados utilizando herramientas de diseño como MockFlow, empleando principios de usabilidad, consistencia visual y coherencia con la identidad del proyecto. Se definieron colores, tipografías y componentes reutilizables para mantener una experiencia de usuario uniforme.

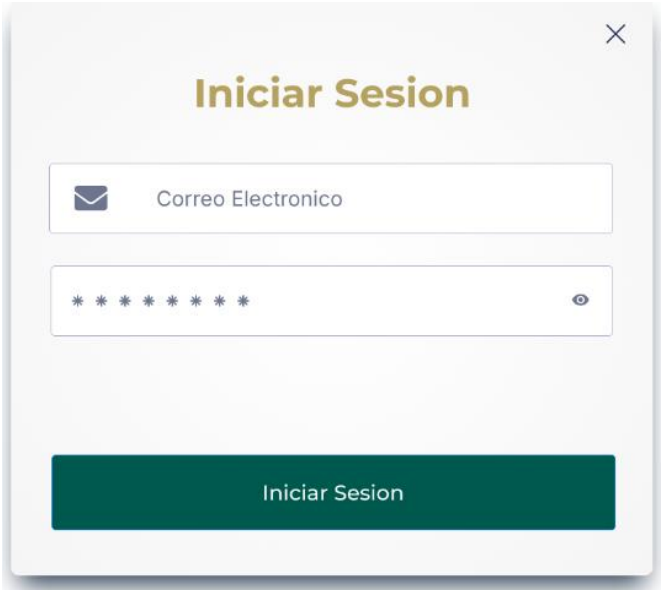
8.11.2 Mockups del proyecto

A continuación, se presentan los mockups correspondientes a las principales pantallas del sistema:

8.11.3 Pantalla de inicio de sesión

Permite el acceso de usuarios registrados mediante correo y contraseña.

8.11.4 Mockup de la pantalla de inicio de sesión.

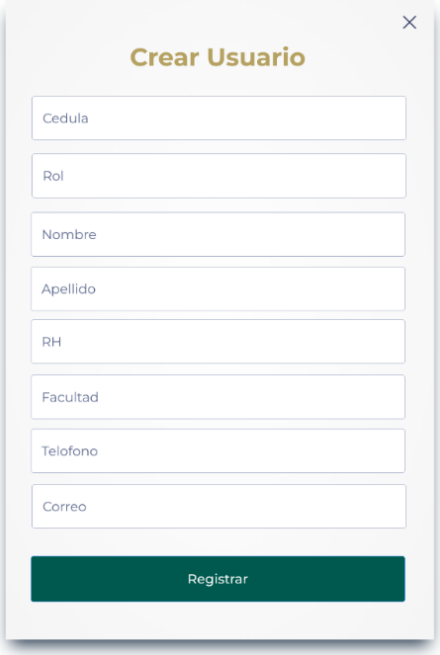


Nota: Elaboración propia en MockFlow, 2026.

8.11.5 Pantalla Crear Usuario

Permite registrar nuevos usuarios en el sistema, incluyendo nombre, correo, contraseña y rol asignado.

8.11.6 Mockup Crear Usuario

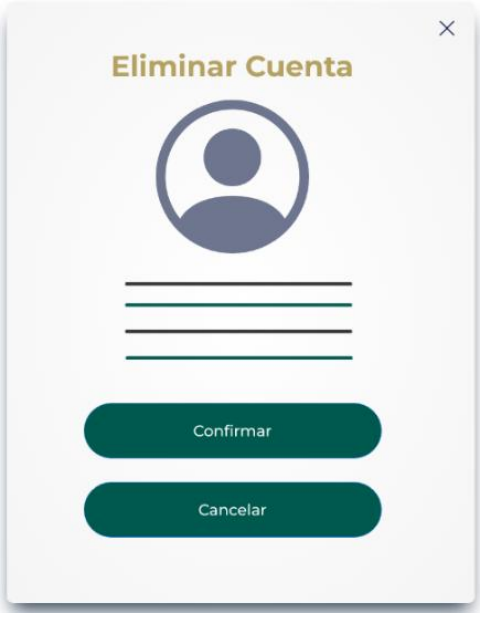


Nota: Elaboración propia en MockFlow, 2026.

8.11.7 Pantalla Eliminar Cuenta

Permite al usuario eliminar una cuenta registrada en el aplicativo web, mostrando un mensaje de confirmación antes de realizar la acción.

8.11.8 Mockup de la pantalla Eliminar Cuenta.

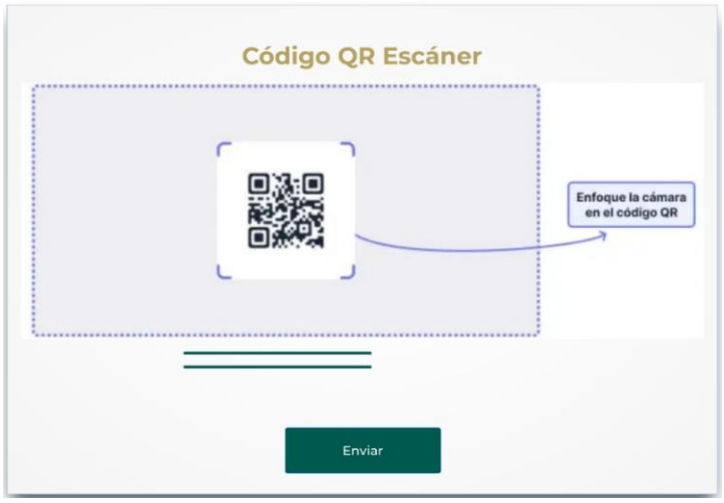


Nota: Elaboración propia en MockFlow, 2026.

8.11.9 Pantalla Escanear QR

Permite al usuario escanear un código QR para validar la información del carnet de manera rápida y segura.

8.11.10 Mockup de la pantalla Escanear QR.

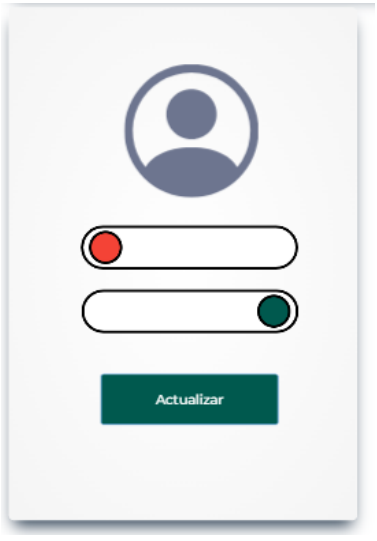


Nota: Elaboración propia en MockFlow, 2026.

8.11.11 Pantalla Estado de Usuario (Activo/Inactivo)

Permite visualizar y actualizar el estado de los usuarios en el aplicativo, marcándolos como activos o inactivos según corresponda.

8.11.12 Mockup de pantalla Estado de Usuario



Nota: Elaboración propia en MockFlow, 2026.

8.11.13 Pantalla Actualizar Información

Permite modificar los datos de los usuarios registrados en el aplicativo web, garantizando que la información se mantenga actualizada y correcta.

8.11.14 Mockup de la pantalla Actualizar Información.



Nota: Elaboración propia en MockFlow, 2026.

8.11.15 Pantalla Lista de Usuarios

Permite visualizar la lista de usuarios registrados en el sistema, incluyendo sus datos personales y el estado (activo/inactivo), con opciones para editar la información de cada usuario.

8.11.16 Mockup de la pantalla Lista de Usuarios.

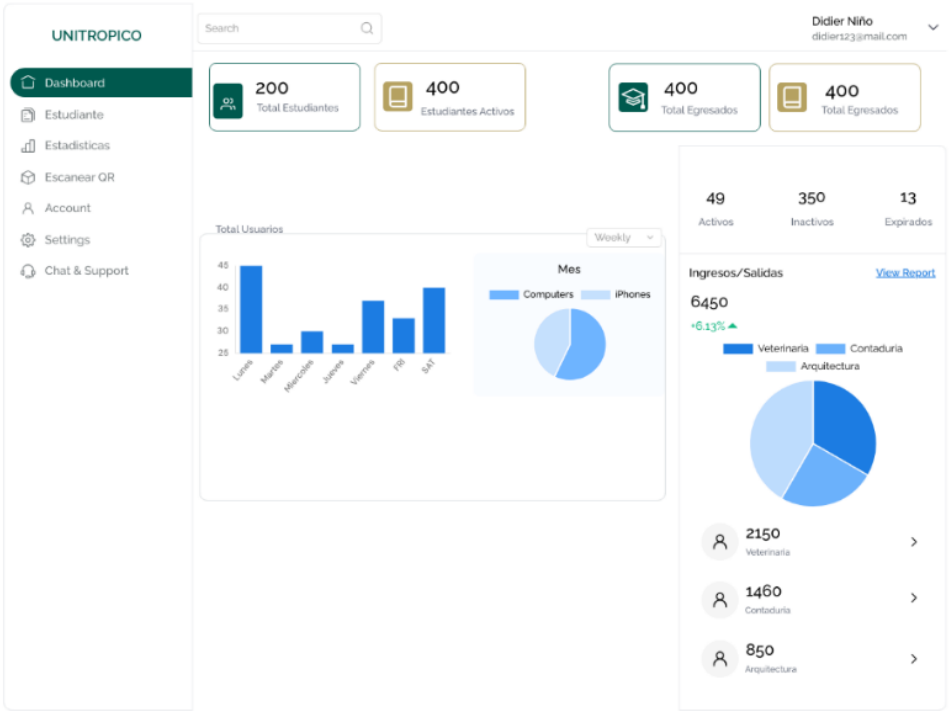


Nota: Elaboración propia en MockFlow, 2026.

8.11.17 Pantalla Dashboard Estadísticas y Datos

Permite visualizar un resumen general del aplicativo web, incluyendo estadísticas de usuarios, indicadores de estado, gráficos de rendimiento y accesos rápidos a los módulos principales.

8.11.18 Mockup de la pantalla Dashboard.

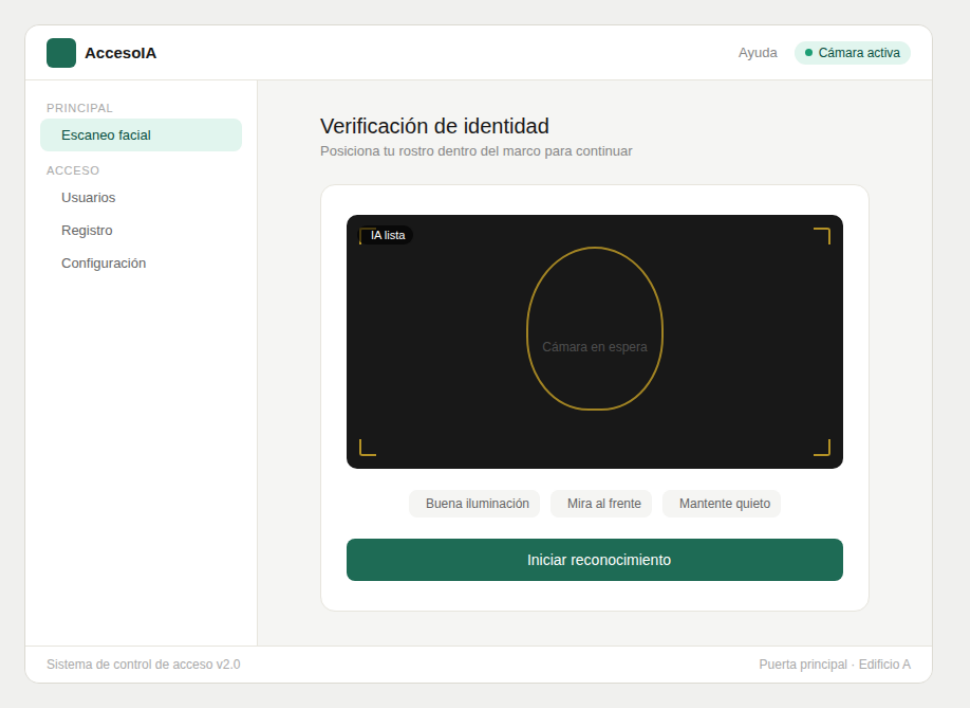


Nota: Elaboración propia en MockFlow, 2026.

8.11.19 Pantalla de escaneo facial

Permite iniciar el proceso de reconocimiento facial para el control de acceso. Muestra la vista de la cámara en tiempo real con una guía de posicionamiento del rostro, indicadores de estado de la IA y consejos para una captura óptima.

8.11.20 Mockup escaneo facial

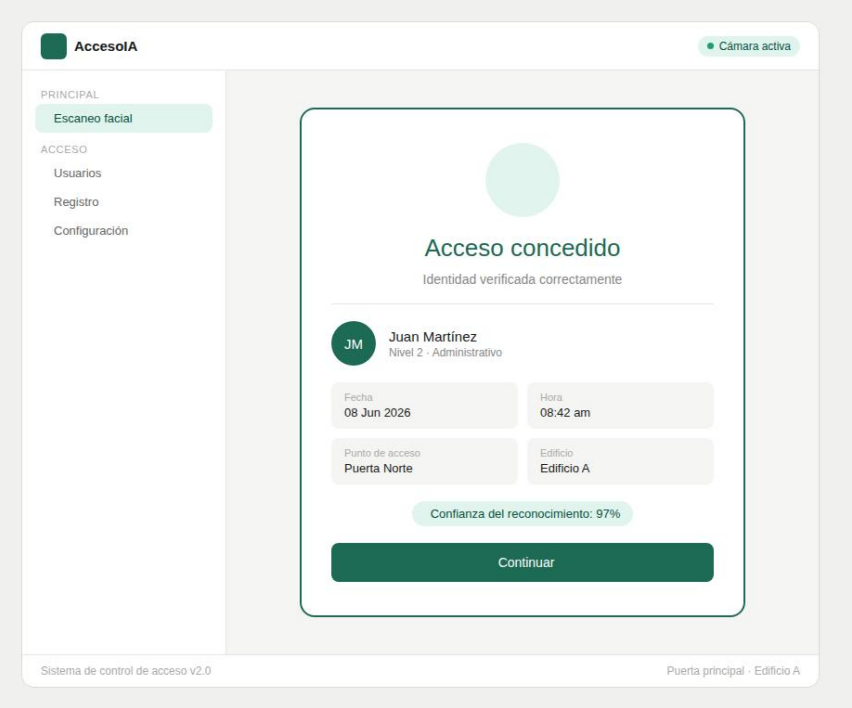


Nota: Elaboración propia en MockFlow, 2026.

8.11.21 Pantalla de resultado Acceso concedido / Acceso denegado

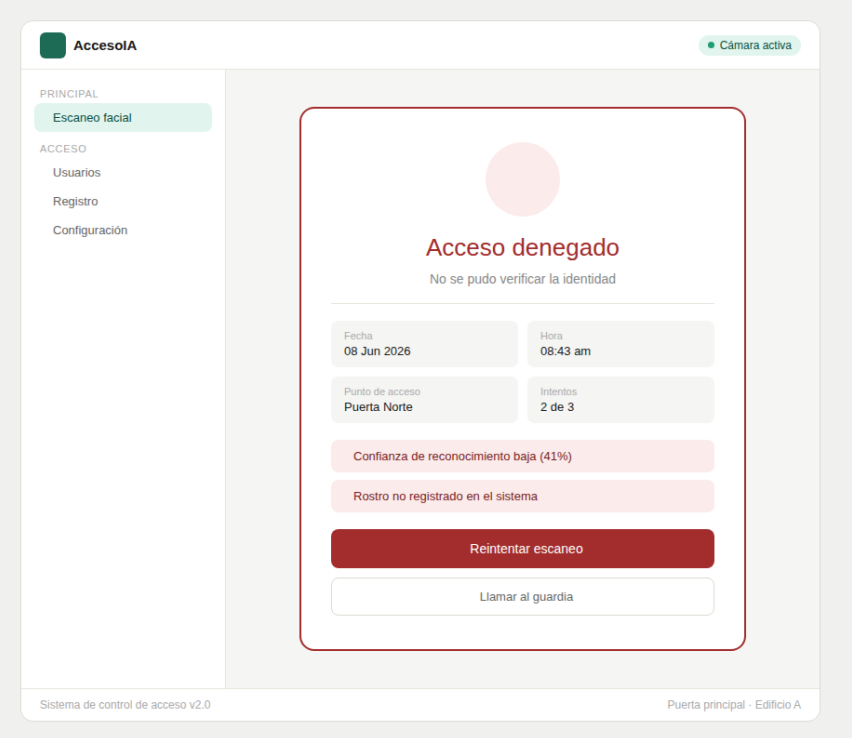
Muestra el resultado del proceso de verificación biométrica. En caso de éxito, presenta los datos del usuario identificado, la hora y el punto de acceso. En caso de fallo, indica el motivo del rechazo y ofrece la opción de reintentar o contactar al guardia.

8.11.22 Mockup acceso concedido



Nota: Elaboración propia en MockFlow, 2026.

8.11.23 Mockup acceso denegado

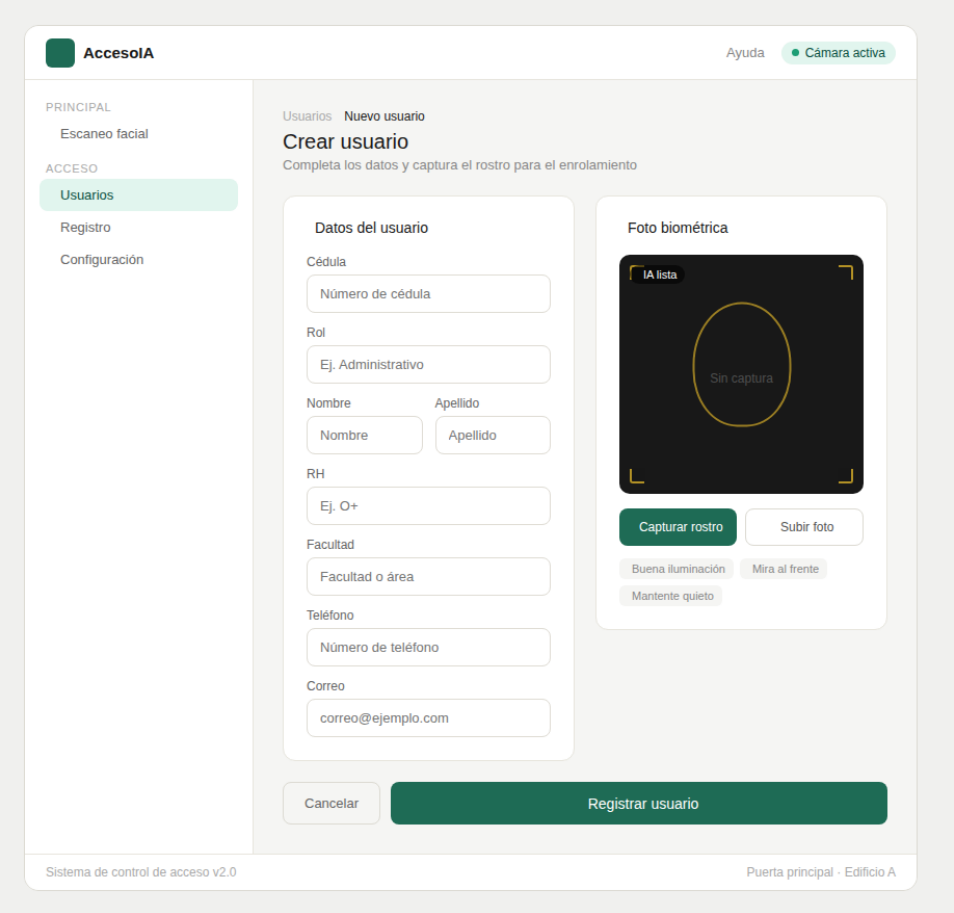


Nota: Elaboración propia en MockFlow, 2026.

8.11.24 Pantalla de registro

Permite registrar un nuevo usuario en el sistema mediante un formulario con sus datos personales (cédula, rol, nombre, apellido, RH, facultad, teléfono y correo) y la captura biométrica de su rostro a través de la cámara integrada.

8.11.25 Mockup crear nuevo usuario



Nota: Elaboración propia en MockFlow, 2026.

Tabla 19. Requisitos Funcionales.

Tabla de Requisitos Funcionales		
Código	**Nombre**	**Descripción**
RF1	Registro de usuarios	El sistema debe permitir registrar un usuario con sus datos básicos de identificación.

RF2	Carga de imagen facial	El sistema debe permitir cargar una imagen facial asociada a un usuario para su proceso de enrolamiento.
RF3	Validación de formato de imagen	El sistema debe validar que la imagen cargada tenga un formato permitido, como JPG, JPEG o PNG.
RF4	Validación de integridad de imagen	El sistema debe verificar que la imagen enviada no esté vacía o corrupta antes de procesarla.
RF5	Detección de rostro	El sistema debe detectar la presencia de un rostro en la imagen suministrada.
RF6	Rechazo de imágenes sin rostro	El sistema debe rechazar las imágenes en las que no se detecte ningún rostro.
RF7	Rechazo de imágenes con múltiples rostros	El sistema debe rechazar las imágenes en las que se detecten múltiples rostros cuando el proceso requiera una única identidad.
RF8	Generación de representación facial	El sistema debe generar una representación digital del rostro detectado para su posterior comparación.
RF9	Enrolamiento facial	El sistema debe almacenar la representación facial generada y asociarla al usuario registrado.
RF10	Validación facial	El sistema debe permitir enviar una nueva imagen facial para compararla contra el registro previamente almacenado de un usuario.
RF11	Comparación de registros faciales	El sistema debe comparar la representación facial actual con la representación facial almacenada del usuario.
RF12	Decisión de coincidencia	El sistema debe determinar si la imagen validada corresponde o no al usuario registrado, de acuerdo con un umbral definido.
RF13	Registro de resultados	El sistema debe almacenar el resultado de cada validación realizada, incluyendo fecha, usuario y resultado de coincidencia.
RF14	Consulta de historial	El sistema debe permitir consultar el historial de validaciones realizadas por usuario.
RF15	Consulta de perfiles registrados	El sistema debe permitir consultar si un usuario cuenta o no con registro facial enrolado.
RF16	Actualización de registro facial	El sistema debe permitir reemplazar o actualizar el registro facial de un usuario cuando sea necesario.
RF17	Eliminación de registro facial	El sistema debe permitir eliminar el registro facial almacenado de un usuario.
RF18	Respuesta del servicio	El sistema debe devolver una respuesta estructurada indicando si el proceso fue exitoso o fallido, junto con el mensaje correspondiente.
RF19	Manejo de errores	El sistema debe informar de manera clara los errores presentados durante el proceso, como

		imagen inválida, usuario inexistente o fallo de procesamiento.
RF20	Exposición de endpoints	El microservicio debe exponer endpoints para enrolamiento, validación, consulta de perfil, consulta de historial y verificación de estado del servicio.

Nota. Elaboración propia (2026).

Tabla 20. Requisitos No Funcionales.

Tabla de Requisitos No Funcionales		
Código	**Nombre**	**Descripción**
RNF1	Rendimiento	El sistema debe responder a las solicitudes de enrolamiento y validación en un tiempo adecuado para entorno de prueba.
RNF2	Disponibilidad	El microservicio debe permanecer disponible durante las sesiones de prueba definidas para el proyecto.
RNF3	Escalabilidad básica	La arquitectura debe permitir futuras mejoras para integrar una base de datos real y una interfaz web más robusta.
RNF4	Mantenibilidad	El código del sistema debe estar organizado en módulos para facilitar su mantenimiento y evolución.
RNF5	Legibilidad del código	El código fuente debe estar documentado y escrito con nombres claros para favorecer su comprensión.
RNF6	Seguridad de acceso	El sistema debe contar con mecanismos básicos de control de acceso a los endpoints del microservicio.
RNF7	Protección de datos	La información facial y los registros de validación deben almacenarse de forma controlada y protegida.
RNF8	Integridad de datos	El sistema debe conservar la consistencia de los registros almacenados durante los procesos de enrolamiento y validación.
RNF9	Usabilidad	La interacción con el sistema de prueba debe ser clara y comprensible para el usuario u operador.
RNF10	Portabilidad	El sistema debe poder ejecutarse en distintos entornos de desarrollo compatibles con Python.
RNF11	Compatibilidad	El microservicio debe aceptar formatos estándar de imagen usados comúnmente en sistemas web.
RNF12	Trazabilidad	Cada validación debe quedar registrada con información suficiente para auditar el proceso realizado.
RNF13	Confiabilidad	El sistema debe manejar errores de forma controlada sin detener inesperadamente el servicio.
RNF14	Reutilización	La solución debe permitir reutilizar componentes como detección, validación y almacenamiento en futuras versiones.

RNF15	Documentación	El sistema debe contar con documentación técnica y de usuario para facilitar su implementación y uso.

Nota. Elaboración propia (2026).

Diagrama de Fases

Tabla 21. Diagrama de Fases.

Semana	Iteración / Fase XP	Objetivo de la iteración	Actividades principales	Entregable esperado	Inicio estimado	Fin estimado	Duración
1	Exploración y planificación	Comprender el problema y definir el alcance inicial	- Levantamiento de necesidades - definición del problema - objetivo general - objetivos específicos - alcance inicial	Visión general del proyecto y alcance definido	2026-05-11	2026-05-17	1 semana
2	Exploración y planificación	Organizar la propuesta bajo enfoque incremental	- Identificación de actores - historias de usuario iniciales - priorización de funcionalidades - planificación general de iteraciones	Historias de usuario priorizadas y plan inicial de iteraciones	2026-05-18	2026-05-24	1 semana
3	Iteración 1: base técnica	Construir la base mínima	- Configuración del entorno de	Microservicio base ejecutándose	2026-05-25	2026-05-31	1 semana

		del sistema	desarrollo - estructura inicial del proyecto - creación de la API base - pruebas de funcionamiento inicial				
4	Iteración 1: base técnica	Validar el funcionamiento de la estructura inicial	- Creación de rutas básicas - pruebas de respuesta - validación del flujo inicial del servicio	API básica funcional con rutas de prueba	2026-06-01	2026-06-07	1 semana
5	Iteración 2: manejo de datos de entrada	Incorporar recepción de datos e imágenes	- Recepción de parámetros - manejo de formularios - carga de imágenes - validaciones básicas de entrada	Endpoint capaz de recibir imágenes y datos	2026-06-08	2026-06-14	1 semana
6	Iteración 2: manejo de datos de entrada	Organizar persistencia inicial	- Diseño de almacenamiento temporal - lectura y escritura en JSON - pruebas con registros simples	Persistencia básica funcional en archivos JSON	2026-06-15	2026-06-21	1 semana
7	Iteración 3: preparación del compone	Definir la estrategia del componente de	- Definición del problema de visión por computador	Diseño técnico del componente de	2026-06-22	2026-06-28	1 semana

	nte inteligente	reconocimiento	- criterios de detección - criterios de validación - planeación de datos necesarios	reconocimiento			
8	Iteración 3: preparación del componente inteligente	Preparar los datos para entrenamiento y prueba	- Recolección de imágenes - organización del conjunto de datos - depuración inicial - separación de muestras	Conjunto de datos organizado	2026-06-29	2026-07-05	1 semana
9	Iteración 4: entrenamiento y validación	Preparar el conjunto de entrenamiento	- Etiquetado de imágenes - revisión de consistencia - corrección de anotaciones - preprocesamiento	Conjunto de datos etiquetado y listo	2026-07-06	2026-07-12	1 semana
10	Iteración 4: entrenamiento y validación	Obtener una primera versión funcional del componente	- Configuración del entorno de entrenamiento - entrenamiento inicial - pruebas preliminares	Primera versión entrenada	2026-07-13	2026-07-19	1 semana
11	Iteración 4: entrenami	Evaluar el desempeño y ajustar	- Validación - análisis de métricas - revisión de	Resultados de evaluación	2026-07-20	2026-07-26	1 semana

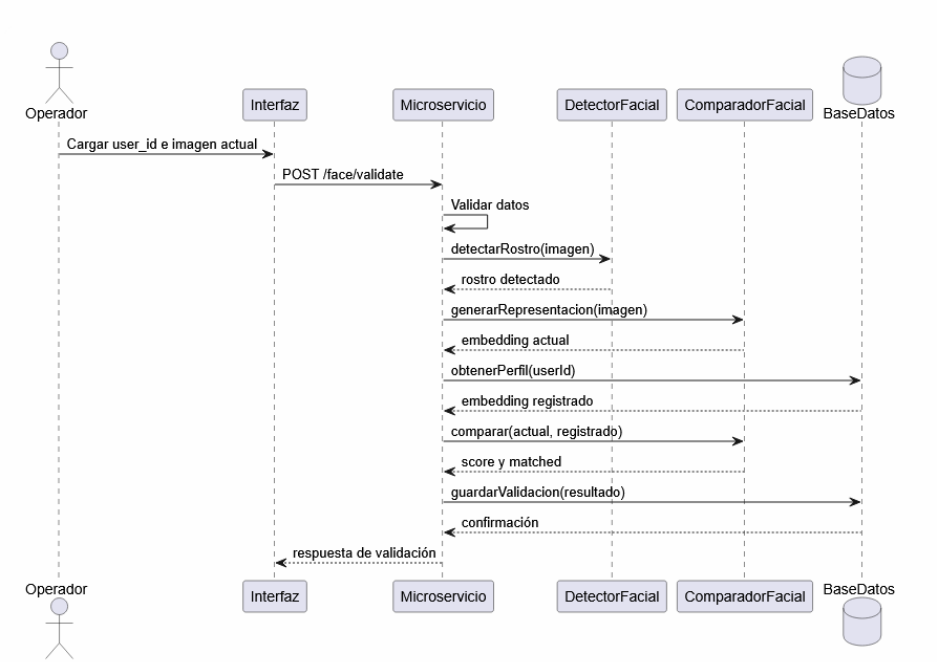
	ento y validación		errores - ajuste de parámetros y umbrales	y ajustes definidos			
12	Iteración 5: enrolamiento	Construir la funcionalidad de registro	- Desarrollo del flujo de enrolamiento - almacenamiento del registro facial - validaciones del proceso	Endpoint de enrolamiento funcional	2026-07-27	2026-08-02	1 semana
13	Iteración 6: validación	Construir la funcionalidad de comparación	- Desarrollo del flujo de validación - comparación contra registro previo - almacenamiento de resultados	Endpoint de validación funcional	2026-08-03	2026-08-09	1 semana
14	Iteración 7: pruebas e integración	Integrar componentes y revisar funcionamiento general	- Integración del componente inteligente con el microservicio - pruebas funcionales - pruebas de error - correcciones	Flujo completo probado	2026-08-10	2026-08-16	1 semana
15	Iteración 8: cierre	Consolidar el resultado	- Documentación técnica -	Documentación final del desarrollo	2026-08-17	2026-08-23	1 semana

		del proyecto	organización de resultados - conclusiones - trabajo futuro - preparación de presentación final				

Nota. Elaboración propia (2026).

8.12 Diseño del sistema

Figura 10. Diagrama de Secuencias.



Nota. Elaboración propia (2026).

El diagrama de secuencia representa el proceso de validación facial dentro del sistema propuesto. En primer lugar, el operador carga en la interfaz el identificador del usuario y la imagen actual que será analizada. Posteriormente, la interfaz envía la

solicitud al microservicio mediante el endpoint de validación. Una vez recibida la petición, el microservicio realiza una validación inicial de los datos y envía la imagen al módulo detector facial para verificar la presencia de un rostro. Si el rostro es detectado correctamente, la imagen es procesada por el módulo comparador facial, el cual genera la representación biométrica o embedding actual. Luego, el microservicio consulta en la base de datos el perfil facial previamente registrado del usuario y recupera el embedding almacenado. Con ambas representaciones disponibles, el comparador facial ejecuta la comparación entre el registro actual y el registro almacenado, obteniendo como resultado un puntaje de similitud y una decisión de coincidencia o no coincidencia. Finalmente, el microservicio guarda el resultado de la validación en la base de datos y devuelve a la interfaz la respuesta final, permitiendo informar al operador si la identidad fue validada exitosamente.

Figura 11. Modelo Entidad Relación.



Nota. Elaboración propia (2026).

9 RESULTADOS

9.1 Introducción

El desarrollo del presente proyecto permitió obtener un prototipo funcional de sistema de identificación y control de acceso para la Universidad Internacional del Trópico Americano. Los resultados obtenidos comprenden el diseño e implementación de un aplicativo web que integra reconocimiento facial mediante inteligencia artificial, complementado con el escaneo del código QR del carnet institucional como mecanismo de verificación alternativo. El sistema quedó estructurado bajo una arquitectura Modelo Vista Controlador (MVC), desarrollado con la metodología ágil de Programación Extrema (XP) y validado mediante pruebas funcionales y evaluación automatizada del módulo de reconocimiento facial.

9.2 Descripción del prototipo

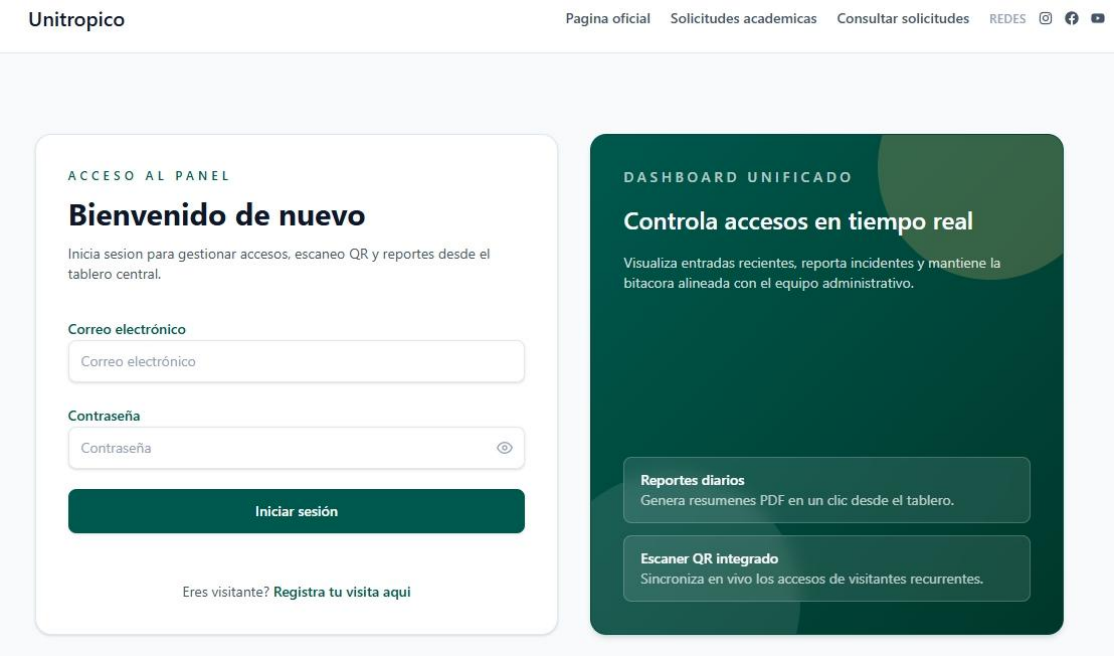
Se exponen los resultados de las pruebas realizadas sobre el frontend y el backend, la validación del funcionamiento del sistema frente a los requerimientos definidos y se ilustra el comportamiento del prototipo mediante la ejecución de los principales flujos de trabajo: inicio de sesión, registro de accesos mediante reconocimiento facial, verificación complementaria por código QR y generación de reportes. De igual manera, se señalan brevemente las limitaciones técnicas observadas en el contexto del prototipo académico.

El principal resultado del proyecto es el diseño y desarrollo de un prototipo funcional de un sistema de control de acceso de personas, orientado a apoyar el proceso de ingreso y salida en Unitrópico, en coherencia con la normativa institucional sobre

carné estudiantil establecida en la Resolución No. 014 de 2021, la Resolución No. 025 de 2021 y la Circular Administrativa No. 024 de 2026.

Figura 12. Login

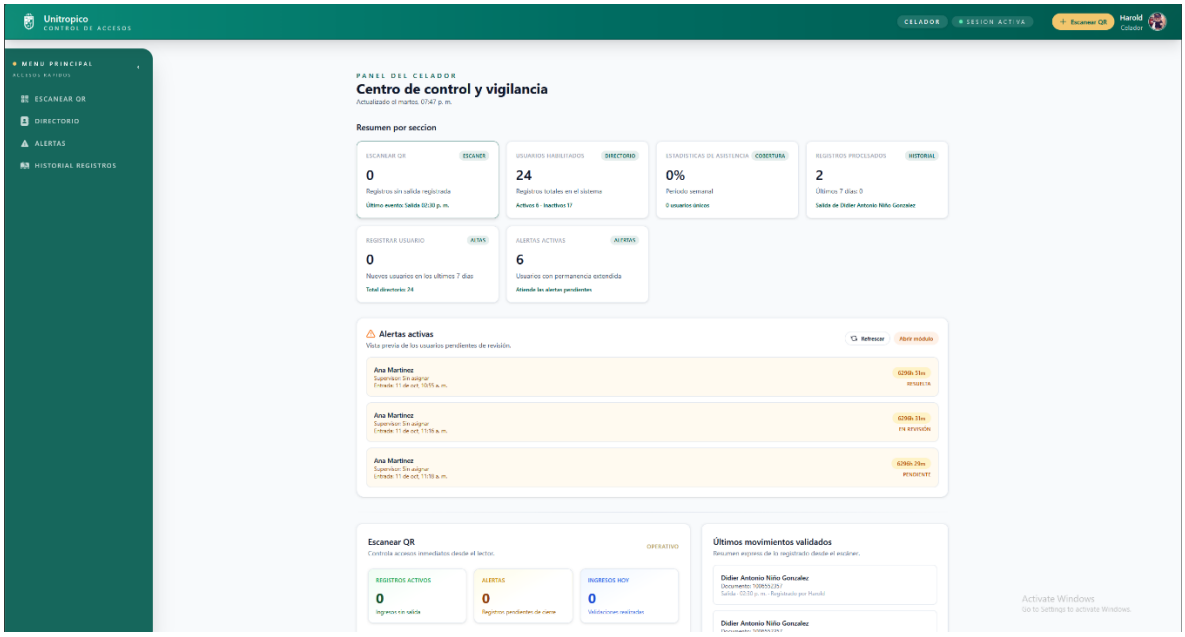
La pantalla de inicio de sesión permite el acceso al sistema mediante correo electrónico y contraseña. El sistema valida las credenciales ingresadas y redirige al usuario a su panel correspondiente según el rol asignado.



Nota. Imagen tomada por los autores (2026).

Figura 13. Panel del celador

Vista general del panel del vigilante, desde el cual se accede a los módulos de escaneo QR, reconocimiento facial, registro de visitantes y consulta de personas dentro del campus.



Nota. Imagen tomada por los autores (2026).

Figura 14. Escaneo del Reconocimiento Facial

Pantalla de captura facial en tiempo real mediante cámara web. El sistema procesa la imagen capturada, extrae el embedding facial y lo compara contra los registros biométricos almacenados para verificar la identidad del usuario.

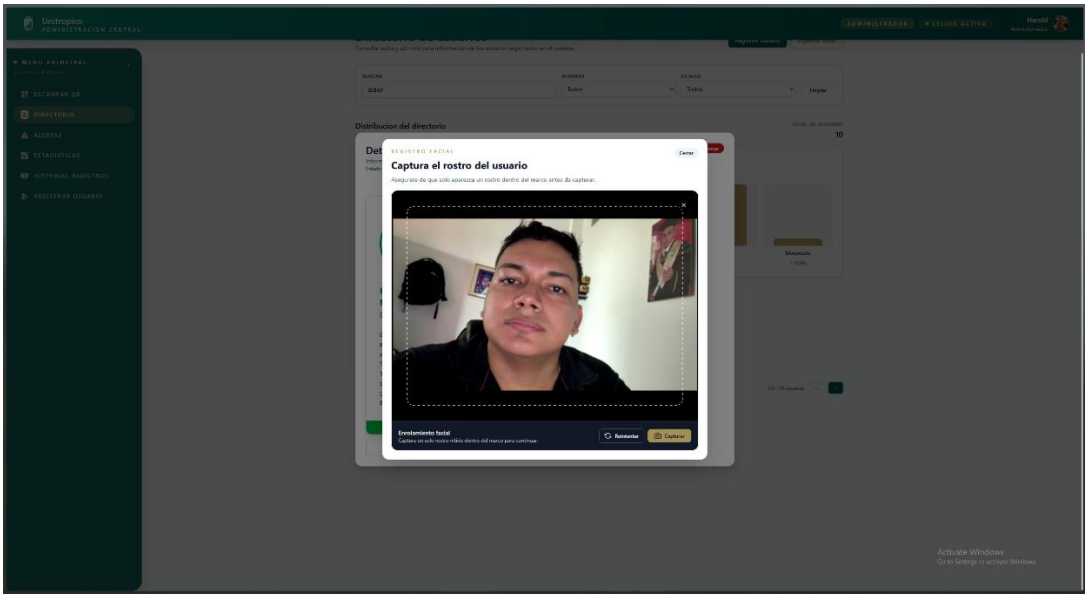


Figura 15. Confirmación del Escaneo del Reconocimiento Facial

Pantalla de resultado del proceso de reconocimiento facial, donde el sistema muestra la identidad verificada del usuario junto con su información básica y el resultado del acceso concedido o denegado.

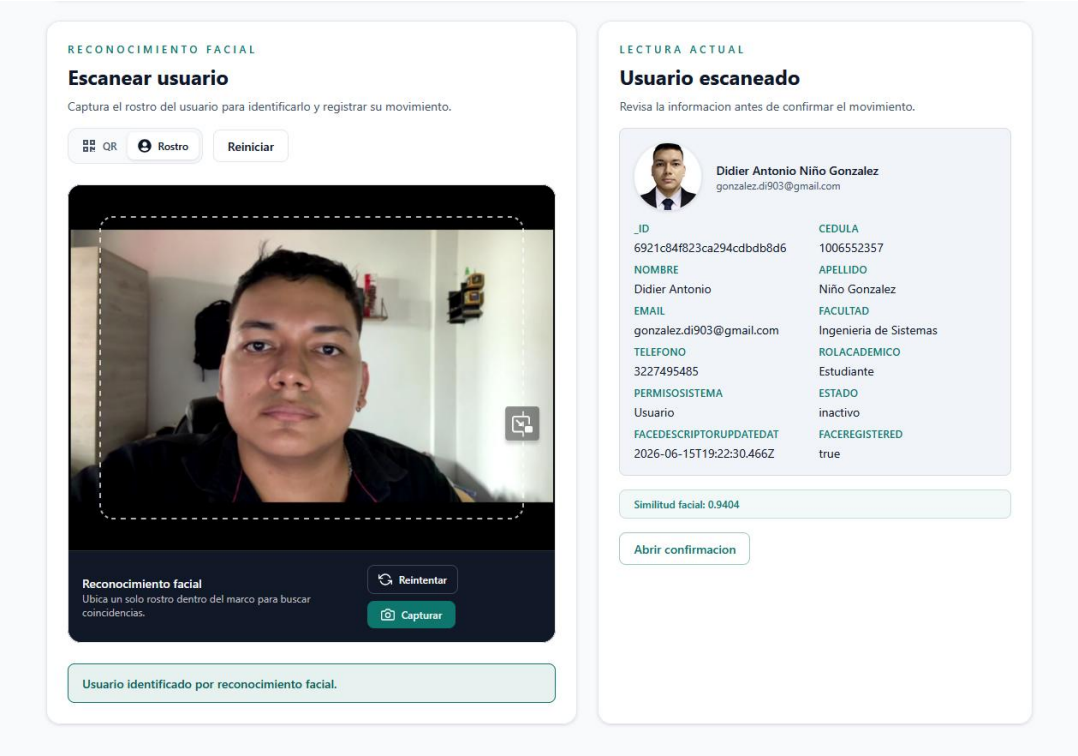


Figura 16. Manejo de error en el reconocimiento facial

Pantalla de error del módulo de reconocimiento facial cuando se detectan múltiples rostros en la imagen. El sistema muestra el mensaje "Se detectaron múltiples rostros. Debe haber exactamente un rostro" e impide continuar hasta que se cumpla el requisito de un único rostro detectable.

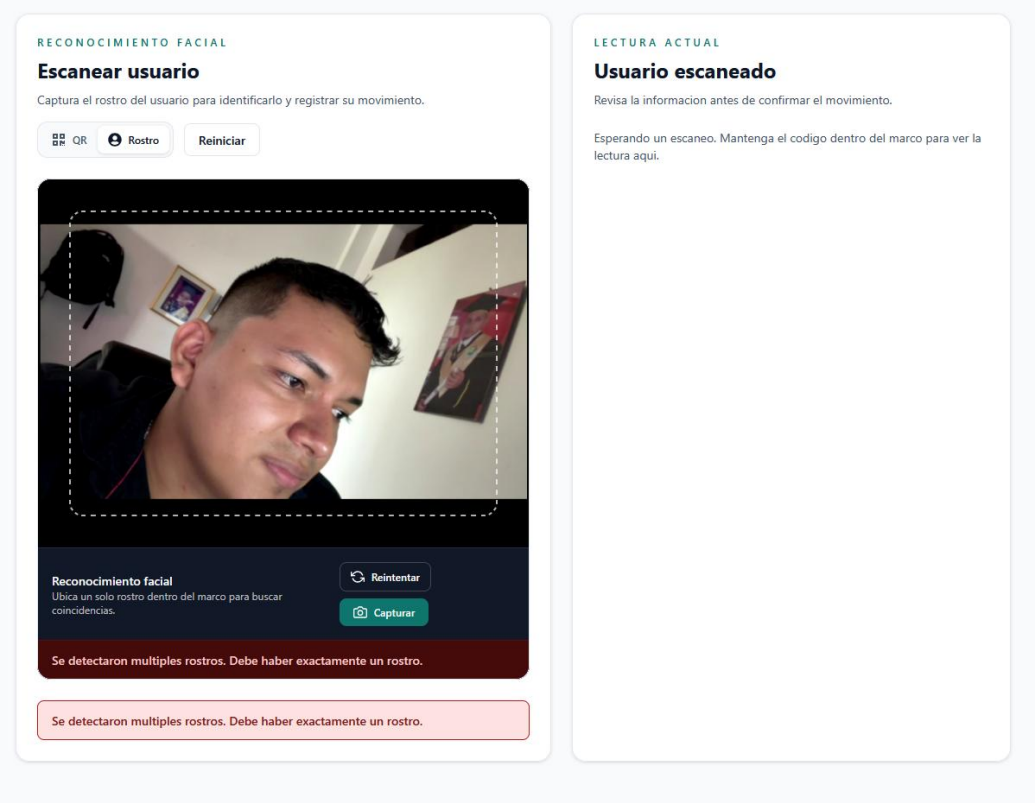


Figura 17. Confirmación exitosa del reconocimiento facial con gafas

Pantalla de confirmación del reconocimiento facial exitoso de un usuario portando gafas, evidenciando la capacidad del sistema para identificar correctamente a usuarios bajo esta condición. El sistema muestra los datos completos del usuario identificado y el mensaje "Usuario identificado por reconocimiento facial" con la similitud facial obtenida.

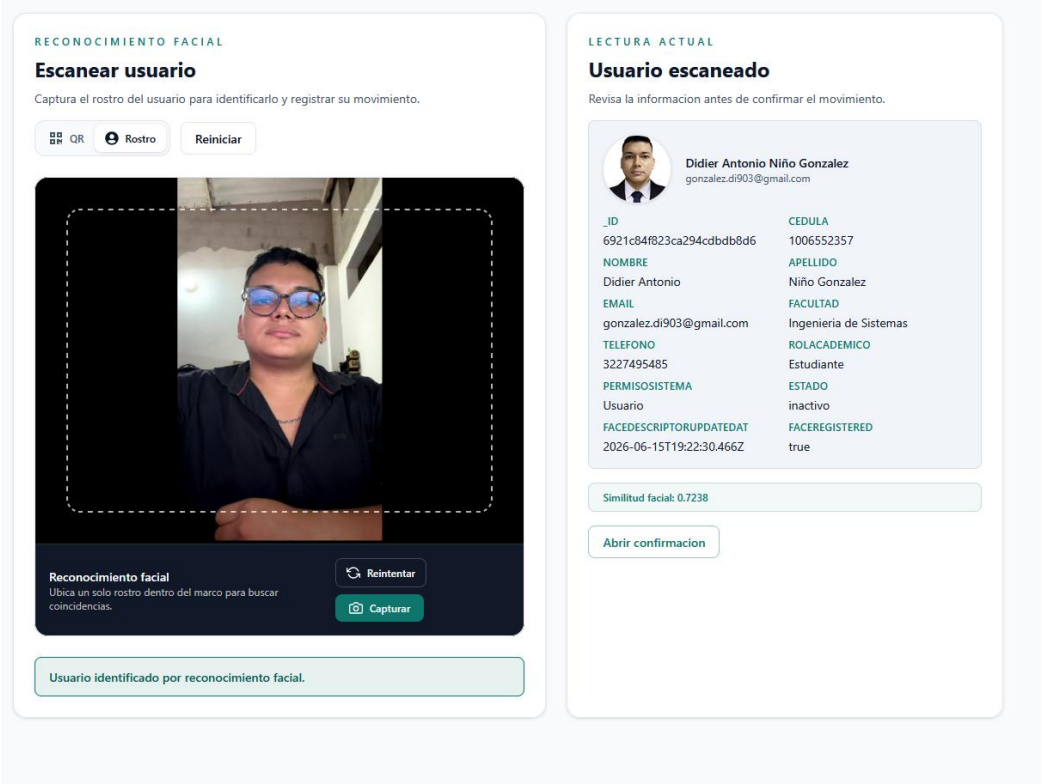


Figura 18. Reconocimiento facial exitoso con gafas oscuras

El sistema identificó correctamente al usuario portando gafas de sol oscuras, obteniendo una similitud facial de 0.5374, valor que aunque más bajo que en condiciones sin accesorios, superó el threshold de 0.50, demostrando la robustez del modelo ante oclusión parcial del rostro.

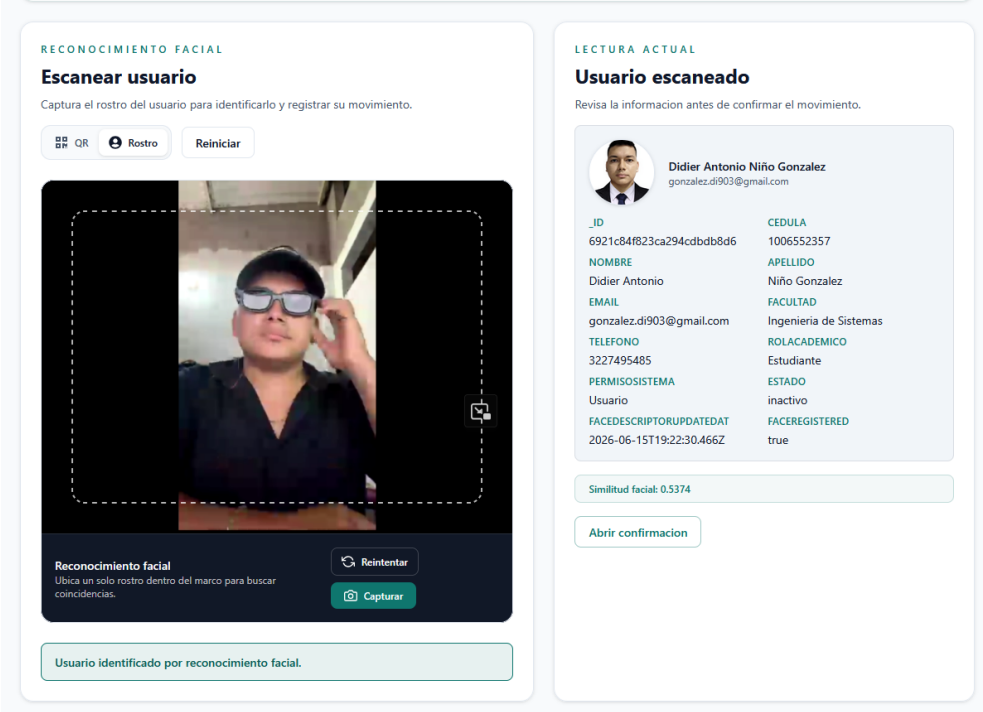


Figura 19. Reconocimiento facial exitoso con gorra

El sistema identificó correctamente al usuario portando gorra, obteniendo una similitud facial de 0.6583, valor que supera el threshold configurado de 0.50. Este resultado evidencia que la oclusión de la parte superior del rostro no afectó significativamente la capacidad de reconocimiento del sistema.

Figura 20. Clasificación de permisos usuario.

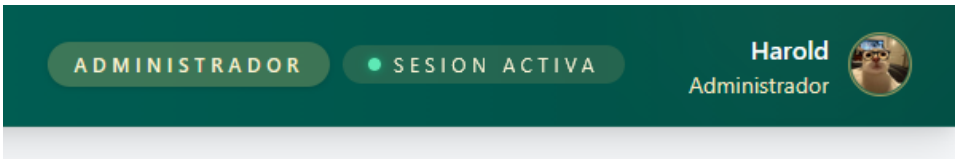
Vista del sistema correspondiente al perfil de usuario general, donde se muestran las funcionalidades disponibles según los permisos asignados a este rol.



Nota. Imagen tomada por los autores (2026).

Figura 21. Clasificación de permisos administrador.

Vista del sistema correspondiente al perfil administrador, que incluye acceso completo a la gestión de usuarios, reportes, estadísticas y configuración del sistema.



Nota. Imagen tomada por los autores (2026).

Figura 22. Clasificación de permisos celador.

Vista del sistema correspondiente al perfil vigilante, con acceso a los módulos de control de ingreso y salida, escaneo QR y reconocimiento facial.



Nota. Imagen tomada por los autores (2026).

Figura 23. Consulta de usuario de Administrador.

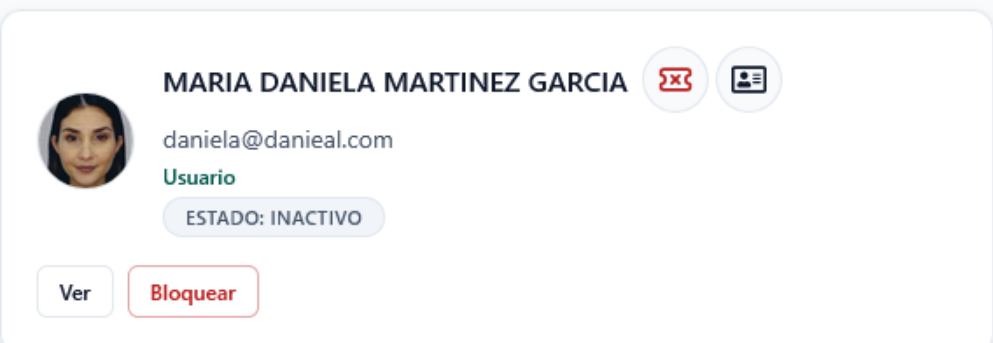
Módulo de administración de usuarios desde el perfil administrador, que permite consultar, crear, actualizar y desactivar cuentas de usuarios registrados en el sistema.



Nota. Imagen tomada por los autores (2026).

Figura 24. Consulta de usuario de Celador.

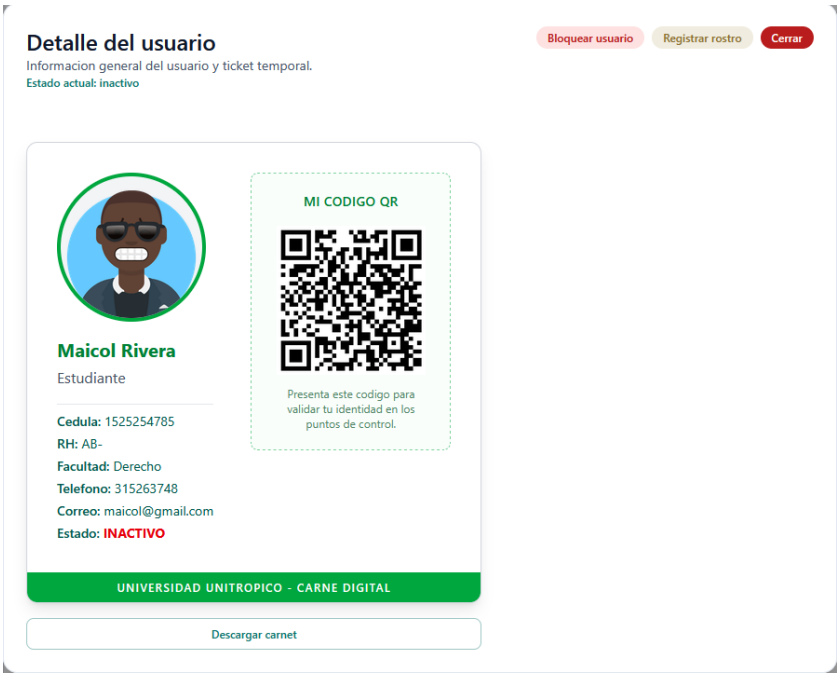
Vista del directorio de usuarios disponible para el perfil vigilante, con acceso limitado a la información necesaria para el proceso de verificación de identidad en el punto de acceso.



Nota. Imagen tomada por los autores (2026).

Figura 25. Visualización de tarjeta usuario.

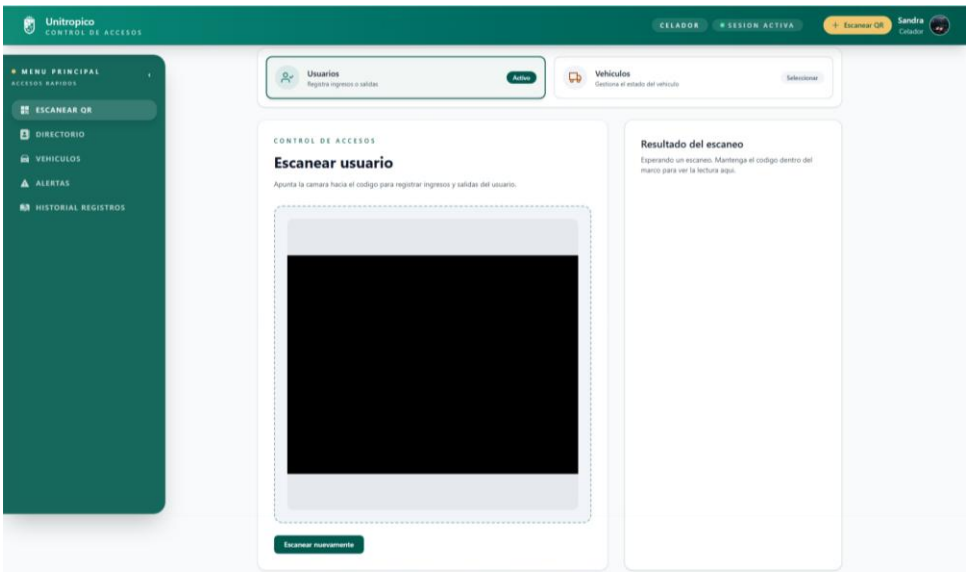
Visualización de la tarjeta de identificación digital del usuario dentro del sistema, que muestra los datos personales, rol, estado y código QR asociado al perfil.



Nota. Imagen tomada por los autores (2026).

Figura 26. Módulo de escaneo QR

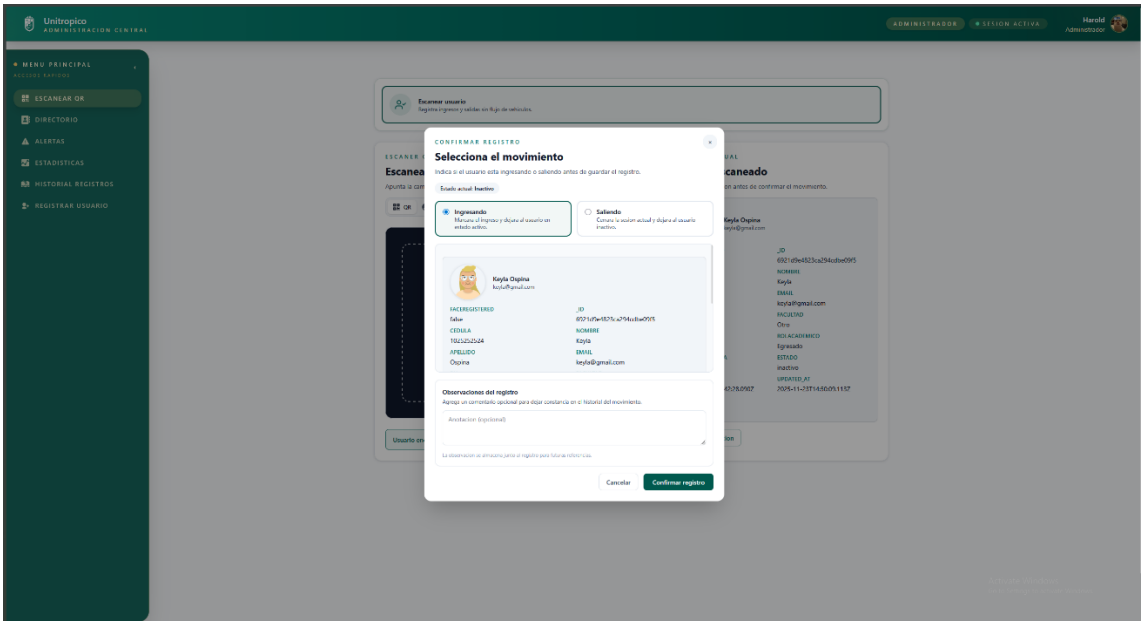
Pantalla de escaneo del código QR del carnet institucional, que se activa como mecanismo complementario de verificación cuando el reconocimiento facial no logra identificar al usuario.



Nota. Imagen tomada por los autores (2026).

Figura 27. Módulo de Confirmación

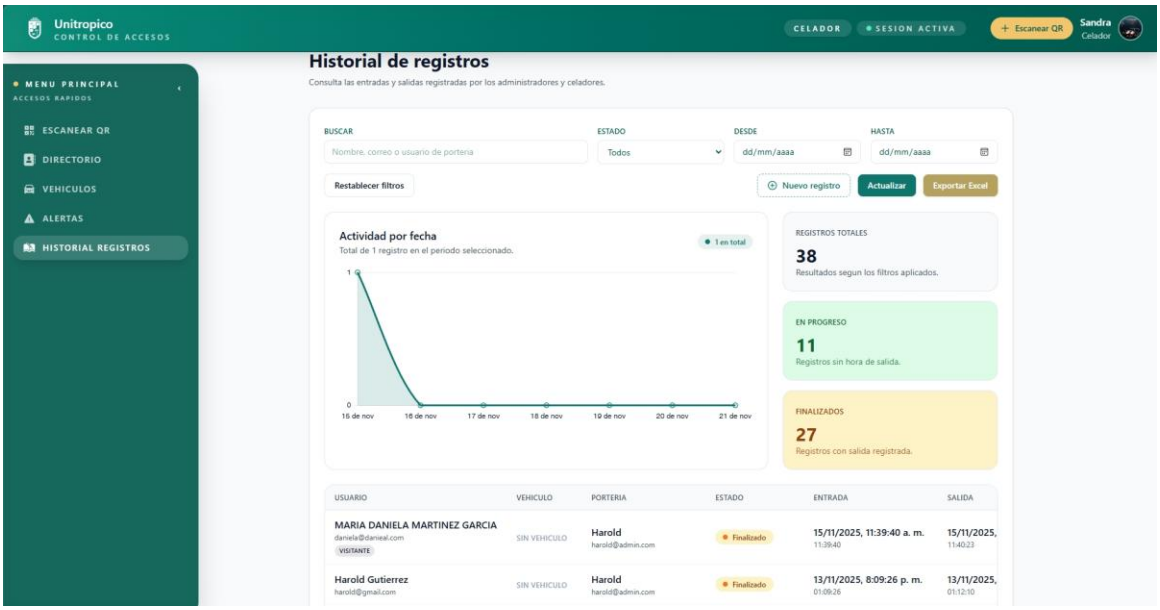
Pantalla de resultado tras el escaneo del código QR, donde el sistema muestra la información del usuario identificado y registra el ingreso o salida según corresponda.



Nota. Imagen tomada por los autores (2026).

Figura 28. Historial de registros de usuarios.

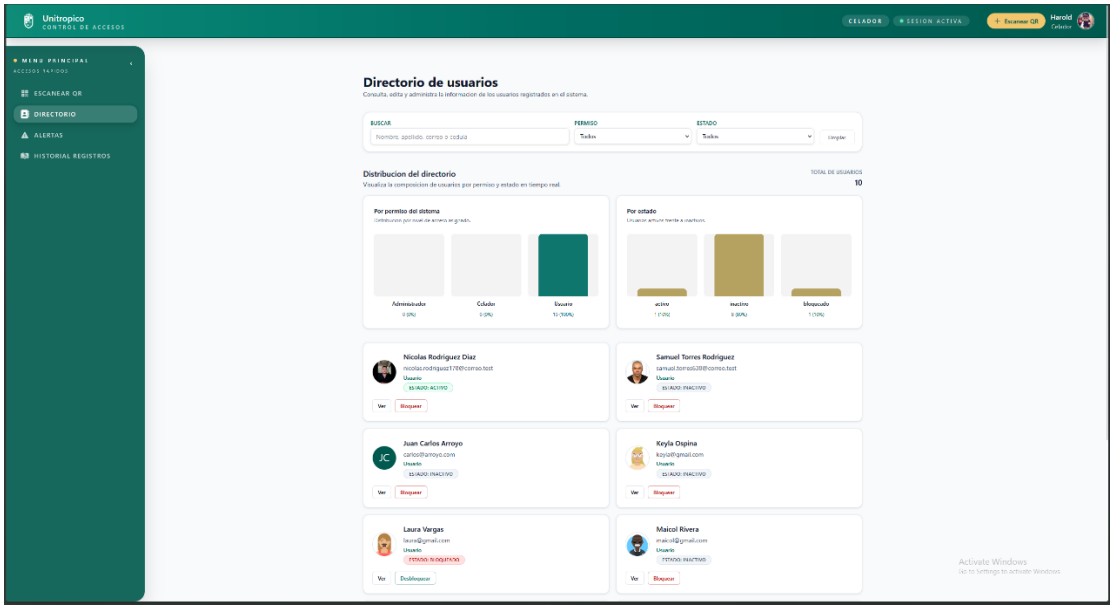
Módulo de consulta del historial de ingresos y salidas registrados en el sistema, con información de fecha, hora, usuario y método de verificación utilizado.



Nota. Imagen tomada por los autores (2026).

Figura 29. Directorio de usuarios

Vista general del directorio de usuarios registrados en el sistema, con opciones de búsqueda, filtrado por rol y acceso a la gestión individual de cada perfil.



Nota. Imagen tomada por los autores (2026).

9.3 Fase 1: Resultados de la evaluación con dataset LFW

La ejecución del evaluation harness sobre el dataset LFW arrojó resultados que permitieron caracterizar el comportamiento del sistema de reconocimiento facial en función del umbral de similitud de coseno aplicado. A continuación, se presentan los resultados obtenidos para los 13 thresholds evaluados.

9.3.1 Resumen de métricas por threshold – Fase 1

Threshold	*TP*	*FP*	*TN*	*FN*	*Precisión*	*Recall*	*F1*	*Errores*
0.30	588	0	5	0	100%	100%	100%	135
0.35	588	0	5	0	100%	100%	100%	135
0.40	587	0	5	1	100%	99.83%	99.91%	135
0.45	585	0	5	3	100%	99.49%	99.74%	135
0.50	582	0	5	6	100%	98.98%	99.49%	135
0.55	573	0	5	15	100%	97.45%	98.71%	135
0.60	543	0	5	45	100%	92.35%	96.02%	135
0.65	479	0	5	109	100%	81.46%	89.78%	135
0.70	334	0	5	254	100%	56.8%	72.45%	135
0.75	160	0	5	428	100%	27.21%	42.78%	135

0.80	36	0	5	552	100%	6.12%	11.54%	135
0.85	2	0	5	586	100%	0.34%	0.68%	135
0.90	0	0	5	588	0%	0%	0%	135

Nota. Elaboración propia (2026).

9.4 Análisis e interpretación de resultados – Fase 1

Los resultados obtenidos evidenciaron que el sistema de reconocimiento facial alcanzó su rendimiento óptimo con un umbral de similitud de coseno de 0.30, obteniendo valores de Precisión, Recall y F1-score del 100% sobre las 588 imágenes procesadas exitosamente. Este resultado indicó que, bajo dicho umbral, el sistema identificó correctamente la totalidad de los usuarios legítimos sin generar ningún falso positivo.

A medida que el umbral se incrementó progresivamente, se observó una degradación sistemática del Recall, mientras que la Precisión se mantuvo en el 100% hasta valores de umbral de 0.85. Este comportamiento es consistente con la naturaleza del umbral de similitud de coseno: valores más altos exigen una mayor similitud entre embeddings, lo que reduce la cantidad de coincidencias aceptadas e incrementa los falsos negativos. Con un umbral de 0.90, el sistema rechazó la totalidad de las imágenes, resultando en métricas nulas.

En cuanto al rendimiento por identidad, la evaluación con el threshold recomendado de 0.30 demostró que las 13 identidades evaluadas obtuvieron individualmente valores de Precisión, Recall y F1-score del 100%, sin registrarse confusiones entre identidades distintas.

Respecto a los errores de extracción, se registraron 135 imágenes no procesadas, distribuidas en tres categorías: 125 correspondientes a detección de múltiples rostros en una misma imagen, 7 por imagen de tamaño insuficiente y 3 por ausencia de rostro

detectable. Estos errores no constituyeron fallos del sistema de reconocimiento sino limitaciones propias de las imágenes del dataset.

9.4.1 Threshold recomendado Fase 1: 0.30

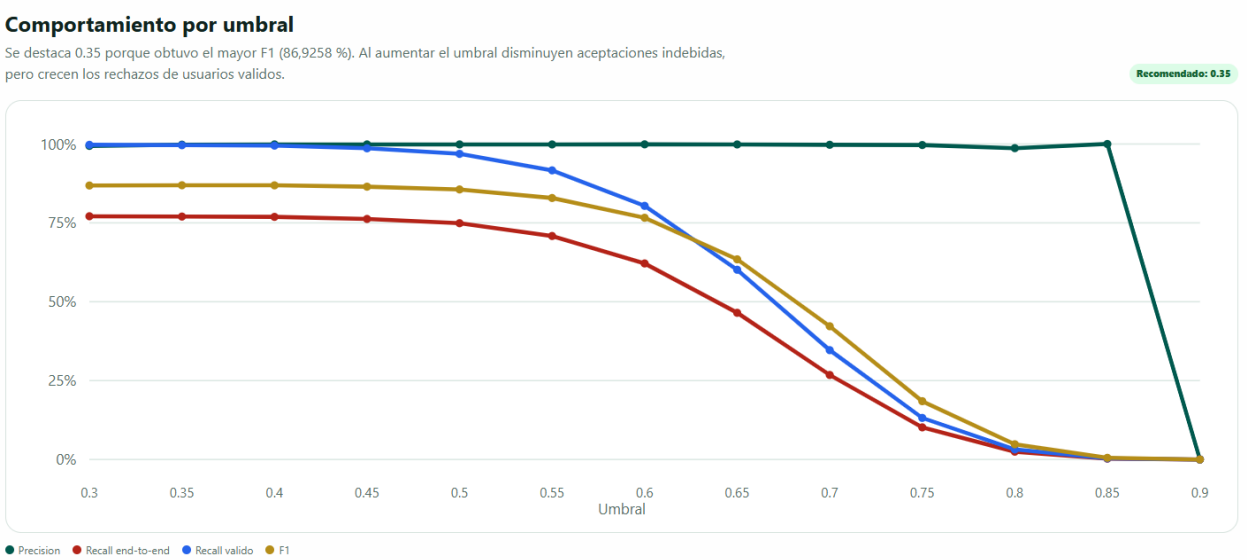
Con base en los resultados obtenidos, el umbral de similitud de coseno de 0.30 fue seleccionado como el valor óptimo para la operación del sistema. Esta selección se fundamentó en que dicho valor maximizó simultáneamente la Precisión y el Recall, alcanzando un F1-score del 100%.

La distribución de scores de los aciertos registró una media de 0.7065 con un rango comprendido entre 0.3531 y 0.8678, confirmando que la mayoría de las coincidencias correctas se ubicaron significativamente por encima del umbral seleccionado, lo que aportó un margen de seguridad adecuado frente a variaciones en las condiciones de captura de imagen.

9.5 Fase 2: Resultados de la evaluación con galería ampliada de 100 perfiles

La segunda fase de evaluación se ejecutó sobre una galería de 100 perfiles enrolados directamente en el sistema a través del módulo de registro de la aplicación web, realizando un total de 12.603 pruebas y 1.018.700 comparaciones de similitud de coseno. A diferencia de la primera fase en la que se utilizó el dataset público LFW con 13 identidades organizadas en directorios locales, en esta fase cada perfil fue registrado mediante la interfaz del sistema, generando automáticamente un embedding de 512 dimensiones almacenado en MongoDB.

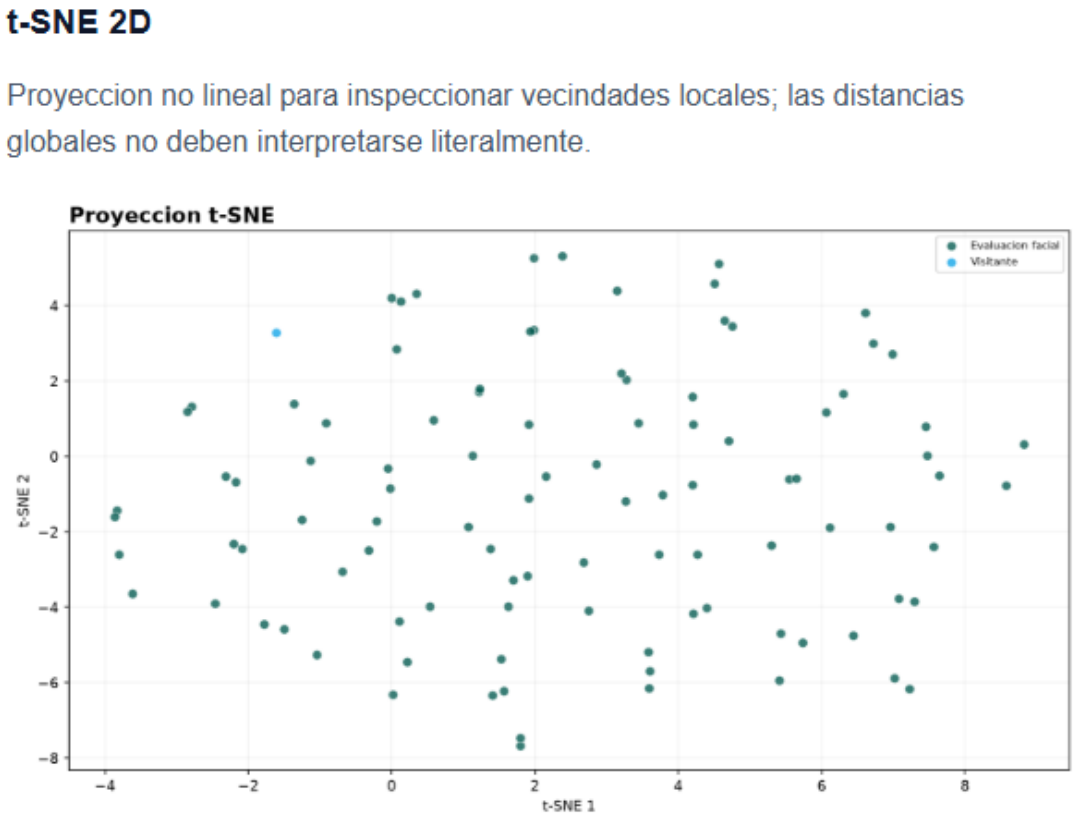
Figura 30. Comportamiento del sistema de reconocimiento facial por umbral



Nota. Elaboración propia (2026).

La gráfica muestra el comportamiento de las métricas Precisión, Recall end-to-end, Recall válido y F1-score en función del umbral de similitud de coseno evaluado. Se destaca el threshold 0.35 como el recomendado por obtener el mayor F1-score de 86.9258%. La Precisión (línea verde) se mantiene cercana al 100% hasta el umbral 0.85, mientras que el Recall end-to-end (línea roja) decrece progresivamente desde 0.30. El Recall válido (línea azul) y el F1-score (línea amarilla) presentan un comportamiento estable hasta el umbral 0.55, a partir del cual comienzan a degradarse significativamente. A partir del umbral 0.60 se evidencia una caída pronunciada en todas las métricas, confirmando que valores superiores a 0.50 resultan excesivamente restrictivos para una galería de 100 identidades.

Figura 31. Proyección bidimensional de los embeddings faciales



La (**Figura *31***) presenta una visualización bidimensional de los embeddings faciales generados por el modelo de reconocimiento mediante el algoritmo t-SNE. Cada punto representa un vector de características extraído de un rostro procesado por el sistema. El algoritmo proyecta los embeddings desde un espacio de alta dimensionalidad hacia dos dimensiones con el fin de facilitar su interpretación visual, preservando principalmente las relaciones de vecindad entre los datos. En la gráfica, los puntos verdes corresponden a los rostros registrados durante la fase de evaluación, mientras que el punto azul representa el visitante sometido al proceso de autenticación. Se observa que el visitante se encuentra separado del conjunto principal de embeddings, lo que indica que sus características faciales presentan baja similitud con las identidades

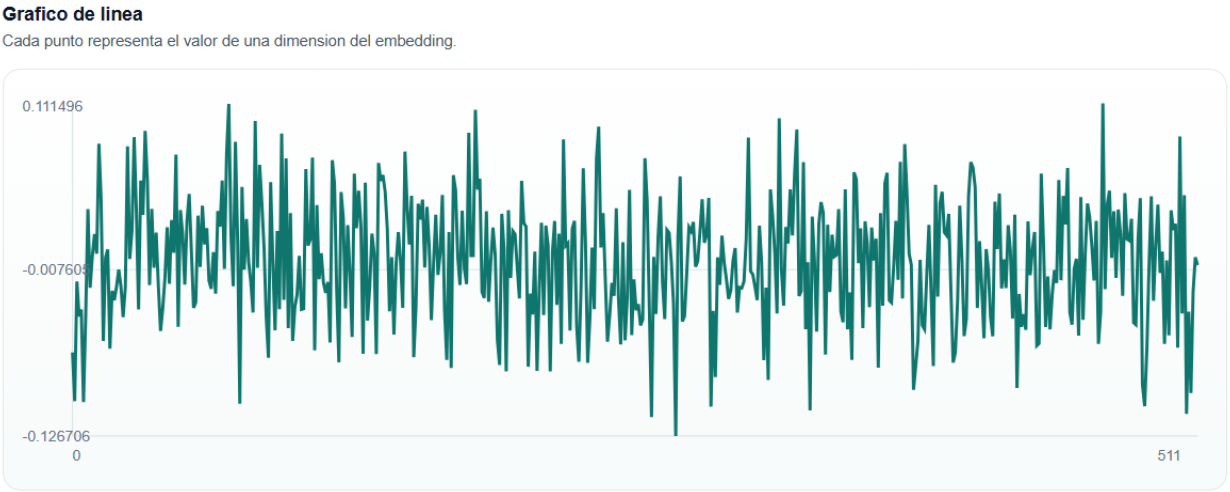
registradas. Esta representación permite verificar visualmente la capacidad del modelo para generar descriptores discriminativos y distinguir entre diferentes individuos.

9.5.1.1 Usuario 1

Dimensiones	Mínimo	Máximo	Promedio	Desv. estándar
512	512	512	512	512

- ✓ Embedding Facial
- ✓ Identificador: Usuario 1
- ✓ Origen: Base de datos de evaluación
- ✓ Vector: 512 dimensiones

Figura 32. Visualización del embedding facial del Usuario 1.



En la (**Figura *32***) Visualización del embedding facial correspondiente al Usuario 1. Se presenta el vector de características generado por el modelo de reconocimiento facial para un usuario anonimizado. Cada punto del gráfico de líneas representa el valor de una de las 512 dimensiones del embedding extraído por la red neuronal.

Estadístico	Estadístico
Estadístico	Valor
Media	0,8684
Mediana	0,8732

Mínimo	0,6575
Máximo	0,9790

La media del score facial fue de 0,8684, valor considerablemente superior al umbral definido para la autenticación (0,50), indicando un desempeño consistente del modelo durante las pruebas realizadas.

Tabla 22. Resumen de métricas por threshold Fase 2

Umbral	Correctas	Incorrectas	Conocidos rechazados	Impostores rechazados	Precisión	Recall total	Recall válido	F1
0.30	2.540	2	4	7.829	95.405%	77.100%	99.744%	86.843%
0.35	2.537	2	7	7.838	99.865%	77.001%	99.164%	86.925%
0.40	2.534	2	10	7.840	99.871%	76.932%	99.488%	86.899%
0.45	2.514	2	30	7.840	99.835%	76.324%	98.636%	86.471%
0.50	2.275	2	71	7.840	99.862%	74.692%	96.883%	85.593%
0.55	2.150	2	194	7.840	99.607%	73.842%	91.454%	82.888%

0.60	1.886	1	459	7.843	99.841 %	62.14 1%	80.59 2%	76.42 0%
0.65	1.411	1	934	7.843	99.685 %	46.49 3%	62.14 4%	35.81 2%
0.70	813	1	1.532	7.843	99.754 %	26.78 7%	34.65 4%	42.23 3%
0.75	309	0	2.037	7.840	99.677 %	10.18 1%	13.17 1%	18.47 5%
0.80	75	0	2.271	7.840	98.684 %	2.471 %	3.196 %	4.821 %
0.85	8	0	2.338	7.841	100%	0.263 %	0.341 %	0.525 %
0.90	0	0	2.346	7.841	0%	0%	0%	0%

Nota. Elaboración propia (2026).

9.5.2 Threshold recomendado Fase 2: 0.35

Con base en los resultados obtenidos, el umbral de similitud de coseno de 0.35 fue seleccionado como el valor óptimo para la segunda fase. Este valor alcanzó una Precisión de 99.865% y un Recall válido de 99.164%, con un F1-score de 86.925%.

El threshold de 0.35 supera al valor de 0.30 utilizado en la primera fase porque al aumentar el tamaño de la galería de 13 a 100 identidades, un umbral más bajo generaba mayor riesgo de confusiones entre identidades con características faciales similares. Con threshold 0.30 la precisión bajó a 95.405% por 2 incorrectas adicionales, mientras que

con 0.35 se mantuvo en 99.865% sin sacrificar significativamente el Recall. Esto demuestra que, a mayor tamaño de galería, el sistema requiere un umbral ligeramente más exigente para mantener la precisión.

9.5.2.1 Tiempos de respuesta

El harness registró los tiempos de cada etapa del proceso mediante performance.now() para cada imagen de prueba, calculando posteriormente los estadísticos descriptivos mediante la función summarizeValues(), que ordena los valores, descarta nulos e inválidos, y calcula media, mediana, mínimo, máximo y percentiles con interpolación lineal mediante la fórmula: posición = (n - 1) × percentil, interpolando entre dos mediciones cuando la posición cae entre valores.

9.5.2.2 ReadMs

Mide el tiempo de leer la imagen desde el disco con fsp.readFile(). Se registraron 12.603 mediciones.

- ✓ Media: 0.5641 ms en promedio leer una imagen tarda menos de 1 ms
- ✓ Mediana: 0.2746 ms valor más representativo del comportamiento normal
- ✓ Máximo: 180.37 ms valor atípico explicado por caché del sistema operativo o latencia de disco
- ✓ P95: 0.7752 ms el 95% de las lecturas completaron en menos de 0.78 ms
- ✓ % del total: (0.5641 / 204.163) × 100 = 0.28%

9.5.2.3 ExtractionMs

Mide el tiempo completo de la solicitud POST /api/face/extract al microservicio facial, incluyendo transporte de red y procesamiento del modelo Buffalo_L para generar el embedding de 512 dimensiones. Se registraron 12.603 mediciones.

- ✓ Media: 190.40 ms es la etapa más lenta del proceso
- ✓ Mediana: 177.60 ms el 50% de las extracciones tardaron menos de 178 ms
- ✓ Máximo: 901.26 ms casos atípicos de alta latencia de red o imágenes complejas
- ✓ P95: 275.82 ms el 95% de las extracciones completaron en menos de 276 ms
- ✓ % del total: (190.40 / 204.163) × 100 = 93.26%

9.5.2.4 ComparisonMs

Mide el cálculo de similitud de coseno entre el embedding extraído y los 100 perfiles enrolados, incluyendo el ordenamiento de resultados. Solo se registraron 10.187 mediciones porque 2.416 fotos no llegaron a esta etapa por errores de extracción.

- ✓ Media: 2.15 ms comparar contra 100 perfiles tarda apenas 2 ms
- ✓ Mediana: 2.23 ms muy cercana a la media, indica tiempos muy consistentes
- ✓ Máximo: 10.91 ms incluso en el peor caso es muy rápido
- ✓ P95: 2.85 ms el 95% de las comparaciones completaron en menos de 3 ms
- ✓ % del total: (2.15 / 204.163) × 100 = 1.05%

9.5.2.5 PersistenceMs

Mide las escrituras en MongoDB: cambio de estado del probe, guardado de candidatos por chunks y guardado del resultado final. Tiene 10.187 mediciones por la misma razón que la comparación.

- ✓ Media: 13.94 ms guardar en MongoDB tarda menos de 14 ms en promedio
- ✓ Mediana: 14.16 ms muy consistente con la media
- ✓ Mínimo: 10.30 ms incluso en el mejor caso tarda ~10 ms por las escrituras múltiples
- ✓ Máximo: 46.58 ms casos de mayor latencia en MongoDB

- ✓ P95: 16.52 ms el 95% de las persistencias completaron en menos de 17 ms
- ✓ % del total: (13.94 / 204.163) × 100 = 6.82%

9.5.2.6 TotalMs

Mide desde antes de leer la imagen hasta completar o fallar el probe.

- ✓ Media: 204.16 ms el sistema procesa cada reconocimiento en ~0.2 segundos
- ✓ Mediana: 194.69 ms más de la mitad de los probes completan en menos de 195 ms
- ✓ Mínimo: 1.67 ms probes que fallaron muy rápido por error de lectura inmediato
- ✓ Máximo: 902.92 ms menos de 1 segundo incluso en el peor caso
- ✓ P95: 279.78 ms el 95% de los probes completaron en menos de 280 ms

9.5.2.7 Errores de extracción

De las 12.603 imágenes procesadas, 2.416 no lograron completar el proceso de extracción, representando el 19.17% del total. Los errores se distribuyeron así:

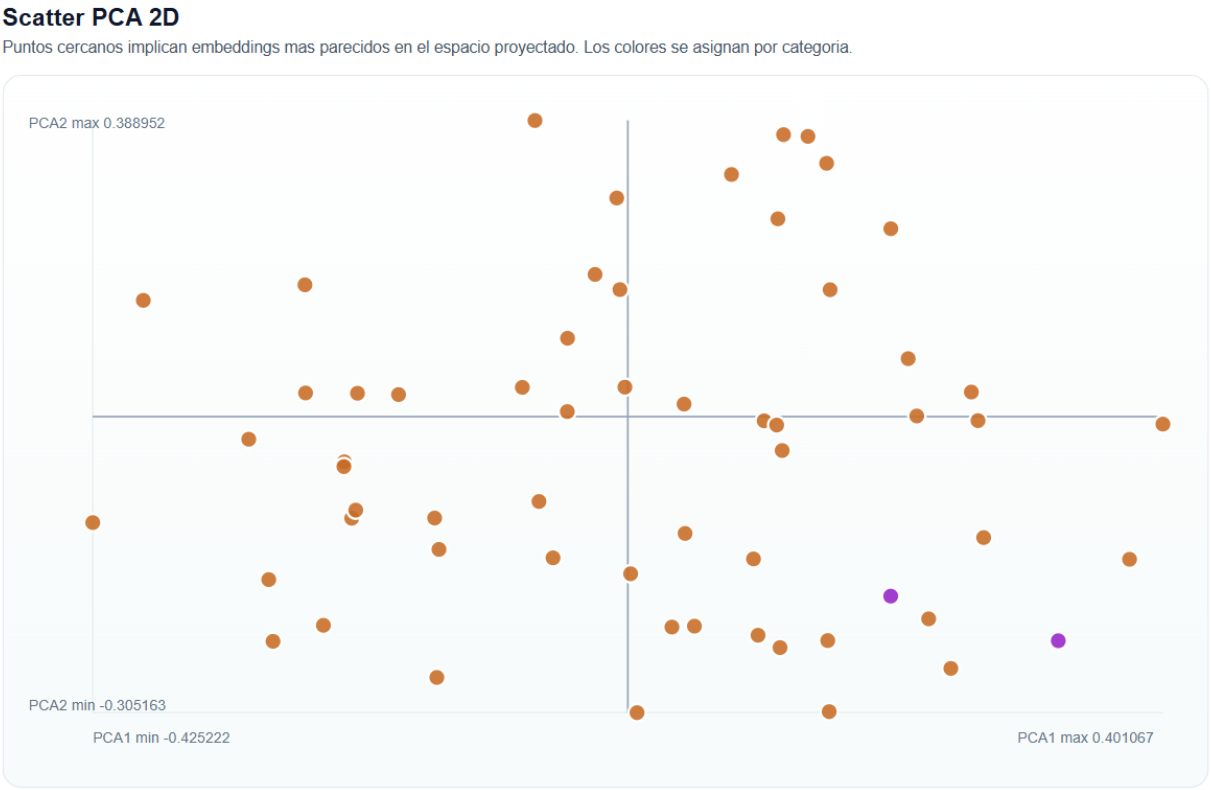
- ✓ 2.181 imágenes (17.30%) múltiples rostros detectados en la misma imagen: (2.181 / 12.603) × 100 = 17.30%
- ✓ 198 imágenes (1.57%) fetch failed, error de conexión con el microservicio: (198 / 12.603) × 100 = 1.57%
- ✓ 37 imágenes (0.30%) ningún rostro detectado en la imagen: (37 / 12.603) × 100 = 0.30%

Estos errores no representan fallos del sistema de reconocimiento sino limitaciones propias de las imágenes del dataset, dado que el sistema requiere exactamente un rostro por imagen para garantizar la integridad del proceso de identificación, tal como se describió en la fase de preprocesamiento.

9.6 Participación en las pruebas de usabilidad con usuarios reales

De los 201 estudiantes contactados durante las jornadas de prueba, 60 participaron voluntariamente, representando el 29.85% del total. De los 141 que no participaron, 35 correspondían a estudiantes menores de edad y 106 no autorizaron el uso de sus datos biométricos de conformidad con la Ley 1581 de 2012. Esta situación redujo el tamaño de la muestra respecto al objetivo inicial, sin embargo, los 60 participantes registrados permitieron evaluar el comportamiento del sistema en condiciones reales de uso.

Figura 33. Mapa PCA 2D con su interpretación



La gráfica muestra la proyección bidimensional mediante Análisis de Componentes Principales (PCA) de los embeddings faciales de 512 dimensiones generados para los participantes registrados durante las pruebas. Los puntos naranjas

representan los embeddings de los estudiantes enrolados y los puntos morados corresponden a docentes que participaron voluntariamente. La distribución espacial de los puntos evidencia que el modelo Buffalo_L generó representaciones matemáticas diferenciadas para cada identidad, sin agrupaciones que indiquen confusión entre identidades distintas, lo que confirma la capacidad del sistema para distinguir correctamente entre los usuarios registrados.

9.7 Pruebas de alcance del reconocimiento facial por dispositivo

Con el propósito de determinar el comportamiento del sistema de reconocimiento facial en condiciones de uso real y establecer la distancia óptima de captura, se realizaron pruebas internas preliminares utilizando el Xiaomi 15T y el iPhone 17. Estas pruebas no corresponden a las pruebas formales con usuarios finales, sino a una evaluación técnica interna realizada por el equipo de desarrollo para caracterizar el rendimiento del sistema antes de ejecutar las pruebas con participantes reales.

Las pruebas consistieron en posicionar a un usuario registrado en el sistema a diferentes distancias de la cámara del dispositivo, evaluando en cada distancia dos modos de captura: automático, en el cual el sistema detecta y procesa el rostro sin intervención del usuario, y manual, en el cual el usuario activa la captura en el momento deseado. Para cada prueba se registró el score de similitud de coseno obtenido y el resultado del reconocimiento frente al threshold configurado de 0.30.

Los resultados obtenidos se presentan en la siguiente tabla:

Distancia	Modo de captura	Xiaomi 15T Score	Xiaomi Resultado	iPhone 17 Score	iPhone Resultado
1 m	Automático	0.7889	Exitoso	0.7520	Exitoso
1 m	Manual	0.7964	Exitoso	0.8004	Exitoso
1.5 m	Automático	0.7819	Exitoso	0.7970	Exitoso
1.5 m	Manual	0.7892	Exitoso	0.7638	Exitoso

2 m	Manual	0.7601	Exitoso	0.8003	Exitoso
3 m	Manual	0.6085	Exitoso	0.7268	Exitoso
4 m	Manual	0.5642	Exitoso	0.6934	Exitoso
5 m	Manual	0.5634	Exitoso	0.6056	Exitoso
6 m	Manual	—	Fallido	0.5463	Exitoso
7 m	Manual	—	Fallido	—	Fallido

Nota. Elaboración propia (2026).

Los resultados evidenciaron que el Xiaomi 15T logró reconocimientos exitosos hasta una distancia de 5 metros, presentando fallo a los 6 metros. El iPhone 17 alcanzó reconocimientos exitosos hasta los 6 metros, fallando a los 7 metros. En ambos dispositivos los scores más altos se registraron en el rango de 1 a 2 metros, donde los valores superaron 0.75, lo que indica una alta confianza en el reconocimiento. A medida que la distancia aumentó, los scores disminuyeron progresivamente, manteniéndose por encima del threshold de 0.30 hasta los límites mencionados.

La diferencia de un metro en el alcance máximo entre ambos dispositivos puede atribuirse a la calidad óptica de la cámara frontal utilizada. El iPhone 17 cuenta con una cámara frontal de 18 MP con sensor Sony IMX914 y estabilización óptica de imagen, mientras que el Xiaomi 15T dispone de una cámara frontal de 32 MP sin estabilización óptica. Aunque el Xiaomi 15T posee mayor resolución nominal, la estabilización óptica del iPhone 17 permitió capturar imágenes del rostro con mayor nitidez a distancias mayores, lo que se tradujo en embeddings de mayor calidad y scores de similitud más altos en distancias largas.

Con base en estos resultados, se estableció como distancia óptima de captura el rango comprendido entre 1 y 3 metros, donde ambos dispositivos obtuvieron scores consistentemente superiores a 0.60, garantizando un reconocimiento confiable. Esta

recomendación técnica define el rango de distancia óptimo para la captura facial en el punto de acceso peatonal de Unitrópico.

Las evidencias fotográficas de cada prueba se encuentran disponibles en el Anexo I del presente documento.

10 IMPACTOS

10.1 Impacto institucional

El proyecto contribuirá al fortalecimiento de los procesos de control de acceso y registro de usuarios en el campus de la Universidad Internacional del Trópico Americano, mediante el desarrollo de una herramienta que permitirá llevar un registro organizado, centralizado y automatizado de los ingresos y salidas de estudiantes, docentes, personal administrativo y visitantes.

Se espera reducir la dependencia de listas en papel y verificaciones manuales, las cuales presentan vulnerabilidades y son propensas a errores o suplantaciones de identidad. De igual manera, el sistema permitirá mejorar la capacidad de respuesta ante incidentes, al disponer de información más precisa y en tiempo real sobre las personas que se encuentran dentro del campus. En este sentido, la incorporación del reconocimiento facial como mecanismo de validación de identidad aportará un mayor nivel de confiabilidad en el control de acceso, disminuyendo la probabilidad de eventos asociados a ingresos no autorizados.

10.2 Impacto académico

El desarrollo del presente proyecto permitirá evidenciar la aplicación de conocimientos en áreas como desarrollo de software, inteligencia artificial y sistemas de información, orientados a la solución de una problemática real del entorno universitario, se espera que sirva como referente para futuros trabajos de grado, al demostrar la integración de metodologías de desarrollo, el análisis de requerimientos y la implementación de tecnologías como el reconocimiento facial en un contexto práctico.

10.3 Impacto tecnológico

Desde el ámbito tecnológico, el proyecto propondrá una solución basada en el desarrollo de sistema que integrará tecnologías actuales para el control de acceso, como el reconocimiento facial y el uso de códigos QR. En este sentido, se espera optimizar el proceso de registro de ingreso y salida de los usuarios, reduciendo la dependencia de métodos manuales y facilitando la gestión de la información de manera automatizada. De igual manera, el uso de estas tecnologías permitirá reducir errores en el registro y mejorar la confiabilidad de la información, contribuyendo a la modernización de los procesos tecnológicos institucionales.

10.4 Impacto organizacional y en la gestión de la información

A nivel organizacional, se espera que el sistema permita una mejor organización y manejo de la información relacionada con el control de acceso, mediante el registro estructurado y centralizado de los datos de ingreso y salida de los usuarios. Esto facilitará la consulta de la información y contribuirá a la reducción de errores asociados a registros manuales.

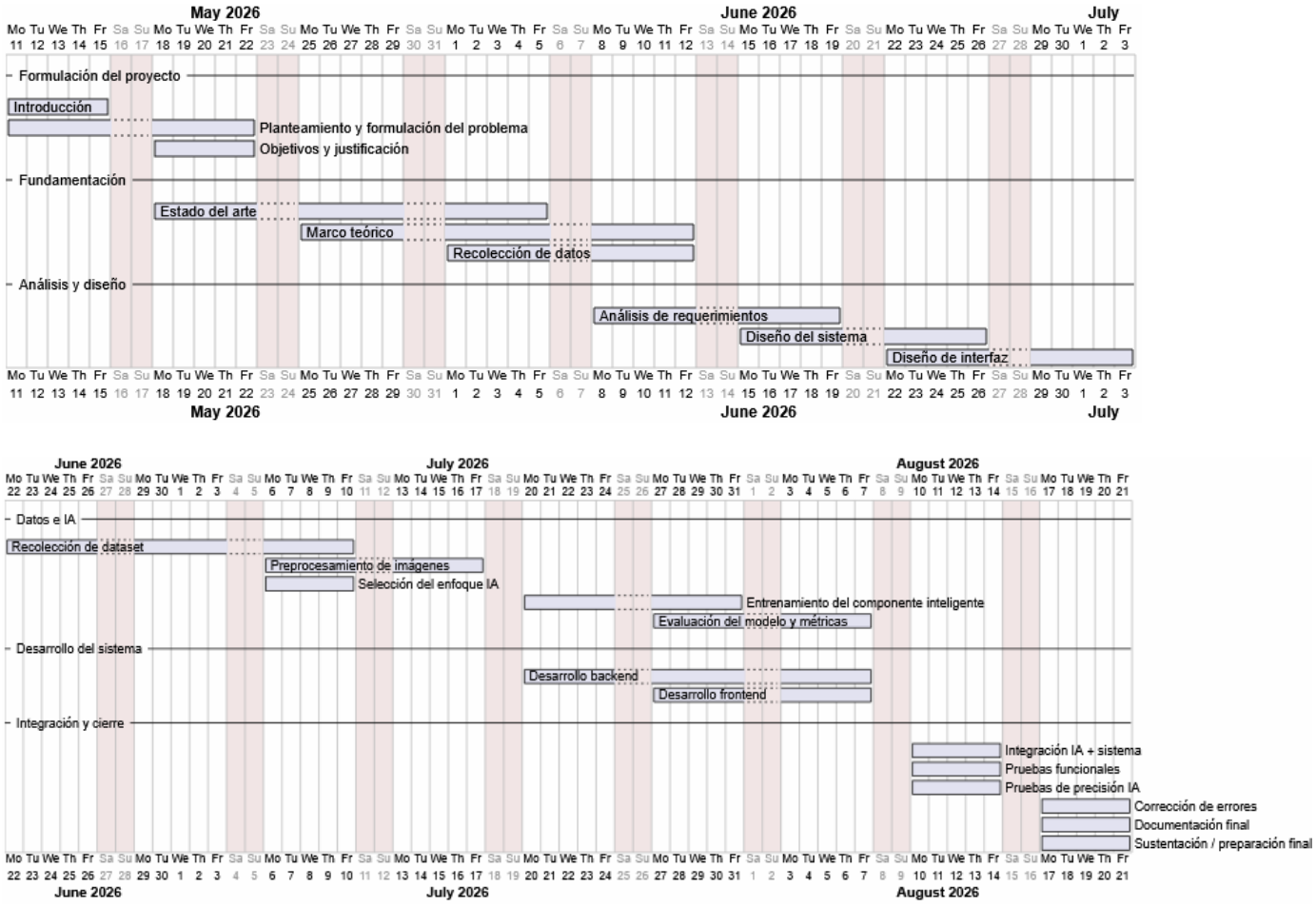
10.5 Alcance del impacto

El impacto descrito corresponderá a un alcance potencial, dado que el proyecto se orientará al diseño y desarrollo de un prototipo funcional del sistema. En este sentido, los beneficios planteados estarán sujetos a su posible implementación en un entorno real dentro de la Universidad Internacional del Trópico Americano, lo cual dependerá de decisiones institucionales, disponibilidad de recursos y ajustes técnicos o normativos requeridos. No obstante, el proyecto dejará planteada una base estructurada que podrá

ser considerada para futuras iniciativas orientadas al mejoramiento del control de acceso en la institución.

11 CRONOGRAMA DE ACTIVIDADES

Figura 34. Cronograma de actividades



Nota. Elaboración propia (2026).

12 PRESUPUESTO

El siguiente apartado detalla el presupuesto asociado al desarrollo del proyecto y se divide en dos categorías principales:

Presupuesto de Hardware: Esta sección engloba toda la parte física utilizada y necesaria para llevar a cabo el proyecto. El hardware en cuestión será proporcionado por parte de la universidad y solo por parte de los integrantes del proyecto.

Presupuesto de Software: Aquí se incluyen todos los programas informáticos utilizados en el proyecto que hayan tenido algún costo asociado.

Tabla 23. Presupuesto.

Presupuesto del proyecto (sin despliegue) y recursos propios				
Categoría	**Ítem / Recurso**	**Cantidad**	**Valor unitario**	**Subtotal / Total**
Talento humano	Estudiante investigador (300 horas)	300	$7.295	$2.188.500
Talento humano	Director del proyecto (22,5 horas)	22,5	$30.000	$675.000
Talento humano	**Subtotal talento humano**			**$2.863.500**
Hardware	Cámara web HD o dispositivo de captura	1	$180.000	$180.000
Hardware	Soporte o accesorios básicos	1	$50.000	$50.000
Hardware	**Subtotal hardware**			**$230.000**
Software	Licencias de software	1	$0	$0
Software	**Subtotal software**			**$0**
Servicios	Internet proporcional al proyecto (4 meses)	4	$40.000	$160.000
Servicios	Energía eléctrica proporcional (4 meses)	4	$25.000	$100.000

Servicios	Transporte a sitio / validaciones (6 salidas)	6	$20.000	$120.000
Servicios	**Subtotal servicios**			**$380.000**
Materiales y suministros	Papelería	1	$40.000	$40.000
Materiales y suministros	Impresiones y anillado	1	$70.000	$70.000
Materiales y suministros	Subtotales materiales			$110.000
Subtotal presupuesto requerido				**$3.583.500**
Imprevistos (8%)				$286.680
Total, presupuesto requerido				$3.870.180
Recursos propios para desarrollo				
Categoría	**Ítem / Recurso**	**Cantidad**	**Valor unitario**	**Subtotal / Total**
Recursos propios	Pavilion HP – Ordenador portátil (15-dk0000)	1	$4.000.000	$4.000.000
Recursos propios	Nitro 5 ACER – Ordenador portátil (AN515-55)	1	$3.999.000	$3.999.000
Recursos propios	HP AIO – Computador (22-dd2004la)	4	$1.189.000	$4.756.000
Recursos propios	Licencia Sistema Operativo Microsoft Windows	4	$88.700	$354.800
Recursos propios	**Total, recursos propios**			**$13.109.800**

Nota. Elaboración propia (2026).

13 BIBLIOGRAFÍA

Alfonso Sierra, J. D., & Castaño Saavedra, D. L. (2021). *Implementación de un modelo computacional basado en inteligencia artificial*.

Alvarado, R., Acosta, K., V, Y., & Buonaffina, M. (2018). *Necesidad de los sistemas de información gerencial para la toma de decisiones en las organizaciones*.

Anden. (2020, octubre 7). *Malla de caras de MediaPipe*. https://github.com/google-ai-edge/mediapipe/wiki/MediaPipe-Face-Mesh

Cano Perfecto, J. E., Ramírez Ruiz, S. Y., Gallegos Olvera, P. A., Varela Leija, N. G., & Hernández Sierra, M. G. (2026). Sistema de toma de asistencia estudiantil con código qr, biometría y geolocalización en tiempo real. *Ciencia Latina Revista Científica Multidisciplinar*, *10*(1), 5115-5136. https://doi.org/10.37811/cl_rcm.v10i1.22615

Cardozo Servian, L. A., & Macen Rojas, C. D. (2023). Reconocimiento biométrico facial para el control de asistencia de alumnos en centros educativos y visualización de resultados en dispositivos móviles. *Revista Ingeniera, Ciencia y Sociedad*, *5*(1). https://doi.org/10.47133/facet-unc-2023-1-5f

Chavez Vargas, R. R. (2025). *Aplicación con reconocimiento facial y la mejora en el proceso de control de asistencia*. https://orcid.org/0000-0001-9660-6354

Claudio, C. J. S. (2024). *Una propuesta para incorporar calidad de datos en criterios de aceptación en historias de usuario*.

Elnozahy Seifeldin Liang, C. L., Pari C, S., & Liang Chu, L. (2025). Raspberry pi based face recognition door lock system. *Internet of Things*, *6*(2). https://doi.org/10.3390/iot6020031

Fidias G., A. (2012). *El proyecto de investigación Introducción a la metodología científica*.

Fortinet. (2025). *Qué es un token de autenticación*. https://www.fortinet.com/lat/resources/cyberglossary/authentication-token

Harish K. (2025, abril 30). *Mi viaje hacia el reconocimiento facial revelando la magia del análisis facial inteligente*.

Hernandez, S., & R. Collado, L. L. (2018). *Cátedra metodología para la investigación en ciencia política*.

IBM. (2024a). *Que es la inteligencia artificial*. https://www.ibm.com/mx-es/think/topics/artificial-intelligence

IBM. (2024b). *Qué es una API*. https://www.ibm.com/es-es/think/topics/api

IBM. (2025). *Qué es la autenticación*. https://www.ibm.com/mx-es/think/topics/authentication

Jaramillo Alberto. (2018). *Guía para la verificación de condiciones institucionales para el otorgamiento del registro calificado*. https://www.mineducacion.gov.co/portal/micrositios-superior/Publicaciones-Educacion-Superior/338168:Guia-para-la-verificacion-de-condiciones-institucionales-para-el-otorgamiento-del-registro-calificado

John Navarrete. (2024, julio 18). *Qué Pasa Yopal - Noticias*. https://quepasayopal.com/yopal-falso-ingeniero-hurta-iphones-en-unitropico/

K, H. (2025, abril 30). *Mi viaje hacia el reconocimiento facial descubriendo la magia del análisis facial inteligente*. https://medium.com/@harishk3493/my-journey-into-face-recognition-unveiling-the-magic-of-intelligent-facial-analysis-9d4f42e4897d

Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Face liveness detection using artificial intelligence techniques: systematic literature review and future directions. En *Big Data and Cognitive Computing* (Vol. 7, Número 1). MDPI. https://doi.org/10.3390/bdcc7010037

Legarda Delgado, F. D., & Loaiza Pabon, O. A. (2022). *Reconocimiento facial para la automatización del registro de asistencia a clase*.

Llanos Bermudez, J. E., & Hurtado Pardo, E. F. (2021). *Sistema de control de asistencia a estudiantes mediante carnet virtual con código qr*.

Luckianto, M. (2026, julio 21). *Conjunto de datos labelled faces in the wild*. https://www.kaggle.com/datasets/marvinluckianto/labelled-faces-in-the-wild-lfw-dataset/data

Lugaresi Camillo. (2019). *Mediapipe un marco para construir canalizaciones de percepción*. https://arxiv.org/abs/1906.08172

Martinez Renteria, F. L., & Florez Burgos, J. G. (2023). *Aplicación móvil utilizando el framework flutter para la carnetización de los estudiantes de la universidad de córdoba*. www.unicordoba.edu.co

Max Rehkopf. (2025, noviembre 21). *Historias de usuario con ejemplos y plantilla*. https://www.atlassian.com/es/agile/project-management/user-stories

Menzinsky, A., Gertrudis, L., Palacio, J., Sobrino, M. Á., Álvarez, R., & Rivas, V. (2026). *Historias de usuario*.

Microsoft. (2025). *Información general de ASP.NET MVC | Microsoft Learn*. https://learn.microsoft.com/es-es/aspnet/mvc/overview/older-versions-1/overview/asp-net-mvc-overview

Misión Visión. (2021). https://www.unitropico.edu.co/index.php/unitropico/mision-vision

Mohamed Idabrahim. (2025, septiembre 24). *InsightFace the open source powerhouse for 2d & 3d face recognition, detection and swapping*. https://www.blog.brightcoding.dev/2025/09/24/insightface-the-open-source-powerhouse-for-2d-3d-face-recognition-detection-and-swapping/

Mukesh. (2024, diciembre 11). *Análisis facial con biblioteca insightface*. https://medium.com/@appanamukesh77/comprehensive-insights-onfacial-analysis-with-insightface-library-796d80464f45

Nasareno, C., Rosario, E., Macías, Á., Genith, K., Gutiérrez, D., Alfredo, D., Hernández, O., & Humberto, E. (2020). *Caracterización de la movilidad vehicular y peatonal en la universidad técnica de manabí*.

Ortiz Cuadros, J. D. (2018). *Control de acceso basado en tecnologías iot en instituciones De educación superior. Prototipo aplicado al control del Ingreso a salones y auditoría en la universidad autónoma de Bucaramanga*.

Otzen, T., & Manterola, C. (2017). Técnicas de muestreo sobre una población a estudio. En *Int. J. Morphol* (Vol. 35, Número 1).

Palomino Sulca, D. C. (2023). *Implementación de un sistema de registro de usuarios temporales utilizando código qr para mejorar el control de acceso a una institución privada*. https://cybertesis.unmsm.edu.pe/item/dd2b12cd-b512-499c-bdc5-30243f456dbd

Paredes, J., Gonzalez, E., Santamaria Castillo, J. G., & Villareal, V. (2023). Sistema para la automatización del registro de asistencia en las aulas de clases. *Revista Tecnología en Marcha*. https://doi.org/10.18845/tm.v36i8.6930

Perez Ibarra, S. G., Quispe Rolando, J., Mullicundo, F. F., & Alberto Lamas, D. (2021). *Herramientas y tecnologías para el desarrollo web desde el frontend al backend*. https://www.campusmvp.es/recursos/post/Desar

Pérez Valdés, D. (2007, octubre 26). *Qué son las bases de datos*. https://www.maestrosdelweb.com/que-son-las-bases-de-datos/

Planeacion estrategica. (2026, junio 30). https://planitone.co/planeacion/#/estadistica

Qasim. (2026, febrero 14). *Cómo construir un sistema de reconocimiento facial con insightface y python*. https://agentbus.sh/posts/how-to-build-a-face-recognition-system-with-insightface/

Reyes Alcivar, N. S. (2026). *Sistema informático para el control de acceso mediante la utilización de dispositivo de reconocimiento facial de docentes y estudiantes de la escuela mathius josue quintanilla sierra de la ciudad de portoviejo*.

Reyes Campos, J. E., Castañeada Rodriguez, C. S., Alva Lujan, L. D., & Mendonza De Los Santos, C. A. (2023). Sistema de reconocimiento facial para el control de accesos mediante inteligencia artificial. En *Revista Innovación y Software* (Vol. 4, Número 1).

Serna Herrera, L. M. (2010). *Manual para el control de ingreso, permanencia y salida al campus universitario vicerrectoría administrativa departamento de vigilancia elaboró*.

Shruthi, M., Sangeetha, M. P., Kodte, A., & Tejaswini, K. V. (2024). Automated Attendance Sentinel. En *International Journal for Research Trends and Innovation (www.ijrti.org)* (Vol. 9). www.ijrti.org

Silva, A. A. G. (2024). *Desarrollo de un sistema para el control de asistencia estudiantil mediante el uso de algoritmos de reconocimiento facial basado en visión artificial*.

Soekarta, R., & Ku-Mahamud, K. R. (2025). Recent facial image preprocessing techniques a review. *Engineering Proceedings*, *84*(1). https://doi.org/10.3390/engproc2025084039

Soukupová, T., & Cech, J. (2016). *Real time eye blink detection using facial landmarks*.

Unitropico. (2026). *Por el cual se aprueba la reforma y actualización del proyecto educativo institucional (pei) de la universidad internacional del trópico americano*. www.unitropico.edu.co

Vargas Encalada, E. E., Rengifo Lozano, R. A., Guizado Oscco, F., & Sánchez Aguirre, F. D. M. (2019). *Sistemas de información como herramienta para reorganizar procesos de manufactura*. https://www.redalyc.org/articulo.oa?

Villegas, B. E. (2022). Metodologías agiles xp y scrum, empleadas para el desarrollo de páginas web, bajo mvc, con lenguaje php y framework laravel. *Revista Amazonía Digital*, *1*(1), e168. https://doi.org/10.55873/rad.v1i1.168

Yang, X., Luo, W., Bao, L., Gao, Y., Gong, D., Zheng, S., Li, Z., & Liu, W. (2019). *Face anti spoofing model matters, so does data*.

Zertucha González, I. J., Rodriguez Ramos, A., Méndez Zambrano, L., Picarin Pérez, H., & Humberto Díaz, P. (2022). Sistema de control de acceso mediante código qr. En *Revista Estudiantil Nacional de Ingeniería y Arquitectura* (Vol. 3, Número 3).

Zhalgas, A., Amirgaliyev, B., & Sovet, A. (2025a). Robust face recognition under challenging conditions: a comprehensive review of deep learning methods and challenges. *Applied Sciences 2025, Vol. 15, Page 9390*, *15*(17), 9390. https://doi.org/10.3390/APP15179390

Zhalgas, A., Amirgaliyev, B., & Sovet, A. (2025b). Robust face recognition under challenging conditions: a comprehensive review of deep learning methods and challenges. En *Applied Sciences (Switzerland)* (Vol. 15, Número 17).

Multidisciplinary Digital Publishing Institute (MDPI).
https://doi.org/10.3390/app15179390

14 ANEXOS

Anexo A. Guía de entrevista semiestructurada

- ¿Cómo se realiza actualmente el proceso de identificación?
- ¿Qué sucede cuando un estudiante deja su carnet?
- ¿En qué momento se deja un documento propio de identificación para recibir una tarjeta de ingreso?

- ¿Cree que actualmente se puede conocer con precisión el quien ingreso y a qué hora?
- ¿Si la Universidad desea saber un registro de una fecha en concreto que debe hacer?
- ¿Qué dificultades o limitaciones presenta el proceso actual?
- ¿Qué riesgos considera que existen con el método actual de validación?
- ¿La Universidad le ofrece algún tipo recurso tecnológico como apoyo?
- ¿Considera que sería útil contar con un sistema que registe automáticamente?

Anexo B. Cuestionario de encuesta.

¿Considera que el proceso actual de identificación/validación es eficiente?

- Sí
- No
- Parcialmente

¿Ha tenido inconvenientes con métodos tradicionales de validación?

- Sí
- No

¿Considera útil implementar un sistema de validación facial?

- Muy útil
- Útil
- Poco útil
- Nada útil

¿Qué tan importante considera la rapidez en el proceso de validación?

- Muy importante
- Importante
- Poco importante
- Nada importante

¿Qué tan importante considera la precisión del sistema?

- Muy importante
- Importante
- Poco importante
- Nada importante

¿Le generaría confianza un sistema de validación facial para este propósito?

- Sí
- No
- No está seguro(a)

¿Qué aspecto considera más importante en el sistema?

- Seguridad

- Rapidez
- Facilidad de uso
- Registro de información
- Otro

¿Tiene alguna preocupación frente al tratamiento de su imagen o datos biométricos?

- Sí
- No
- En caso afirmativo, ¿cuál?

¿Estaría dispuesto(a) a participar en pruebas del sistema?

- Sí
- No

Anexo C. Formato consentimiento informado para tratamiento de datos biométricos

FORMATO DE CONSENTIMIENTO INFORMADO

1. INFORMACIÓN GENERAL DEL ESTUDIO

Por medio del presente documento, se invita al participante a autorizar de manera libre, previa, expresa e informada la captura y uso de imágenes faciales con fines

exclusivamente académicos e investigativos, como parte del desarrollo del proyecto de grado denominado:

"DISEÑO Y DESARROLLO DE UN PROTOTIPO FUNCIONAL DE SISTEMA DE IDENTIFICACIÓN Y CONTROL DE ACCESO PEATONAL A LAS INSTALACIONES EN LA UNIVERSIDAD INTERNACIONAL DEL TRÓPICO AMERICANO"

El propósito del proyecto es desarrollar y evaluar un sistema basado en inteligencia artificial y reconocimiento facial que permita identificar y validar personas mediante el análisis automatizado de características biométricas del rostro.

2. PROCEDIMIENTO

Si usted acepta participar, se realizará la captura de fotografías de su rostro. Estas imágenes serán incorporadas a una base de datos destinada exclusivamente a la prueba y validación del sistema desarrollado dentro del proyecto académico.

3. USO Y TRATAMIENTO DE LA INFORMACIÓN

Las imágenes recolectadas serán utilizadas únicamente para:

- Validación y pruebas del aplicativo desarrollado.
- Presentación de resultados académicos del proyecto.
- Sustentación universitaria y documentación técnica asociada.

4. PARTICIPACIÓN VOLUNTARIA

Su participación es completamente voluntaria. Usted podrá retirar su consentimiento en cualquier momento solicitando la eliminación de sus imágenes y datos del proyecto, sin que ello genere consecuencia alguna.

5. AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES

De conformidad con la Ley 1581 de 2012 sobre protección de datos personales en Colombia, autorizo a los responsables del proyecto para recolectar, almacenar, procesar y utilizar mis imágenes faciales para los fines descritos anteriormente. Las imágenes serán eliminadas dentro de los 30 días siguientes a la aprobación final del trabajo de grado.

6. DERECHOS DEL TITULAR

Como titular de los datos, usted tiene derecho a conocer, actualizar y rectificar sus imágenes faciales tratadas; solicitar prueba de la autorización otorgada; y presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a la Ley 1581 de 2012.

7. DECLARACIÓN DE CONSENTIMIENTO

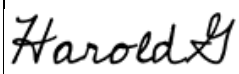
Nombre completo:	
Tipo de documento:	
Número de documento:	

Declaro que:

- He leído y comprendido la información contenida en este documento.
- He tenido la oportunidad de realizar preguntas y estas han sido respondidas satisfactoriamente.
- Entiendo que mi participación es voluntaria.
- Autorizo la captura y tratamiento de mis imágenes faciales para el proyecto descrito.

FIRMA DEL PARTICIPANTE

FIRMA DE LOS INVESTIGADORES RESPONSABLES


Nombre: Harold Stiven Gutiérrez Orduz
Contacto: 3175110860


Nombre: Didier Antonio Niño González
Contacto: 3227495485

Nota. Elaboración propia (2026).

Anexo D. Entrevista a Jefe del Departamento de Sistemas

(Estudiantes) Nuestro proyecto de grado es más que todo, como una automatización al ingreso y salida de los estudiantes. La idea que teníamos era ya que los carnets tienen un código QR, pues a utilizar ese mismo, esa misma tecnología para hacer el control de ingreso, entonces estamos pensando en hacer como un aplicativo web en el cual ingresen los administradores y pues bueno, cuando administradores pueden ser gente acá de la Universidad como gerentes o que quieran verificar información, los mismos porteros que son los encargados de hacer el ingreso de los estudiantes, entonces, ese aplicativo web tendrá un botón en el cual identifica el código QR, se escanee. Lo que estamos pensando era por medio de la Cámara, ya que pues no contamos con lectores QR, entonces por ahora entonces al menos hacerlo por medio de las cámaras, lea el QR certifiquen la base de datos que la persona está en la Universidad y a lo que otra vez se vuelve a hacer la lectura del código QR, se quita esa verificación de que está en la Universidad es, en pocas palabras, es el sistema que teníamos pensado así como a grandes rasgos, entonces el ingeniero Cristian, pues lo estaba complementando con ciertas ideas que nos decía, por ejemplo, hacer algunas consultas en SQL en la cual en los verifiqué sistemáticamente cosas más estadísticas, que por ejemplo, tema, horarios, tema fechas, tema tipo qué tanta gente hubo en tal lapso de tiempo? Entonces es más que todo ese tipo del tema y también una idea, pero bueno, eso ya es más en veremos. Es también como modernizar el por la portabilidad del carnet y hacerla virtual como tipo, aplicación en la cual simplemente sea un login específico en el cual puede ingresar con su correo institucional, ingrese y simplemente sea como una plantilla en donde esté la foto, el nombre y el mismo código QR y que ese mismo código QR se utilice para el ingreso. Eso sí, en pocas palabras, es como el proyecto que queríamos hacer, Entonces, por ejemplo, queremos más que todo preguntarle como si qué impedimentos podría haber sugerencias, pues algunos requerimientos que vea correspondientes acerca del tema.

(Ing. Luis Parra) Pues bueno la idea me pareció muy interesante, muy buenas márgenes, pero estamos trabajando lo que les dije, una parte con biblioteca por el momento, pero sí mi idea era implementar algo que, al vigilante, sobre todo y en las 3 entradas que tenemos porque por ejemplo la vehicular, ¿cómo lo vamos a hacer? La vehicular tiene un problema, todos los que entran en el carro entran como si nada ¿Y no se mide, ¿quién entra y quién no entra, eso es algo que hay que ver cómo lo vamos a hacer? Y sí, algo que el guardia o el vigilante pueda ver que la persona sí está, es decir que sí. ¿Lo que pasó en el carnet, si está porque yo he visto personas que tienen a otro carne que no les pertenece y han entrado y lo he visto y lo he lo he presenciado entonces, eso me parece interesante, mí me gustaría es si ya tienen un bosquejo de eso porque el alcance está bien, está muy bien, ¿Y si tienen algún tipo de bosquejo de cómo se va a administrar, como les dije a ustedes, la idea es que me lleguen como 8 lectores de QR, 8 o 10 no me acuerdo ahorita los cuales nos van a ayudar a **“Tener eso para no**

depender de un celular, sí, sobre todo para los vigilantes y que eso esté conectado a un equipo de cómputo que le vamos a instalar allá a los vigilantes".

(Estudiantes) No, pues bosquejo hasta ahora no, no tenemos como tal un bosquejo, o sea, tenemos más que todo los requerimientos para realizar el bosquejo, a ver si se necesitaban más cosas, por ejemplo, lo que decía el ingeniero, lo de las consultas es SQL entonces implementar eso más bien también en la plantilla que nosotros teníamos. Pues por el momento simplemente es la aplicativo con el Login de administrador, ingresa a la página y en ese punto es donde debería estar todo lo consecuente a los estudiantes, la información de los estudiantes, el escaneo y las consultas que se quieran realizar, eso es más que todo el bosquejo, pero no tenemos como tal el físico, lo que tenemos es una idea ahí. Otro tema también es de las personas que llegan, pero no son de la Universidad, los que no tienen carnet, invitados, entonces ese tema también lo quería mirar porque no sabría cómo agregarlos al sistema o quería agregarlos al sistema, pero no sabría es cómo, sí, por lo que he mirado es simplemente una lista en papel de las personas que ingresan, se le toma datos y ya eso es más que todo, como el sistema que tienen ahí en la entrada. Pues es una idea que tenía era hacerlo virtual también, entonces por medio de la aplicación, tal vez hacer un formulario en el cual se registre y haga como un usuario temporal. También podría ser una solución, no sé, no sabría qué tan buena idea hacer, pero pues como una primera idea era el de lo que teníamos pensado también, ¿Sino de qué tal? ¿Qué tal parezca?

(Ing. Luis Parra) Me gusta, me gusta, yo lo que les digo es tener muy claro el tema de lo que va a pasar. Ósea yo pienso que como lo están planeando, está muy bien, ya nos toca es empezar, ¿y eso va a estar desarrollado específicamente en?

(Estudiantes) Pues la idea es comenzar ya con el desarrollo, entonces sería como máximo 2 meses por mucho, dependiendo de si el ingeniero nos guíe. ¿Cómo va a ser el en sí el aplicativo? Entonces, dependiendo si se va a cambiar cositas o se va a hacer como la ruta que teníamos, establecía más o menos 2 meses, por mucho el teníamos estimado que se realizaba todo, ¿Qué otros requerimientos específicos se necesitarán?

(Ing. Luis Parra) Pues, los míos ya se los dije, no sé si necesitan que se los envíe por correo o algo, básicamente eso es lo que yo quiero, tener un control más específico y una vez eso dejarlo ahí en pie para lo de la biblioteca tenga como poder cuantificar eso para los ingresos de allá.

(Estudiantes) Tema consultas, por ejemplo, ¿Qué al tener este sistema como qué? ¿Qué tipo de consultas le gustaría saber acerca de los estudiantes?, para implementarlo ahí.

(Ing. Luis Parra) ¿De los estudiantes?

(Estudiantes) Por ejemplo, si su merced tiene el sistema y tiene el control de quiénes entran y quiénes salen, ¿quiénes están en la Universidad, por ejemplo, que le gustaría ver?, se centra el sistema que le gustaría ver qué información le gustaría conocer acerca de?

(Ing. Luis Parra) Pues básicamente, primero, el nivel de acceso que tenemos, es decir, ¿cuántos estudiantes entran al día, cuantos, al mes, ¿cuánto es eso?, primero eso como estadística, segundo, obtener quiénes entran como invitados porque obviamente los que lleguen y que ese invitado se registre, hay es algo que tienen que pensar sí, ¿es decir el que tiene carnet le lee el QR y sale cierto? No hay problema, pero y el que no, debe haber una excepción que esto que especifique qué tipo de invitado es, o un es estudiante que se le quedó el carnet y entonces, después de la tercera vez que se le quedó el carné se le llama la atención, porque de nada sirve tener invitados y van a entrar siempre como invitados los estudiantes, entonces el estudiante con la identificación, aquí viene una cuestión, el estudiante debe, o sea el que llega y entre debe haber una verificación de la célula, sí, el que entre a entrar con documento de identidad al verificar la cédula si aparece como estudiante hay que decirle el motivo del por qué no tiene el carnet, ¿Sí, sí, después de los 3 llamados de que por qué no tiene carnet?, Ósea, después de que el sistema me diga a mí que el estudiante ha entrado 3 veces sin carnet, ahí yo le llamo la atención académica para que académica le llame la atención al estudiante porque no ha tramitado el carnet.

LUIS ANTONIO PARRA
Jefe del departamento de sistemas (Entrevistado)

HAROLD ESTIVEN GUITERREZ ORDUZ
DIDIER ANTONIO NIÑO GONZALEZ
Estudiantes de ingeniería de Sistemas (Entrevistadores)

Anexo E. Entrevista Vigilante No. 01

(Estudiantes) Pregunta lo del carnet. Y luego, y que una pregunta, nosotros queríamos a ver de cerca de cómo se maneja, ¿eh?

(Vigilante) Cuando un estudiante olvida su carnet, bueno, cuando los estudiantes olvidan su carne, ahí está. Como pueden ver acá hasta la libreta, se tienen que registrar con su documento, el nombre, documento, lo que está estudiando, la firma la hora y ya puede seguir.

(Estudiantes) Y en caso de cuando es invitado?

(Vigilante) Bueno, el tema invitado, ellos un procedimiento, pero ellos tienen que dar un documento y se le entrega un carnet que dice visitan y ella pueden ingresar. Ese es el procedimiento de los visitantes y el procedimiento igual del de los estudiantes para los dos.

(Estudiantes) Muchas gracias.

HAROLD ESTIVEN GUITERREZ ORDUZ
DIDIER ANTONIO NIÑO GONZALEZ
Estudiantes de ingeniería de Sistemas (Entrevistadores)

Anexo F. Entrevista Vigilante No. 02

Estudiante: ¿Cómo se realiza actualmente la identificación para el ingreso? ¿Con el carnet de estudiante o con un documento personal cuando no traen el carnet?

Vigilante: Cuando no tienen carnet se utiliza la minuta de registro.

Estudiante: ¿Esto que utilizan como minuta, es para estudiantes solamente?

Vigilante: No, es para todo el mundo: docentes, estudiantes, administrativos, visitantes y personal externo. Se utiliza cuando no tienen carnet.

Estudiante: ¿Se utiliza cuando no tienen identificación?

Vigilante: Cuando no tienen carnet.

Estudiante: ¿Cree que actualmente se puede conocer con precisión quién ingresó y a qué hora?

Vigilante: Sí, porque en la minuta del registro se coloca la hora, el nombre y hacia dónde se dirige la persona.

Estudiante: Si la universidad quisiera revisar el registro de forma más organizada, ¿cómo tendría la posibilidad de hacerlo?

Vigilante: Enviando un correo directamente al jefe de operaciones.

Estudiante: ¿Qué dificultad o limitación ha visto que presenta el sistema actual, o ha funcionado todo correctamente?

Vigilante: La dificultad principal es que los estudiantes no portan el carnet como lo exige la norma.

Estudiante: ¿La universidad le ofrece algún tipo de recurso tecnológico o apoyo con respecto a este sistema?

Vigilante: No. Todo es por parte de la empresa.

Estudiante: ¿Considera que sería útil contar con un sistema automático de registro?

Vigilante: Sí, sería bueno implementar un sistema biométrico integrado con el carnet.

Anexo G. Entrevista Vigilante No. 03

Estudiante: ¿Cómo se realiza actualmente el proceso de identificación para el ingreso?

Vigilante: El carnet es el requisito de la universidad para identificarse como estudiante. Una persona que no tiene carnet quiere decir que no pertenece a la universidad. En esta entrada solo se valida el carnet en físico para poder ingresar; si no lo trae, se le dirige a la entrada peatonal.

Estudiante: ¿Qué sucede cuando un estudiante olvida su carnet?

Vigilante: En la entrada peatonal existe el proceso donde, si se le queda el carnet, debe dejar un documento y hacer un registro de ingreso para que quede constancia de que esa persona está dentro de la universidad. En esta entrada no se maneja ese proceso.

Estudiante: ¿En qué momento se deja un documento propio de identificación para recibir una tarjeta de ingreso?

Vigilante: Eso aplica únicamente en la entrada peatonal. En esta entrada no se maneja eso; aquí solo ingresa quien presente el carnet en físico.

Estudiante: ¿Cree que actualmente se puede conocer con precisión quién ingresó y a qué hora?

Vigilante: Puede existir una hora aproximada, pero no una hora precisa. Para tener una hora precisa se tendría que automatizar todo, con un código que registre automáticamente cada ingreso. Registrar en un libro a mil o tres mil personas es imposible hacerlo con precisión; por eso puede existir una hora próxima pero no una exacta.

Estudiante: ¿Si la Universidad desea saber el registro de una fecha en concreto, ¿qué debe hacer?

Vigilante: Debe oficiar a la empresa. Todo llega de empresa a universidad; los respaldos están en la empresa. Si la universidad quiere verificar registros de alguna fecha, le oficia a la empresa y nosotros le informamos. La universidad no nos oficia directamente a nosotros sino a la empresa, y la empresa nos informa.

Estudiante: ¿Qué dificultades o limitaciones presenta el proceso actual?

Vigilante: El tema principal es la identificación. Mucha gente no porta el carnet, pero no es porque no sepan sino por responsabilidad de cada persona. El uso del carnet es obligatorio y está establecido en el manual. Un estudiante que porta el carnet visible simplemente entra sin ningún inconveniente.

Estudiante: ¿Qué riesgos considera que existen con el método actual de validación?

Vigilante: Sin un registro automatizado no es posible saber con certeza cuántas personas quedan dentro de las instalaciones en un momento dado. Esto representa un riesgo especialmente en situaciones de emergencia, donde sería necesario saber exactamente cuántas personas están dentro para una eventual evacuación.

Estudiante: ¿La Universidad le ofrece algún tipo de recurso tecnológico como apoyo?

Vigilante: Entre la empresa y la universidad existe un acuerdo en el que la universidad presenta sus requerimientos y la empresa responde a ellos. La universidad le dice a la empresa cómo quiere que se hagan las cosas y la empresa cumple ese requerimiento. Lo que hay actualmente, como la libreta de registro en la entrada peatonal, responde a lo que la universidad solicitó; la empresa simplemente cumple la exigencia.

Estudiante: ¿Considera que sería útil contar con un sistema que registre automáticamente?

Vigilante: Sí, facilitaría mucho los ingresos y permitiría verificar entradas, salidas, reportes y consultas fácilmente. Por ejemplo, el carnet con un código que al pasarlo registre automáticamente la entrada y la salida. Esto ya se ha aplicado en conjuntos residenciales, donde el sistema indica cuántas personas quedan dentro en tiempo real, lo cual es muy útil especialmente para situaciones de emergencia o evacuación.

Vigilante: La relación entre la empresa y la universidad funciona así: la empresa presenta su propuesta y la universidad establece sus requerimientos; la empresa responde a lo que el cliente solicita. Por ejemplo, si la universidad dice que se requisen todas las motos a la salida, la empresa lo implementa. La responsabilidad del control de acceso está definida por lo que la universidad le exige a la empresa, no por iniciativa propia de la empresa.

Anexo H. Guía de observación directa

Registro Día 1

Fecha:	Martes 12 de mayo de 2026
Lugar:	Acceso peatonal principal – Carrera 19 No. 39-40, Yopal

Franja horaria	Total, ingresos	Sin carnet	% Sin carnet	Registro minuta
6:00 a.m. – 8:00 a.m.	522	36	6.90%	12
12:00 p.m. – 2:00 p.m.	399	41	10.28%	27
5:00 p.m. – 7:00 p.m.	428	20	4.67%	15
Total, día	1.349	97	7.19%	54

Registro Día 2

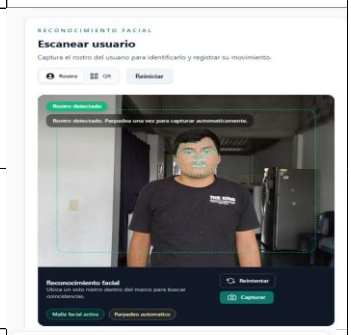
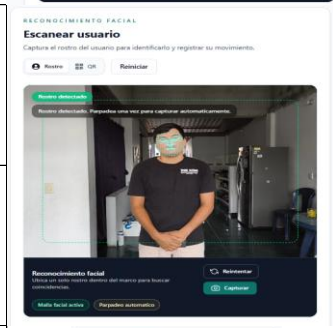
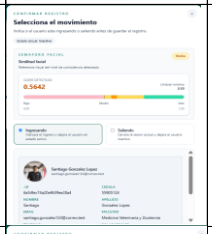
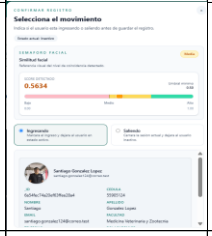
Fecha:	Jueves 14 de mayo de 2026
Lugar:	Acceso peatonal principal – Carrera 19 No. 39-40, Yopal

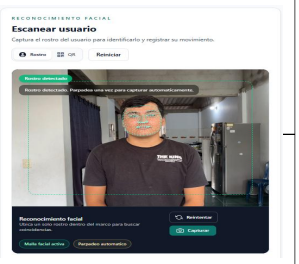
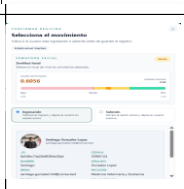
Franja horaria	Total, ingresos	Sin carnet	% Sin carnet	Registro minuta
6:00 a.m. – 8:00 a.m.	498	34	6.83%	11
12:00 p.m. – 2:00 p.m.	412	38	9.22%	25
5:00 p.m. – 7:00 p.m.	415	22	5.30%	14
Total, día	1.325	94	7.09%	50

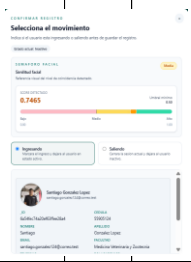
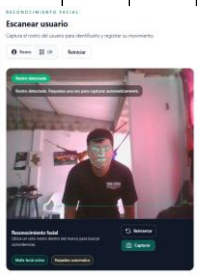
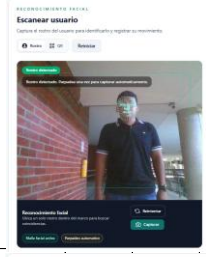
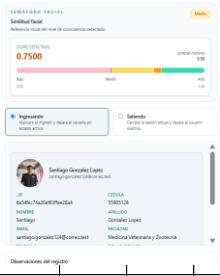
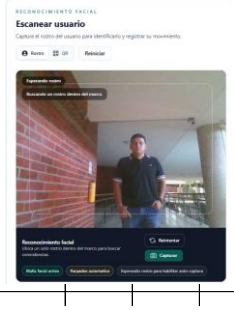
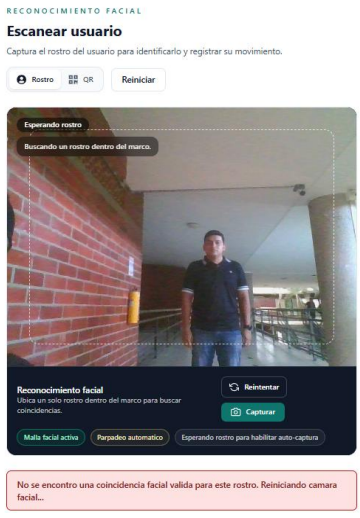
Promedio de los dos días

Franja horaria	Promedio ingresos	Sin carnet	% Sin carnet	Registro minuta
6:00 a.m. – 8:00 a.m.	510	35	6.86%	12
12:00 p.m. – 2:00 p.m.	406	40	9.85%	26
5:00 p.m. – 7:00 p.m.	422	21	4.98%	15
Promedio total diario	1.337	96	7.18%	52

Anexo I. Evidencias fotográficas de pruebas de alcance

Distancia (Metros)	Dispositivo	Modo de captura (Automatico / Manual)	Score obtenido	Evidencia	Resultado (Exitoso / Fallido)	Evidencia
1 m	Xiaomi 15T	Automatico	0.7889		Exitoso	
1 m	Xiaomi 15T	Manual	0.7964		Exitoso	
1,5 m	Xiaomi 15T	Automatico	0.7819		Exitoso	
1,5 m	Xiaomi 15T	Manual	0.7892		Exitoso	
2 m	Xiaomi 15T	Manual	0.7601		Exitoso	
3 m	Xiaomi 15T	Manual	0.6085		Exitoso	
4 m	Xiaomi 15T	Manual	0.5642		Exitoso	
5	Xiaomi 15T	Manual	0.5634		Exitoso	
6	Xiaomi 15T	Manual			Fallido	

Distancia (Metros)	Dispositivo	Modo de captura (Automatico / Manual)	Score obtenido	Evidencia	Resultado (Exitoso / Fallido)	Evidencia
1 m	Iphone 17 Base	Automatico	0.7520		Exitoso	
1 m	Iphone 17 Base	Manual	0.8004		Exitoso	
1,5 m	Iphone 17 Base	Automatico	0.7970		Exitoso	
1,5	Iphone 17 Base	Manual	0.7638		Exitoso	
2 m	Iphone 17 Base	Manual	0.8003		Exitoso	
3 m	Iphone 17 Base	Manual	0.7268		Exitoso	
4 m	Iphone 17 Base	Manual	0.6934		Exitoso	
5	Iphone 17 Base	Manual	0.6056		Exitoso	
6	Iphone 17 Base	Manual	0.5463		Exitoso	
7	Iphone 17 Base	Manual			Fallido	

Distancia (Metros)	Dispositivo	Modo de captura (Automatico / Manual)	Score obtenido		
1 m	Hp Pavilion Gaming Laptop	Automatico			
1 m	Hp Pavilion Gaming Laptop	Manual			
1,5 m	Hp Pavilion Gaming Laptop	Automatico			
1,5	Hp Pavilion Gaming Laptop	Manual			
2 m	Hp Pavilion Gaming Laptop				