UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

PROYECTO INTEGRADOR

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

SISTEMA INFORMÁTICO CON REDES NEURONALES PARA LA SEGURIDAD EN LA SALA DE PROFESORES DE TI Y SOFTWARE DE LA ULEAM EXT. EL CARMEN

LOOR MERA NAYELI MARIA

AUTOR/ES

ING. SINCHIGUANO CHIRIBOGA CÉSAR AUGUSTO, MG.
TUTOR

EL CARMEN, AGOSTO 2025

CERTIFICACIÓN DEL TUTOR

Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-010
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor de la Extensión El Carmen de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido y revisado el trabajo de Integración Curricular bajo la autoría de la estudiante **LOOR MERA NAYELI MARIA** legalmente matriculados en la carrera de Tecnologías de la Información, período académico 2025(1), cumpliendo el total de 360 horas, cuyo tema del proyecto es: **SISTEMA INFORMÁTICO CON REDES NEURONALES PARA LA SEGURIDAD EN LA SALA DE PROFESORES DE TI Y SOFTWARE DE LA ULEAM EXT EL CARMEN.**

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Lugar, El Carmen 18 de agosto del 2025.

Lo certifico,

Ing. César Sinchiguano Chiriboga
Docente Tutor
Área: Tecnologías de la Información

TRIBUNAL DE SUSTENTACIÓN

Universidad Laica Eloy Alfaro de Manabí
Extensión El Carmen
Carrera de Ingeniería en Tecnologías de la Información

TRIBUNAL DE SUSTENTACIÓN

Título del Trabajo de Titulación: Sistema Informatico con Redes Neuronales para la Seguridad en la Sala de Profesores de TI y Software de la Uleam Extensión El Carmen

Modalidad: Proyector Integrador

Autora: Loor Mera Nayeli Maria

Tutor: Ing. Sinchiguano Chiriboga Cesar Augusto, Mg.

Tribunal de Sustentación:

Presidente:
Ing. Mora Marcillo Alex Bladimir, Mg.

Miembro:
Ing. Arévalo Hermida Rómulo Danilo, Mg.

Miembro:
Ing. Quiroz Valencia Arturo Patricio, Mg.

Fecha de Sustentación: 11 de septiembre de 2025

DECLARACIÓN DE AUTORÍA

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: Sistema Informático con redes neuronales para la seguridad en la sala de profesores de TI y Software de la ULEAM Ext El Carmen, corresponde exclusivamente a: Loor Mera Nayeli Maria con CI:1317451308, y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

Autor: Loor Mera Nayeli Maria

C.I. 1317451308

DEDICATORIA

Dedico este trabajo a Dios por darme la vida, la fortaleza y la sabiduría para superar cada desafío durante este proceso, su guía ha sido mi refugio y mi impulso constante.

A mi madre Gissela Mera por su amor incondicional, su apoyo en todo momento y por ser mi ejemplo de esfuerzo y perseverancia, gracias por cada palabra de aliento, por la paciencia y por creer en mí incluso en los días más difíciles.

A mi padre Kleiner Loor, mis familiares y amigos, por estar siempre presentes con su cariño y ánimo constante, su apoyo ha sido fundamental en este logro.

Y con profundo respeto y cariño, dedico este trabajo a la memoria de mi compañero Wellington Muñoz, cuya partida dejó un vacío, pero también el recuerdo de su amistad, su energía y dedicación, su huella permanece en quienes tuvimos la dicha de compartir este camino con él.

Nayeli Loor

AGRADECIMIENTO

Agradezco profundamente a la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, por brindarme la oportunidad de formarme profesionalmente en un entorno académico comprometido con la excelencia.

Mi gratitud también se extiende a los docentes de la carrera de Tecnologías de la Información, quienes, con su conocimiento, guía y vocación educativa, contribuyeron de manera significativa a mi crecimiento académico.

A mi tutor César Sinchiguano, por su acompañamiento, paciencia y orientación técnica durante el desarrollo de este proyecto. Su apoyo fue fundamental para convertir esta investigación en una realidad.

Asimismo, agradezco sinceramente a mis padres, familiares y amigos, por estar presentes en cada paso del camino, por su apoyo incondicional, sus palabras de aliento y la confianza depositada en mí, su compañía ha sido esencial para alcanzar este logro académico.

Nayeli Loor

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo tiene como objetivo desarrollar e implementar un sistema informático basado en redes neuronales para el control de acceso mediante reconocimiento facial, orientado a reforzar la seguridad en la sala de profesores de las carreras de Tecnología de la Información y Software de la Universidad Laica “Eloy Alfaro” de Manabí, Extensión El Carmen. Como no hay ninguna tecnología que controle el acceso en este sitio, la idea fue proponer un sistema con Raspberry Pi que permita reconocer de manera confiable a los docentes autorizados mediante el rostro. Para llegar ahí, bueno, se trabajó con un enfoque mixto: por un lado, se aplicaron encuestas y entrevistas para recoger opiniones, y por otro, se hicieron pruebas prácticas donde se midió el rendimiento, la precisión y, en definitiva, qué tan efectivo resultaba todo el sistema. Los resultados dejan ver mejoras notables: el control de acceso se volvió más eficiente, los riesgos bajaron y, además, se optimizó el uso tanto del personal como de la parte tecnológica. Y bueno, vale la pena mencionar que no se queda solo aquí esta propuesta fácilmente podría replicarse en otros entornos académicos. A decir verdad, también abre la puerta a que la inteligencia artificial se meta de lleno en la seguridad de las instituciones.

Palabras clave: Reconocimiento facial, redes neuronales, Raspberry Pi, sistemas embebidos, seguridad académica.

ABSTRACT

This work aims to develop and implement a neural network-based computer system for access control using facial recognition, aimed at strengthening security in the faculty lounge of the Information Technology and Software programs at the Eloy Alfaro Laica University in Manabí, El Carmen Extension. Since there is no technology controlling access at this location, the idea was to propose a system using a Raspberry Pi that would reliably recognize authorized faculty members by face. To achieve this, a mixed approach was used: on the one hand, surveys and interviews were conducted to gather opinions, and on the other, practical tests were conducted to measure performance, accuracy, and, ultimately, the effectiveness of the entire system. The results show notable improvements: access control became more efficient, risks decreased, and the use of both staff and technology was optimized. And it's worth mentioning that the solution doesn't end there; this proposal could easily be replicated in other academic settings. In fact, it also opens the door for artificial intelligence to become deeply involved in institutional security.

Keywords: Facial recognition, neural networks, Raspberry Pi, embedded systems, academic security.

CAPÍTULO I

1. INTRODUCCIÓN

La seguridad en entornos académicos constituye un aspecto esencial para garantizar la integridad institucional, la protección del personal docente y la confidencialidad de la información. No obstante, los mecanismos tradicionales de control de acceso, como las llaves físicas o los registros manuales, resultan vulnerables e ineficientes.

En la actualidad, la identificación facial y las redes neuronales se utilizan de manera creciente como soporte para reforzar la seguridad en instituciones. La automatización del acceso mediante visión por computadora permite una detección más precisa de las personas autorizadas, lo que reduce los intentos de suplantación y los ingresos no permitidos.

El presente proyecto propone el desarrollo de un sistema informático basado en redes neuronales que fortalezca la seguridad en la sala de profesores de las carreras de Tecnología de la Información y Software de la Universidad Laica “Eloy Alfaro” de Manabí, Extensión El Carmen. Para su implementación se empleó una Raspberry Pi, seleccionada por sus ventajas en costo, portabilidad, bajo consumo energético y compatibilidad con aplicaciones de inteligencia artificial.

La metodología aplicada integra encuestas y entrevistas para conocer la percepción de los usuarios, además de pruebas experimentales orientadas a evaluar la precisión, el rendimiento y la efectividad del sistema. Se espera como resultado un control de acceso más eficiente, con menores riesgos de intrusión y un aprovechamiento óptimo de los recursos disponibles. Asimismo, el sistema posee potencial de adaptación a otros entornos, tanto académicos como empresariales.

1.1. Presentación del tema

La falta de un sistema automatizado de control de acceso en la sala de profesores constituye una vulnerabilidad significativa para la seguridad institucional. En la actualidad no se dispone de mecanismos que registren de manera precisa los ingresos y la identidad de las personas, lo cual incrementa el riesgo de pérdidas materiales y genera incertidumbre entre el personal docente. Esta problemática evidencia la necesidad de implementar una herramienta tecnológica que garantice un acceso seguro, eficaz y confiable.

1.2. Ubicación y contextualización de la problemática

El proyecto se desarrolla en la Universidad Laica "Eloy Alfaro" de Manabí, Extensión El Carmen, específicamente en la sala de profesores ubicada en el segundo piso del edificio Tiempo Completo 2. Este espacio es utilizado por los docentes de las carreras de Tecnología de la Información y Software para trabajo académico, planificación y resguardo de materiales.

En la actualidad, la sala carece de un sistema que controle de manera adecuada el acceso. La cerradura principal presenta fallas que impiden su correcto funcionamiento, lo que permite el ingreso de docentes, estudiantes y personas externas sin restricción alguna. Esta situación pone en riesgo la seguridad de los equipos, los documentos y las pertenencias personales, generando vulnerabilidad en el entorno académico. Ante esta problemática, se plantea la necesidad de implementar una alternativa tecnológica que limite el acceso únicamente a personal autorizado y que garantice la protección de los recursos institucionales.

1.3. Planteamiento del problema

1.3.1. Problematización

El crecimiento académico y tecnológico de la carrera de Tecnología de la Información y Software no ha estado acompañado por una infraestructura de seguridad acorde en áreas sensibles, como la sala de profesores. La ausencia de mecanismos automatizados de control de acceso impide registrar de manera confiable los ingresos, lo que incrementa el riesgo de suplantación de identidad, ingreso no autorizado y pérdida de pertenencias. Esta situación compromete la seguridad institucional y afecta la productividad del personal docente, al mantenerse la dependencia de métodos manuales poco efectivos.

Pregunta problema:

¿De qué manera la implementación de un sistema moderno de control de acceso basado en redes neuronales puede mejorar la seguridad en la sala de profesores de TI y Software de la ULEAM, Extensión El Carmen?

1.3.2. Génesis del problema

Desde el inicio de la carrera en el año 2016, la sala de profesores no ha contado con un mecanismo eficaz que garantice el ingreso exclusivo de personal autorizado. El acceso se mantiene mediante llaves físicas y, al no existir un sistema digital de registros, se han generado riesgos, especialmente en los casos en que se producen ingresos fuera del horario establecido.

1.3.3. Estado actual del problema

La ULEAM Extensión El Carmen enfrenta un desafío significativo en la seguridad y gestión de la sala de profesores de las carreras de Tecnología de la Información (TI) y Software,

debido a la ausencia de un sistema adecuado de control de acceso. La falta de un registro de entrada y salida impide controlar quién accede a la sala, dificultando la identificación de las personas presentes en determinado momento y la asignación de responsabilidades en caso de pérdida o daño de equipos y materiales.

Del mismo modo, no contar con un registro de horarios genera incertidumbre sobre la disponibilidad del espacio, lo que abre la puerta a ingresos no autorizados y a posibles problemas de seguridad. A eso se suma que no existen datos claros sobre la presencia del personal encargado de abrir la sala, lo que termina provocando retrasos y pérdida de tiempo para los docentes, en definitiva, afecta su eficiencia y la organización de las actividades académicas.

1.4. Diagrama causa – efecto del problema

Figura 1

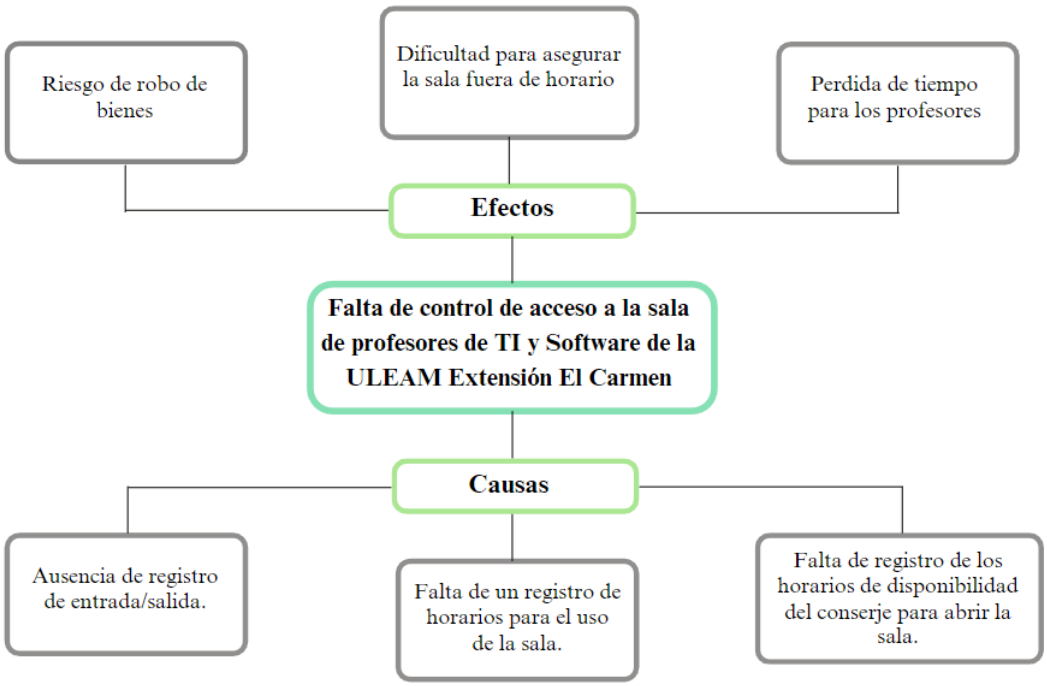


Diagrama causa-efecto

Fuente: Elaboración propia (2025).

1.5. Objetivos

1.5.1. Objetivo general

Implementar un sistema informático con redes neuronales para la seguridad en la sala de profesores de TI y Software de la ULEAM Extensión El Carmen.

1.5.2. Objetivos específicos

- Analizar bibliográfica actualizada sobre tecnologías de reconocimiento facial, redes neuronales y sistemas embebidos.
- Identificar, a través de encuestas y entrevistas, los requisitos funcionales y expectativas de los usuarios respecto al sistema.
- Implementar un sistema embebido que integre reconocimiento facial y almacenamiento digital de registros de acceso.
- Evaluar el sistema mediante pruebas experimentales orientadas a medir su rendimiento, precisión y confiabilidad.

1.6. Justificación

El estudio se fundamenta en la necesidad de optimizar la seguridad en el área de profesores de la carrera de Tecnologías de la Información y Software de la Universidad Laica “Eloy Alfaro” de Manabí, Extensión El Carmen. Los sistemas convencionales, basados en llaves físicas y registros manuales, presentan debilidades como accesos no autorizados, ausencia de registros confiables y pérdida de bienes, lo que afecta de manera negativa la confianza del personal docente y de la administración académica.

El trabajo se desarrolla bajo un enfoque de investigación orientado a la comparación y validación de algoritmos de reconocimiento facial, específicamente Histogram of Oriented Gradients (HOG) y Convolutional Neural Networks (CNN), implementados en un sistema embebido accesible como la Raspberry Pi 5. El análisis incluye la evaluación de aspectos como la precisión, la velocidad de procesamiento, la fiabilidad y la seguridad frente a intentos de suplantación, con el fin de generar un recurso de inteligencia artificial aplicado a la seguridad universitaria.

La propuesta busca garantizar un espacio académico protegido mediante la incorporación de un método innovador de reconocimiento facial, que además contribuye a la sostenibilidad al reemplazar el uso de llaves físicas y registros en papel. Se trata de una solución tecnológica que fortalece la seguridad institucional en el marco de la transformación digital.

1.7. Impactos esperados

1.7.1. Impacto tecnológico

El sistema propuesto moderniza la gestión de accesos, reemplazando las prácticas manuales poco seguras por herramientas más eficientes. La integración de una base de datos confiable permite registrar y analizar información sobre el uso del espacio, lo que facilita la toma de decisiones en el ámbito institucional. Asimismo, la propuesta presenta flexibilidad, ya que puede implementarse en otros contextos sin mayores complicaciones.

1.7.2. Impacto social

El sistema garantiza que únicamente los individuos autorizados puedan acceder al área, protegiendo la seguridad del personal docente y de los recursos materiales. Además, promueve

un entorno institucional que enfatiza la prevención, la responsabilidad y el uso adecuado de las áreas comunes, fortaleciendo la confianza del personal educativo en su lugar de trabajo.

1.7.3. Impacto ecológico

El sistema digital elimina los registros en papel, reduciendo la dependencia de llaves físicas y tarjetas plásticas. Asimismo, la Raspberry Pi, por su bajo consumo energético, permite un manejo más eficiente de los recursos y contribuye a disminuir la huella ambiental en comparación con soluciones que requieren mayor consumo eléctrico.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes históricos

De acuerdo con Martínez y Gómez (2023), la historia de los sistemas informáticos se remonta a los primeros dispositivos mecánicos utilizados para el cálculo. Fue durante la segunda mitad del siglo XX cuando surgieron avances decisivos con la aparición de las computadoras electrónicas digitales. El desarrollo de sistemas operativos permitió una gestión más eficiente del hardware, sentando las bases para la evolución hacia sistemas complejos. La miniaturización de los dispositivos y la expansión de la informática personal en los años 80 democratizaron el acceso a la tecnología.

Smith (2023) afirma que este progreso reciente es en su mayoría un resultado del aumento masivo en la generación de datos y la demanda de tecnologías capaces de administrarlos de forma eficaz, mediante el uso de instrumentos como la informática en la nube y la inteligencia artificial han significado un rol fundamental en esta transformación, promoviendo de esta forma la automatización permitiendo que sea más eficaz el procedimiento de tomar decisiones estratégicas.

Desde sus orígenes, la humanidad ha buscado mejorar sus condiciones de vida mediante herramientas que faciliten tanto el trabajo físico como el mental. En este contexto, las redes neuronales artificiales surgieron como un intento de replicar la arquitectura del cerebro humano, con el objetivo de crear sistemas capaces de aprender y adaptarse a partir de la experiencia (Restrepo et al., 2021). La evolución de estos modelos ha pasado por diversas etapas, comenzando con el perceptrón en la década de 1950, hasta llegar a las modernas redes neuronales profundas, capaces de procesar grandes volúmenes de datos. Posteriormente,

surgieron las redes neuronales recurrentes (RNN) y sus variantes, como las Long Short-Term Memory (LSTM), diseñadas para trabajar con datos secuenciales y conservar información pasada que influya en decisiones futuras (Botana, 2024).

Por otro lado, García y Torres (2022), indican que la seguridad física ha progresado notablemente gracias a la inclusión de tecnologías de reconocimiento biométrico. Hoy en día, métodos como la verificación por huellas dactilares, el reconocimiento facial y el análisis del iris han ido reemplazando los clásicos sistemas de llaves o tarjetas, haciendo que la identificación sea más precisa y reduciendo el riesgo de accesos no autorizados. Además, la biometría permite, de alguna manera, mantener un ojo en tiempo real sobre quién está dentro de las áreas seguras y eso sí le da un plus a la vigilancia.

Según López (2023), en los últimos años la adopción de sistemas biométricos en lugares críticos ha crecido bastante, motivada por la necesidad de contar con soluciones más confiables y sofisticadas, al combinarse la biometría con inteligencia artificial, ha generado que la autenticación se vuelve más exacta y se pueden detectar intentos de fraude con mayor facilidad, siendo esto algo que toma relevancia en sitios como salas de docentes, laboratorios o centros de datos donde es necesario cuidar el acceso físico, es un punto clave para proteger información y recursos tecnológicos.

Es importante considerar que los avances en informática han transformado los sistemas de simples máquinas mecánicas a dispositivos complejos, innovaciones tanto la inteligencia artificial como la biometría han cambiado por completo la manera de pensar la seguridad física. Las fusiones de estas dos tecnologías han generado un proceso de mejora al momento de ser más precisos con la autenticación, además es crucial para proteger información y bienes en áreas sensibles.

En resumen, los progresos en computación digital han llevado a que los sistemas informáticos pasen de ser simples máquinas mecánicas a dispositivos bastante complejos. Y bueno, la verdad es que tecnologías como la inteligencia artificial y la biometría han dado un giro completo a la seguridad física. La mezcla de estas herramientas no solo hace que la autenticación sea más precisa, sino que además resulta clave para proteger información y recursos en lugares sensibles a espacios donde cualquier descuido podría ser un problema.

2.2. Antecedentes de investigaciones relacionadas al tema presentado

2.2.1. Feasibility enterprise time and attendance system using artificial vision based on neural networks with Python and Raspberry Pi.

En un estudio que hicieron Núñez y su equipo en 2024 en la Escuela Superior Politécnica de Chimborazo (ESPOCH), presentaron un sistema para llevar el control de asistencia en empresas. La verdad es que me pareció bastante interesante: usaron reconocimiento facial con redes neuronales, todo montado en una Raspberry Pi y programado en Python. Para que te hagas una idea, recurrieron a técnicas de visión por computadora como Haar Cascade y PCA, y también al modelo LBPH FaceRecognizer de OpenCV. El resultado una tasa de éxito del 100% eso sí, bajo condiciones bien controladas. Ahora, hay que decir que no lo probaron en situaciones más complicadas, como con cambios de luz o movimientos, así que en definitiva su uso en escenarios más reales está un poco limitado.

2.2.2. Diseño e implementación de un sistema de control de acceso mediante reconocimiento facial para la academia Titanes de Cuenca.

Vaca y Rivera (2022) crearon un sistema de reconocimiento facial para la institución Titanes Cuenca con la finalidad de limitar la entrada de individuos no autorizados y administrar

las inscripciones de los usuarios. El sistema combinaba redes neuronales y una hoja de cálculo de Excel que contrastaba las imágenes tomadas con el registro de usuarios activos, facilitando la activación o desactivación de una cerradura electromagnética. Esta metodología mejoró notablemente la seguridad y la gestión administrativa del establecimiento.

2.2.3. Diseño y desarrollo de un sistema de video vigilancia basado en dispositivos embebidos, técnicas de visión artificial y algoritmos inteligentes.

Gutiérrez y Damián (2021), de la Universidad Politécnica Salesiana en Cuenca, desarrollaron un sistema de videovigilancia de bajo costo orientado al reconocimiento facial. El sistema enviaba notificaciones al dispositivo móvil ante la detección de accesos no autorizados. Para la identificación de rostros se emplearon herramientas como OpenCV, dlib y las cascadas de Haar. La propuesta fue diseñada específicamente para la seguridad en entornos residenciales, permitiendo monitorear el acceso y mantener el orden. Sin embargo, presentaba limitaciones al aplicarse únicamente en viviendas, ya que no estaba adaptada para entornos educativos, donde los mecanismos de control de acceso funcionan de manera diferente.

2.2.4. Estado del Arte

El uso de tecnologías biométricas para el control de acceso ha cobrado importancia recientemente, dado que se busca asegurar la protección en contextos educativos, corporativos y gubernamentales. En especial la biometría facial ha probado ser una solución eficaz en comparación con métodos convencionales como llaves, tarjetas o impresiones digitales, al proporcionar un registro seguro de entradas y salidas y la capacidad de autenticación instantánea.

2.2.4.1. Trabajos en Ecuador

En Ecuador, los sistemas de control de acceso han estado centrados principalmente en biometría de huella dactilar y tarjetas de proximidad. Por ejemplo:

- **Pérez et al. (2022)** implementaron un sistema basado en huellas dactilares para una universidad, logrando un registro exacto de usuarios, pero con limitaciones en la gestión de múltiples usuarios y ausencia de autenticación avanzada por reconocimiento facial.
- **Gómez y Castillo (2023)** desarrollaron un prototipo de control de acceso para laboratorios de cómputo utilizando tarjetas RFID; aunque efectivo en la identificación de estudiantes, el sistema dependía completamente del personal administrativo y no incluía un registro automático de la entrada y salida de usuarios.

De acuerdo con la investigación realizada en Ecuador, los sistemas de control de asistencia actualmente implementados presentan diversas limitaciones, ya que integran escasamente tecnología moderna y dependen en gran medida del personal administrativo, lo que genera una problemática en la gestión de registros. Asimismo, se identifica una carencia significativa de métodos biométricos avanzados que permitan verificar la presencia efectiva de los usuarios, es decir, sistemas de detección de vida, lo que representa una limitante en términos de eficacia en escenarios con mayores requerimientos de seguridad.

2.2.4.2. Trabajos en Latinoamérica

En el área de América Latina, los estudios se han encaminado hacia la combinación de redes neuronales y técnicas de identificación facial:

- **Brasil – Silva et al. (2021):** Sistema de identificación facial en tiempo real utilizado en entornos empresariales. Elevada exactitud en circunstancias reguladas, sin embargo, restringido en situaciones con luz variable y rostros en parte ocultos.
- **México – López y Rodríguez (2023):** Sistema para laboratorios universitarios usando HOG y cámaras IP. Detección rápida, pero con una base de datos poco robusta y sin métricas de desempeño detalladas.
- **Colombia – Ramírez y Torres (2022):** Implementación de un sistema biométrico híbrido (huella y rostro) en instituciones educativas. Mejor precisión que métodos individuales, pero elevada complejidad y costos de implementación.

Estos estudios evidencian avances importantes en el desarrollo de sistemas de control de acceso; sin embargo, también muestran limitaciones relevantes. Entre ellas se encuentran la dificultad para adaptarse a entornos dinámicos y la deficiente integración con bases de datos robustas. Asimismo, los mecanismos de verificación de identidad mediante técnicas de antispoofing presentan deficiencias, y los sistemas carecen de criterios claros para medir su rendimiento, lo que dificulta evaluar su eficacia en la práctica.

2.2.4.3. Cuadro comparativo de trabajos previos

Tabla 1

Cuadro comparativo de trabajos previos

Autor y año	País	Tecnología	Aplicación	Limitaciones
Pérez et al., 2022	Ecuador	Huella dactilar	Universidad	Gestión limitada de usuarios, sin autenticación avanzada

Autor y año	País	Tecnología	Aplicación	Limitaciones
Gómez y Castillo, 2023	Ecuador	Tarjetas RFID	Laboratorios de cómputo	Dependencia de personal administrativo, sin registro automático
Silva et al., 2021	Brasil	Reconocimiento facial (CNN)	Oficinas corporativas	Limitado en iluminación variable, rostros cubiertos
López y Rodríguez, 2023	México	HOG + cámaras IP	Laboratorios universitarios	Base de datos poco robusta, sin métricas de desempeño
Ramírez y Torres, 2022	Colombia	Biometría híbrida (huella + rostro)	Instituciones educativas	Complejidad alta, costos elevados

2.2.4.4. Brechas y aporte de la investigación

A partir del análisis de los trabajos previos, se identifican las siguientes brechas que la presente investigación busca cubrir:

- Implementación de un sistema de reconocimiento facial en tiempo real, adaptable a la sala de profesores de TI y Software de la ULEAM Extensión El Carmen.
- Integración de detección de vida (antispoofing) para evitar suplantaciones.
- Uso de Raspberry Pi como plataforma de bajo costo, con base de datos integrada para el registro de múltiples usuarios.
- Establecimiento de indicadores de rendimiento, teniendo en cuenta la precisión, exactitud, recalificación y puntaje F1, para posteriormente evaluar la eficacia del sistema.
- Creación de una interfaz visual intuitiva que facilite el registro y la administración de usuarios de manera rápida y eficaz.

Con esto se pretende no solo aumentar la seguridad tangible, sino también ofrecer un patrón que pueda ser reproducido y ampliado para otras entidades educativas en Ecuador y América Latina, ayudando a la creación de soluciones biométricas más efectivas y seguras en el área.

2.3. Definiciones conceptuales

2.3.1. Sistemas informáticos

2.3.1.1. Definición de Sistemas Informáticos

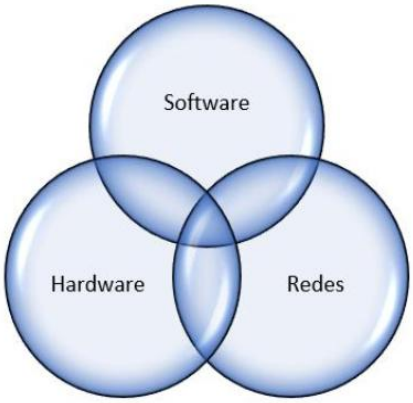
Un sistema de computación actual está formado por tres componentes esenciales que funcionan de manera interrelacionada: hardware, software y redes de comunicación. El software es un conjunto de directrices que permiten llevar a cabo funciones específicas, pero necesita del hardware como el entorno físico para ser utilizado. Al mismo tiempo, el hardware carecería de utilidad sin las directrices que le brinda el software.

Además, se destaca la importancia de las redes de comunicación, como WiFi y Ethernet, las cuales resultan esenciales para mantener la conectividad constante de los sistemas informáticos. La integración de estas tecnologías permite que los sistemas operen de manera coordinada y eficiente, asegurando un funcionamiento continuo y estable.

Briano (2023) señala que los sistemas de información constituyen herramientas clave para optimizar procesos, mejorar la eficiencia y apoyar la toma de decisiones en empresas, instituciones y organizaciones. Estos sistemas facilitan el control de gastos, la gestión contable y de seguridad, la automatización de tareas y el análisis de datos para identificar oportunidades y administrar recursos de manera estratégica. No obstante, su implementación representa un

desafío, ya que requiere una planificación adecuada para garantizar su correcto funcionamiento.

Figura 2



Constitución del Software

Fuente: Briano, 2023. *Compilación de apuntes sobre conceptos fundamentales de la Ingeniería de Software*.

2.3.1.2. Base de datos

Briano (2023) define una base de datos como un sistema estructurado para almacenar y gestionar información de manera eficiente. En este caso, se empleó una base de datos relacional para registrar los datos de los usuarios y sus accesos, garantizando la protección, integridad y fácil consulta de la información. Una correcta organización y diseño de la base de datos es fundamental para el funcionamiento del sistema de reconocimiento facial, ya que permite almacenar las imágenes de los rostros y los registros de acceso en tiempo real de manera confiable y eficiente.

2.3.1.3. Sistemas embebidos

Los sistemas embebidos son dispositivos electrónicos especializados diseñados para ejecutar funciones específicas dentro de un sistema mayor, integrando todos sus componentes en una única placa de circuito impreso (Freire, 2023). Se aplican en sectores industrial, médico, doméstico y de seguridad, incluyendo detectores de humo, sistemas de control de acceso y tecnologías wearable. En cuanto al desarrollo de software, estos sistemas soportan lenguajes de bajo nivel, como ensamblador y C, así como lenguajes de mayor abstracción, como Java, aunque presentan limitaciones en aplicaciones de tiempo real (Sepúlveda & García, 2022). Plataformas de prototipado, como Arduino, facilitan la programación, validación y despliegue de aplicaciones embebidas.

2.3.1.4. Rasberry Pi

Halfacree (2020) describe el Raspberry Pi como un ordenador compacto, económico y versátil. A pesar de su reducido tamaño, es capaz de ejecutar programas, procesar datos y controlar dispositivos de manera eficiente. En el presente proyecto, el Raspberry Pi actúa como el núcleo del sistema, gestionando el reconocimiento facial y el control de accesos, integrando la cámara, la base de datos y la interfaz de usuario en un solo equipo. Además, su bajo consumo energético y facilidad de programación lo hacen adecuado para aplicaciones en sistemas integrados.

2.3.1.5. Visión computacional

La visión computacional permite que los sistemas analicen e interpreten imágenes de manera automatizada. Según Domínguez (2021), esta tecnología no solo procesa píxeles, sino que permite extraer información relevante de las imágenes para la toma de decisiones. En el presente proyecto, se empleará para el reconocimiento facial, identificando a los usuarios y controlando el acceso a la sala de docentes. La automatización de la validación biométrica

incrementa la seguridad, reduce la necesidad de supervisión constante y se integra eficientemente con sistemas de bajo costo, como el Raspberry Pi.

2.3.2. Redes Neuronales

2.3.2.1. Historia de las redes neuronales

El desarrollo de las redes neuronales artificiales se remonta a la década de 1940, cuando Warren McCulloch y Walter Pitts proponen el primer modelo computacional el cual está inspirado en el comportamiento de las neuronas biológicas, aun así, el verdadero auge de estas tecnologías no se materializó sino varias décadas después.

La inteligencia artificial ha experimentado un desarrollo significativo desde la década de 1960, cuando la introducción del algoritmo de retropropagación permitió que las redes neuronales ajustaran sus conexiones de manera más efectiva, facilitando el aprendizaje automático. No obstante, durante varias décadas, las redes neuronales presentaron limitaciones debido a restricciones tecnológicas y dificultades en su capacidad de generalización.

Fue a partir de la década de 2010 que se produjo un avance sustancial, impulsado por la disponibilidad de mayor potencia de cómputo, grandes volúmenes de datos y métodos de entrenamiento más sofisticados. Durante este periodo, las redes neuronales demostraron un rendimiento sobresaliente en tareas de clasificación, predicción y reconocimiento de patrones, destacándose en competencias internacionales de inteligencia artificial. Actualmente, las redes neuronales se aplican en diversos ámbitos, entre los que destacan:

- Vehículos autónomos.
- Diagnósticos médicos asistidos por inteligencia artificial.
- Detección de fraudes en el sector financiero.

- Sistemas de reconocimiento facial.
- Generación automática de contenido multimedia.

Su adaptabilidad y capacidad de aprendizaje continuo las posicionan como una de las tecnologías más influyentes del siglo XXI (Kinsley & Kukieła, 2020).

2.3.2.2. Introducción a redes neuronales

Como señala Tuấn (2019), los seres vivos realizan con naturalidad tareas complejas para los sistemas computacionales, como el reconocimiento de rostros, la identificación de objetos o la comprensión del entorno. Por ejemplo, un perro puede identificar a su dueño sin dificultad, y un niño distingue entre animales, colores o miembros de su familia con precisión sorprendente. Esta capacidad cognitiva, sustentada en un cerebro con aproximadamente 86 mil millones de neuronas interconectadas, inspiró el desarrollo de las redes neuronales artificiales.

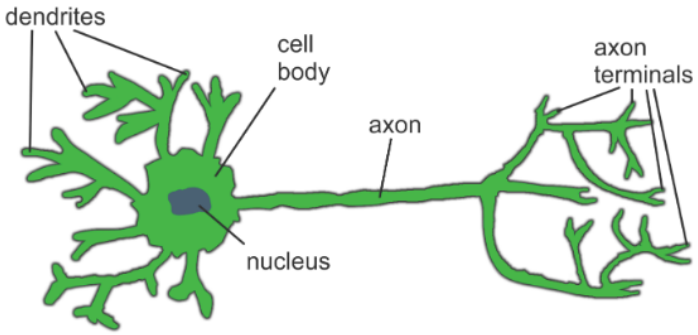
Las redes neuronales artificiales son estructuras computacionales compuestas por múltiples elementos interconectados, denominados neuronas sintéticas, que trabajan de manera coordinada para reconocer y aprender patrones complejos mediante operaciones matemáticas. Estas neuronas artificiales presentan paralelismos funcionales con las neuronas biológicas:

- Dendritas biológicas, que reciben señales electroquímicas, equivalen a las entradas ponderadas de las neuronas artificiales.
- Soma, que integra las señales recibidas, corresponde a la función de activación.
- Axón, que transmite impulsos eléctricos, se asemeja a la propagación del valor activado hacia otras neuronas.
- Terminales sinápticos, que permiten la comunicación entre neuronas, son equivalentes a las salidas conectadas a otras unidades.

El procesamiento de información mediante estas estructuras permite realizar tareas asociadas tradicionalmente con la inteligencia humana, como clasificación, predicción y reconocimiento de patrones.

No obstante, estructuras como el núcleo celular no tienen contraparte directa en los modelos computacionales. Esta analogía permite que las redes neuronales emulen ciertos procesos cognitivos, abriendo posibilidades en visión computacional, procesamiento de lenguaje natural y toma de decisiones autónomas (Haohan & Bhiksha, 2017).

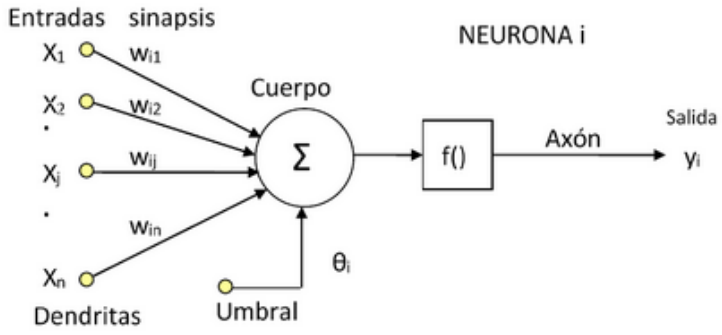
Figura 3



Neurona Biológica

Fuente: Kinsley & Kukieła, 2020. *Neural Networks from Scratch in Python*.

Figura 4



Neurona artificial

Fuente: Vorobioff et al., 2022. *Inteligencia Artificial y Redes Neuronales: Fundamentos, Ejercicios y Aplicaciones con Python y Matlab.*

2.3.2.3. Aprendizaje profundo: la revolución silenciosa de la IA

La inteligencia artificial se sustenta principalmente en dos pilares complementarios: el aprendizaje automático (machine learning) y el aprendizaje profundo (deep learning). El aprendizaje automático se clasifica en tres ramas principales:

- Aprendizaje supervisado: requiere ejemplos previamente etiquetados para entrenar al modelo, permitiendo guiar el proceso de aprendizaje.
- Aprendizaje no supervisado: busca patrones ocultos en datos no etiquetados, identificando estructuras subyacentes sin intervención externa.
- Aprendizaje por refuerzo: optimiza el desempeño del modelo mediante un sistema de recompensas basado en ensayo y error.

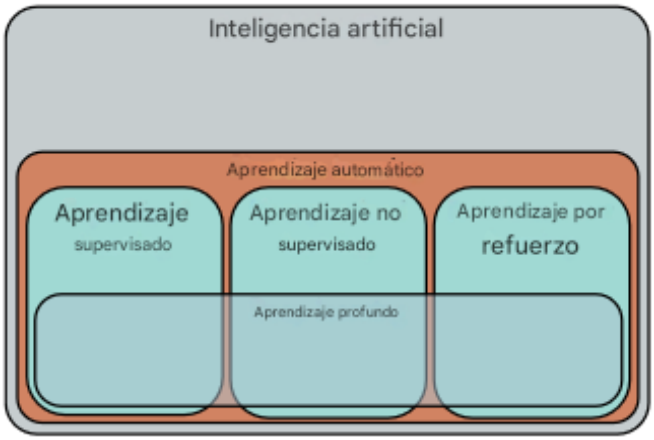
Este método facilita que los sistemas informáticos obtengan conocimientos a partir de datos pasados usando fórmulas matemáticas, tal como árboles de decisiones o modelos de categorización, sin requerir programación específica para cada caso (Vorobioff et al., 2022).

El aprendizaje profundo constituye un enfoque avanzado dentro de la inteligencia artificial, basado en redes neuronales artificiales de múltiples capas diseñadas para replicar ciertos procesos del razonamiento humano. Estas redes se destacan por su capacidad para resolver problemas complejos y manejar datos no estructurados. Su efectividad ha sido demostrada en diversas áreas, entre las que se incluyen:

- Análisis automático de imágenes.
- Identificación y generación de voz.
- Interpretación del lenguaje natural.

En estas áreas, los modelos de aprendizaje profundo superan significativamente el desempeño de los métodos algorítmicos tradicionales (Prince, 2023).

Figura 5



Aprendizaje profundo

Fuente: Prince, 2023. *Understanding Deep Learning.*

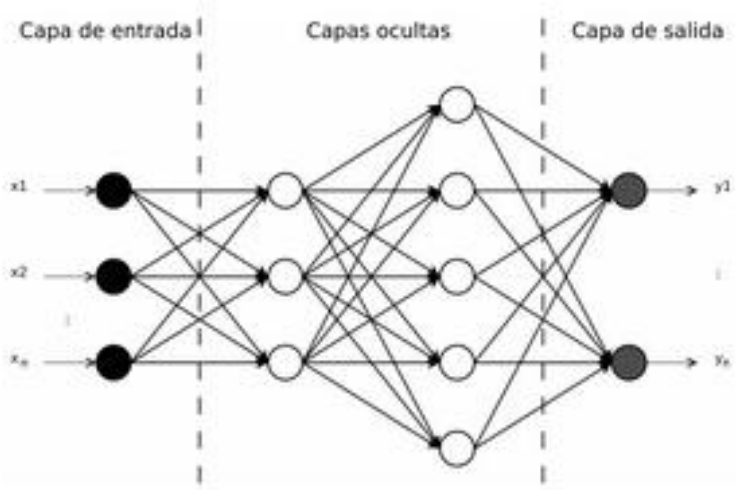
2.3.2.4. Funcionamiento de una red neuronal

Según Vorobioff, Cerrotta y Amadio (2022), una red neuronal puede entenderse como un equipo de trabajo especializado que procesa información imitando el funcionamiento del cerebro humano. Esta estructura está conformada por tres componentes interconectados:

- **El equipo de recepción (capa de entrada):** actúa como interfaz sensorial encargada de recibir y normalizar datos heterogéneos, tales como variables ambientales, señales audiovisuales u otros tipos de entradas.

- **Los analistas especializados (capa oculta):** encargados de procesar y transformar la información recibida, extraer patrones y realizar análisis intermedios.
- **El equipo de conclusiones (capa de salida):** responsable de generar los resultados o respuestas finales basándose en el procesamiento previo.

Figura 6 *Capas de una neurona*



Capas de una neurona

Fuente: Meneses & Alvarado, 2017

Cada neurona artificial en una red neuronal trabaja por su cuenta, haciendo tres cosas clave, es como un mini procesador.

- Recolección de datos (inputs) y estructuración según su peso sináptico.
- Suma lineal de las señales ponderadas.
- Generación de una salida (output) mediante una función de activación.

La adquisición de conocimiento en estas redes se alcanza a través del ajuste repetido de los pesos sinápticos utilizando métodos de optimización, dentro de estos destacan el algoritmo de descenso del gradiente, este proceso facilita que la red aumente de una forma gradual su

nivel de exactitud en cada una de las predicciones a medida que se entrena con información, este parecido a la forma en que los sistemas cognitivos naturales aprenden mediante la experiencia. (Osval et al., 2022).

2.3.2.5. Predecir, comparar y aprender (retropropagación)

Weidman (2019) describe detalladamente el mecanismo mediante el cual una red neuronal artificial aprende, compara y predice resultados a partir de datos. Según el autor, una red neuronal tiene como objetivo fundamental aprender patrones entre los datos de entrada X y las salidas esperadas Y. En esencia, el aprendizaje consiste en encontrar una función f tal que f(X)=P donde P representa las predicciones que idealmente se aproximan lo más posible a Y. El proceso de aprendizaje de una red neuronal se desarrolla en tres fases principales:

- **Paso Adelante (FeedForward):** La red recibe un conjunto de entradas **X** y las procesa secuencialmente a través de múltiples capas. Cada capa aplica una transformación matemática, típicamente una combinación lineal seguida de una función de activación no lineal. Este proceso se expresa como:

$$\boldsymbol{Z^{(l)} = \mathbf{W}^{(l)}\mathbf{A}^{(l-1)} + \mathbf{b}^{(l)} \text{ y } \mathbf{A}^{(l)} = \boldsymbol{\sigma}\left(\mathbf{Z}^{(l)}\right)}$$

  donde $\mathbf{W}^{(l)}$ *y* $\mathbf{b}^{(l)}$ son los pesos y sesgos de la capa $\boldsymbol{l, \sigma}$ es la función de activación, y $\mathbf{A}^{(l)}$representa la activación de dicha capa.

- **Cálculo del Error o descenso de la gradiente (Loss gradient):** Una vez obtenida la predicción **P**, se calcula la función de pérdida $\boldsymbol{L(Y, P)}$, la cual mide la discrepancia entre la salida real y la predicción. Posteriormente, se determina el gradiente de esta función respecto a cada parámetro del modelo:

$$\frac{\boldsymbol{\partial L}}{\boldsymbol{\partial \theta}}$$

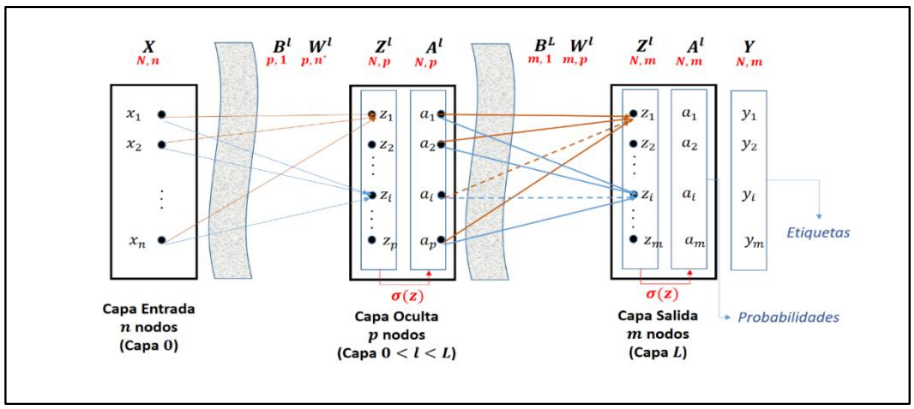
Este gradiente indica cómo varía el error en función de los parámetros **θ**, facilitando la optimización mediante técnicas como descenso del gradiente.

- **Propagación hacia atrás (Backpropagation):** El gradiente calculado se propaga en sentido inverso a través de las capas de la red, ajustando cada uno de los parámetros mediante la regla:

$$\boldsymbol{\theta \leftarrow \theta - \eta \frac{\partial L}{\partial \theta}}$$

A través de múltiples iteraciones de este ciclo feedforward, cálculo del error y backpropagation la red ajusta sus parámetros internos, mejorando así su capacidad predictiva. Se puede considerar como un procedimiento similar al aprendizaje de las personas, en el cual cada fallo ofrece datos importantes para aumentar el rendimiento en el futuro.

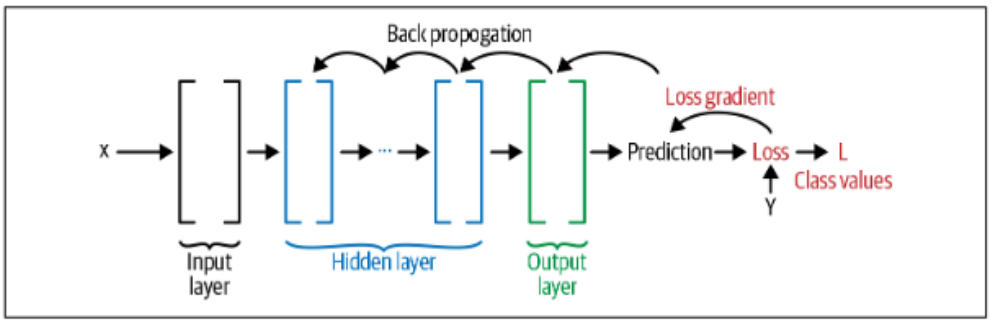
Figura 7



Redes neuronales multicapa

Fuente: Politécnica, 2021.

Figura 8



Retropropagación

Fuente: Weidman, 2019. *Deep Learning from Scratch*.

2.3.2.6. Redes neuronales: Múltiple entrada o salida

Las redes neuronales de múltiples entradas y salidas representan un avance significativo en el aprendizaje automático. Inspiradas en el funcionamiento del cerebro, procesan datos de manera paralela y generan resultados integrados. A diferencia de las redes neuronales convencionales, que operan con una única entrada y salida, estas redes pueden manejar simultáneamente varios tipos de datos y producir resultados armonizados.

Su funcionamiento se basa en el procesamiento distribuido de la información a través de capas interconectadas, permitiendo que cada componente contribuya a la evolución gradual de los datos. Un ejemplo paradigmático de este enfoque se observa en sistemas avanzados de reconocimiento facial, donde la red analiza distintos aspectos, como la geometría facial, las expresiones emocionales y características biométricas, para generar estimaciones coordinadas de identidad, edad, género y estado emocional (Trask, 2019).

2.3.2.7. Clasificación de redes neuronales

Según Vorobioff, Cerrotta y Amadio (2022), las redes neuronales pueden clasificarse desde diversas perspectivas que abarcan su funcionalidad, arquitectura, métodos de aprendizaje y temporalidad, entre otros aspectos. A continuación, se presenta un resumen de esta clasificación:

Tabla 2

Clasificación de redes neuronales

Criterio	Tipo de Red	Características principales	Aplicaciones típicas
Por función	Clasificación	Asigna entradas a categorías discretas (ej: binarias/múltiples clases)	Diagnóstico médico, filtrado de spam
	Regresión	Predice valores continuos	Pronósticos financieros, análisis de mercado
Por arquitectura	Monocapa	Una sola capa de procesamiento (entrada-salida directa)	Problemas linealmente separables
	Multicapa	Múltiples capas ocultas para modelar relaciones no lineales	Visión artificial, NLP
Por aprendizaje	Supervisado	Entrenamiento con datos etiquetados (input-output conocido)	Reconocimiento de patrones
	No supervisado	Descubre patrones intrínsecos sin etiquetas	Segmentación de clientes
	Por refuerzo	Aprendizaje basado en recompensas/penalizaciones	Control robótico
Por tendencia temporal	Estática	Procesamiento sin memoria (solo entrada actual)	Análisis de imágenes estáticas
	Dinámica	Modela dependencias temporales (memoria de estados previos)	Procesamiento de voz

Criterio	Tipo de Red	Características principales	Aplicaciones típicas
Por conexiones	Feedforward	Flujo unidireccional sin ciclos	Clasificación básica
	Recurrente	Conexiones retroalimentadas para capturar dependencias secuenciales	Traducción automática

Fuente: Vorobioff et al., 2022.

2.3.3. Seguridad

2.3.3.1. Conceptualización contemporánea de la seguridad

La seguridad, desde la perspectiva de Jiménez y Díaz (2010), constituye un derecho fundamental cuya ausencia representa una amenaza directa para las personas y las comunidades, dicho concepto requiere un enfoque colaborativo, en el que el Estado actúe como protector, las instituciones desempeñen un rol preventivo y los ciudadanos participen activamente. No obstante, su conceptualización es compleja ya que se trata de un fenómeno multifacético que debe analizarse desde distintas dimensiones tanto económicas, culturales, ambientales y sociopolíticas.

Los métodos clásicos de seguridad, centrados en riesgos externos y orden social, no dan la talla hoy en día. Por eso, se está enfocando hacia estrategias más completas y proactivas. Rico et al. (2020), en su libro Enfoques y gestión en seguridad integral retoman la idea de Font y Ortega (2012) sobre el origen de la seguridad en la necesidad humana, señalando que:

El tema de la seguridad humana muestra que todos los seres humanos están interactuando constantemente en un solo escenario mundial, donde las amenazas surgen por diversas razones: falta de educación, salud, diferencias económicas y falta de respeto a los derechos humanos (p. 170).

2.3.3.2. Aplicación de tecnologías digitales en entornos construidos

Los sistemas ciberfísicos, que integran componentes digitales y físicos, están generando transformaciones significativas en diversos sectores. Su implementación permite la automatización y optimización de procesos críticos, evidenciándose en entornos hospitalarios mediante equipos médicos inteligentes, en la industria a través de procesos automatizados y en la agricultura mediante sistemas de riego autónomos basados en sensores.

Esta innovación impacta tanto en la manufactura como en los servicios esenciales, incluyendo sistemas avanzados de transporte, redes eléctricas autorreparables y dispositivos médicos autónomos. No obstante, su adopción enfrenta desafíos importantes, principalmente relacionados con la escasez de personal cualificado para el desarrollo y mantenimiento de estos sistemas. Las organizaciones presentan dificultades para atraer profesionales especializados, mientras que las instituciones educativas aún no satisfacen completamente la creciente demanda de capacitación en este campo. Adicionalmente, la limitada disponibilidad de laboratorios especializados y sus elevados costos representan un obstáculo significativo para la expansión de estas tecnologías (Chimay & Nazila, 2020).

2.3.3.2.1. Objetivo de la seguridad en entornos ciberfísicos

Según House (2022), el objetivo principal de la seguridad en sistemas ciberfísicos es garantizar la continuidad operacional y proteger integralmente tanto los componentes físicos como digitales en infraestructuras inteligentes. Para cumplir este propósito, la seguridad debe abordar los siguientes aspectos:

- **Disponibilidad de servicios críticos:** asegurar que los servicios esenciales permanezcan operativos de manera continua.

- **Integridad de la información:** garantizar que los datos transmitidos y almacenados no sufran alteraciones.
- **Protección frente a accesos no autorizados:** prevenir intrusiones y asegurar que únicamente personal autorizado acceda a los sistemas.

Adicionalmente, este marco de seguridad contempla el mantenimiento y resguardo de dispositivos del Internet de las Cosas (IoT), incluyendo sensores, unidades de control embebidas y otros componentes conectados, con el fin de asegurar un funcionamiento óptimo y mitigar los riesgos asociados a su integración con plataformas corporativas y servicios en la nube.

2.3.3.2.2. Función y características de los sistemas ciberfísicos

Los sistemas ciberfísicos, conocidos por sus siglas en inglés CPS, se pueden describir como la fusión de capacidades informáticas en objetos materiales, otorgándoles una forma de "inteligencia" que les permite relacionarse con su entorno de forma independiente. Esta fusión propicia que los objetos físicos lleven a cabo decisiones al instante según la información que reciben de su entorno.

Estos sistemas tienen aplicaciones en muchos campos, desde semáforos inteligentes que mejoran la circulación en tiempo real, hasta hospitales que asignan de manera automática dispositivos médicos según lo que requiera cada paciente, o fábricas que suspenden el funcionamiento de una máquina al identificar un posible fallo.

Un CPS integra sensores que recolectan información del entorno físico, redes que envían datos a alta velocidad y actuadores que transforman dicha información en acciones específicas, esta interacción constante se basa entre lo digital y lo físico estableciendo así un

flujo bidireccional que posibilita la toma de decisiones autónoma y en tiempo real. Sin embargo, su implementación demanda un diseño robusto y seguro, ya que un error o un ataque cibernético podría poner en riesgo vidas humanas o paralizar ciudades enteras (Chimay & Nazila, 2020).

Componentes principales de un sistema ciberfísico:

- **Unidades de percepción (sensores):** Dispositivos capaces de cuantificar con alta precisión variables ambientales como temperatura, humedad y movimiento, así como parámetros biométricos como el reconocimiento facial o dactilar (Khaitan & McCalley, 2020).
- **Mecanismos de actuación:** Dispositivos electromecánicos, como servomotores y válvulas solenoides, que ejecutan acciones físicas a partir de señales digitales, transformando energía según lo requiera el sistema (Baheti & Gill, 2020).
- **Núcleo de procesamiento:** Sistemas embebidos que procesan los datos recibidos mediante algoritmos de control adaptativo y aprendizaje automático, lo que les permite tomar decisiones de forma autónoma (Gan et al., 2023).

2.3.3.3. Ciberseguridad

La ciberseguridad ha cobrado gran relevancia debido al crecimiento exponencial de los riesgos y amenazas cibernéticas a nivel global, los cuales impactan los ámbitos político, social y económico. Esta disciplina no se limita a restringir accesos no autorizados, sino que busca garantizar la protección, integridad y disponibilidad continua de la información y de los sistemas tecnológicos, asegurando la continuidad operativa de las organizaciones (Jiménez & Díaz, 2010; House, 2022).

La ciberseguridad moderna requiere una visión integral que considere amenazas externas, vulnerabilidades físicas, contingencias operativas y el factor humano. Esto implica la implementación de infraestructuras robustas, protocolos de contingencia avanzados y una cultura organizacional orientada a la prevención, con el fin de mitigar riesgos, mantener la resiliencia operativa y proteger los activos digitales críticos (House, 2022).

2.3.3.3.1. Reconocimiento facial

La tecnología de reconocimiento facial ha generado un debate significativo en América Latina debido a su implementación en áreas de seguridad, muchas veces sin contar con la regulación adecuada. Países como Brasil, México y El Salvador utilizan estos sistemas para prevenir la delincuencia mediante reconocimiento facial automatizado. Sin embargo, diversas investigaciones indican que dichos sistemas pueden presentar fallos en la identificación de personas de grupos demográficos diversos, lo que podría derivar en arrestos injustos o vulneraciones de derechos fundamentales (Hinestroza, 2024).

A pesar de estos riesgos, la inteligencia artificial aplicada al reconocimiento facial permite optimizar ciertos procesos en el ámbito judicial, como la búsqueda de precedentes, el análisis de casos a partir de datos y la automatización de trámites administrativos, contribuyendo a mejorar la eficiencia sin comprometer los derechos de las personas.

En Europa, la implementación de esta tecnología se encuentra regulada por normativas estrictas, lo que ha permitido reducir los índices de error. En contraste, en América Latina, la adopción de sistemas de reconocimiento facial avanza con insuficiente transparencia y ausencia de análisis detallados sobre sus impactos, lo que genera riesgos importantes, incluyendo el uso potencial de esta tecnología como instrumento de vigilancia masiva, afectando derechos

esenciales como la privacidad, la protección de datos personales y la presunción de inocencia (Hinestroza, 2024).

2.4. Conclusiones del marco teórico

El Marco Teórico evidencia que los sistemas informáticos integrados con dispositivos del Internet de las Cosas permiten la automatización y el control eficiente de procesos, mejorando la gestión de accesos y el registro de información en tiempo real.

Asimismo, las redes neuronales aplicadas al reconocimiento facial y al control de acceso permiten el desarrollo de sistemas inteligentes capaces de aprender patrones, reconocer rostros con precisión y tomar decisiones autónomas, aumentando la eficiencia y confiabilidad de los sistemas.

Finalmente, la seguridad en sistemas informáticos y ciberfísicos es un componente esencial, ya que garantiza la integridad de la información, la protección de datos y el acceso autorizado, mitigando riesgos asociados al mal uso de la tecnología y asegurando la confiabilidad de los sistemas de control de acceso.

En conjunto, estos elementos proporcionan una base teórica sólida para el diseño e implementación de sistemas de control de acceso inteligentes y seguros, destacando la importancia de la integración entre tecnología, aprendizaje automático y medidas de seguridad.

CAPÍTULO III

3. MARCO INVESTIGATIVO

3.1. Introducción

En este capítulo se describió el marco investigativo del estudio, detallando el enfoque y los tipos de investigación que se aplicaron para evaluar la eficiencia y precisión del sistema de reconocimiento facial implementado mediante Raspberry Pi. Asimismo, se analizó la influencia de esta tecnología, basada en redes neuronales, sobre la seguridad en la sala de profesores de la universidad. De igual manera, se presentó la metodología utilizada para la recolección y análisis de datos, así como los métodos y herramientas empleados para validar la funcionalidad y efectividad del sistema propuesto.

3.2. Tipos de investigación

La investigación adoptó un enfoque cuantitativo, al centrarse en la medición de variables numéricas que permitieron evaluar la eficiencia y precisión del sistema de reconocimiento facial basado en Raspberry Pi. Asimismo, se analizó el impacto de esta tecnología en el mejoramiento de las condiciones de seguridad en la sala de profesores. El desarrollo del estudio se sustentó en una combinación de enfoques de investigación aplicada, experimental y tecnológica, los cuales permitieron tanto la implementación de un sistema funcional como la generación de conocimiento aplicable en entornos educativos.

3.2.1. Investigación Experimental

La investigación experimental se caracterizó por la intervención controlada del investigador sobre el objeto de estudio, con el propósito de observar los efectos de dichas acciones y validar las hipótesis previamente planteadas. Desde el paradigma positivista, este

método se consideró uno de los más rigurosos para la generación de conocimiento científico, ya que permitió el control de variables y el establecimiento de relaciones causales (Bernal, 2010).

En el estudio se evaluó el proceso de identificación de rostros mediante redes neuronales, comparando el desempeño de los métodos HOG y CNN en términos de eficacia y seguridad. Se analizaron factores como la iluminación, la distancia de la cámara y la calidad de las imágenes, con el fin de determinar cuál de los dos métodos alcanzó un mejor equilibrio entre precisión, recall, F1-score y velocidad de procesamiento en la Raspberry Pi.

Los resultados se analizaron mediante métricas concretas de rendimiento aplicadas a los modelos de reconocimiento facial, lo que permitió fundamentar decisiones técnicas orientadas a aplicaciones prácticas, como sistemas de vigilancia o control de acceso.

3.2.2. Investigación Aplicada

El método se desarrolló de manera gradual mediante evaluación, diseño de soluciones y pruebas preliminares, con el objetivo de aplicar la teoría a la práctica y lograr mejoras concretas. Su influencia se evidenció en la optimización de procesos, en la solución de problemas cotidianos y en el mejoramiento de la calidad de vida de los usuarios, demostrando que la ciencia puede constituyese como un instrumento esencial para el avance humano (Vásquez et al., 2023).

La investigación se enmarcó en el enfoque aplicado, dado que se tomaron conocimientos teóricos sobre reconocimiento facial y tecnologías embebidas para desarrollar una solución concreta: un sistema de control de acceso mediante Raspberry Pi, adaptado a las necesidades de seguridad de la sala de profesores de la ULEAM Extensión El Carmen. Este

enfoque permitió transformar la teoría en una herramienta funcional con impacto directo en un entorno real.

3.2.3. Investigación Tecnológica

La indagación tecnológica se caracterizó por un enfoque ordenado, basado en prueba y error, que utilizó métodos específicos para encontrar soluciones prácticas y generar productos orientados a satisfacer necesidades tecnológicas concretas. Este enfoque integró conocimientos técnicos y científicos para diseñar, mejorar o crear procesos, objetos o servicios aplicables tanto al ámbito académico como al social. Se combinaron observaciones, análisis y acciones prácticas, adoptando procedimientos estructurados que abarcaron desde la concepción hasta la producción o adaptación de tecnologías (Barbachán, 2021).

En el proyecto se desarrolló un prototipo funcional mediante el uso de una Raspberry Pi con cámara y un software diseñado con algoritmos de aprendizaje automático en un sistema embebido. El proceso se ejecutó en etapas que incluyeron la selección y entrenamiento de modelos de redes neuronales, el preprocesamiento de imágenes para garantizar la calidad de los resultados, así como la integración con bases de datos y servicios complementarios.

Asimismo, se evaluó el rendimiento del sistema en escenarios reales, identificando limitaciones y oportunidades de mejora. Como resultado, se obtuvo un sistema de seguridad basado en reconocimiento facial, funcional, escalable y debidamente documentado, que demostró la viabilidad de aplicar tecnologías avanzadas en entornos educativos para fortalecer la seguridad y el control de acceso.

3.3. Métodos de investigación

Para poner en marcha el sistema de seguridad basado en reconocimiento facial mediante redes neuronales en una Raspberry Pi, se utilizó un plan metodológico de carácter mixto. Este plan combinó análisis y síntesis e integró enfoques cuantitativos y cualitativos, con el fin de obtener una visión clara y completa del desarrollo del proyecto.

3.3.1. Método cuantitativo

El enfoque cuantitativo se caracterizó por ser un método estructurado y verificable, en el que cada etapa del proceso investigativo se desarrolló de manera ordenada y sistemática. Este tipo de investigación partió de una idea inicial que se depuró mediante la formulación de preguntas e hipótesis medibles, sustentadas en una base teórica sólida.

Mediante diseños específicos, este método permitió cuantificar variables, aplicar instrumentos estandarizados de medición y analizar datos numéricos para validar o refutar los supuestos. Su fortaleza radicó en la objetividad, la replicabilidad y la capacidad de generalizar hallazgos, manteniendo un enfoque deductivo que transitó de lo general a lo particular (Hernández et al., 2010).

En la tesis se midió el desempeño del sistema de reconocimiento facial implementado en una Raspberry Pi bajo un enfoque cuantitativo. Para ello, se recopilaron datos relacionados con precisión, recall, F1-score, velocidad de procesamiento y consumo de recursos. Las pruebas se realizaron en diferentes condiciones de iluminación, ángulos de captura y distancias de la cámara, lo que permitió evaluar comparativamente el rendimiento de los algoritmos HOG y CNN.

3.3.2. Método cualitativo

El enfoque avanzó de manera progresiva mediante evaluación, diseño de soluciones y pruebas iniciales, con el objetivo de aplicar la teoría a la práctica y generar mejoras concretas. Sus efectos se evidenciaron en la optimización de procesos, en la resolución de problemas cotidianos y en el mejoramiento de la calidad de vida de los usuarios, confirmando que la ciencia puede constituyese como una herramienta clave para el progreso humano (Vásquez et al., 2023).

En el estudio se indagó en las percepciones y experiencias de los docentes mediante encuestas y entrevistas estructuradas. Estos instrumentos permitieron recopilar información cualitativa que no podía ser expresada únicamente en términos numéricos, incluyendo necesidades de seguridad, deficiencias percibidas en el sistema actual, preocupaciones sobre la protección de datos y sugerencias relacionadas con el nuevo sistema. Las entrevistas proporcionaron información detallada y profunda, mientras que las encuestas ofrecieron una visión general del contexto. La combinación de ambos instrumentos facilitó la toma de decisiones fundamentadas durante el diseño del sistema.

3.3.3. Método analítico-sintético

El método analítico-sintético constituyó un enfoque de investigación que permitió abordar fenómenos complejos mediante un proceso secuencial. En la primera etapa, el objeto de estudio se descompuso en sus componentes fundamentales para ser analizados de manera detallada, identificando sus características, relaciones y comportamientos particulares. En la segunda etapa, dichos elementos previamente analizados se integraron nuevamente con el objetivo de comprender el sistema en su totalidad y obtener una visión global de su

funcionamiento. Este método resultó especialmente útil en el estudio de sistemas tecnológicos complejos, como el desarrollado en esta investigación (Rodríguez, 2007).

En el trabajo se aplicó el método analítico-sintético para examinar componentes tales como las redes neuronales, la Raspberry Pi y los algoritmos de detección facial. Este análisis permitió identificar sus características técnicas y la manera en que se integraron en un sistema funcional. La aplicación de este enfoque contribuyó a desarrollar la solución de forma ordenada y a garantizar su adecuación a las necesidades de seguridad planteadas en el contexto educativo.

3.4. Fuentes de información de datos

3.4.1. Encuesta

El cuestionario o encuesta es visto como uno de los instrumentos más empleados en investigación, ya que facilita la recolección de datos de manera sistemática y estandarizada. Este se compone de un conjunto organizado de preguntas diseñadas para examinar variables de interés, según con los objetivos del estudio definidos y las hipótesis propuestas. Este dispositivo se distingue por su eficacia ya que agiliza la recolección de datos de forma eficaz en diferentes escenarios asegurando la comparabilidad de los datos; el cuestionario es un instrumento adaptable que, al ser apropiadamente desarrollado, proporciona resultados fiables y generalizables (Hernández et al., 2010).

La recolección de datos se realizó a través de Google Forms, una plataforma diseñada para facilitar la recopilación de información en teléfonos móviles y computadoras de escritorio, asegurando que los participantes pudieran acceder a ella de manera sencilla y en cualquier momento. La encuesta fue respondida por los 12 docentes que conformaron el grupo de estudio,

quienes participaron de manera continua en el ámbito educativo en el que se pretendía implementar el sistema de control de acceso.

Este grupo fue seleccionado debido a su conocimiento profundo del funcionamiento interno de la institución, lo que permitió obtener datos cuantitativos relevantes y representativos para el análisis. Además, el uso de Google Forms facilitó la organización, recopilación y posterior análisis de los resultados.

3.4.2. Entrevista

La entrevista emerge como un recurso esencial para recolectar datos cualitativos, dado que promueve la interacción directa entre el investigador y el participante. En resumen, esto ayuda a adquirir información valiosa mediante un diálogo más o menos planificado, donde el entrevistador orienta la conversación con preguntas diseñadas para examinar diferentes facetas del fenómeno que se está estudiando. Naturalmente, a diferencia de otros métodos, la entrevista no se limita a las respuestas verbales; también posibilita la observación de elementos como la entonación, los gestos o las posturas, y todo esto, en esencia, potencia destacada la interpretación de la información (Bernal, 2010).

Las entrevistas se realizaron con dos docentes de mayor trayectoria y experiencia en la carrera de Ingeniería de Software de la ULEAM, Extensión El Carmen, quienes fueron seleccionados como muestra por conveniencia debido a su amplio conocimiento en el área y su familiaridad con las necesidades del entorno educativo. Mediante un formato de preguntas abiertas, se recopiló información cualitativa basada en la experiencia docente, relacionada con la seguridad, los desafíos existentes en la sala de profesores y la implementación del sistema de control de acceso.

3.5. Estrategia operacional para la recolección de datos

3.5.1. Población

En el presente proyecto, la población objeto de estudio estuvo conformada por los 12 docentes que integraron la sala de profesores de la carrera de Tecnologías de la Información y Software de la ULEAM Extensión El Carmen. Este grupo constituyó el entorno principal donde se implementó el sistema informático con redes neuronales para fortalecer la seguridad del espacio. Dado que fueron los usuarios directos del sistema, su interacción con la tecnología propuesta resultó fundamental para evaluar su eficacia en el control de acceso y en la protección de sus pertenencias, lo que, a su vez, garantizó un ambiente confiable dentro de la institución.

3.5.2. Muestra

Debido al pequeño tamaño de la población, compuesta por 12 docentes del área de Tecnología de la Información y Software, se empleó un muestreo por conveniencia. La encuesta se aplicó a todos los docentes, lo que permitió una recolección completa de información sobre sus opiniones y requerimientos respecto a la seguridad en la sala de profesores.

Adicionalmente, se realizó una entrevista semiestructurada a dos docentes con mayor antigüedad en el departamento, seleccionados por su experiencia institucional y conocimiento profundo del funcionamiento de la sala. Esta técnica cualitativa permitió profundizar en aspectos específicos de la gestión de seguridad que no pudieron ser capturados mediante la encuesta.

Finalmente, se llevó a cabo un examen previo de los instrumentos de recolección de información con el fin de confirmar su adecuación y eficiencia, asegurando que los datos recolectados fueran significativos y útiles para los objetivos de la investigación.

3.5.3. Análisis de las herramientas de recolección de datos a utilizar

3.5.3.1. Encuesta

La encuesta se diseñó con un enfoque práctico, con el objetivo de recoger datos de manera eficiente. Se aplicó a los 12 docentes del programa de Ingeniería de Software durante un período de tres días, utilizando la plataforma Google Forms, la cual permitió que los participantes respondieran desde sus dispositivos móviles o computadoras. Esta herramienta facilitó la recolección automática de los datos y generó gráficos estadísticos que permitieron identificar patrones y tendencias relevantes.

3.5.3.2. Entrevista

La técnica de entrevista se aplicó a dos docentes con amplia trayectoria en la carrera de Ingeniería de Software, aportando una perspectiva basada en la experiencia profesional. Las entrevistas se desarrollaron en un ambiente estructurado y reflexivo, lo que permitió obtener información detallada sobre percepciones, inquietudes y sugerencias relacionadas con la seguridad y la funcionalidad del sistema propuesto. Aunque el número de entrevistas fue limitado, la profundidad de la información recopilada complementó eficazmente los resultados de la encuesta, equilibrando los enfoques cuantitativo y cualitativo y ofreciendo una visión integral del problema investigado.

3.5.3.3. Estructura de los instrumentos de recolección de datos aplicados

Para la recolección de datos se emplearon dos herramientas complementarias. La encuesta, realizada mediante la plataforma Google Forms, incluyó preguntas de tipo múltiple y cerrado, lo que permitió recopilar de manera eficiente los resultados numéricos de los 12 docentes.

Como complemento, se llevaron a cabo entrevistas semiestructuradas con dos docentes de mayor trayectoria en la carrera, siguiendo un guion flexible que facilitó la exploración de percepciones detalladas sobre la seguridad institucional y el sistema propuesto.

Esta estrategia metodológica permitió comparar las tendencias generales identificadas en la encuesta con las perspectivas cualitativas obtenidas en las entrevistas, lo que enriqueció el análisis y proporcionó información relevante para ajustar y mejorar el sistema de reconocimiento facial.

3.5.4. Plan de recolección de datos

Tabla 3

Cronograma de actividades

Cronograma		
Fecha	**Actividad**	**Resultado Esperado**
03/05/2025	Programación de la encuesta	Encuesta estructurada y lista para aplicar
05/05/2025	Programación de la entrevista	Preguntas validadas y lista para aplicar
07/05/2025	Aplicación de la encuesta	Encuestas aplicadas a la muestra definida
07/05/2025	Aplicación de la entrevista	Entrevistas realizadas y transcritas

Cronograma		
14/05/2025	Análisis de resultados	Datos listos para ser usados

3.6. Análisis y presentación de resultados

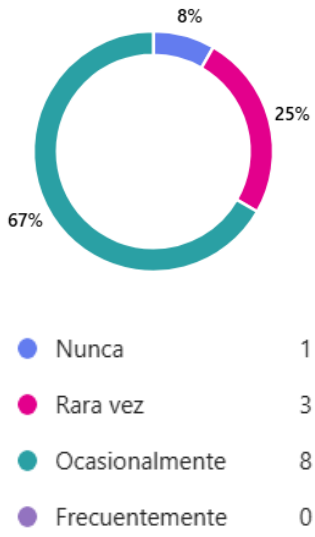
3.6.1. Tabulación

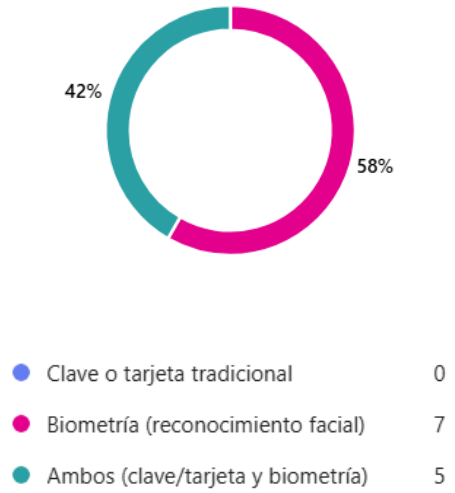
a) Encuesta

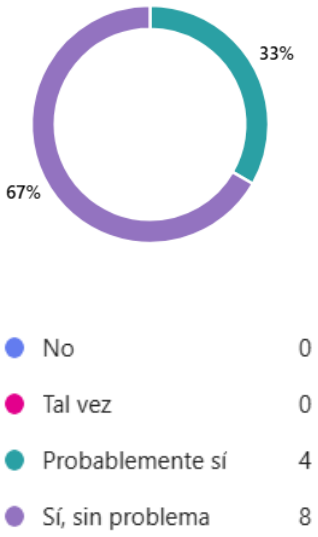
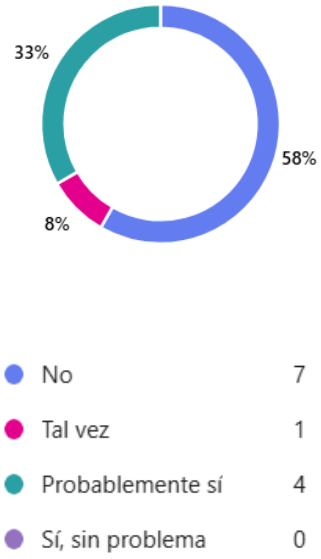
Tabla 4

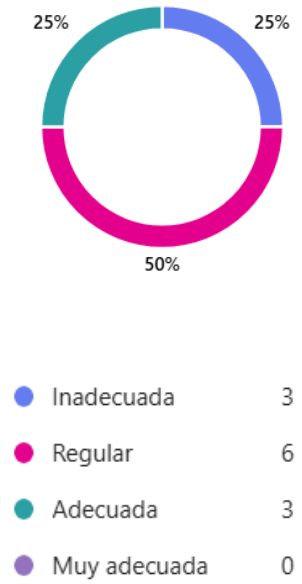
Análisis de las respuestas de la encuesta aplicada a los profesores

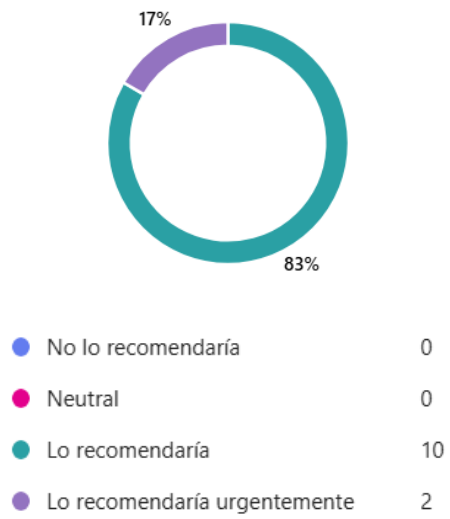
Pregunta	Gráfico	Interpretación
1. ¿Considera necesario implementar un sistema automatizado de control de acceso en la sala de profesores de TI/Software?		Casi todos los profesores están convencidos de que hace falta un sistema automático para controlar las entradas, y eso, la verdad, muestra que están realmente preocupados por la seguridad en la sala de profesores.

Pregunta	Gráfico	Interpretación
2.¿Qué tan importante es para usted la seguridad de los equipos y documentos dentro de la sala de profesores?		Los docentes afirman que los resultados son muy importantes porque permiten proteger tanto datos personales como sus dispositivos inteligentes y archivos importantes.
3.¿Ha tenido experiencias con accesos no autorizados a la sala de profesores?		Un buen grupo de los encuestados contó que ha lidiado con accesos no autorizados, lo que deja clarísimo que el sistema actual tiene fallos. Así que, bueno, está más que justificado que se necesita un método más seguro y confiable.

Pregunta	Gráfico	Interpretación
4. ¿Qué tipo de sistema de acceso prefiere?		Los resultados muestran que el reconocimiento facial es una de las opciones favoritas, y no es para menos, porque es fácil de usar y bastante automático. Eso sí, también hay quienes le ven potencial a otras alternativas, como tarjetas o contraseñas, así que no estaría mal considerar una solución que mezcle un poco de todo.
5. ¿Qué tan importante considera que es registrar los datos de acceso (horarios e intentos fallidos)?		La gran parte de los asistentes ve como algo fundamental anotar los detalles de ingreso, lo que muestra que aprecian la seguimiento y la supervisión del empleo del lugar..

Pregunta	Gráfico	Interpretación
6. ¿Estaría dispuesto a registrar su rostro en una base de datos institucional para utilizar este sistema?		Una gran parte de los profesores estaría abierta a registrar su imagen, lo que facilita la puesta en marcha del sistema de identificación facial..
7. ¿Cree que el uso de este sistema podría afectar su privacidad?		De acuerdo a la privacidad los docentes expresan sus preocupaciones, pues es un aspecto muy importante que debe ser almacenado de forma segura, donde exista un acceso restringido y uso exclusivo de la institución.

Pregunta	Gráfico	Interpretación
8. ¿Cómo calificaría la infraestructura tecnológica actual de la sala para soportar el nuevo sistema?		Las respuestas muestran una visión variada o restringida acerca de la tecnología disponible en este momento. Esto implica que podría ser importante llevar a cabo actualizaciones en la conectividad, el suministro eléctrico o los dispositivos para asegurar el adecuado desempeño del sistema..
9. ¿Qué nivel de importancia le atribuye a la rapidez con la que el sistema de reconocimiento facial permite el acceso a la sala?		Los profesores tienen claro que la velocidad es clave: el sistema tiene que ser rápido y eficiente, sin dar muchas vueltas. La verdad, me parece interesante cómo la mayoría de los encuestados dice que recomendaría este sistema para otras áreas, lo que da a entender que el proyecto podría crecer y convertirse en algo sólido para toda la institución.

Pregunta	Gráfico	Interpretación
10. ¿Recomendaría la implementación de este proyecto a otros departamentos de la universidad?		La verdad, me parece interesante cómo la mayoría de los encuestados dice que recomendaría este sistema para otras áreas, lo que da a entender que el proyecto podría crecer y convertirse en algo sólido para toda la institución.

b) Entrevista

Tabla 5

Análisis de los resultados de la entrevista aplicada al profesor y coordinador de la carrera de TI/Software.

Pregunta	Profesor	Coordinador	Análisis
1. Desde su experiencia, ¿cuáles son los principales riesgos de seguridad en el acceso actual a la sala de profesores de TI/Software?	Actualmente no hay ningún sistema de seguridad; la cerradura no funciona, lo que significa que cualquier	Que los riesgos corresponden a las pertenencias personales debió a que no hay una seguridad adecuada en la sala.	Los dos entrevistados están de acuerdo en la ausencia de acciones eficaces para tratar el problema y la seguridad en el espacio de la sala de docentes. Si indica que la no cerradura funciona, lo que implica que expuso incluyen pertenencias y pertenencias. individuales al

Pregunta	Profesor	Coordinador	Análisis
	persona puede ingresar.		peligro de remoción. Esto es resalta la información urgentísima necesidad de poner en marcha un del sistema automatizado de procesos de automatización automatizado de regulación de accesos.
2. ¿Qué ventajas y desventajas observa en implementar un sistema de reconocimiento facial con redes neuronales, en comparación con métodos tradicionales como claves o tarjetas?	Tendría varias ventajas, como el hecho de solo acercarse para poder ingresar a un determinado lugar o acceder a cuentas bancarias, entre otros. Como desventaja, requiere procesar grandes volúmenes de datos.	Ventaja considero que es un proyecto de innovación y un sistema rápido, como desventaja toca ver la brecha de privacidad.	La rapidez, la facilidad de uso y lo innovador del sistema son un gran punto a favor... pero, bueno, dos de los profesores señalaron problemas serios, como la falta de privacidad y el problema de manejar datos, que, a decir verdad, plantea retos éticos y técnicos que no son poca cosa.
3. ¿Considera que la iluminación como un	El ángulo desde donde se realice	Considero que sí, se basa en la tecnología	Ambos participantes coinciden en que factores

Pregunta	Profesor	Coordinador	Análisis
factor de entorno puede afectar el funcionamiento del sistema de reconocimiento facial?	la captura y los accesorios que la persona pueda tener en su rostro pueden afectar el reconocimiento facial.	o si la cámara tiene visión nocturna.	como la iluminación, el ángulo de la toma y elementos en el rostro pueden afectar la eficiencia del sistema. El responsable señala que un modelo de cámara con visión nocturna, por decirlo así, puede mitigar este problema, lo que resalta lo importante que es elegir el hardware adecuado.
4. Según su criterio, ¿qué requisitos técnicos debe cumplir el sistema para ser viable en la ULEAM extensión El Carmen?	Un buen equipo de reconocimiento facial, que las imágenes estén bien alineadas, bien recortadas.	Debe ser altamente fiable ya que he visto que algunos sistemas son vulnerables.	Los entrevistados coinciden en la necesidad de contar con hardware confiable, imágenes bien procesadas el sistema tiene que ser preciso y confiable, o sea, el prototipo necesita estar bien pulido, optimizado y entrenado a fondo para que funcione como debe en el entorno universitario..
5. ¿Qué desafíos institucionales anticipa para su implementación de este sistema (por	El uso que se les pueda dar, como el control de	En la parte de los costos y el modelo que se vaya a utilizar, no considero que se haga capacitación ya	El docente subraya la aplicación institucional de la plataforma como un beneficio, específicamente para el seguimiento de asistencia.

Pregunta	Profesor	Coordinador	Análisis
ejemplo: capacitación del personal, costos, ¿resistencia al cambio)?	asistencias a todo el personal.	que somos ingenieros de tecnologías	Por otro lado, el coordinador centra su atención en los gastos y la oposición al cambio. Ambos reducen la importancia de la formación, partiendo de la premisa de que el equipo ya tiene habilidades técnicas previas.
6. ¿Cómo debería manejarse el acceso de personas externas autorizadas como personal administrativo o invitados)?	Si están autorizadas, si constan en la base de datos; si no, son autorizadas llevando un registro para personas externas donde se registren varios datos importantes.	El sistema debería ser implementado para docentes, ya para personas administrativas o invitados debería recurrir al sistema manual o tradicional.	Hay una diferencia de opiniones: el docente sugiere incluir a individuos ajenos a través de un registro y base de datos, por otro lado, el coordinador prefiere conservar un sistema manual convencional para estas situaciones. Esto indica que la resolución definitiva debe ser versátil y capaz de adaptarse según las clases de usuario.
7. ¿Cuál es su opinión sobre la sensibilidad y el correcto manejo de los datos	De que estos datos puedan ser usados para otros fines.	En todo tipo de sistemas de reconocimiento se debe registrar y se necesitan imágenes, pero al ser de la	El profesor muestra preocupación por el posible uso indebido de los datos biométricos, mientras que el coordinador, aunque se reconoce que el tema de los

Pregunta	Profesor	Coordinador	Análisis
biométricos que serán almacenados?		universidad no vería tan sensible el manejo de datos biométricos.	datos es delicado, la verdad es que, al ser un sistema interno de la universidad, el riesgo se reduce un poco..
8. ¿Qué protocolos de emergencia deberían contemplarse en el sistema? (por ejemplo: fallos técnicos, intentos de acceso no autorizado)	Alertas y bloqueos.	Debemos mantener el tema de acceso manual, ya que suelen haber cortes de luz y con los intentos no autorizados el sistema debe reconocer a los de la carrera para dar acceso.	Tanto los profesores como el coordinador coinciden en que no se pueden ignorar los problemas eléctricos ni los accesos no autorizados. Por eso, proponen alternativas manuales y sistemas de alerta, lo que, a decir verdad, muestra que hace falta un plan de contingencia sólido.
9. ¿Qué aspectos éticos o legales se debe considerar al implementar un sistema con inteligencia artificial en el entorno universitario?	Protección y privacidad de los datos, responsabilidad y seguridad.	Se debe revisar la normativa en cuanto el uso de datos personales para que el proyecto cumpla con esos parámetros.	La protección de datos y el cumplimiento de las normas vigentes son puntos clave, el coordinador insiste en que hay que revisar bien la normativa sobre el manejo de información personal, y eso resalta la responsabilidad ética y legal que lleva este proyecto.

Pregunta	Profesor	Coordinador	Análisis
10. ¿Qué recomendaciones clave daría a los desarrolladores del proyecto para garantizar su éxito?	Realizar una investigación exhaustiva del tema, tener bien claros cuáles son los recursos y requerimientos necesarios para que sea un proyecto de calidad, utilizando las tendencias tecnológicas actuales.	Un buen entrenamiento a los modelos y tener el sistema manual en caso de haber fallos eléctricos y con respecto a la implementación que realice varias pruebas, de pronto podría que entrene al modelo para que de apertura de los docentes en un tiempo específico por ejemplo que el docente se acerque y alce la mano y lo registre.	Las sugerencias indican la investigación detallada y las pruebas constantes, excelente preparación del modelo y capacidad para incluir funciones avanzadas como gestos físicos, esto señala que la relevancia de un desarrollo iterativo orientado por solicitudes reales y la implicación activa de los usuarios.

3.6.2. Presentación y descripción de los resultados obtenidos

Del análisis conjunto de la encuesta (Tabla 3) y las entrevistas (Tabla 4), se evidenció que la principal problemática en la sala de profesores correspondió a la ausencia de un sistema de seguridad efectivo. La mayoría de los docentes consideró necesaria la implementación de un sistema automatizado (pregunta 1), valorando especialmente la protección de equipos y documentos (pregunta 2). Esta percepción coincidió con lo señalado por los entrevistados, quienes confirmaron que actualmente no existía control alguno de ingreso.

Con respecto a la viabilidad del sistema propuesto, las preguntas 4, 5 y 6 de la encuesta mostraron que los docentes se inclinaron por el uso del reconocimiento facial, principalmente por su eficiencia y automatización. No obstante, también consideraron fundamental llevar un registro de los accesos y de los errores, con el fin de mantener un control adecuado. Los docentes enfatizaron la necesidad de contar con equipos de calidad y una correcta alineación de las imágenes, al tiempo que señalaron preocupaciones relacionadas con la privacidad y cierta resistencia al cambio, factores habituales en este tipo de implementaciones.

La información obtenida a partir de los datos biométricos de la encuesta y las entrevistas resaltó inquietudes vinculadas con la privacidad, enfatizando la necesidad de establecer políticas claras sobre la protección de los datos. Asimismo, se evidenció que, aunque la rapidez del sistema constituyó una ventaja significativa, era necesario implementar mejoras continuas.

Por otro lado, la pregunta 10 mostró una actitud positiva respecto a la posibilidad de escalar el proyecto, siempre que se consideraran adecuadamente los aspectos técnicos, éticos y legales. Los entrevistados recomendaron realizar pruebas exhaustivas, prever posibles fallos y establecer protocolos de emergencia para garantizar la correcta implementación del sistema.

3.6.3. Informe final del análisis de los datos

Tanto las encuestas como las entrevistas evidenciaron la necesidad de mejorar la seguridad en la sala de profesores de TI y Software, dado que el sistema actual de control de acceso no cumplía con los requerimientos esperados. Los docentes mostraron disposición para utilizar tecnologías como el reconocimiento facial, valorando principalmente su rapidez, automatización y capacidad de registrar los accesos. No obstante, también manifestaron preocupaciones relacionadas con la privacidad y el estado de la infraestructura existente.

Las entrevistas reforzaron estos hallazgos, enfatizando la necesidad de contar con equipos adecuados, planes de contingencia y políticas claras para la gestión de datos biométricos. En síntesis, se concluyó que el sistema era factible, siempre que se consideraran cuidadosamente los aspectos técnicos, éticos y operativos para garantizar su correcto funcionamiento.

CAPÍTULO IV

4. MARCO PROPOSITIVO

4.1. Introducción

En este proceso se identificaron y valoraron los componentes fundamentales del sistema de reconocimiento facial, cuyo objetivo consistió en fortalecer la seguridad en la sala de profesores de TI y Software. Para alcanzar dicho objetivo, se consideró esencial disponer de los recursos humanos, tecnológicos y económicos necesarios para garantizar la ejecución exitosa del proyecto.

Durante la aplicación de la metodología, se analizaron las condiciones físicas y técnicas del entorno, incluyendo factores como la iluminación, los accesos y las posibles vulnerabilidades. Mediante la comparación de diversos dispositivos y herramientas, se seleccionaron aquellos más adecuados, tales como cámaras compatibles con Raspberry Pi, módulos de procesamiento de imágenes y elementos de control de acceso, como cerraduras eléctricas.

Con base en una evaluación comparativa de técnicas, se determinaron los dispositivos más apropiados para asegurar una implementación segura y operativa, centrada en la protección del personal y los recursos de la oficina.

4.2. Descripción de la propuesta

La propuesta consistió en desarrollar un sistema informático basado en redes neuronales para reforzar el control de acceso en la sala de profesores de la carrera de TI y Software de la Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen. El objetivo principal fue

mejorar la seguridad mediante un sistema capaz de identificar automáticamente a los usuarios autorizados, asegurando que únicamente el personal registrado pudiera acceder al área.

Se realizó un estudio detallado del entorno para determinar los puntos estratégicos de ubicación de la cámara, la cual se conectó a una Raspberry Pi con capacidad suficiente para ejecutar el modelo de reconocimiento facial seleccionado. La cámara se instaló en la puerta principal con el fin de cubrir eficazmente la zona de acceso, minimizando los puntos ciegos y garantizando el funcionamiento adecuado del sistema.

4.2.1. Justificación técnica de los modelos de reconocimiento facial

El sistema integrará dos enfoques de reconocimiento facial evaluados para determinar su aplicabilidad:

HOG + SVM:

- HOG (Histogram of Oriented Gradients) es un método de extracción de características que identifica patrones de bordes y gradientes en las imágenes faciales.
- SVM (Support Vector Machine) funciona como clasificador, determinando si la imagen corresponde a un rostro registrado.
- Esta unión proporciona velocidad y efectividad, permitiendo la manipulación de imágenes al instante en la Raspberry Pi 5. No obstante, su exactitud se ve afectada por cambios en la iluminación, las expresiones del rostro o diferentes perspectivas.

CNN (Convolutional Neural Networks):

- CNN permite aprender automáticamente las representaciones faciales directamente de las imágenes, sin necesidad de diseño manual de características.
- Ofrece mayor precisión y robustez, reduciendo falsos positivos y negativos incluso ante cambios de iluminación, posturas y expresiones faciales.

Aunque estos modelos requirieron mayor potencia computacional, se consideró conveniente emplearlos para garantizar un acceso seguro y confiable, priorizando la precisión sobre la velocidad. La selección de los modelos se basó en un análisis detallado de su rendimiento: el modelo HOG + SVM resultó adecuado cuando se requirió rapidez y el hardware presentó limitaciones, mientras que la CNN se adoptó como opción principal debido a su mayor precisión y confiabilidad, contribuyendo así al cumplimiento de los objetivos de seguridad establecidos.

4.3. Determinación de recursos

Para crear el sistema que regule el acceso, se reconocieron elementos tecnológicos como la Raspberry Pi 5, una cámara digital, una cerradura eléctrica y piezas electrónicas básicas, además de software como OpenCV. La ejecución del proyecto será responsabilidad de la estudiante investigadora, supervisada por el docente tutor. También se calculó el financiamiento requerido. Esta estrategia completa pretende asegurar un sistema operativo, eficaz y sostenible que mejore la seguridad en el aula de profesores.

4.3.1. Humanos

Tabla 6

Recursos Humanos

Personal	Función
Ingeniero en Sistemas	Responsable del desarrollo e implementación del sistema en Raspberry Pi.
Científico de Datos	Diseña, entrena y optimiza el modelo de red neuronal.
Administrador del sistema	Registra usuarios, gestiona el sistema y supervisa el funcionamiento general.
Usuario Final (Docente)	Interactúa con el sistema para el reconocimiento facial y control de acceso.

4.3.2. Tecnológicos

Los instrumentos tecnológicos son esenciales para asegurar el rendimiento adecuado y seguro del sistema sugerido. La elección de estos componentes se llevó a cabo basándose en su adecuación, eficacia y acceso en el mercado regional.

Tabla 7

Recursos Tecnológicos

Hardware principal	Descripción
Raspberry Pi 5 (8 GB RAM)	Unidad central de procesamiento que ejecutará el sistema de reconocimiento facial y controlará los eventos de acceso.
Cámara web full HD	Para la captura de imágenes faciales, incluso en condiciones de baja iluminación.
Tarjeta microSD	Almacenamiento del sistema operativo y la base de datos local de rostros.
Fuente de alimentación de 5V 5A (USB-C) para Raspberry Pi	Proporciona energía estable y segura.
Cerradura eléctrica QWORK 12V fail-secure	Dispositivo físico de seguridad que controla el acceso.

Hardware principal	Descripción
Diodo 1N4007	Protección contra retroalimentación de voltaje.
Cables jumper macho-hembra, hembra-hembra, macho-macho.	Elementos auxiliares para la conexión y pruebas del circuito.
Software y herramientas:	**Descripción**
OpenCV	Un conjunto de herramientas súper útil para visión artificial, enfocado en trabajar con imágenes.
face_recognition	Interfaz de programación en Python sustentada por dlib para identificar rostros.
Python	Lenguaje de programación principal para la lógica del sistema.
IDE Thonny	Para el desarrollo y depuración del código.
Sistema operativo Raspberry Pi OS	Un sistema operativo basado en Debian, optimizado para la Raspberry Pi y compatible con todas las herramientas que necesitamos.

4.3.3. Económicos

El presupuesto estimado para el desarrollo del sistema fue calculado considerando la compra de componentes electrónicos, dispositivos principales y materiales auxiliares. A continuación, se presenta un desglose aproximado de los costos en dólares estadounidenses (USD):

Tabla 8

Recursos Económicos

Elemento	Costo estimado (USD)
1 RasTech Raspberry Pi 5 Kit 8GB RAM	175,00
1 Cámara web full HD	23,00

Elemento	Costo estimado (USD)
1 Tarjeta microSD (128GB)	20,00
1 Fuente de alimentación 5V 5A(27W)	17,24
1 Módulo relé de 3V (1 canal)	2,39
1 Diodo 1N4007	0,09
1 Cerradura eléctrica 12V	32,60
36 cables jumper hembra-hembra, macho-macho, macho-hembra	3, 12
1 cable HDMI a micro HDMI	3,48
1 Adaptador 12V 2A	4,26
1 Caja de paso 15x15x9cm	7,79
5m Cable Flx.14 negro y 5m rojo	4,00
Iva 15%	38,94
Envío	5,50
Mano de obra profesional (834 h × 5 USD/h)	4.170,00
TOTAL	**$ 4.467,64**

4.4. Desarrollo en cascada

4.4.1. Fase I: Recolección de Requisitos.

En la primera etapa se recopilaron los requerimientos del sistema, tanto funcionales como no funcionales. Para ello, se realizaron entrevistas con dos docentes, se efectuaron observaciones directas en el entorno de la sala y se revisaron documentos existentes. Estos datos resultaron fundamentales para definir las características básicas y los estándares de calidad que el sistema debía cumplir.

Tabla 9

Técnicas utilizadas para la recolección de requisitos en el sistema de reconocimiento facial.

Técnica	Objetivo	Herramientas / Métodos empleados
Entrevistas	Recopilar requerimientos funcionales y no funcionales con usuarios clave (administradores, docentes).	Entrevistas directas con personal administrativo y docentes.
Observación directa	Comprender el entorno físico y uso del espacio de la sala de profesores para identificar necesidades de control de acceso.	Observación en el sitio, toma de notas, registro de flujo de personas.
Análisis documental	Revisar documentos de normativas de seguridad y sistemas que sean antiguos es clave para marcar pautas y límites.	Documentos institucionales, manuales, reglamentos internos.

4.4.1.1. Requerimientos funcionales:

- Captura de rostros mediante una cámara conectada a la Raspberry Pi.
- Entrenamiento de una red neuronal para el reconocimiento facial.
- Identificación facial en tiempo real.
- Registro de accesos en una base de datos local.

4.4.1.2. Requerimientos no funcionales:

- Uso eficiente de los recursos de hardware disponibles, especialmente la Raspberry Pi 5.
- Alta precisión en el reconocimiento facial (superior al 90 %).
- Interfaz gráfica sencilla, intuitiva y operativa para el personal autorizado.

4.4.1.3. Requerimientos de hardware y software

Tabla 10

Requerimientos de hardware y software

Requerimientos de hardware y software	
Raspberry Pi 5	Unidad principal de procesamiento. Ejecuta el sistema de reconocimiento facial.
Cámara web USB	Dispositivo de captura de imágenes faciales en tiempo real.
MicroSD ≥64 GB	Almacenamiento del sistema operativo, base de datos y codificaciones faciales.
Python 3	Lenguaje de programación utilizado para la lógica del sistema.
OpenCV + Face Recognition	Bibliotecas empleadas para la detección y reconocimiento facial.
SQLite3	Base de datos local ligera para el registro de accesos.
Tkinter	Herramienta gráfica para la interfaz del administrador del sistema.

4.4.1.4. Tipos y roles de usuario

Tabla 11

Tipos y roles de usuario

Usuario	Rol
Administrador	Registra rostros, gestiona accesos, consulta registros.
Docente autorizado	Es identificado automáticamente por el sistema al ingresar.
Usuario no autorizado	No es reconocido; su intento puede ser registrado como alerta.

4.4.2. Fase II: Diseño del sistema.

4.4.2.1. Diseño Arquitectónico

La propuesta planteada consistió en un sistema cliente-servidor en el que la Raspberry Pi 5 actuó como el núcleo principal, integrando el reconocimiento facial, una base de datos local y una interfaz de usuario. Este sistema permitió capturar imágenes en tiempo real, procesar los rasgos faciales mediante redes neuronales convolucionales y gestionar la información sin requerir conexión a internet. Los componentes funcionales fueron los siguientes:

Figura 9

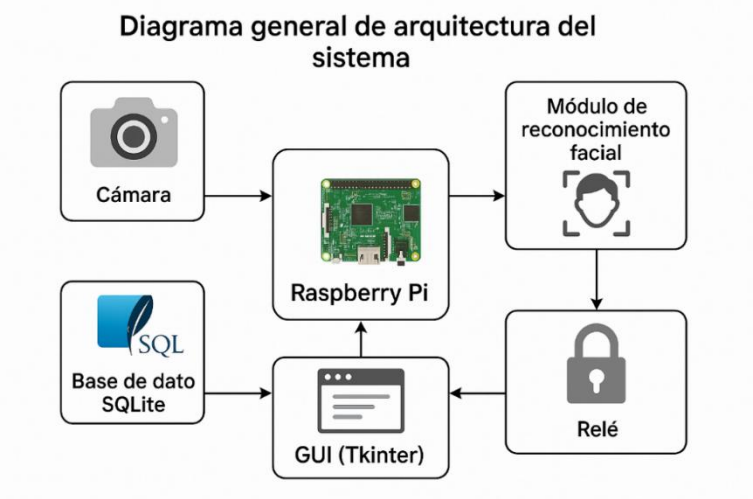


Diagrama general de arquitectura del sistema

Fuente: Elaboración propia (2025)

- **Interfaz gráfica de usuario (GUI):**

Desarrollada en Python con la biblioteca Tkinter, permite una experiencia visual intuitiva y funcional, incluso para usuarios sin conocimientos técnicos. La interfaz cuenta con diseño responsivo y estilos personalizados, y facilita el acceso a las funcionalidades clave:

- Registro de nuevos usuarios protegido por contraseña de administrador.

- Inicio y detención del control de acceso con un solo clic.
- Visualización de la cámara en vivo integrada en la ventana principal.
- Consulta del historial de accesos a través de una ventana emergente que accede a la base de datos SQLite.
- La barra de progreso y consola durante el registro facial, muestra el avance de capturas y mensajes del sistema.

- **Módulo de reconocimiento facial**

Este módulo resultó fundamental para la identificación biométrica. Se emplearon las bibliotecas face_recognition y OpenCV para analizar las imágenes capturadas por la cámara, localizar los rostros, codificarlos y compararlos con aquellos previamente almacenados en la base de datos.

- **Detección de rostros:** se utilizó la función face_recognition.face_locations() con el modelo CNN (Convolutional Neural Network), el cual proporcionó una mayor precisión en la identificación de rasgos faciales.
- **Codificación:** se aplicó face_recognition.face_encodings() para generar vectores numéricos únicos de cada rostro.
- **Comparación:** mediante face_recognition.face_distance() se midió la distancia entre vectores con el fin de establecer la concordancia, considerando un umbral previamente definido.
- **Captura en tiempo real:** OpenCV permitió gestionar la cámara, capturar cada fotograma y enviarlo al módulo de reconocimiento.

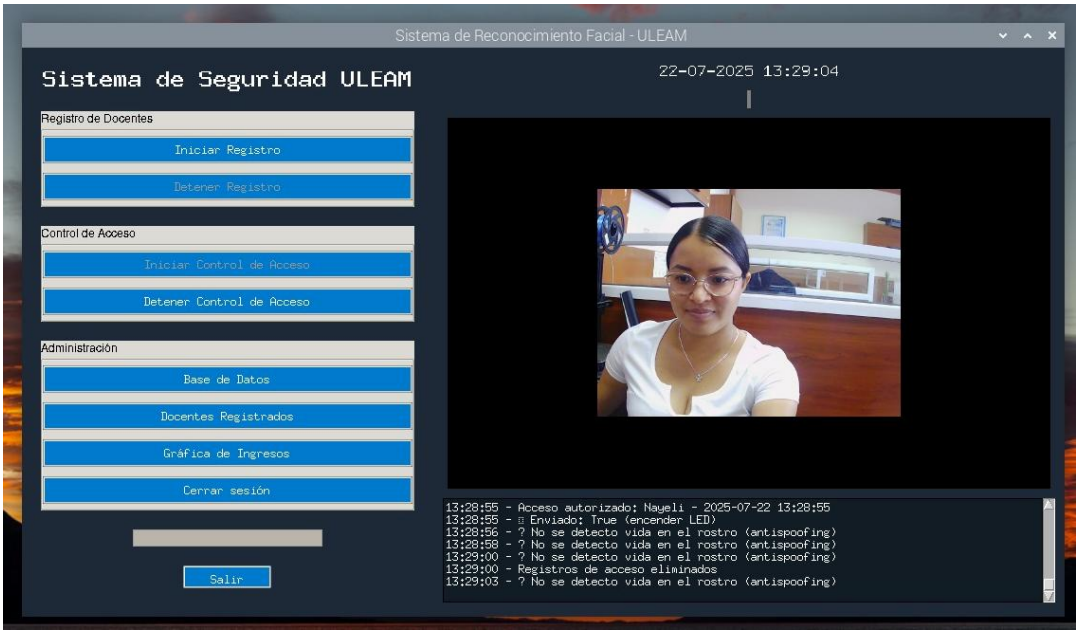
El módulo también incorporó una funcionalidad básica de antispoofing, consistente en la detección de parpadeo, utilizada como mecanismo de protección frente a intentos de suplantación de identidad mediante fotografías.

4.4.2.2. Diseño de la Interfaz de Usuario

La interfaz gráfica de usuario (GUI) fue diseñada con el propósito de facilitar la gestión del sistema sin comprometer su seguridad. La ventana principal incluyó botones de navegación y elementos visuales que permitieron ejecutar las siguientes acciones:

- **Módulo de autenticación administrativa:** se requirió el ingreso de una contraseña para acceder al módulo de registro. En caso de que la contraseña fuera incorrecta, se mostró una advertencia y no se permitió continuar con el proceso.

Figura 10



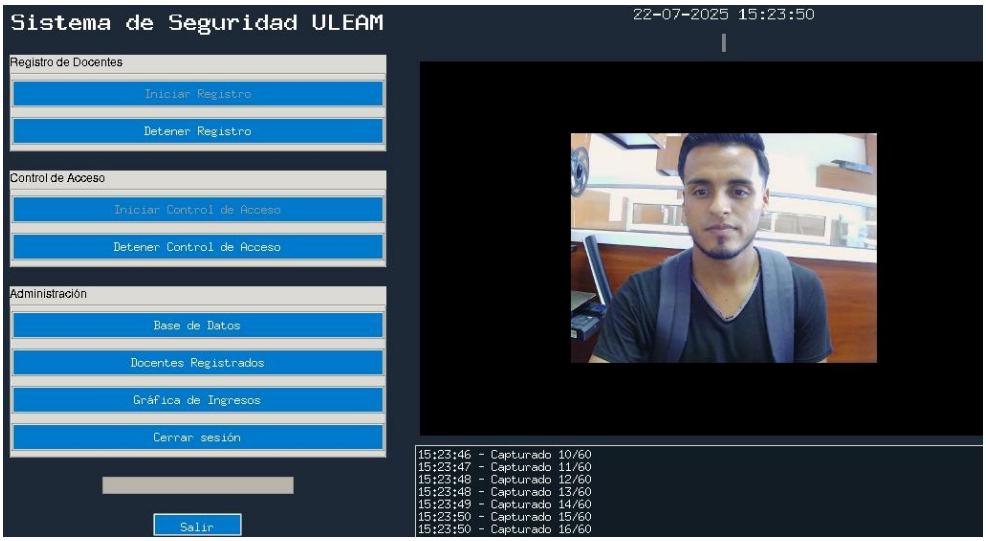
Módulo de autenticación administrativa

Fuente: Elaboración propia (2025).

• **Módulo de registro facial:** permite registrar nuevos usuarios (docentes), capturando 60 imágenes desde la cámara en tiempo real. Cada imagen es procesada y

codificada en un vector numérico. Estos datos se almacenan como archivo .npz, junto con el nombre del docente.

Figura 11

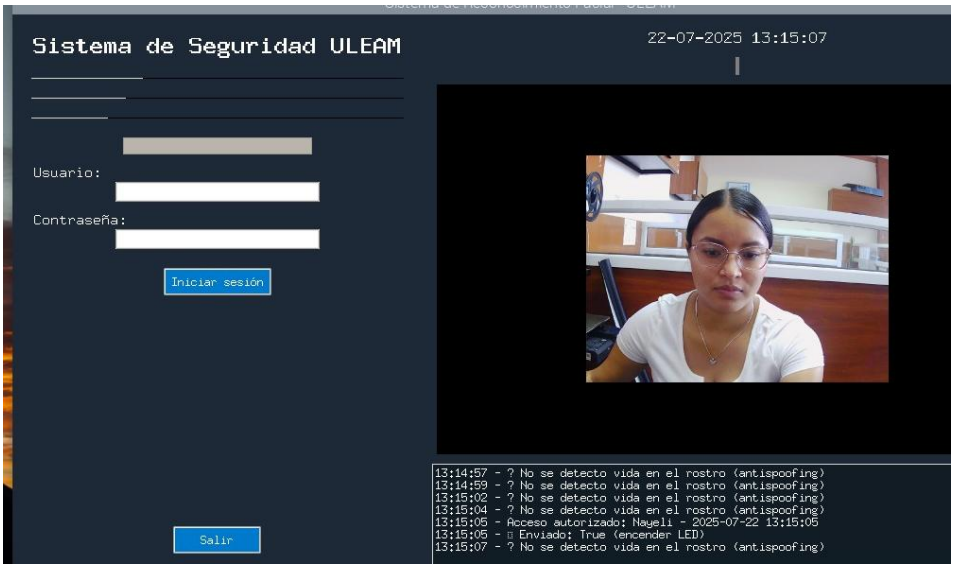


Módulo de registro facial

Fuente: Elaboración propia (2025).

• **Módulo de control de acceso:** activa el reconocimiento facial instantáneo. Al identificar una cara, enseña la foto tomada, el nombre del profesor y anota el suceso. Si no se identifica, aparece un aviso de "Acceso denegado".

Figura 12

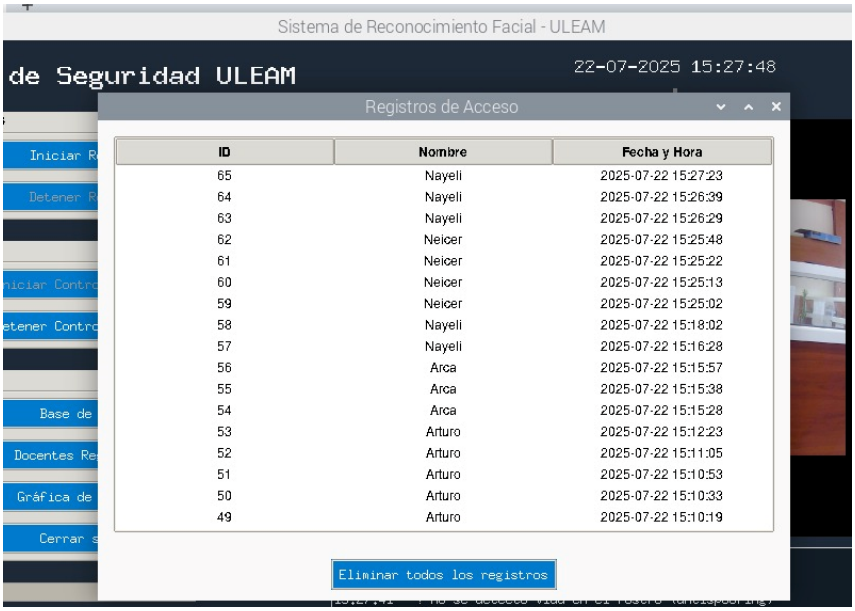


Módulo de control de acceso

Fuente: Elaboración propia (2025).

• **Módulo de consulta de registros:** mediante una ventana emergente, permite visualizar los registros de accesos guardados en la base de datos, incluyendo nombre, fecha y hora. También se pueden eliminar usuarios existentes desde este módulo.

Figura 13



Módulo de consulta de registros

Fuente: Elaboración propia (2025).

• **Consola y reloj en tiempo real: e**n la parte inferior de la interfaz se muestra una consola con eventos del sistema y un reloj digital actualizado cada segundo.

4.4.2.3. Diseño de la Base de Datos

Para el sistema se diseñó una base de datos local en SQLite, orientada a garantizar operaciones rápidas y un manejo seguro de la información. Su estructura contempla dos tablas principales:

Tabla users: almacena los datos básicos de los docentes registrados en el sistema.

- **id:** Identificador único y autoincremental del usuario.
- **name:** Nombre del docente, definido como campo único para evitar duplicidad.

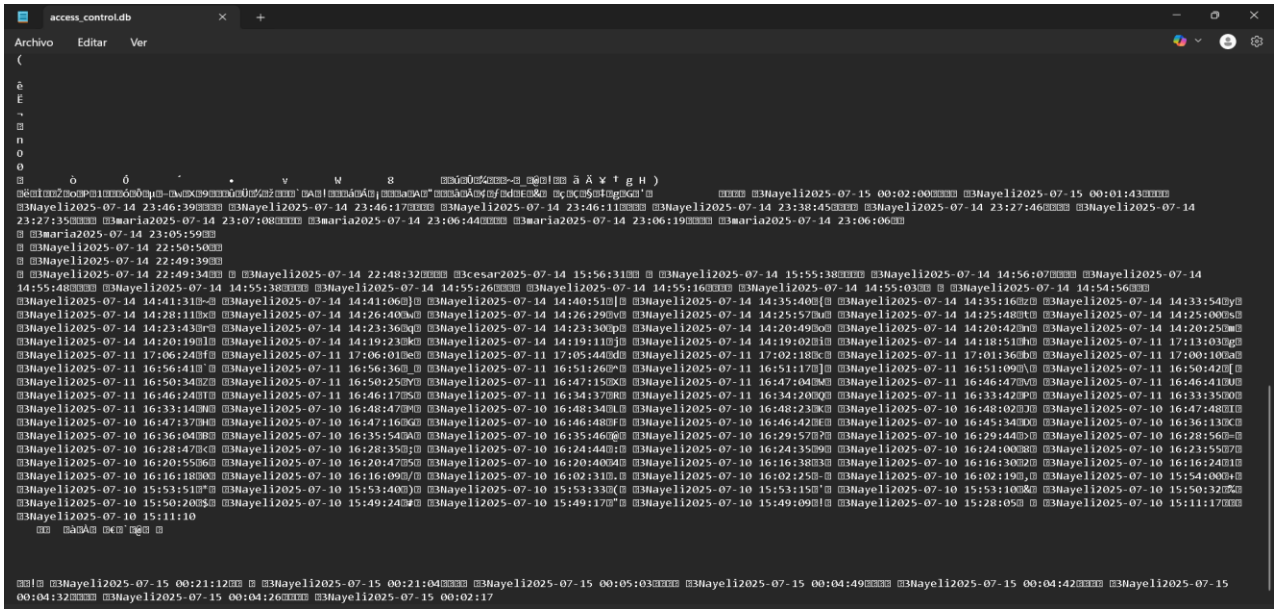
Tabla access_logs: registra de manera histórica los eventos de acceso.

- **id:** Identificador único y autoincremental del registro.
- **user_id:** Clave foránea que enlaza con la tabla users, permitiendo relacionar cada acceso con el docente correspondiente.
- **name:** Nombre del usuario reconocido en el evento.
- **timestamp:** Fecha y hora exacta en que ocurrió el intento de acceso (formato AAAA-MM-DD HH:MM:SS).

Codificaciones faciales

- Se almacenan como vectores .npz generados al momento del registro.
- Este formato impide la reconstrucción directa de rostros, mejorando la privacidad de los datos biométricos. Este formato permite búsquedas ágiles y fomenta la vinculación con la interfaz visual para supervisar y rectificar sucesos.

Figura 14



Módulo de consulta de registros

Fuente: Elaboración propia (2025).

4.4.2.4. Diagrama de Flujo de Datos

Figura 15

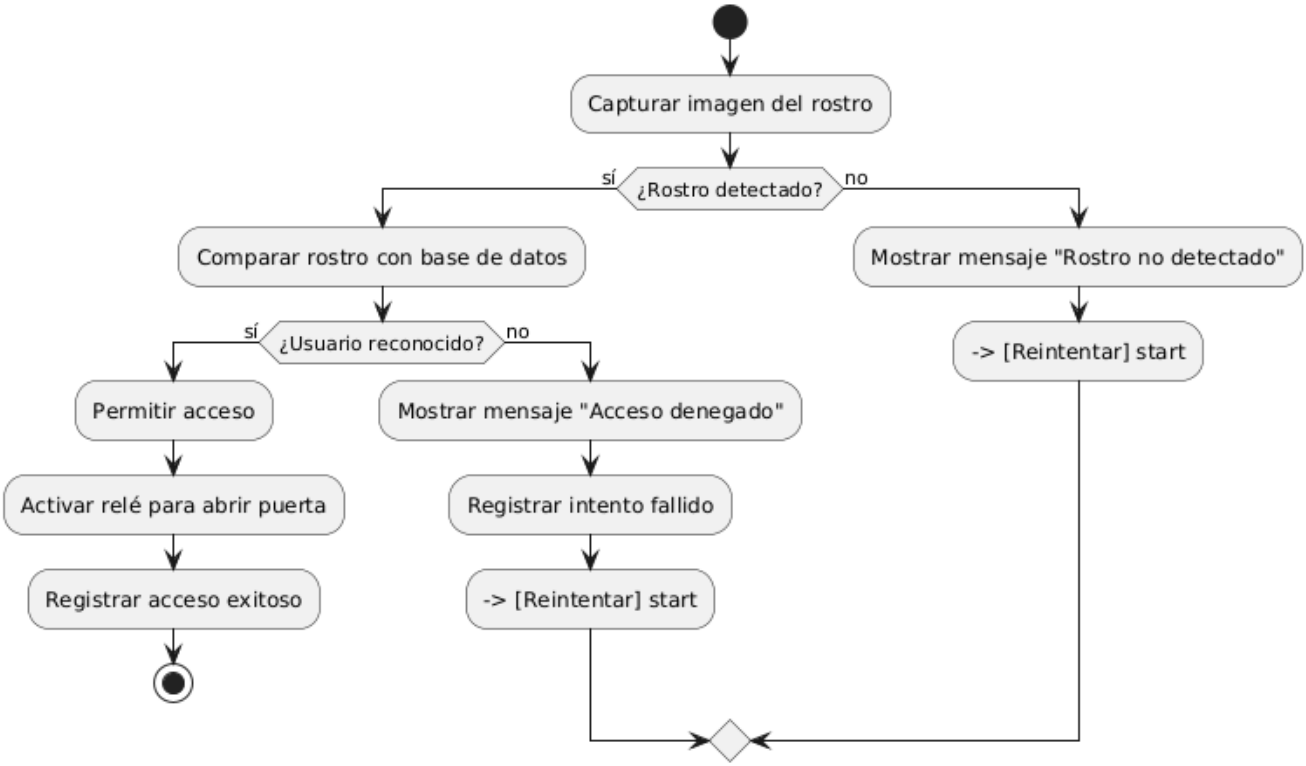


Diagrama de flujo Control de acceso

Fuente: Elaboración propia (2025).

Figura 16

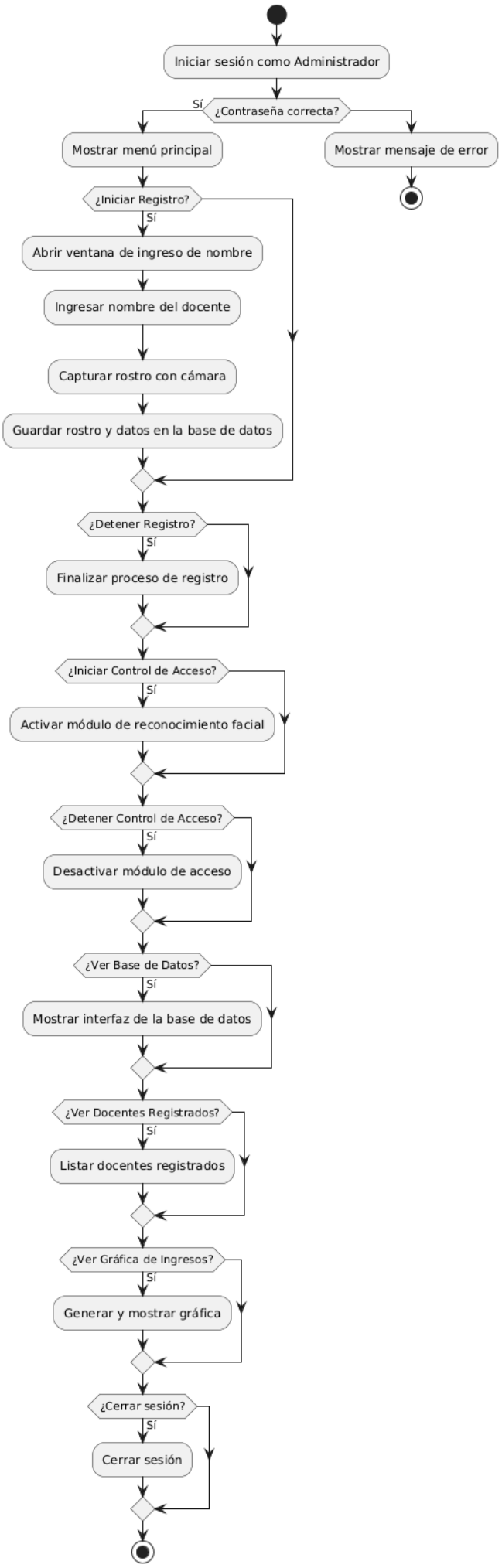

Iniciar sesión como Administrador
¿Contraseña correcta?
Sí
Mostrar menú principal
Mostrar mensaje de error
¿Iniciar Registro?
Sí
Abrir ventana de ingreso de nombre
Ingresar nombre del docente
Capturar rostro con cámara
Guardar rostro y datos en la base de datos
¿Detener Registro?
Sí
Finalizar proceso de registro
¿Iniciar Control de Acceso?
Sí
Activar módulo de reconocimiento facial
¿Detener Control de Acceso?
Sí
Desactivar módulo de acceso
¿Ver Base de Datos?
Sí
Mostrar interfaz de la base de datos
¿Ver Docentes Registrados?
Sí
Listar docentes registrados
¿Ver Gráfica de Ingresos?
Sí
Generar y mostrar gráfica
¿Cerrar sesión?
Sí
Cerrar sesión

Diagrama de flujo Administrativa

Fuente: Elaboración propia (2025).

4.4.2.5. Diagrama de Casos de Uso

Figura 17

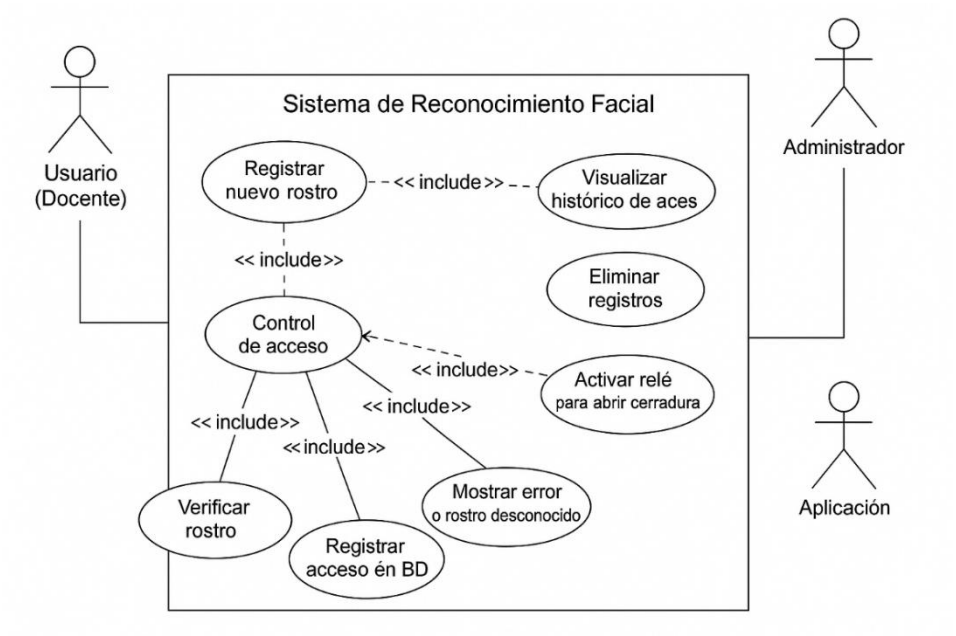


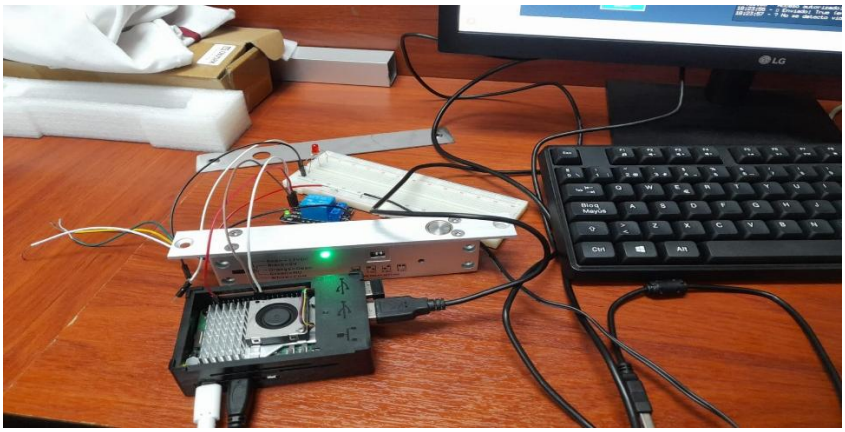
Diagrama de Casos de Uso

Fuente: Elaboración propia (2025).

4.4.3. Fase III: Implementación del Sistema

En esta fase se desarrolló lo práctico del sistema de reconocimiento facial para el control de acceso en la sala de profesores de TI y Software de la ULEAM Extensión El Carmen. La implementación se realizó en una Raspberry Pi 5, integrando la interfaz gráfica, el procesamiento de imágenes y la gestión de la base de datos. A continuación, se detallan los componentes implementados:

Figura 18



Raspberry conectada al relé y chapa eléctrica

Fuente: Elaboración propia (2025).

4.4.3.1. Entorno de desarrollo

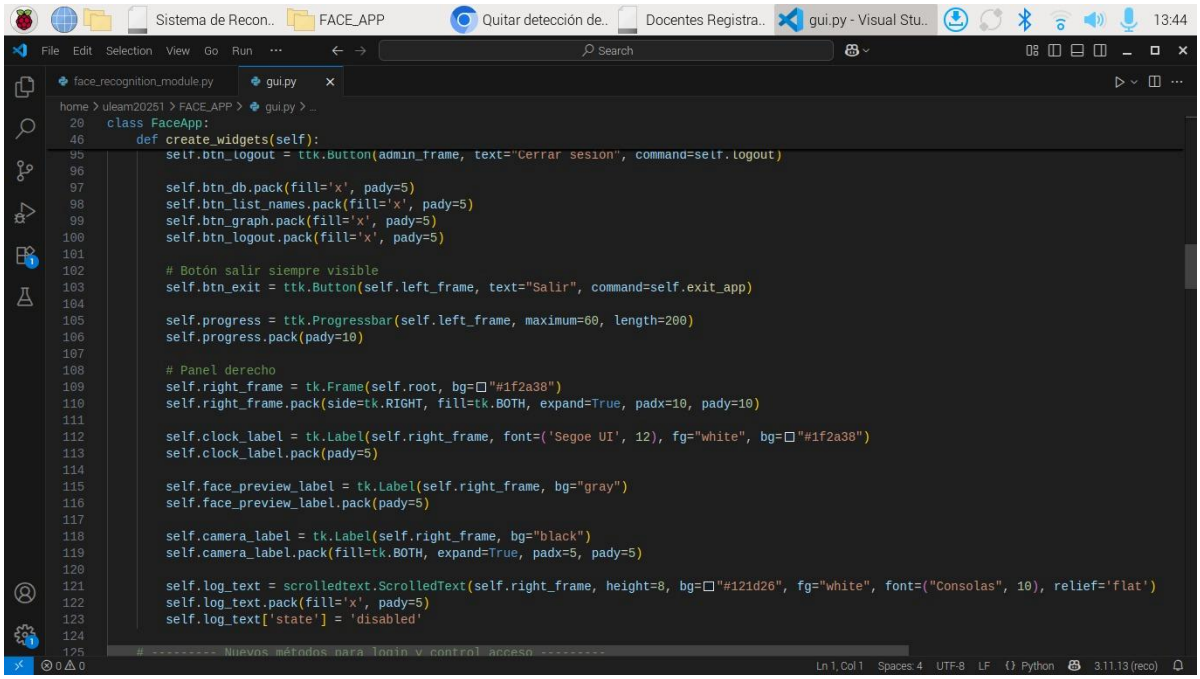
Para llevar a cabo la implementación del sistema digital de identificación facial con control de acceso, se utilizó un entorno de desarrollo conformado por herramientas de software y hardware compatibles con sistemas integrados. A continuación, se presentan los elementos empleados:

- **Lenguaje de programación:** Python 3.11, debido a su flexibilidad, fácil sintaxis y gran compatibilidad con bibliotecas de tratamiento de imágenes e interfaces visuales.
    - **Bibliotecas utilizadas:**
        - **OpenCV:** Para la captura y procesamiento de video.
        - **face_recognition:** Para la detección y reconocimiento facial basado en redes neuronales.
        - **Tkinter:** Para el desarrollo de la interfaz gráfica del usuario (GUI).

- **NumPy:** Para el manejo eficiente de matrices y operaciones numéricas.
- **SQLite3:** Para la gestión de la base de datos local.
- **os y datetime:** Para operaciones del sistema y gestión de fechas y horas.
- **PIL (Pillow):** Para la manipulación de imágenes dentro de la interfaz.

- **Base de datos:** SQLite, elegida por su ligereza, facilidad de integración con Python y por no requerir un servidor de base de datos.
- **Hardware:** Raspberry Pi 5 con 8 GB de memoria RAM, seleccionado por ser un sistema embebido de bajo consumo energético y alto rendimiento, ideal para aplicaciones de seguridad y control de acceso.
- **Sistema operativo:** Raspberry Pi OS, una versión oficial fundamentada en Debian, optimizada para el hardware de Raspberry Pi.
- **Cámara:** Módulo de cámara web compatible por USB, utilizado para la captura de rostros en tiempo real.)

Figura 19



Captura de pantalla del editor de código que se utilizó (Visual Studio Code)

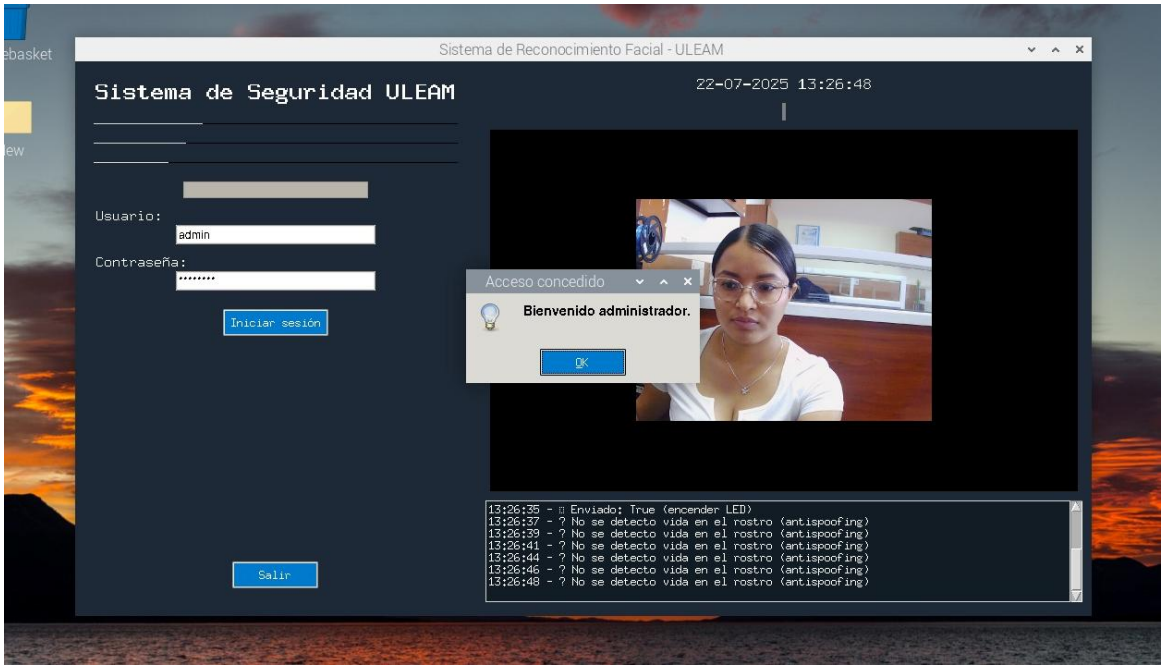
Fuente: Elaboración propia (2025).

4.4.3.2. Implementación del módulo de registro facial

Este componente fue desarrollado en Python con una interfaz en Tkinter y tuvo como propósito facilitar la gestión de accesos por parte del personal autorizado. Su función principal consistió en registrar nuevos docentes mediante reconocimiento facial, garantizando que únicamente las personas autorizadas pudieran ingresar. El proceso se estructuró en diversas fases:

- **Validación administrativa:** se requirió el ingreso de una clave de administrador, lo cual aseguró que únicamente el personal autorizado pudiera realizar registros en el sistema.

Figura 20

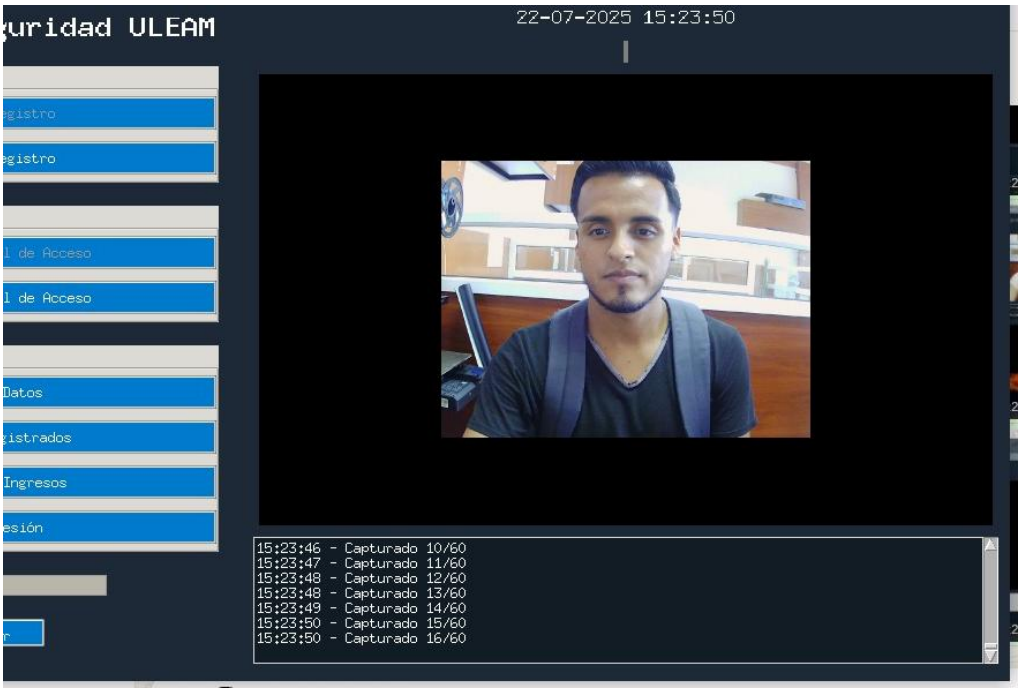


Validación administrativa

Fuente: Elaboración propia (2025).

- **Captura de muestras:** una vez que el administrador ingresó la clave y se autenticó, el sistema se conectó a la cámara y procedió a capturar 60 imágenes del docente en tiempo real. Este procedimiento permitió registrar variaciones en la expresión y en los ángulos faciales, lo cual incrementó la precisión del modelo de reconocimiento.

Figura 21



Captura de muestras

Fuente: Elaboración propia (2025)

- **Codificación de los rostros:** cada imagen capturada se transformó en un vector de características faciales utilizando la función face_encodings de la biblioteca face_recognition. Este vector, también conocido como encoding, representa matemáticamente las características únicas del rostro del docente.

Figura 22

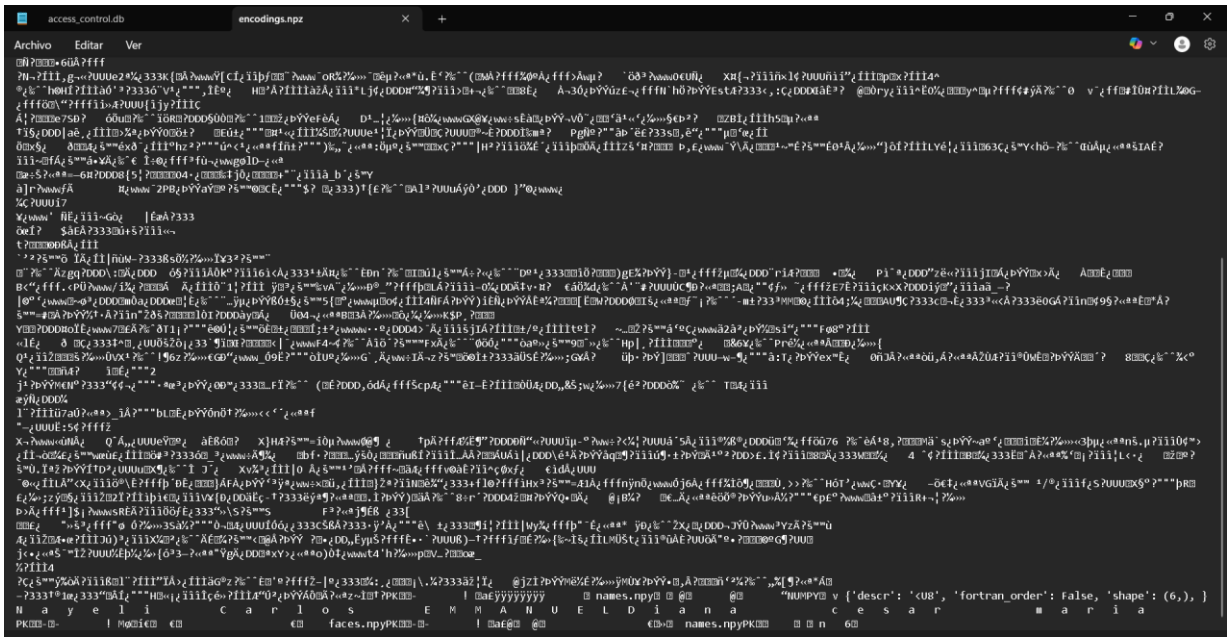
```
76
77      def obtener_encodings(self, frame):
78          small_frame = cv2.resize(frame, (0, 0), fx=0.25, fy=0.25)
79          rgb = cv2.cvtColor(small_frame, cv2.COLOR_BGR2RGB)
80          face_locations = face_recognition.face_locations(rgb, model='cnn')
81          encodings = face_recognition.face_encodings(rgb, face_locations)
82          return encodings, face_locations
83
```

Codificación de los rostros

Fuente: Elaboración propia (2025).

- **Almacenamiento del modelo facial:** las muestras capturadas se almacenaron en un archivo con extensión .npz (formato comprimido de NumPy) identificado con el nombre del docente. Dicho archivo funcionó como referencia para las comparaciones realizadas en la etapa de identificación facial.

Figura 23



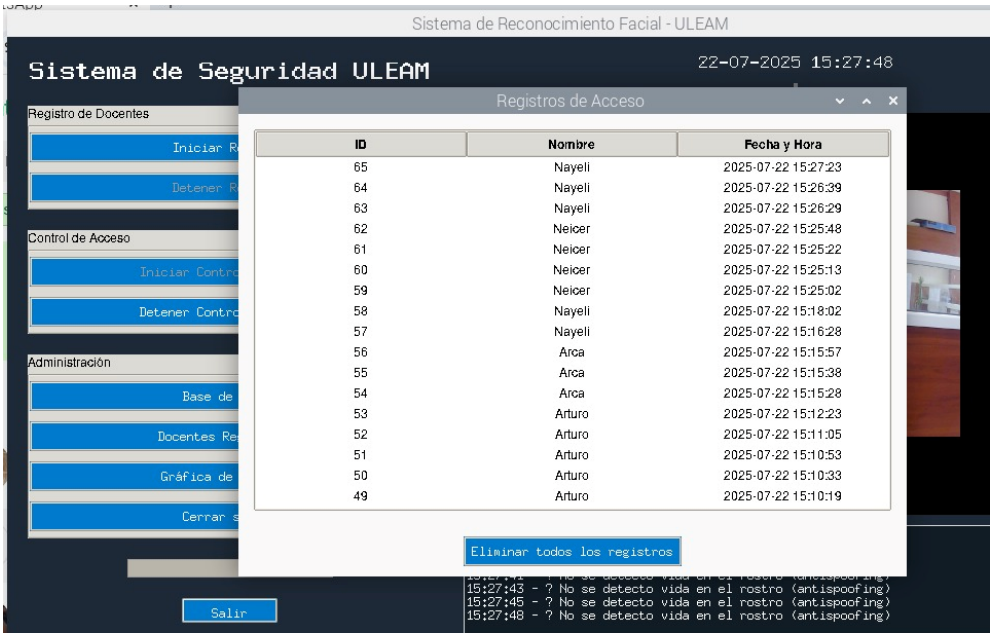
Archivo encodings.npz

Fuente: Elaboración propia (2025).

- **Registro en la base de datos:** finalmente, el sistema insertó un nuevo registro en la base de datos SQLite, almacenando el nombre del docente y la fecha de finalización

del proceso de registro. Esta información permitió mantener un control organizado de los usuarios del sistema.

Figura 24



Registro de acceso en la base de datos

Fuente: Elaboración propia (2025).

4.4.3.3. Implementación del módulo de control de acceso

El componente de gestión de acceso constituyó el elemento central del sistema, ya que se encargó de verificar la identidad del personal docente mediante reconocimiento facial y de autorizar o denegar su ingreso a la sala de profesores. Todo el procedimiento se ejecutó de manera independiente en el dispositivo Raspberry Pi, garantizando rapidez y seguridad sin requerir conexión a internet.

El procedimiento de funcionamiento se desarrolló de la siguiente manera:

- **Captura de rostro:** la cámara conectada a la Raspberry Pi capturó de forma continua la imagen del usuario frente al dispositivo.
- **Comparación de descriptores faciales:** la imagen capturada se transformó en un vector de características mediante la biblioteca face_recognition, el cual se comparó con los descriptores almacenados previamente en archivos .npz generados durante el proceso de registro.
- **Reconocimiento exitoso:** en caso de encontrarse coincidencias, se concedió el acceso, se registró internamente la hora del ingreso y la Raspberry Pi activó el relé encargado de suministrar electricidad a la cerradura eléctrica de 12 V, liberando así la puerta para permitir el paso del usuario.
- **Rostro no reconocido:** si no se identificó al usuario, se denegó el acceso y se desplegó un mensaje notificando el rechazo del ingreso.

Este procedimiento se realizó de forma totalmente local en la Raspberry Pi, incrementando tanto la seguridad como la privacidad de los datos.

4.4.3.4. Implementación del módulo de administración

Dentro del sistema se implementó un módulo de administración, diseñado para proporcionar al personal autorizado un control sobre todas las funciones del sistema de reconocimiento facial. Este módulo estuvo protegido mediante una contraseña, lo que garantizó la seguridad y permitió que únicamente el personal autorizado accediera a los datos y pudiera gestionarlos y supervisarlos.

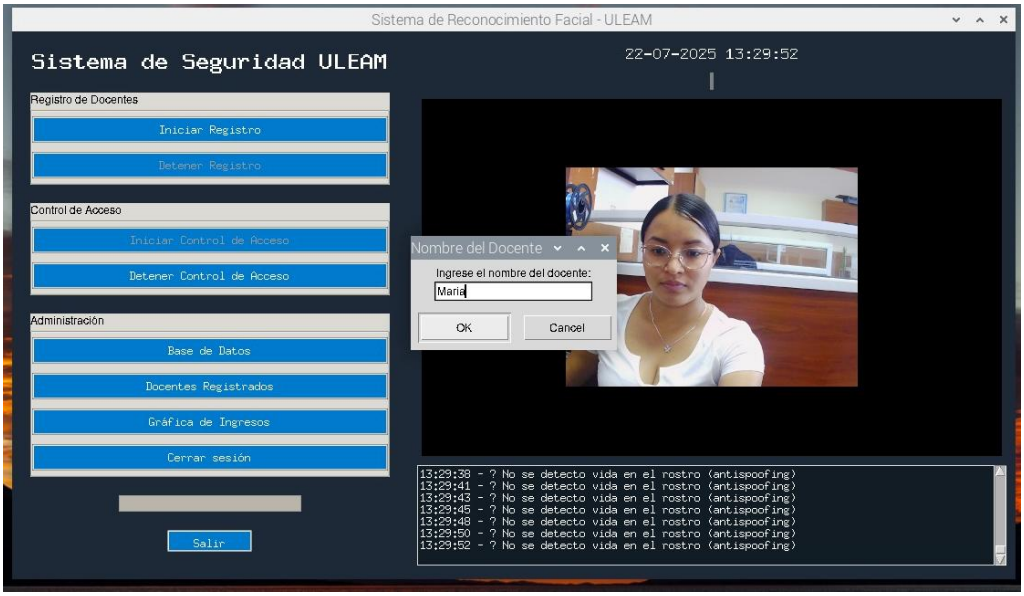
La interfaz, desarrollada en Tkinter, presentó un diseño intuitivo, con botones y ventanas emergentes que facilitaron la interacción con el sistema. Entre las funcionalidades del módulo de administración se incluyeron:

Funcionalidades principales del módulo de administración:

Registrar nuevo docente:

Al seleccionar la opción “Iniciar Registro”, se abrió una ventana en la que se ingresó el nombre del docente. El sistema capturó automáticamente 60 imágenes del usuario, las cuales fueron procesadas mediante la biblioteca face_recognition y almacenadas en un archivo .npz. Este archivo, junto con el nombre del docente y la fecha correspondiente, se registró en la base de datos SQLite.

Figura 25



Registrar nuevo docente

Fuente: Elaboración propia (2025).

Detener registro:

Mientras se está haciendo el registro facial, el administrador puede apretar el botón “Detener registro” para detener todo y cerrar la ventana de captura sin guardar nada a medias.

Iniciar control de acceso:

En esta etapa se inició el módulo de reconocimiento facial en tiempo real, en el cual el sistema capturó imágenes de los rostros mediante la cámara conectada y las comparó con los modelos previamente almacenados, con el fin de autorizar o denegar el acceso a la sala.

Detener control de acceso:

Esta función es para cortar de inmediato la cámara y el reconocimiento facial.

Ver docentes registrados:

El administrador pudo acceder a una ventana que mostró todos los docentes previamente registrados, incluyendo su nombre y la fecha de registro. Esta vista permitió realizar un seguimiento cronológico de los usuarios del sistema.

Eliminar docente:

Desde la misma lista de docentes, el administrador pudo seleccionar un usuario específico y activar la opción “Eliminar”. Esta acción eliminó:

- El archivo .npz que contenía las codificaciones faciales.
- El registro correspondiente en la base de datos SQLite.

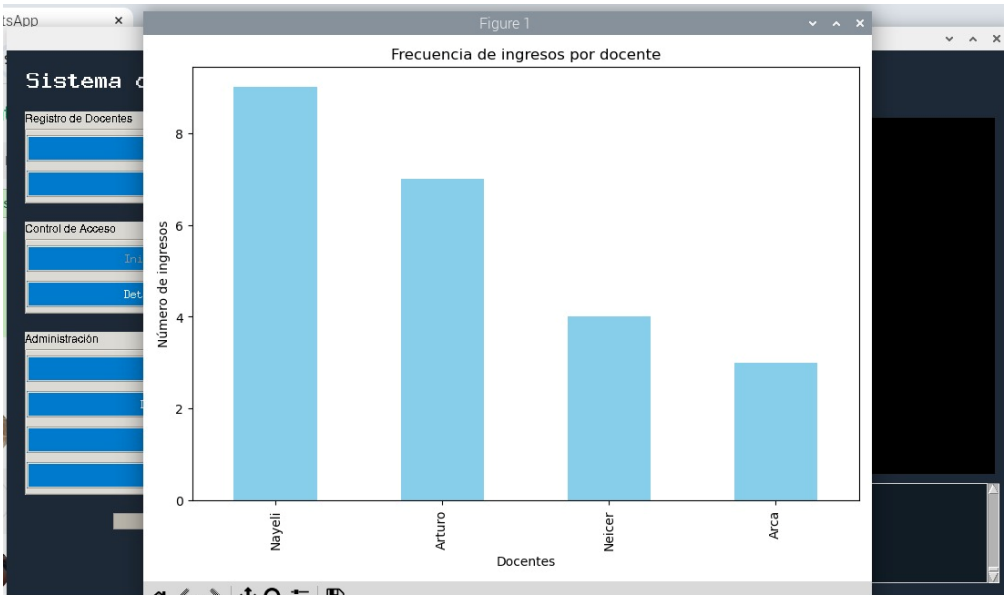
Antes de finalizar el proceso de eliminación, el sistema solicitó una validación para prevenir errores no intencionados.

Visualizar gráfica de ingresos:

El sistema proporcionó al administrador la opción de generar un gráfico que mostró, de manera clara, la cantidad de ingresos de cada docente. Esta funcionalidad, implementada con

matplotlib, permitió analizar el uso del sistema y detectar patrones o hábitos de acceso, contribuyendo al estudio del comportamiento de los usuarios.

Figura 26



Frecuencia de ingresos por docente

Fuente: Elaboración propia (2025).

Ver base de datos completa:

El administrador no solo pudo consultar la lista de docentes, sino que también accedió a una visión general de la base de datos SQLite, la cual contenía todos los datos de los usuarios y los registros de ingresos. La información se presentó en una tabla organizada dentro de la interfaz, facilitando la gestión y supervisión de los datos.

Cerrar sesión:

Finalmente, mediante el botón “Cerrar sesión”, el administrador pudo salir de la interfaz de manera segura y regresar al menú principal. Esta función garantizó que únicamente el

personal autorizado tuviera acceso a las funciones administrativas después de finalizar la gestión.

4.4.3.5. Interfaz gráfica del sistema

La interfaz gráfica de usuario (GUI) fue empleada mediante la biblioteca Tkinter de Python siendo su principal objetivo brindar una interacción precisa, intuitiva y además que sea funcional con el sistema de control de acceso dado mediante el reconocimiento facial, esta interfaz funciona mediante la Raspberry Pi 5, permitiendo así que sea idónea para usarla dentro del laboratorio, existen varios elementos que podemos encontrar, como:

- **Botón para registrar nuevo docente:** abre una ventana emergente donde se ingresa el nombre del docente y luego se inicia la captura de muestras faciales de cada docente.
- **Botón para detener el registro del docente:** permite cancelar el proceso de captura antes de que se completen las 60 muestras.
- **Botón para iniciar el control de acceso:** activa el reconocimiento facial en tiempo real y habilita el sistema de validación de identidades.
- **Botón para detener el control de acceso:** apaga la cámara y frena la identificación facial, conveniente cuando no está en servicio o durante labores de mantenimiento.
- **Botón para ver la base de datos:** muestra en una ventana tabular los registros almacenados de accesos realizados.
- **Botón para ver los docentes registrados:** presenta una lista con los nombres y fechas de registro de los docentes habilitados.

- **Botón para ver la gráfica de ingresos:** genera una visualización estadística que representa la frecuencia de accesos por usuario.
- **Botón para cerrar sesión:** finaliza la sesión actual del administrador, retornando al menú principal protegido por contraseña.
- **Visualización en tiempo real:** presenta en la pantalla la foto tomada por la cámara y el marco de reconocimiento facial que está en uso.
- **Mensajes de estado en pantalla:** se muestra mensajes claros en pantalla, como “Acceso concedido”, “Acceso denegado”, “Registro exitoso” o “Error de reconocimiento”.

4.4.3.6. Integración final del sistema

La integración final del sistema consistió en unificar todos los módulos desarrollados reconocimiento facial, control de acceso físico, gestión de base de datos, almacenamiento de codificaciones faciales y la interfaz gráfica dentro de la Raspberry Pi 5, generando un entorno operativo funcional y autónomo.

Cada componente del sistema se interconectó de manera coordinada, garantizando su funcionamiento conjunto. El resultado fue un sistema robusto, práctico y adecuado para entornos educativos que requieren seguridad, manteniendo la operatividad sin complejidad innecesaria. A continuación, se describe la integración de los elementos esenciales:

Reconocimiento facial en tiempo real: la Raspberry Pi gestionó la captura, detección, extracción y comparación de rasgos faciales mediante OpenCV y face_recognition, utilizando una cámara USB conectada al dispositivo. Este proceso requirió una configuración adecuada para garantizar su correcto funcionamiento.

Control físico de acceso: una vez que el sistema reconoció y validó al usuario, la Raspberry Pi envió una señal a través del puerto GPIO a un relé, el cual activó la cerradura eléctrica, permitiendo el ingreso autorizado.

Base de datos local (SQLite): los registros de docentes, incluyendo nombres y fechas de acceso, se almacenaron en una base de datos SQLite accesible desde la interfaz gráfica. Esta base de datos operó sin conexión a internet, asegurando su funcionalidad en entornos aislados.

Codificaciones faciales (.npz): durante el registro de los rasgos faciales, se generaron archivos .npz que almacenaron las codificaciones, permitiendo que las verificaciones posteriores fueran más rápidas al evitar procesar las imágenes desde cero en cada comparación.

Interfaz gráfica (Tkinter): la interfaz permitió al administrador interactuar con el sistema, gestionar registros, visualizar estadísticas, monitorear el control de acceso en tiempo real y acceder a los datos almacenados, todo desde una única ventana.

Sincronización de procesos: para garantizar un funcionamiento fluido, se implementaron técnicas de multithreading y estructuras de control que permitieron la ejecución simultánea del reconocimiento facial, la interfaz gráfica y el control del relé, evitando retardos en el sistema.

La integración de estos elementos generó un sistema embebido que arrancó de manera autónoma, cargó los módulos necesarios, estableció comunicación con los dispositivos conectados y presentó la interfaz lista para el uso del administrador. Las pruebas realizadas en entornos reales demostraron su correcto funcionamiento, constituyendo una solución sólida para instituciones educativas que requieren controlar de manera eficiente el acceso al personal autorizado.

4.4.4. Fase IV: Pruebas del Sistema

El propósito de esta fase consistió en verificar que el sistema de control de acceso mediante reconocimiento facial cumpliera los requisitos funcionales de rendimiento y seguridad establecidos en etapas previas. Se llevaron a cabo diversas pruebas con el fin de garantizar su correcto funcionamiento en entornos reales.

4.4.4.1. Pruebas Funcionales

Se evaluaron las funcionalidades clave del sistema para confirmar que cada una opere de manera correcta:

Tabla 12

Prueba de funcionalidad

Funcionalidad probada	Descripción	Resultado esperado	Resultado obtenido
Registro facial	Captura y codificación de 60 muestras de rostro	Registro exitoso del docente	Correcto
Control de acceso	Validación del rostro ante la cámara en tiempo real	Acceso concedido o denegado	Correcto
Eliminación de usuario	Autenticación administrativa y borrado del registro	Usuario eliminado y archivo .npz borrado	Correcto
Navegación en la interfaz gráfica	Uso de botones, campos de entrada y mensajes	Fluidez en navegación y respuestas visibles	Correcto

4.4.4.2. Pruebas de Rendimiento

Las pruebas de rendimiento se diseñaron para evaluar la eficiencia, velocidad y estabilidad del sistema de control de acceso mediante reconocimiento facial, implementado

sobre una Raspberry Pi 5. Se consideraron métricas como el tiempo promedio de reconocimiento, la velocidad de procesamiento de cada modelo y la capacidad de respuesta en tiempo real.

Tiempo de reconocimiento

Se realizaron pruebas para medir el tiempo que tardó el sistema en reconocer a un usuario, desde la detección inicial por la cámara hasta la autorización del acceso. Se compararon dos modelos de reconocimiento facial: HOG y CNN. Los tiempos promedio obtenidos fueron los siguientes:

Tabla 13

Tiempo de reconocimiento

Modelo	Tiempo promedio de reconocimiento
HOG + SVM	0.84 segundos
CNN	1.39 segundos

Interpretación: el modelo HOG demostró ser más rápido y adecuado para procesamiento en tiempo real sobre dispositivos con limitaciones de hardware como el Raspberry Pi, mientras que el modelo CNN, aunque más preciso, mostró mayor latencia.

Velocidad de procesamiento

Durante las pruebas, se midió el número de fotogramas por segundo (FPS) que el sistema es capaz de procesar en cada modelo, considerando además la carga de la detección de vida (detección de parpadeo con MediaPipe):

Tabla 14

Velocidad de procesamiento

Modelo	FPS sin liveness	FPS con liveness (MediaPipe)
HOG + SVM	14.2 fps	10.5 fps
CNN	8.7 fps	6.1 fps

Interpretación: se evidenció una disminución esperada en el rendimiento al activar la detección de vida; no obstante, los valores obtenidos resultaron suficientes para garantizar un reconocimiento fluido. Para aplicaciones con mayores requerimientos, se recomendó implementar soluciones de mayor capacidad o reducir la carga asociada a la detección.

Consumo de recursos

Durante las pruebas, se comprobó cómo reaccionó la Raspberry Pi en términos de CPU y memoria. Aquí un resumen:

Tabla 15

Consumo de recursos

Componente	Uso promedio (HOG + SVM)	Uso promedio (CNN)
CPU	61 %	78 %
RAM	512 MB	850 MB

Interpretación: Se observó que el modelo CNN consumió más recursos, lo que podría afectar el rendimiento cuando el sistema ejecutaba múltiples procesos simultáneamente. Por su

parte, el modelo HOG, al ser más ligero, resultó más adecuado para un uso constante y en tiempo real, ofreciendo un equilibrio entre eficiencia y desempeño en la Raspberry Pi.

4.4.4.3. Pruebas de Seguridad

Las pruebas de seguridad resultaron fundamentales para verificar que el sistema protegiera correctamente el acceso a la sala de profesores, evitando suplantaciones de identidad, accesos no autorizados y manipulación indebida del sistema. Se realizaron diversas pruebas de ataque para evaluar la resistencia del sistema frente a distintas amenazas:

A. Prueba de suplantación con fotografía

Objetivo: Determinar si el sistema podía ser engañado con una fotografía del rostro de un usuario registrado.

Procedimiento:

- Se presentó una fotografía a tamaño real frente a la cámara.
- Se simuló un parpadeo moviendo manualmente la imagen.

Resultado: El acceso fue denegado. La detección de vida basada en parpadeo no identificó movimiento ocular natural, permitiendo al sistema distinguir entre un rostro real y una imagen.

B. Prueba de suplantación con video

Objetivo: Evaluar la susceptibilidad del sistema frente a una grabación de un usuario registrado realizando parpadeo.

Procedimiento:

- Se reprodujo un video del usuario parpadeando frente a la cámara.
- Se realizaron varios intentos desde distintos ángulos.

Resultado: El acceso fue denegado. A pesar de que el parpadeo era visible, la falta de profundidad, los reflejos y la incoherencia entre fotogramas permitieron al sistema identificar la falsificación.

C. Prueba de intento de acceso sin autorización

Objetivo: Verificar que individuos no registrados no pudieran ingresar al sistema.

Procedimiento:

Se presentó frente a la cámara a personas que no estaban incluidas en la base de datos.

Resultado: El acceso fue denegado y el sistema mostró el mensaje "Persona no reconocida".

D. Prueba de acceso al sistema administrativo

Objetivo: Evaluar la seguridad del módulo de administración del sistema (registro, eliminación de docentes, visualización de la base de datos).

Procedimiento:

- Se intentó acceder sin ingresar usuario y contraseña.
- Se intentó manipular botones administrativos.

Resultado: El acceso fue restringido. La plataforma no permitió utilizar las opciones de gestión hasta que el administrador se identificó con las credenciales correspondientes.

E. Protección de datos almacenados

Objetivo: Validar que las codificaciones faciales y la base de datos estuvieran protegidas.

Procedimiento:

- Se inspeccionó el almacenamiento de archivos .npz y la base de datos SQLite.
- Se verificó que no existieran imágenes completas ni información personal sin procesar.

Resultado: El sistema no almacenó fotografías completas, únicamente codificaciones faciales en forma de vectores numéricos, lo que redujo significativamente el riesgo de exposición de datos sensibles.

4.4.4.4. Resultados Generales

Los hallazgos obtenidos durante la ejecución y evaluación del sistema indicaron que se cumplieron de manera efectiva los objetivos establecidos. El sistema permitió la captura y validación de rostros en tiempo real, gestionando de forma adecuada la base de datos de docentes autorizados. El modelo HOG, debido a su menor tiempo de respuesta (0,84 s), se identificó como el más adecuado para la Raspberry Pi, mientras que el modelo CNN presentó una mayor precisión, aunque con un mayor consumo de recursos.

Se incorporó un sistema de detección de vida basado en el parpadeo, con el objetivo de prevenir intentos de suplantación mediante fotografías o videos, lo que aumentó la seguridad del sistema. Las funciones administrativas requirieron siempre la introducción de una contraseña, y la interfaz proporcionó una experiencia de uso intuitiva, facilitando la gestión y operación por parte del personal autorizado.

En condiciones normales, el sistema alcanzó un 98,7 % de exactitud. Sin embargo, en entornos con iluminación reducida se observó una disminución del rendimiento, la cual pudo ser corregida mediante ajustes en la configuración. Estos resultados indicaron que el sistema era confiable, aunque requirió optimización para mantener un desempeño óptimo en distintas condiciones ambientales.

4.4.5. Fase V: Mantenimiento del Sistema

Esta fase incluyó las tareas necesarias para garantizar el funcionamiento continuo del sistema a largo plazo, abarcando la corrección de fallos potenciales, la optimización de características y la adaptación a variaciones en el entorno o en los requerimientos.

4.4.5.1. Mantenimiento Correctivo

Se definió como el conjunto de acciones destinadas a resolver errores detectados durante la operación del sistema en condiciones reales:

- Se corrigieron errores menores en la interfaz gráfica, como etiquetas mal alineadas o botones sin respuesta.
- Se ajustó el umbral de similitud para mejorar la precisión del reconocimiento facial.
- Se solucionaron fallos de inicialización de la cámara cuando el sistema se ejecutaba de manera continua durante períodos prolongados.

4.4.5.2. Mantenimiento Preventivo

Este tipo de mantenimiento se realizó con el objetivo de prevenir fallos futuros y prolongar la vida útil del sistema:

- Se efectuó limpieza periódica del módulo de cámara para garantizar una correcta captura de imágenes.

- Se verificó y respaldó mensualmente la base de datos SQLite.
- Se comprobó el estado térmico y el rendimiento de la Raspberry Pi para evitar sobrecalentamiento.
- Se actualizaron el sistema operativo y las bibliotecas utilizadas (Python, OpenCV, face_recognition) cuando fue necesario.

4.4.5.3. Mantenimiento Evolutivo

- Se evaluó la posible integración del registro de horarios de ingreso y salida de los docentes para generar reportes.
- Se consideró la inclusión de notificaciones por correo electrónico o mensajes locales ante intentos fallidos de acceso.
- Se planificó la mejora de la interfaz gráfica para facilitar su uso en pantallas táctiles.
- Se proyectó la implementación futura de reconocimiento de múltiples rostros simultáneos, por ejemplo, en clases compartidas.

4.4.5.4. Plan de Actualización del Sistema

Se planteó un plan de revisión periódica del sistema para garantizar su correcto funcionamiento:

Tabla 16

Plan de actualización del sistema

Periodicidad	Actividad
Mensual	Verificación de base de datos y archivos `.npz`
Bimensual	Prueba general del sistema con docente y administrador

Trimestral	Revisión de versiones de bibliotecas y sistema operativo
Semestral	Evaluación de nuevas funcionalidades necesarias

CAPÍTULO V

5. EVALUACIÓN DE RESULTADOS

5.1. Introducción

Este capítulo presenta la evaluación de los resultados obtenidos tras la implementación del sistema informático de control de acceso basado en reconocimiento facial, desarrollado para la sala de profesores de la carrera de Tecnologías de la Información. El propósito de esta etapa consistió en validar que el sistema cumpliera con los objetivos establecidos en términos de funcionalidad, rendimiento y seguridad.

Para la evaluación del sistema, se diseñó un plan de pruebas integral, ejecutado en entornos reales, mediante el cual se observó el funcionamiento de los módulos y se analizaron los datos utilizando métricas de clasificación. Se comparó el desempeño de los modelos HOG + SVM y CNN de la biblioteca face_recognition en las tareas de reconocimiento y verificación de rostros. Se realizaron pruebas funcionales, de rendimiento y de seguridad, considerando métricas como precisión, exactitud, tiempos de respuesta y F1-score, lo que permitió verificar la correcta operación de cada componente del sistema. Este enfoque facilitó la determinación de la idoneidad del sistema para entornos educativos y la selección del modelo más adecuado para un control de acceso seguro y eficiente.

5.2. Presentación y monitoreo de resultados

La evaluación del sistema se basó en un enfoque experimental, donde se realizaron diversas pruebas controladas para medir el comportamiento del sistema en distintos escenarios. Para asegurar una comparación válida, se procesaron las mismas imágenes con ambos modelos

de detección facial (HOG + SVM y CNN), y se observaron métricas clave como precisión, exactitud, sensibilidad, F1-score y tasas de error.

5.2.1. Ejecución del monitoreo

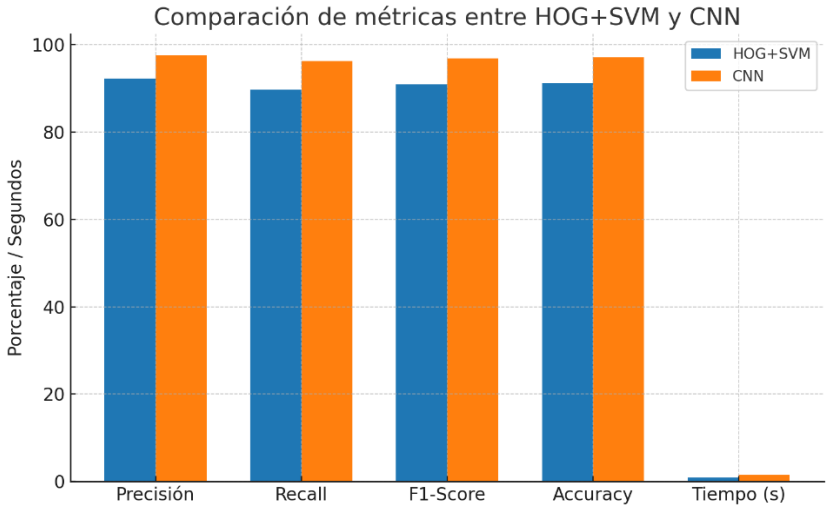
Durante esta fase se realizaron pruebas para evaluar el desempeño del sistema de reconocimiento facial, considerando métricas como el tiempo de respuesta, la exactitud del modelo, precisión, sensibilidad (recall) y F1-score. Además, se compararon los resultados entre los modelos HOG + SVM y CNN. A continuación, se presenta el resumen de los resultados obtenidos:

Tabla 17

Resultados de evaluación del sistema de reconocimiento facial

Métrica	Modelo HOG + SVM	Modelo CNN
Precisión	92.3 %	97.6 %
Recall (Sensibilidad)	89.7 %	96.2 %
F1-Score	90.9 %	96.9 %
Accuracy general	91.2 %	97.1 %
Tiempo promedio (s)	0.87	1.46

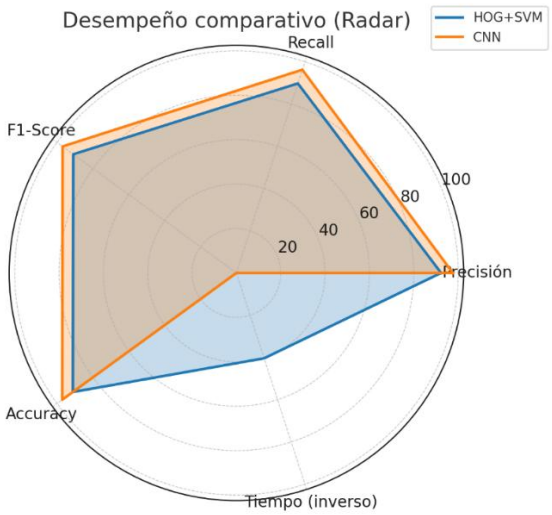
Figura 27



Comparación de métricas de desempeño entre HOG + SVM y CNN

Fuente: Elaboración propia (2025).

Figura 28



Representación del desempeño global de los modelos

Fuente: Elaboración propia (2025).

5.3. Interpretación objetiva

Los resultados demostraron que el sistema cumplió con los objetivos establecidos al inicio del proyecto. El rendimiento del sistema fue aceptable incluso en dispositivos como la Raspberry Pi, donde el modelo HOG + SVM proporcionó respuestas rápidas con una precisión razonable, mientras que el modelo CNN, aunque presentó un menor tiempo de reacción, ofreció mayor exactitud en la identificación. La implementación de la detección de vida se consideró un elemento clave para reforzar la seguridad, ya que redujo significativamente la posibilidad de intentos de suplantación mediante fotografías.

En términos generales, el sistema funcionó correctamente desde el registro de rostros hasta la gestión de accesos y la eliminación de usuarios. La base de datos almacenó los registros de manera confiable, y la interfaz gráfica permitió al personal autorizado operar el sistema de forma intuitiva. La evaluación mediante métricas estándar confirmó de manera objetiva que el sistema no solo cumplió con los objetivos planteados, sino que también demostró resistencia frente a intentos de acceso no autorizado.

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

La revisión bibliográfica permitió identificar avances recientes en reconocimiento facial, redes neuronales y sistemas embebidos, estableciendo un marco conceptual sólido que orientó la selección de metodologías y herramientas apropiadas para el desarrollo del sistema.

Las encuestas y entrevistas realizadas evidenciaron que los principales requerimientos de los usuarios se centraban en seguridad, facilidad de uso y fiabilidad, lo que permitió definir especificaciones alineadas con las necesidades de la comunidad académica.

El desarrollo e implementación del sistema embebido, que integra reconocimiento facial con una base de datos para el registro de accesos, demostró la viabilidad de una solución tecnológica práctica, adaptable y económica para proteger los recursos institucionales.

Las pruebas realizadas mostraron que el sistema alcanza niveles adecuados de precisión, recall, F1-score y exactitud general, confirmando su efectividad para el control de accesos. No obstante, se identificaron limitaciones relacionadas con el tamaño del conjunto de datos y las condiciones ambientales durante las pruebas.

6.2. Recomendaciones

Mantener una revisión periódica de la literatura científica sobre reconocimiento facial, redes neuronales y sistemas embebidos, con el fin de incorporar avances tecnológicos y asegurar la actualización del sistema frente a nuevas técnicas de seguridad biométrica.

Realizar evaluaciones continuas con los usuarios mediante encuestas o entrevistas, para adaptar el sistema a las necesidades reales del entorno académico.

Fortalecer la estructura del sistema con miras a su escalabilidad y posible implementación en otras áreas de la institución, garantizando la protección de los datos biométricos conforme a normativas de privacidad y seguridad.

Ampliar y diversificar la base de datos de imágenes con distintos ángulos, expresiones faciales y condiciones de iluminación, para mejorar la eficacia del modelo y asegurar un funcionamiento robusto en distintos contextos.

BIBLIOGRAFÍA

Acevedo, G., Perez, J., & Gómez, A. (2023). *Aprovechamiento e integración de la tecnología RFID en la administración de la educación*. 10. https://doi.org/10.61117/ipsumtec.v6i5.234

Ameijeiras, D., Gonzáles, H., & Hernándes, Y. (2020). *Revisión de algoritmos de detección y seguimiento de objetos con redes profundas para videovigilancia inteligente*. *14*(3). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992020000300165

Barbachán, E. (2021). *INVESTIGACIÓN TECNOLÓGICA Y PROTOCOLO DE DESARROLLO*. 21.

Bernal, C. (2010). *Metodología de la investigación*. https://abacoenred.org/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf

Botana, J. (2024). *Redes neuronales recurrentes y Transformers para modelos cognitivos del lenguaje*. Ediciones Complutenses. https://www.researchgate.net/publication/382073083_Redes_neuronales_recurrentes_y_Transformers_para_modelos_cognitivos_del_lenguaje

Briano, L. C. A. (2023). *Ingeniería de Software*. http://bibliotecadigital.econ.uba.ar/download/libros/Briano_compilacion_apuntes.pdf

Caeiro, C. (2022). *Regulating facial recognition in Latin America: Policy lessons from police surveillance in Buenos Aires and São Paulo*. Royal Institute of International Affairs. https://doi.org/10.55317/9781784135409

Caturegli, C., & D'Angelo, V. (2022). *Conceptos computacionales con Arduino*. Teseopress. https://www.researchgate.net/publication/375579017_Conceptos_computacionales_con_Arduino

Chimay, A., & Nazila, R. (2020). *Sistemas ciberfísicos en el entorno construido*. https://doi.org/https://doi.org/10.1007/978-3-030-41560-0

Coelho, M. A., Oliveira, F. A. D., Dessimoni, L. H., & Libório, N. S. (2022). Cyber-physical production system assessment within the manufacturing industries in the Amazon. *International Journal of Production Management and Engineering*, *10*(1), 51-64. https://doi.org/10.4995/ijpme.2022.16130

Domínguez, T. (2021). *VISIÓN ARTIFICIAL APLICACIONES PRÁCTICAS CON OPENCV - PYTHON*. https://pocketbook.de/de_de/downloadable/download/sample/sample_id/5448550/?srsltid=AfmBOoqTiGws31bHidF25s_E8op4svtJOSHcBqMRvSBwY3SE8uG4pp-D

Freire, L. A. (2023). *Electrónica y sistemas embebidos. Una visión a nivel técnico y tecnológico*. Centro de Investigación y Desarrollo Ecuador (CIDE). https://repositorio.cidecuador.org/jspui/bitstream/123456789/2398/5/19-12-2024%20Libro%20Electronica%20y%20Sistemas%20Embebidos.pdf

Fuela, J. G. (2022). *Diseño e implementación de una seguridad biométrica con cobertura de red, usando mensajería programada con Telegram asociado con Raspberry pi3 y Arduino para la empresa PHONIX-CELL*. Universidad Politécnica Salesiana.

Gan, W., Hu, K., Huang, G., Chien, W.-C., Chao, H.-C., & Meng, W. (2023). Data Analytic

for Healthcare Cyber Physical System. *IEEE Transactions on Network Science and Engineering*, *10*(5), 2490-2502. https://doi.org/10.1109/TNSE.2023.3278674

Gutiérrez, M., & Damián, M. (2021). *Diseño y desarrollo de un sistema de video vigilancia basado en dispositivos embebidos, técnicas de visión artificial y algoritmos inteligentes*. http://dspace.ups.edu.ec/handle/123456789/19956

Halfacree, G. (2020). *La guía oficial de Raspberry Pi para principiantes: Cómo usa tu nuevo ordenador* (4th edición). Raspberry Pi Trading Ltd. https://www.mclibre.org/descargar/docs/revistas/magpi-books/raspberry-pi-beginners-book-4-es-202011.pdf

Haohan, W., & Bhiksha, R. (2017). *On the Origin of Deep Learning* (No. arXiv:1702.07800). arXiv. https://doi.org/10.48550/arXiv.1702.07800

Hernández, R., Fernández, C., & Baptista, M. del P. (2010). *Metodología de la investigación*. McGRAW-HILL / INTERAMERICANA. https://www.smujerescoahuila.gob.mx/wp-content/uploads/2020/05/Sampieri.Met.Inv.pdf

Hinestroza, V. (2024). *Inteligencia artificial en la seguridad pública y en el sistema penal en América Latina*. https://www.fairtrials.org/app/uploads/2024/08/Inteligencia-artificial-en-la-seguridad-publica-y-en-el-sistema-penal-en-America-Latina.pdf

House, M. (with Institution of Engineering and Technology). (2021). *Code of practice for cyber security in the built environment*. Institution of Engineering and Technology. https://electrical.theiet.org/media/2761/code-of-practice-cyber-security-in-the-built-environment-revised-second-edition.pdf

Jiménez, I. (2018). *Reconocimiento facial basado en redes neuronales convolucionales*. 77.

Jiménez, O., & Díaz, A. (2010). *La seguridad integral: España 2020* (Electronic ed). https://fundacionalternativas.org/wp-content/uploads/2022/07/9e1f8bd80c98311bbef05f6aaf1f3077.pdf

Jiménez, Y., & Merchan, D. (2024). *Desarrollo de un sistema de reconocimiento de imágenes para la clasificación de limones usando Raspberry PI 4 con Python* [UNIVERSIDAD POLITECNICA SALESIANA]. https://dspace.ups.edu.ec/bitstream/123456789/29334/1/UPS-GT005952.pdf?utm_source=chatgpt.com

Khaitan, S., & McCalley, J. (2015). *Design Techniques and Applications of Cyberphysical Systems: A Survey*. *9*(2). https://doi.org/10.1109/jsyst.2014.2322503

Kinsley, H., & Kukieła, D. (2020). *Redes neuronales desde cero en Python*. https://es.scribd.com/document/859991059/Harrison-Kinsley-Daniel-Kukie%C5%82a-Neural-Networks-from-Scratch-in-Python-2020-1-30?utm_source=chatgpt.com

León, A. R., Rodriguez, M., Ponce, G. C., Honorio, L. M., Ruiz, J., & Contreras, J. (2022). *Sistema de reconocimiento facial para control de seguridad en el ingreso a las empresas. Facial recognition system for security control at company entrances. Sistema de reconhecimento facial para controle de segurança nas entradas da empresa*. https://doi.org/10.18050/ingnosis.v8i1.2445

Melo, P. V., & Serra, P. (2022). Tecnologia de Reconhecimento Facial e Segurança Pública

nas Capitais Brasileiras: Apontamentos e Problematizações. *Comunicação e Sociedade*, *42*, 205-220. https://doi.org/10.17231/comsoc.42(2022).3984

Meneses, F. D., & Alvarado, M. (2017). Pronóstico del tipo de cambio USD/MXN con redes neuronales de retropropagación. *Research in Computing Science*, *139*(1), 97-110. https://doi.org/10.13053/rcs-139-1-8

Meneses, G., & Marcelo, D. (2021). *Diseño y desarrollo de un sistema de video vigilancia basado en dispositivos embebidos, técnicas de visión artificial y algoritmos inteligentes*. https://dspace.ups.edu.ec/bitstream/123456789/19956/1/UPS-CT008985.pdf

Nunes, P. (2025, abril 27). *São Paulo, un gran hermano de 25.000 cámaras y reconocimiento facial contra el crimen*. https://elpais.com/america/2025-04-27/sao-paulo-un-gran-hermano-de-25000-camaras-y-reconocimiento-facial-contra-el-crimen.html

Núñez, A., Jácome, J., Vaca, K., Balseca, B., & Jara, R. (2024). Feasibility Enterprise Time and Attendance System Using Artificial Vision Based on Neural Networks with Python and Raspberry Pi. *ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.*, *3*(2), 72-84. https://doi.org/10.18502/espoch.v4i1.15803

Olabe, X. B. (2008). *REDES NEURONALES ARTIFICIALES Y SUS APLICACIONES*. https://ocw.ehu.eus/pluginfile.php/40137/mod_resource/content/1/redes_neuro/contenidos/pdf/libro-del-curso.pdf

Osval, A., López, A., & López, J. (2022). *Métodos de aprendizaje automático estadístico multivariante para la predicción genómica*.

https://link.springer.com/book/10.1007/978-3-030-89010-0

Prince, S. J. D. (2023). *Understanding Deep Learning* (UdBOOK). https://anthology-of-data.science/resources/prince2023udl.pdf?utm_source=chatgpt.com

Restrepo, D., Viloria, J., & Robles, C. (2021). *El camino a las redes neuronales artificiales*. Editorial Unimagdalena. https://doi.org/10.21676/9789587464290

Rico, Y., Lopez, D., & Cerón, A. (2020). *Enfoques y gestión en Seguridad Integral*. https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/Enfoques%20y%20gestio%CC%81n%20en%20Seguridad%20Integral%20EPFA.pdf?ver=1622305517365&utm_source=chatgpt.com

Rivera, I., & Zambrano, D. (2022). *Implementación de reconocimiento facial y visión artificial en robot nao con Python y Opencv* [Universidad Politécnica Salesiana]. https://dspace.ups.edu.ec/bitstream/123456789/22605/1/UPS-GT003738.pdf

Rodríguez, F. (2007). *GENERALIDADES ACERCA DE LAS TÉCNICAS DE INVESTIGACIÓN CUANTITATIVA*. *2*(1). https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://dialnet.unirioja.es/descarga/articulo/4942053.pdf&ved=2ahUKEwjR8diV-PSMAxWUQjABHWNMB3oQFnoECBcQAQ&usg=AOvVaw1LDEaO7SLY2HkW7dXg9N8K

Samad, T., Annaswamy, A., & Annaswamy, A. (2020). *OvErvIEw, SUCCESS STOrIES, AND rESEArCh ChAllENGES*.

Sepúlveda, N., & García, Y. (2022). *Aprendizaje Basado en Proyectos con Arduino*.

https://www.researchgate.net/publication/364242069_Aprendizaje_Basado_en_Proyectos_con_Arduino

Smith, S. (2023). *AI-Driven Cybersecurity: Leveraging Big Data for Advanced Threat Detection and Risk Mitigation*. https://www.researchgate.net/publication/384473262_AI-Driven_Cybersecurity_Leveraging_Big_Data_for_Advanced_Threat_Detection_and_Risk_Mitigation

Toro, A., & Gutiérrez, D. (2020). *Implementación de redes neuronales en Raspberry Pi 3 con Movidius Neural Compute Stick* [Universidad de Sevilla]. https://biblus.us.es/bibing/proyectos/abreproy/71685/fichero/TFM-1685+TORO+VALDERAS%2C+ANTONIO+JOS%C3%89.pdf

Trask, A. W. (2019). *Grokking deep learning*. Manning. https://edu.anarcho-copy.org/Algorithm/grokking-deep-learning.pdf

Tuấn, N. (2019). *Deep Learning*. file:///C:/Users/Usuario/Downloads/Sa_ch_Deep_Learning_co_ba_n.pdf

Universidad de Cartagena, Colombia, Tovar, L. C., Echavez, M. E., Universidad de Cartagena, Colombia, Martelo, R. J., & Universidad de Cartagena, Colombia. (2020). Diseño e implementación de un sistema de biometría facial para el control de acceso en instituciones de educación superior. *Espacios*, *41*(44). https://doi.org/10.48082/espacios-a20v41n44p26

Universidad, P. (2021). *Introducción al Aprendizaje Automático*.

https://dcain.etsin.upm.es/~carlos/bookAA/introAA.html#

Vaca, F., & Rivera, F. (2022). *Diseño e implementación de un sistema de control de acceso mediante reconocimiento facial para la academia Titanes Cuenca*. https://dspace.ups.edu.ec/bitstream/123456789/24611/1/UPS-CT010421.pdf

Vásquez, A. A., Guanuchi, L. M., Cahuana, R., Vera, R., & Holgado, J. (2023). *Métodos de investigación científica* (1.ª ed.). Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. https://doi.org/10.35622/inudi.b.094

Vega Luna, J. I., Sánchez-Rangel, F. J., Salgado-Guzmán, G., & Lagos-Acosta, M. A. (2018). Sistema de acceso usando una tarjeta RFiD y verificación de rostro. *Ingenius*, *20*, 108-118. https://doi.org/10.17163/ings.n20.2018.10

Vorobioff, J., Cerrotta, S., & Amadio, A. (2022). *Inteligencia Artificial y Redes Neuronales Fundamentos, Ejercicios y Aplicaciones:* EdUTecNe. https://www.researchgate.net/publication/359716455_Inteligencia_Artificial_y_Redes_Neuronales_Fundamentos_Ejercicios_y_Aplicaciones

Weidman, S. (2019). *Aprendizaje profundo desde cero: Construyendo con Python desde los primeros principios* (ilustrada ed.). https://www.coursehero.com/file/181845251/deeplearningfromscratchpdf/?utm_source=chatgpt.com

ANEXOS

ANEXO A:

Aprobación de tema

Universidad Laica Eloy Alfaro de Manabí

Periodo 2024-2025(2) - Notificación de tutor asignado - TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Estimad@
Docente y Estudiante
Uleam

En cumplimiento de lo establecido en la Ley, el Reglamento de Régimen Académico y las disposiciones estatutarias de la Uleam, por medio de la presente se oficializa la dirección y tutoría en el desarrollo del Trabajo de Integración curricular / Trabajo de Titulación del siguiente estudiante:

Tema: SISTEMA INFORMATICO CON REDES NEURONALES PARA LA SEGURIDAD EN LA SALA DE PROFESORES DE TI Y SOFTWARE DE LA ULEAM EXTENSIÓN EL CARMEN

Estado de aprobación: Aprobado

Tipo de titulación: Trabajo de Integración Curricular

Tipo de proyecto: Trabajo de Integración Curricular / Trabajo de titulación se articula con proyectos y programas de Investigación.

Apellidos y nombres del tutor asginado: SINCHIGUANO CHIRIBOGA CESAR AUGUSTO

Apellidos y nombres del estudiante: LOOR MERA NAYELI MARIA

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2024-2025(2)

ANEXO B:

Certificado de coincidencias académicas

CERTIFICADO DE ANÁLISIS
magister

Trabajo_Titulacion_Fase_Resultados_NayeliLoorMera

7% Textos sospechosos

- 1% Similitudes
  0% similitudes entre comillas
  < 1% entre las fuentes mencionadas
- 3% Idiomas no reconocidos
- 4% Textos potencialmente generados por la IA

Nombre del documento: Trabajo_Titulacion_Fase_Resultados_NayeliLoorMera.pdf
ID del documento: b3c5100b0b610d2fe2f87ae5befe08d9f17870bc
Tamaño del documento original: 4,12 MB

Depositante: CESAR SINCHIGUANO CHIRIBOGA
Fecha de depósito: 25/8/2025
Tipo de carga: interface
fecha de fin de análisis: 25/8/2025

Número de palabras: 21.817
Número de caracteres: 163.618

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dx.doi.org | Asistencia inteligente: optimizando el registro de asistencia en la Univ... http://dx.doi.org/10.26507/paper.3917	< 1%		Palabras idénticas: < 1% (54 palabras)
2	repositorio.uleam.edu.ec https://repositorio.uleam.edu.ec/bitstream/123456789/7519/1/ULEAM-TEC-INF-072.pdf	< 1%		Palabras idénticas: < 1% (46 palabras)
3	www.mendeley.com | Pronóstico del tipo de cambio USD... preview & related inf... https://www.mendeley.com/catalogue/ba224cba-bf84-3776-9bc1-4c46f19f9837/	< 1%		Palabras idénticas: < 1% (22 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dspace.ups.edu.ec | Diseño e implementación de un sistema de control de acces... http://dspace.ups.edu.ec/handle/123456789/24611	< 1%		Palabras idénticas: < 1% (34 palabras)
2	doi.org | Feasibility Enterprise Time and Attendance System Using Artificial Vision ... https://doi.org/10.18502/espoch.v4i1.15803	< 1%		Palabras idénticas: < 1% (29 palabras)
3	Suly Gabriela Caicedo Mero y Evelyn Jamileth Chavarria Mendoza.doc... #3a3608 Viene de de mi grupo	< 1%		Palabras idénticas: < 1% (30 palabras)
4	rraae.cedia.edu.ec | Record Citations https://rraae.cedia.edu.ec/Record/UPS_6b95d420e03c59aace4fdcb1dbfe837e/Cite	< 1%		Palabras idénticas: < 1% (30 palabras)
5	dspace.ups.edu.ec | Diseño y desarrollo de un sistema de video vigilancia basad... http://dspace.ups.edu.ec/handle/123456789/19956	< 1%		Palabras idénticas: < 1% (20 palabras)

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1. https://doi.org/10.61117/ipsumtec.v6i5.234
2. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992020000300165
3. https://abacoenred.org/wp
4. https://www.researchgate.net/publication/382073083_Redes_neuronales_recurrentes
5. http://bibliotecadigital.econ.uba.ar/download/libros/Briano_compilacion_apuntes.pdf

ANEXO C:

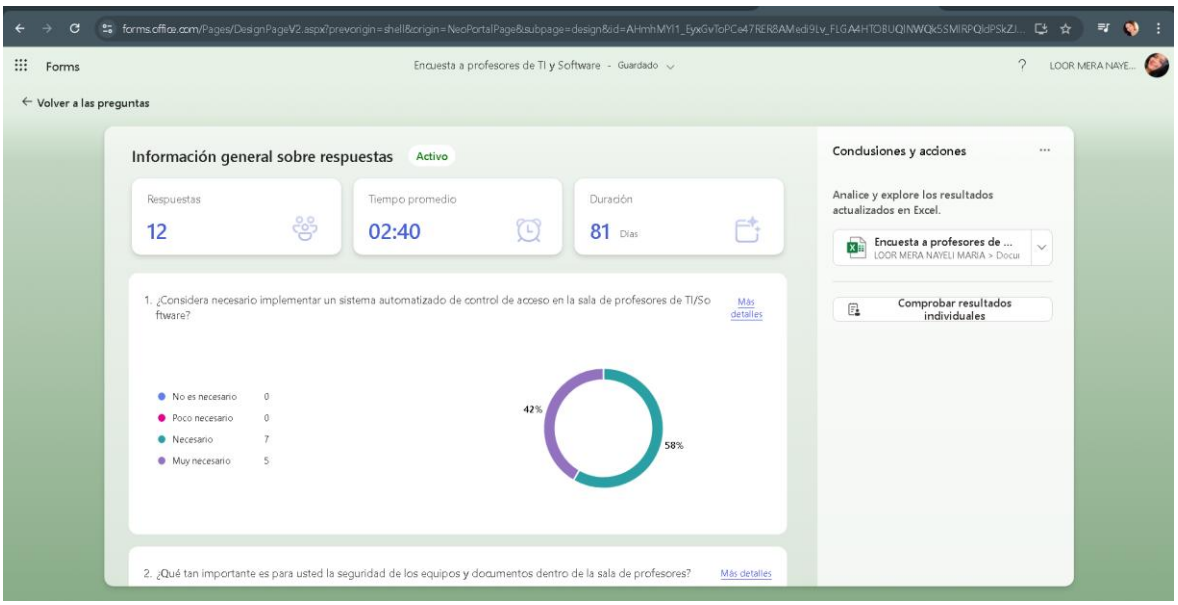
Tutoría con docente tutor

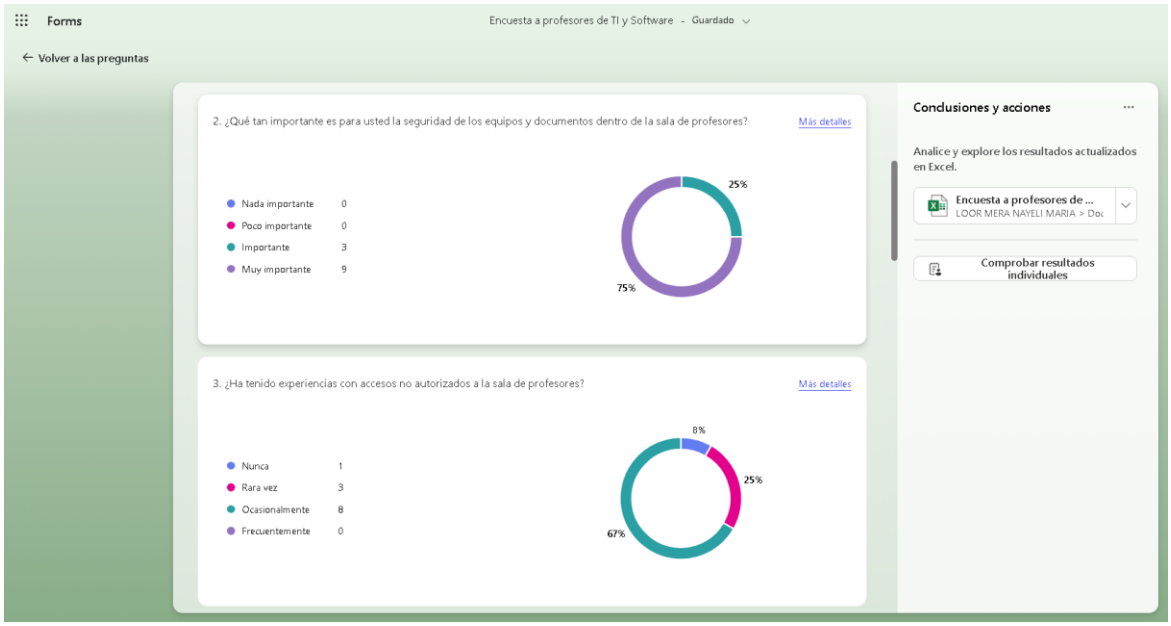
Capturando imágenes del docente

ANEXO D:

Evidencia de aplicación de encuestas y entrevistas

Evidencia de encuestas





Evidencia de entrevista

ENTREVISTA

Entrevistado: Ing. Rocío Mendoza	**Fecha:** 07/05/2025
Objetivo: Profundizar en las experiencias, expectativas y recomendaciones de expertos sobre el sistema propuesto.	

Preguntas:

1. Desde su experiencia, ¿cuáles son los principales riesgos de seguridad en el acceso actual a la sala de profesores de TI/Software?

Actualmente no hay ningun sistema de seguridad la cerradura no vale, lo que significa que cualquier persona puede ingresar

2. ¿Qué ventajas y desventajas observa en implementar un sistema de reconocimiento facial con redes neuronales, en comparación con métodos tradicionales como claves o tarjetas?

Tendria varias ventajas desde solo acercarse y poder ingresar a un determinado lugar, de acceder a cuentas bancarias, etc. desventaja necesitan procesar grandes volumnes de dato

3. ¿Considera que factores del entorno, como la iluminación, pueden afectar el funcionamiento del sistema de reconocimiento facial?

el angulos de donde se realice la captura y accserios que la persona puede tener en su rostro

4. Según su criterio, ¿qué requisitos técnicos debe cumplir el sistema para ser viable en la ULEAM extensión El Carmen?

un buen equipo de reconocimiento facial, que las imagenes esten bien alieadas, bien recortadas

5. ¿Qué desafíos institucionales anticipa para su implementación de este sistema (por ejemplo: capacitación del personal, costos, ¿resistencia al cambio)?

El uso que se les pueda dar como el control de asistencias a todo el personal

6. ¿Cómo debería manejarse el acceso de personas externas autorizadas como personal administrativo o invitados)?

si estan autorizadas si constan en la BD, sino son autorizadas llevar un registro para persona externas donde se registres varios datos importantes

7. ¿Cuál es su opinión sobre la sensibilidad y el correcto manejo de los datos biométricos que serán almacenados?

De que estos datos puedan ser usados para otros fines

8. ¿Qué protocolos de emergencia deberían contemplarse en el sistema? (por ejemplo: fallos técnicos, intentos de acceso no autorizado)

alertas, bloqueos

GLOSARIO

Aprendizaje profundo (Deep Learning): Subcampo de la inteligencia artificial que utiliza redes neuronales multicapa para procesar y analizar datos complejos, como imágenes, audio o texto.

Antispoofing: Conjunto de técnicas que evitan fraudes en sistemas biométricos mediante fotos, videos o máscaras para suplantar la identidad de una persona.

Autenticación biométrica: Proceso de verificación de identidad basado en características físicas únicas, como rostro, huella dactilar o iris, que garantiza el acceso seguro a sistemas y espacios.

Base de datos relacional: Modelo de almacenamiento de información organizado en tablas relacionadas mediante claves primarias y foráneas.

Biometría: Técnica de identificación de personas mediante características físicas o conductuales únicas, como huellas dactilares, iris, voz o rostro.

Ciberseguridad: Conjunto de prácticas, tecnologías y procesos destinados a proteger sistemas informáticos, redes y datos frente a amenazas digitales o accesos no autorizados.

CNN (Convolutional Neural Network): Red neuronal especializada en el procesamiento de imágenes mediante convolución, capaz de identificar patrones y características espaciales.

Codificación facial (Face Encoding): Representación numérica de los rasgos faciales que permite comparar y reconocer rostros de manera automática.

Detección de vida (Liveness Detection): Técnica utilizada en sistemas de reconocimiento facial para verificar que el rostro capturado corresponde a una persona real y no a una foto o máscara.

Face_recognition: Biblioteca de Python que permite reconocer rostros mediante codificación y comparación con una base de datos de imágenes.

HOG (Histogram of Oriented Gradients): Algoritmo que detecta objetos o personas analizando gradientes de intensidad en las imágenes.

Inteligencia Artificial (IA): Disciplina que desarrolla sistemas capaces de realizar tareas que requieren inteligencia humana, como aprendizaje, razonamiento y percepción.

Interfaz gráfica (GUI): Medio visual de interacción entre el usuario y el sistema, que facilita la gestión de funciones como registro de usuarios y control de acceso.

OpenCV: Biblioteca de código abierto que proporciona herramientas para procesar imágenes y video en tiempo real.

Parpadeo o blink detection: Técnica que analiza el movimiento de los párpados para verificar que la persona frente a la cámara es real.

Raspberry Pi: Computadora de bajo costo y tamaño reducido, utilizada en sistemas embebidos para procesamiento local de datos y control de dispositivos.

Redes neuronales: Modelos computacionales inspirados en el cerebro humano que aprenden patrones a partir de datos de entrada y pueden realizar predicciones o clasificaciones.

Reconocimiento facial: Técnica que identifica o verifica la identidad de una persona mediante el análisis de sus rasgos faciales.

Registro de accesos: Proceso de almacenar y consultar información sobre las entradas y salidas de personas a un determinado espacio.

Relé: Componente electrónico que permite controlar dispositivos físicos, como puertas o luces, desde sistemas embebidos.

Seguridad física: Conjunto de medidas y procedimientos destinados a proteger espacios, personas y recursos frente a accesos no autorizados.

Sistemas embebidos: Dispositivos electrónicos diseñados para realizar funciones específicas de manera autónoma, integrando hardware y software en un mismo sistema.

SQLite: Sistema de gestión de bases de datos ligero que permite almacenar y consultar información localmente.

Visión computacional: Área de la inteligencia artificial que se encarga de interpretar y procesar imágenes o videos para que las máquinas puedan analizar el entorno.