



PORTADA

**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 INGENIERA EN
TECNOLOGÍAS DE LA INFORMACIÓN**

**SISTEMA INFORMÁTICO CON REDES NEURONALES PARA LA
SEGURIDAD FÍSICA EN EL LABORATORIO DE CÓMPUTO 1 DE LA
ULEAM EXTENSIÓN EL CARMEN.**

**VELÁZQUEZ VERGARA EVELYN JAZMIN
AUTOR**

**ING. MORA MARCILLO ALEX BLADIMIR, MG.
TUTOR**

EL CARMEN, AGOSTO 2025



CERTIFICACIÓN DEL TUTOR

	NOMBRE DEL DOCUMENTO:	CÓDIGO: PAT-04-F-004
	CERTIFICADO DE TUTOR(A).	REVISIÓN: 1
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	Página 1 de 1

CERTIFICACIÓN

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

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría de la estudiante VELAZQUEZ VERGARA EVELYN JAZMIN, legalmente matriculado en la carrera de Tecnologías de la Información, período académico 2025(1), cumpliendo el total de 384 horas, cuyo tema del proyecto es "SISTEMA INFORMATICO CON REDES NEURONALES PARA LA SEGURIDAD FISICA EN EL LABORATORIO DE COMPUTO 1 DE LA ULEAM EXTENSION 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, y la originalidad del mismo, requisitos 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.

El Carmen, 20 de agosto de 2025.

Lo certifico,



Ing. Alex Bladimir Mora Marcillo, Mg.
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 Fisica en el Laboratorio de Cómputo 1 de la Uleam Extension El Carmen

Modalidad: Proyector Integrador

Autora: Velazquez Vergara Evelyn Jazmin

Tutor: Ing. Mora Marcillo Alex Bladimir, Mg.

Tribunal de Sustentación:

Presidente:

Mg. Minaya Macias Renelmo Wladimir.

Miembro:

Ing. Pozo Hernandez Clara Guadalupe, Mg.

Miembro:

Ing. Arévalo Hermida Rómulo Danilo, Mg.

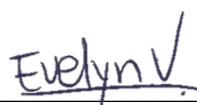
Fecha de Sustentación: 10 de septiembre de 2025

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 física en el laboratorio de cómputo 1 de la ULEAM Extensión El Carmen, corresponde exclusivamente a: Velazquez Vergara Evelyn Jazmin con CI. 1727315689 y los derechos patrimoniales de la misma corresponden a la Universidad Laica “Eloy Alfaro” de Manabí.



Velazquez Vergara Evelyn Jazmin

C.I. 1727315689

DEDICATORIA

Este logro se lo dedico a mis padres, quienes han sido el motor que me impulsó a alcanzar cada uno de mis sueños.

A mi madre, por ser mi guía inquebrantable, por mantenerme firme en los momentos más difíciles, por sus oraciones constantes, sus sabios consejos, y por secar mis lágrimas cuando sentí que no podía más. Gracias por tu fortaleza, por tu amor incansable y por no rendirte nunca, incluso cuando el camino se volvía cuesta arriba, eres el pilar que me sostuvo y me enseñó a caminar con fe y determinación.

A mi padre, cuya presencia ha sido constante a pesar de la distancia, con su esfuerzo diario y trabajo incansable me enseñó que el amor también se demuestra en el compromiso, en la responsabilidad y en el sacrificio silencioso. Sus palabras de aliento, siempre oportunas, fueron un sostén en los momentos en que flaqueaba. Gracias por ser un pilar firme en este proceso, por mostrarme con tu vida el verdadero valor del esfuerzo y la dedicación.

Este título no solo representa una meta alcanzada, sino que lleva impreso el amor, la sabiduría y los valores que me inculcaron. Espero ser el ser humano y profesional que tanto anhelaron, sin olvidar mis raíces y llevando con orgullo los apellidos de quienes me formaron con tanto amor.

Todo esto, y mucho más, es por y para ustedes. Los amo profundamente.

Velázquez Vergara Evelyn Jazmin

AGRADECIMIENTO

Gracias, Dios, por acompañarme cada día, por darme fuerza cuando creí rendirme, y por poner en mi vida personas que fueron luz en este camino. A mis padres, por su amor incondicional y por enseñarme que siempre puedo volver al hogar donde me esperan con fe, paciencia y ternura. A mis hermanos, por su presencia silenciosa pero constante, por ser parte de mi fuerza. A mi hija Alaia, por enseñarme lo que es el amor más puro y ser mi impulso diario. A mi pequeño René, por habitar mi corazón y recordarme que el amor no necesita presencia física para ser eterno. A mi compañero de vida, por sostenerme con su amor firme y caminar conmigo incluso en mis pasos más cansados. Este logro también es tuyo. A mis amigas verdaderas, por estar, por creer en mí y por su apoyo sincero. A mis docentes, por su guía, su paciencia y por compartir mucho más que conocimiento. Gracias por dejar huellas que me acompañarán siempre. Y a ti, mi amigo que partiste...gracias por tu apoyo, tus palabras, tu fe en mí. Este logro también lleva tu nombre. Siempre vivirás en mi memoria.

Velázquez Vergara Evelyn Jazmin

ÍNDICE GENERAL

PORTADA.....	I
CERTIFICACIÓN DEL TUTOR.....	II
TRIBUNAL DE SUSTENTACIÓN.....	III
DECLARACIÓN DE AUTORÍA.....	IV
DEDICATORIA	V
AGRADECIMIENTO	VI
ÍNDICE GENERAL	VII
ÍNDICE DE TABLAS	XII
ÍNDICE DE ILUSTRACIONES	XIV
ÍNDICE DE ANEXOS	XVII
RESUMEN	XVIII
ABSTRACT.....	XIX
CAPÍTULO I	1
1. INTRODUCCIÓN.....	1
1.1 Preámbulo.....	1
1.2 Presentación del tema.....	1
1.3 Ubicación y contextualización de la problemática.....	1
1.4 Planteamiento del problema	2
1.4.1 Problematización.....	2

1.4.2	Génesis del problema	2
1.4.3	Estado actual del problema	3
1.5	Diagrama causa – efecto del problema	4
1.6	Objetivos	4
1.6.1	Objetivo general.....	4
1.6.2	Objetivos específicos	4
1.7	Justificación.....	5
1.8	Impactos esperados	5
1.8.1	Impacto tecnológico.....	5
1.8.2	Impacto social	5
1.8.3	Impacto ecológico	6
CAPÍTULO II		7
2.	MARCO TEÓRICO.....	7
2.1	Antecedentes históricos.....	7
2.1.1	Sistemas informáticos	7
2.1.2	Redes neuronales	7
2.1.3	Seguridad física.....	8
2.2	Antecedentes de investigaciones relacionadas al tema presentado	8
2.3	Definiciones conceptuales.....	9
2.3.1	Sistema Informático	9
2.3.2	Seguridad física.....	16

2.4	Conclusiones del marco teórico	20
CAPÍTULO III.....		22
3.	MARCO INVESTIGATIVO	22
3.1	Introducción	22
3.2	Tipos de investigación.....	22
3.2.1	Investigación Bibliográfica.....	22
3.2.2	Investigación Aplicada.....	22
3.2.3	Investigación de campo.....	23
3.3	Métodos de investigación.....	23
3.3.1	Estudio de caso	23
3.3.2	Método cualitativo	24
3.3.3	Método cuantitativo	24
3.4	Fuentes de información de datos.....	25
3.4.1	Fuente primaria	25
3.4.2	Fuente secundaria.....	25
3.5	Estrategia operacional para la recolección de datos.....	26
3.5.1	Población.....	26
3.5.2	Análisis de las herramientas de recolección de datos a utilizar	26
3.5.3	Plan de recolección de datos	27
3.6	Análisis y presentación de resultados.....	28
3.6.1	Análisis encuesta.....	28

3.6.2	Análisis entrevista.....	32
3.6.3	Presentación y descripción de los resultados obtenidos	37
3.6.4	Informe final del análisis de los datos.....	38
CAPÍTULO IV.....		39
4.	MARCO PROPOSITIVO	39
4.1	Introducción	39
4.2	Descripción de la propuesta	39
4.3	Determinación de recursos	41
4.3.1	Humanos	41
4.3.2	Hardware.....	41
4.3.3	Software	42
4.3.4	Económicos.....	43
4.4	Desarrollo <i>SCRUM</i>	44
4.4.1	Roles	45
4.4.2	Historias de usuario.....	46
4.4.3	Product backlog	49
4.4.4	Estimación Product Backlog.....	52
4.4.5	Requerimientos del sistema	52
4.4.6	Identificación de riesgos	53
4.4.7	Sprint 1.....	54
4.4.8	Sprint 2.....	66

4.4.9	Sprint 3.....	75
4.4.10	Mapa de navegación del sistema.....	85
4.4.11	Proceso de pruebas	85
CAPÍTULO V.....		90
5.	EVALUACIÓN DE RESULTADOS	90
5.1	Introducción	90
5.2	Presentación y monitoreo de resultados	90
5.2.1	Problemas detectados encuestas y entrevistas (El problema).....	90
5.2.2	Planificación de la evaluación	91
5.2.3	Ejecución del monitoreo	92
5.3	Interpretación objetiva.....	94
CAPÍTULO VI.....		96
6.	CONCLUSIONES Y RECOMENDACIONES	96
6.1	Conclusiones	96
6.2	Recomendaciones.....	97
BIBLIOGRAFÍA		98
ANEXOS		107
GLOSARIO		112

ÍNDICE DE TABLAS

Tabla 1: Eventos y artefactos SCRUM. (Zalimben, 2022).....	20
Tabla 2: Análisis de encuesta.....	32
Tabla 3: Análisis de entrevista.....	37
Tabla 4: Recursos Humanos	41
Tabla 5. Hardware utilizado.....	42
Tabla 6. software utilizado.....	42
Tabla 7. costos de implementación.....	44
Tabla 8: Roles Scrum.....	46
Tabla 9: Historia 1 login usuarios.....	46
Tabla 10: Historia 2 Registro docentes.....	46
Tabla 11: Historia3 Reconocimiento facial	47
Tabla 12: Historia4 Validación de horarios	47
Tabla 13: Historia5 gestión de horarios	48
Tabla 14: Historia6 Generación de reportes	48
Tabla 15: Historia 7 configuración de sistema	48
Tabla 16: Historia 8 apertura de cerradura	49
Tabla 17: Historia 9 Optimización.....	49
Tabla 18: Product Backlog.....	51
Tabla 19. Estimación Product Backlog.....	52
Tabla 20: Riesgos.....	54

Tabla 21: Sprint Planning (sprint1).....	54
Tabla 22: Especificación caso de uso Sprint1.....	55
Tabla 23. Dailys Sprint 1	58
Tabla 24. Burn-Down Sprint 1.....	58
Tabla 25:: Sprint Planning (sprint2)	66
Tabla 26.Dailys Sprint 2	69
Tabla 27. Burn-Down Sprint 2.....	70
Tabla 28:: Sprint Planning (sprint3)	75
Tabla 29: Caso de uso Sprint 3	76
Tabla 30.Dailys Sprint 3	77
Tabla 31. Burn-Down Sprint 3.....	78
Tabla 32: Pruebas de sistema.....	84
Tabla 33:Frecuencia de problemas por ausencia del conserje	90
Tabla 34:Consecuencias de no tener control de acceso	91
Tabla 35:Opinión sobre reconocimiento facial como solución	91
Tabla 36: Indicadores definidos para la evaluación del sistema.....	92
Tabla 37: Resultados obtenidos en las pruebas funcionales del sistema	92
Tabla 38:Resultados de la encuesta de satisfacción (resumen de docentes).....	93
Tabla 39: Monitoreo registro de docente	93

ÍNDICE DE ILUSTRACIONES

Ilustración 1: Estructura de un sistema informático.	10
Ilustración 2 Componentes Principales de un Sistema Informático. (Marcatoma, 2022)	11
Ilustración 3: Modelo de funcionamiento	41
Ilustración 4: Caso de uso Sprint 1	55
Ilustración 5: Diagrama de secuencia registro docente.....	56
Ilustración 6: Diagrama de estado registro docente.....	56
Ilustración 7. Release Burn-Down Sprint 1	59
Ilustración 8: Diseño de base de datos	60
Ilustración 9: Diseño Login	60
Ilustración 10: Código Validación JS Login.....	61
Ilustración 11: Código Login API.....	62
Ilustración 12: Formulario Registro Docente	63
Ilustración 13: Código Captura de rostro con cámara	64
Ilustración 14: Código Envío de rostro a Flask	64
Ilustración 15: Código Proceso de reconocimiento y validación.....	65
Ilustración 16. Caso de uso Sprint 2	67
Ilustración 17: Especificación caso de uso Sprint 2.....	67
Ilustración 18: Diagrama de secuencia gestión de horarios.....	68
Ilustración 19: Diagrama de estados horarios.....	68
Ilustración 20. Release Burn-Down Sprint 2	71

Ilustración 21: CRUD Horarios	72
Ilustración 22: Código Listar Horarios	73
Ilustración 23: Código Validación de Horarios	74
Ilustración 24: Hardware (ESP32+CERRADURA)	74
Ilustración 25. Caso de uso Sprint 2	75
Ilustración 26: Diagrama de secuencia reportes	76
Ilustración 27: Diagrama de estado reportes.....	77
Ilustración 28. Release Burn-Down Sprint 3	78
Ilustración 29: Diseño de Lista de Reportes de Acceso	79
Ilustración 30: Diseño de lista de Aulas	80
Ilustración 31: Diseño de lista de Periodos.....	80
Ilustración 32: Código del listado de Reportes	81
Ilustración 33: Código del listado de aulas	82
Ilustración 34: Código C# en el ESP32, parte 1	82
Ilustración 35: Código C# en el ESP32, parte 2	83
Ilustración 36: Pruebas físicas	83
Ilustración 37: Mapa de navegación. Elaboración Propia	85
Ilustración 38: Prueba caja negra, formulario login.....	85
Ilustración 39: Prueba caja negra, formulario Registro docente.....	86
Ilustración 40: Prueba caja negra, formularios horarios	86
Ilustración 41: Prueba caja negra, formulario aulas.....	87

Ilustración 42:Prueba caja negra, formulario periodos	87
Ilustración 43:Prueba caja blanca, formulario login	87
Ilustración 44:Prueba caja blanca, formulario Registro docente	88
Ilustración 45: Prueba caja blanca, formularios horarios.....	88
Ilustración 46:Prueba caja blanca, formulario aulas	89
Ilustración 47:Prueba caja blanca, formulario periodos	89
Ilustración 48: Modelo de reconocimiento	94
Ilustración 49: Prueba de esp32	109
Ilustración 50: Prueba de apertura de cerradura	109
Ilustración 51: Encuesta a docentes	110
Ilustración 52: Encuesta a docentes	110
Ilustración 53: Entrevista a técnico.....	111

ÍNDICE DE ANEXOS

Anexos 1: Asignación de tutor	107
Anexos 2: Reporte del sistema antiplagio	108
Anexos 3: Fotografías.....	109
Anexos 4: Evidencia de aplicación de encuestas y entrevistas	110

RESUMEN

Este proyecto tiene el objetivo de mejorar seguridad y control de acceso en el laboratorio de cómputo 1 de la ULEAM Extensión El Carmen, donde la gestión actual causaba accesos no autorizados y usos ineficientes de los recursos, por ello, se propuso y desarrollo un sistema informático de la mano de herramientas de seguridad física, donde se usó redes neuronales, para automatizar el acceso y asegurar que solo personal autorizado ingrese, mejorando así la gestión del laboratorio. Para ello, se investigó el tema de la seguridad física y el uso de las redes neuronales en el reconocimiento facial, con investigaciones como la bibliográfica, aplicada y de campo. Y métodos cuantitativos y cualitativos enfocados a la recolección de información clave mediante las técnicas de encuesta y entrevista a una muestra de 9 personas de una población de la misma cantidad conformada solo de docentes y el encargado del laboratorio, el desarrollo se realizó con la metodología ágil SCRUM, construyendo un backend con lenguajes como flask, php, c#, javascript y dotándolo de reconocimiento facial en donde use tecnologías como OpenCV y face_recognition, complementado por un frontend en react para una interacción sencilla. Los resultados obtenidos en cuanto a la velocidad de autenticación es un tiempo de 5 segundos y en precisión al momento de reconocer los rostros obtuvo un 84% según las pruebas realizadas. La gran mayoría de los docentes consideró que el sistema tiene una alta facilidad de uso y felicitó la innovación en la gestión de ingresos al laboratorio. La parte para considerar fue que el sistema mostró limitaciones en ambientes con baja iluminación al no poder procesar las imágenes. En resumen, se puede concluir que resulta una solución efectiva y viable a la problemática de seguridad en el laboratorio, sirviendo de ejemplo a futuras implementaciones.

ABSTRACT

This project aims to improve security and access control in computer lab 1 at ULEAM Extensión El Carmen. The existing management system led to unauthorized access and inefficient use of resources. To address this, a new computer system was proposed and developed, incorporating physical security tools and using neural networks to automate access and ensure only authorized personnel can enter, thereby improving lab management. To achieve this, research was conducted on physical security and the use of neural networks for facial recognition, utilizing bibliographic, applied, and field research methods. We also employed quantitative and qualitative methods to collect key information through surveys and interviews with a sample of 9 people from a population of the same size, consisting of teachers and the lab manager. The development was carried out using the SCRUM agile methodology. The backend was built with languages like Flask, PHP, C#, and JavaScript, and it was equipped with facial recognition using technologies like OpenCV and face_recognition. This was complemented by a React frontend for a simple user experience. The authentication speed results showed a time of 5 seconds, and the facial recognition accuracy was 84% based on the tests performed. The vast majority of teachers considered the system to be very easy to use and commended the innovation in managing lab access. A limitation to consider was the system's inability to process images in low-light environments. In summary, we can conclude that this is an effective and viable solution to the lab's security problem, serving as an example for future implementations.

CAPÍTULO I

1. INTRODUCCIÓN

1.1 Preámbulo

En la "Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen," se ha identificado una problemática significativa relacionada con la gestión de la seguridad y el control de acceso en el Laboratorio de Cómputo 1. En la actualidad, el acceso al laboratorio se maneja de manera manual, lo que ha dado lugar a problemas como el acceso no autorizado y el mal uso de los recursos disponibles. Este enfoque tradicional no solo pone en riesgo la seguridad de los equipos, sino que también afecta la eficiencia y puntualidad de las actividades académicas debido a la dependencia del conserje para abrir el laboratorio.

Como solución a la problemática encontrada se propone el desarrollo e implementación de un sistema informático basado en redes neuronales para el control de acceso en el laboratorio de cómputo 1, con este proyecto se busca tener mayor control y automatizar las entradas y salidas del laboratorio, y así garantizar que solo personas autorizadas tengan ingreso y se lleve un registro de ello.

A continuación, se muestra por qué el proyecto es viable y que cual es el impacto esperado. Primeramente, la implementación del sistema no solo resolverá los problemas actuales de seguridad y gestión de ingresos, sino que también servirá como modelo para futuras aplicaciones tecnológicas en otros espacios académicos de la universidad, así como también se espera su amplia influencia en el ámbito social, tecnológico y ecológico de la institución.

1.2 Presentación del tema

Sistema informático con redes neuronales para la seguridad física en el laboratorio de cómputo 1 de la ULEAM Extensión El Carmen.

1.3 Ubicación y contextualización de la problemática

La Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen, se encuentra en la provincia de Manabí, en el cantón El Carmen, con una sede principal en Manta. Esta institución es altamente reconocida en la región por su compromiso con la excelencia educativa y su amplia oferta académica. Desde sus inicios, la universidad ha dado como prioridad proporcionar una educación digna y de calidad, siempre buscando estar a la vanguardia en la implementación de nuevas tecnologías.

A pesar de estas mejoras físicas, el laboratorio enfrenta serios problemas relacionados con la seguridad y la gestión. La carencia de un sistema para el control de acceso ha dejado al laboratorio vulnerable a accesos de personas mal intencionadas que podrían dar un mal uso de los recursos. Los docentes frecuentemente no vigilan el cierre del laboratorio al finalizar sus clases, por lo que muchas veces quedan personas dentro y sin supervisión. Además, la necesidad de buscar al conserje para abrir la puerta en caso de acceso puede causar retrasos en las actividades y afecta la puntualidad.

La ausencia de un sistema de registro efectivo impide un control adecuado sobre quién entra y sale del laboratorio, así como un seguimiento del uso de los recursos. Esto no solo compromete la seguridad de los equipos, sino que también dificulta la gestión y la correcta utilización del espacio.

Para resolver los problemas de seguridad en el laboratorio de cómputo 1, la propuesta es crear un sistema que use inteligencia artificial para reforzar la seguridad física. La idea principal es tener un control más estricto y eficiente de quién entra y quién sale. El sistema registrará automáticamente a las personas, así asegura de que solo la gente autorizada pueda entrar.

1.4 Planteamiento del problema

1.4.1 Problematicación

La falta de un sistema de control de acceso en el laboratorio 1 de la Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen ha provocado diversos inconvenientes relacionados con la seguridad y el uso no autorizado de los recursos del laboratorio. Actualmente, el acceso a los laboratorios se realiza manualmente sin registros precisos de quién ha ingresado, lo que aumenta el riesgo de robo o uso indebido del equipo. Este problema afecta tanto a administradores como a estudiantes porque amenaza la seguridad de los activos y el uso ordenado de los recursos.

1.4.2 Génesis del problema

En muchas ocasiones, al finalizar las clases, los docentes se retiran sin cerrar el laboratorio, dejando el espacio abierto y sin supervisión. Además, el docente que tiene la siguiente clase no siempre se dirige directamente al laboratorio, sino que se queda en el aula, lo que permite que el laboratorio quede vulnerable al acceso de personas no autorizadas. Por

ello es preocupante que los equipos corran algún tipo de riesgo al estar sin vigilancia y de puerta abierta a robos o problemas aún mayores.

Uno de los problemas que enfrentan los docentes es que, al momento de querer impartir clases en el laboratorio, estos se encuentran cerrados y deben recurrir al conserje para que les de acceso, y muchas veces el conserje se encuentra en otros lugares haciendo diligencias y es difícil dar con él, por ello se pierde tiempo. Por esto un sistema como el planteado ahorraría tiempo y daría más puntualidad a las clases.

Actualmente, no existe un sistema que registre el acceso y las actividades realizadas en el laboratorio. La falta de control sobre quién entra y sale, así como sobre el uso de los recursos, dificulta la correcta gestión del laboratorio. Esto no solo impide conocer los patrones de uso, sino que también incrementa el riesgo de mal uso o desgaste prematuro de los equipos.

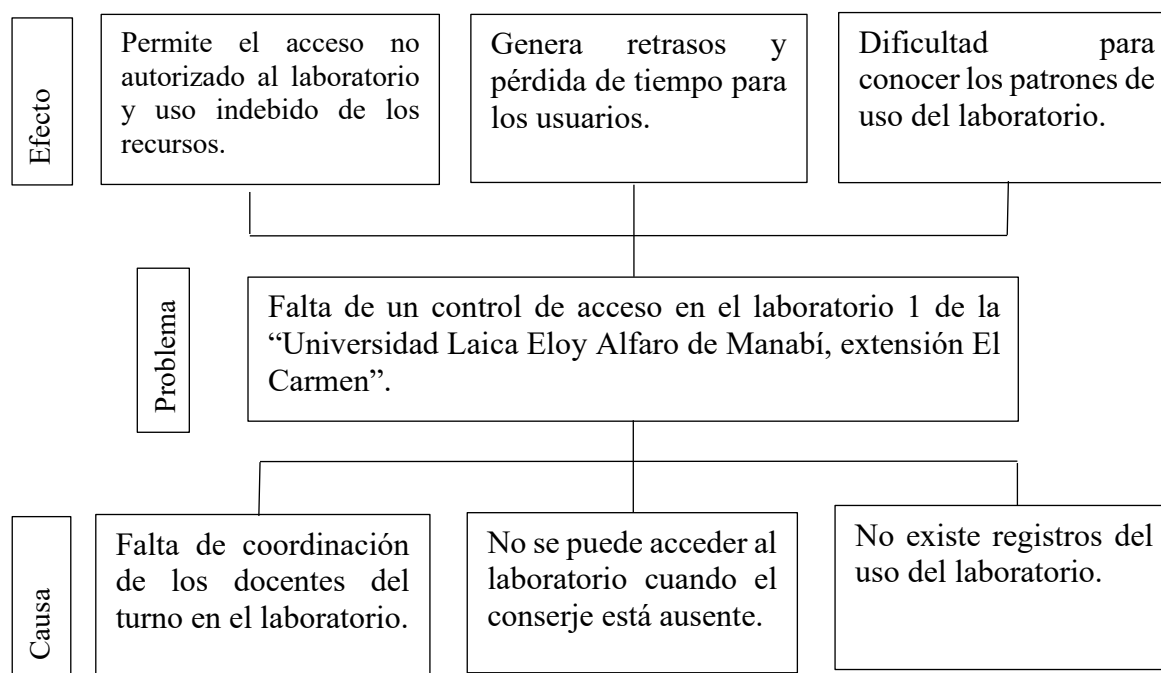
1.4.3 Estado actual del problema

La falta de un control adecuado facilita que personas no autorizadas ingresen al laboratorio, lo que puede resultar en el uso indebido de los recursos tecnológicos y académicos, comprometiendo la seguridad de los equipos y el entorno de trabajo.

La dependencia del conserje para acceder al laboratorio y la falta de un sistema automatizado de acceso provocan demoras significativas, lo que genera retrasos en el inicio de las clases y actividades, afectando el rendimiento académico y frustrando a los usuarios.

Ahora mismo no se sabe cómo se usa realmente el laboratorio porque no se lleva registros de quién entra ni cuándo, esto nos deja sin la información necesaria para tomar decisiones lo que hace que sea imposible planificar bien y asignar los recursos de manera eficiente, el espacio no se aprovecha al máximo y eso termina afectando negativamente a todos, tanto a los estudiantes como a los profesores en sus actividades diarias.

1.5 Diagrama causa – efecto del problema



1.6 Objetivos

1.6.1 Objetivo general

Implementar un sistema informático con redes neuronales para la seguridad física en el laboratorio de cómputo 1 de la ULEAM Extensión El Carmen.

1.6.2 Objetivos específicos

- Investigar los antecedentes y conceptos clave sobre sistemas de seguridad física y redes neuronales.
- Recolectar datos mediante encuestas aplicadas a docentes y entrevistas con los encargados del laboratorio para obtener información detallada sobre la gestión y las necesidades del laboratorio.
- Desarrollar un sistema informático para el control de acceso en el laboratorio utilizando la metodología Scrum, lo que permitirá una gestión continua de riesgos y adaptación a cambios durante el proceso de desarrollo.
- Realizar pruebas para validar la funcionalidad y efectividad del sistema.

1.7 Justificación

La seguridad en cualquier entorno académico es un aspecto fundamental para garantizar el uso adecuado de los recursos disponibles. En el caso del Laboratorio 1 de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, la falta de un control automatizado de acceso ha generado problemas como el uso no autorizado de los equipos y retrasos en las actividades. Este proyecto propone la implementación de un sistema informático con redes neuronales, diseñado específicamente para mejorar la seguridad física del laboratorio y gestionar el acceso de manera más eficiente.

Este proyecto parece bastante bueno incluso implementarlo daría un montón de beneficios, para empezar, más seguridad, ya que se acabarían las entradas de gente que no tiene permiso, también ayudaría a optimizar el tiempo, haciendo que no se pierdan minutos valiosos de clase en el laboratorio, y llevar un registro de quién entra y sale sería mucho más fácil, lo que bajaría el riesgo de que se pierdan o se dañen los equipos.

En resumen, este sistema podría cambiar por completo la forma en que se maneja el acceso a los espacios académicos de la universidad, mejorando la seguridad para todos y ayudando a gestionar mejor los recursos del laboratorio.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

La implementación de un sistema informático con redes neuronales para la seguridad física en el Laboratorio 1 mejorará significativamente la infraestructura tecnológica de la universidad. Permitirá la automatización del control de acceso, reduciendo la dependencia de métodos manuales, lo que incrementará la eficiencia y la precisión en la gestión de usuarios. Este avance tecnológico servirá de modelo para futuras aplicaciones en otros laboratorios y espacios académicos de la institución, fortaleciendo la innovación tecnológica en el entorno universitario.

1.8.2 Impacto social

A nivel social, este proyecto contribuirá a mejorar el bienestar de estudiantes y docentes al garantizar la seguridad de los recursos académicos y reducir los problemas asociados al acceso no autorizado. Los usuarios experimentarán un entorno más organizado, seguro y eficiente, lo que facilitará el desarrollo de las actividades académicas sin interrupciones ni

preocupaciones por el uso indebido de los equipos. Además, la mejora en la gestión del laboratorio impactará positivamente en la calidad de la enseñanza y aprendizaje.

1.8.3 Impacto ecológico

El impacto ecológico que conlleva la implantación de este proyecto primero es prevenir accidentes como incendios en los laboratorios, disminuir el número de daños en los dispositivos del laboratorio aumentando la vida útil de las computadoras y haciendo que se produzcan menos desechos electrónicos al año. Igualmente, al usar placas d bajo consumo para este sistema ayuda a disminuir la huella de carbono.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes históricos

2.1.1 Sistemas informáticos

La informática nació del ingenio humano para simplificar cálculos, evolucionando desde rudimentarios métodos de conteo hasta la visión de Babbage de una "máquina analítica" programable, precursora de las computadoras modernas. El siglo XX marcó hitos clave: las primeras calculadoras electrónicas acercaron la tecnología al público, y ARPANET sembró la semilla de internet, completando su revolución con el primer email y la web de Berners-Lee. Momentos icónicos como el surgimiento de Google demostraron el poder creciente de la tecnología, que hoy se encuentra presente en cada aspecto de nuestra vida a través de herramientas como Pandora FMS, culminando un viaje que transformó dispositivos mecánicos en extensiones digitales de la mente humana. (Santillán, 2016)

La historia de los sistemas informáticos surge desde las primeras herramientas que el ser humano ideó para simplificar el cálculo. Todo empezó con métodos simples, como contar con los dedos o usar piedritas para llevar la cuenta. Con el tiempo, la gente se puso más creativa y creó cosas como el ábaco, permitía hacer cálculos básicos. Pero el gran salto vino en el siglo XIX con el telar de Jacquard, una idea genial que usaba tarjetas perforadas para programar patrones. Y pensar que ese invento sería clave para las computadoras muchos años después. Pero fue Charles Babbage quien dio el salto conceptual más audaz con su máquina analítica, un diseño revolucionario que ya incluía componentes como memoria, unidad de procesamiento y almacenamiento, que el esqueleto de lo que hoy es considerado una computadora. Aunque limitaciones técnicas de la época impidieron su realización completa, estas innovaciones mecánicas de la época, junto con las calculadoras de Schickard, Pascal y Leibniz, tejieron los cimientos sobre los que se construiría la revolución digital del siglo XX. (Ramos, 2023)

2.1.2 Redes neuronales

Matich (2021) indica linealmente el desarrollo de las redes neuronales y la inteligencia artificial, la cual parte de su nacimiento teórico en papel entre los años (1936–1950s), hasta sus primeros pasos en desarrollo en 1956 con la formalización de la IA como disciplina y los primeros pasos en redes neuronales en 1957 y principios de los 1960s:

- Alan Turing (1936): vinculó el cerebro con modelos computacionales.
- McCulloch y Pitts (1943): propusieron redes neuronales con circuitos eléctricos.
- Donald Hebb (1949): estableció las bases del aprendizaje neuronal.
- Karl Lashley (1950): sugirió que la información cerebral está distribuida.
- El Congreso de Dartmouth (1956): formalizó la IA como disciplina.
- Frank Rosenblatt (1957): creó el perceptrón.
- Widrow y Hoff (1960): desarrollaron Adaline.

Por otro lado, Aranzana (2020) complementa la historia con el desarrollo de las redes neuronales a partir de 1969 con las crisis y críticas sobre perceptrón, además del nacimiento del hito más importante en las redes neuronales entre los años (1974–1986) que fue la retro programación y finalmente en los 1980s su aplicación a reconocimiento de patrones:

- Minsky y Papert (1969) expusieron limitaciones del perceptrón, frenando la investigación.
- Paul Werbos (1974) propuso el algoritmo de retropropagación.
- Rumelhart e Hinton (1986) lo optimizaron, permitiendo redes multicapa eficientes.
- Las redes neuronales se aplicaron en reconocimiento de patrones, optimización y *machine learning*.

2.1.3 Seguridad física

La seguridad ha cambiado mucho, inicialmente se caracterizaba por medidas tradicionales, como el uso de personal de vigilancia, puertas y rejas, enfocándose exclusivamente en la protección física, entonces la gente solo reaccionaba cuando ya había pasado algo malo, si había un delito, entonces actuaban. Después, las cosas mejoraron y se volvieron más preventivas; los expertos empezaron a analizar los riesgos y a poner medidas para que no pasaran los problemas, con la inteligencia artificial, se puede ayudar frente a amenazas. (Fennelly, 2016)

2.2 Antecedentes de investigaciones relacionadas al tema presentado

Este estudio de un sistema de reconocimiento facial para el control de accesos con inteligencia artificial dio en el clavo. Donde se utilizó Python junto a librerías como opencv, para entrenar el modelo, fue entrenado con un montón de fotos aproximadamente 450 por persona, logrando un impresionante nivel de precisión. Este trabajo dejó claro que las redes neuronales convolucionales son una herramienta poderosa para identificar personas, mostrando que funcionan de maravilla para controlar quién entra y quién no del laboratorio. Con este proyecto se puede ver que apostar por estas redes es una jugada inteligente y efectiva para crear

sistemas de control de acceso basados en reconocimiento facial. (Campos, Rodríguez, Luján, & Santos, 2023)

Se realizó una investigación titulada "Sistema de reconocimiento facial para el control de ingreso de personas a la UNJBG", en la Universidad Nacional Jorge Basadre Grohmann (UNJBG). El objetivo primordial fue desarrollar y evaluar un sistema de reconocimiento facial con el propósito de mejorar la seguridad de personas y bienes, así como optimizar el control de acceso a la universidad. La investigación utilizó una muestra de veinte estudiantes de 2018 y empleó el método de observación pasiva para recopilar datos, sin omitir los registros generados por el sistema ni las hojas de campo. El trabajo contribuyó a mejorar el control de accesos, destacando la relevancia de los sistemas de reconocimiento facial en el ámbito universitario. (Cruz & Gunar , 2022)

Esta investigación titulada "Aplicación de reconocimiento facial para el control de asistencia de estudiantes mediante modelos de visión artificial", en la Universidad Técnica de Machala (UTMACH), Ecuador. El propósito fue desarrollar una aplicación web para registrar la asistencia de estudiantes utilizando modelos de reconocimiento facial, el proyecto implementó la metodología CRISP-DM para entrenar un modelo de IA con un dataset de imágenes, y utilizó la metodología XP para el desarrollo de la aplicación web, el modelo Face-Api.js fue seleccionado por su precisión en condiciones variables de luz, posición y resolución de las imágenes, el sistema logró identificar a los estudiantes con alta precisión, evaluado bajo la norma de calidad ISO 9126 en términos de funcionabilidad, usabilidad y eficiencia. (Campoverde & Mendieta , 2023)

2.3 Definiciones conceptuales

2.3.1 Sistema Informático

Un sistema informático es un conjunto de componentes físicos y lógicos, diseñados para procesar, almacenar y gestionar datos, permitiendo la interacción con agentes externos, incluidos los humanos, estos sistemas pueden operar localmente, conectados físicamente o de forma remota utilizando varios métodos de comunicación, su objetivo principal es apoyar el procesamiento y la gestión eficaz de la información en función de las necesidades específicas del entorno de uso de la información, además, el sistema informático incluye recursos humanos para el funcionamiento del sistema y documentación que describe los procedimientos necesarios para su correcto funcionamiento. (Pérez, 2012)

La importancia la define Almache, Remache, Pijal, & Benavides (2023) quienes lo interpreta de la siguiente manera: Los sistemas informáticos con los años se han convertido en un pilar esencial para las empresas, ya que optimizan operaciones como ventas, compras y gestión de proveedores, reduciendo significativamente el tiempo requerido en comparación con los procesos manuales, los cuales demandan mayor esfuerzo y coordinación. Además, estos sistemas permiten presentar información de forma clara, así como generar reportes automatizados, facilitando así la toma de decisiones. Por esta razón, la mayoría de las organizaciones dependen de estas herramientas para agilizar y gestionar eficientemente sus actividades diarias.

Según Ramos (2023), los sistemas informáticos consisten en un conjunto de elementos esenciales diseñados para procesar y gestionar información, estos sistemas son fundamentales en diversos ámbitos gracias a su capacidad para facilitar la resolución de problemas y la automatización de tareas complejas, estos son:

- **Hardware:** Es la parte física del sistema está constituida por todos sus componentes como son: procesadores, memorias, discos duros, circuitos electrónicos.
- **Software:** Es la parte lógica del sistema como lo son: los sistemas operativos, las aplicaciones y los datos.
- **Componente humano:** Es fundamental, ya que los sistemas informáticos no funcionan de nada sin personas que las configuren, mantengan y utilice. Estas pueden ser profesionales como técnicos, programadores y administradores de sistemas.

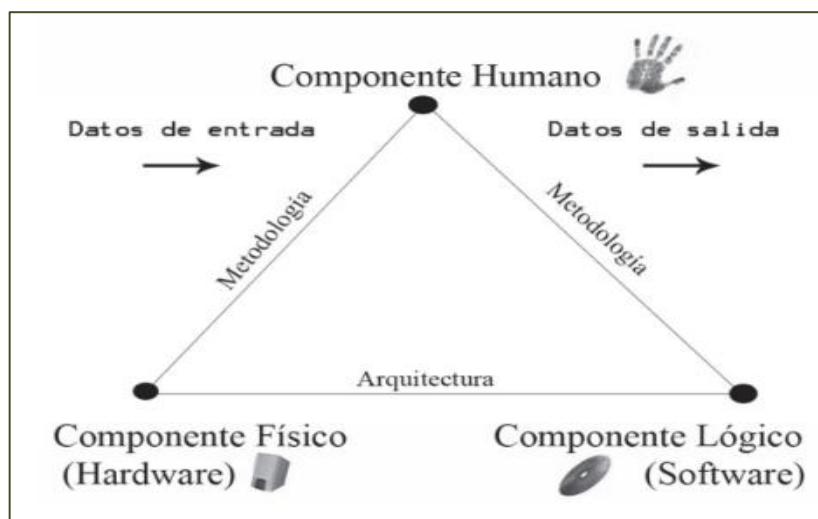


Ilustración 1: Estructura de un sistema informático.

Extraído de (Cabrera, 2011)

Un sistema informático se divide en dos componentes principales, el primero es el "sistema central," encargado de procesar la información a través de dispositivos periféricos que cumplen funciones de entrada y salida de datos, permitiendo la interacción con el entorno físico, el segundo componente es el "sistema informático" o software, que actúa como intermediario entre el sistema central y el usuario, su principal objetivo es procesar los datos de entrada para generar resultados de salida comprensibles y útiles, ambos componentes trabajan de manera conjunta para garantizar el correcto funcionamiento y la efectividad de un sistema informático. (Marcatoma, 2022)

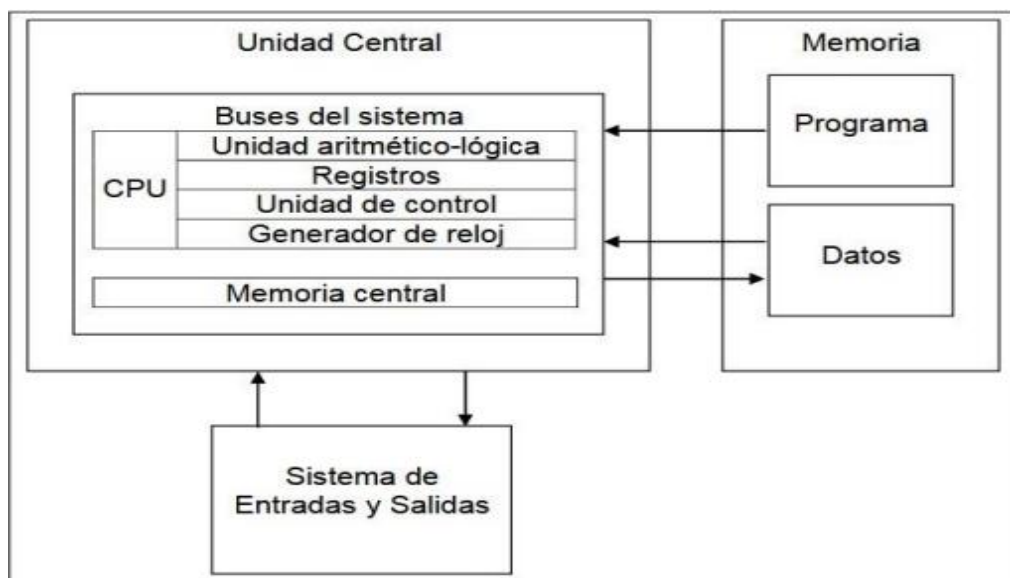


Ilustración 2 Componentes Principales de un Sistema Informático. (Marcatoma, 2022)

El hardware incluye componentes físicos como la CPU, la memoria RAM y los dispositivos de almacenamiento, que permiten procesar y guardar datos, también los periféricos y las tarjetas de interfaz permiten la interacción con el sistema y la conexión con otros dispositivos, el software es fundamental para coordinar el funcionamiento del hardware, siendo el sistema operativo el encargado de gestionar los recursos y la comunicación entre aplicaciones y dispositivos, las aplicaciones de software realizan tareas específicas, mientras que los controladores permiten que el sistema operativo interactúe con el hardware, también, las bibliotecas de software y los entornos de desarrollo integrados facilitan la creación de programas. (Floyd, 2006)

2.3.1.1 Estructura Física

Este apartado de la temática aborda los elementos cruciales de la estructura física de una computadora; de acuerdo con Querol, Monge, & Monge (2023), por un lado, la unidad

central de procesamiento es la imagen principal de procesamiento de una computadora y se conoce como el “cerebro” de máquina porque coordina y les da uso a todas las responsabilidades críticas de ejecución del sistema.

En cuanto a la memoria interna, esta resulta crucial para el funcionamiento de los sistemas informáticos, ya que almacena temporalmente los datos e instrucciones necesarias para la ejecución de los procesos, la memoria interna está organizada jerárquicamente para maximizar la velocidad de acceso y el rendimiento del sistema, en la capa más rápida y pequeña, se encontraron los registros, que están integrados en la CPU y almacenan de manera temporal los datos necesarios para el procesamiento. (Schmidt, 2020)

Por otro lado, el almacenamiento externo juega un papel clave al permitir la conservación de grandes volúmenes de datos, especialmente porque ofrece una capacidad mucho mayor que la memoria interna, con el creciente acceso a la información desde diversos dispositivos y ubicaciones, el almacenamiento externo se ha vuelto cada vez más relevante, y el uso de soluciones en la nube ha incrementado debido a su capacidad para permitir el acceso remoto a la información. (Cardoso, Cardoso, & Morales, 2024)

2.3.1.2 Tipos

2.3.1.2.1 Sistemas de Información Gerencial

Los Sistemas de Información Gerencial (SIG) son herramientas esenciales que permiten a los estudiantes comprender cómo las organizaciones utilizan tecnologías y sistemas de información para alcanzar sus objetivos, esta asignatura teórico-práctica, diseñada para modalidad a distancia, busca fomentar un aprendizaje autónomo y significativo, sus contenidos abarcan aspectos clave como la administración en las organizaciones, nuevas tendencias tecnológicas, y aplicaciones de sistemas en la era digital, promoviendo el análisis, la investigación, y la planificación estratégica para resolver tareas académicas y profesionales. (Rojas, 2017)

Un Sistema de Información Gerencial es un conjunto de sistemas y procesos que recopilan, organizan y presentan datos de diversas fuentes en una base de datos computarizada, esta información se presenta de forma accesible para que los gerentes puedan tomar decisiones informadas, desde las operativas diarias hasta las estrategias a largo plazo, considerado una herramienta estratégica empresarial, facilita la coherencia y consistencia de los datos, mejorando el rendimiento organizacional, también asegura que los procesos clave sean

identificados y comprendidos desde el principio para evitar problemas futuros, y operan mediante tres actividades: la recopilación de datos, su procesamiento para hacerlos comprensibles y la entrega de información útil a las personas adecuadas. (Melara, 2022)

2.3.1.2.2 Sistema Transaccional

Un sistema transaccional es un tipo de sistema de información diseñado para recopilar, almacenar, modificar y recuperar la información generada a partir de transacciones en una organización, las transacciones se refieren a eventos o procesos que crean o alteran datos, los cuales son almacenados para su posterior consulta o procesamiento. Entre sus principales características destacan aspectos como la seguridad, la integridad de los datos y la capacidad de procesar múltiples operaciones de manera eficiente. (Dranca, 2020)

Además, un sistema transaccional para ser considerado como tal, debe cumplir con el test ACID: Atomicidad, que asegura que una transacción se ejecuta completamente o no se ejecuta en absoluto; Consistencia, que garantiza que los datos siempre se mantengan en un estado válido; Aislamiento, que permite la ejecución concurrente de transacciones sin interferencias entre ellas; y Durabilidad, que asegura que los cambios de una transacción son permanentes, incluso en caso de fallos del sistema. Estos sistemas también deben ser rápidos, fiables, escalables y contar con mecanismos de auditoría para registrar transacciones y modificaciones, lo que permite generar informes para análisis y toma de decisiones. (Alegsa, 2023)

2.3.1.2.3 Sistema de Apoyo a la Toma de Decisiones

Linares, Sevillano, & Viejó (2023) define en su artículo a un sistema de apoyo a la toma de decisiones como un sistema informático que, a través de modelos matemáticos, facilita a los usuarios la toma de decisiones en diversas situaciones, estos sistemas recopilan información de diferentes entornos, como bases de datos y experiencias previas, identificando problemas, desafíos o patrones de comportamiento, y proporcionando recomendaciones para la toma de decisiones

Mientras que Villalba, Palacios, Romero, & Patarón (2019) complementa su definición diciendo que los sistemas de apoyo a la decisión son herramientas que a ser clave en la toma de decisiones, permiten visualizar datos y descubrir tendencias en tiempo real, lo que ayuda a mejorar la eficiencia y detectar áreas de crecimiento, entre sus ventajas están el acceso a información histórica para análisis de tendencias, la accesibilidad para todos los usuarios de la

organización, el análisis multidimensional, y la automatización de procesos, también algunos sistemas integran inteligencia artificial para procesar grandes volúmenes de información y ofrecer soluciones basadas en datos, aunque la decisión final sigue siendo humana.

2.3.1.2.4 Sistemas Estratégicos

Los sistemas estratégicos están diseñados para integrarse con paquetes preexistentes en el mercado y adaptarse a las necesidades específicas de una organización, su principal función es optimizar procesos y añadir funcionalidades que potencien el desarrollo empresarial. La integración de sistemas es el proceso de conectar diferentes sistemas de TI, aplicaciones de software y fuentes de datos dentro de una organización para que funcionen como una unidad cohesiva. Permite el intercambio de datos y la interoperabilidad sin interrupciones, lo que facilita el acceso a los datos en tiempo real y mejora la precisión y la confiabilidad de la información en toda la organización. (Merchant, 2024)

2.3.1.3 Redes neuronales artificiales

Una red neuronal es un modelo computacional inspirado en el cerebro humano, utilizado en inteligencia artificial y aprendizaje automático, están formadas por neuronas artificiales o nodos, organizadas en capas:

- Capa de entrada: En esta capa son recibidos los datos iniciales.
- Capas ocultas: En esta capa se procesa toda la información que ingresa mediante cálculos.
- Capa de salida: Esta capa entrega el resultado de los datos ya procesados.

Cada enlace entre las neuronas lleva un peso que se va ajustando mientras la red aprende, afinándose para cometer menos errores con la ayuda de funciones de pérdida y optimizadores. Además, usa funciones de activación como sigmoide para captar relaciones no lineales. Estas redes neuronales son eficientes, sobresalen en cosas como reconocer voces, identificar imágenes o incluso predecir tendencias financieras, resolviendo hasta los problemas más locos. (Rebolledo, 2024)

2.3.1.3.1 Neuronas Artificiales

Las neuronas artificiales, o nodos, son la base de las redes neuronales, inspiradas en las neuronas biológicas del cerebro humano, estas procesan información mediante entradas numéricas, que representan datos como píxeles o texto, y las ponderan con pesos para determinar su relevancia, también suman estas entradas ponderadas, añaden un sesgo para

ajustar el resultado y aplican una función de activación, que les permite manejar relaciones no lineales y decidir si deben activarse o no, este proceso les otorga flexibilidad y capacidad para aprender patrones complejos, las neuronas trabajan en conjunto dentro de redes más grandes, lo que permite abordar tareas como la clasificación de imágenes, la predicción de tendencias o el reconocimiento de patrones en datos diversos. (Rouse, 2024)

2.3.1.3.2 Componentes de una neurona artificial

Las redes neuronales artificiales se clasifican según su arquitectura y función, destacando tres componentes esenciales: las neuronas de entrada, que reciben los datos iniciales del entorno; las neuronas ocultas, que procesan la información internamente sin interactuar directamente con el exterior; y las neuronas de salida, que generan los resultados finales. El aprendizaje profundo o Deep Learning lleva este concepto más allá, utilizando redes neuronales con múltiples capas ocultas que permiten el reconocimiento automático de patrones complejos. Estas arquitecturas profundas son capaces de identificar características relevantes en los datos mientras filtran información irrelevante, lo que mejora significativamente su capacidad de clasificación. (Rebolledo, 2024)

Gracias a estos avances, el aprendizaje profundo ha logrado resolver problemas que antes eran inalcanzables para la inteligencia artificial tradicional, encontrando aplicaciones en numerosos campos del conocimiento. La diferencia que existe entre el aprendizaje superficial y el profundo es que en el primero solo reproduce la información es básicamente una duplicación de una información, a diferencia del profundo que trata de comprender la información dada y dar información más precisa. Por ello las redes neuronales profundas usan múltiples capas y técnicas como la regularización para procesar la información, ajustando sus parámetros para un buen rendimiento. (Sánchez, Escobar, & Huincho, 2024)

2.3.1.3.3 Aplicaciones de las redes neuronales

Las redes neuronales son altamente efectivas para reconocer patrones en grandes volúmenes de datos, en el reconocimiento de voz, pueden convertir ondas sonoras en texto al identificar patrones en el sonido, en la clasificación de imágenes, son capaces de reconocer características como forma y color para agrupar imágenes en categorías, también destacan en el procesamiento de lenguaje natural, permitiendo traducción automática y generación de texto coherente, como en los traductores y asistentes virtuales, también en visión por computadora, pueden identificar objetos en imágenes y videos, útiles en seguridad y clasificación, gracias a su capacidad de reconocimiento de patrones, las redes neuronales también se aplican en la

predicción y toma de decisiones, como predecir preferencias de compra, analizar riesgos o evaluar el riesgo de enfermedades en pacientes. (Huet, 2023)

2.3.1.4 Aplicaciones de redes neuronales en sistemas informáticos

Ramirez & Knigh (2020), presentaron el ejemplo de FaceID, introducido por Apple con el iPhone X, como una tecnología innovadora que marcó un avance significativo en hardware al ofrecer una nueva forma de proteger dispositivos, este sistema, basado en reconocimiento facial, destaca por utilizar tecnología 3D y sensores infrarrojos, lo que minimiza el margen de error y aumenta la precisión del reconocimiento, este ejemplo evidencia cómo el desarrollo de hardware especializado potencia las capacidades de sistemas basados en redes neuronales, haciéndolos más seguros y eficaces.

Un sistema informático permite que la parte visual que ve el usuario final interactúe de manera fluida con otros componentes lógicos como base de datos y lenguaje de programación, los cuales funcionan con secuencias de instrucciones siendo fundamentales en dar vida al sistema y garantizar el funcionamiento. Carrasco (2019)

Según García (2022), los algoritmos de aprendizaje automático son la base del aprendizaje profundo y emulan un cerebro humano, permitiendo a estos sistemas aprender de los datos proporcionados y mejorar su desempeño basado en experiencia. El aprendizaje automático combina materias como: estadística, matemáticas y computación, que son elementos clave para procesar grandes cantidades de datos y realizar predicciones eficaces.

2.3.2 Seguridad física

Según Reina (2014), la seguridad se define como el bienestar que percibe y disfruta una persona en cualquier escenario, para que este concepto sea efectivo en la práctica, es esencial aplicar los pilares de la seguridad, que incluyen vigilar, proteger, disuadir y prevenir, considerando qué, quién y cómo se protegerá, el término "seguridad disuasiva" se refiere a la capacidad de desviar la intención del delincuente o hacer que se intimide ante los métodos de protección, sin recurrir a medidas que desgasten la gestión del grupo de seguridad, esto se aplica en entornos como supermercados o grandes superficies, donde se utilizan métodos disuasivos como detectores de códigos de barras, arcos de detección, sellos plásticos y CCTV, con el fin de minimizar la intención delictiva.

La seguridad física ha evolucionado más allá de cerraduras y candados, actualmente existen sistemas para reconocimiento facial, para detectar huellas, retina y ni hablar de los altos sistemas de vigilancia con cámaras inteligentes. Estas nuevas tecnologías están protegiendo y dando mejor gestión en nichos de seguridad a lo que era antes. La llegada de la tecnología y sus dispositivos IoT y sistemas en la nube facilita aún más la gestión y monitoreo remoto, permitiendo respuestas rápidas y eficientes ante riesgos. (Madeo, 2024)

2.3.2.1 Control de acceso

Para optimizar la seguridad física, es esencial restringir y controlar quién tiene acceso a las instalaciones mediante sistemas de control de acceso, este enfoque se centra en limitar el acceso a activos y áreas específicas solo al personal autorizado, utilizando herramientas como teclados, tarjetas de identificación, sistemas biométricos y la presencia de guardias de seguridad, la arquitectura del edificio, que incluye muros, rejas y puertas estratégicamente ubicadas, actúa como una primera línea de defensa contra posibles intrusos, también medidas complementarias como alambres de espino y cerraduras adicionales pueden disuadir intentos de entrada no autorizada. (Perry, 2017)

Los sistemas de control de acceso también han evolucionado hacia soluciones más tecnológicas, como el uso de tarjetas de identificación que emplean tecnología comunicación de campo cercano o identificación por radiofrecuencia para autenticar la identidad de los empleados al ingresar a diferentes áreas del edificio, las empresas pueden proporcionar tarjetas especiales a los visitantes para gestionar su acceso a zonas determinadas, la implementación de autenticadores móviles y la autenticación multifactorial añaden capas adicionales de seguridad al requerir múltiples formas de verificación antes de permitir el ingreso, también estas medidas no solo ayudan a prevenir el acceso no autorizado, sino que también pueden proteger las instalaciones contra desastres naturales mediante barreras físicas adecuadas, lo que es crucial para mitigar riesgos según la ubicación geográfica de la empresa. (Bourgeat, 2024)

2.3.2.2 Mejora de la seguridad con IA y Sistemas Integrados

La integración de sistemas de seguridad física con tecnologías de la información crea entornos más seguros y eficientes, esta convergencia permite una gestión centralizada de los recursos de seguridad, facilitando la coordinación y respuesta ante incidentes, al combinar capacidades analíticas avanzadas con controles físicos tradicionales, las organizaciones pueden

mejorar significativamente su capacidad para gestionar riesgos y proteger sus activos. (De Buen, 2024)

La implementación de tecnologías de inteligencia artificial y análisis predictivo en la seguridad física permite anticipar y prevenir incidentes, mejorando la eficacia de los sistemas de protección, estas herramientas analizan grandes volúmenes de datos para identificar patrones y comportamientos inusuales, facilitando la detección temprana de amenazas y la respuesta rápida ante situaciones de riesgo, esto no solo optimiza la seguridad, sino que también reduce el tiempo de reacción ante incidentes, minimizando así posibles daños. (Ramanpreet, Dusan, & Klobucar, 2023)

2.3.2.3 Ventajas de la Integración de Sistemas de Seguridad Física y Tecnologías de la Información

La integración de sistemas de seguridad física con tecnologías de la información ofrece múltiples ventajas que mejoran la protección y la eficiencia operativa en las organizaciones, en primer lugar, permite un control centralizado, lo que facilita la gestión de todos los dispositivos de seguridad desde una única plataforma, optimizando la supervisión y la respuesta ante incidentes, también esta convergencia mejora la visibilidad y detección de amenazas, ya que combina datos visuales y analíticos para identificar patrones y comportamientos inusuales. (Stockholm, 2023)

También reduce errores humanos a través de la automatización de procesos, lo que incrementa la confiabilidad de las operaciones de seguridad, la integración ayuda a cumplir con normativas y estándares de seguridad, al proporcionar un marco unificado para gestionar riesgos, asimismo, en caso de un incidente, permite una respuesta rápida y coordinada, lo que puede ser crucial para mitigar daños, también al optimizar recursos y mejorar la asignación del personal, las organizaciones pueden operar de manera más eficiente mientras protegen sus activos e información confidencial. (Templo de Kendall, 2024)

2.3.2.4 Metodología ágil SCRUM

Scrum es un marco de trabajo ágil diseñado para reducir la complejidad en el desarrollo de productos, promoviendo la colaboración entre equipos y la gerencia para satisfacer las necesidades del cliente, basado en un modelo empírico, Scrum fomenta la autoorganización de los equipos, quienes trabajan de manera incremental, inspeccionando y adaptándose

continuamente para resolver problemas complejos, creado por Ken Schwaber y Jeff Sutherland, es una herramienta sencilla y no prescriptiva, explicada en la Guía Scrum, que se centra en el respeto por las personas y la entrega constante de valor. (Sutherland, 2016)

2.3.2.4.1 Los Roles Fundamentales en SCRUM

La clave de Scrum está en los roles los cuales colaboran como iguales, sin jerarquías, enfocados en entregar valor de forma iterativa e incremental. Según SCRUMstudy (2017), en Scrum existen tres roles principales y 2 secundarios que trabajan en igualdad de condiciones para alcanzar los objetivos del proyecto:

- **El Product Owner:** actúa como enlace entre el negocio y el equipo. Su misión es maximizar el valor del producto priorizando requerimientos y tomando decisiones clave, siempre representando las necesidades del cliente.
- **El Scrum Máster:** es la persona que hace de facilitador, se asegura de que el grupo siga scrum al pie de la letra. No dirige como un jefe, sino que guía y enseña.
- **El Equipo Scrum:** son el equipo de desarrolladores, quienes tienen la función de transformar los requerimientos en acciones funcionales del sistema para cada iteración.
- También, hay roles secundarios como los stakeholders que son el usuario final o clientes que aportan perspectivas valiosas.

2.3.2.4.2 Eventos y artefactos SCRUM

Zalimben (2022) muestra como Scrum organiza el trabajo en 3 artefactos que guían el trabajo y en cuatro eventos estructurados que mantienen el ritmo y la mejora continua. Estos elementos trabajan juntos para asegurar transparencia, adaptabilidad y entrega constante de valor, principios centrales de Scrum:

Artefactos:	Eventos:
Product Backlog: La lista dinámica de funcionalidades priorizadas, siempre actualizada por el Product Owner.	Sprint Planning: Aquí el equipo define qué trabajará, por qué y cómo lo hará.
Sprint Backlog: Las tareas seleccionadas para el Sprint actual, con un objetivo claro.	Daily Scrum: Una sincronización rápida donde cada miembro comparte: qué hizo ayer, qué hará hoy y qué obstáculos enfrenta. Esto evita reuniones innecesarias y mantiene el foco.
Incremento: El resultado tangible del Sprint, que debe cumplir con los criterios de calidad acordados.	Sprint Review: Al final del Sprint, el equipo muestra el incremento terminado a los stakeholders. Se discute el progreso, se recibe feedback y se ajusta el Product Backlog para el próximo ciclo.
	Sprint Retrospective: El equipo reflexiona sobre qué funcionó, qué no y cómo mejorar procesos, herramientas o colaboración para el siguiente Sprint.

Tabla 1: Eventos y artefactos SCRUM. (Zalimben, 2022)

2.3.2.4.3 Beneficios de SCRUM

La implementación de Scrum ofrece múltiples beneficios que transforman la forma de trabajar de los equipos. Scrum ayuda al equipo a enfocarse en tareas pequeñas y manejables, permite que se avance de manera más fluida en un proyecto por el hecho de disminuir la documentación. Además, lleva a que el equipo sea más colaborativo y enfocado a objetivos. Es ideal para proyectos de un tiempo de desarrollo mediano o corto. (Cabrera, y otros, 2025)

2.4 Conclusiones del marco teórico

Los sistemas informáticos que utilizan redes neuronales representan una evolución significativa en el procesamiento de datos, permitiendo la automatización y mejora en tareas complejas como el reconocimiento de patrones y la predicción, estas redes, inspiradas en el funcionamiento del cerebro humano, son capaces de aprender y adaptarse a nuevas informaciones, lo que las hace especialmente útiles en aplicaciones como la visión por computadora y el procesamiento de lenguaje natural, su integración en sistemas informáticos no solo optimiza la gestión de datos, sino que también potencia la toma de decisiones informadas al ofrecer análisis precisos y eficientes.

La metodología Scrum encaja como anillo al dedo cuando se trata de desarrollar sistemas informáticos en tiempos cortos con resultados excelentes. Su enfoque ágil hace que los equipos puedan trabajar a su ritmo y fomentado la colaboración por las reuniones que se hacen diarias. En trabajos como este de redes neuronales la flexibilidad de scrum le permite adaptarse a cambios en lo que el proyecto necesita, asegurando que el sistema final rentable y realmente y cumpla su función.

Por otro lado, la seguridad física es algo básico pero fundamental para cuidar los recursos de cualquier entidad. Se habla de medidas como el manejo del control de acceso o cámaras de vigilancia que funcionan muy bien frente a amenazas, ya sea que estas vengan de fuera o de dentro. Poner en marcha buenos hábitos y herramientas de seguridad física no solo protege el hardware, sino que también garantiza que la información que manejan esos sistemas esté segura y disponible cuando se la necesita.

Las redes neuronales son fundamentales al momento de analizar datos o en el caso de la detección facial es imprescindible para identificar a la persona autorizada. Todo esto en conjunto a herramientas y dispositivos físicos como IoT y un sistema informático complementan un tridente de seguridad eficiente.

CAPÍTULO III

3. MARCO INVESTIGATIVO

3.1 Introducción

El acceso no restringido a los recursos compartidos puede causar ineficiencias, problemas de seguridad y daños en los equipos, este estudio se centró en abordar estas dificultades en el laboratorio de computación de la extensión El Carmen de la ULEAM, donde se identificaron fallas en los sistemas actuales de control de acceso, a través de encuestas y entrevistas con el profesorado y el responsable del laboratorio, se buscó entender los factores detrás de estos problemas y las necesidades específicas de los usuarios.

Se hizo uso de una mezcla entre el método cuantitativo y cualitativo, que dieron como resultado la necesidad urgente de un sistema físico automático que garantice un control de acceso seguro sin demoras, con esto se busca mejorar la gestión de ingreso e incentivar a el uso adecuado del recuerdo en el laboratorio y evitar actos vandálicos.

3.2 Tipos de investigación

3.2.1 Investigación Bibliográfica

El método de investigación documental se emplea principalmente en estudios cualitativos y se basa en el análisis de fuentes secundarias escritas o visuales generadas por personas o instituciones, este enfoque permite acceder a datos, experiencias, actividades y conocimientos sin modificar el contenido original de los documentos, es un método útil para analizar discursos y textos en su contexto social, abarcando documentos oficiales, gubernamentales, políticos, institucionales y otros materiales que aportan información o testimonios sobre una realidad específica (Revilla , Degola, Poma, Trelles , & Tafur , 2020).

La investigación documental fue fundamental para la recolección de datos de fuentes teóricas de confianza como estudios científicos como artículos de investigación y libros relacionados a los temas planteados. Con este método se dota de información valiosa y se forma un marco teórico sólido.

3.2.2 Investigación Aplicada

La investigación aplicada se enfoca en resolver problemas prácticos y encontrar soluciones concretas para situaciones del día a día. Lo que se busca con esto es crear

conocimiento que sirva para solucionar problemas de la vida real, como inventar cosas nuevas, mejorar cómo se producen las cosas o encontrar la cura para enfermedades. Para lograrlo, se tomó ideas y métodos que ya existen y se ajustó a lo requerido. Aunque los pasos a seguir no son tan estrictos como en otros estudios, la idea es que los resultados se usen directamente para mejorar situaciones concretas, como la agricultura o cómo se usa la energía (Rodríguez, 2020).

Esta investigación es totalmente práctica, porque se está usando para solucionar problemas reales del laboratorio de la ULEAM, como el acceso no autorizado y el uso inapropiado de los recursos. La idea es analizar lo que pasa ahí para poder desarrollar soluciones que sean efectivas justo en ese contexto y de esta manera, se aplican los conocimientos y métodos actuales para optimizar los procesos y lograr resultados que beneficien directamente a la universidad.

3.2.3 Investigación de campo

La investigación de campo es un método que consiste en recopilar información directamente en ambientes reales y no controlados, fuera de un laboratorio o entorno artificial. Este enfoque permite obtener datos precisos y específicos al observar o interactuar con fenómenos en su contexto natural. Es común en disciplinas como biología, sociología y meteorología, donde se requiere estudiar el comportamiento de organismos, las interacciones sociales o las condiciones climáticas en escenarios reales (Pereyra, 2020).

La investigación de campo es la que permite ir al lugar exacto de la investigación que en este caso fue el laboratorio 1, donde se fue a detectar posibles fallos o debilidades en seguridad que no hayan sido detectadas para más adelante poder ser de ayuda con la implementación de este proyecto. Con los datos obtenidos se cayó en cuenta de que el acceso al laboratorio lo tiene cualquiera y que no existe seguridad para los recursos del laboratorio.

3.3 Métodos de investigación

3.3.1 Estudio de caso

El estudio de caso es una estrategia metodológica valiosa en la investigación, que permite analizar en profundidad fenómenos o situaciones específicas mediante el registro y la observación detallada de la conducta de los individuos involucrados, esta metodología ha sido ampliamente aplicada en diversas disciplinas, especialmente en las ciencias sociales, la

educación, y la gerencia, y se emplea no solo para investigaciones exploratorias, sino también descriptivas, explicativas y para la generación de teorías (Ramírez , Rivas , & Cardona , 2019).

Los estudios de caso con relación a este proyecto permitieron analizar el comportamiento de los docentes que son las personas que tendrán relación directa con el sistema, donde se notan los problemas que existen cuando van a ingresar al laboratorio a dar clases y al salir la manera que se cierra el laboratorio o como se hace con las personas que aun necesitan hacer uso de este.

3.3.2 Método cualitativo

La investigación cualitativa se centra en comprender fenómenos desde la perspectiva de los participantes, explorándolos en su ambiente natural y en relación con el contexto, este enfoque dinámico permite identificar conceptos centrales, revisarlos y adaptarlos conforme se evalúan los datos recolectados, utiliza muestras no probabilísticas, sino propositivas, y se apoya en métodos como entrevistas, el proceso incluye la recolección, organización, codificación y descripción de datos, generando conceptos, hipótesis y teorías basadas en los mismos (Hernández & Mendoza, 2018).

Con respecto a la investigación cualitativa se trató de comprender el comportamiento y las experiencias que han tenido tanto docentes como estudiantes en cuanto a problemas de acceso o con algún tipo de vandalismo que les haya ocurrido en el laboratorio, si fue dentro o fuera del horario de clases.

3.3.3 Método cuantitativo

El enfoque cuantitativo se caracteriza por el uso de métodos y técnicas que permiten medir variables y analizar datos mediante procedimientos estadísticos, con el objetivo de probar hipótesis y responder preguntas de investigación, también está influenciado por el positivismo y el neopositivismo, y se basa en la observación, medición, muestreo y análisis riguroso, aplicando el método científico para descubrir nuevos conocimientos, utiliza herramientas como la estadística descriptiva e inferencial, el diseño formalizado de investigación y la formulación de hipótesis, tomado principalmente de las ciencias naturales y formales (Ñaupas, Valdivia, Palacios, & Romero, 2013).

El enfoque cuantitativo fue más medido a través de las herramientas de recolección de datos donde dejó en evidencia la necesidad de un sistema que controle el acceso. Estos datos

obtenidos son medibles y fue lo que permitió deducir que nuestra problemática era real y era más necesaria de lo que se pensaba.

3.4 Fuentes de información de datos

3.4.1 Fuente primaria

La encuesta es una herramienta utilizada para recolectar información sobre opiniones, comportamientos o percepciones a través de cuestionarios dirigidos, puede generar datos tanto cuantitativos como cualitativos, dependiendo de su diseño y enfoque, su versatilidad permite emplearla como técnica para recopilar información específica o como método dentro de un proceso más amplio de investigación, aunque es ampliamente utilizada en diferentes áreas, su aplicación requiere cuidado para asegurar que los resultados son útiles y alineados con los objetivos del estudio (Arias, 2021).

Como fuente primaria se aplicó la técnica recolección de encuestas a los docentes que imparten clases en el laboratorio 1. Esta encuesta estuvo centrada en preguntas cerradas, lo que permite obtener resultados cuantitativos, se realizó de manera digital mediante la plataforma Google Forms, esta información es clave para mejorar la propuesta del proyecto.

3.4.2 Fuente secundaria

La entrevista estructurada consiste en preguntas cerradas que buscan respuestas precisas y cuantificables, codificadas mediante valores numéricos para facilitar su análisis, se elabora previamente con preguntas fijas y ordenadas, garantizando criterios unificados, esta técnica es mecánica y auto administrada, permitiendo que el entrevistado responda sin ayuda adicional, es útil para evaluar comportamientos, experiencias y opiniones, especialmente en el análisis de funciones dentro de una organización (Díaz, Torruco, Martínez, & Varela, 2013).

Como fuente secundaria, se aplica la técnica de la entrevista al encargado de los laboratorios de Tecnologías de la Información de la ULEAM Extensión El Carmen, cuyo propósito es conocer su punto de vista más amplio, ya que está compuesta por preguntas abiertas y semiestructuradas, realizadas de manera presencial, la entrevista permite explorar los problemas asociados al acceso y seguridad en el laboratorio, identificando las dificultades de los métodos tradicionales y evaluando la viabilidad de implementar un sistema automatizado basado en reconocimiento facial.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población

La población de esta investigación estuvo conformada por los 9 profesores y la persona encargada del Laboratorio de Cómputo 1 en la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, este laboratorio es utilizado principalmente para actividades prácticas relacionadas con las carreras de Tecnologías de la Información y Software, los profesores seleccionados son responsables de coordinar y supervisar estas actividades, por lo que su participación fue clave para comprender el acceso y uso de los recursos en el laboratorio. Y el encargado lleva un papel fundamental en su administración y repartición de horarios.

Dado que el tamaño de la población es muy reducido al estar formada por solo 9 profesores y el encargado del Laboratorio, no fue necesario realizar un muestreo con lo que se sugirió hacer una encuesta a los 9 profesores y entrevista a el encargado del laboratorio, asegurando así que la información recopilada sea completa y refleje la realidad de manera directa.

3.5.2 Análisis de las herramientas de recolección de datos a utilizar

3.5.2.1 Encuesta

Se diseñó una encuesta mediante Google Forms, compuesta por 9 preguntas cerradas de selección múltiple, dirigida a 9 docentes de la ULEAM Extensión El Carmen, el cuestionario se enfocó en recopilar datos sobre los principales problemas relacionados con el acceso al laboratorio de cómputo, la percepción sobre la seguridad física y la viabilidad de implementar un sistema automatizado de control de acceso.

3.5.2.2 Entrevista

Se realizó una entrevista abierta al encargado de los laboratorios de la carrera de Tecnologías de la Información, específicamente del Laboratorio de Cómputo 1 de la ULEAM Extensión El Carmen, esta entrevista tuvo como objetivo recopilar información detallada sobre los procesos actuales de control de acceso y seguridad física, así como evaluar la percepción y viabilidad de implementar un sistema de reconocimiento facial basado en inteligencia artificial.

3.5.2.3 Estructura de los instrumentos de recolección de datos aplicados

Para recopilar información relevante, se utilizan dos técnicas complementarias, la primera es una encuesta dirigida a 9 docentes de la ULEAM Extensión El Carmen, implementada de forma online mediante Google Forms, con el propósito de recolectar datos sobre los principales problemas relacionados con el acceso y la seguridad en el Laboratorio de Cómputo 1, esta técnica permite obtener una visión general de las percepciones y desafíos existentes en la gestión de los laboratorios.

La segunda técnica consiste en una entrevista semiestructurada realizada de manera presencial al encargado de los laboratorios de Tecnologías de la Información de la misma institución, este instrumento tiene como objetivo profundizar en los temas identificados a través de la encuesta, explorando desde una perspectiva más detallada los problemas actuales del control de acceso tradicional y evaluando la viabilidad de implementar un sistema automatizado basado en reconocimiento facial.

3.5.3 Plan de recolección de datos

El plan de recolección de datos del Proyecto Integrador "Sistema Informático con Redes Neuronales para la Seguridad Física en el Laboratorio de Cómputo 1 de la ULEAM Extensión El Carmen" se llevó a cabo durante la segunda semana de diciembre de 2024 en la ULEAM Extensión El Carmen. El objetivo principal fue recopilar información clave para cumplir con los objetivos planteados en la investigación.

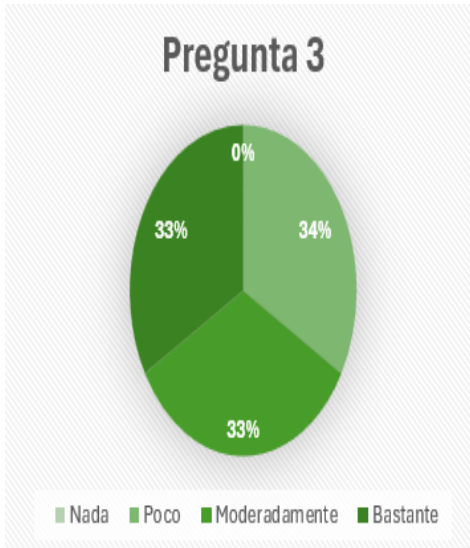
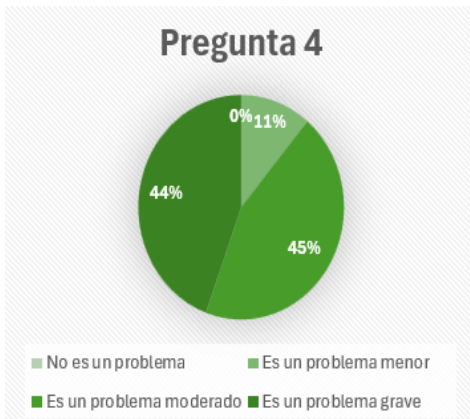
Las técnicas de recolección de datos que se usaron en este proyecto fueron 2 que son la encuesta y la entrevista. La primera fue aplicada a los docentes que usan el laboratorio 1, mientras que la entrevista fue el encargado de los laboratorios donde se profundizaron los temas y se trató de conocer más de primera mano las experiencias que se han presentado con los años.

La primera fase de la recolección de datos se dio entre las fechas 05/07/2025 y 15/07/2025 donde mediante la herramienta digital Google Forms se realizó las encuestas a los profesores enviando la misma por medios digitales usando la red social WhatsApp. La siguiente fase de esta figura en la fecha 10/07/2025 donde mediante una visita física a la oficina del ingeniero encargado del laboratorio 1 este nos atendió y dio el tiempo de responder cada pregunta y amablemente me permitió grabar la entrevista para su respectiva tabulación.

3.6 Análisis y presentación de resultados

3.6.1 Análisis encuesta

Preguntas	Respuestas	Interpretación										
1. ¿Con qué frecuencia has tenido problemas para acceder al laboratorio debido a la ausencia del conserje?	Pregunta 1 <table><thead><tr><th>Respuesta</th><th>Porcentaje</th></tr></thead><tbody><tr><td>Nunca</td><td>11%</td></tr><tr><td>Rara vez</td><td>67%</td></tr><tr><td>A veces</td><td>22%</td></tr><tr><td>Siempre</td><td>0%</td></tr></tbody></table>	Respuesta	Porcentaje	Nunca	11%	Rara vez	67%	A veces	22%	Siempre	0%	Esto sugiere que este problema no es constante, pero es lo suficientemente frecuente como para considerarse un inconveniente, la falta de acceso al laboratorio puede causar retrasos en las actividades y frustración entre los usuarios.
Respuesta	Porcentaje											
Nunca	11%											
Rara vez	67%											
A veces	22%											
Siempre	0%											
2. ¿Crees que la ausencia de un sistema para el uso del laboratorio contribuye a problemas como el acceso no autorizado, el uso indebido de recursos o incluso la pérdida de equipos?	Pregunta 2 <table><thead><tr><th>Respuesta</th><th>Porcentaje</th></tr></thead><tbody><tr><td>sí</td><td>89%</td></tr><tr><td>no</td><td>11%</td></tr><tr><td>no lo sé</td><td>0%</td></tr></tbody></table>	Respuesta	Porcentaje	sí	89%	no	11%	no lo sé	0%	La mayoría de los encuestados considera que la ausencia de un sistema de control en el laboratorio ha generado problemas. Esto evidencia la necesidad de implementar un mecanismo de supervisión que garantice mayor seguridad y control en el uso del laboratorio. Solo un pequeño porcentaje opina lo contrario, lo que refuerza la percepción general de que este es un problema significativo.		
Respuesta	Porcentaje											
sí	89%											
no	11%											
no lo sé	0%											

Preguntas	Respuestas	Interpretación								
3. ¿En qué medida la falta de coordinación entre los docentes al momento de abrir y cerrar el laboratorio ha afectado sus actividades?	Pregunta 3 <table><tr><td>Nada</td><td>0%</td></tr><tr><td>Poco</td><td>34%</td></tr><tr><td>Moderadamente</td><td>33%</td></tr><tr><td>Bastante</td><td>33%</td></tr></table>	Nada	0%	Poco	34%	Moderadamente	33%	Bastante	33%	Aunque no todos perciben este problema como algo grave, sí hay un impacto distribuido entre quienes lo consideran moderado o significativo, esto sugiere que esta falta de organización genera inconvenientes recurrentes que podrían mitigarse con un sistema automatizado que elimine la dependencia de los docentes para gestionar el acceso.
Nada	0%									
Poco	34%									
Moderadamente	33%									
Bastante	33%									
4. ¿Consideras que el uso no autorizado del laboratorio y sus recursos es un problema?	Pregunta 4 <table><tr><td>No es un problema</td><td>0%</td></tr><tr><td>Es un problema menor</td><td>11%</td></tr><tr><td>Es un problema moderado</td><td>44%</td></tr><tr><td>Es un problema grave</td><td>45%</td></tr></table>	No es un problema	0%	Es un problema menor	11%	Es un problema moderado	44%	Es un problema grave	45%	La mayoría lo considera moderado, lo que indica que existe una preocupación real sobre la seguridad de los recursos y el uso indebido de las instalaciones, esto refleja la necesidad de implementar medidas de control para garantizar que solo las personas autorizadas puedan acceder al laboratorio.
No es un problema	0%									
Es un problema menor	11%									
Es un problema moderado	44%									
Es un problema grave	45%									

Preguntas	Respuestas	Interpretación								
5. ¿Cuáles crees que son las principales consecuencias de no contar con un control de acceso en el laboratorio?	Pregunta 5 <table> <tr> <td>Retrasos</td> <td>37%</td> </tr> <tr> <td>Pérdida de recursos</td> <td>25%</td> </tr> <tr> <td>Acceso no autorizado</td> <td>38%</td> </tr> </table>	Retrasos	37%	Pérdida de recursos	25%	Acceso no autorizado	38%	Estas respuestas resaltan cómo la ausencia de un sistema adecuado afecta tanto la eficiencia operativa como la seguridad del laboratorio, la implementación de un sistema de acceso controlado podría resolver estos problemas y mejorar la gestión del laboratorio en general.		
Retrasos	37%									
Pérdida de recursos	25%									
Acceso no autorizado	38%									
6. ¿Qué tan importante consideras que es la existencia de un sistema automatizado de control de acceso al laboratorio?	Pregunta 6 <table> <tr> <td>Nada importante</td> <td>0%</td> </tr> <tr> <td>Poco importante</td> <td>22%</td> </tr> <tr> <td>Moderadamente importante</td> <td>78%</td> </tr> <tr> <td>Muy importante</td> <td>0%</td> </tr> </table>	Nada importante	0%	Poco importante	22%	Moderadamente importante	78%	Muy importante	0%	Se puede notar que hay un reconocimiento claro de que la implementación de este tipo de tecnología es fundamental para solucionar los problemas actuales relacionados con el acceso al laboratorio, aunque algunos lo ven como moderadamente importante, el consenso general es que el sistema automatizado es necesario para mejorar la gestión y la seguridad.
Nada importante	0%									
Poco importante	22%									
Moderadamente importante	78%									
Muy importante	0%									

Preguntas	Respuestas	Interpretación								
7. ¿Qué tan urgente consideras la implementación de un sistema de control de acceso en el laboratorio?	Pregunta 7 <table><tr><td>Nada urgente</td><td>0%</td></tr><tr><td>Poco urgente</td><td>44%</td></tr><tr><td>Moderadamente urgente</td><td>56%</td></tr><tr><td>Muy urgente</td><td>0%</td></tr></table>	Nada urgente	0%	Poco urgente	44%	Moderadamente urgente	56%	Muy urgente	0%	En cuanto a la urgencia, los encuestados destacan que la implementación del sistema de control de acceso es percibida como una necesidad importante, con una mayoría inclinándose hacia considerarlo muy urgente, esto refleja la presión que genera la situación actual y la percepción de que la solución tecnológica debe implementarse.
Nada urgente	0%									
Poco urgente	44%									
Moderadamente urgente	56%									
Muy urgente	0%									
8. ¿Qué opinas sobre la implementación de un sistema de reconocimiento facial para mejorar el acceso y la seguridad en el laboratorio?	Pregunta 8 <table><tr><td>No estoy de acuerdo</td><td>0%</td></tr><tr><td>Tengo dudas</td><td>44%</td></tr><tr><td>Me parece útil</td><td>56%</td></tr><tr><td>Es una solución ideal</td><td>0%</td></tr></table>	No estoy de acuerdo	0%	Tengo dudas	44%	Me parece útil	56%	Es una solución ideal	0%	La mayoría de los encuestados lo considera útil, mientras que otros lo califican como una solución ideal, esto muestra un fuerte apoyo hacia esta tecnología como una herramienta innovadora y eficiente para mejorar tanto el acceso como la seguridad en el laboratorio.
No estoy de acuerdo	0%									
Tengo dudas	44%									
Me parece útil	56%									
Es una solución ideal	0%									

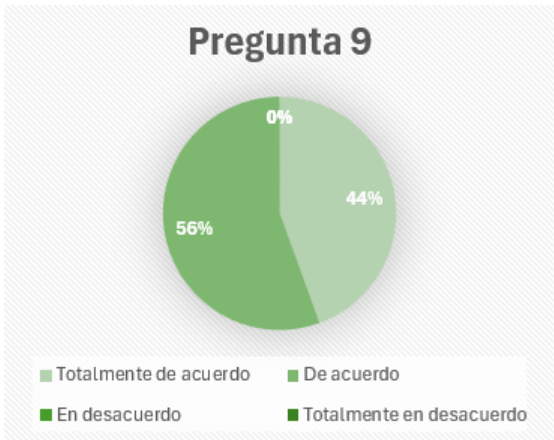
Preguntas	Respuestas	Interpretación
9. ¿Considera que la implementación de un sistema de reconocimiento facial basado en inteligencia artificial sería una solución adecuada para aumentar la seguridad en el laboratorio?	 A pie chart titled "Pregunta 9" displays the distribution of responses. The chart is divided into four segments: a large light green segment representing "Totalmente de acuerdo" at 44%, a slightly larger medium green segment for "De acuerdo" at 56%, and two very small segments for "En desacuerdo" and "Totalmente en desacuerdo", both labeled as 0%.	Es vista como una solución adecuada por todos los encuestado, no hubo respuestas negativas, lo que refuerza el nivel de aceptación de esta tecnología, este resultado evidencia un alto grado de confianza en que este sistema puede resolver de manera efectiva los problemas actuales relacionados con el acceso y la seguridad en el laboratorio.

Tabla 2: Análisis de encuesta

3.6.2 Análisis entrevista

Preguntas	Respuestas	Interpretación
1. ¿Con qué frecuencia has experimentado problemas para acceder al laboratorio debido a la ausencia del conserje encargado de abrirlo?	“Seguido, siempre está cerrado”	La respuesta muestra que el laboratorio más que todo en las primeras horas de la mañana y en primeras horas de mas tarde pasa más cerrado. Debido a que el conserje las cierra y solo él puede abrirlas y a veces cuesta

Preguntas	Respuestas	Interpretación
		encontrarlo y se pierde tiempo valioso.
2. ¿Consideras que la ausencia de un sistema de control para el uso del laboratorio ha generado problemas como el acceso no autorizado, el uso indebido de recursos o incluso la pérdida de equipos?	‘Si definitivamente hemos tenido problemas hemos encontrado maquinas en mal estado teclados, mouse y cables dañados’	La falta de un sistema de control ha resultado en daños y deterioro de los equipos, lo que evidencia la vulnerabilidad del laboratorio ante el uso inadecuado y la falta de supervisión. Esto resalta la necesidad de un mecanismo que regule y limite el acceso.

Preguntas	Respuestas	Interpretación
3. ¿En qué medida cree que la implementación de un sistema de reconocimiento facial para el acceso al laboratorio podría solucionar los problemas ocasionados por la falta de coordinación entre los docentes al abrir y cerrar el espacio?	‘...creo que un sistema de reconocimiento facial facilitaría primero el ingreso de cada uno de los docentes ...’	Se percibe el reconocimiento facial como una solución efectiva, ya que permitiría el acceso solo a personal autorizado en horarios específicos, reduciendo la entrada de personas no asignadas y mejorando la seguridad y organización en el uso del laboratorio.
4. ¿El uso no autorizado de los recursos del laboratorio es un problema serio? ¿Por qué?	‘...si es un problema serio ya que esas máquinas fueron asignadas a la institución a la extensión y por ende somos responsables directos de lo que pase con esa máquina...’	El uso no autorizado es un problema grave, ya que la institución es responsable de los equipos. Además, al ser un espacio público, la reparación de los dispositivos dañados depende de la disponibilidad de recursos externos, lo que puede generar demoras

Preguntas	Respuestas	Interpretación
		en la restauración del laboratorio.
5. ¿Cuáles cree que son las principales consecuencias de no tener un control de acceso en el laboratorio?	‘...las principales consecuencias el acceso a personal no autorizado y el robo de partes también de las computadoras...personas que se prestan para dañar las computadoras...’	La falta de control de acceso ha permitido la entrada de personas no autorizadas, lo que ha resultado en robos y daños en las computadoras. Esto evidencia la necesidad urgente de implementar medidas de seguridad para proteger los equipos y garantizar su buen estado.
6. ¿Qué tan importante considera implementar un sistema automatizado de control de acceso al laboratorio?	‘...lo considero de suma importancia, ya que así disminuimos el este el robo de partes de computadoras...’	La implementación de un sistema de control de acceso es considerada fundamental para reducir el robo de partes y extender la vida útil del equipo, lo que beneficiaría el

Preguntas	Respuestas	Interpretación
		funcionamiento del laboratorio a largo plazo.
7. ¿Cree que es urgente implementar un sistema de control de acceso en el laboratorio? ¿Por qué?	“...creo que sí que es urgente de manera urgente, deberíamos implementar un sistema de control de acceso...”	Existe un sentido de urgencia en la implementación de un sistema de control, ya que se considera una medida necesaria para preservar el laboratorio y garantizar su disponibilidad para la comunidad educativa.
8. ¿Cuál es su opinión sobre la implementación de un sistema de reconocimiento facial para gestionar el acceso y seguridad en el laboratorio?	‘...Sería muy importante la implementación de este sistema y a su vez también para el reconocimiento de la carrera a través de la comunidad...’	Se ve que tendrá buena acogida la implementación del sistema, no solo por la mejora en seguridad, sino también como una oportunidad para proyectar la innovación tecnológica de la institución hacia otros centros educativos del cantón.

Preguntas	Respuestas	Interpretación
9. Desde su perspectiva, ¿cree que la implementación de un sistema de reconocimiento facial basado en inteligencia artificial sería una solución efectiva para mejorar la seguridad en el laboratorio?	‘...sí, creo que sería efectivo ya que obtendremos el control este totalitario de las personas que ingresen...’	Se considera que el reconocimiento facial permitiría un control riguroso sobre las personas que ingresan al laboratorio. En caso de incidentes, este sistema facilitaría la identificación de los responsables, promoviendo un ambiente más seguro y regulado.

Tabla 3: Análisis de entrevista

3.6.3 Presentación y descripción de los resultados obtenidos

El objetivo de todo esto era claro: encontrar los problemas de acceso y seguridad en el Laboratorio de Cómputo 1 de la ULEAM, Extensión El Carmen, y proponer soluciones para que las cosas funcionen mejor.

Por lo que se vio en las encuestas y entrevistas, registrar quién entra al laboratorio a mano es una pérdida de tiempo y la gente se equivoca, como este proceso depende de una persona, la eficiencia se va al piso, sobre todo cuando hay mucha gente queriendo entrar al mismo tiempo.

Además, los sistemas que usan ahora para controlar quién entra y sale del laboratorio no son muy confiables. Esto hace que cualquiera pueda entrar sin permiso y usar los recursos de forma indebida, lo que es un gran problema para la seguridad del lugar.

Las preguntas 3 de la entrevista y 9 de la encuesta demuestra los registros en papel se pueden perder o dañar fácilmente. También el hecho de que una sola persona tenga que abrir

el laboratorio causa retrasos y frustración entre los usuarios. Todos estos problemas demuestran que, sin duda, urge un sistema digital y automatizado.

Las preguntas 4 de la encuesta y 7 de la entrevista muestran que, debido a la falta de supervisión continua, los recursos del laboratorio quedan expuestos a posibles daños o mal uso, un sistema de control automatizado reduciría la carga de trabajo del personal y permitiría un monitoreo más efectivo en tiempo real.

Las respuestas obtenidas en la pregunta 5 de la encuesta y la pregunta 8 de la entrevista resaltan la importancia de contar con un respaldo digital para los registros, actualmente la ausencia de esta herramienta significa que cualquier pérdida o daño físico en los registros resulta en la pérdida irreversible de información, lo que representa una amenaza importante para la gestión del laboratorio.

3.6.4 Informe final del análisis de los datos

En las entrevistas y encuestas realizadas, se identificaron problemas recurrentes en el acceso al laboratorio, como la falta de presencia del conserje, lo que causa retrasos y frustración entre los usuarios, la falta de coordinación entre los docentes para abrir y cerrar el laboratorio también afecta la organización y el uso eficiente del espacio, la implementación de un sistema automatizado de control de acceso podría resolver estos problemas al garantizar un acceso más organizado.

Otro de los problemas encontrados fue el mal uso de los dispositivos en el laboratorio como descargas de archivos maliciosos o muy pesados que llevan a enlentecer las computadoras, también el uso desmedido de la fuerza en mouse o teclados que les produce daños y no dejan continuar adecuadamente a los alumnos con sus prácticas profesionales, pero eso es importante implantar medidas preventivas de seguridad.

Un sistema de control de acceso que use inteligencia artificial para la identificación es tomado como la solución ideal por la mayoría de los encuestados y el entrevistado que según los datos obtenidos dan a conocer la necesidad urgente, por acciones como robos o daño de equipos, llevar un control mejoraría esto dando acceso solo a personal autorizado.

La implementación de un sistema automatizado de control de acceso también fue vista como urgente. Tanto encuestados como el entrevistado coincidieron en que esta medida es crucial para proteger los equipos y garantizar su disponibilidad para todos los usuarios.

CAPÍTULO IV

4. MARCO PROPOSITIVO

4.1 Introducción

En la actualidad, la seguridad física en entornos educativos, como los laboratorios de cómputo, se ha convertido en una prioridad debido al aumento de incidentes relacionados con el acceso no autorizado. Para dar solución a esta problemática, el proyecto propone el desarrollo de un sistema informático para el control de acceso al Laboratorio 1. Este sistema utiliza una Esp32 como hardware principal y técnicas de inteligencia artificial para la identificación de usuarios

Scrum fue la metodología que mejor se adapta a este proyecto por lo que es ágil y permitirá un desarrollo en menor tiempo, fomenta la colaboración en el equipo. Lo más importante es que tiene una gran adaptabilidad a los cambios y es capaz de hacer una mejora continua. Esta metodología definirá los roles, las tareas medidas por dificultad y e iterará en 3 Sprint: el primero enfocado al reconocimiento facial y base de datos, el segundo se basa en optimización del sistema, manejo de horarios y el último se dedica a la configuración del sistema.

El sistema utiliza técnicas de inteligencia artificial basadas en redes neuronales a través de la biblioteca face_recognition para identificar y autenticar a los usuarios autorizados mediante reconocimiento facial. Además de la identificación, incluye medidas de seguridad avanzadas como la detección de distancia y la verificación de "mirada sostenida" para prevenir intentos de suplantación con fotos o videos. Todos estos elementos garantizan un control de acceso robusto y confiable, mejorando significativamente la seguridad del laboratorio.

4.2 Descripción de la propuesta

En la Universidad Laica Eloy Alfaro de Manabí (ULEAM), Extensión El Carmen, el Laboratorio de Cómputo 1 enfrenta graves problemas de seguridad debido a la falta de un sistema automatizado de control de acceso. Actualmente, el ingreso se gestiona de manera manual, sin registros confiables, lo que facilita el acceso no autorizado, el uso indebido de equipos e incluso posibles robos. Esta situación perjudica tanto a la Universidad, que no puede monitorear eficientemente el laboratorio, cuyos recursos académicos están en riesgo.

El problema principal obtiene una solución con el sistema informático de reconocimiento facial de control de acceso planteado en el proyecto, que con ayuda de herramientas tecnológicas actuales garanticen un sistema intuitivo y de fácil uso. El sistema se divide en 4 módulos los cuales son frontend, backend, base de datos y hardware. Por otro lado, se hizo uso de React.js para manejar las interfaces de usuario, y el reconocimiento facial fue de la mano de librerías como opencv y face_recognition, las API, de comunicación fueron desarrolladas en php y mysql fue el gestor de datos utilizado en este proyecto. Para controlar la cerradura física fue necesario un esp32 que maneje la parte física.

Lo que son el manejo de fechas se realizará con la librería datetime y timedelta lo que permitirá gestionar y trabajar con fechas y horas que resultan fundamentales en este proyecto. En las API se manejarán solicitudes http como Request, lo que se espera haga una comunicación fluida en te hardware y software.

El proyecto se llevará a cabo bajo la metodología scrum que, con sus iteraciones ágiles y tareas divididas, se espera que se haga un trabajo más fluido y entregas más rápidas. Además de permitir hacer pruebas rápidas para mejorar mediante retroalimentación. Con la implementación de esta solución, se espera reducir el acceso no autorizado mediante autenticación biométrica precisa, optimizar la gestión administrativa con un panel de control en tiempo real, minimizar riesgos de robo o daño a los equipos del laboratorio, entre otros.

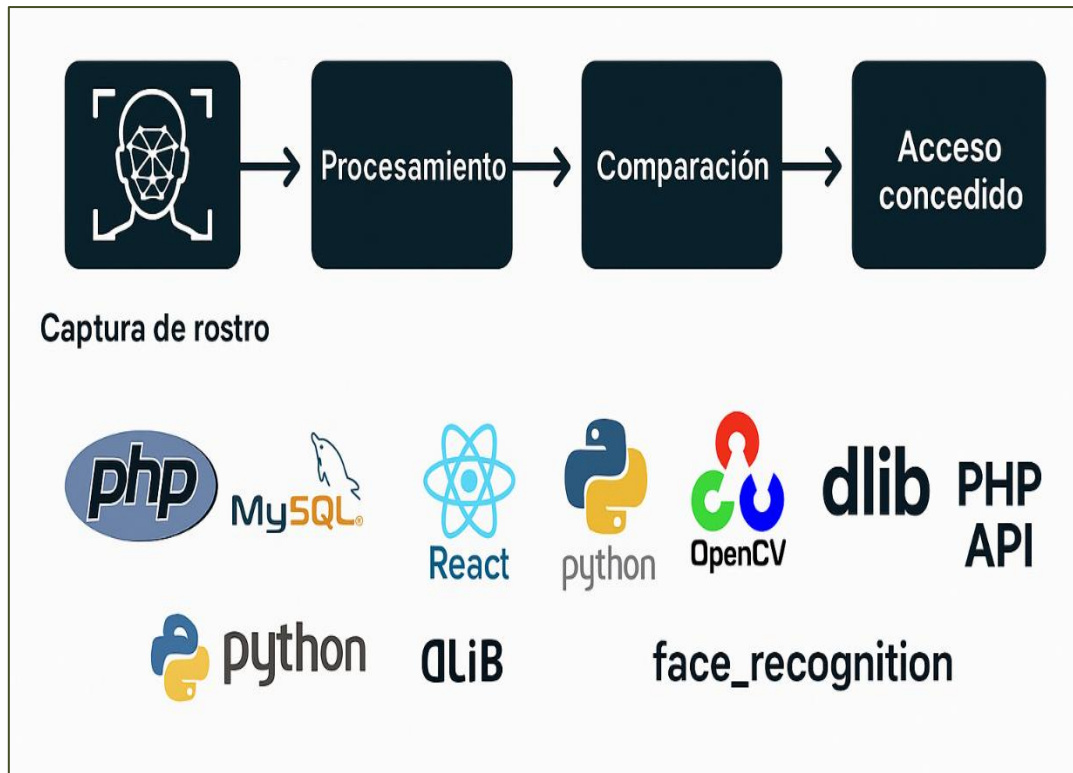


Ilustración 3: Modelo de funcionamiento

4.3 Determinación de recursos

4.3.1 Humanos

Personas que intervienen en las diferentes etapas del desarrollo del proyecto directa e indirectamente:

Cantidad	función	Detalles
1	desarrollador, autor	Autora y encargada de codificación, diseño, implementación del proyecto (Evelyn Velázquez)
1	Tutor	Tutor presente y guía en el proyecto (Ing. Bladimir Mora)

Tabla 4: Recursos Humanos

4.3.2 Hardware

Son todas las herramientas físicas usadas mediante la implementación del sistema de control de acceso. Entre estos destacan cables, computadora, tornillos y el módulo esp32.

HARDWARE	ESPECIFICACIONES
Laptop	windows 11 64 bits
	8GB RAM
	Intel(R) Core i7
	2.4 GHz velocidad del reloj
	1TB de disco solido
Cámara IP	2 MP
Conector JR45	CAT 6
Cable UTP	CAT6
Switch poe	4 puertos
ESP32	N/A
Módulo Relé	N/A
Adaptador	5V 1A
Cerradura Eléctrica	N/A
Adaptador	12V 2A
Cajetin Tigre	N/A
Enchufe Tauros	N/A
Bornera	N/A
Cable Gemew	#16
Toma Napow	N/A
Tornillo M4 8mm	N/A
Canaleta	N/A

Tabla 5. Hardware utilizado

4.3.3 Software

Son las herramientas lógicas que se usaron durante el desarrollo y codificación del sistema de control de acceso.

SOFTWARE	ESPECIFICACIONES
IDE	Visual Studio Code
Alojamiento	Servidor Apache, Xampp
Lenguajes empleados	php, JavaScript, python, React, HTML, c#
Librerías	react-router-dom, hooks (usestate, useeffect, useeref, useparams, usenavigate), web apis (getusermedia, todataurl), flask, flask-cors, opencv (cv2), face_recognition, numpy, requests, datetime, timedelta.

Tabla 6. software utilizado

4.3.4 Económicos

Recursos necesarios para llevar a cabo el proyecto tanto en hardware, software, mantenimiento, implementación:

Cantidad	Concepto	Características	C/U	Subtotal
1	Laptop	requerida para el desarrollo y programación	\$ 700,00	\$ 700,00
1	Cámara IP	necesaria para la identificación facial	\$ 64,00	\$ 64,00
4	Conector JR45	necesarios para conexiones ethernet	\$ 0,25	\$ 1,00
30 METROS	Cable UTP	necesarios para conexiones ethernet	\$ 0,65	\$ 19,50
1	Switch poe	necesarios para conexiones ethernet	\$ 25,00	\$ 40,00
1	ESP32	placa de procesamiento de datos para manejo inteligente de cerradura	\$ 11,00	\$ 11,00
1	Módulo Relé	herramienta para manejo de cerradura	\$ 2,86	\$ 2,86
1	Adaptador 12V 2A	permite la conexión entre dispositivos	\$ 4,05	\$ 4,05
1	Adaptador 5V 1A	permite la conexión entre dispositivos	\$2,75	\$2,75
1	Cerradura Eléctrica	responsable de la apertura y cierre de la puerta.	\$ 25,00	\$ 25,00
1	cajetín Tigre	necesario para instalación	\$ 13,50	\$ 13,50
1	Enchufe Tauros	necesario para instalación	\$ 1,00	\$ 1,00
1	Bornera	necesario para instalación	\$ 2,00	\$ 2,00
1 METRO	Cable Gemew	necesario para instalación	\$ 4,50	\$ 4,50
1	Toma Napoli	necesario para instalación	\$ 1,75	\$ 1,75
4	Tornillo M4 8mm	necesario para colocar cerradura	\$ 0,18	\$ 0,72
1	Batería	Necesaria para el servidor	\$30,00	\$30,00

Cantidad	Concepto	Características	C/U	Subtotal
2	canaletas	Proteger cableado	\$1,00	\$2,00
1	Caja de pazo	Proteger cableado	\$2,25	\$2,25
1	Impresión A3	Necesario para el usuario	\$5,00	\$5,00
500	Horas de trabajo	horas usadas para el desarrollo del sistema	\$ 15,00	\$ 7.500,00
6 MESES	Alojamiento	necesario para guardar los datos de los usuarios	\$ 15,00	\$ 90,00
6 MESES	Internet	necesario para la conexión con el servidor	\$ 30,00	\$ 180,00
TOTAL				\$ 8,702.88

Tabla 7. costos de implementación

4.4 Desarrollo SCRUM

SCRUM se posiciona como la metodología más adecuada para este tipo de proyecto debido a su enfoque ágil, flexible y centrado en la entrega de valor incremental. Como uno de los principales puntos fuertes de scrum es que se puede dividir estratégicamente en sprints, dividiendo el proyecto en partes complicadas que a su vez se dividen en diversas tareas que sean más manejable y permitan hacer los entregables de manera ágil.

Otro punto ventajoso de scrum son sus reuniones diarias o conocidas como daylis que permite hacer una retrospectiva de las tareas que se están llevando a cabo y mejorar en caso de ser necesario, como mejorar o cambiar el algoritmo de reconocimiento de ser necesaria una apreciación mayor, lo que aseguro un trabajo Robusto.

Bueno en conclusión con scrum se puede decir que da la agilidad necesaria para llevar a cabo un proyecto robusto y una implementación ordenada y eficiente de sistema. Al combinar entregas incrementales, adaptabilidad técnica y participación de los usuarios finales, se asegura un producto final que cumpla con los estándares de seguridad, precisión y usabilidad exigidos por la ULEAM, protegiendo así sus recursos y optimizando la gestión del laboratorio.

4.4.1 Roles

Rol	Descripción	Responsabilidades	Perfil	Responsable
Product Owner (PO)	Este rol fue asumido por la estudiante investigadora, responsable de priorizar los requerimientos, definir las funcionalidades esenciales del sistema de control de acceso y velar por que la solución desarrollada respondiera a las necesidades reales del laboratorio. A través de reuniones frecuentes con el tutor y de la recolección de datos mediante encuestas y entrevistas, logró identificar y documentar historias de usuario relevantes para construir un product backlog claro.	Definir y priorizar el Product Backlog	Estudiante	Evelyn Velázquez
		Validar el Incrementos		
Scrum Master (SM)	El tutor académico actuó como Scrum Master, guiando el proceso de desarrollo ágil. Su papel fue asegurar que se respetaran los principios de SCRUM, facilitando el cumplimiento de los plazos establecidos para cada sprint. También ofreció retroalimentación continua durante las revisiones de sprint, ayudando a eliminar obstáculos que pudieran afectar la entrega de valor del proyecto.	Facilitar reuniones	Tutor	Ing. Bladimir Mora
		Asegurar que el equipo siga Scrum.		
Equipo de Desarrollo	El equipo de desarrollo estuvo compuesto por la misma autora del proyecto, quien se encargó del diseño, desarrollo e implementación técnica del sistema. Entre sus responsabilidades figuraron: la configuración de la ESP3, el entrenamiento del modelo de reconocimiento facial, el diseño de la interfaz y la integración con la base de datos, así como la documentación del sistema. Esta distribución permitió una ejecución ágil, enfocada y adaptativa, respondiendo con eficiencia a los desafíos técnicos y metodológicos que	Domina las tecnologías requeridas (PHP, Python, React).	Estudiante	Evelyn Velázquez
		Disponibilidad para trabajar en el proyecto.		

Rol	Descripción	Responsabilidades	Perfil	Responsable
	surgieron durante el desarrollo del proyecto.			

Tabla 8: Roles Scrum

4.4.2 Historias de usuario

HU-001		Login de usuarios		
Dependencia		Ninguna (base)		
Tipo:	Funcional	Criterios:	✓ Formulario implementado en React.js	Puntos de historia: 5
Tecnologías:	React.js, PHP, MySQL, JWT, react-router-dom		✓ Validación de credenciales en backend PHP + MySQL	Sprint: 1
Estado:	Pendiente		✓ Generación de token de sesión JWT	Objetivo:
Prioridad:	Alta		✓ Redirección según rol (administrador o docente)	Acceder al sistema según rol autorizado

Tabla 9: Historia 1 login usuarios

HU-002		Registro de docentes		
Dependencia		HU-001		
Tipo:	Funcional	Criterios:	✓ El sistema debe permitir cargar datos personales.	Puntos de historia: 8
Tecnologías:	React, Flask, OpenCV, face_recognition, PHP, MySQL		✓ Permitir registrar rostros mediante la cámara web (frontend en React usando getUserMedia y <canvas>).	Sprint: 2
Estado:	Pendiente		✓ Confirmación de datos guardados en la base de datos MySQL (backend PHP).	Objetivo:
Prioridad:	Media-Alta			Habilitar acceso al sistema

Tabla 10: Historia 2 Registro docentes

HU-003		Reconocimiento facial		
Dependencia		HU-002		
Tipo:	Técnica	Criterios:	✓ Captura de imagen en tiempo real (React + Canvas + getUserMedia) ✓ Envío de datos al backend IA (Flask) ✓ Procesamiento con OpenCV y face_recognition (encodings 128D) ✓ Comparación contra la base de datos de rostros ✓ Respuesta menor a 8 segundos ✓ Validación del usuario para acceso	Puntos de historia: 13
Tecnologías:	Python, OpenCV, dlib, NumPy, PHP API, face_recognition			Sprint: 1
Estado:	Pendiente			Objetivo:
Prioridad:	Crítico			Permitir o denegar acceso mediante reconocimiento facial.

Tabla 11: Historia3 Reconocimiento facial

HU-004		Validación de horarios		
Dependencia		HU-001		
Tipo:	Funcional	Criterios:	✓ Validación en backend (PHP) si el usuario tiene un horario activo ✓ Cruce con la base de datos de horarios en MySQL (datetime y timedelta) ✓ Respuesta: acceso permitido, fuera de horario o denegado ✓ Registro de la acción en logs	Puntos de historia: 5
Tecnologías:	PHP, MySQL, React, datetime, timedelta			Sprint: 1
Estado:	Pendiente			Objetivo:
Prioridad:	Alta			Controlar acceso por horario/aula

Tabla 12: Historia4 Validación de horarios

HU-005		Gestión de horarios (CRUD)		
Dependencia		HU-001, HU-004		
Tipo:	Funcional	Criterios:	✓ Interfaz de gestión con calendario (React + FullCalendar) ✓ Crear, editar y eliminar horarios ✓ Prevenir solapamiento de horarios ✓ Persistencia en MySQL	Puntos de historia: 8
Tecnologías:	React, FullCalendar, PHP, MySQL			Sprint: 2
Estado:	Pendiente			Objetivo:
Prioridad:	Alta			Asignar y modificar los horarios de acceso para docentes

Tabla 13: Historia5 gestión de horarios

HU-006		Generación de reportes, gestión de aulas y periodos		
Dependencia		HU-004, HU-005		
Tipo:	Funcional	Criterios:	✓ Visualización de reportes, aulas y periodos.	Puntos de historia: 5
Tecnologías:	React, Chart.js, PHP, MySQL			Sprint: 3
Estado:	Pendiente			Objetivo:
Prioridad:	Bajo-Medio			Monitoreo uso del laboratorio

Tabla 14: Historia6 Generación de reportes

HU-007		Configuración del sistema		
Dependencia		HU-003		
Tipo:	Funcional	Criterios:	✓ Ajuste de parámetros del reconocimiento facial (ej. tolerancia) ✓ Gestión de módulos activos (cámara, ESP32, logs) ✓ Persistencia de configuración en base de datos	Puntos de historia: 3
Tecnologías:	React, PHP, MySQL			Sprint: 3
Estado:	Pendiente			Objetivo:
Prioridad:	Baja			Permitir modificar parámetros operativos del sistema.

Tabla 15: Historia 7 configuración de sistema

HU-008		Apertura de cerradura mediante ESP32		
Dependencia		HU-003, HU-004		
Tipo:	Técnica	Criterios:	✓ Comunicación Flask → ESP32 vía HTTP o MQTT ✓ Activación del relé para desbloquear la cerradura ✓ Verificación de identidad + horario antes de abrir ✓ Confirmación visual del estado (éxito/error) en frontend	Puntos de historia: 8
Tecnologías:	Python (Flask), ESP32, MQTT/HTTP, React			Sprint: 2
Estado:	Pendiente			Objetivo:
Prioridad:	Alta			Control físico del acceso mediante la apertura de la cerradura.

Tabla 16: Historia 8 apertura de cerradura

HU-009		Detección de Mirada Sostenida		
Dependencia		HU-003		
Tipo:	Funcional	Criterios:	✓ Captura de imagen del rostro mediante la cámara ✓ Estimación de Distancia (la persona a una distancia específica). ✓ Activación de acción secundaria (ej. apertura manual de puerta)	Puntos de historia: 5
Tecnologías:	Python, OpenCV, React			Sprint: 2
Estado:	Pendiente			Objetivo:
Prioridad:	Media			Permitir confirmación o apertura mediante un gesto visual.

Tabla 17: Historia 9 Optimización

4.4.3 Product backlog

ID	Historia	Prioridad	H-P	Depende	Criterios de Aceptación	Tecnologías
HU-001	Login de usuarios	Alta	5	Ninguna	✓ Login funcional por roles (admin/docente). ✓ Validación de usuario y contraseña contra MySQL. ✓ Manejo de sesiones. ✓ Seguridad: manejo de contraseñas cifradas. ✓ Error si credenciales son inválidas.	React.js, PHP, MySQL, CSS, react-router-dom

ID	Historia	Prioridad	H-P	Depende	Criterios de Aceptación	Tecnologías
					✓ Redirección según rol al ingresar.	
HU-002	Registro de usuarios (docentes)	Alta	8	HU-001	✓ Formulario de datos personales. ✓ Captura de rostro con cámara (getUserMedia + Canvas). ✓ Generación de encodings faciales. ✓ Almacenamiento de datos y rostro. ✓ Confirmación visual de éxito. ✓ Permitir actualizar datos o eliminar usuarios. ✓ Validación de campos obligatorios.	React.js, Python (Flask), OpenCV, face_recognition, Navigator MediaDevices, Canvas API, PHP + MySQL
HU-003	Reconocimiento facial para acceso	Crítica	13	HU-002	✓ Captura de imagen en tiempo real. ✓ Procesamiento con OpenCV + face_recognition. ✓ Comparación contra base de datos. ✓ Tiempo de respuesta < 8 segundos. ✓ Soporte para múltiples rostros registrados.	Python (Flask), OpenCV, face_recognition, NumPy, React + Canvas, Flask-CORS, JSON
HU-004	Validación de horarios	Alta	5	HU-001	✓ Consulta de horarios desde base MySQL. ✓ Validación si está dentro del horario permitido. ✓ Se puede aplicar restricción por año electivo y hora. ✓ Registro del intento en logs.	PHP + MySQL, React.js, datetime + timedelta (Python), Request (comunicación API)
HU-005	Gestión de horarios (CRUD)	Alta	8	HU-004	✓ Formulario para agregar, modificar y eliminar horarios. ✓ Visualización mediante calendario. ✓ Validación de horarios duplicados. ✓ Almacenamiento seguro en MySQL. ✓ Edición de horarios fácilmente desde el frontend.	React.js, PHP + MySQL, FullCalendar, request

ID	Historia	Prioridad	H-P	Depende	Criterios de Aceptación	Tecnologías
					✓ Mensajes al guardar, modificar o eliminar.	
HU-006	Reportes de acceso, gestión de aulas y periodos	Media	5	HU-004, HU-005	✓ Listado detallado de fechas de ingreso. ✓ Reportes de ingresos. ✓ Mostrar aulas y periodos ✓ Editar aulas y periodos ✓ Mostrar totales de accesos por periodo. ✓ Interfaz intuitiva para reportes.	React.js, PHP + MySQL, FileSaver.js, request
HU-007	Configuración del sistema (parámetros IA)	Media	3	HU-003	✓ Modificar la tolerancia del reconocimiento facial. ✓ Interfaz para ajustar parámetros. ✓ Guardado persistente en MySQL. ✓ Confirmación visual al aplicar cambios.	React.js, PHP + MySQL, Flask, request
HU-008	Apertura de cerradura mediante ESP32	Alta	8	HU-003, HU-004	✓ Comunicación entre Flask y ESP32 vía HTTP o MQTT. ✓ Validación de rostro + horario antes de apertura. ✓ Control físico del relé conectado a la cerradura. ✓ Registro del evento (acceso físico) en la base de datos.	Python (Flask), ESP32 (Microcontrolador), MQTT o HTTP, Relé + Hardware eléctrico, React.js
HU-009	Detección de Mirada Sostenida	Media	5	HU-003	✓ "Mirada Sostenida" (tiempo de visibilidad del rostro). ✓ Reconocimiento facial (con rostro de la persona). ✓ Estimación de Distancia (la persona a una distancia específica). ✓ Desencadenar acción secundaria	Python (Flask), , OpenCV, React.js, Canvas API

Tabla 18: Product Backlog

4.4.4 Estimación Product Backlog

Sprint	Título del Sprint	Historias Incluidas	Puntos de Historia	Tiempo Estimado (Días)
Sprint 1	Núcleo del Sistema y Reconocimiento Facial	HU-001 - Login de usuarios	5	2 días
		HU-002 - Registro de usuarios	8	4 días
		HU-003 - Reconocimiento facial	13	7 días
Subtotal Sprint 1			26 puntos	13 días (2 semanas)
Sprint 2	Control de Acceso Físico y Horarios	HU-004 - Validación de horarios	5	2 días
		HU-005 - Gestión de horarios (CRUD)	8	4 días
		HU-008 - Apertura de cerradura	8	4 días
		HU-009 - Detección de gesto	5	2 días
Subtotal Sprint 2			26 puntos	12 días (2 semanas)
Sprint 3	Reportes, Configuración y Notificaciones	HU-006 - Reportes de acceso	5	3 días
		HU-007 - Configuración del sistema	3	2 días
Subtotal Sprint 3			8 puntos	5 días (1 semana)
60 PUNTOS DE HISTORIA				

Tabla 19. Estimación Product Backlog

4.4.5 Requerimientos del sistema

4.4.5.1 Requerimientos funcionales

- ✓ **Autenticación mediante reconocimiento facial:** El sistema deberá identificar a los usuarios registrados mediante una cámara integrada con tecnología de redes neuronales.
- ✓ **Registro de accesos:** Se debe almacenar la fecha, hora de entrada, y nombre del usuario cada vez que accede al laboratorio.
- ✓ **Gestión de usuarios:** El sistema permitirá registrar, modificar y eliminar perfiles de usuarios autorizados (docentes, administrador).
- ✓ **Gestión de horarios:** El sistema debe asociar a cada usuario un horario de acceso permitido según la planificación académica.

- ✓ **Generación de reportes:** El sistema deberá generar reportes de accesos por usuario.
- ✓ **Control de apertura automática:** Una vez que el usuario sea autenticado, el sistema deberá habilitar el acceso físico mediante un sistema eléctrico de cerradura.
- ✓ **Interfaz de administración:** Se debe contar con una interfaz web para que el administrador del sistema gestione usuarios, horarios y revise reportes.

4.4.5.2 Requerimientos no funcionales

- ✓ **Disponibilidad:** El sistema debe estar disponible durante todo el horario académico (mínimo 12 horas diarias), con capacidad de reinicio automático en caso de fallas.
- ✓ **Escalabilidad:** El sistema deberá permitir integrar nuevos laboratorios y usuarios sin necesidad de rediseñar la arquitectura base.
- ✓ **Usabilidad:** La interfaz debe ser fácil de usar por el usuario final y amigable a la vista con colores agradables a la percepción de los docentes.
- ✓ **Seguridad:** Los datos de entrada a la aplicación como datos personales del registro y los datos faciales del reconocimiento deben estar cifrados o deben estar protegidos, haciéndolos de difícil acceso.
- ✓ **Precisión:** El sistema planteado en este proyecto sería eficiente al tener una precisión mínima del 80%, pero en lo práctico se buscará un porcentaje más alto en el reconocimiento facial para evitar ingresos no deseados.
- ✓ **Tiempo de respuesta:** hablando del tiempo que se toma entre el escaneo del rostro y el acceso al laboratorio no debe superar los 8 segundos.
- ✓ **Compatibilidad:** El sistema debe ser compatible con sensores Esp32, bases de datos MySQL, y librerías de IA como OpenCV.
- ✓ **Respaldo y recuperación:** Se debe implementar un sistema de respaldo automático de los registros de acceso y configuración del sistema para evitar pérdida de información ante fallos.

4.4.6 Identificación de riesgos

Durante la planificación y ejecución del proyecto, se identificaron posibles riesgos técnicos y operativos. A continuación, se presenta un análisis con sus respectivos planes de mitigación:

Riesgo identificado	Impacto	Probabilidad	Plan de mitigación
Baja precisión del reconocimiento facial en condiciones de poca luz	Alto	Media	Mejorar el dataset con imágenes variadas e incluir luces LED de refuerzo
Fallo en la conectividad entre la ESP32 y el servidor	Alto	Alta	Utilizar una red estable, implementar reintentos automáticos y logs de error
Limitaciones de memoria en la ESP32	Medio	Alta	Optimizar el código, reducir resolución innecesaria y usar compresión de imágenes
Pérdida de datos en la base de datos	Alto	Baja	Implementar backups automáticos y registros redundantes
Robo o daño de la ESP32	Medio	Baja	Instalar en carcasa protegida y advertencia disuasiva visible
Rechazo de usuarios al reconocimiento facial	Bajo	Baja	Capacitación previa y campaña de sensibilización sobre seguridad

Tabla 20: Riesgos

4.4.7 Sprint 1

4.4.7.1 Sprint Planning

Sprint	Título del Sprint	Historias Incluidas	Puntos de Historia	Tiempo Estimado	Inicio - Fin
Sprint 1	Núcleo del Sistema y Reconocimiento Facial	HU-001 - Login de usuarios	5	2 días	28/04/25-30/04/25
		HU-002 - Registro de usuarios	8	4 días	01/05/25-05/05/25
		HU-003 - Reconocimiento facial	13	7 días	06/05/25-13/05/25
Subtotal Sprint 1			26 puntos	13 días (2 semanas)	

Tabla 21: Sprint Planning (sprint1)

4.4.7.2 UML

4.4.7.2.1 Caso de Uso: Sprint 1

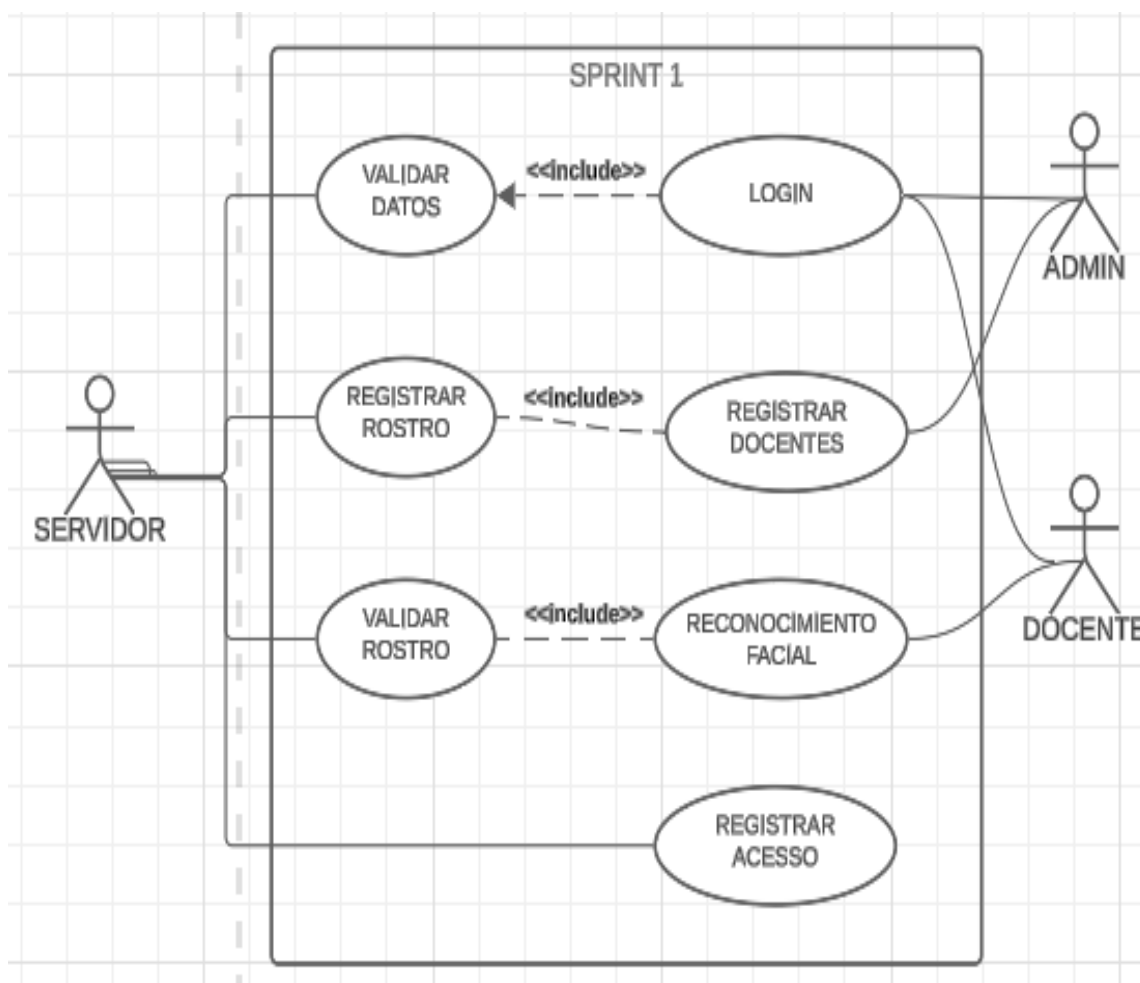


Ilustración 4: Caso de uso Sprint 1

Caso de uso: Sprint 1	Historias de usuario: HU1, HU2, HU3	
Criterios de aceptación: Ingreso al sistema Reconocimiento facial validación de datos	actor: -Docentes	Depende de: ninguno
	descripción: detección facial	
Autor: Evelyn Velásquez	Responsable: administrador	versión: 2.0

Tabla 22: Especificación caso de uso Sprint1

4.4.7.2.2 Diagrama de Secuencia: Registro docente

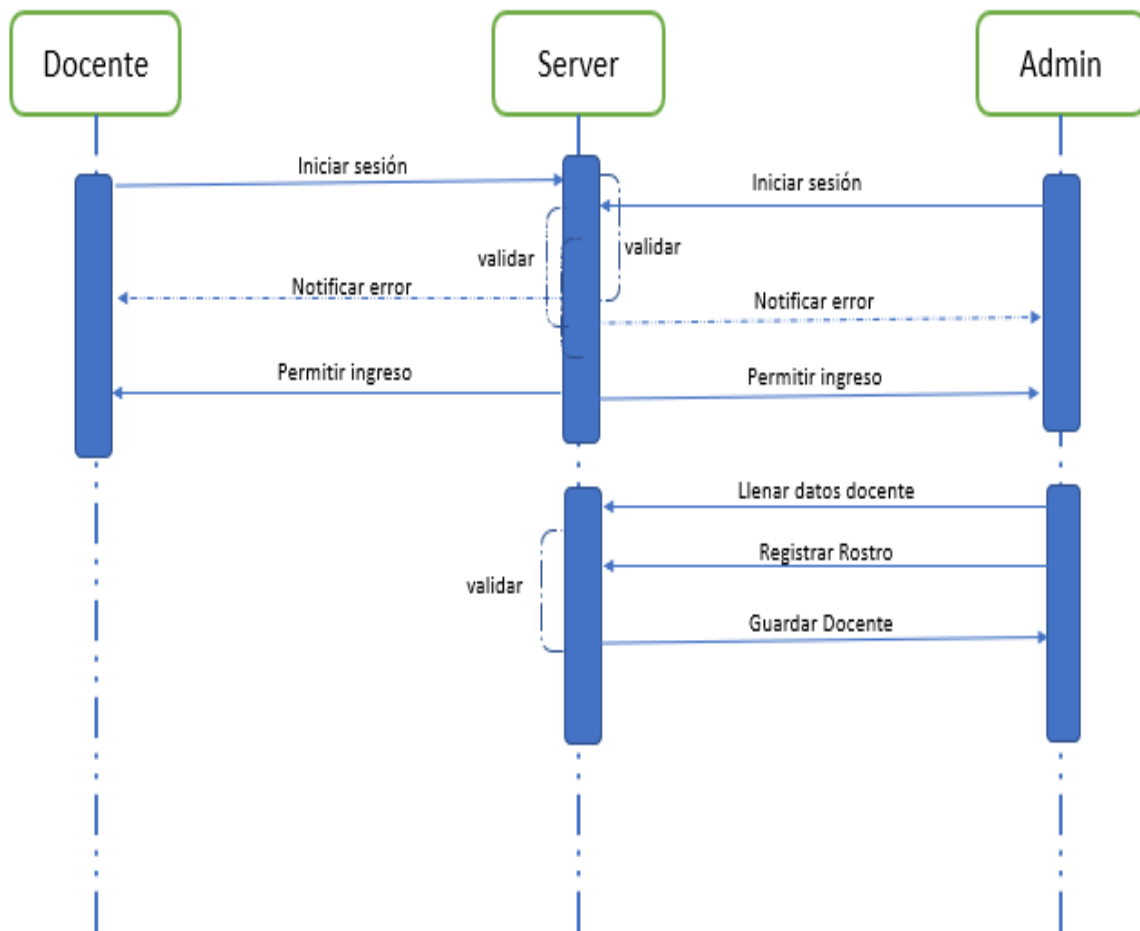


Ilustración 5: Diagrama de secuencia registro docente

4.4.7.2.3 Diagrama de Estado: Registro docente

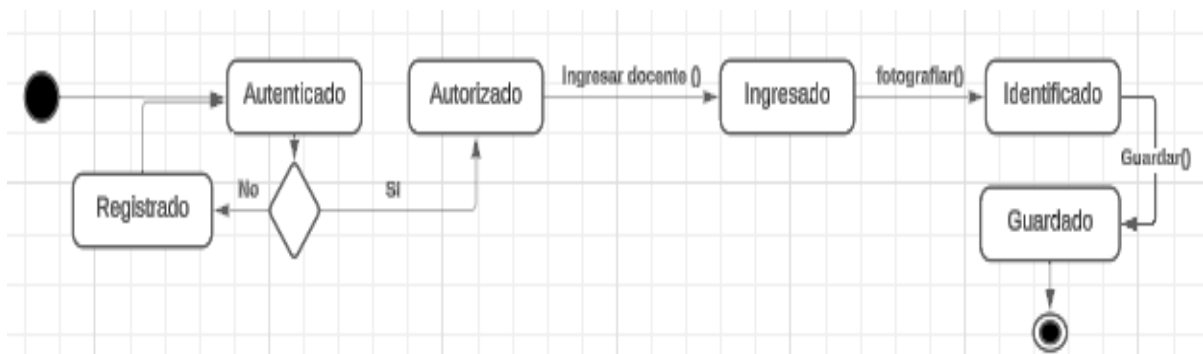


Ilustración 6: Diagrama de estado registro docente.

4.4.7.3 Dailys (Reuniones)

Fecha	Tema de la Reunión	¿Qué hice ayer?	¿Qué haré hoy?	¿Impedimentos?	Resumen
28/4/2025	Inicio de Sprint	Realicé la instalación de herramientas.	Iniciar la creación de la base de datos.	No.	Configuración del entorno y repaso de backlog.
29/4/2025	Diseño de base de datos	Avancé en el diseño del modelo entidad-relación.	Comenzar desarrollo de backend.	No.	Modelado de datos finalizado.
30/4/2025	Desarrollo de backend	Inicié desarrollo de las APIs.	Integrar APIs con base de datos.	No.	Primeros endpoints funcionando.
1/5/2025	Backend y validaciones	Se hicieron pruebas básicas.	Refinar endpoints y asegurar autenticación.	Feriado.	Validación de APIs (reunión opcional por feriado).
2/5/2025	Reconocimiento facial	Integré OpenCV y librerías de reconocimiento.	Ajustar el modelo de reconocimiento facial.	Baja precisión inicial en detección.	Inicio de pruebas con dataset.
5/5/2025	Pruebas reconocimiento	Ajusté parámetros del modelo.	Mejorar dataset y aumentar imágenes.	Dataset insuficiente.	Pruebas funcionales del modelo facial.
6/5/2025	Optimización de modelo	Implementé aumento de datos.	Integrar reconocimiento con backend.	No.	Mejora en la precisión del modelo.
7/5/2025	Integración API + AI	Hice pruebas de integración API.	Testear flujos completos.	No.	Backend conectado con reconocimiento facial.
8/5/2025	Interfaz de usuario UI	Diseñé las pantallas iniciales.	Continuar desarrollo UI.	No.	Desarrollo de interfaz web básico.
9/5/2025	Testeo flujo completo	Realicé pruebas unitarias.	Documentar APIs y errores.	No.	Flujo de registro con reconocimiento funcionando.
12/5/2025	Documentación	Avancé en documentación del sistema.	Validar documentación y hacer pruebas finales.	No.	Manual técnico preliminar listo.

Fecha	Tema de la Reunión	¿Qué hice ayer?	¿Qué haré hoy?	¿Impedimentos?	Resumen
13/5/2025	Cierre Sprint 1	Realicé pruebas finales.	Preparar presentación del sprint.	No.	Demostración MVP funcional.

Tabla 23. Dailys Sprint 1

4.4.7.4 Sprint Retrospective

4.4.7.4.1 Sprint burn-down

BURN-DOWN CHART																
NUMERO DE ITERACION														SPRINT 1		
ESFUERZO ESPERADO														26		
DIAS DEL SPRINT														13		
Product Backlog		días (Puntos completos)													Residuo	
Actividades	Balance inicial	1	2	3	4	5	6	7	8	9	10	11	12	13	Balance final	completado (%)
HU-001 - Login de usuarios	5	2	3												0	100%
HU-002 - Registro de usuarios	8			1	2	3	2								0	100%
HU-003 - Reconocimiento facial	13							1	2	3	3	2	1	1	0	100%
Esfuerzo restante	26	24	21	20	18	15	13	12	10	7	4	2	1	0	0	100%
Tendencia ideal	26	23	20	18	17	15	13	11	10	9	8	2	1	0		

Tabla 24. Burn-Down Sprint 1

4.4.7.4.2 Release burn-down

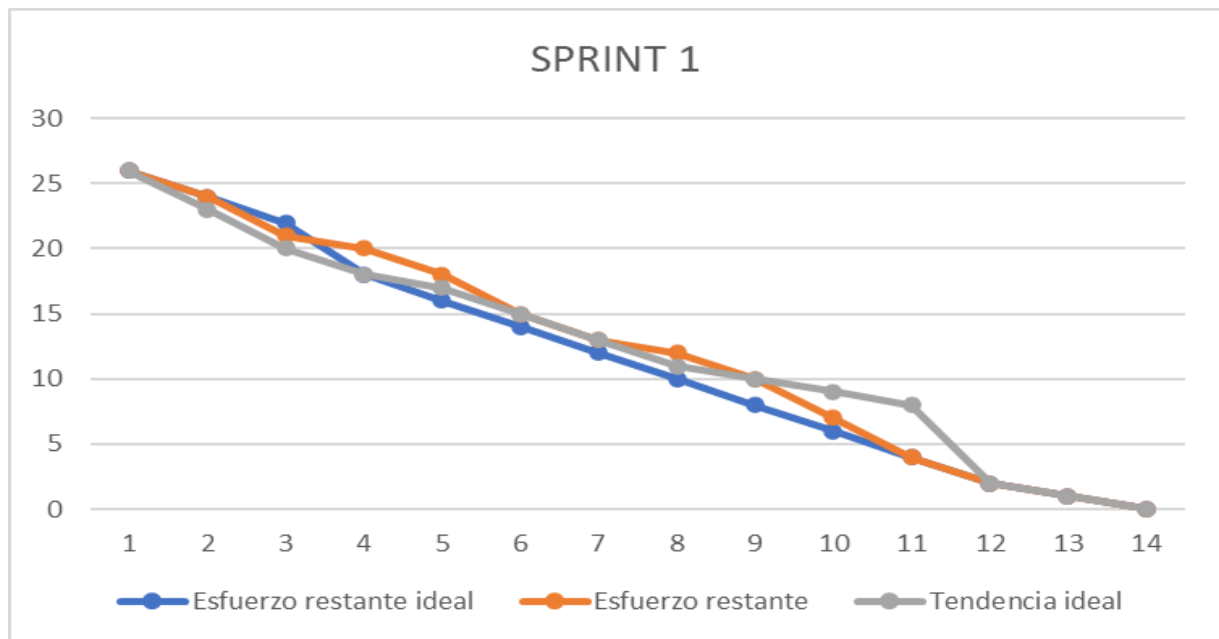


Ilustración 7. Release Burn-Down Sprint 1

4.4.7.4.3 Evidencias

Resumen:

Durante el Sprint 1 se desarrollaron las funcionalidades esenciales del sistema, enfocándose principalmente en el diseño e implementación de la base de datos y en el módulo de reconocimiento facial. Se construyó el backend utilizando Flask y se desarrollaron las APIs necesarias para el inicio de sesión y registro de usuarios. Para realizar el reconocimiento facial fueron necesarias herramientas como opencv y fase_recognition, lo que facilitó la captura y procesamiento de los rostros de los docentes para su respectivo registro y posterior uso del mecanismo. La vista del sistema web fue realizada con javascript mediante react.js esto incluyó el desarrollo de los formularios como login y registro. En esta primera iteración se le buscó dar funcionamiento a su arma más importante el reconocimiento. La documentación inicial y el soporte técnico fueron generados paralelamente para mantener la trazabilidad del desarrollo.

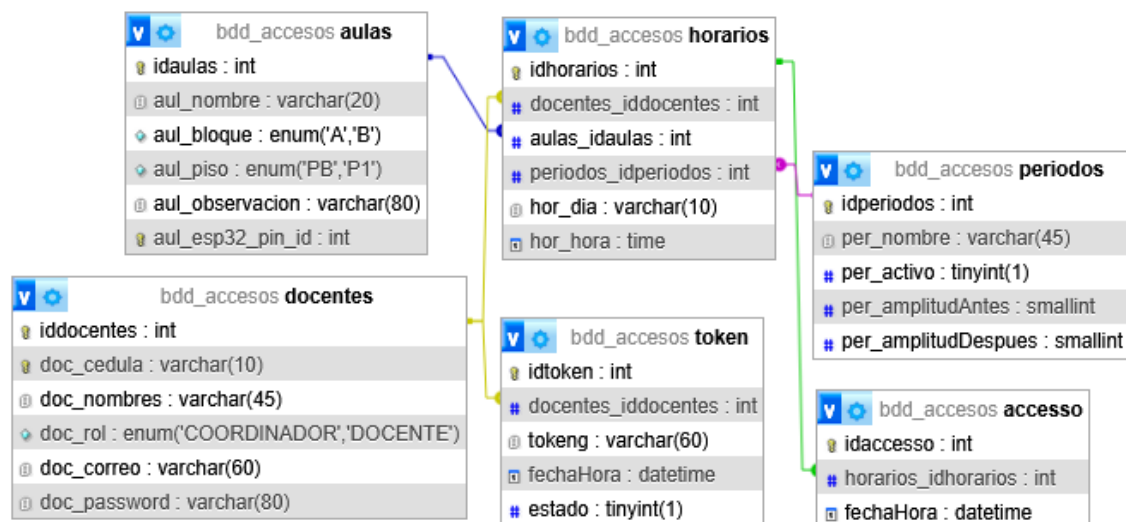


Ilustración 8: Diseño de base de datos

Muestra el diseño de la base de datos en MYSQL con el gestor phpMYADMIN cuenta con sus principales entidades: docentes, horarios, periodos, aulas, token, acceso y sus relaciones tanto 1:1 como 0:1.

Uleam
UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ
EXTENSION EL CARMEN

Cédula

Contraseña

Inicia sesión

Ilustración 9: Diseño Login

La ilustración 9 muestra el formulario de la pantalla inicial del sistema que es el login o inicio de sesión, el mismo cuenta con campos de ingreso de texto de cedula y contraseña y

su respectivo botón de ingreso, usa uno de los colores característicos de la universidad que es el rojo, en contraste con el blanco del fondo.

```
33     try {
34         const response = await fetch('http://localhost/COA-LAB/backend/api/login.php', {
35             method: 'POST',
36             headers: {
37                 'Content-Type': 'application/json',
38             },
39             body: JSON.stringify({ cedula, password }),
40         });
41         const data = await response.json();
42         if (response.ok && data.success && data.user && Object.keys(data.user).length > 0) {
43             login(data.user);
44         } else {
45             setError(data.message || 'Error al iniciar sesión. Credenciales inválidas o datos de usuario incompletos.');
```

```
46             console.error('Error de login o datos incompletos:', data);
47         }
48     } catch (err) {
49         setError('No se pudo conectar con el servidor. Por favor, asegúrate de que WAMP/XAMPP esté corriendo y el backend PHP sea accesible.');
```

```
50         console.error('Error de conexión:', err);
51     } finally {
52         setLoading(false);
53     }
54 }
```

Ilustración 10: Código Validación JS Login

La ilustración 10 muestra la lógica de programación usada en la validación de los datos enviados desde el inicio de sesión, lo que hace es que en caso de tener datos incorrectos de ingreso como credenciales invalidas o problemas en el servidor, esta muestra mensajes de error que guían al usuario sobre el error cometido, para que este pueda rectificar y autenticarse bien.

```

59 if ($docente) {
60     if (password_verify($password_plain, $docente['doc_password'])) {
61         $response['success'] = true; // El login fue exitoso
62         $response['message'] = "Login successful";
63         $response['user'] = [ // Datos del usuario para enviar al frontend
64             'iddocentes' => $docente['iddocentes'],
65             'cedula' => $docente['doc_cedula'],
66             'nombres' => $docente['doc_nombres'],
67             'rol' => $docente['doc_rol'], // Es crucial enviar el rol
68             'correo' => $docente['doc_correo']
69         ];
70         $status_code = 200; // HTTP 200 OK
71
72         // --- DEPURACIÓN: Login exitoso ---
73         error_log("[LOGIN_SUCCESS] Contraseña verifica. Login exitoso para " . $docente['doc_nombres']);
74     } else {
75         // Contraseña incorrecta
76         $response['message'] = "Cédula o contraseña incorrecta.";
77         // $response['success'] ya es false por defecto
78         // --- DEPURACIÓN: Contraseña NO verifica ---
79         error_log("[LOGIN_FAIL] Contraseña NO verifica. Contraseña enviada: '" . $password_plain . "', Hash DB: '" . $docente['doc_password'] . "'");
80     }
81 } else {
82     // Docente no encontrado
83     $response['message'] = "Cédula o contraseña incorrecta.";
84     // $response['success'] ya es false por defecto
85 }

```

Ilustración 11: Código Login API

La ilustración 11 muestra la codificación en el API de login creada en el lenguaje PHP. Donde primeramente el sistema valida si es docente o administrador y luego valida la existencia de los datos enviados, de estos existir, pasa a validar el ingreso y permitir al usuario acceder.

Iniciando cámara para REGISTRO... Por favor, mire a la cámara.

Cédula:

 1727315689

Nombres:

 Evelyn Velázquez

Rol:

 DOCENTE

Correo:

 eve@gmail.com

Contraseña:

 •••••

Registro Facial

Mire a la cámara y asegúrese de que su rostro esté bien visible para el registro.

Ilustración 12: Formulario Registro Docente

La ilustración 12 muestra la vista del formulario de los docentes con campos de texto como cédula, nombre, rol, correo y contraseña, para lo último también está el registro del rostro del docente, donde al presionar se abre la cámara del computador y guarda la foto tomada del docente.

```

169  const captureFace = () => {
170      console.log("DEBUG: captureFace llamado.");
171      if (!videoRef.current || !canvasRef.current || !isCameraActiveForEnrollment) {
172          setMessage('Error: La cámara no está activa para captura.');
```

```

173          setMessageType('error');
174          return;
175      }
176
177      const video = videoRef.current;
178      const canvas = canvasRef.current;
179      const context = canvas.getContext('2d');
```

```

180
181      canvas.width = video.videoWidth;
182      canvas.height = video.videoHeight;
183      context.drawImage(video, 0, 0, canvas.width, canvas.height);
184
185      const imageData = canvas.toDataURL('image/jpeg', 0.9); // Calidad 90%
186      setCapturedFaceData(imageData);
187      setMessage('Rostro capturado. Ahora puede hacer clic en "Agregar Docente a BD.");
188      setMessageType('success');
189      stopCameraForEnrollment(); // Detener la cámara después de capturar
190      console.log("DEBUG: Rostro capturado y cámara detenida.");
191  };
192

```

Ilustración 13: Código Captura de rostro con cámara

La ilustración 13 hace muestra del código de captura de con la cámara que esta implementado en el formulario de registro de docente. Donde al capturar la foto le da un tamaño con ancho y alto., también un formato para su respectivo almacenamiento.

```

193  // Esta función envia el rostro capturado al servidor Flask para REGISTRO
194  const sendFaceToFlask = async () => {
195      console.log("DEBUG: sendFaceToFlask llamado.");
196      if (!capturedFaceData) {
197          return { success: false, message: 'No hay rostro capturado para enviar.' };
198      }
199
200      try {
201          const response = await fetch(FACE_REGISTER_API_URL, {
202              method: 'POST',
203              headers: { 'Content-Type': 'application/json' },
204              body: JSON.stringify({
205                  cedula: formData.cedula,
206                  nombres: formData.nombres,
207                  image_data: capturedFaceData
208              }),
209          });
210
211          const data = await response.json();
212          if (response.ok && data.success) {
213              console.log("DEBUG: Rostro registrado en Flask exitosamente.");
214              return { success: true, message: data.message };
215          } else {
216              console.error('Error del servidor Flask (registro):', data);
217              return { success: false, message: data.message || 'Error desconocido del servidor Flask.' };
218          }
219      } catch (error) {
220          console.error('Error de red al enviar rostro a Flask (registro):', error);
221          return { success: false, message: 'Error de conexión con el servidor de reconocimiento facial (Flask). Asegúrese de que esté corriendo.' };
222      }
223  };

```

Ilustración 14: Código Envío de rostro a Flask

En la ilustración 14 la imagen muestra cómo se envían los datos del rostro a la librería flask. El archivo de imagen se transfiere vía http con el método Post para su respectivo

procesamiento. Flask lo compara con las fotos registradas y si hay coincidencia, se valida la identidad, para permitir el ingreso.

```
4 def process_camera_feed():
75     global last_access_times, active_gaze_sessions, distance_frames_count
76
77     cap = cv2.VideoCapture(IP_CAMERA_URL)
78     if not cap.isOpened():
79         print(f"Error: No se pudo abrir el stream de la cámara IP en {IP_CAMERA_URL}. Verifique
80             time.sleep(10)
81             return
82
83     print("Iniciando reconocimiento automático desde la cámara IP |...")
84     frame_counter = 0
85
86     while True:
87         now = datetime.now()
88         current_day_name_os = now.strftime('%A')
89         current_time = now.time()
90
91         day_mapping = {
92             'monday': 'Lunes', 'tuesday': 'Martes', 'wednesday': 'Miércoles',
93             'thursday': 'Jueves', 'friday': 'Viernes', 'saturday': 'Sábado',
94
95         }
96         current_day_name_normalized = day_mapping.get(current_day_name_os.lower(), current_day_n
97
98         is_recognition_active_for_schedule = False
99
100        for cedula_docente_registered in known_face_cedulas:
101            try:
102                response_horario = requests.get(PHP_API_HORARIOS_URL, params={'cedula_docente':
103                response_horario.raise_for_status()
104                horario_data = response_horario.json()
```

Ilustración 15: Código Proceso de reconocimiento y validación

Se muestra el flujo completo del reconocimiento facial. Incluye desde la captura hasta la verificación final del usuario. El sistema responde si el rostro coincide con uno registrado. Si es válido y está dentro del horario permitido, se autoriza el ingreso. Representa la función más crítica del sistema.

4.4.8 Sprint 2

4.4.8.1 Sprint Planning

Sprint	Título del Sprint	Historias Incluidas	Puntos de Historia	Tiempo Estimado	Inicio - Fin
Sprint 2	Control de Acceso Físico y Horarios	HU-004 - Validación de horarios	5	2 días	14/05/25-16/05/25
		HU-005 - Gestión de horarios (CRUD)	8	4 días	17/05/25-21/05/25
		HU-008 - Apertura de cerradura	8	4 días	29/05/25-02/06/25
		HU-009 - Detección de gestos	5	2 días	03/06/25-05/06/25
Subtotal Sprint 2			26 puntos	12 días (2 semanas)	

Tabla 25:: Sprint Planning (sprint2)

4.4.8.2 UML

4.4.8.2.1 Caso de uso: Sprint 2

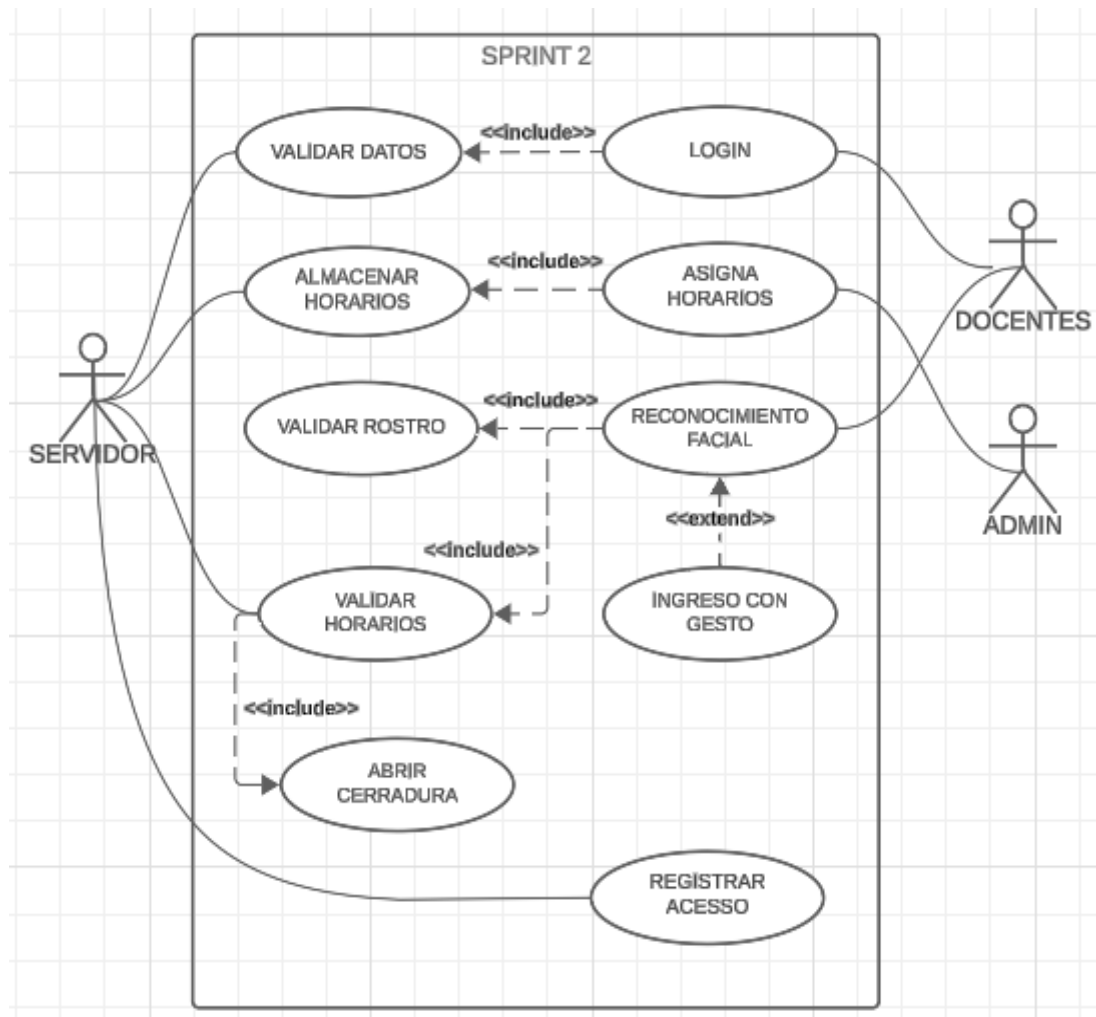


Ilustración 16. Caso de uso Sprint 2

Caso de uso: Sprint 2	Historias de usuario: HU4, HU5, HU8 HU9	
Criterios de aceptación: Ingreso al sistema Registro de rostro y docentes Definir horarios y almacenar	actor: -Docentes, administrador, servidor	Depende de: sprint1
	descripción: registro de docentes	
Autor: Evelyn Velásquez	Responsable: administrador	versión: 2.0

Ilustración 17: Especificación caso de uso Sprint 2

1.1.1.1.1 Diagrama de Secuencia: Gestión de horarios

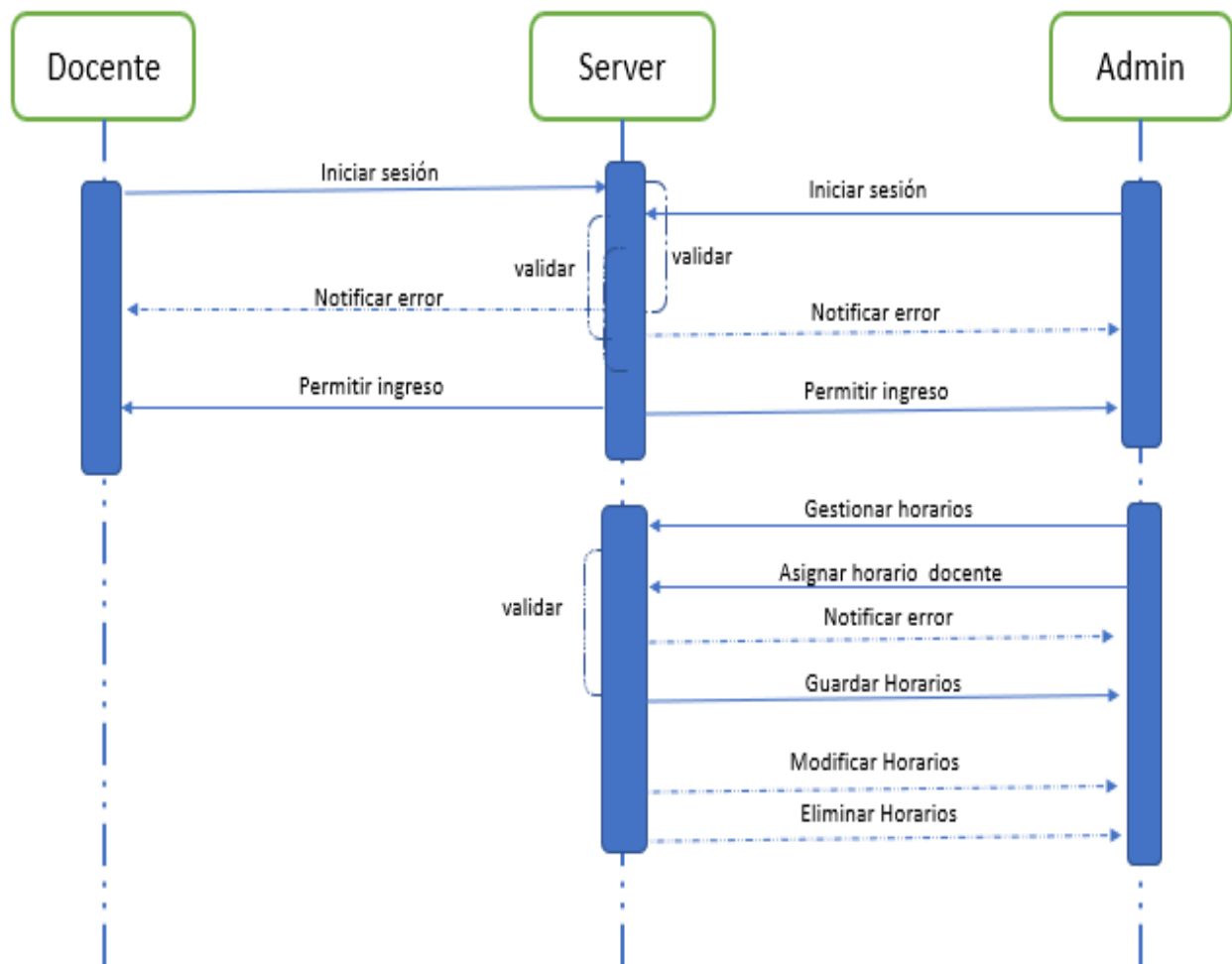


Ilustración 18: Diagrama de secuencia gestión de horarios

4.4.8.2.2 Diagrama de Estado: Gestión de horarios

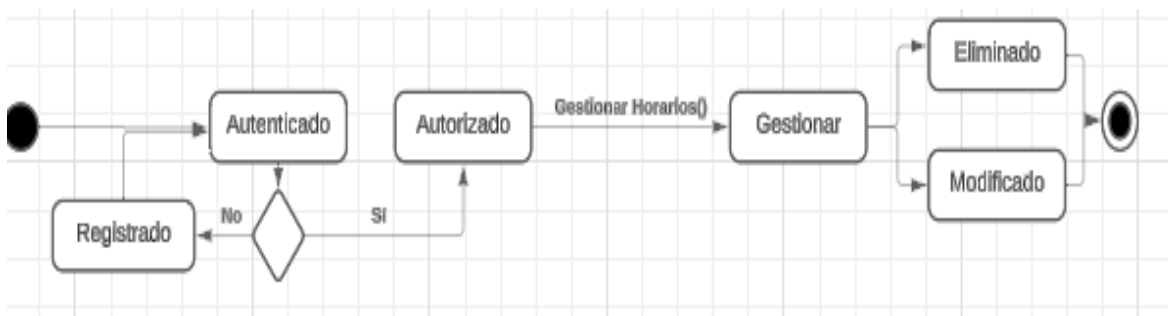


Ilustración 19: Diagrama de estados horarios

1.1.1.1 Dailys (Reuniones)

Fecha	Tema de la Reunión	¿Qué hice ayer?	¿Qué haré hoy?	¿Hay impedimentos?	Resumen
14/5/2025	Inicio de Sprint 2	Cierre Sprint 1 y backlog.	Crear módulo de usuarios.	No.	Definición de tareas: roles y horarios.
15/5/2025	Roles de usuarios	Programación de permisos.	Desarrollar horarios.	No.	Roles implementados.
16/5/2025	Módulo de horarios	Creación de BD horarios.	Integrar horarios con login y AI.	No.	Horarios funcionales.
17/5/2025	Validación horarios	Validación inicial.	Refinar excepciones y horarios.	No.	Pruebas funcionales de horarios.
20/5/2025	UI gestión de usuarios	Interfaz de usuarios.	Agregar edición y eliminación.	No.	Pantalla de gestión desarrollada.
21/5/2025	Pruebas control acceso	Pruebas con usuarios.	Preparar integración con hardware.	Casos límite por definir.	Validación de roles y horarios.
29/5/2025	Corrección errores	Ajustes en validación.	Configurar acceso físico.	No.	Errores solucionados.
30/5/2025	Validación con hardware	Configuración ESP32.	Pruebas apertura puerta.	Problemas conexión ESP32.	Inicio de conexión con ESP32.
2/6/2025	Integración completa HW	Solucioné conexión hardware.	Pruebas fallos y seguridad.	No.	Prueba hardware + software exitoso.
3/6/2025	Testeo con hardware	Validación hardware.	Documentar hardware.	No.	Flujo completo operativo.
4/6/2025	Documentación	Redacción de manual hardware.	Cierre documentación.	No.	Manual usuario + técnico.
5/6/2025	Cierre Sprint 2	Pruebas finales.	Preparar demo y cierre.	No.	Acceso físico + validación horarios funcionando.

Tabla 26. Dailys Sprint 2

1.1.1.1 Sprint Retrospective

4.4.8.2.3 Sprint burn-down

BURNDOWN CHART															
NUMERO DE ITERACION														SPRINT 2	
ESFUERZO ESPERADO														26	
DIAS DEL SPRINT														12	
Product Backlog		dias (Puntos completos)												Residuo	
Actividades	Balance inicial	1	2	3	4	5	6	7	8	9	10	11	12	Balance final	completado (%)
HU-004 - Validación de horarios	5	3	2											0	100%
HU-005 - Gestión de horarios (CRUD)	8			3	2	2	1							0	100%
HU-008 - Apertura de cerradura	8							1	2	3	2			0	100%
HU-009 - Detección de gesto	5											3	2	0	100%
Esfuerzo restante	26	23	21	18	16	14	13	12	10	7	5	2	0	0	100%
Tendencia ideal	26	25	22	18	17	14	13	11	10	5	4	2	0		

Tabla 27. Burn-Down Sprint 2

4.4.8.2.4 Release burn-down

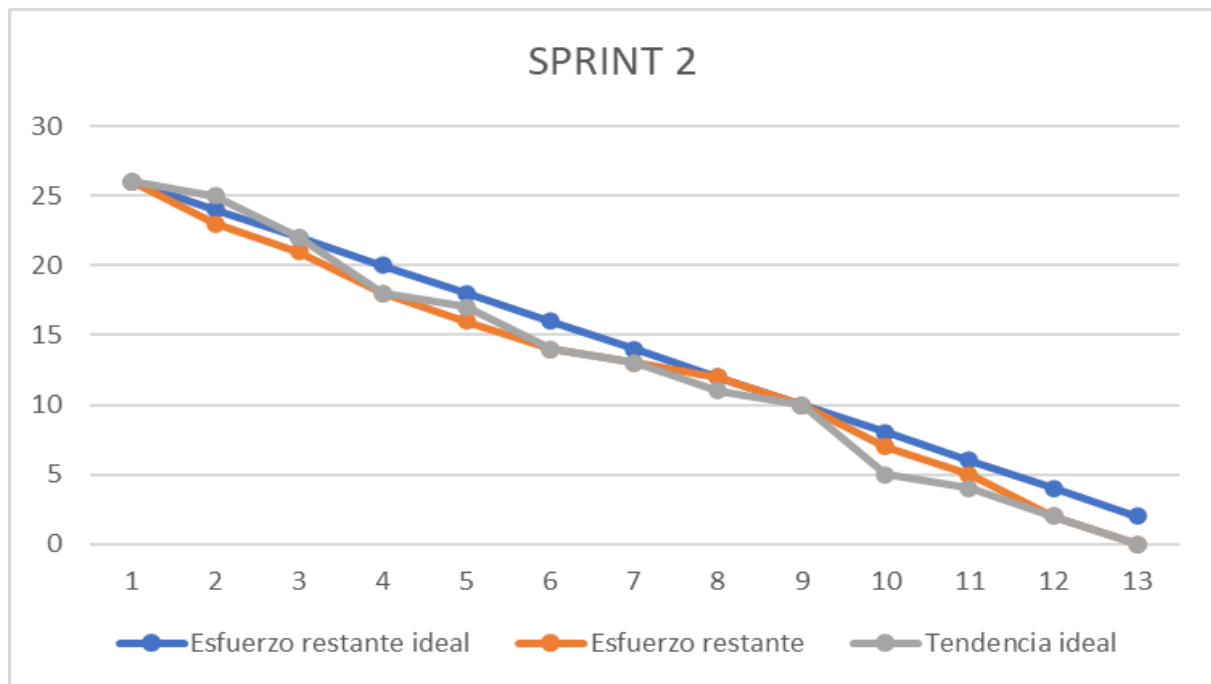


Ilustración 20. Release Burn-Down Sprint 2

4.4.8.2.5 Evidencias

Resumen:

En el segundo sprint, el foco principal fue la integración del sistema informático con los dispositivos físicos para el control de acceso. Se desarrolló el módulo de horarios del sistema, que permite al administrador definir los turnos y las ventanas de tiempo de acceso para los docentes. Esta información es consumida por el servidor de inteligencia artificial para validar el acceso en tiempo real. A través de un código basado en redes neuronales, el sistema realiza la validación facial y, al verificar un rostro, envía una señal a la placa ESP32 para activar la cerradura. Finalmente, esta implementación fue probada en situaciones reales para ajustar detalles técnicos de conexión, respuesta y latencia, asegurando un sistema confiable y robusto.



Lista de Horarios

Opciones

ID	DOCENTE	AULA	PERIODO	DÍA	HORA	ACCIONES
1	Evelyn Velázquez	Laboratorio 1 TI	2029-2	Lunes	10:00	Modificar Eliminar
13	Alaia Loor	Laboratorio 1 TI	2029-2	Martes	11:00	Modificar Eliminar
14	Alaia Loor	Laboratorio 1 TI	2029-2	Martes	12:00	Modificar Eliminar
10	Jordan Loor	Laboratorio 1 TI	2029-2	Miércoles	20:00	Modificar Eliminar
2	Evelyn Velázquez	Laboratorio 1 TI	2029-2	Viernes	10:00	Modificar Eliminar

Ilustración 21: CRUD Horarios

Esta es la ilustración 21 y se muestra la interfaz del módulo crud de horarios, aquí se registran, editan o eliminan turnos de acceso al laboratorio para docentes. Aquí es donde se otorgan los horarios de laboratorio y debe estar validado que estos no se repitan, ya que causaría conflictos.

```

33  const fetchHorarios = async () => {
34      setLoading(true);
35      setError('');
36      try {
37          const response = await fetch(API_BASE_URL_HORARIOS);
38          if (response.ok) {
39              const data = await response.json();
40              if (data.success) {
41                  setHorarios(data.horarios);
42              } else {
43                  setError(data.message || 'Error al cargar los horarios.');

```

Ilustración 22: Código Listar Horarios

La ilustración 22 es esta imagen se observa y donde se muestra el código que permite listar los horarios desde la base de datos hacia la vista del docente y administrador. Se usa para mostrar en pantalla mediante el sistema web qué turnos están corresponden a cada docente. También muestra un error de no tener conexión al servidor

```

268 // Verificar conflicto para el aula
269 $stmt_check_aula = $conn->prepare("SELECT COUNT(*) FROM horarios WHERE aulas_idaulas = ?
270 AND hor_dia = ? AND hor_hora = ? AND periodos_idperiodos = ? AND idhorarios != ?");
271 $stmt_check_aula->bind_param("issii", $newAulaId, $newDia, $newHora, $newPeriodoId, $id);
272 $stmt_check_aula->execute();
273 $stmt_check_aula->bind_result($count_aula);
274 $stmt_check_aula->fetch();
275 $stmt_check_aula->close();
276
277 if ($count_aula > 0) {
278     $response['message'] = "El aula ya está ocupada por otro horario para ese día y hora en el período actual.";
279     $status_code = 409;
280     break;
281 }
282

```

Ilustración 23: Código Validación de Horarios

La ilustración 23 trata del código de validación de los horarios como se dijo antes estos no pueden chocar porque causaría conflictos y el problema inicial fuera a peor. Mediante una consulta mysql se verifica que no exista nadie más con el horario que se va a registrar.

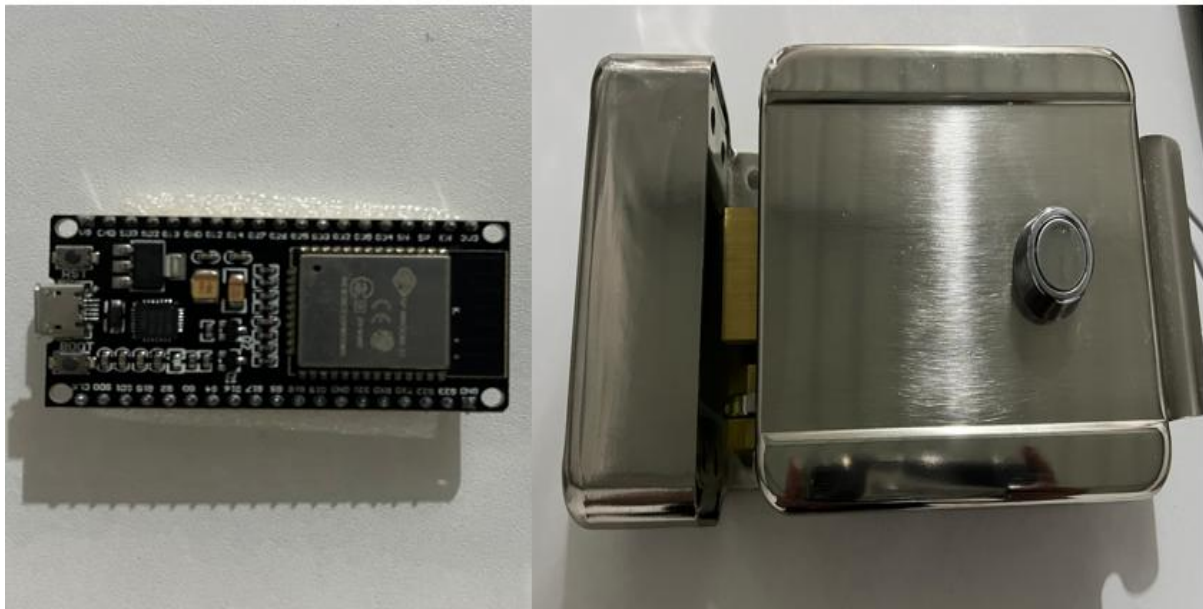


Ilustración 24: Hardware (ESP32+CERRADURA)

Presenta una fotografía del hardware: la placa ESP32 conectada a una cerradura eléctrica. Este componente permite abrir físicamente la puerta del laboratorio. La apertura solo ocurre si el sistema valida rostro y horario. Integra software y hardware en una solución real. Es prueba tangible del sistema físico.

4.4.9 Sprint 3

4.4.9.1 Sprint Planning

Sprint	Título del Sprint	Historias Incluidas	Puntos de Historia	Tiempo Estimado	Inicio - Fin
Sprint 3	Reportes, Configuración y Notificaciones	HU-006 - Reportes de acceso, gestión de aulas y periodos.	5	3 días	22/05/25-25/05/25
		HU-007 - Configuración del sistema	3	2 días	26/05/25-28/05/25
Subtotal Sprint 3			11 puntos	5 días (1 semana)	

Tabla 28:: Sprint Planning (sprint3)

4.4.9.2 UML

4.4.9.2.1 Caso de uso: Sprint 3

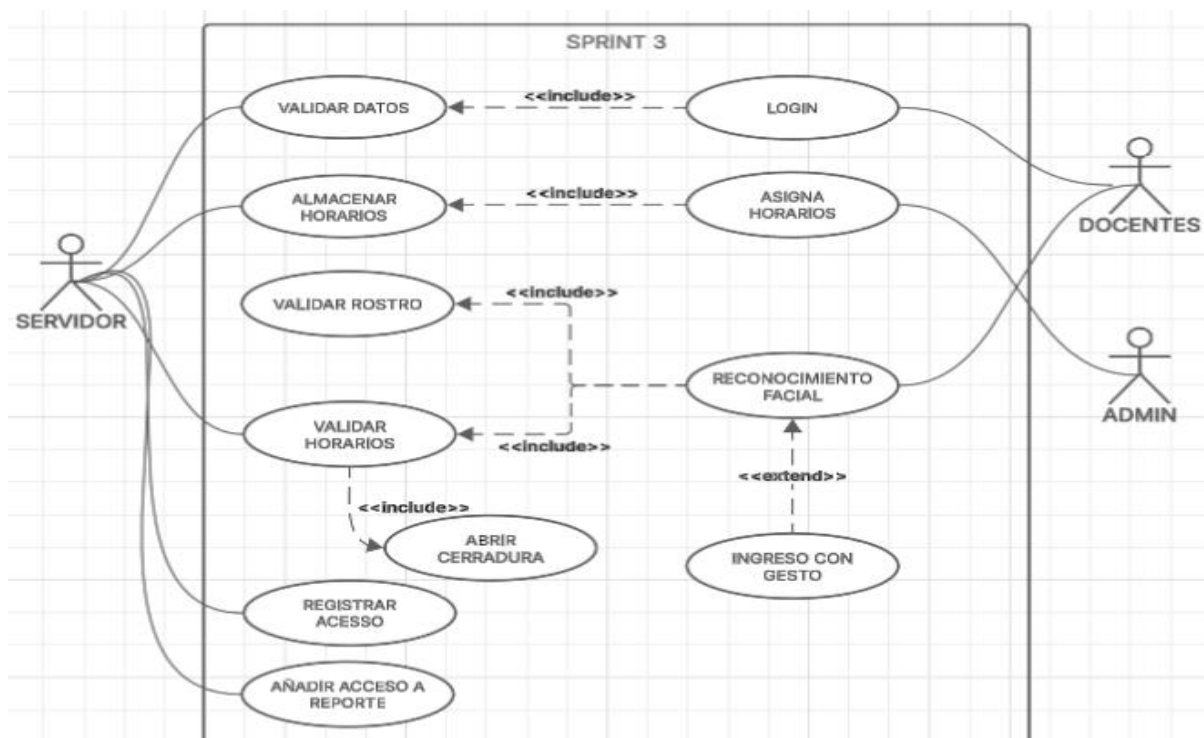


Ilustración 25. Caso de uso Sprint 2

Caso de uso: Sprint 3	Historias de usuario: HU6, HU7	
Criterios de aceptación: Ingreso al sistema Registro de rostro y docentes Definir horarios y almacenar Reporte de acceso	actor: -Docentes, administrador, servidor	Depende de: sprint1, sprint2
	descripción: reporte de acceso	
Autor: Evelyn Velásquez	Responsable: administrador	versión: 2.0

Tabla 29: Caso de uso Sprint 3

1.1.1.1.1 Diagrama de Secuencia: Reportes

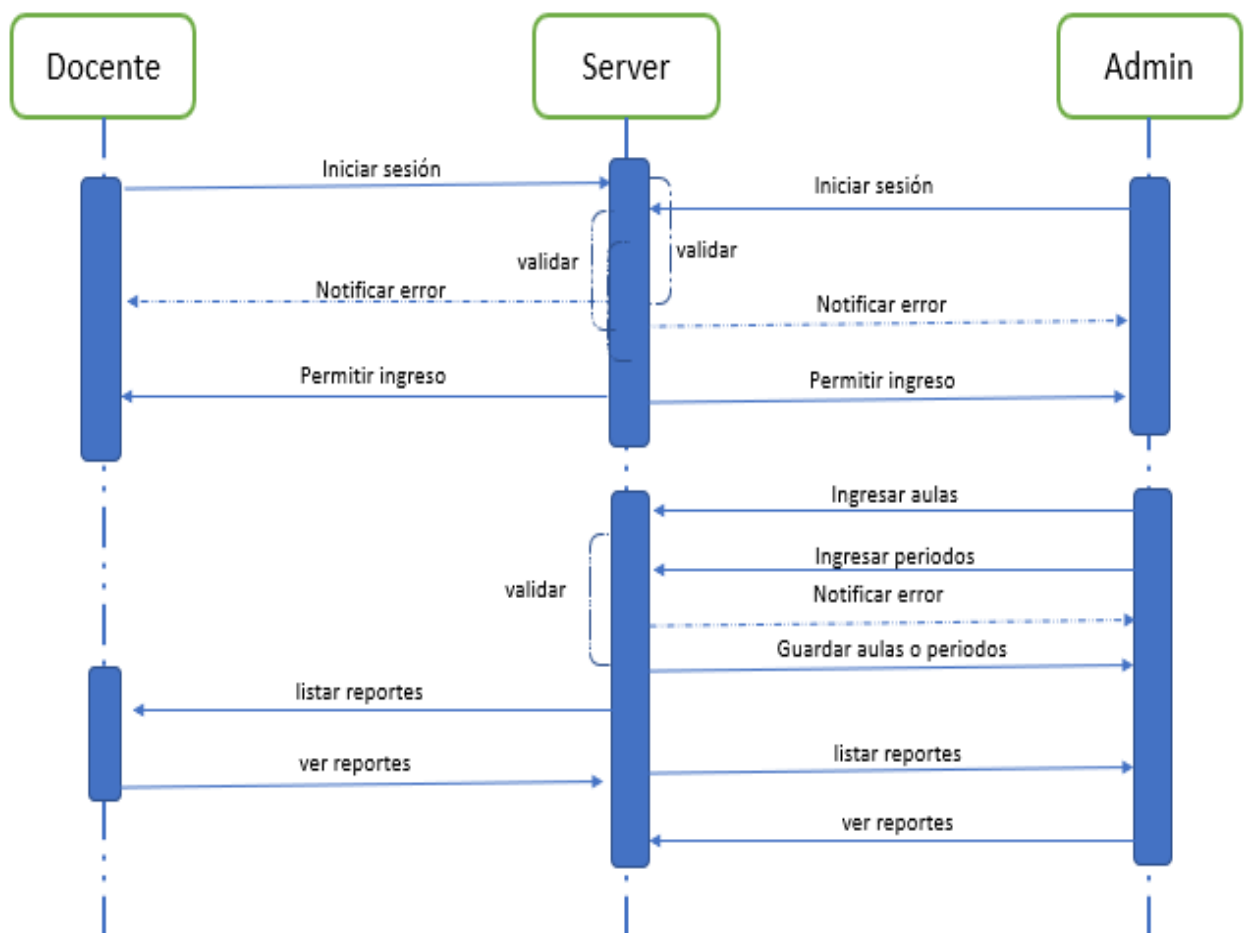


Ilustración 26: Diagrama de secuencia reportes

4.4.9.2.2 Diagrama de Estado: Reportes

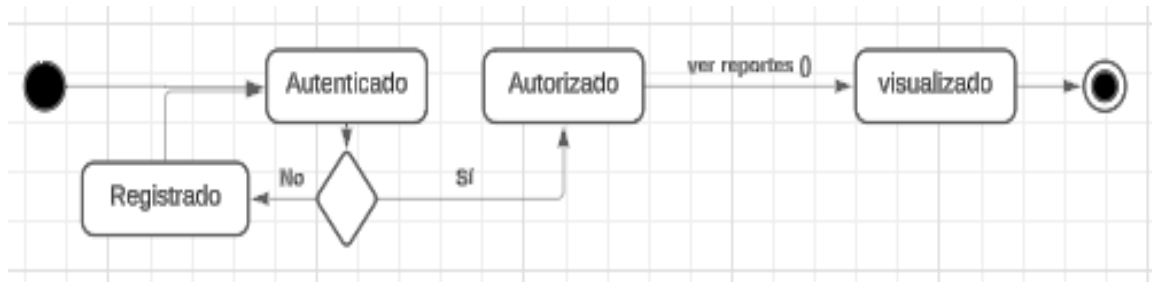


Ilustración 27: Diagrama de estado reportes.

1.1.1.1 Dailys (Reuniones)

Fecha	Tema de la Reunión	¿Qué hice ayer?	¿Qué haré hoy?	¿Hay impedimentos?	Resumen
22/5/2025	Inicio Sprint 3	Repaso backlog.	Iniciar módulo de reportes.	No.	Planificación: reportes y alertas.
23/5/2025	Reportes básicos	Desarrollo reportes base.	Mejorar filtros y diseño.	No.	Reportes de accesos y horarios.
25/5/2025	Pruebas de alertas	Validación de notificaciones.	Pruebas generales.	No.	Sistema de alertas funcionando.
26/5/2025	Configuración avanzada	Añadí opciones de gestión.	Validar sistema completo.	No.	Panel de configuración completo.
27/5/2025	Validación completa	Pruebas generales finales.	Documentación y demo.	No.	Sistema validado hardware + software.
28/5/2025	Cierre Sprint 3	Validación final.	Preparar sustentación y entrega.	No.	Sistema completo listo para entrega.

Tabla 30.Dailys Sprint 3

1.1.1.1 Sprint Retrospective

4.4.9.2.3 Sprint burn-down

BURNDOWN CHART								
NUMERO DE ITERACION						SPRINT 3		
ESFUERZO ESPERADO						8		
DIAS DEL SPRINT						5		
Product Backlog		dias (Puntos completos)					Residuo	
Actividades	Balance inicial	1	2	3	4	5	Balance final	completado (%)
HU-006 - Reportes de acceso, gestión de aulas y periodos	5	1	2	2			0	100%
HU-007 - Configuración del sistema	3				2	1	0	100%
Esfuerzo restante	8	7	5	3	1	0	0	100%
Tendencia ideal	8	6,5	4	3,5	2	0		

Tabla 31. Burn-Down Sprint 3

4.4.9.2.4 Release burn-down

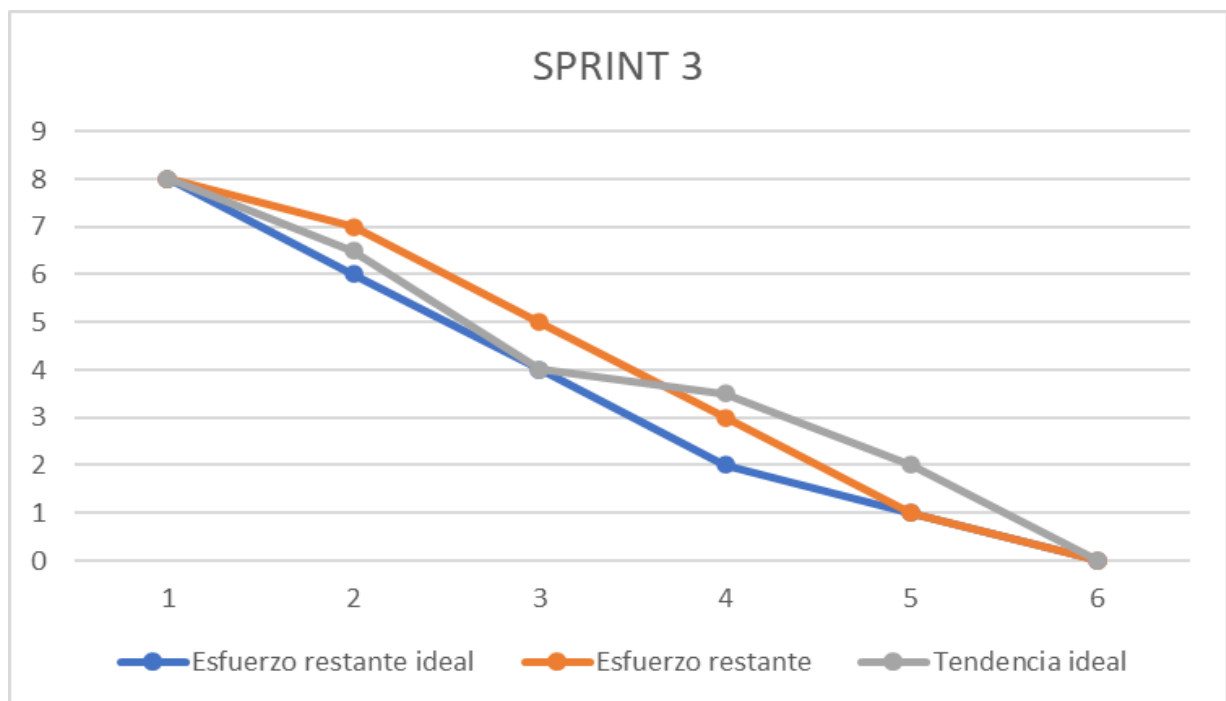
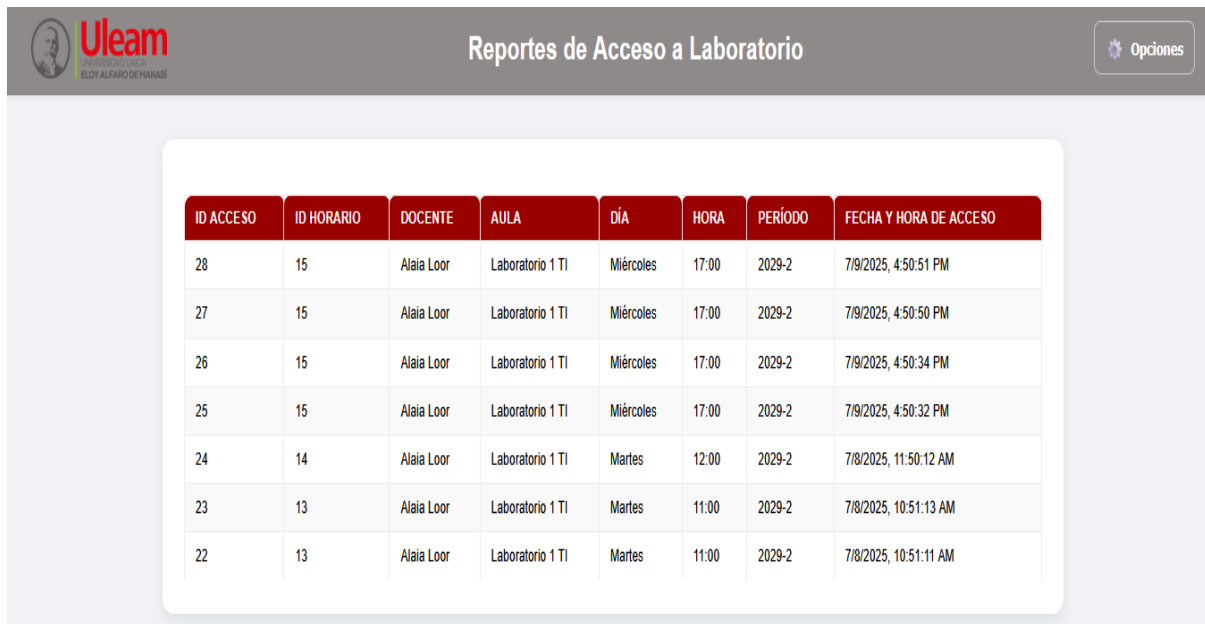


Ilustración 28. Release Burn-Down Sprint 3

4.4.9.2.5 Evidencias

Resumen:

Durante el Sprint 3 se desarrollaron las funcionalidades relacionadas con los reportes del sistema y la configuración avanzada. Se implementaron los reportes de acceso, gestión de aulas y periodos, así como la interfaz para modificar parámetros del sistema. Las actividades iniciaron con la planificación del módulo de reportes, seguido de su desarrollo, validación de alertas y pruebas generales. A continuación, se trabajó en la configuración del sistema, se dieron los últimos arreglos como comprobar el correcto funcionamiento de la cerradura y si el sistema no fallaba en diversos ambientes o con poca luz, dejando todo listo para la implantación final.



The screenshot displays a web application interface titled 'Reportes de Acceso a Laboratorio'. The header includes the Uleam logo (Universidad Eloy Alfaro de Manabí) on the left and an 'Opciones' button on the right. The main content area features a table with the following data:

ID ACCESO	ID HORARIO	DOCENTE	AULA	DÍA	HORA	PERÍODO	FECHA Y HORA DE ACCESO
28	15	Alaia Loor	Laboratorio 1 TI	Miércoles	17:00	2029-2	7/9/2025, 4:50:51 PM
27	15	Alaia Loor	Laboratorio 1 TI	Miércoles	17:00	2029-2	7/9/2025, 4:50:50 PM
26	15	Alaia Loor	Laboratorio 1 TI	Miércoles	17:00	2029-2	7/9/2025, 4:50:34 PM
25	15	Alaia Loor	Laboratorio 1 TI	Miércoles	17:00	2029-2	7/9/2025, 4:50:32 PM
24	14	Alaia Loor	Laboratorio 1 TI	Martes	12:00	2029-2	7/8/2025, 11:50:12 AM
23	13	Alaia Loor	Laboratorio 1 TI	Martes	11:00	2029-2	7/8/2025, 10:51:13 AM
22	13	Alaia Loor	Laboratorio 1 TI	Martes	11:00	2029-2	7/8/2025, 10:51:11 AM

Ilustración 29: Diseño de Lista de Reportes de Acceso

La imagen corresponde a al diseño de la lista plasmada en una tabla de los reportes de las personas que han accedido al laboratorio, mediante el uso del sistema de control de acceso propuesto. Que especifica la hora y la fecha de ingreso.

Lista de Aulas							Opciones
ID	NOMBRE	BLOQUE	PISO	OBSERVACIÓN	PIN ESP32	ACCIONES	
2	Laboratorio 1	A	P1	Solo ingresan 20 estudiantes	2	Modificar Eliminar	
1	Laboratorio 2 TI	A	P1	Solo ingresan 20 estudiantes	1	Modificar Eliminar	

Ilustración 30: Diseño de lista de Aulas

Esta es la visualización de la lista de las aulas que se plasman en unas tablas y es traída directamente de la base de datos y cuenta con dos acciones como son modificar y eliminar, todo esto administrado por el administrador de los laboratorios.

Lista de Períodos						Opciones
ID	NOMBRE	ACTIVO	AMPLITUD ANTES	AMPLITUD DESPUÉS	ACCIONES	
9	2029-2	Si	10	10	Modificar Eliminar	
8	2029-1	No	11	11	Modificar Eliminar	
7	2028-2	No	10	10	Modificar Eliminar	
6	2028-1	No	10	10	Modificar Eliminar	
5	2027-1	No	10	10	Modificar Eliminar	
4	2026-2	No	10	10	Modificar Eliminar	
1	2025-1	No	10	10	Modificar Eliminar	

Ilustración 31: Diseño de lista de Periodos

Esta imagen exhibe como es el panel de administración de los periodos electivos, con las opciones de modificar y eliminar, donde el administrador podrá ingresar cada periodo nuevo

de una manera fácil e intuitiva, para que esos datos sean usados posteriormente en otro formulario por el docente.

```
16
17 const API_BASE_URL_ACCESO = 'http://localhost/CDA-LAB/backend/api/accesso.php';
18 useEffect(() => {
19   const fetchReportes = async () => {
20     setLoading(true);
21     setError('');
22     try {
23       const response = await fetch(API_BASE_URL_ACCESO);
24       if (!response.ok) {
25         const errorData = await response.json();
26         throw new Error(errorData.message || `Error HTTP: ${response.status}`);
27       }
28       const data = await response.json();
29
30       // CORREGIDO: La clave en la respuesta del backend ahora es 'accesso'
31       if (data.success && Array.isArray(data.accesso)) {
32         setReportes(data.accesso); // Cambiado de data.acceso a data.accesso
33       } else if (data.success && data.message) {
34         setReportes([]);
35         setError(data.message);
36       } else {
37         setError(data.message || 'Formato de respuesta inesperado al cargar reportes.');
```

Ilustración 32: Código del listado de Reportes

Aquí se muestra el código para mostrar la lista de reportes, se hace un llamado al api para que consulte la lista de reportes y las traiga para posterior mente plasmarlas en un atable en la pantalla, de existir un error también será mostrado.

```

45 // Obtener todas las aulas
46 $sql = "SELECT idaulas, aul_nombre, aul_bloque, aul_piso, aul_observacion FROM aulas";
47 $result = $conn->query($sql);
48
49 if ($result) {
50     $aulas = [];
51     while ($row = $result->fetch_assoc()) {
52         $aulas[] = $row;
53     }
54     $response['success'] = true;
55     $response['aulas'] = $aulas;
56     $response['message'] = "Lista de aulas obtenida exitosamente.";
57 } else {
58     $response['message'] = "Error al obtener aulas de la base de datos.";
59     $status_code = 500; // Internal Server Error
60 }
61 }
62 break;

```

Ilustración 33: Código del listado de aulas

En esta evidencia se muestra el código que consulta de las aulas y plasma la lista de aulas en una lista desplegable. Estos datos son traídos de la base de datos hecha en mysql. Es una parte esencial dentro de las tareas de la historia de usuario 6 del Sprint 3.

```

47 // Verificar el token de seguridad
48 if (token == AUTH_TOKEN) {
49     int puertaID = puerta.toInt(); // Convierte el String "puerta" a un entero
50     int pinToActivate = -1; // Variable para almacenar el pin a activar
51     String salaName = "";
52
53     switch (puertaID) {
54         case 1: pinToActivate = RELAY_PIN_SALA1; salaName = "Sala 1"; break;
55         case 2: pinToActivate = RELAY_PIN_SALA2; salaName = "Sala 2"; break;
56         case 3: pinToActivate = RELAY_PIN_SALA3; salaName = "Sala 3"; break;
57         case 4: pinToActivate = RELAY_PIN_SALA4; salaName = "Sala 4"; break;
58         case 5: pinToActivate = RELAY_PIN_SALA5; salaName = "Sala 5"; break;
59         case 6: pinToActivate = RELAY_PIN_SALA6; salaName = "Sala 6"; break;
60         case 7: pinToActivate = RELAY_PIN_SALA7; salaName = "Sala 7"; break;
61         case 8: pinToActivate = RELAY_PIN_SALA8; salaName = "Sala 8"; break;
62         case 9: pinToActivate = RELAY_PIN_SALA9; salaName = "Sala 9"; break;
63         case 10: pinToActivate = RELAY_PIN_SALA10; salaName = "Sala 10"; break;
64         case 11: pinToActivate = RELAY_PIN_SALA11; salaName = "Sala 11"; break;
65         case 12: pinToActivate = RELAY_PIN_SALA12; salaName = "Sala 12"; break;
66         case 13: pinToActivate = RELAY_PIN_SALA13; salaName = "Sala 13"; break;
67         case 14: pinToActivate = RELAY_PIN_SALA14; salaName = "Sala 14"; break;
68         default:
69             responseMessage = "ID de puerta no reconocido. Use un numero del 1 al 14.";
70             statusCode = 400; // Bad Request
71             break;
72     }
73 }

```

Ilustración 34: Código C# en el ESP32, parte 1

En la función **handleAbrir()** que es función para manejar la petición de apertura de la cerradura, donde primero se verifica si existen los argumentos “token” y “puerta”, luego se verifica el valor del argumento “token” que sea igual al token de autorización, de ser correcto se activan los pines del relay de la “puerta” especificada en el argumento.

```
74     if (pinToActivate != -1) { // Si se encontró un pin válido
75         Serial.print("Recibido comando para abrir ");
76         Serial.println(salaName);
77         // Activar el relé
78         // NOTA: La mayoría de los módulos de relé con optoacoplador son 'activo en bajo' (LOW = ON, HIGH = OFF).
79         // Si el relé es 'activo en bajo', cambiar HIGH por LOW y LOW por HIGH.
80         digitalWrite(pinToActivate, HIGH); // Activa el relé (asumiendo activo en HIGH)
81         delay(TIEMPO_APERTURA_MS);        // Mantiene el relé activo por el tiempo definido
82         digitalWrite(pinToActivate, LOW);   // Desactiva el relé
83         responseMessage = salaName + " accionada.";
84         statusCode = 200; // OK
85     }
86 } else {
87     Serial.println("Intento de acceso con token invalido: " + token);
88 }
89 } else {
90     Serial.println("Comando incompleto. Faltan parametros 'puerta' o 'token'.");
91     responseMessage = "Comando incompleto. Uso: /abrir?puerta=X&token=TU_TOKEN";
92     statusCode = 400; // Bad Request
93 }
```

Ilustración 35: Código C# en el ESP32, parte 2

A continuación, se valida si existe algún pin valido, se da la instrucción para activar el relé, se mantiene el relé activo por el tiempo especificado y luego se desactiva el relé. En caso de que los argumentos no tengan valores se mostraran mensajes de error como “token invalido” o “comando incompleto”.

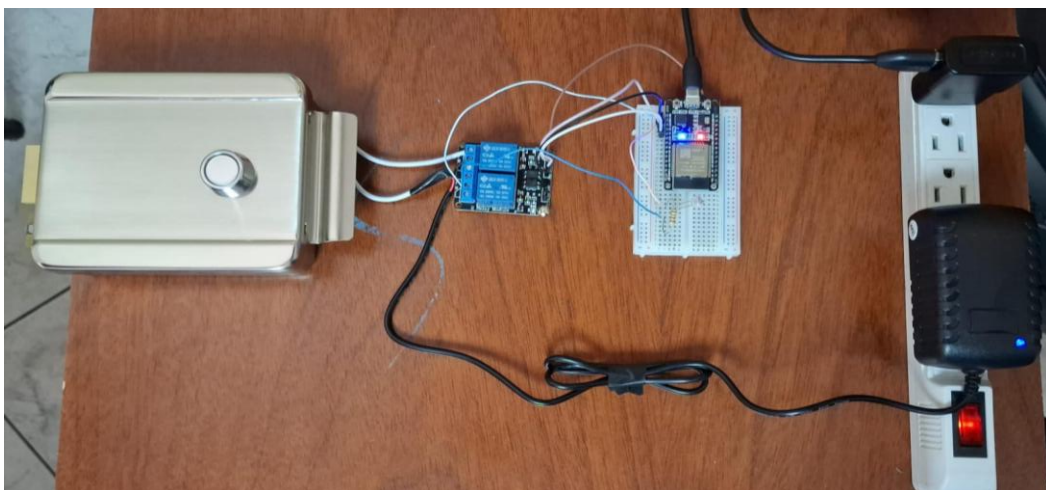


Ilustración 36: Pruebas físicas

Una vez hecho el reconocimiento facial en la aplicación web esta manda una señal (con un token y la puerta) a la placa ESP32 y este de ser valido el acceso manda la señal al Relé y esta manda la señal a la cerradura para que realice la apertura, la autorización se da si cumple con los requisitos como autenticación facial, el horario y el tiempo de amplitud.

4.4.9.3 Casos de Prueba de sistema

Durante el tercer sprint, se aplicaron casos de prueba para validar la funcionalidad del sistema desarrollado. Estos casos permitieron verificar que el sistema cumpla los criterios de aceptación definidos en las historias de usuario.

Caso de Prueba	Descripción	Entrada	Resultado Esperado	Resultado Real	Estado
CP-01	Verificar ingreso con rostro autorizado	Imagen de docente registrado	Acceso concedido	Acceso concedido	OK
CP-02	Verificar ingreso con rostro no registrado	Imagen desconocida	Acceso denegado	Acceso denegado	OK
CP-03	Registrar ingreso en base de datos	Imagen de rostro válido	Registro con fecha y hora	Registro correcto	OK
CP-04	Fallo de red durante verificación	Desconexión de ESP32	Mensaje de error y bloqueo de acceso	Sistema detectó error	OK
CP-05	Condiciones de baja luz	Imagen con baja iluminación	Reconocimiento aceptable	Precisión del 84%	OK

Tabla 32: Pruebas de sistema

4.4.9.4 Implementación

4.4.10 Mapa de navegación del sistema

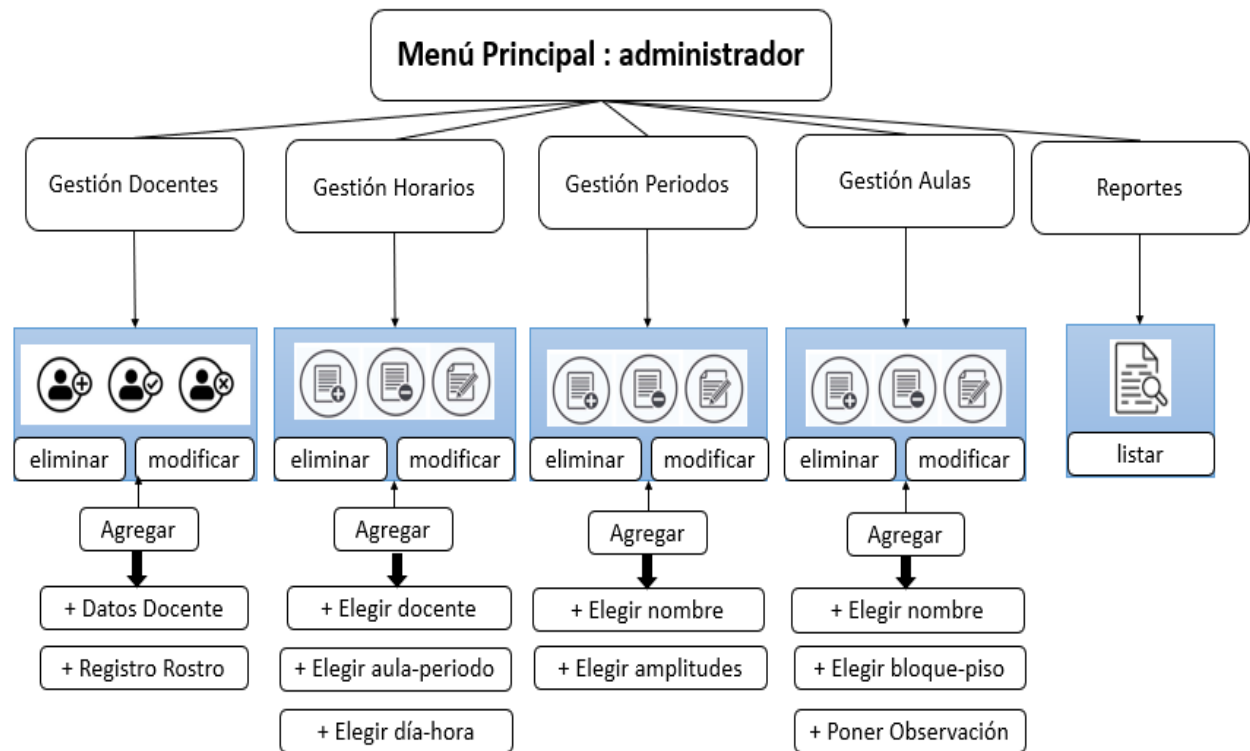


Ilustración 37: Mapa de navegación. Elaboración Propia

4.4.11 Proceso de pruebas

4.4.11.1 Prueba de caja negra

4.4.11.1.1 Formulario Login

Nombre del campo	Tipo de campo	Valor permitido	Observación
Usuario	Texto	Letras y/o números	Debe coincidir con el nombre de usuario válido
Contraseña	Contraseña	Mínimo 6 caracteres alfanum.	Debe coincidir con la clave almacenada

Ilustración 38: Prueba caja negra, formulario login

4.4.11.1.2 Formulario Registro Docente

Nombre del campo	Tipo de campo	Valor permitido	Observación
Cédula	Numérico (texto)	10 dígitos numéricos (Ecuador)	Validación obligatoria. Debe ser única y cumplir el formato nacional.
Nombre completo	Texto	Letras, máximo 100 caracteres	No debe contener números. Campo obligatorio.
Rol	Lista desplegable	“Docente”	Campo predefinido. No editable por el usuario en este formulario.
Correo electrónico	Texto (formato email)	Formato válido: usuario@dominio.com	Debe ser único. Se valida con expresión regular.
Imagen de rostro	Archivo (imagen)	JPG, JPEG o PNG. Tamaño máximo 5 MB	Imagen clara y frontal. Es obligatoria para el entrenamiento del sistema.
Contraseña	Contraseña	Mínimo 6 caracteres, letras y números	Se recomienda usar mayúsculas, minúsculas y números. Debe confirmarse aparte.

Ilustración 39: Prueba caja negra, formulario Registro docente

4.4.11.1.3 Formulario Horarios

Nombre del campo	Tipo de campo	Valor permitido	Observación
Docente	Lista desplegable	Nombres de docentes registrados previamente	Campo obligatorio. Se selecciona un docente ya registrado en el sistema.
Aula	Lista desplegable	"Laboratorio 1", "Laboratorio 2", etc. (según disponibilidad)	El aula debe estar habilitada para asignación de horarios.
Período	Lista desplegable	Ejemplo: “2025-2”, “2026-1”	Formato controlado. Puede validarse automáticamente por el sistema.
Día	Lista desplegable	Lunes, martes, miércoles, jueves, viernes, sábado	No se permite duplicar día y hora para el mismo docente en el mismo período.
Hora	Lista desplegable	Ejemplo: 08:00	No debe solaparse con otro horario.

Ilustración 40: Prueba caja negra, formularios horarios

4.4.11.1.4 Formulario Aulas

Nombre del campo	Tipo de campo	Valor permitido	Observación
Nombre	Texto	Letras y números (Ej: "Laboratorio 1", "Aula 202")	Campo obligatorio. Debe ser único. No se permite duplicación.
Bloque	Lista desplegable	Letras o códigos predefinidos	El valor debe estar en la lista de bloques registrados en la institución.
Piso	Lista desplegable	Planta baja o planta alta.	Elegir si el aula se encuentra en la planta baja o planta alta.
Observaciones	Texto libre	Cualquier texto alfanumérico (máx. 250 caracteres)	Opcional. Puede usarse para detalles como "Laboratorio con proyector".

Ilustración 41: Prueba caja negra, formulario aulas

4.4.11.1.5 Formulario Periodos

Nombre del campo	Tipo de campo	Valor permitido	Observación
Nombre	Texto	Letras, números y guiones (Ej: "2025-1", "marzo 2025")	Campo obligatorio. Debe ser único. No se permiten duplicados.
Amplitud antes	Numérico (entero)	Números enteros ≥ 0 (Ej: 5, 10, 15...)	Representa cuántos minutos antes del horario se permite ingresar.
Amplitud después	Numérico (entero)	Números enteros ≥ 0 (Ej: 5, 10, 20...)	Representa cuántos minutos después se sigue permitiendo el ingreso.

Ilustración 42: Prueba caja negra, formulario periodos

4.4.11.2 Prueba de caja blanca

4.4.11.2.1 Formulario Login

Nombre del campo	Tipo de campo	Valor permitido	Observación
Usuario	Variable string	"admin"	Verifica si existe y coincide con el sistema
Contraseña	Variable string	"admin123"	Validación estricta contra la base de datos

Ilustración 43: Prueba caja blanca, formulario login

4.4.11.2.2 Formulario Registro Docente

Nombre del campo	Tipo de campo	Valor permitido	Observación
Cédula	Variable tipo string (numérica)	10 dígitos numéricos (Ecuador)	Se verifica que: Tiene exactamente 10 dígitos
Nombre completo	Variable tipo string	Letras con espacios, longitud entre 3 y 100 caracteres	Se valida que no contenga números ni caracteres especiales. Obligatorio.
Rol	Variable tipo enum	“Docente” (en este formulario está fijo)	Valor fijo o preseleccionado en el código. Validación por lista.
Correo electrónico	Variable tipo string	Formato tipo email (usuario@dominio.com)	Validado con tipo email. Campo unique en la BD.
Imagen de rostro	Variable tipo archivo	Formatos: JPG, JPEG, PNG. Tamaño $\leq$ 5MB	Validación del tipo, resolución mínima y tamaño. Imagen obligatoria.
Contraseña	Variable tipo string	Mínimo 6 caracteres, debe contener letras y números	Se comprueba longitud y complejidad.

Ilustración 44: Prueba caja blanca, formulario Registro docente

4.4.11.2.3 Formulario Horarios

Nombre del campo	Tipo de campo	Valor permitido	Observación
Docente	Variable tipo string (ID o nombre)	Debe existir previamente en la base de datos de usuarios	Se valida con una consulta: SELECT * FROM docentes WHERE id = ?
Aula	Variable tipo string	Nombre válido de aula registrada	Se verifica existencia: SELECT * FROM aulas WHERE nombre = ?
Período	Variable tipo string o id	Formato válido (“2025-1”)	Validación que se seleccione una opción
Día	Variable tipo string	Lunes a sábado	Se controla que el valor esté dentro del conjunto permitido (enum)
Hora	Variables tipo string	Formato HH:MM (24h)	Se valida el rango horario y se revisa que no haya solapamientos

Ilustración 45: Prueba caja blanca, formularios horarios

4.4.11.2.4 Formulario Aulas

Nombre del campo	Tipo de campo	Valor permitido	Observación
Nombre	Variable tipo string	Letras y/o números, longitud 3–50 caracteres	Validación de unicidad: no debe repetirse con otra aula ya registrada.
Bloque	Variable tipo string	"Bloque A", "Bloque B", etc.	Validación contra lista predefinida de bloques disponibles.
Piso	Variable tipo int	Números enteros positivos (ej. 1, 2, 3...)	Se valida que no sea nulol.
Observaciones	Variable tipo string	Texto libre, hasta 250 caracteres	Campo opcional. Se valida longitud máxima.

Ilustración 46: Prueba caja blanca, formulario aulas

4.4.11.2.5 Formulario Periodos

Nombre del campo	Tipo de campo	Valor permitido	Observación
Nombre	Variable tipo string	Letras, números, guiones (Ej: "2025-1", "marzo 2025")	Validación de unicidad: no debe estar ya registrado. Longitud entre 4 y 20 caracteres.
Amplitud antes	Variable tipo int	Números enteros positivos (Ej: 5, 10, 15...)	No debe ser negativo.
Amplitud después	Variable tipo int	Números enteros positivos (Ej: 5, 10, 20...)	No debe ser negativo.

Ilustración 47: Prueba caja blanca, formulario periodos

CAPÍTULO V

5. EVALUACIÓN DE RESULTADOS

5.1 Introducción

En este capítulo se presenta la evaluación del sistema informático con redes neuronales desarrollado para mejorar la seguridad física del Laboratorio de Cómputo 1 de la ULEAM Extensión El Carmen. Se detallan los mecanismos utilizados para medir la eficacia del sistema, considerando los criterios definidos desde la fase de planificación, así como los resultados obtenidos tras su implementación y pruebas de funcionamiento. Esta evaluación permite comprobar el cumplimiento de los objetivos específicos y validar la viabilidad de la solución propuesta para resolver los problemas identificados en el diagnóstico inicial.

5.2 Presentación y monitoreo de resultados

5.2.1 Problemas detectados encuestas y entrevistas (El problema)

La recolección de datos se realizó mediante dos instrumentos: una encuesta con preguntas cerradas dirigida a los docentes que utilizan el laboratorio, y una entrevista semiestructurada aplicada al encargado técnico del mismo. Ambos instrumentos evaluaron aspectos como la seguridad, la urgencia de un sistema de acceso automatizado, y la aceptación del reconocimiento facial como solución tecnológica. A continuación, se presentan algunas tablas representativas con los resultados obtenidos y su análisis:

Opción de respuesta	Porcentaje
Frecuente	67%
Ocasional	22%
Rara vez	11%
Nunca	0%

Tabla 33: Frecuencia de problemas por ausencia del conserje

Más de dos tercios de los docentes afirmaron que frecuentemente encuentran el laboratorio cerrado por ausencia del conserje. Esto demuestra una dependencia ineficiente del personal manual de acceso.

Consecuencia	Porcentaje de menciones
Ingreso no autorizado	80%
Robo o daño	77%
Retrasos en clases	65%
Falta de registros del uso del laboratorio	88%

Tabla 34: Consecuencias de no tener control de acceso

Las consecuencias están directamente relacionadas con las causas del problema inicial. Estos resultados evidencian la necesidad urgente de un sistema de control automatizado y confiable.

Opción	Porcentaje
Ideal	44%
Muy útil	33%
Moderadamente útil	22%
Poco útil / No útil	0%

Tabla 35: Opinión sobre reconocimiento facial como solución

Existe una aceptación generalizada hacia la tecnología propuesta. No se registraron respuestas negativas, lo que refleja la confianza del personal académico en la aplicación del sistema de reconocimiento facial basado en IA.

5.2.2 Planificación de la evaluación

La evaluación del sistema se planificó tomando como base los criterios: funcionalidad, usabilidad y eficiencia. Los indicadores utilizados para la medición fueron definidos de la siguiente manera:

Indicador	Descripción	Método de Medición	Meta esperada
Tiempo promedio de autenticación	Tiempo en segundos que tarda el sistema en identificar al usuario	Cronometrado durante pruebas	≤ 8 segundos
Precisión del reconocimiento	Porcentaje de accesos exitosos en comparación con el total de intentos	Registro automático del sistema	$\geq 80\%$

Indicador	Descripción	Método de Medición	Meta esperada
Satisfacción del usuario	Nivel de aceptación del sistema por parte de los usuarios	Encuesta	$\geq 80\%$ positiva
Reducción de accesos no autorizados	Disminución de ingresos de personas no autorizadas	Comparación antes y después	$\geq 70\%$ reducción

Tabla 36: Indicadores definidos para la evaluación del sistema

5.2.3 Ejecución del monitoreo

5.2.3.1 Medición de tiempos

Durante el monitoreo, se implementó el sistema en condiciones reales en el laboratorio. Se realizaron pruebas con 9 docentes. Se midieron los tiempos de autenticación, se monitoreó la precisión del sistema, y se aplicaron encuestas de satisfacción. Los resultados fueron los siguientes:

Prueba realizada	Resultado obtenido	Valor esperado	Cumplimiento
Tiempo promedio de autenticación	5 segundos	≤ 8 segundos	✓ Cumplido
Precisión del reconocimiento facial	84%	$\geq 80\%$	✓ Cumplido
Reducción de accesos no autorizados	78% de reducción	$\geq 70\%$	✓ Cumplido
Nivel de satisfacción de los usuarios	88% de aprobación	$\geq 80\%$	✓ Cumplido

Tabla 37: Resultados obtenidos en las pruebas funcionales del sistema

Ítem evaluado	Muy de acuerdo	De acuerdo	En desacuerdo	Total positivo
El sistema es fácil de usar	5	3	1	88.9%
El reconocimiento facial es confiable	4	4	1	88.9%
Ha mejorado la organización del laboratorio	6	3	0	100%
Reduce la pérdida de tiempo por llaves	7	2	0	100%

Me gustaría que se aplique en otros laboratorios	6	2	1	88.9%
--	---	---	---	-------

Tabla 38: Resultados de la encuesta de satisfacción (resumen de docentes)

5.2.3.2 Monitoreo de Resultados: Registrar Docente

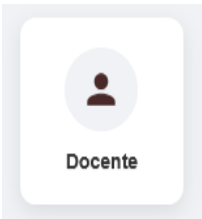
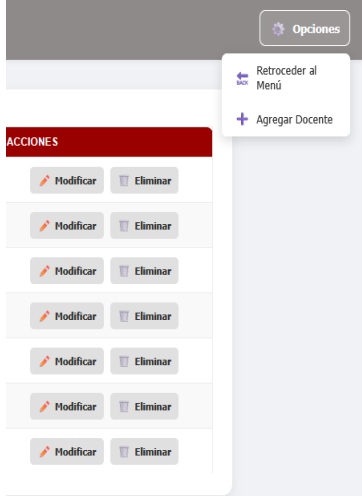
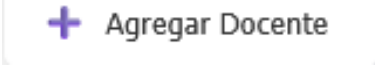
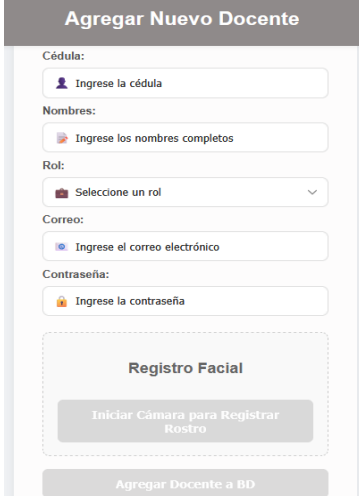
Paso 1	Paso 2	Paso 3
		
Primeramente, para realizar un registro de docente, el administrador deberá ingresar a la aplicación usando su usuario (cédula) y su contraseña personal.	Ya permitido el ingreso, se muestra el menú de inicio del sistema con todas las opciones disponibles en el rol de administrador.	Elegir la opción llamada "gestión de docentes"
Paso 1	Paso 2	Paso 3
		
La pestaña siguiente muestra la lista de docentes registrados y las opciones de agregar, modificar y eliminar.	Elegir la opción "agregar usuario"	Formulario de ingreso de docente y registro de rostro a docente.

Tabla 39: Monitoreo registro de docente

5.2.3.3 Pruebas de identificación facial

```
Cargando rostros conocidos...
Cargado: Anthony (Cédula: 1313528398)
Cargado: Silvana Daza (Cédula: 1317972253)
Cargado: Alaia Loor (Cédula: 1323540953)
Cargado: MORA MARCILLO ALEX BLADIMIR (Cédula: 1717955684)
Cargados 4 rostros conocidos.
* Serving Flask app 'app'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a produc
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5000
* Running on http://192.168.1.123:5000
Press CTRL+C to quit
Iniciando reconocimiento automático desde la cámara IP con detección de objetos y distancia..
DEBUG: ¡Ventana de acceso ACTIVA para 1323540953! De 20:31:00 a 21:01:00
DEBUG: ¡Ventana de acceso ACTIVA para 1323540953! De 20:31:00 a 21:01:00
DEBUG: Rostro detectado a 1.44 metros. Rango requerido: 1.4-1.9m.
Rostro detectado: Alaia Loor (Cédula: 1323540953)
Horario válido para Alaia Loor en el aula Laboratorio 1 TI. Mirada sostenida por
.
DEBUG: Intentando enviar comando de apertura a ESP32 para el pin ID: 1.
Rostro detectado: Silvana Daza (Cédula: 1317972253)
No hay horario válido para Silvana Daza (Cédula: 1317972253) en este momento.
DEBUG: ¡Ventana de acceso ACTIVA para 1323540953! De 20:31:00 a 21:01:00
DEBUG: ¡Ventana de acceso ACTIVA para 1323540953! De 20:31:00 a 21:01:00
DEBUG: ¡Ventana de acceso ACTIVA para 1323540953! De 20:31:00 a 21:01:00
DEBUG: ¡Ventana de acceso ACTIVA para 1323540953! De 20:31:00 a 21:01:00
DEBUG: ¡Ventana de acceso ACTIVA para 1323540953! De 20:31:00 a 21:01:00
DEBUG: Rostro detectado a 1.76 metros. Rango requerido: 1.4-1.9m.
Rostro detectado pero no reconocido.
```

Ilustración 48: Modelo de reconocimiento

Mediante datos emitidos por el sistema en consola al momento de que el docente trata de identificar su rostro en la cámara IP se pueden observar mensajes de registros exitosos y validación de horarios y mensajes de rostros detectados y no reconocidos por el sistema.

5.3 Interpretación objetiva

La información obtenida revela una clara correlación entre las causas detectadas inicialmente y los efectos negativos en la operatividad del laboratorio. Los usuarios encuestados que fueron los docentes veían precaria la forma de buscar a la persona encargada para que abra el laboratorio, lo que muchas veces terminaba por hacer perder tiempo y cuando eran exámenes el tiempo es fundamental. Muchos otros problemas que son arrastrados con esto, ya que no siempre se cerraban los laboratorios al finalizar y eso daba entrada a daño de dispositivos o robos.

Los resultados que dieron las pruebas del sistema lograron constatar que la identificación facial toma un tiempo promedio de 5 segundos, lo cual es un poco más bajo de lo que se planteó en un inicio que eran 8 segundos. También la precisión se esperaba que para ser viable sea del 80% pero con las pruebas dio un 94% lo que representa una alta eficiencia.

De la vista de los encuestados más de la mitad de los mismo vieron como positiva la implementación y el entrevistado lo vio como una solución innovadora, ya con las pruebas los docentes destacaron su facilidad de uso y ahorro de tiempo, a la forma anterior que constaba de buscar al conserje y abrir el laboratorio. Muchos vieron bien la implementación y creen que es necesarios en más laboratorios como en aulas con los estudiantes, porque esos problemas no son exclusivos del laboratorio.

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Se puede concluir que el proyecto logró implementar con éxito un sistema informático basado en redes neuronales para mejorar la seguridad física en el Laboratorio de Cómputo 1 de la ULEAM Extensión El Carmen. El sistema automatizó el control de acceso mediante reconocimiento facial, alcanzando una precisión del 84%, superando la meta del 80%. Esta automatización redujo significativamente los accesos no autorizados en un 78%, abordando los problemas identificados de dependencia del acceso manual y la falta de registros de entrada y salida.
- La investigación bibliográfica fue un pilar fundamental para la aplicación de este sistema en el laboratorio, ya que las bases teóricas de temas y proyectos relacionados a este fueron un incentivo al desarrollo de este proyecto, como dieron distintos puntos de vista de las diferentes herramientas que se pueden usar para realizar este tipo de proyectos.
- Las encuestas y entrevistas realizadas a docentes y el administrador respectivamente, proporcionaron datos cualitativos y cuantitativos que proporcionó información crítica de los problemas que se presentan en el laboratorio y la necesidad urgente de la implementación de un sistema con control de acceso.
- El sistema diseñado bajo la metodología de desarrollo de mediano plazo scrum, permitió una gestión de los cambios oportuna debido a las reuniones diarias y agilidad de desarrollo por el fraccionamiento de las tareas. Las 3 iteraciones realizadas dividieron muy bien el tiempo y concordó con el tiempo de implementación y presentación.
- Las pruebas realizadas en ambientes reales con los docentes fueron de resultados muy buenos y superados a los esperados como el tiempo de respuesta promedio del sistema fue de 5 segundos, cuando se esperaba 8 segundos y la precisión fue de un 14% más a la esperada de 80%.
- Los problemas identificados como los robos constantes debido a los accesos indebidos se espera reduzcan al ya no contar con este tipo de accesos ya que el sistema solo permite el acceso a rostros registrados y durante los horarios permitidos por el sistema,

ya que a su vez este cumple con reportes de ingreso. En futuras actualizaciones del sistema se buscará, hacerlo global y que identifique el rol con el rostro, además de manejar el sistema de asistencias de alumnos.

- El uso de las redes neuronales junto con dispositivos físicos como es la placa esp32 es símbolo de avance e innovación en la universidad Uleam, pero es solo el punto de partida para futuros proyectos inspirados en esta hacia el crecimiento tecnológico en la institución.

6.2 Recomendaciones

- Dada la efectividad del sistema en el Laboratorio 1 (88.9% de aprobación para una aplicación más amplia), se recomienda extender su implementación a otros laboratorios de la ULEAM Extensión El Carmen. Esto estandarizaría el control de acceso en la institución, mejorando la seguridad y la gestión de recursos.
- Para mejorar la precisión a $> 90\%$, se debe actualizar periódicamente el conjunto de datos de reconocimiento facial en diferentes ambientes y distintas condiciones de iluminación, también se debe corregir errores que aparecieron en el periodo de pruebas como los ingresos con fotografías o videos de las personas autorizadas. Especialmente en escenarios con iluminación pobre, también nunca olvidar los mantenimientos regulares al hardware y software del sistema.
- Es recomendable hacer capacitación constante por la rotación de docentes y administradores, además de campañas de concienciación para el cuidado de estas herramientas, en especial la no manipulación de terceros o golpes que puedan resultar en evitar su función.
- Por otro lado, se recomienda mejorar el consumo energético de estas herramientas, dando pie a códigos más optimizados y tiempos más cortos de procesamiento, uso de energías alternativas como la solar. Además de incentivar a la no contaminación y reciclaje de dispositivos que toque remplazar.
- Realizar estudios de seguimiento para evaluar el rendimiento del sistema a largo plazo y recopilar retroalimentación de los usuarios tras un uso prolongado. Investigar la integración de análisis predictivo para anticipar riesgos de seguridad, alineándose con la tendencia hacia modelos de seguridad predictiva señalada en el marco teórico.

BIBLIOGRAFÍA

Batarse Cardenas, E. (20 de Junio de 2019). *reparaciondecomputadora*. Obtenido de reparaciondecomputadora: <https://www.reparaciondecomputadora.mx/que-es-un-software>

López Querol, J., Campos Monge, E., & Campos Monge, M. (2023). *Algoritmia y Base de Datos*. RA-MA. Obtenido de [https://books.google.com.ec/books?id=1VW6EAAAQBAJ&pg=PA7&dq=Estructura +F%C3%ADsica:+CPU+Memoria+Interna+y+Externa+Unidades+de+almacenamiento&hl=es-419&newbks=1&newbks_redir=0&sa=X&ved=2ahUKEwjO79OxwYKKAxVVVTA BHZ52FAAQ6AF6BAgMEAI#v=onepage&q=Estructura%20F](https://books.google.com.ec/books?id=1VW6EAAAQBAJ&pg=PA7&dq=Estructura+F%C3%ADsica:+CPU+Memoria+Interna+y+Externa+Unidades+de+almacenamiento&hl=es-419&newbks=1&newbks_redir=0&sa=X&ved=2ahUKEwjO79OxwYKKAxVVVTA BHZ52FAAQ6AF6BAgMEAI#v=onepage&q=Estructura%20F)

Alegre Ramos, M. (2023). *Sistemas informáticos*. Ediciones Paraninfo, S.A. Obtenido de https://www.google.com.ec/books/edition/Sistemas_inform%C3%A1ticos/kR3JEAA AQB AJ?hl=es-419&gbpv=1

Alegsa, L. (09 de Julio de 2023). *Alegsa*. Obtenido de Alegsa: https://www.alegsa.com.ar/Dic/sistema_transaccional.php#gsc.tab=0

Algre Ramos, M. (2023). *Sistemas informáticos*. Paraninfo. Obtenido de https://books.google.com.ec/books?id=kR3JEAAAQBAJ&source=gbs_navlinks_s

Allen Ramirez, Y., & Tucker Knigh, L. (2020). *Sistema de reconocimiento facial de control de entrada y salida de los empleados de la universidad BICU recinto Bluefields, primer semestre del año 2020*. Bluefields Indian & Caribbean University (BICU). Obtenido de http://repositorio.bicu.edu.ni/1243/1/Proyecto%20Final%20Rev%20Yelsi%20y%20L orvic_1.pdf

Arias, J. (2021). *Diseño y Metodología de la Investigación*. Enfoques Consulting EIRL. Obtenido de https://apps.utel.edu.mx/recursos/files/r161r/w26022w/Arias_S2.pdf

- Bourgeat, J. (12 de Julio de 2024). *Linkedin*. Obtenido de *Linkedin*:
<https://es.linkedin.com/pulse/las-mejores-pr%C3%A1cticas-en-seguridad-f%C3%ADsica-para-joseph-bourgeat-kmyie>
- Buñay Marcatoma, R. (2022). *Diseño e Implementación de un Sistema Informático para el Registro de Mantenimiento de los Equipos de Cómputo del GAD Municipal de Alausí*. Instituto Superior Universitario “San Gabriel”. Obtenido de
<https://www.sangabrielriobamba.edu.ec/tesis/sistemas/tesis34.pdf>
- Calles Carrasco, M. (2019). *istema Informático de Reconocimiento Facial para el Registro y Control de Asistencia de los Socios de la Cooperativa de Taxis y Camionetas Puyo*. Universidad Regional Autonoma de los Andes. Obtenido de
<https://dspace.uniandes.edu.ec/bitstream/123456789/9765/1/PIUPSIS0004-2019.pdf>
- Campoverde, J., & Mendieta, L. (2023). *Aplicación de reconocimiento facial para el control de asistencia de estudiantes mediante modelos de visión artificial*. Universidad Técnica de Machala. Obtenido de <http://repositorio.utmachala.edu.ec/handle/48000/22031>
- Cardoso, J. M., Cardoso, S. L., & Morales, M. M. (20 de Julio de 2024). *BASE DE Datos*. UCE. Obtenido de Skyone: <https://www.studocu.com/ec/document/universidad-central-del-ecuador/base-de-datos/libro-base-de-datos-version-mayo-2020/30002464>
- Castañeda Sánchez, W., Polo Escobar, B., & Huincho, F. (2024). *Redes neuronales artificiales: una medición de aprendizajes de pronósticos como demanda potencial*. Universidad, Ciencia y Tecnología. Obtenido de https://ve.scielo.org/scielo.php?pid=S1316-48212023000100051&script=sci_arttext
- Checa Cabrera, M. A., Díaz Ayala, J. O., Jácome Ayala, P. J., Montalvo Loza, C. H., Montenegro Rivera, A. M., Narváez Quinteros, J. L., & Valladares Correa, G. G. (2025). *SCRUM: Guía didáctica*. ALUMNI. Obtenido de
<https://alumnieditora.com/omp/index.php/home/catalog/download/11/14/39?inline=1>

- Cruz , S., & Gunar , E. (2022). *Sistema de reconocimiento facial para el control de ingreso de personas a la UNJBG*. Universidad Nacional Jorge Basadre Grohmann. Obtenido de 2022_cruz_sucasaca_ge_informatica.pdf (6.23 MB)
- De Buen, M. (26 de Enero de 2024). *Mopecsecurity*. Obtenido de Mopecsecurity: <https://mopecsecurity.com/tendencias-de-seguridad-fisica-para-2024/>
- Delgado, J. (29 de Agosto de 2015). *Gestiopolis*. Obtenido de Gestiopolis: <https://www.gestiopolis.com/sistemas-transaccionales-sistemas-de-apoyo-a-las-decisiones-y-sistemas-estrategicos/>
- Delgado, J. (29 de Agosto de 2015). *Gestiopolis*. Obtenido de Gestiopolis: <https://www.gestiopolis.com/sistemas-transaccionales-sistemas-de-apoyo-a-las-decisiones-y-sistemas-estrategicos>
- Díaz, L., Torruco, U., Martínez, M., & Varela, M. (2013). *La entrevista, recurso flexible y dinámico*. doi:<https://www.scielo.org.mx/pdf/iem/v2n7/v2n7a9.pdf>
- Diccionario De Informática Y Tecnología. (29 de Agosto de 2015). *Gestiopolis*. Obtenido de Gestiopolis: <https://www.gestiopolis.com/sistemas-transaccionales-sistemas-de-apoyo-a-las-decisiones-y-sistemas-estrategicos/>
- Equipo de Imagina. (24 de Septiembre de 2024). *Imagina*. Obtenido de Imagina: <https://imaginaformacion.com/tutoriales/que-es-la-metodologia-scrum>
- Fennelly, L. J. (2016). *Effective Physical Security: Fifth Edition*. Obtenido de https://www.researchgate.net/publication/319253656_Effective_Physical_Security_Fifth_Edition
- Fennelly, L., & Perry, M. (2017). *Physical Security: 150 Things You Should Know, Second Edition is a useful reference for those at any stage of their security career*. Butterworth-Heinemann. doi:<https://doi.org/10.1016/C2015-0-05410-7>

- Floyd, T. L. (25 de Marzo de 2006). *Fundamentos de sistemas digitales*. Obtenido de InformatECDigital: <https://electronicautm.wordpress.com/wp-content/uploads/2014/06/fundamentos-de-sistemas-digitales-floyd-9ed.pdf>
- Guanoluisa Almache, F., Bosquez Remache, J., Esparza Pijal, S., & Benavides. (2023). Apuntes sobre los métodos de investigación y técnicas de recolección de datos en la investigación jurídica. *Bibliotecas. Anales de Investigacion*, 17. Obtenido de https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://dialnet.unirioja.es/descarga/articulo/9285926.pdf&ved=2ahUKEwj9sdn0ubCOAxUfRDABHdOKA8gQFnoECBgQAQ&usg=AOvVaw268IfeM_Sm_PF2zGviYKvg
- Heras Aranzana, P. (2020). *Predicción de la Radiación mediante el Uso de una Red Neuronal Recurrente*. Universidad Politécnica de Madrid. Obtenido de https://oa.upm.es/63345/1/TFG_PABLO_HERAS_ARANZANA.pdf
- Hernández, R., & Mendoza, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta*. Editorial Mc Graw Hill Education. doi:<https://doi.org/10.22201/fesc.20072236e.2019.10.18.6>
- Hostingplus. (23 de Noviembre de 2021). *Hostingplus*. Obtenido de Hostingplus: <https://www.hostingplus.pe/blog/metodologia-de-espiral-fases-y-desarrollo/>
- Huambachano , J. (25 de Septiembre de 2017). *Scrum.org*. Obtenido de Scrum.org: <https://www.scrum.org/resources/blog/que-es-scrum>
- Huérffano Lenis, C. (2020). *Identificación Predictiva de Fallos POS A Través del Uso de Algoritmos de Aprendizaje Automático*. Universidad De Bogotá Jorge Tadeo Lozano. Obtenido de <https://expeditiorepositorio.utadeo.edu.co/bitstream/handle/20.500.12010/10167/Trabajo%20d%20grado.pdf?sequence=1&isAllowed=y>
- Huet, P. (13 de Abril de 2023). *Openwebinars*. Obtenido de Openwebinars: <https://openwebinars.net/blog/que-son-las-redes-neuronales-y-sus-aplicaciones/>

INCIBE. (29 de Agosto de 2023). *INCIBE*. Obtenido de INCIBE:
<https://www.incibe.es/empresas/blog/la-ciberseguridad-desde-los-inicios-evolucion-de-la-seguridad>

Jean, R. C., Christian, C. R., Luis, A. L., & Alberto, M. d. (2023). Sistema de reconocimiento facial para el control de accesos mediante. *Revista Innovación y Software*, 4(1), 24-36. Obtenido de <https://revistas.ulasalle.edu.pe/innosoft>

Linares, a. A., Sevillano, R. P., & Viejó, o. L. (2023). Importancia de los sistemas de información para. *Ciencia Digital*, 15. Obtenido de <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://cienciadigital.org/revistacienciadigital2/index.php/ConcienciaDigital/article/download/2442/5958/&ved=2ahUKEwiM98efhoCNAxU-RTABHQNpBl8QFnoECDkQAQ&usg=AOvVaw3zXvPTplqGMuI2YW9cXktV>

Madeo, D. (16 de Agosto de 2024). *Revistainnovacion.com*. Obtenido de [Revistainnovacion.com:
https://revistainnovacion.com/nota/12387/evolucion_de_la_seguridad_del_pasado_al_futuro/](https://revistainnovacion.com/nota/12387/evolucion_de_la_seguridad_del_pasado_al_futuro/)

Mancuzo, G. (13 de Mayo de 2021). *ComparaSoftware*. Obtenido de [ComparaSoftware:
https://blog.comparasoftware.com/ventajas-de-la-metodologia-en-espiral/](https://blog.comparasoftware.com/ventajas-de-la-metodologia-en-espiral/)

Martins, J. (15 de Febrero de 2024). *Asana*. Obtenido de [Asana:
https://asana.com/es/resources/what-is-scrum](https://asana.com/es/resources/what-is-scrum)

Matich, D. (2001). *Redes Neuronales: Conceptos Básicos y Aplicaciones*. Universidad Tecnológica Nacional. Obtenido de https://www.firro.utn.edu.ar/repositorio/catedras/quimica/5_anio/orientadora1/monografias/matich-redesneuronales.pdf

Melara, M. (27 de Julio de 2022). *Soyadministrador*. Obtenido de [Soyadministrador:
https://soyadministrador.net/sistema-de-informacion-gerencial/](https://soyadministrador.net/sistema-de-informacion-gerencial/)

- Merchant, S. (14 de Junio de 2024). *Alumio*. Obtenido de Alumio: <https://www.alumio.com/es/blog/system-integration-methods-tools-and-benefits>
- Montilla García, H. (2022). *Algoritmo de aprendizaje automático supervisado en la predicción del rendimiento académico*. Universidad Nacional de San Martín. Obtenido de <https://tesis.unsm.edu.pe/bitstream/11458/4667/1/Maest.%20Tec.%20Informaci%C3%B3n%20-%20Henry%20Montilla%20Garc%C3%ada.pdf>
- Moreno Pérez, J. (2012). *Sistemas informáticos y redes locales*. Ra-Ma. Obtenido de https://books.google.com.ec/books?id=Z6a6EAAQBAJ&pg=PA1&dq=Sistemas+Inform%C3%A1ticos+de+Juan+Carlos+P%C3%A9rez&hl=es-419&newbks=1&newbks_redir=0&sa=X&ved=2ahUKEwj9qcX-reKJAxWNRjABHUpI BUYQuwV6BAgFEAc#v=onepage&q=Sistemas%20Inform%C3%A1ticos%20de%20Juan%2
- Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2013). *Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis*. Ediciones de la U. Obtenido de <https://escuelitamedica.com/2024/10/24/metodologia-de-la-investigacion/>
- Olavsrud, T. (30 de Enero de 2024). *CIO*. Obtenido de CIO: <https://www.cio.com/article/1314134/sistemas-de-apoyo-a-la-toma-de-decisiones-la-herramienta-clave-para-el-analisis-de-datos-empresariales.html>
- Pardo, D. (28 de Febrero de 2024). *Pandorafms*. Obtenido de Pandorafms: <https://pandorafms.com/blog/es/historia-de-la-informatica/>
- Pereyra, L. (2020). *Metodología de la investigación*. Klik. Obtenido de https://www.google.com.ec/books/edition/Metodolog%C3%ADa_de_la_investigaci%C3%B3n/x9s6EAAQBAJ?hl=es&gbpv=0
- Ramanpreet, K., Dusan, G., & Klobucar, T. (2023). *Artificial intelligence for cybersecurity: Literature review and future*. Elsevier.

- Ramirez , M., Rivas , E., & Cardona , C. (2019). *El estudio de caso como estrategia metodológica*. Espacios. Obtenido de <https://www.revistaespacios.com/a19v40n23/a19v40n23p30.pdf>
- Raya Cabrera, J. (2011). *Sistemas Informáticos*. Ra-Ma. Obtenido de <https://books.google.com.ec/books?hl=es&lr=&id=36W6EAAAQBAJ&oi=fnd&pg=PP2&dq=sistemas+inform%C3%A1ticos&ots=M4nWR2FiGb&sig=PLzE3LaOKNVruXm-2sbenhBHq0M#v=onepage&q=sistemas%20inform%C3%A1ticos&f=false>
- Recla. (19 de Diciembre de 2023). *Recla*. Obtenido de Recla: <https://recla.org/blog/modelo-spiral/>
- Reina, S. (2014). *La seguridad disuasiva como método de disminución de riesgos de seguridad física en las instituciones de educación superior en Colombia*. Universidad Militar Nueva Granada. Obtenido de <https://repository.unimilitar.edu.co/server/api/core/bitstreams/6ce713ca-2cb0-4bfb-b011-68bf2f952e06/content>
- Revilla , D., Degola, M., Poma, L., Trelles , L., & Tafur , R. (2020). *Los métodos de investigación para la elaboración de las tesis de maestría en educación*. Facultad de Educacion. Obtenido de <https://posgrado.pucp.edu.pe/wp-content/uploads/2021/10/libro-los-metodos-de-investigacion-maestria-2020-botones-2.pdf>
- Rodríguez, Y. (2020). *Metodología de la investigación*. Klik. Obtenido de https://www.google.com.ec/books/edition/Metodolog%C3%ADa_de_la_investigaci%C3%B3n/x9s6EAAAQBAJ?hl=es&gbpv=0
- Rouse, M. (28 de Marzo de 2024). *Techopedia*. Obtenido de Techopedia: <https://www.techopedia.com/es/definicion/inteligencia-artificial-neurona>
- San Martín, X. (09 de Febrero de 2024). *Aodatacloud*. Obtenido de Aodatacloud: <https://aodatacloud.es/blog/hardware-concepto-tipos-y-componentes>

- Santillán, J. V. (2016). *Informatica*. Grupo Editorial Patria. Obtenido de <https://biblioteca.ceves.edu.mx/themes/default/resources/js/pdfjs/web/viewer.html?file=/eBooks/2020/December/5fe60bdde5262/Inform%C3%A1tica%201,%202da%20Edici%C3%B3n%20-%20Jorge%20Vasconcelos%20Santill%C3%A1n-22.pdf>
- Schmidt, C. (18 de Noviembre de 2020). *Guía completa A+ de hardware y software de TI*. Obtenido de Profesionalreview: https://dokumen-pub.translate.google.com/complete-a-guide-to-it-hardware-and-software-aa-comptia-a-core-1-220-1001-amp-comptia-a-core-2-220-1002-textbook-8thnbsped-978-0-7897-6050-0.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc#Cheryl+Schmidt
- SCRUMstudy. (03 de Diciembre de 2017). *Una guía integral para la entrega de proyectos utilizando Scrum*. VMedu. Obtenido de Iebs: <https://primeconsultores.com.pe/wp-content/uploads/2021/02/SCRUMstudy-SBOK-Guide-3rd-edition-Spanish.pdf>
- Simona Bernardi, L. D. (21 de Marzo de 2020). *Sistemas de informacion para la direccion*. Centro Universitario de la Defensa. Obtenido de IBM: <https://zagan.unizar.es/record/88358/files/BOOK-2020-024.pdf>
- Stockholm. (07 de Septiembre de 2023). *Linkedin*. Obtenido de Linkedin: <https://es.linkedin.com/pulse/medidas-de-seguridad-f%C3%ADsica-implementaci%C3%B3n-know-how-plus>
- Sutherland, J. (2016). *SCRUM. The Art of Doing Twice the Work in Half the Time*. Editorial Océano de México, S.A. Obtenido de <https://assets.super.so/e745dfd7-232e-47c1-a806-753f45b941ba/files/e5c9770b-4e7d-4df6-880f-a9a15ace7b51.pdf>
- Sy Corvo, H. (23 de Mayo de 2021). *Lifeder*. Obtenido de Lifeder: <https://www.lifeder.com/modelo-espiral/>
- Templo de Kendall. (23 de Julio de 2024). *Securetrust*. Obtenido de Securetrust: <https://securetrust.io/blog/automation-in-siem-reducing-human-error-and-response-times/>

- Velasco Rebolledo, J. (2024). *Machine learning*. Díaz de Santos. Obtenido de https://books.google.com.ec/books?id=eMYpEQAAQBAJ&pg=PA93&dq=Redes+Neuronales+Convolucionales+para+el+Reconocimiento+Facial&hl=es&newbks=1&newbks_redir=0&sa=X&ved=2ahUKewjW6sOAtuKJAxUxfjABHd-kIKkQ6AF6BAgJEAI#v=onepage&q=Redes%20Neuronales%20Convolucionales
- Veli Rojas, D. (2017). *Sistemas de Información Gerencial. Manual Autoformativo Interactivo*. Huancayo: Universidad Continental. Obtenido de https://repositorio.continental.edu.pe/bitstream/20.500.12394/4268/1/DO_UC_EG_MAI_SistemasdeInformaci%c3%b3nGerencial.pdf
- Villalba, M. F., Palacios, A. J., Romero, J. L., & Patarón., E. K. (2019). Sistemas de apoyo a la toma de decisiones: caso de estudio dirección comercial. *Dilemas contemporaneos* , 15. doi.: <https://doi.org/10.46377/dilemas.v30i1.1157>
- Zalimben, S. (2022). *Una pequeña guía de Scrum*. Creative Commons Share-Alike Attribution Commons. Obtenido de https://www.researchgate.net/publication/347993246_Una_pequena_guia_de_Scrum_2da_Edicion

ANEXOS

Anexo 1: Asignación de tutor



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 FISICA EN EL LABORATORIO DE COMPUTO 1 DE LA ULEAM EXTENSION 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 asignado: MORA MARCILLO ALEX BLADIMIR

Apellidos y nombres del estudiante: VELAZQUEZ VERGARA EVELYN JAZMIN

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2024-2025(2)

Sírvase(n) cumplir con lo dispuesto en el Manual de Procedimientos de TITULACIÓN DE ESTUDIANTES DE GRADO: TRABAJO DE INTEGRACIÓN CURRICULAR <https://departamentos.uleam.edu.ec/gestion-aseguramiento-calidad/files/2023/04/Titulacion-de-Est.-Grado-Bajo-la-Unidad-Integr.-Curri.-V.2-1-1.pdf>.

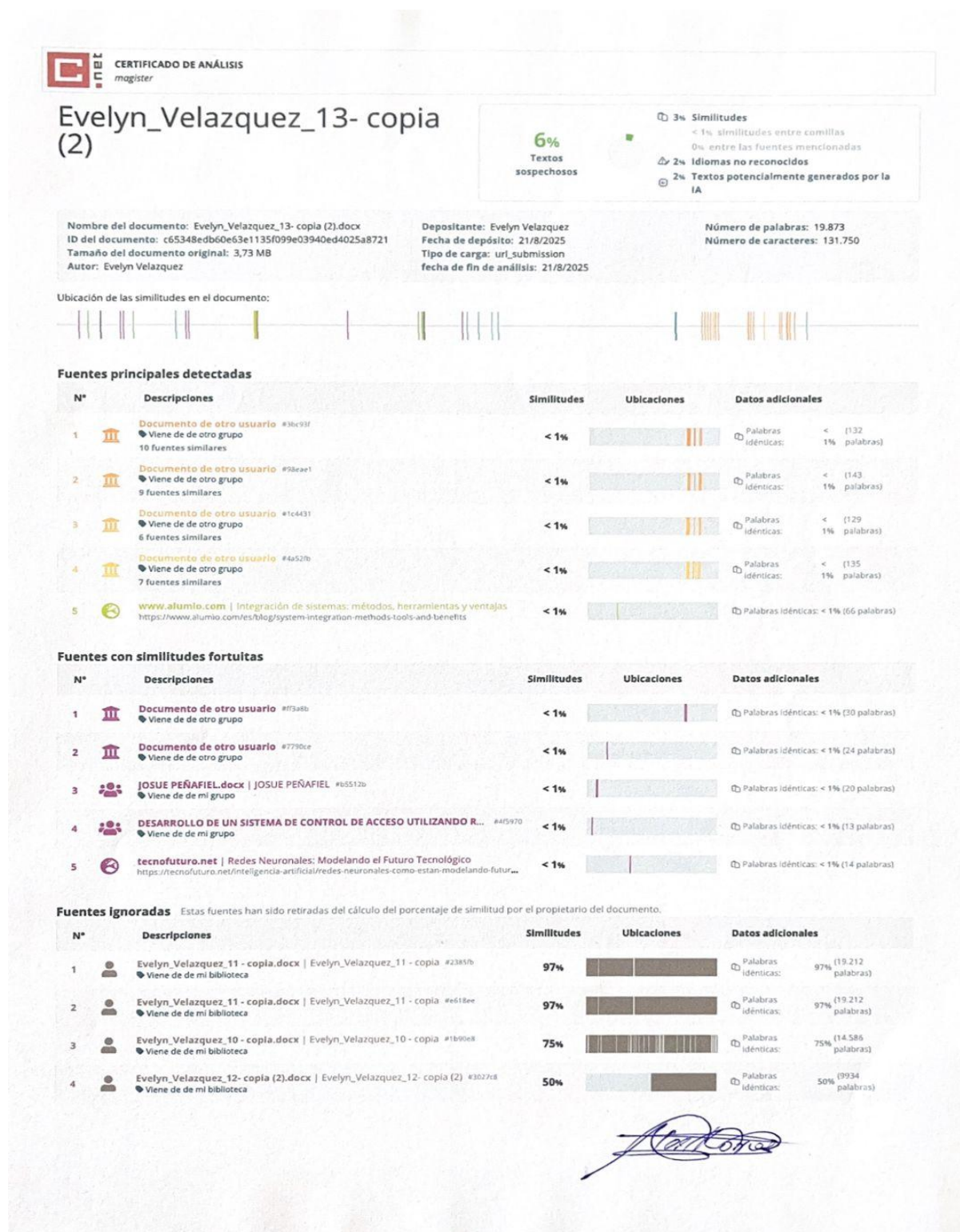
Particular que se informa para los fines consiguientes.

Atentamente,

Comisión Académica y Responsable de Titulación.

Anexos 1: Asignación de tutor

Anexo 2: Reporte del sistema antiplagio



Anexos 2: Reporte del sistema antiplagio

Anexos 3:Fotografías



Ilustración 49: Prueba de esp32

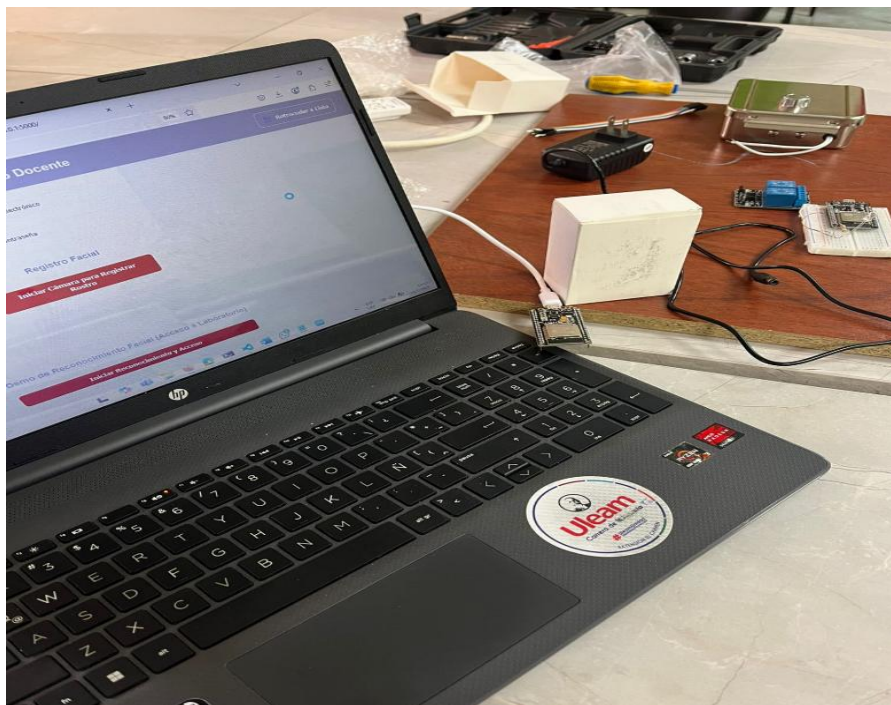


Ilustración 50: Prueba de apertura de cerradura

Anexos 4:Evidencia de aplicación de encuestas y entrevistas

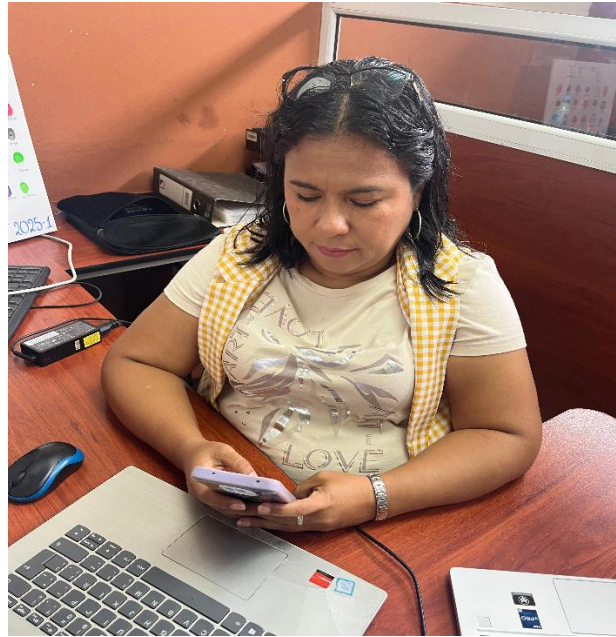


Ilustración 51: Encuesta a docentes



Ilustración 52: Encuesta a docentes



Ilustración 53: Entrevista a técnico

GLOSARIO

ADALINE (Adaptive Linear Neuron): Un tipo de red neuronal artificial simple desarrollada por Widrow y Hoff en 1960.

Algoritmo de Retropropagación (Backpropagation): Un algoritmo fundamental para entrenar redes neuronales, ajustando los pesos de las conexiones neuronales basándose en el error de la salida.

API (Application Programming Interface): Conjunto de definiciones y protocolos para diseñar e integrar software, permitiendo la comunicación entre sistemas.

ARPANET: Red precursora de internet, desarrollada en la segunda mitad del siglo XX, que sentó las bases para la comunicación en red.

Burn-Down Chart: Gráfico utilizado en metodologías ágiles como SCRUM para visualizar el progreso del trabajo restante en un Sprint.

Caja Blanca (White Box Testing): Método de prueba de software que examina la estructura interna del código y el diseño.

Caja Negra (Black Box Testing): Método de prueba de software que evalúa la funcionalidad sin conocer su estructura interna, centrándose en la entrada y salida.

CPU (Central Processing Unit): La unidad central de procesamiento, el "cerebro" de la computadora, responsable de ejecutar las operaciones críticas del sistema.

CRUD (Create, Read, Update, Delete): Acrónimo que describe las cuatro operaciones básicas sobre datos en una base de datos.

CRISP-DM (Cross-Industry Standard Process for Data Mining): Una metodología estructurada para proyectos de minería de datos.

ESP32: Un microcontrolador de bajo costo y bajo consumo con Wi-Fi y Bluetooth, comúnmente usado en proyectos de IoT.

Face-API.js: Librería de JavaScript para reconocimiento facial basada en modelos de visión artificial.

Flask: Un micro-framework de desarrollo web para Python, utilizado para construir el backend de aplicaciones web.

Imutils: Colección de funciones de conveniencia para facilitar tareas de procesamiento de imágenes con OpenCV.

Machine Learning (Aprendizaje Automático): Rama de la IA que permite a los sistemas aprender de datos, identificar patrones y tomar decisiones.

Metodología XP (Extreme Programming): Una metodología ágil de desarrollo de software que busca entregar software de alta calidad de forma rápida y continua.

Perceptrón: Uno de los primeros algoritmos de red neuronal, creado por Frank Rosenblatt en 1957.

Redes Neuronales (Neural Networks): Modelos computacionales inspirados en el cerebro humano, capaces de aprender y realizar tareas complejas (ej., reconocimiento de imágenes).

Redes Neuronales Convolucionales (CNN - Convolutional Neural Networks): Tipo especializado de redes neuronales, muy efectivo para el procesamiento de imágenes y visión por computadora.

Reconocimiento Facial: Tecnología que identifica o verifica la identidad de una persona a partir de una imagen o video.

Visión por Computadora (Computer Vision): Campo de la IA que permite a las computadoras "ver" e interpretar el mundo visual (imágenes y videos).