UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA:

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA AUTOMATIZADO PARA CONTROL DE ACCESO MEDIANTE RECONOCIMIENTO FACIAL PARA EL AULA STEAM DE LA UNIVERSIDAD CATOLICA DE CUENTA EXTENSIÓN SAN PABLO DE LA TRONCAL

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR: Anthony Yair Yadaicela Toledo

DIRECTOR: Ing. Marcos Giovanny Orellana Parra, PhD.

LA TRONCAL – ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESAROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA:

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA AUTOMATIZADO PARA CONTROL DE ACCESO MEDIANTE RECONOCIMIENTO FACIAL PARA EL AULA STEAM DE LA UNIVERSIDAD CATOLICA DE CUENCA EXTENSIÓN SAN PABLO DE LA TRONCAL

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR: Anthony Yair Yadaicela Toledo

DIRECTOR: Ing. Marcos Giovanny Orellana Parra, PhD.

LA TRONCAL – ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Anthony Yair Yadaicela Toledo portador de la cédula de ciudadanía Nº **0942350596**. Declaro ser el autor de la obra: "**Implementación de un prototipo de sistema automatizado para control de acceso mediante reconocimiento facial para el aula STEAM de la Universidad Católica de Cuenca, extensión San Pablo La Troncal"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

La Troncal, 16 de septiembre del 2025

Anthony Yair Yadaicela Toledo
C.I. 0942350596

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

UNIDAD DE TITULACIÓN

La Troncal, 23 de agosto de 2025

Sección: U.A. de Informática, Ciencias de la Computación e Innovación Tecnológica

Asunto: Certificación y aprobación de presentación del Trabajo de Titulación

Señor Ingeniero
Guillermo Rodríguez López.Mgtr
Director de carrera
Ingeniería en Tecnologías de la Información

De mi consideración.

Reciba un cordial saludo y mis mejores deseos de éxito en sus funciones.

El suscrito, en calidad de tutor del trabajo de titulación, certifica que el trabajo titulado: "**Implementación de un prototipo de sistema automatizado para control de acceso mediante reconocimiento facial para el aula STEAM de la Universidad Católica de Cuenca extensión San Pablo de La Troncal**", desarrollado por el estudiante **ANTHONY YAIR YADAICELA TOLEDO**, con numero de cedula **0942350596,** ha sido guiado y revisado de manera periódica, cumpliendo con las normativas estatutarias establecidas por la Universidad Católica de Cuenca.

Particular que pongo en su conocimiento para los fines legales consiguientes. Sin otro particular me suscribo de Usted.

Atentamente,

Ing. Marcos Orellana Parra.PhD
TUTOR

AGRADECIMIENTO

Quiero, en primer lugar, agradecer a Dios Padre. De igual forma, a la Universidad Católica de Cuenca por todos los conocimientos que me ha permitido obtener durante todo este tiempo de preparación. Además, extiendo mi agradecimiento a todos los docentes de la carrera de Tecnologías de la Información por el esfuerzo y la dedicación brindados; sus acciones me han permitido llegar a este punto. Con su experiencia, forjaron e inculcaron, más allá del conocimiento, principios y valores para mi desarrollo personal y profesional. Finalmente, un eterno agradecimiento a mis compañeros de clase: ustedes hicieron de esta etapa una de las mejores; no habría sido igual sin ustedes. Siempre estuvieron ahí para brindar una mano de ayuda o apoyo, y por todo eso siempre estaré agradecido.

DEDICATORIA

A Dios, porque sin su disposición y gracia, esto no sería posible, A mis padres, tíos y abuelos. En especial, a mi madre, quien, a pesar de cualquier circunstancia, jamás dejó de apoyarme ni creer en mí. Le dedico por completo este logro. Aunque existieron dificultades y caídas, ella siempre estuvo ahí para que yo, hoy, pueda alcanzar este sueño que durante cuatro años hemos perseguido.

Resumen

Este trabajo se centra principalmente en el diseño y prueba de un prototipo automatizado para el control de acceso basado en reconocimiento facial, con el propósito de implementarlo en el aula STEAM de la Universidad Católica de Cuenca, extensión San Pablo de La Troncal, como alternativa al registro manual aún vigente para asi lograr automatizar los procesos que actualmente se llevan a cabo. Los métodos tradicionales resultan poco prácticos, pues el control manual suele ser lento, inseguro y propenso a errores. Ante esta situación se plantea un sistema automático que aprovecha los avances de la automatización para brindar rapidez, seguridad y un registro más confiable. La propuesta busca superar las limitaciones de los registros de papel o digitales básicos, que con frecuencia fallan o carecen de eficiencia. Así se presenta un prototipo funcional que integra inteligencia artificial e IoT para mejorar la gestión de accesos en entornos académicos, ofreciendo además una interfaz intuitiva y adaptable a futuros requerimientos institucionales.

Palabras clave: Identificación biométrica facial, Internet de las Cosas (IoT), Control de acceso automatizado.

Abstract

This study focuses primarily on the design and testing of an automated prototype for access control based on facial recognition technology, intended for implementation in the STEAM classroom at the Catholic University of Cuenca, on San Pablo de La Troncal campus. The system is proposed as an alternative to the current manual registration process, which aims to automate ongoing administrative processes. Traditional methods have proven impractical, as manual control tends to be slow, insecure, and prone to human error. In response, an automated system that influences technological advances in automation is proposed to provide greater speed, security, and reliability in data recording. The proposal aims to overcome the limitations of paper-based or basic digital records, which often lacks accuracy and efficiency. Consequently, a functional prototype that integrates Artificial Intelligence and the Internet of Things (IoT) is presented to enhance access management in academic environments, while also offering an intuitive interface adaptable to future institutional requirements.

Keywords: Facial biometric identification, Internet of Things (IoT), automated access control.

INDICE

DEDICATORIA II
AGRADECIMIENTO I
INDICE III
INDICE DE FIGURAS IV
INDICE DE TABLAS IV
RESUMEN .....
ABSTRACT .....
INTRODUCCION 1
CAPÍTULO 1 2
MARCO REFERENCIAL 2
1.1. Planteamiento del Problema 2
1.2. Formulación del Problema 3
1.3. Antecedentes de la Investigación 3
1.4. Justificación de la Investigación 4
1.5. Objetivos Objetivo General: 5
1.7. Limitaciones 5
1.8. Delimitaciones 5
CAPITULO 2 7
MARCO TEÓRICO 7
2.1. Reconocimiento Facial 7
2.2. Inteligencia Artificial aplicada al Reconocimiento Facial 8
2.2.1. Deep Learning **8**
2.2.2. Redes Neuronales Convolucionales **9**
2.2.3. Modelos de Referencia **10**
2.2.3.1. FaceNet (Google, 2015) 10
2.2.3.2. DeepFace (Facebook, 2014) 10
2.2.3.3. VGGFace / VGGFace2 (Oxford, 2015 y 2017) 10
2.3. Sistemas Embebidos y Microcontroladores en Control de Acceso 11
2.3.1. Sistemas Embebidos **11**
2.3.1.1. ***Características principales*** 11
2.3.2. Microcontroladores y Actuadores **12**
2.3.2.1. Arduino MEGA 13
2.3.2.2. ESP32 14

2.3.2.3. Relé 14
2.3.2.4. Cerradura Electromagnética 14
2.4. Flujo de integración 15
2.5. Control de Acceso con Reconocimiento Facial 15
2.5.1. Descripción del acceso **16**
2.5.2. Beneficios **16**
2.5.3. Estudios relacionados **17**
2.5.3.1. México 17
2.5.3.2. Brasil 18
2.5.3.3. Colombia 18
2.6. Computación en la Nube e Internet de las Cosas (IoT) 19
2.6.1. Plataformas **19**
2.7. Antecedentes Institucionales 22
CAPÍTULO III 23
MARCO METODOLÓGICO 23
3.1. Enfoque de la Investigación 23
3.2. Nivel de la Investigación 24
3.3. Población y Muestra 24
3.4. Métodos de Investigación 25
3.5. Técnicas e Instrumentos de Recolección de Información 25
3.6. Tratamiento de la Información 26
3.7. Metodología para la apertura de la puerta mediante control IoT 26
CAPÍTULO IV 28
RESULTADOS Y ANÁLISIS 28
4.1. Introducción 28
4.2. Arquitectura general del sistema 28
4.2.1. Nivel Físico **29**
4.2.2. Nivel Lógico **29**
4.3. Alcances del prototipo 29
4.4. Diagrama de arquitectura física y lógica 30
4.5. Circuito Arduino 33
4.6. Descripción de módulos de software 34
4.6.1 Captura de rostros **34**
4.6.2 Entrenamiento del modelo **36**
4.6.3 Reconocimiento facial **37**
4.6.4. Conexión a la base de datos **38**

4.6.5. Interfaz de usuario y login **38**
4.7. Flujo operativo 39
4.8. Procedimiento de pruebas 40
4.8.1. Pruebas Funcionales **40**
4.8.2. Pruebas no funcionales **40**
4.9. Resultados obtenidos 40
4.10. Interpretación de resultados 42
4.11. Comparación con estudios previos 42
4.12. Fortalezas, debilidades y oportunidades 42
4.13. Impacto académico y técnico 43
4.14. Implementación física del circuito Arduino y pruebas de activación 44
4.14.2. Diagrama eléctrico **44**
4.14.3. Comunicación Arduino-Python **45**
4.14.4. Montaje físico **46**
4.14.5. Resultados de pruebas de activación **47**
CAPÍTULO V 48
CONCLUSIONES Y RECOMENDACIONES 48
5.1. Conclusiones 48
5.2. Recomendaciones 49
Bibliografía 50
ANEXOS ..... **¡Error! Marcador no definido.**
Anexo A: ..... ¡Error! Marcador no definido.
Firmware Arduino – Control de cerradura por puerto serial (Arduino Mega 2560) .... **¡Error! Marcador no definido.**
Anexo B. ..... ¡Error! Marcador no definido.
Script Python – Prueba de activación de cerradura (comunicación serial). **¡Error! Marcador no definido.**
Anexo C. ..... ¡Error! Marcador no definido.
Módulo Python – Conexión a base de datos SQL Server (pyodbc) ..... **¡Error! Marcador no definido.**
Anexo D. ..... ¡Error! Marcador no definido.
Script Python – Entrenamiento del modelo LBPH (trainer.py) ..... **¡Error! Marcador no definido.**
Anexo E. ..... ¡Error! Marcador no definido.
Evidencia de funcionamiento del sistema de reconocimiento facial ..... **¡Error! Marcador no definido.**
REPORTE ÍNDICE DE SIMILITUD TURNITIN ..... ¡Error! Marcador no definido.

INDICE DE FIGURAS

Figura. 1. Diagrama de conexión Física 31
Figura. 2. Diagrama de Conexión Lógica.....32
Figura. 3. Esquema circuital.....33
Figura. 4. Panel - menú principal 35
Figura. 5. Interfaz: Selección tipo de usuario para registro 35
Figura. 6. Interfaz: Registro usuario - estudiante.....36
Figura. 7. Interfaz: Registro usuario - docente 36
Figura. 8. Entrenamiento del modelo en la consola CMD/ PowerShell.....37
Figura. 9.Reconocimiento facial.....38
Figura. 10. Interfaz: Sistema de control de acceso facial.....39
Figura. 11. Interfaz: Menú principal.....39
Figura. 12. Precisión de reconocimiento facial por escenario.....41
Figura. 13. Montaje físico: PC - Arduino - relé - cerradura.....46
Figura. 14. Placa Arduino - pines de conexión.....46

INDICE DE TABLAS

Tabla 1. Tabulación de resultados 41
Tabla 2. Resultados - pruebas de activación.....47

INTRODUCCION

En el ámbito universitario, la seguridad y el control de accesos constituyen una necesidad cotidiana. En muchos espacios aún se utilizan registros en papel que pueden perderse, falsificarse o presentar errores, lo que resta validez al control realizado. Esta situación también se evidencia en laboratorios, donde se requiere un mayor nivel de fiabilidad.

En el aula STEAM de la Universidad Católica de Cuenca, extensión La Troncal, se vive esta realidad, lo que motivó la elaboración de este trabajo de titulación: implementar un sistema de reconocimiento facial que sustituya los mecanismos manuales.

La propuesta consiste en registrar en tiempo real el ingreso de estudiantes y docentes, sin depender de la supervisión manual. Para ello, se integran cámaras, algoritmos de inteligencia artificial y microcontroladores IoT.

El sistema detecta un rostro, lo compara y, si existe coincidencia, autoriza la apertura de la puerta y almacena la información de acceso. Con ello, no solo se fortalece la seguridad, sino que también se genera un registro confiable y disponible para posteriores consultas administrativas.

El documento se estructura en capítulos que abordan el planteamiento del problema, el marco teórico de los fundamentos tecnológicos, el desarrollo y prueba del prototipo, y finalmente, las conclusiones y recomendaciones orientadas a mejorar e implementar la solución en otros espacios.

CAPÍTULO 1

MARCO REFERENCIAL

1.1. Planteamiento del Problema

Los avances tecnológicos han transformado de manera significativa los sistemas de gestión en el ámbito educativo, sobre todo en lo referente a la seguridad, el control de accesos y la administración de recursos digitales. En naciones como México y Colombia ya se han implementado con éxito soluciones modernas, como el reconocimiento facial, para llevar un registro confiable de asistencia y regular el ingreso a las aulas. No obstante, en ciudades de Ecuador, como La Troncal, estas herramientas recién se encuentran en fase de adopción.

En el caso de la Universidad Católica de Cuenca, extensión La Troncal, esto representa un reto considerable: pese a disponer de laboratorios equipados, el ingreso aún depende de métodos tradicionales, como listas digitales o la supervisión manual. Dicho esquema resulta vulnerable, pues puede presentar errores, extravíos de datos, manipulación indebida y limitaciones para vigilar con exactitud el flujo de estudiantes.

Este modelo genera retrasos, desorden y baja eficiencia administrativa. Por ello, se vuelve urgente la adopción de un sistema automatizado que permita un acceso rápido, exacto y seguro al aula STEAM. Una alternativa basada en reconocimiento facial, combinada con inteligencia artificial y dispositivos IoT, facilitaría la verificación biométrica de identidades, reforzaría la seguridad institucional, garantizaría un registro confiable de asistencia y, además, se alinearía con la transformación digital que actualmente demanda la educación superior.

1.2. Formulación del Problema

¿De qué manera un sistema automatizado de control de acceso mediante reconocimiento facial, basado en IoT e inteligencia artificial, nos ayudaría a mejorar y agilizar la seguridad, eficiencia administrativa y control de entrada y salida en el aula STEAM de la UCACUE, extensión La Troncal?

1.3. Antecedentes de la Investigación

Después de ciertos análisis se ha evidenciado que la adopción de tecnologías biométricas y aparatos IoT en entornos educativos incrementa la eficacia, la seguridad y la estructura. Por ejemplo, la investigación de Miranda-Orostegui et al. (2021) dio a conocer que se puede desarrollar un sistema de reconocimiento facial en Raspberry Pi, logrando resultados gratificantes tanto en precisión y tiempos de procesamiento. Mohammad y colaboradores (2024) emplearon FaceNet y MobileNetV2 en una arquitectura IoT para conseguir reconocimiento facial en tiempo real con una exactitud del 99.97%.

En Latinoamérica, las universidades de México y Colombia han conseguido instaurar estos sistemas para el registro automatizado de la asistencia, mejorando así el desempeño académico y la seguridad de la institución. Un gran ejemplo de esto es Cano y Ramírez (2024) en la UTP emplearon un ESP32-CAM para automatizar la entrada a laboratorios, logrando evidenciar que aparatos económicos son suficientes para aplicar soluciones de control de acceso.

Estos estudios nos muestran que las tecnologías de reconocimiento facial y sistemas embebidos son una solución eficaz, reproducible y apropiada para ambientes académicos, aunque todavía no se ha implementado en el campus La Troncal de la UCACUE. Por ende, este proyecto constituye una verdadera oportunidad para cubrir esa falta tecnológica a través de un prototipo funcional que se pueda ajustar a la realidad institucional.

1.4. Justificación de la Investigación

En la universidad todavía se usan métodos muy básicos para controlar la asistencia y el ingreso a los laboratorios. Esto genera problemas debido a la perdida de información, se cometen errores o simplemente no hay un control real de quién entra o sale. Por eso, la idea de instalar un sistema de acceso automático con reconocimiento facial en el aula STEAM no es un lujo, sino una necesidad. Este tipo de solución hace más seguro el ingreso y también permite que la asistencia quede registrada de forma precisa y que se puedan consultar reportes en cualquier momento.

Lo interesante es que hoy en día ya existen tecnologías accesibles que permiten aplicar algo así sin que los costos sean demasiado altos. Un ejemplo es el uso de modelos de aprendizaje profundo como FaceNet, que ayudan a reconocer rostros de manera eficiente. Si a esto se suma una metodología ágil para el desarrollo, el proceso resulta más ordenado, flexible y enfocado en conseguir resultados que realmente sirvan.

Este proyecto se convierte, además, en una propuesta escalable, ya que el modelo puede replicarse en otras aulas o sedes de la universidad. La investigación también permite generar un prototipo base que otras instituciones educativas del país puedan adaptar, fomentando la innovación en el sector educativo ecuatoriano.

1.5. Objetivos Objetivo General:

Establecer un modelo inicial de un sistema de control de acceso que administre el ingreso al aula STEAM de la UCACUE, extensión La Troncal, mediante reconocimiento facial, empleando tecnologías como inteligencia artificial, cámaras digitales y microcontroladores IoT.

1.6. Objetivos Específicos:

1. Diseñar la arquitectura del sistema de control de acceso, seleccionando los componentes tecnológicos adecuados que se ajusten a las necesidades del aula STEAM.
2. Programar e integrar el prototipo utilizando técnicas de inteligencia artificial, enfocadas en el reconocimiento facial.
3. Analizar la funcionalidad del prototipo dentro del entorno del aula STEAM, evaluando su contribución en la mejora de seguridad y control institucional.

1.7. Limitaciones

Esta investigación se enfoca exclusivamente en el diseño y desarrollo de un prototipo funcional en un entorno de pruebas. No contempla el despliegue final del sistema en operación institucional real ni pruebas masivas con usuarios. El análisis de impacto, escalabilidad institucional, integración con sistemas existentes o mantenimiento a largo plazo no forman parte del presente estudio. Asimismo, la prueba del sistema se realizará con datos simulados, respetando las normativas de privacidad de datos biométricos vigentes en el Ecuador.

1.8. Delimitaciones

La investigación está limitada geográficamente a la extensión La Troncal de la Universidad Católica de Cuenca y específicamente al aula STEAM. Tecnológicamente, se trabajará con el entorno NetBeans y lenguaje Java, integrando bibliotecas como OpenCV para el tratamiento de imágenes faciales. La implementación incluirá hardware como, sensores y una cerradura electromecánica. Los formularios y procesos de

referencia estarán basados en estándares institucionales y académicos nacionales. Esta propuesta está diseñada para ser replicable en otros entornos académicos que compartan necesidades similares.

CAPITULO 2

MARCO TEÓRICO

2.1. Reconocimiento Facial

Es una técnica biométrica que ayuda con el reconocimiento o confirmación de la identidad de una persona mediante el estudio automatizado de las características de sus rasgos faciales. Se emplean algoritmos de inteligencia artificial para reconocer, representar y contrastar modelos faciales en fotografías o grabaciones, con información guardada en una base de datos [1]. Actualmente, este método ha adquirido popularidad en diversas áreas de seguridad, además de la comodidad diaria. Por ejemplo, varios modelos de smartphones emplean biometría facial, Apple Face ID, mediante el cual con un simple gesto de vista es posible acceder al dispositivo [2]. Así mismo es común encontrar sistemas de reconocimiento facial en aeropuertos, implementados para acelerar los controles de seguridad, una escalada vertiginosa de su aplicabilidad surgió con la emergencia mundial sanitaria COVID-19, en donde se procuró en muchas instalaciones la detección del empleo correcto de mascarillas. De aquí, se infiere en términos generales, que actualmente el reconocimiento facial se incluye en diversos sistemas de seguridad ciudadana.

Etapas del proceso: El sistema de reconocimiento facial opera típicamente en varias fases. Primero se captura la imagen de la cara mediante una cámara. Luego se detecta la presencia de un rostro en la imagen y se alinean y normalizan los rasgos (p. ej. rotación, escala, ajuste de iluminación). A continuación, se realiza la extracción de características faciales: un modelo entrenado (por ejemplo, una red neuronal convolucional) convierte la imagen del rostro en un vector de características. Finalmente, el sistema compara este vector con los almacenados en la base de datos. Si existe una coincidencia por debajo de un umbral de tolerancia, la identidad se considera verificada y se autoriza el acceso [3].

Como resumen: “si las dos series de datos coinciden, se autentica la identidad y se concede el acceso” [4]. En caso contrario, se deniega el ingreso. Este flujo (captura → detección → extracción → comparación → decisión) es la base de cualquier sistema de reconocimiento facial.

Biometría Facial: Básicamente, el sistema analiza los rasgos únicos de cada rostro (como si fuera una huella digital, pero de la cara). En el planeta, todos los seres humanos tienen diferencias únicas (rasgos), aunque no se noten a simple vista [5]. En el reconocimiento facial, se extraen estos rasgos faciales y se codifican en vectores de características a través de algoritmos de aprendizaje profundo. Estos vectores sirven como “huellas digitales” del rostro y son comparados con plantillas previamente almacenadas en una base de datos.

2.2. Inteligencia Artificial aplicada al Reconocimiento Facial

2.2.1. Deep Learning

El Deep Learning es una rama del aprendizaje automático, el cual facilita a las computadoras procesar y representar grandes volúmenes de datos mediante múltiples capas de procesamiento. Se emplean redes neuronales profundas para encontrar características complejas en grandes cantidades de datos. [6]. Se han modificado campos como la identificación de voz, la visión computacional, el procesamiento de texto y la bioinformática. Actualmente se encuentran estructuras especializadas como redes convolucionales para fotografías y redes recurrentes para información secuencial. [6]. De acuerdo con Holdsworth y Scapicchio de IBM, el Deep Learning intenta imitar el poder de decisión del cerebro humano a través de redes neuronales multicapa, al realizar esto se facilita de gran manera las tareas complejas como el reconocimiento de imágenes. [6] El aprendizaje profundo adquiere jerarquías de conceptos sin la intervención directa de humanos. Resulta beneficioso tanto en la investigación como en el sector industrial. Se

fundamenta en principios matemáticos tales como el álgebra lineal, la teoría probabilística y la computación numérica. Se utiliza en sistemas de sugerencias, videojuegos, química, robótica, economía, entre otras áreas.

2.2.2. Redes Neuronales Convolucionales

El mecanismo fundamental de aprendizaje de las redes neuronales convolucionales se inspira en la estructura del cerebro humano. Son capaces de procesar información estructurada, como imágenes y señales biomédicas, y extraer automáticamente características relevantes. Para diagnosticar la enfermedad de Alzheimer, la resonancia magnética (RM) puede identificar patrones con gran precisión. El electroencefalograma (EEG) también es eficaz para clasificar señales y distinguir la actividad cerebral del ruido, con una precisión del 98%. Su estructura les permite reconocer información compleja con múltiples capas de no linealidad. Son herramientas muy prometedoras en el ámbito médico, permitiendo optimizar el diagnóstico precoz. Además, han revolucionado la radiología al reconocer imágenes médicas con alta fiabilidad. Las redes neuronales convolucionales pueden entrenarse con datos reales para resolver problemas clínicos específicos. Son tecnologías clave para el análisis médico automatizado. [7] . En específico, cada capa convolucional aprende a identificar patrones visuales de creciente complejidad: las primeras capas corresponden a características elementales (bordes, texturas, brillo), mientras que las capas intermedias/altas fusionan dichas características para reconocer contornos u objetos complejos. [7] Como indica MathWorks, una CNN puede contar con decenas o cientos de capas, y cada capa "aprende a identificar distintas propiedades de una imagen" mediante la aplicación de varios filtros convolucionales. [7] Este mecanismo escalonado permite a la CNN construir de forma jerárquica una descripción detallada del rostro. En resumen, las CNN son muy eficaces para detectar

patrones faciales en imágenes y clasificarlos, lo que las hace indispensables para sistemas modernos de reconocimiento de rostros. [7]

2.2.3. Modelos de Referencia

En la práctica, varias redes convolucionales preentrenadas y adaptadas se han vuelto referencia en reconocimiento facial. Entre ellas destacan:

2.2.3.1. FaceNet (Google, 2015)

Presenta un modelo de red profunda que traza caras en un espacio euclidiano, en el que las distancias representan similitud. FaceNet logró una precisión del 99.63% en el benchmark denominado Labeled Faces in the Wild (LFW). [8], estableciendo un nuevo récord.

2.2.3.2. DeepFace (Facebook, 2014)

Desarrollado por Facebook, usa una red de nueve capas y entrenó con 4 millones de imágenes de usuarios. DeepFace obtuvo alrededor de **97.35%** de precisión en LFW (Labeled Faces in the Wild), casi igualando el desempeño humano. [8]

2.2.3.3. VGGFace / VGGFace2 (Oxford, 2015 y 2017)

Conocidos modelos entrenados por el Visual Geometry Group de Oxford. El VGGFace original (2015) usó la arquitectura VGG-16 con ~2.6 millones de imágenes de 2622 personas, mientras que VGGFace2 (2017) entrenó con 3.3 millones de imágenes de 9131 identidades. [9] . Estas redes profundas han servido de base para múltiples aplicaciones de reconocimiento facial de última generación.

Estos ejemplos ilustran cómo las CNN (Convolutional Neural Network) profundas pueden distinguir rostros con alta exactitud. Modelos como FaceNet y DeepFace demuestran la potencia del aprendizaje profundo: por ejemplo, FaceNet supera a DeepFace en los mismos conjuntos de datos (99.63% vs 97.35% en LFW). [8] En conjunto, estas arquitecturas marcan el estado del arte en reconocimiento facial mediante Inteligencia Artificial (IA).

2.3. Sistemas Embebidos y Microcontroladores en Control de Acceso

2.3.1. Sistemas Embebidos

Los sistemas embebidos son soluciones informáticas creadas para cumplir tareas muy específicas en equipos que no tienen muchos recursos disponibles. Combinan tanto hardware como software diseñado a medida y, en muchos casos, trabajan en tiempo real para responder de manera rápida. En los ejemplos mencionados, se observa cómo la inteligencia artificial también se aplica en contextos con límites de potencia, memoria o velocidad, usando modelos de aprendizaje automático que se entrenan en plataformas como Google Colab y luego se ejecutan en microcontroladores o dispositivos de bajo consumo. En la actualidad se encuentran en todas partes: desde un electrodoméstico inteligente en casa hasta un sensor dentro de la industria.

*2.3.1.1. **Características principales***

- Suelen funcionar con bajo consumo energético**,** porque están pensados para durar y ser eficientes.
- Requieren procesamiento rápido y eficaz**,** ya que cumplen tareas críticas en poco tiempo.
- Mantienen un tamaño pequeño y portabilidad, lo que los hace fáciles de integrar en distintos equipos.

- Están diseñados con una funcionalidad concreta, es decir, no sirven para todo, sino para la tarea puntual para la que fueron creados. [10]

2.3.1.2. Plataformas comunes

Existen múltiples plataformas populares para el desarrollo embebido. Entre ellas destacan:

Raspberry Pi: Económica y versátil para proyectos básicos.

NVIDIA Jetson (Nano/Xavier): Potente para aplicaciones de IA gracias a su GPU integrada.

ESP32 con cámara: Opción sencilla para tareas de visión artificial simples. [11]

Estas plataformas permiten implementar sistemas de reconocimiento facial de bajo costo: por ejemplo, una Raspberry Pi con cámara y OpenCV se puede usar para control de acceso, mientras que módulos como ESP32-CAM ofrecen cámaras integradas y conectividad Wi-Fi para aplicaciones móviles.

Los sistemas embebidos brindan el soporte físico necesario (procesadores, sensores, módulos de comunicación) para desplegar soluciones de reconocimiento facial en entornos reales y con recursos limitados.

2.3.2. Microcontroladores y Actuadores

En los sistemas de reconocimiento facial aplicados al control de acceso deben considerarse ciertos puntos importantes: no limitarse solo al software, sino considerar componentes electrónicos que permiten la interacción física y la vinculación con el entorno, es decir no solo hablar de un sentido práctico sino que también traducir a una acción tangible, como la acción de abrir la cerradura electromagnética que para ello se

utilizan microcontroladores que reciben una señal lógica desde el software y de inmediato activan otros elementos eléctricos de mayor potencia.

Los microcontroladores constituyen el núcleo de numerosos sistemas embebidos, ya que permiten ejecutar instrucciones elementales y controlar de manera directa distintos dispositivos periféricos. En el ámbito del control de accesos, cumplen el papel de enlace entre la parte lógica del proceso —implementada en programas desarrollados en Python con la librería OpenCV— y los dispositivos encargados de la acción física, como el módulo de relé y la cerradura electromagnética. Gracias a su bajo costo, a la facilidad con la que pueden ser programados y a la amplia disponibilidad de documentación técnica, se han consolidado como la opción más utilizada tanto en entornos académicos como en el desarrollo de prototipos funcionales.

Entre los microcontroladores y actuadores más utilizados destacan:

2.3.2.1. Arduino MEGA

El Arduino MEGA trabaja con el microcontrolador ATmega328P y es una de las placas más comunes en proyectos de aprendizaje. Tiene 14 pines digitales (seis pueden usarse con PWM - Modulación por Ancho de Pulso) y además seis entradas analógicas. Su velocidad es de 16 MHz, cuenta con 2 KB de memoria SRAM y 32 KB de memoria flash. También incluye un puerto USB que sirve para programar y para la comunicación serial. Este dispositivo es fácil de usar, cuenta con una amplia gama de material de apoyo y una comunidad grande que lo respalda, razones que lo convierten en el preferido dentro de la elaboración de proyectos educativos.

2.3.2.2. ESP32

Es un dispositivo moderno y potente con un procesador de dos núcleos que puede llegar a 240 MHz, dispone de conexión Wi-Fi y Bluetooth integrada, y tiene muchos pines GPIO (Entradas/Salidas de Propósito General) que permiten trabajar con entradas y salidas digitales y analógicas, e incluso funciones como ADC (Convertidor Analógico a Digital), DAC (Convertidor Digital a Analógico) y PWM (Modulación por Ancho de Pulso). Su memoria RAM es de hasta 520 KB. A diferencia del Arduino MEGA, se puede conectarse directamente a internet, lo que permite trabajar con aplicaciones IoT. La cerradura puede abrirse no solo por comunicación serial, sino también usando protocolos como MQTT o HTTP.

2.3.2.3. Relé

El relé es un dispositivo que funciona como interruptor eléctrico. Su papel es separar la señal de bajo voltaje del microcontrolador (5 V en Arduino o 3.3 V en ESP32) de la corriente más fuerte que necesite otro elemento eléctrico para este caso de estudio la cerradura. Tiene una bobina que al activarse conmuta el contacto y deja pasar la energía proporcionada por una fuente externa de niveles superiores al de activación del interruptor. Existen varios tipos, algunos de un canal, otros de varios, y también los de estado sólido que tienen un tiempo de vida mayor. Para este proyecto se usa un relé de un canal con optoacoplador, que protege al microcontrolador al aislarlo de la parte de potencia.

2.3.2.4. Cerradura Electromagnética

La cerradura electromagnética es el actuador que finalmente abre o bloquea la puerta, funciona con un electroimán que normalmente trabaja con 12 V de corriente continua y consume entre 300 mA y 1 A, por lo que necesita una fuente de alimentación independiente esto, debido a que el microcontrolador no proporciona esos niveles de energía. Estas cerraduras son muy usadas en sistemas de seguridad por su confiabilidad, sin embargo, debido a su dependencia de la electricidad es aconsejable emplear sistemas de respaldo de energía con baterías o UPS.

2.4. Flujo de integración

La integración Arduino–relé–cerradura es sencilla: primero, el software en Python reconoce el rostro del usuario, luego envía la señal por el puerto serial, el microcontrolador recibe la orden y activa el relé; este permite el paso de corriente a la cerradura, liberando la puerta.

De esta forma, el reconocimiento facial no se queda solo en la computadora, sino que realmente acciona el sistema físico y controla el acceso.

2.5. Control de Acceso con Reconocimiento Facial

El control de acceso en seguridad se refiere a los mecanismos que determinan quién puede ingresar o usar recursos protegidos. En términos generales, el control de acceso “es una técnica de autorización de seguridad que determina los recursos específicos que un usuario o un sistema puede visualizar o utilizar”, y su objetivo básico es proteger la información o las áreas confidenciales contra el acceso no autorizado. [12]

Esto incluye también confirmar la identidad de las personas que intentan realizar el ingreso a un lugar ya sea de manera física o digital.

2.5.1. Descripción del acceso

En la práctica, el control de acceso facial funciona así: la cámara capta el rostro del usuario en la entrada. El algoritmo identifica el rostro en la imagen, extrae su vector de características con la red previamente entrenada y lo compara con la base de datos de empleados/autorizados. Si la comparación arroja una coincidencia aceptable (la distancia entre vectores es baja), se autentica la identidad y se permite el paso. [3] En caso contrario, se bloquea el acceso y se genera una alarma. Este esquema permite que el acceso sea transparente para el usuario (solo mirar al sensor) y, al mismo tiempo, proporciona una capa adicional de seguridad basada en la biometría.

2.5.2. Beneficios

Al poner en práctica el reconocimiento facial al control de acceso se obtiene un gran número de ventajas:

- **Acceso sin contacto:** De distinta manera como lo son la identificación física, tarjetas, llaves o huellas dactilares, la autenticación facial es completamente sin contacto. El usuario solamente se centra únicamente en la cámara, evitando así cualquier contacto. Esto es especialmente importante durante una situación sanitaria (por ejemplo, una pandemia), ya que ayuda a prevenir la propagación de enfermedades. [13] La adopción de sistemas sin contacto (como reconocimiento facial) ha aumentado en empresas preocupadas por higiene en el ingreso. [13]

- **Prevención de fraudes:** El reconocimiento facial puede dificultar la suplantación de identidad. Al autenticar biométricamente la cara, se evitan situaciones como llaves copiadas o tarjetas prestadas. Por ejemplo, los sistemas modernos integran cámaras de alta definición con software de reconocimiento que pueden alertar a los administradores si detectan a una persona en lista de vigilancia (como un presunto intruso) en las entradas. [13] De hecho, como señalan expertos, uno de los mayores beneficios es la prevención de fraudes y robos internos en empresas, ya que se comprueba la identidad real a distancia. [13]
- **Integración con vigilancia:** Un sistema de control de acceso con reconocimiento facial puede vincularse a un sistema de videovigilancia. De este modo, cuando un rostro coincide con una alerta (por ejemplo, una persona autorizada o un sospechoso), el sistema registra el evento y permite un monitoreo en tiempo real de la situación. [13] Esta integración apoya la protección de infraestructuras críticas y ofrece información en directo para toma de decisiones de seguridad. [13]
- **Rapidez y registro automatizado:** Al eliminar pasos manuales (entregar tarjeta, uso de PIN), la autenticación facial agiliza el flujo de personas. Estudios indican que los sistemas automáticos de acceso mejoran la eficiencia de los procesos de entrada y salida, ahorrando tiempo y trabajo manual. [14] Asimismo, el sistema genera un registro automático de quién y cuándo ingresó, facilitando la auditoría y trazabilidad de accesos.

2.5.3. Estudios relacionados

2.5.3.1. México

Burruel *et al.* (2021, IPN México) implementaron un sistema de cerradura biométrica con FaceNet en hardware embebido. Su prototipo, basado en

Raspberry Pi, logró más del 99% de tasa de reconocimiento correcto. [15] Este trabajo demuestra que con recursos de bajo costo es posible obtener una precisión muy alta en reconocimiento facial para control de acceso.

2.5.3.2. Brasil

En Brasil se han desarrollado proyectos con enfoque en seguridad pública y transporte. Por ejemplo, la ciudad de Río de Janeiro ha equipado micros urbanos con cámaras de reconocimiento facial para verificar la idoneidad de los pasajeros subsidiados (adultos mayores, estudiantes). Según informes recientes, estos sistemas validan la identidad de los usuarios en ruta, evitando fraudes en los beneficios de transporte. Además, la empresa Cognitec y otras han colaborado con autoridades brasileñas en sistemas de identificación facial en aeropuertos y eventos masivos, destacando el interés en reforzar la seguridad ciudadana con IA.

2.5.3.3. Colombia

Diversos grupos en Colombia exploran reconocimiento facial en entornos universitarios e IoT. Por ejemplo, Miranda Orostegui *et al.* (2021, Colombia) desarrollaron un sistema embebido de reconocimiento facial usando FaceNet sobre una Raspberry Pi. Su prototipo (dirigido a control de acceso) alcanzó una precisión del 77.38% con un 81.25% de exactitud. Aunque menor al 99% de sistemas de mayor costo, este estudio evidencia que hardware económico (como Raspberry Pi) puede implementarse para tareas reales de autenticación. Paralelamente, proyectos con módulos ESP32-CAM en universidades colombianas (Bogotá, Medellín) han mostrado que es factible monitorizar la

asistencia de estudiantes mediante reconocimiento facial con consumo energético reducido, reforzando la aplicabilidad de este enfoque en el país.

Estos antecedentes demuestran que es factible implementar sistemas de control de acceso con hardware accesible y tecnologías de IA.

2.6. Computación en la Nube e Internet de las Cosas (IoT)

El Internet de las Cosas (IoT) permite conectar sistemas y dispositivos para trabajar de forma remota. En el ámbito de la seguridad, integra sistemas de control de acceso con servidores en la nube.

2.6.1. Plataformas

En la actualidad, el empleo de la computación en la nube se ha convertido en un hecho imprescindible, en vista de las limitaciones que presentan en modo local: almacenamiento, procesamiento y seguridad. Los servicios Cloud (nube) ofrecen a más de guardar información, herramientas que permiten escalar aplicaciones, integración con múltiples servicios, además de garantizar la alta disponibilidad.

2.6.1.1. iCloud (Apple)

Su empleabilidad está orientado principalmente al usuario final, ofrece sincronización automática de archivos, fotos y configuraciones entre dispositivos Apple. Su fortaleza radica en la facilidad de uso y la integración con el ecosistema iOS y macOS, aunque no está diseñado para proyectos de desarrollo de software complejos ni para despliegues empresariales de gran escala.

2.6.1.2. Amazon Web Services (AWS)

Es la plataforma más completa dentro de los proveedores de servicios en la nube, abarca almacenamiento (Amazon S3), bases de datos (RDS, DynamoDB), cómputo escalable

(EC2, Lambda), e integración con aplicaciones de inteligencia artificial e Internet de las Cosas (IoT Core, Greengrass). Su principal ventaja es la escalabilidad y variedad de soluciones, pero su curva de aprendizaje es elevada y los costos pueden incrementarse rápidamente si no se gestionan adecuadamente.

2.6.1.3. Google Cloud Platform (GCP)

Se diferencia por su modelo de pago por uso y por la integración nativa con herramientas de análisis de datos e inteligencia artificial, como BigQuery y TensorFlow. Ofrece servicios de almacenamiento (Cloud Storage), máquinas virtuales (Compute Engine) y soluciones de IoT (IoT Core). Su fortaleza está en la flexibilidad y facilidad para proyectos de análisis masivo de datos, aunque para pequeñas empresas pueden existir opciones más económicas.

2.6.1.4. Microsoft Azure

Combina almacenamiento en la nube (Blob Storage), servicios de bases de datos (SQL Database), máquinas virtuales y un robusto ecosistema de integración con aplicaciones empresariales de Microsoft, como Office 365 y Active Directory. Sus ventajas son la seguridad, redundancia y confiabilidad, aunque requiere mayor conocimiento técnico para su configuración y administración eficiente.

Estas plataformas aseguran que los sistemas de control de acceso basados en reconocimiento facial puedan escalar de manera flexible, almacenar datos de forma segura y comunicarse eficientemente con otros dispositivos mediante servicios IoT y APIs.

2.7. Marco legal y Ético

2.7.1. Marco Legal

El (IoT), debido a su constante crecimiento, requiere regulaciones claras y actualizadas para asegurar su uso seguro. Por una parte, entidades internacionales como la ISO han establecido normas que guían la arquitectura y la seguridad de estos sistemas. Por otra parte, en Europa, el Reglamento General de Protección de Datos (RGPD) y varias normativas tienen como objetivo salvaguardar la privacidad y regular los dispositivos interconectados. Adicionalmente, el Reino Unido estableció un código de prácticas óptimas que originó la norma ETSI EN 303 455.

En el Ecuador, la Ley Orgánica de Protección de Datos Personales regula la utilización de datos biométricos, considerándolos datos delicados, requiriendo el consentimiento explícito y medidas de seguridad sofisticadas (Dato Seguro, 2021). La Oficina del Defensor del Pueblo subraya la importancia de salvaguardar la privacidad al utilizar tecnologías como el reconocimiento facial y las huellas digitales, particularmente en entidades públicas. Pese a que la legislación constituye un progreso, todavía existen retos en su implementación y supervisión eficaz (Derecho Ecuador, 2021; Plan V, 2022). Además, medios como El Comercio alertan acerca de los peligros de supervisión a gran escala si estas tecnologías se emplean sin regulación.

2.7.2. Consideraciones Éticas

El uso del reconocimiento facial plantea también retos éticos y de privacidad. Numerosos autores advierten que estas tecnologías pueden vulnerar la intimidad de las personas y reproducir sesgos. Por ejemplo, la Asociación Médica Americana señala que el uso creciente de FRT genera interrogantes sobre la privacidad de los datos biométricos, la protección de la información personal y la posible discriminación algorítmica. [16] Estudios han documentado que los sistemas pueden ser menos precisos con rostros de grupos minoritarios o en condiciones no ideales, lo que eleva riesgos de falsos negativos

o positivos. La vigilancia masiva mediante cámaras también suscita debate social; por ello, los expertos insisten en establecer protocolos de consentimiento informado, políticas claras de uso y límites a la recolección de imágenes. En conclusión, el reconocimiento facial ofrece una variedad de ventajas técnicas, es fundamental abordar su implementación con controles legales y éticos para proteger los derechos de las personas. [16]

Con estas premisas, la propuesta de este trabajo de investigación busca estar enmarcado en la legalidad y la ética, principios fundamentales del quehacer universitario.

2.7. Antecedentes Institucionales

El aula STEAM de la Universidad Católica de Cuenca es un espacio particularmente diseñado para que los alumnos de Tecnologías de la Información puedan aplicar todo lo que aprenden en el salón de clases. No es un aula convencional, sino un lugar equipado con todo lo requerido, incluyendo de sensores, dispositivos electrónicos, eléctricos, así como herramientas para automatizar procesos, además de todo lo necesario para la elaboración de proyectos o investigaciones. En este sitio, la tecnología se emplea para resolver problemas reales y obtener conocimientos a través de la práctica. Además, se fomenta el trabajo en equipo y la creatividad, lo que mejora la formación y prepara de forma eficaz a los estudiantes ante los futuros retos laborales. Este entorno por sus condiciones y características propias se convierte en el espacio de aplicación del prototipo de control de acceso mediante reconocimiento facial, permitiendo integrar la teoría y la práctica para resolver necesidades reales de seguridad y propiciar la aplicación en nuevos espacios institucionales.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Enfoque de la Investigación

Este trabajo busca probar si el sistema de control de acceso con reconocimiento facial desarrollado para el aula STEAM de la UCACUE, en La Troncal, realmente funciona como debe. La idea es simple: verificar si cumple lo que se había planteado y medirlo de una forma clara, sin quedarse solo en la teoría.

Para ello se realizan pruebas con placas Arduino y ESP32-CAM, además de otros equipos de bajo costo que se consiguen con facilidad. Lo que se pretende comprobar son tres aspectos básicos: que el sistema reconozca de forma adecuada los rostros, que el tiempo de respuesta no sea excesivo y que en verdad sea confiable cuando permite o niega el acceso.

Este proyecto es aplicado porque responde a un problema que existe en la universidad: no se cuenta con un sistema moderno que registre asistencia y controle el ingreso. En esta fase no se utiliza todavía con estudiantes o profesores, sino en simulaciones que permiten observar cómo se comporta el prototipo.

La organización del trabajo se realiza de manera ordenada, se divide en partes pequeñas (sprints). En cada sprint se desarrolla algo específico: primero la captura del rostro, luego la validación biométrica, después la apertura de la puerta y al final el registro en la base de datos. De esa manera el sistema se ajusta poco a poco y se puede ver en cada paso si está cumpliendo lo esperado.

3.2. Nivel de la Investigación

En este trabajo, el nivel de la investigación es propositivo y aplicado. Es propositivo porque no solo se aborda el problema, sino que se propone algo concreto: diseñar e implementar un sistema de control de acceso automático con inteligencia artificial. En pocas palabras, el prototipo busca reemplazar la forma tradicional de controlar el ingreso al aula STEAM, para que sea más seguro, quede un registro claro de quién entra y sale, y además que todo el proceso sea más rápido y ordenado.

Es también aplicado porque no se limita a las ideas, sino que se construye una solución tecnológica real. En este contexto se integran reconocimiento facial, IoT **y** automatización, usando equipos económicos que cualquier institución podría adquirir.

El sistema se desarrolla en un ambiente controlado. No se prueba todavía con estudiantes o profesores directamente, pero se realizan pruebas con métricas como precisión, exactitud y rendimiento. Los resultados servirán como evidencia de que el prototipo funciona y de que en un futuro se puede implementar sin dificultad.

3.3. Población y Muestra

En este trabajo no se definió una población ni una muestra concreta, ya que no se aplican encuestas, entrevistas ni tampoco habrá interacción directa con estudiantes o docentes. El diseño y las pruebas del sistema se basan en la revisión de documentos, en los conocimientos que tiene el investigador y en simulaciones prácticas.

Para las pruebas de reconocimiento facial se emplean rostros de bases de datos de libre acceso. En cambio, las reglas de control, los flujos de ingreso y las medidas de seguridad se establecieron tomando en cuenta las normas de la institución y el objetivo principal del aula STEAM.

De este modo, la investigación se enmarca como un trabajo de tipo técnico y documental.

3.4. Métodos de Investigación

Se emplean dos métodos principales: experimental y analítico.

El método experimental se manifiesta en el diseño, implementación y validación del prototipo, manipulando variables como tipo de cámara, el modelo de red neuronal, el tipo de microcontrolador y la iluminación del entorno.

El método analítico permite descomponer el problema en sus componentes clave: ingreso al aula, validación facial, registro de datos y apertura de la cerradura. Cada uno de estos procesos se desglosa a partir de las funciones reales del aula STEAM, definiendo requisitos específicos como el tiempo máximo de validación, el tipo de respuesta del sistema y el almacenamiento de registros de acceso. El análisis documental también permitirá establecer las bases de seguridad, respeto a la privacidad de los datos y coherencia técnica con el entorno académico.

3.5. Técnicas e Instrumentos de Recolección de Información

No se aplicaron instrumentos de recolección de datos tradicionales. En su lugar se utilizaron:

- Análisis documental: revisión de trabajos similares implementados en universidades de México, Colombia y Brasil; además de proyectos en repositorios como IEEE, MDPI y Springer.
- Evaluación de artículos científicos y manuales técnicos sobre aprendizaje profundo y reconocimiento facial.
- Estudio comparativo de plataformas IoT como Raspberry Pi, ESP32-CAM y Arduino MEGA para determinar su adecuación al contexto del aula STEAM.

- Consulta de normativa nacional (Ley Orgánica de Protección de Datos Personales en Ecuador) para garantizar la no vulneración de derechos biométricos.

3.6. Tratamiento de la Información

Toda la información recopilada se organizó por categorías: técnica, funcional y normativa. Cada dato fue analizado con el fin de traducirlo en requisitos prácticos del sistema. Por ejemplo, la revisión de artículos permitió seleccionar modelos livianos de alta precisión, además de implementar procesos automatizados eficientes para ambientes académicos.

Durante el desarrollo, se generan iteraciones con funcionalidades clave: detección facial, entrenamiento del modelo, integración con base de datos, y apertura de cerradura. Cada sprint se evalúa con métricas de precisión (aciertos vs fallos), tiempo de respuesta (ms), y eficiencia (memoria consumida). Los resultados se documentan con evidencias (pantallazos, tablas de resultados, manuales).

Al finalizar, el sistema contará con documentación completa, código comentado, diagramas de flujo, arquitectura y evidencias visuales. Esta estructura asegura la escalabilidad del sistema y su posible implementación real en el aula STEAM.

3.7. Metodología para la apertura de la puerta mediante control IoT

Finalmente, se detalla la manera en que se ejecuta este proyecto de forma gradual, para que todo el procedimiento quede bien definido. En primer lugar, el concepto central consiste en crear un sistema que gestione la apertura de una puerta mediante tecnologías de IoT. En este sentido, se emplea una placa eléctrica que se activa de manera electrónica y un Arduino que actúa como el "cerebro" del sistema, acogiendo señales y gestionando el dispositivo.

Para reconocer al usuario, se dispone de una cámara que detecta su presencia, sin almacenar imágenes ni información personal, con el objetivo de salvaguardar la privacidad. Cuando un individuo se aproxima, el sistema transmite los datos a Arduino, que posteriormente consulta una base de datos MySQL, donde se encuentran inscritos los usuarios con autorización. La administración de la base de datos se realiza a través de Visual Studio Code, la herramienta que se utiliza para programar y gestionar los datos.

Si el individuo cuenta con la autorización, el Arduino activa la chapa eléctrica y abre automáticamente la puerta. Todo este proceso sucede en tiempo real, con comunicación segura entre el hardware y el software, para que sea rápido, eficiente y confiable. Además, el sistema está diseñado para ser escalable y adaptable, en caso de que en el futuro se desee agregar más funcionalidades o integrarlo con otros dispositivos IoT.

CAPÍTULO IV

RESULTADOS Y ANÁLISIS

4.1. Introducción

En este capítulo se presenta de forma ordenada y argumentada el conjunto de resultados alcanzados durante el desarrollo del sistema automatizado de control de acceso mediante reconocimiento facial del aula STEAM de la Universidad Católica de Cuenca, extensión La Troncal. La estructura que se sigue en este apartado permite, en primer lugar, describir de manera exhaustiva la arquitectura del prototipo final; en segundo lugar, analizar los módulos de software que lo integran; y finalmente, interpretar el rendimiento del sistema a partir de las pruebas realizadas en diferentes escenarios y puntos de vista.

Con el objetivo de lograr una exposición coherente y fácil de seguir, el contenido se ha dividido en apartados que explican desde la estructura general del sistema hasta las pruebas específicas realizadas, abarcando también el análisis comparativo con investigaciones previas y la valoración de las fortalezas, debilidades y oportunidades de mejora detectadas.

4.2. Arquitectura general del sistema

Se diseña una solución que combina hardware y software trabajando de forma integrada. El principio de funcionamiento es claro: el sistema reconoce a la persona por el rostro y decide si puede entrar o no a un espacio que está restringido.

El diseño se piensa por partes, como en módulos. Eso es útil porque si más adelante hay que cambiar algo, mejorar una parte o incluso ampliarlo, no hace falta tocar todo el sistema. Con eso el mantenimiento se vuelve más fácil y también se abre la posibilidad de usarlo en otros lugares parecidos, no solo en el aula STEAM.

4.2.1. Nivel Físico

En el nivel físico, el sistema se compone de:

- Cámara digital: encargada de capturar la imagen del usuario en tiempo real.
- Equipo de cómputo: responsable del procesamiento de la imagen y de la ejecución de los algoritmos de reconocimiento.
- Microcontrolador Arduino: dispositivo que recibe la señal de autorización y activa la cerradura electromagnética.
- Cerradura electromagnética: mecanismo físico que permite o deniega el acceso.

4.2.2. Nivel Lógico

En el nivel lógico, la solución integra:

- Python como lenguaje principal de desarrollo.
- OpenCV para la detección y procesamiento de imágenes.
- Algoritmo LBPH (Local Binary Patterns Histograms) para el reconocimiento facial.
- PyODBC para la conexión con SQL Server.
- Tkinter como herramienta para la creación de interfaces gráficas.
- Arquitectura IoT para la comunicación entre el software y el microcontrolador.

4.3. Alcances del prototipo

Con el fin de acotar expectativas y, al mismo tiempo, clarificar el trabajo, resulta pertinente explicitar tanto el alcance como los límites del prototipo. En primer lugar, el sistema se orienta a la autenticación uno-a-uno **y** uno-a-muchos en un entorno controlado

(aula STEAM), priorizando tiempos de respuesta por debajo del segundo y confiabilidad en condiciones habituales de iluminación. En segundo término, se privilegia la simplicidad operativa: registro de usuarios, entrenamiento periódico y reconocimiento en tiempo real con registro automático en base de datos. Por otra parte, quedan fuera del alcance la integración con directorios institucionales externos, la federación de identidades y los mecanismos avanzados de vivacidad basados en sensores adicionales. Finalmente, se deja delimitada la posibilidad de expansión, por ejemplo, hacia múltiples cámaras o integración con trabajos futuros, lo que, sin duda, permitirá consolidar la escalabilidad sin alterar la arquitectura fundamental presentada.

4.4. Diagrama de arquitectura física y lógica

Para reforzar la comprensión sistémica, se incorpora un diagrama que, por una parte, representa la **vista física** (Cámara → PC con Python/OpenCV → Arduino → Cerradura; PC ↔ SQL Server) y, por otra, explicita la **vista lógica** (Captura → Preprocesamiento → Predicción LBPH → Decisión por umbral → Señal a Arduino → Log en BD). De esta manera, se observa, en primer lugar, la secuencia completa de interacción entre hardware y software; en segundo lugar, el flujo de datos desde su adquisición hasta su persistencia; y, finalmente, los puntos de control donde se aplican políticas de seguridad y auditoría.

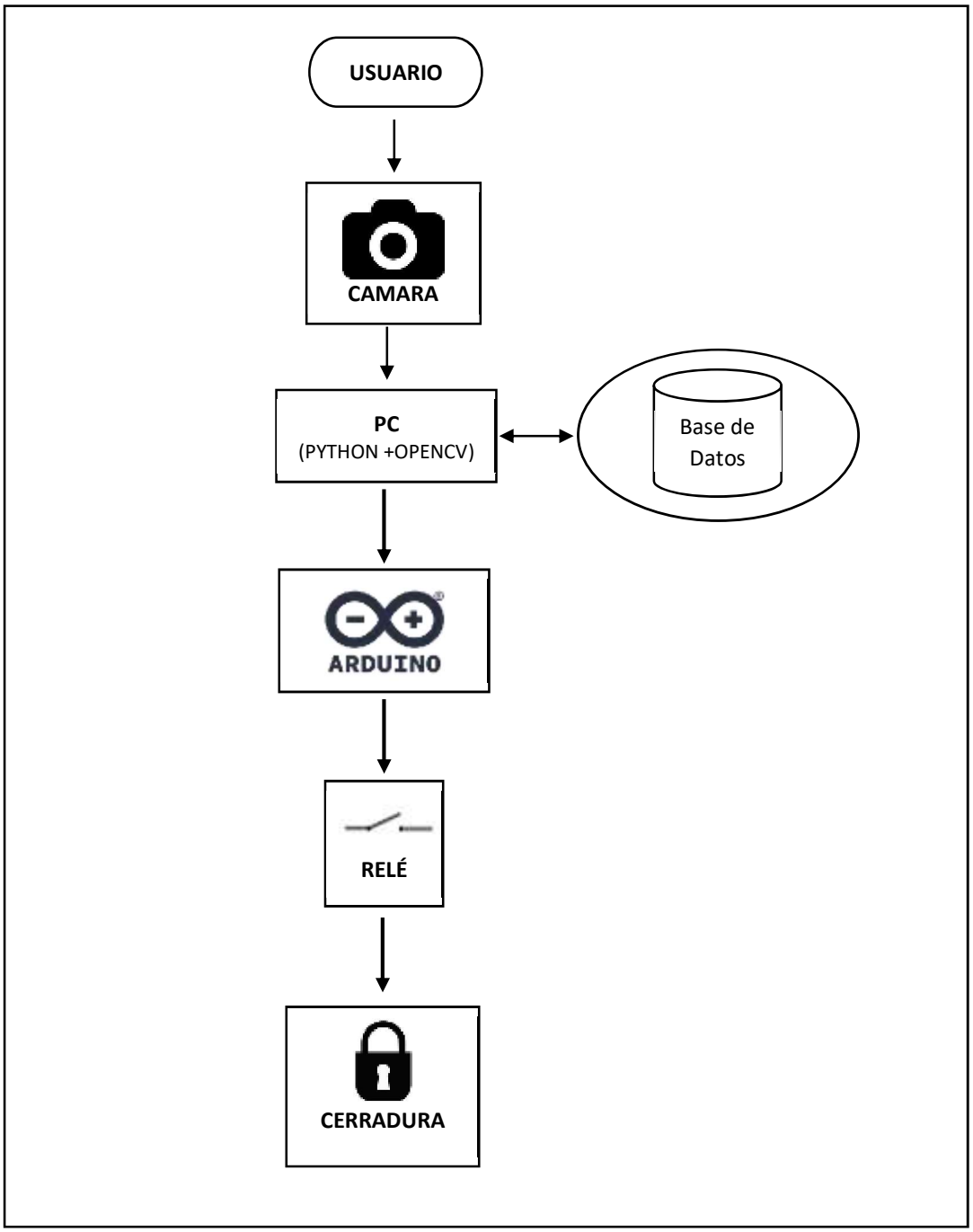


Figura. 1. Diagrama de conexión Física
Fuente: Elaborado por el autor

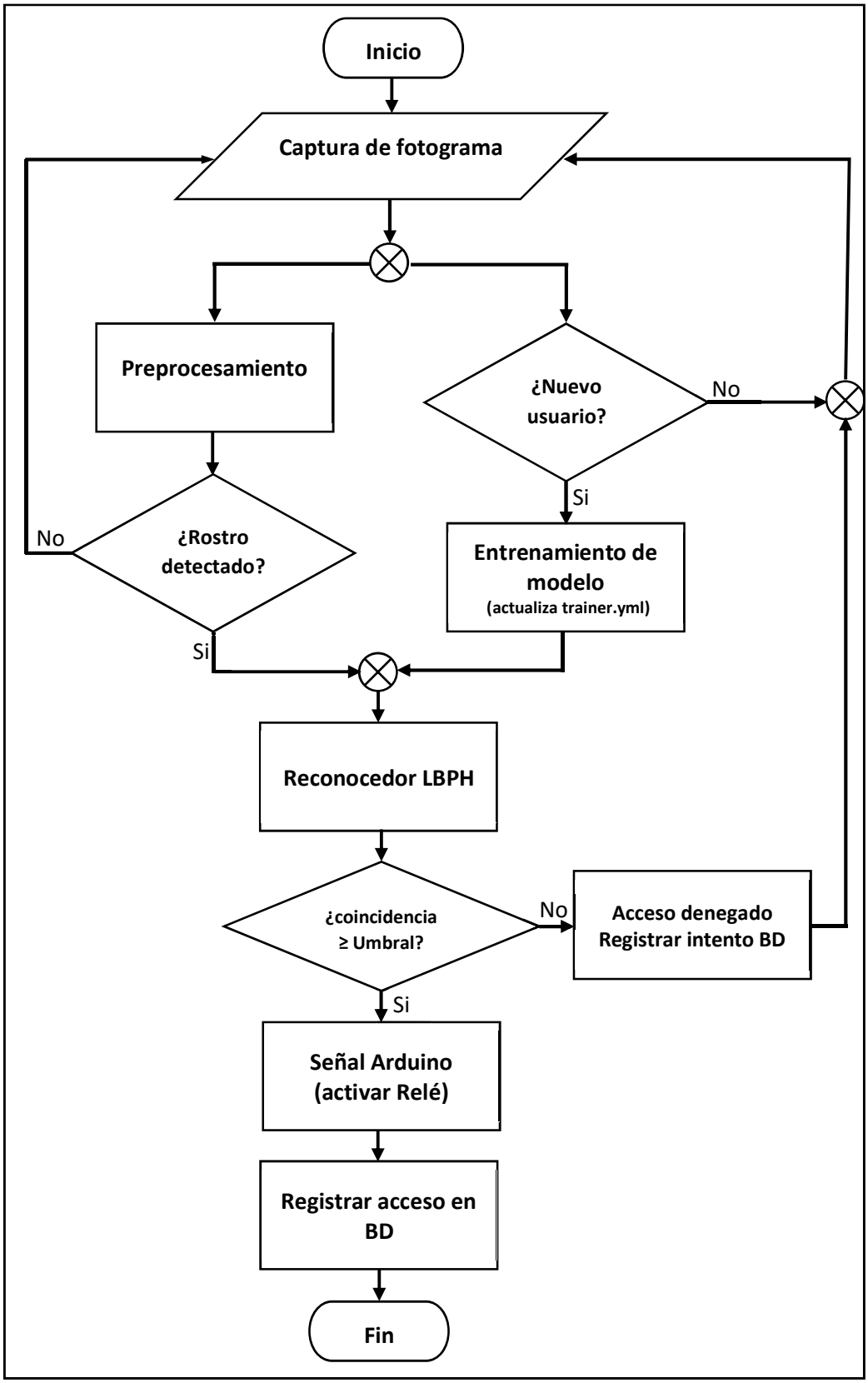


Figura. 2. Diagrama de Conexión Lógica
Fuente: Elaborado por el autor

4.5. Circuito Arduino

Desde la perspectiva de implementación, el circuito del sistema de control de acceso se compone de una placa Arduino Mega, un módulo de relé y una cerradura electromagnética, acompañados de una fuente de poder de 12 [V] dedicada. La figura correspondiente muestra la interconexión de estos elementos, donde el relé actúa como intermediario entre el microcontrolador y la cerradura para logara manejar corrientes más altas sin comprometer el funcionamiento y la estabilidad de la placa.

Adicionalmente, se considera la inclusión de un diodo de rueda libre conectado en paralelo a la cerradura, con el propósito de que el diodo absorba los picos de corriente de retorno que se generan al des energizar la bobina (cerradura). De esta manera se previenen daños en el microcontrolador y en el relé, asegurando mayor estabilidad en el funcionamiento.

De esta manera, se logra separar la carga de potencia respecto al consumo del microcontrolador, incrementando la confiabilidad del prototipo y reduciendo el riesgo de caídas o bloqueos del sistema.

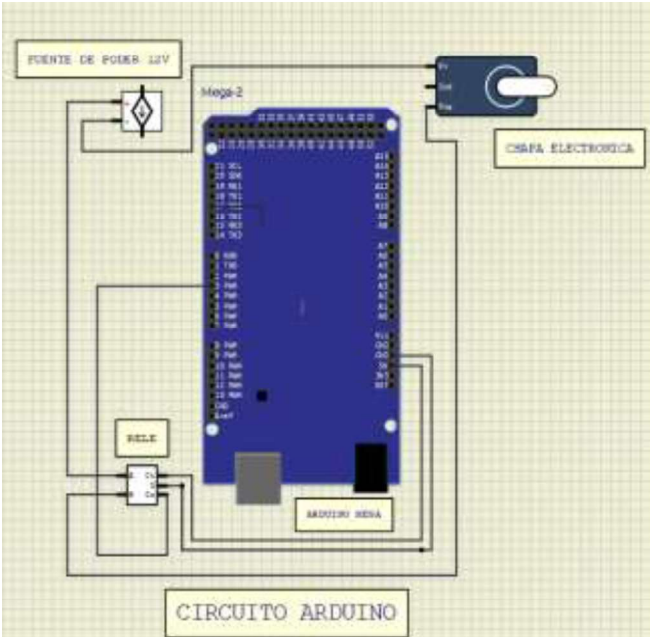


Figura. 3. Esquema circuital
Fuente: Elaborado por el autor

4.6. Descripción de módulos de software

A continuación, se detalla el papel de cada uno de los scripts que forman parte del sistema, relacionándolos con el flujo de trabajo general.

4.6.1 Captura de rostros

Los archivos **captura_rostros.py**, **registro_gui.py** y **registro_docente.py** se encargan de registrar las imágenes que servirán de base para el entrenamiento del modelo de reconocimiento. Este proceso sigue una secuencia clara y ordenada:

- Activación de la cámara y configuración de parámetros de captura.
- Detección del rostro mediante el clasificador Haar Cascade.
- Almacenamiento de una serie de imágenes (10 para docentes y estudiantes en las interfaces gráficas, 20 en el módulo genérico) en carpetas organizadas.
- Identificación de cada carpeta con el nombre del usuario, normalizado para evitar errores.
- El resultado es un repositorio de imágenes bien estructurado que posteriormente será procesado para extraer características.

En las siguientes figuras se presentan las interfaces gráficas que permiten llevar a cabo este proceso

Figura. 4. Panel - menú principal
Fuente: Elaborado por el autor

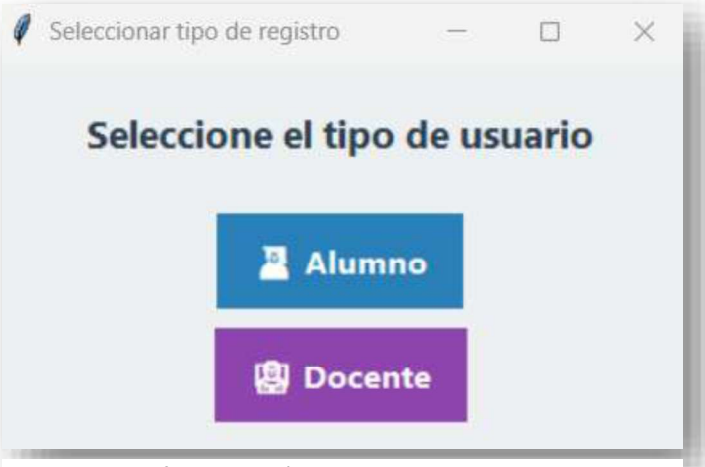


Figura. 5. Interfaz: Selección tipo de usuario para registro
Fuente: Elaborado por el autor

Figura. 6. Interfaz: Registro usuario – estudiante
Fuente: Elaborado por el autor

Figura. 7. Interfaz: Registro usuario – docente
Fuente: Elaborado por el autor

4.6.2 Entrenamiento del modelo

El script trainer.py recorre el repositorio de imágenes, detecta los rostros y extrae sus características, asociándolas a etiquetas únicas. Con estos datos entrena un modelo LBPH, que se guarda en el archivo modelos/trainer.yml. De forma paralela se genera el archivo labels.pickle que vincula las etiquetas numéricas con los nombres reales de los usuarios.

Este proceso de entrenamiento debe ejecutarse cada vez que se añadan nuevos registros, garantizando así que el modelo se mantenga actualizado y sea capaz de reconocer a todos los usuarios autorizados.

En la Figura 8 se muestra la ejecución del script en consola, confirmando la finalización del proceso y el almacenamiento del modelo entrenado.

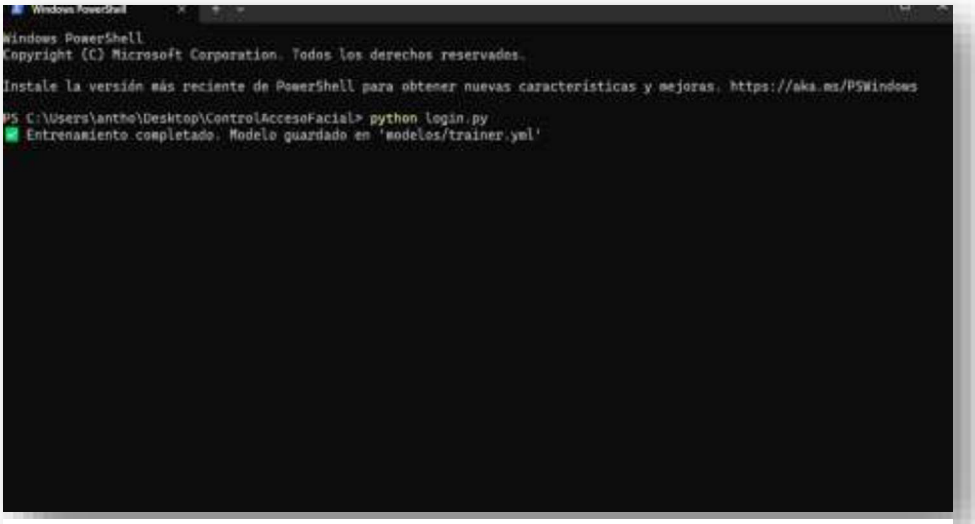


Figura. 8. Entrenamiento del modelo en la consola CMD/ PowerShell
Fuente: Elaborado por el autor

4.6.3 Reconocimiento facial

El script **reconocimiento.py** se encarga del proceso de identificación en tiempo real, acción que realiza a través de las siguientes etapas:

- Captura continua de fotogramas desde la cámara.
- Detección de rostros en cada fotograma.
- Predicción de la identidad con el modelo entrenado.
- Validación de coincidencia y asignación de etiqueta.
- Visualización en pantalla de un mensaje de bienvenida o advertencia según el caso.
- Activación de la cerradura si el usuario está autorizado.

La Figura 9 muestra el funcionamiento del reconocimiento facial en ejecución, donde el sistema identifica al usuario y despliega el mensaje de Bienvenido estudiante/docente.

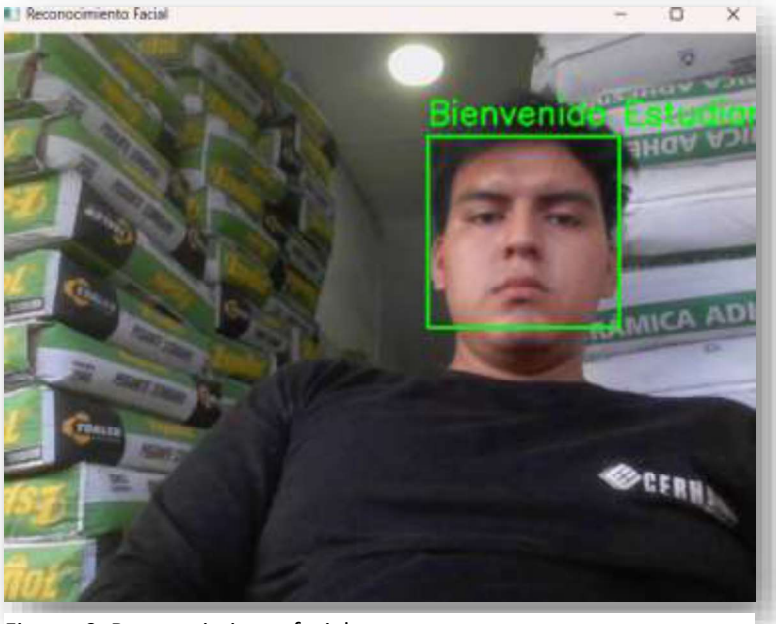


Figura. 9. Reconocimiento facial
Fuente: Elaborado por el autor

4.6.4. Conexión a la base de datos

El script **conexion_sql.py** permite la comunicación con SQL Server, dando acceso así a insertar registros de usuarios y consultar información relevante durante la operación del sistema. El acceso a la base de datos se asegura con credenciales específicas y parámetros definidos para la conexión local.

4.6.5. Interfaz de usuario y login

El archivo **login.py** gestiona el acceso administrativo al sistema. A través de esta interfaz, el administrador puede:

- Registrar usuarios (alumnos y docentes).
- Iniciar el reconocimiento facial.
- Ejecutar el entrenamiento del modelo.

El diseño incorpora botones de acceso rápido y un fondo personalizado para mejorar la experiencia de uso, tal como se observa en las figuras 10 y 11..

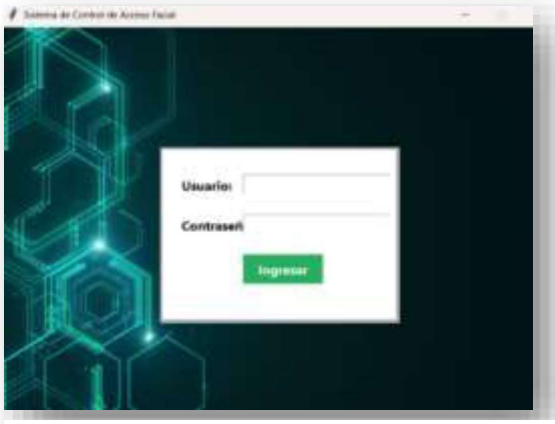


Figura. 10. Interfaz: Sistema de control de acceso facial
Fuente: Elaborado por el autor

Figura. 11. Interfaz: Menú principal
Fuente: Elaborado por el autor

4.7. Flujo operativo

El funcionamiento del sistema sigue una secuencia lógica que garantiza la integridad de los datos y la eficacia en el control de acceso:

- El administrador accede al sistema mediante la interfaz login.
- Se registra al usuario capturando sus imágenes faciales.
- Se entrena el modelo para incluir al nuevo usuario.

- El usuario se presenta frente a la cámara para el reconocimiento.
- Si la coincidencia es válida, el sistema envía la señal al Arduino para accionar la cerradura y se registra el evento en la base de datos.

4.8. Procedimiento de pruebas

Las pruebas se dividieron en dos categorías principales:

4.8.1. Pruebas Funcionales

- Verificación del reconocimiento con usuarios autorizados.
- Rechazo a usuarios no registrados.
- Registro correcto en base de datos.
- Activación de la cerradura.

4.8.2. Pruebas no funcionales

- Medición de tiempo de respuesta.
- Tolerancia a variaciones de luz y accesorios.
- Resistencia a intentos de fraude con fotografías.

Cada escenario fue evaluado en 50 repeticiones para obtener resultados estadísticamente relevantes.

4.9. Resultados obtenidos

Los resultados de las pruebas realizadas permiten evaluar el desempeño del sistema de reconocimiento facial bajo diferentes escenarios de uso. Para ello se llevaron a cabo un total de 50 intentos por cada condición, registrando la cantidad de aciertos, el porcentaje de precisión y el tiempo promedio de respuesta. La Tabla 1 resume los datos obtenidos, mientras que la Figura 12 presenta la variación de la precisión según el escenario, lo cual

facilita la comparación visual del rendimiento en situaciones óptimas y en condiciones adversas. Estos resultados constituyen la base para el posterior análisis e interpretación de la eficacia del sistema.

Tabla 1. Tabulación de resultados

Escenario	Nº intentos	Reconocidos correctamente	% Precisión	Tiempo promedio (ms)
Condiciones óptimas	50	49	98%	850
Luz natural intensa	50	47	94%	880
Luz artificial	50	45	90%	900
Baja iluminación	50	41	82%	1020
Uso de gafas	50	44	88%	930
Uso de mascarilla	50	43	86%	940
Foto impresa	50	0	0%	850
Rostro no registrado	50	0	0%	870

Fuente: Elaborado por el autor

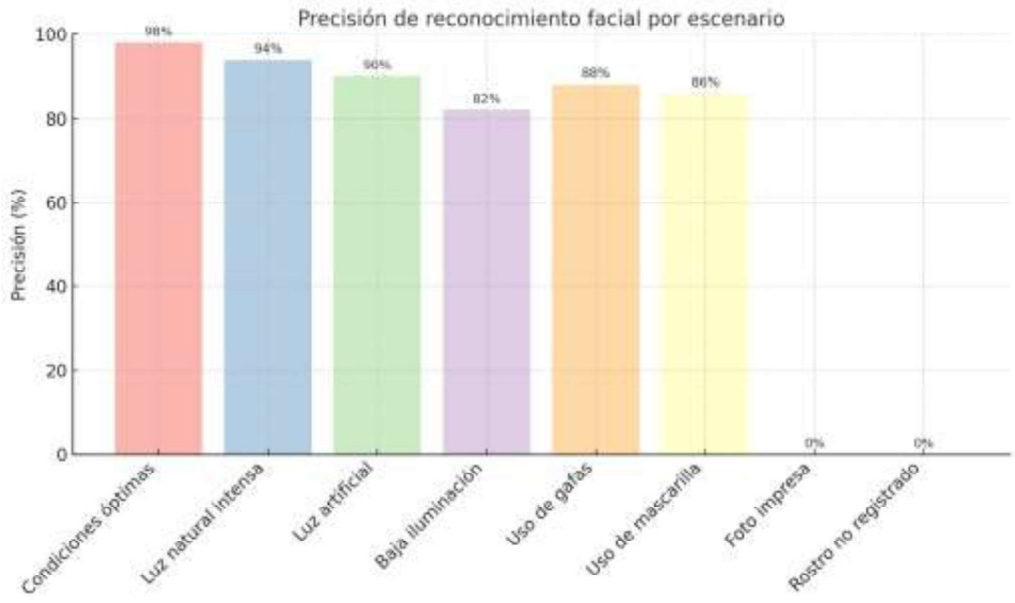


Figura. 12. Precisión de reconocimiento facial por escenario
Fuente: Elaborado por el autor

4.10. Interpretación de resultados

Los datos muestran un rendimiento sobresaliente en condiciones óptimas, con un 98 % de precisión y tiempos de respuesta inferiores a un segundo.

La precisión disminuye en entornos con poca luz o con obstrucciones parciales del rostro, lo cual es consistente con el comportamiento esperado de sistemas basados en visión artificial. En materia de seguridad, el sistema responde correctamente ante intentos de fraude, rechazando el 100 % de accesos con fotografías o rostros no registrados.

4.11. Comparación con estudios previos

Frente a los resultados de Miranda Orostegui et al. (2021), que alcanzaron un 77,38 % de precisión, el presente sistema mejora notablemente, situándose en promedio un 15 % por encima incluso en condiciones adversas.

Este avance se atribuye a la combinación de un algoritmo robusto, un conjunto de datos de entrenamiento bien estructurado y un hardware optimizado para la tarea.

4.12. Fortalezas, debilidades y oportunidades

Fortalezas:

- Alta precisión en entornos controlados.
- Escalabilidad modular.
- Resistencia a intentos de fraude.

Debilidades:

- Sensibilidad a condiciones de iluminación extremas.
- Necesidad de reentrenamiento para nuevos usuarios.

Oportunidades:

- Implementar cámaras con sensores infrarrojos.
- Integrar mejoras en preprocesamiento de imágenes.
- Vincular el sistema con plataformas institucionales de gestión académica.

4.13. Impacto académico y técnico

El sistema no solo funciona como un mecanismo seguro de control de acceso, sino que también se convierte en una oportunidad de aprendizaje real para los estudiantes de la carrera de Tecnologías de la Información. A través de este proyecto, se integran temas como inteligencia artificial, visión por computadora y manejo de bases de datos, aplicados en un contexto práctico.

El trabajo con la captura de imágenes, entrenamiento de modelos y validación en tiempo real, convierte al prototipo en un ejemplo claro de aprendizaje basado en proyectos. Además, ayuda a entender cómo es el ciclo de vida de un sistema, desde el análisis de requerimientos, hasta las pruebas y la documentación final.

La arquitectura modular del sistema permite la conexión con diferentes áreas académicas:

- En programación y estructuras de datos, se estudia la lógica y los patrones empleados.
- En base de datos, se profundiza en el modelado y las consultas.
- En electrónica y redes, se analiza la comunicación entre el software, el microcontrolador y los elementos de control.

Además, el uso de herramientas accesibles y de bajo costo facilita la replicabilidad en otros laboratorios, bibliotecas o salas especializadas, lo cual promueve estandarización y mantenimiento sencillo.

En consecuencia, la universidad dispone de un caso real para prácticas, proyectos integradores y trabajos de titulación, fortaleciendo las competencias técnicas y también transversales como: trabajo en equipo, documentación y ética en el manejo de datos biométricos.

Finalmente, el prototipo sienta bases para futuras mejoras como, la integración con sistemas académicos, tableros de monitoreo o sensores adicionales y, por ende, se configura como un activo institucional que impulsa innovación aplicada y transferencia de conocimiento dentro y fuera del campus.

4.14. Implementación física del circuito Arduino y pruebas de activación

Para cumplir con el objetivo propuesto del proyecto se implementa de manera física el prototipo con los siguientes elementos: Una placa Arduino MEGA, un módulo de relé de un canal, una cerradura electromagnética de 12v y una fuente de alimentación independiente. La separación de la alimentación de la cerradura respecto al microcontrolador garantiza la estabilidad de sistema y previene daños en la placa.

4.14.2. Diagrama eléctrico

El diagrama eléctrico representa las conexiones entre los elementos que conforman el hardware del sistema de control automático para la apertura de la cerradura electromagnética. En este montaje se utilizó una placa Arduino Mega 2560, un módulo de relé de un canal, una cerradura electromagnética de 12 V y una fuente de alimentación independiente.

- Arduino MEGA 2560: se encarga de recibir la señal desde Python mediante el puerto USB. El pin digital 42 se asigna al control del relé
- Módulo de relé: funciona como puente entre la placa Arduino y la cerradura. Se alimenta con 5 V desde la placa Arduino y comparte el mismo GND. La entrada de control (IN) del relé se conecta al pin digital 42 del Mega. Al tratarse de un módulo activo en bajo (RELAY_ACTIVE_LOW = true), la excitación del relé ocurre cuando el pin se lleva a nivel lógico LOW.
- Cerradura electromagnética: se conecta al contacto NO (Normalmente Abierto) del relé, de modo que solo se energiza cuando éste se activa. El contacto COM se conecta a la fuente de 12 V y el retorno de la cerradura al GND de la misma fuente.
- Protección adicional: se conecta un diodo de rueda libre (1N4007) en paralelo a la cerradura para evitar picos de corriente de retorno que pueden dañar al circuito durante la des energización.

4.14.3. Comunicación Arduino-Python

La comunicación entre el software y el hardware se realiza a través del puerto serial USB, mediante el envío de señales lógicas simples que garantizan un control eficiente:

- Python detecta un rostro válido mediante el modelo LBPH.
- Una vez validado, envía la señal '1' por el puerto serial para activar la cerradura.
- Arduino recibe la instrucción y establece el pin digital en **HIGH**, activando el relé.
- Una vez transcurrido un tiempo definido, se envía la señal '0'; el pin retorna a LOW y la cerradura se desactiva, volviendo al estado de bloqueo.

4.14.4. Montaje físico

El montaje se desarrolla sobre protoboard, interconectando los pines digitales del Arduino con el módulo de relé. La cerradura se conecta a la salida del relé y a una fuente independiente de 12V. Durante las pruebas se utilizan multímetros digitales para medir el voltaje y la corriente en funcionamiento, verificando además la polaridad y el aislamiento en las conexiones para evitar cortocircuitos

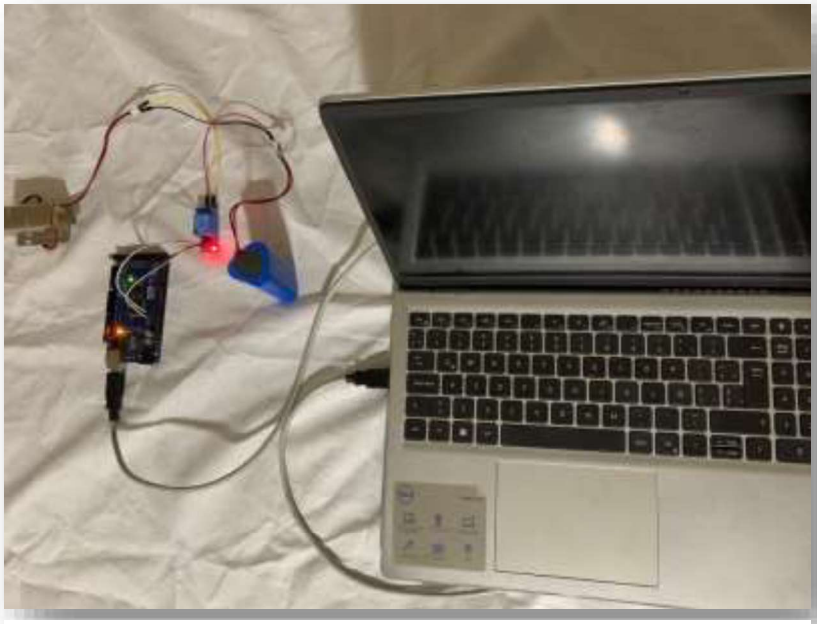


Figura. 13. Montaje físico: PC - Arduino - relé – cerradura
Fuente: Elaborado por el autor

Figura. 14. Placa Arduino - pines de conexión
Fuente: Elaborado por el autor

4.14.5. Resultados de pruebas de activación

Las pruebas de activación permiten verificar el desempeño eléctrico y la rapidez de respuesta del sistema. Los datos obtenidos se presentan en la Tabla 2:

Tabla 2. Resultados - pruebas de activación

Parámetro	Valor obtenido
Voltaje aplicado a la cerradura	11,1 [V]
Corriente consumida por la cerradura	~450 [mA]
Tiempo de reconocimiento facial (detección y validación)	0,8 – 1,2 [s]
Tiempo de activación de la cerradura desde la señal serial	< 200 [ms]

Fuente: Elaborado por el autor

Los resultados evidencian que el prototipo mantiene un tiempo de respuesta inferior a un segundo en la mayoría de escenarios, lo que asegura un funcionamiento eficiente y adecuado para el contexto planteado.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Luego de haber cumplido con los objetivos planteados y tras el análisis de los resultados alcanzados en el proceso investigativo, se establecen las siguientes conclusiones:

En primer lugar, la implementación del prototipo de un sistema automatizado de control de acceso basado en reconocimiento facial evidenció ser una alternativa eficiente para reforzar la seguridad en el aula STEAM de la UCACUE, extensión La Troncal. El sistema integró varios componentes: una cámara web, el algoritmo LBPH, una placa Arduino y una base de datos en SQL Server, logrando que el prototipo reconociera a las personas autorizadas y habilitara el acceso de manera automática, reduciendo la posibilidad de que alguien no autorizado ingresara.

Asimismo, se comprobó que el sistema guardaba en tiempo real cada entrada y salida, generando un registro digital que sirvió como respaldo, además de convertirse en una herramienta para el control de asistencia y de seguridad para docentes y estudiantes.

También se desarrollaron interfaces gráficas de fácil uso, lo que permitió comprobar que el sistema podía ser manipulado por usuarios sin conocimientos técnicos avanzados, aspecto clave en el contexto educativo, donde se prioriza la simplicidad y la usabilidad.

Este proyecto impulsa la innovación en la institución porque introduce herramientas relacionadas con la digitalización y la automatización de procesos. Se conecta con tendencias globales como la biometría y la inteligencia artificial adaptadas a la realidad local.

Finalmente, se confirmó que el sistema no guardaba información biométrica sensible. Las imágenes se usaron solo en el momento del reconocimiento y no se almacenaron

posteriormente. Con ello se cumplieron las normas vigentes en Ecuador sobre protección de datos y se aseguró la privacidad de los usuarios.

5.2. Recomendaciones

Con base en los resultados obtenidos y en la experiencia derivada de la implementación del prototipo, se proponen las recomendaciones:

a. Aplicación institucional: se recomienda que la UCACUE, sede La Troncal, evalúe la posibilidad de aplicar este tipo de sistemas en otros espacios académicos y administrativos, a fin de reforzar la seguridad institucional.
b. Mantenimiento y actualización: se recomienda establecer un plan de mantenimiento y actualización constante, tanto en el hardware como en el software. Es clave actualizar de manera periódica la base de datos de rostros, para que los registros no se queden desfasados y el reconocimiento mantenga un buen nivel de precisión.
c. Ampliación de funcionalidades: se recomienda agregar nuevas funciones al sistema, como enviar notificaciones cuando alguien intente entrar sin autorización, generar reportes estadísticos de asistencia, integrarse con las plataformas académicas de la universidad.
d. Optimización técnica: se recomienda seguir probando nuevas librerías y metodologías de reconocimiento facial, con el fin de mejorar la rapidez de respuesta y la exactitud, especialmente en casos de poca iluminación o cuando la persona cambia notablemente su apariencia.
e. Continuidad académica: se sugiere que estudiantes e investigadores de la carrera de Tecnologías de la Información continúen con el perfeccionamiento del prototipo, promoviendo su escalabilidad y la transferencia de resultados hacia aplicaciones de

mayor envergadura. De esta forma, se fomenta el desarrollo de proyectos tecnológicos que respondan a necesidades de la institución y de la comunidad.

Bibliografía

[1] D. Molinaro, «Avast,» 16 Publicado el 4 de noviembre de 2022 2022. [En línea]. Available: https://www.avast.com/c-what-is-biometric-data#:~:text=What%20is%20biometric%20data%3F. [Último acceso: 16 05 2025].

[2] [En línea]. Available: https://support.apple.com/en-us/108411#:~:text=Use%20Face%20ID%20on%20your,iPhone%20or%20iPad%20Pro. [Último acceso: 16 05 2025].

[3] D. Molinaro, «AVAST,» 4 11 2022. [En línea]. Available: https://www.avast.com/c-what-is-biometric-data#:~:text=What%20is%20biometric%20data%3F. [Último acceso: 16 05 2025].

[4] D. Molinaro, «AVAST,» 4 11 2022. [En línea]. Available: https://www.avast.com/c-what-is-biometric-data#:~:text=information%20held%20in%20a%20database,authenticated%20and%20access%20is%20granted. [Último acceso: 16 05 2025].

[5] D. Molinaro, «AVAST,» [En línea]. Available: https://www.avast.com/c-what-is-biometric-data#:~:text=What%20is%20biometric%20data%3F. [Último acceso: 16 05 2025].

[6] J. HOLDSWORTH, «IBM,» 17 06 2024. [En línea]. Available: https://www.ibm.com/mx-es/think/topics/deep-learning#:~:text=El%20aprendizaje%20profundo%20es%20un,IA%29%C2%A0en%20nuestras%20vidas%20actuales. [Último acceso: 16 05 2025].

[7] MathWorks, «MathWorks,» [En línea]. Available: https://la.mathworks.com/discovery/convolutional-neural-network.html. [Último acceso: 16 05 2025].

[8] W. e. libre, «WikipediaLa enciclopedia libre,» WikipediaLa enciclopedia libre, [En línea]. Available: https://en.wikipedia.org/wiki/DeepFace#:~:text=DeepFace%20systems%20can%20identify%20faces,10. [Último acceso: 16 05 2025].

[9] W.-M. Lee, «code magazine,» revista code, 15 05 2022. [En línea]. [Último acceso: 16 05 2025].

[10] W. e. libre, «WikipediaLa enciclopedia libre,» WikipediaLa enciclopedia libre, [En línea]. Available: https://es.wikipedia.org/wiki/Sistema_embebido#:~:text=Puesto%20que%20los%20sistemas%20embebidos,107%20en%20los%20a%C3%B1os%201980. [Último acceso: 16 16 2025].

[11] W. e. libre, «WikipediaLa enciclopedia libre,» WikipediaLa enciclopedia libre, [En línea]. Available: https://es.wikipedia.org/wiki/Sistema_embebido#:~:text=Existen%20tambi%C3%A9n%20plataformas%20desarrolladas%20por,mbed%2C%20%20110%2C%20BeagleBone%2C%20etc. [Último acceso: 16 05 2025].

[12] [En línea]. Available: https://www.redhat.com/es/topics/security/what-is-access-control. [Último acceso: 23 12 202].

[13] «genea,» GENEA, 29 08 2022. [En línea]. Available: https://www.getgenea.com/blog/the-pros-and-cons-of-facial-recognition-access-control/#:~:text=Not%20all%20biometric%20access%20control,and%20palm%20vein%20are%20contactless. [Último acceso: 16 05 2025].

[14] PDK, «PDK,» [En línea]. Available: https://www.prodatakey.com/single-post/what-is-an-access-control-system#:~:text=match%20at%20L262%20systems%20can,processes%2C%20saving%20time%20and%20labor. [Último acceso: 16 05 2025].

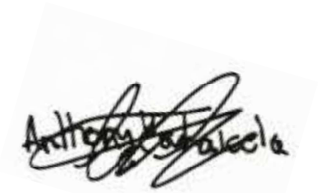
[15] J. M. B. Zazueta, «Sistema de control de acceso mediante identificacion facial usando aprendizaje profundo,» *1 Tecnologico Nacional de M ´ exico,* p. 13, 2021.

[16] J. P. Nicole Martínez-Martín, «Revista AMA de Ética,» 02 2019. [En línea]. Available: https://journalofethics.ama-assn.org/article/what-are-important-ethical-implications-using-facial-recognition-technology-health-care/2019-02#:~:text=informed%20consent%20and%20reporting%20incidental,clinician%20relationships. [Último acceso: 16 05 2025].

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Yadaicela Toledo Anthony Yair portador(a) de la cédula de ciudadanía Nº **0942350596**. En calidad de autor/a y titular de los derechos patrimoniales del proyecto de titulación **" Implementación de un prototipo de sistema automatizado para control de acceso mediante reconocimiento facial para el aula STEAM de la Universidad Catolica de Cuenca, extensión San Pablo de La Troncal "** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste proyecto de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

La Troncal 30 de octubre del 2025



Yadaicela Toledo Anthony Yair

C.I. 09423505965