UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

PROYECTO INTEGRADOR

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

TEMA

SISTEMA DE VIDEOVIGILANCIA CON IA PARA LA GESTIÓN DE SEGURIDAD EN EL LABORATORIO DE ELECTROMECÁNICA DE ULEAM EL CARMEN

VERA LOOR MILLER EFRAN

AUTOR

ING. MORA MARCILLO ALEX BLADIMIR

TUTOR

EL CARMEN, AGOSTO 2026

Certificación de tutor

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

CERTIFICACIÓN

En calidad de docente tutor de la Extensión 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 VERA LOOR MILLER EFRAIN, legalmente matriculado en la carrera de Tecnologías de la Información, período académico 2026-1, cumpliendo el total de 384 horas, cuyo tema del proyecto es "SISTEMA DE VIDEOVIGILANCIA CON IA PARA LA GESTIÓN DE SEGURIDAD EN EL LABORATORIO DE ELECTROMECÁNICA DE ULEAM 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, 31 de julio de 2026.

Lo certifico,

Ing. Alex Bladimir Mora Marcillo, Mg.
Docente Tutor
Área: Tecnologías de la Información

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 DE VIDEOVIGILANCIA CON IA PARA LA GESTIÓN DE SEGURIDAD EN EL LABORATORIO DE ELECTROMECÁNICA DE ULEAM EL CARMEN

Modalidad: Proyecto Integrador

Autor: Miller Efraín Vrea Loor

Tutor: Ing. Mora Marcillo Alex Bladimir, Mg.

Tribunal de Sustentación:

- **Presidente:**

  Ing. Reascos Pinchao Raul Saed, Mg

- **Miembro:**

  Ing. Pozo Hernández Clara Guadalupe, Mg

- **Miembro:**

  Ing. Arca Zavala Jefferson Omar, Mg

Fecha de Sustentación: 21 de agosto de 2026

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 de videovigilancia con IA para la gestión de seguridad en el laboratorio de Electromecánica de la Uleam El Carmen, corresponde exclusivamente a: Vera Loor Miller Efrain con C.I. 1351912348 y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

Vera Loor Miller Efrain

C.I. 1351912348

Tribunal de sustentación

Declaración de autoría

UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: sistema de videovigilancia con IA para la gestión de seguridad en el laboratorio de electromecánica de uleam el carmen, corresponde exclusivamente a: Vera Looe Miller Efrain con CI. 1351912348, y los derechos patrimoniales de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí.

_____

Vera Loor Miller Efrain

C.I. 1351912348

Dedicatoria

Primero darle las gracias a Dios, por ser la fuente de mi fortaleza y el guía constante en cada paso de este camino académico. En los momentos de incertidumbre y dificultad, fue su luz la

que me dio esperanza, su sabiduría la que me oriento y su amor infinito el que me sostuvo para no desfallecer. Sin Su presencia, este logro no habría sido posible.

A mi querida abuela, la señora Cielo Marlene Moreisa Sanches, cuyo cariño, consejos y ejemplo de vida han sido un faro que iluminó mi sendero. Su apoyo incondicional y sus palabras de aliento me recordaron siempre la importancia de la perseverancia y la humildad. Este trabajo es también un homenaje a su entrega y dedicación, que me inspiran a ser mejor cada día.

Al señor José Secundino Zambrano Proaño, por su respaldo y confianza en mí. Su apoyo fue un estímulo invaluable que me motivó a continuar con firmeza, incluso cuando las circunstancias parecían adversas. Su ejemplo de compromiso y responsabilidad me enseñó que los sueños se alcanzan con disciplina y esfuerzo.

A mis amigos y conocidos, quienes con su apoyo moral y compañía me recordaron que nunca estaba solo en este proceso. Sus palabras de ánimo, su paciencia y su presencia en los momentos más difíciles fueron un sostén que me permitió seguir adelante. Gracias por ser parte de este camino y por demostrarme que la amistad verdadera es un tesoro invaluable.

Y finalmente, a mí mismo, por no rendirme a pesar de las adversidades, por mantener la fe en mis capacidades y por demostrar que con esfuerzo, dedicación y constancia los sueños pueden hacerse realidad. Este logro es también un recordatorio de que cada caída fue una oportunidad para levantarme con más fuerza, y cada obstáculo una lección que me acercó a la meta.

Miller Vera

Agradecimiento

Agradezco a mis docentes por haberme guiado con sus conocimientos, cada enseñanza cada lección con las cuales pude formarme y prepararme como profesional, agradezco a mi tutor por guiarme de manera profesional su paciencia y dedicación en cada etapa de este trabajo. La experiencia y compromiso fue fundamental para que este proyecto fuera una experiencia única para seguir mejorando como profesional cada día.

Miller Vera

Índice de contenidos

Índice de tablas

Índice de gráficos e ilustraciones

Índice de anexos

Resumen

El presente proyecto de titulación se desarrolló ante la necesidad de optimizar la seguridad y el control de activos en el Laboratorio de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), Extensión El Carmen. El monitoreo de los equipos informáticos dependía de procesos manuales y supervisiones presenciales esporádicas lo que incrementaba el riesgo de vulnerabilidades, pérdidas o daños en el recinto. Para dar solución a esta problemática, se diseñó e implementó un sistema inteligente de videovigilancia basado en visión artificial. La metodología aplicada se estructuró bajo el marco de trabajo ágil Scrum, permitiendo organizar el desarrollo del software en ciclos iterativos adaptados a los requerimientos del entorno académico. En el núcleo tecnológico se integró el lenguaje de programación Python mediante Visual Studio, el microframework Flask para la gestión web y el protocolo RTSP para la captura de vídeo en directo. Asimismo, se entrenó un modelo de detección de objetos con Roboflow utilizando técnicas de aumento de datos, logrando que la red neuronal reconozca con precisión los equipos bajo diversas condiciones lumínicas. El sistema incorpora además un algoritmo de consistencia temporal en hilos de segundo plano para evitar falsas alarmas, y se vincula con la API de Twilio para el envío automatizado de alertas vía WhatsApp ante cualquier ausencia imprevista. Los resultados de la evaluación demostraron que la plataforma opera de manera estable, sustituyendo eficazmente el control manual por un entorno digital, seguro y automatizado.

Abstract

This graduation project was developed to optimize security and asset control in the Laboratory at the Universidad Laica Eloy Alfaro de Manabí (ULEAM), El Carmen Extension. The monitoring of computer equipment depended on manual processes and sporadic physical supervision, which increased the risk of vulnerabilities, losses, or damage in the facility. To address this issue, an intelligent video surveillance system based on computer vision was designed and implemented. The applied methodology was structured under the Scrum agile framework, allowing software development to be organized into iterative cycles adapted to the requirements of the academic environment. At its technological core, the Python programming language was integrated using Visual Studio, alongside the Flask microframework for web management and the RTSP protocol for live video capture. Additionally, an object detection model was trained using Roboflow with data augmentation techniques, enabling the neural network to accurately recognize the equipment under diverse lighting conditions. The system

also incorporates a temporal consistency algorithm running on background threads to prevent false alarms, and links with the Twilio API for the automated dispatch of WhatsApp alerts in case of any unforeseen absence. The evaluation results demonstrated that the platform operates stably, effectively replacing manual control with a secure, automated digital environment.

Capítulo I

1 Introducción

1.1 Preámbulo

La protección institucional es un elemento clave para llevar a cabo tareas académicas, sobre todo en lugares que acogen equipos de gran valor y prácticas técnicas especializadas. En este marco, el laboratorio de Electromecánica de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, constituye un ambiente crucial para la capacitación de alumnos en la rama de ingeniería. No obstante, se han descubierto fallas notables en los métodos de supervisión continua, control de acceso y registro de actividades, lo cual ha causado amenazas potenciales a la integridad física de los usuarios y al mantenimiento de los recursos tecnológicos.

Hoy en día la integración de sistemas inteligentes ha sido muy útil y han marcado un antes y después en la vigilancia, las tareas avanzadas se han automatizado mediante la inteligencia artificial (IA) desde el reconocimiento facial hasta el análisis predictivo de conductas, en las instituciones se ha logrado administrar una seguridad más robustica ciudadano de cualquier incidente.

El objetivo de este trabajo es crear e implementar un sistema inteligente de videovigilancia basado en IA, con el fin de mejorar la seguridad digital y física del laboratorio de Electromecánica. La idea es combinar módulos de análisis visual, cámaras IP de alta resolución, una base de datos central y un panel para monitorear automáticamente las instalaciones con el objetivo de asegurar un control eficaz, constante y seguro.

Este proyecto transciende a nueva tecnología a través de convertir el laboratorio en innovación. Al implementar un sistema basado con IA en la institución no solo resuelve la seguridad, sino motivar a adaptarse a tecnologías para el futuro. Para los estudiantes es un beneficio crucial de espacios seguros y mostrar las habilidades en aplicaciones reales de visión por computadora y análisis de datos. Así, la tesis se vuelve una herramienta que alinea la educación universitaria con las demandas del mercado de trabajo y las tendencias actuales de digitalización a nivel mundial.

1.2 Presentación del tema

Este estudio tiene como objetivo diseñar, desarrollar y poner en práctica un sistema de videovigilancia inteligente basado en la inteligencia artificial y el procesamiento digital de

imágenes para el Laboratorio de electromecánica de la Universidad Laica Eloy Alfaro de Manabí y Tecnología El Carmen. El sistema combina redes locales de área geográfica y algoritmos de procesamiento de vídeo. El resultado final es una solución que no solo puede grabar imágenes en formato digital, como el sistema estándar comercial, sino también gestionar la seguridad del laboratorio mediante el análisis en tiempo real de las secuencias de vídeo. activo en la gestión de la seguridad del laboratorio.

Un aspecto importante del funcionamiento se consigue mediante la instalación de los llamados «módulos» que permiten reconocer rostros humanos y seguir su movimiento en grupos (horarios) concretos dentro del recinto del laboratorio. El flujo metodológico abarca desde el diagnóstico técnico de la infraestructura de red actual de la universidad y la selección de cámaras con protocolos IP adecuados hasta el entrenamiento y acoplamiento de modelos de visión artificial optimizados para funcionar en condiciones cambiantes de luz y movimiento. El resultado final se estructurará como una plataforma centralizada que alertará automáticamente al personal responsable de cualquier anomalía detectada, generará un registro digital automático que eliminará el uso del registro manual y optimizará la trazabilidad interna de la sala inspeccionada.

1.3 Ubicación y contextualización de la problemática

El presente proyecto se desarrollará en el Laboratorio de Electromecánica de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen, ubicado en la avenida Chone, cantón El Carmen. La extensión universitaria se encuentra en las instalaciones donde anteriormente funcionaba el Colegio de Señoritas Lastenías Vera, en dirección hacia la Unidad Educativa José Ramón Zambrano. Dentro de las instalaciones de la extensión, el Laboratorio de Electromecánica se encuentra ubicado en la planta alta, correspondiente al Laboratorio 1, espacio destinado principalmente al desarrollo de actividades académicas y prácticas de los estudiantes y docentes de la carrera de Electromecánica.

Este tipo de software resulta ventajoso porque puede automatizar diversas tareas y facilitar una gestión integral de la información sobre incidentes. Así pues, analicemos múltiples características que debe tener el sistema propuesto para reforzar significantemente la seguridad del centro: reconocimiento de patrones, algoritmos de reconocimiento facial, cámaras IP provistas de visión nocturna e implementación de sistemas centralizados de registro policial. El proyecto contribuye a reducir considerablemente los índices de producción defectuosa y a garantizar el correcto funcionamiento de los robots industriales.

Extensión El Carmen opera según un esquema de acceso general durante el día y la noche, lo que dificulta el control de cada aula o taller individualmente si solo se confía en guardias de seguridad o conserjes. Debido a la naturaleza de los proyectos que allí se llevan a cabo, el laboratorio de electromecánica suele permanecer abierto fuera del horario habitual de docencia para que los estudiantes desarrollen sus proyectos de grado o trabajos integradores.

Esta vez, la flexibilidad esencial para el crecimiento académico entra en conflicto directo con la capacidad de supervisión de la institución. En los últimos años, la dinámica de inseguridad poblacional observada a escala nacional permea también el ambiente escolar, por lo que las universidades deben adoptar medidas especiales de seguridad tecnológica para proteger sus laboratorios del robo de componentes costosos y monitorear incidentes que amenacen la seguridad de los usuarios.

1.4 Planteamiento del problema

1.4.1 Problematización

El laboratorio de electromecánica de la ULEAM Extensión El Carmen carece actualmente de un mecanismo tecnológico centralizado y autónomo que monitoree continuamente sus accesos y perímetros internos. El control del funcionamiento de esta sala se realiza mediante procesos manuales que incluyen el préstamo físico de llaves, firmas en cuadernos de asistencia y revisión esporádica por parte del docente responsable. Este método tradicional tiene graves fallas de seguridad: no permite verificar confiablemente que las personas que ingresan están autorizadas y no genera advertencias inmediatas si la intrusión ocurre fuera del horario laboral autorizado o si el equipo es manipulado sin la debida supervisión técnica.

La falta de automatización no sólo aumenta el riesgo de pérdidas materiales, que afectarán directamente a las arcas de la institución y al nivel académico de la educación, sino que también deja a la administración en una actitud puramente reactiva. Cuando las herramientas de trabajo se violan o dañan, los técnicos deben pasar horas revisando manualmente secuencias de video continuas (si las cámaras locales están funcionando), un proceso ineficiente que rara vez resulta en identificar quién es el responsable. Considerando esta realidad, es necesario formular las siguientes preguntas de investigación:

1.4.2 Génesis del problema

Procedimientos de supervisión manual: El personal de conserjería del campus o los maestros son los únicos responsables de supervisar el área al principio y al final del día. Para

proteger una gran propiedad universitaria, el personal de seguridad no puede estar apostado permanentemente en la puerta del laboratorio, lo que crea ventanas de vulnerabilidad que son aprovechadas por agentes externos o usuarios no registrados.

Falta de control para acceder físicamente: Las puertas de los laboratorios carecen de cerraduras electrónicas o sistemas biométricos que verifiquen las identidades de los estudiantes en tiempo real. Esto permite el libre acceso a personas ajenas a la práctica electromecánica y reduce la responsabilidad individual por el uso y cuidado de los materiales allí almacenados.

Insuficiencia de supervisión en horarios extendidos: El laboratorio no tiene supervisión durante horas de escaso flujo o cuando el personal administrativo está ausente, lo que incrementa la posibilidad de incidentes.

1.4.3 Estado actual del problema

Riesgo para la integridad de los estudiantes: Durante los turnos de trabajo de los empleados, los fines de semana, los recesos administrativos o a altas horas de la noche, el laboratorio permanece completamente desprotegido. Los sistemas de grabación actuales, que son pasivos, retienen el vídeo, pero son incapaces de distinguir si el movimiento detectado a primera hora de la mañana corresponde a un vector de riesgo o a una falsa alarma provocada por factores ambientales.

Desaparición de equipos y materiales: Los instrumentos calibrados, osciloscopios, fuentes de alimentación y computadoras diseñadas para el diseño de ingeniería de software pueden perderse o manipularse incorrectamente, acortando su vida útil. La falta de un registro visual clasificado inteligentemente hace imposible determinar exactamente qué usuario manipuló un equipo en particular antes de que se informara un accidente.

Bajo rendimiento en la gestión de seguridad: La gestión administrativa de la ampliación se ve obligada a operar con un enfoque puramente correctivo. La falta de mediciones e indicadores en tiempo real de los flujos de recubrimiento de laboratorio limita la toma de decisiones informadas destinadas a optimizar los recursos de seguridad de la universidad.

1.5 Diagrama causa–efecto del problema

El laboratorio de Electromecánica presenta inseguridad principalmente por la falta de herramientas tecnológicas que permiten un control eficiente en el acceso, supervisión y monitoreo de las actividades. Esta situación muestra un entorno vulnerable ante cualquier

riesgo de manipulación de equipos y datos debido a la ausencia de vigilancia apropiada. Los principales factores a este problema incluyen:

- Procesos de supervisión manual.
- Control para acceder físicamente.
- Falta de supervisión en horarios extendidos.
- Impactos desfavorables.
- Riesgo para la integridad de los estudiantes.
- Perdida de equipos y materiales.
- Bajo rendimiento en la gestión de seguridad.
- Conclusión del análisis de causa y efecto.

La conexión directa entre las causas detectadas y los efectos perjudiciales que se han producido pone de manifiesto la necesidad de poner en funcionamiento un sistema automatizado de videovigilancia inteligente. Este tipo de solución tecnológica va a posibilitar un mejor control, la disminución de riesgos, el fortalecimiento del control de acceso y la optimización del empleo de los recursos institucionales, lo que asegurará un ambiente más eficaz y seguro para alumnos, profesores y personal administrativo.

Un estudio cuidadoso de los factores que afectan al laboratorio electromecánico muestra una conexión clara entre las razones y los impactos logísticos que perjudican el entorno universitario. Al mirar el tema de los procedimientos de monitoreo manual, se hace evidente que el error humano y el cansancio son factores que no se pueden evitar en cualquier sistema analógico. Un guardia de seguridad que está mirando varias pantallas pierde más del 80% de los detalles pequeños de una escena después de observarla durante veinte minutos sin parar. Este fenómeno ha sido estudiado en detalle en los libros sobre ingeniería industrial y psicología organizacional. Como resultado, el efecto inmediato de esta falta es un mal rendimiento en general en la gestión de la seguridad del campus. En cambio, la ausencia de un control físico automatizado hace que el perímetro del laboratorio sea más vulnerable.

Como no hay un filtro que cruce los datos de acceso con las bases de datos en la carrera de Tecnologías de la Información o Electromecánica, el taller se transforma en un lugar donde todos pueden moverse libremente. Este fenómeno ayuda a la rápida desaparición de materiales pequeños pero caros, como conectores, herramientas manuales y componentes electrónicos pequeños, una sustitución que sigue creciendo.

Al final, la ausencia de vigilancia durante la noche o en las últimas horas genera un espacio donde se puede actuar sin temor a ser atrapado. La mezcla de estas razones hace que haya un ambiente donde ocurren accidentes, y la única solución posible es cambiar los circuitos reactivos por una tecnología que use computación avanzada e inteligencia artificial. Esto le dará al laboratorio la habilidad de responder de manera rápida y automática.

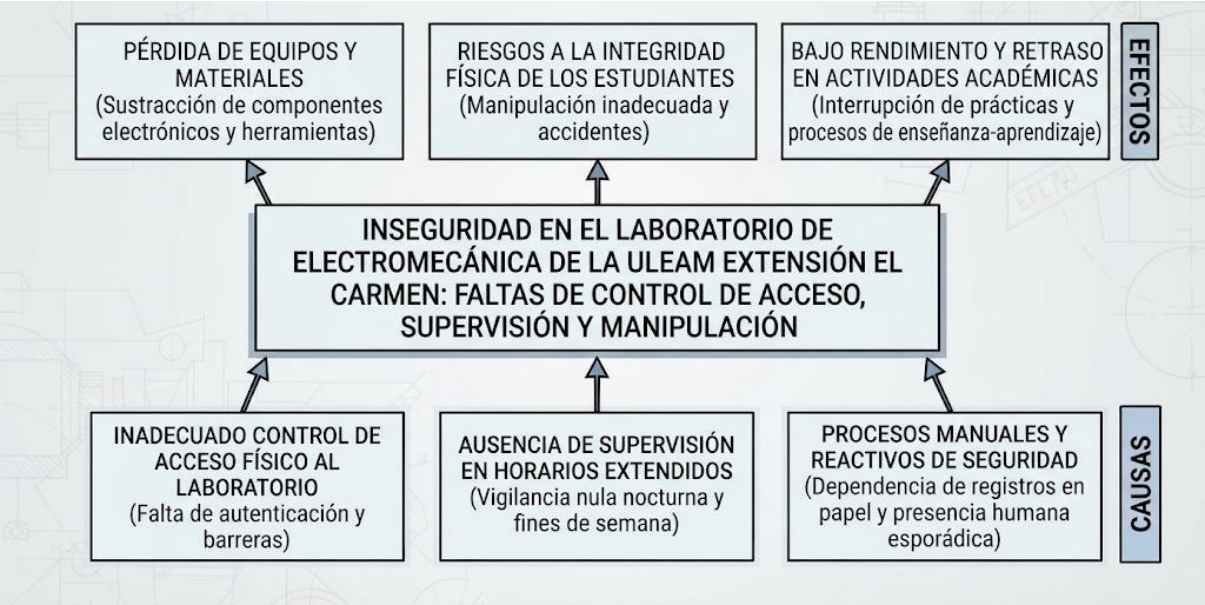


Ilustración 1Diagrama de causa y efecto

1.6 Objetivos

1.6.1 Objetivo general

Implementar un Sistema De Videovigilancia Con IA Para La Gestión De Seguridad En El Laboratorio De Electromecánica De la Uleam Ext El Carmen.

1.6.2 Objetivos específicos

Este estudio le ofrece a la administración universitaria una solución clara, concreta y fácil de aplicar desde ya. Cuando el proyecto esté terminado, la Ampliación será para proteger la inversión hecha en el laboratorio de electromecánica. Los docentes podrán trabajar tranquilos, sabiendo que sus espacios están seguros con alertas en tiempo real. Y los estudiantes disfrutarán de un ambiente seguro donde podrán desarrollar sus prácticas de ingeniería con total confianza, sin que el miedo a la seguridad física limite su tiempo o sus ganas de aprender.

- Diagnosticar la situación actual de inseguridad en el Laboratorio de Electromecánica de la ULEAM Extensión El Carmen, identificando las vulnerabilidades críticas en los procesos de control, supervisión y acceso mediante el análisis de causas y efectos.
- Fundamentar teóricamente la viabilidad del uso de algoritmos de aprendizaje profundo (Deep Learning) como soluciones eficientes para la videovigilancia inteligente en entornos con limitaciones tecnológicas locales.
- Definir el proceso de desarrollo del sistema utilizando la metodología Scrum, estableciendo los roles, artefactos y eventos necesarios para el desarrollo iterativo del software de monitoreo y detección de manipulación de equipos.
- Desarrollar e integrar el software de videovigilancia inteligente que permita detectar la manipulación no autorizada de equipos y validar los accesos al laboratorio, optimizando el rendimiento del modelo para el hardware institucional disponible.
- Evaluar el impacto de la implementación del sistema automatizado mediante pruebas de campo, verificando su eficacia en la reducción de riesgos y la mejora de la seguridad del laboratorio en comparación con el esquema de supervisión manual previo.

1.7 1Justificación

El objetivo de esta investigación es adecuar y fortalecer la seguridad del laboratorio de Electromecánica en la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, debido a la urgencia necesaria de implementar mecanismos de control y seguimiento en el aula. Este entorno académico cuenta con equipos especializados, materiales de valor y herramientas esenciales para la formación profesional, es indispensable proteger estos activos para garantizar condiciones de estudio óptimas y dignas para los estudiantes. A pesar de los esfuerzos actuales la vigilancia en la universidad enfrenta una supervisión y control de acceso por un proceso manual que son propensos a errores.

Al ser necesario un sistema de seguridad se presenta este proyecto que permite romper las limitaciones de los métodos tradicionales ofreciendo un monitoreo continuo y una detección de intrusos mucho más precisa. La ventaja es la capacidad de respuestas en tiempo real con la integración de reconocimiento facial y el análisis de comportamiento, no solo registra los

eventos, sino una tranquilidad y capacidad de anticipar posibles incidentes que afecten a la universidad.

En el entorno académico es un impacto directo al contribuir el proceso tecnológico, no solo modernizar la infraestructura, sino motivar a los estudiantes a ser protagonistas del diseño y evaluar el sistema que hoy lidera el sector de la ingeniería. No solo es instalar cámaras, es mas de avanzar y aprovechar las tecnologías para elevar los estándares de la universidad fortaleciendo la calidad del entorno educativo.

Metodológicamente, este trabajo desarrolla un modelo de arquitectura de software que es escalable y que puede ser utilizado como ejemplo en otros laboratorios universitarios, como laboratorios de computación, talleres de reparación de automóviles o en áreas de investigación de posgrado. El método organizado que se usa para el diagnóstico, el diseño de bases de datos, la segmentación de redes y la implementación de software servirá como una guía clara y detallada para estudiantes y desarrolladores universitarios que deseen llevar a cabo proyectos enfocados en la automatización de la seguridad física, utilizando el Internet de las cosas y la inteligencia artificial.

1.8 Impactos esperados

Esta sección describe los beneficios que se espera obtener al implementar el sistema de videovigilancia inteligente, basado en inteligencia artificial, en el laboratorio de Electromecánica. Con el objetivo de demostrar la importancia integral del proyecto en el contexto institucional y académico.

1.8.1 Impacto tecnológico

La implementación de esta plataforma significa un avance tecnológico importante para la ULEAM Extensión El Carmen. Esto reemplaza el uso de viejos grabadores analógicos por una infraestructura moderna que utiliza cámaras IP con alimentación PoE y servidores para el análisis perimetral. Este efecto se ve en el uso de arquitecturas distribuidas, donde el procesamiento de las imágenes sucede cerca de donde se capturan, lo que reduce el tiempo de respuesta de las alertas y previene la congestión de los canales de datos en la red principal de la universidad. La llegada de la inteligencia artificial en el control de accesos coloca a la carrera de Tecnologías de la Información como un impulsor de innovación dentro de la organización, mostrando que las habilidades que se aprenden en las aulas pueden solucionar problemas operativos de la misma institución.

Entorno académico más seguro: El efecto social de esta propuesta va más allá de la simple identificación de incidentes. Se fomenta dentro de la comunidad universitaria una cultura de seguridad proactiva al implementar un sistema de vigilancia inteligente. La convicción de que el laboratorio es monitoreado de manera precisa y constante genera un aumento significativo en la sensación de seguridad entre los alumnos, los maestros y el personal administrativo. Para que los estudiantes se concentren en sus tareas académicas, es esencial tener un entorno de confianza más elevado, ya que esto disminuye las distracciones y preocupaciones relacionadas con la posibilidad de riesgos. inteligente.

Disminución de incidentes: Permite reducir los incidentes al anticipar las conductas ni autorizados antes intrusos o daños del equipo.

Responsabilidad: El registro digital de actividades del usuario para motivar a tener un comportamiento responsable al utilizar el laboratorio.

Respaldo de la institución: La universidad no solo protege sus activos, sino que actúa para modernizar sus gestiones administrativas bajo estándares de alta eficiencia.

Este impacto, en general, ayuda a que el laboratorio se ubique como un lugar actualizado y que sigue las tendencias tecnológicas actuales.

1.8.2 Impacto social

En el ámbito social, el proyecto fomenta el desarrollo de una cultura de corresponsabilidad, disciplina y orden en todos los niveles de la comunidad universitaria que se relaciona con el laboratorio. Saber que el acceso es controlado por un sistema automático que reconoce caras hace que los estudiantes se comporten de manera más cuidadosa y sigan mejor las reglas internas. Además, el efecto social más importante es que la seguridad se vuelve más accesible para todos: se asegura que tanto los estudiantes que van por la mañana como los que están en las residencias, muchos de los cuales trabajan y estudian al mismo tiempo, tengan los mismos niveles de protección y ayuda técnica pasiva en caso de un accidente o incidente en el taller.

Seguridad en el entorno académico: La inteligencia artificial ha generado un impacto significativo en la comunidad universitaria, transformando la supervisión tradicional en un modelo de gestión avanzado para estudiantes y profesores. El objetivo trasciende de la

detección de incidentes hasta la búsqueda de registro eficiente de la actividad realizada, la implementación de un sistema de vigilancia fortalece la seguridad en el entorno universitario como la alineación de proyectos tecnológicos a futuro. Al tenerla disponibilidad de un monitoreo constante se asegura un entorno de aprendizaje estable y confiable para los estudiantes, profesores y administradores. Este entorno de confianza incrementada es esencial para poder concentrarse en las actividades académicas, disminuyendo así las distracciones y preocupaciones vinculadas a la eventual ocurrencia de riesgos.

Prevención de incidentes: La automatización en el control de acceso permite identificar comportamientos no irregulares.

Responsabilidad: El beneficio es crucial al integrar la tecnología al comportamiento humano. La presencia de un registro digital y permanente de las actividades y accesos crea un grado de trazabilidad que motiva a los usuarios a adoptar conductas más prudentes y respetuosas con las reglas de uso. El sistema inteligente no solo da importancia a la seguridad, sino a la diciplina y el cumplimiento de los protocolos que son fundamentales en este entorno donde las practicas son esenciales.

Gestión institucional: cuidar y mejorar nuestra segunda casa es nuestra prioridad, una universidad ordenada y segura es la base principal para los estudiantes, un enfoque de mejoramiento en su aprendizaje.

1.8.3 Impacto ecológico

Aunque el proyecto tecnológico principalmente, tiene como efectos en el medio ambiente la sostenibilidad institucional ya que estos son muy importantes. Al automatizar todos los registros de entrada y salida, así como los informes de novedades y problemas diarios, se elimina totalmente la necesidad de usar formularios impresos y cuadernos de papel. Esto ayuda a que los procesos administrativos de la universidad estén en línea con las políticas internacionales de reducción de emisiones de carbono y de la huella ecológica. En el laboratorio de Electromecánica al darle un seguro constante e inteligente da buenos frutos para evitar un mal manejo de los equipos, con estos beneficios ayuda a alargar la vida útil, prevenir desgastes temprano y disminuir la cantidad de residuos.

Digitación y ahorro papel: La digitalización de los informes de incidentes y de los registros de acceso reduce la necesidad de documentos en papel.

Mejorar la utilidad de los equipos: Al dar una supervisión constante se reducen el ingreso de desconocidos o el mal uso que da mayor tiempo de vida a los quipos del laboratorio.

Menor energía: El mejoramiento de los sistemas con IA y cámaras IP modernas fueron creadas con menos consumo energético y así disminuye el efecto del medioambiente.

Cuidados de equipos: Proteger el hardware del laboratorio proviene los riesgos de daño y deterioro prematuro lo que disminuye la acumulación de basura digital.

Estos elementos evidencian que el proyecto, además de reforzar la seguridad, fomenta prácticas sustentables en la entidad.

Capítulo II

2 Marco teórico de la investigación

2.1 Antecedentes históricos

Los sistemas de videovigilancia, que están bajo la supervisión continua de un ser humano y se orientan a la observación pasiva, fueron desarrollados mediante sistemas analógicos de circuito cerrado (CCTV). Su diseño original unía cámaras con grabadoras de cinta y monitores, los cuales tenían serias limitaciones en términos de almacenamiento, escalabilidad y calidad de imagen. Este modelo fue el más común hasta finales de la década de 1990, cuando la digitalización permitió que las infraestructuras conectadas fueran más efectivas. (Li, 2020)

A partir del 2020, la videovigilancia se ha transformado en un sistema proactivo que tiene la capacidad de automatizar tareas complejas mediante el uso de inteligencia artificial (IA) y aprendizaje profundo. Estas tareas abarcan la identificación de anomalías, el reconocimiento de acciones violentas, la Re identificación de personas y la activación en tiempo real de alertas. Los marcos híbridos que juntan diversas tareas en un mismo pipeline reducen los falsos positivos y mejoran la precisión operativa en circunstancias difíciles. (Evany Anne, 2025)

Las evaluaciones prácticas llevadas a cabo en ciudades inteligentes sugieren que la videovigilancia con inteligencia artificial tiene un impacto más allá de la seguridad, debido a que también gestiona el tráfico, controla los flujos urbanos y asiste para mantener la resiliencia frente a circunstancias críticas. Este enfoque necesita de la gobernanza de datos, una evaluación ética y de diseños escalables que se fundamenten en arquitecturas de nube perimetral para garantizar el procesamiento en tiempo real. (IEEE Access , 2024)

La migración hacia lo digital incluyó cámaras IP, compresión de video y gestores de video (VMS), lo que permitió una resolución más alta, un registro más extenso y acceso a distancia. Esta fase estableció la videovigilancia como infraestructura que funciona de manera interoperable con redes corporativas y móviles, y sentó las bases para el análisis avanzado y la gestión centralizada a nivel institucional. (Evany Anne, 2025)

La arquitectura de computación en el borde (Edge Computing) surgió como un componente fundamental para disminuir la latencia y optimizar los tiempos de respuesta al procesar datos próximos a las cámaras y aliviar la carga de red. Estos diseños facilitan la

exportación segura de evidencias y respuestas rápidas en contextos que exigen una latencia reducida, como las fábricas e instalaciones industriales, así como su integración con VMS. (San Román Lana, 2019)

En el sector educativo, los laboratorios y los lugares de investigación necesitan rastrear accesos, supervisar en horarios extendidos y proteger activos de gran valor. Integrar VMS con análisis de IA y políticas de privacidad, para equilibrar la seguridad y el cumplimiento institucional a través de controles de acceso por roles, cifrado y retención responsable de datos, es lo que sugiere la evidencia académica (Evany Anne, 2025).

En conclusión, la evolución histórica va desde el CCTV analógico con supervisión pasiva hasta las plataformas digitales que incorporan análisis de inteligencia artificial y Edge Computing, que tienen la capacidad de analizar comportamientos en tiempo real. Según este marco técnico e histórico, es importante poner en marcha un sistema de videovigilancia inteligente en el laboratorio de Electromecánica: se optimiza la administración institucional, se mejora la seguridad operacional y la capacitación ingenieril se adapta a la transformación digital actual. (Li, 2020)

Conforme la tecnología avanzaba en la década de 2010, comenzaron a fusionarse las plataformas en la nube y los sistemas de análisis de datos con la videovigilancia. Gracias a esta integración, se pudo almacenar grandes volúmenes de información y acceder a ellos desde lugares remotos. Gracias a esta integración, se han podido desarrollar sistemas más sólidos y escalables, que tienen la capacidad de gestionar varias cámaras y usuarios simultáneamente. Dardour, El Haji y Achkari Begdouri (2025) sostienen que la incorporación de inteligencia artificial en los sistemas de videovigilancia ha transformado esta tecnología en una herramienta clave para la seguridad urbana y la gestión institucional. Esto es así porque permite no solo identificar incidentes en tiempo real, sino también anticipar comportamientos tanto en espacios públicos como privados.

La historia de la videovigilancia comenzó a principios del siglo XX. Las primeras cámaras de video eran costosas y básicas cambiaron la historia por completo. En 1942 la empresa alemana Siemens desarrolló la primera cámara de televisión con capacidad de grabación, un avance que transformo la seguridad para siempre y dio un inicio a la era analógica de las cámaras CCTV.

Por muchos años los sistemas de circuito cerrados de televisión (CCTV) fueron líder de la industria de seguridad y videovigilancia, estás cámaras analógicas utilizaban cintas de vídeo

y sistemas de grabación. A pesar de las limitaciones en resolución y capacidad de almacenamiento, CCTV supuso un avance significativo en seguridad. (Ariel, 2023)

2.2 Antecedentes de investigaciones relacionadas al tema presentado

a) "Sistema de videovigilancia basado en visión artificial para espacios institucionales"

Gutiérrez Meneses hizo una tesis en la Universidad Politécnica Salesiana en el año 2021. Diseñé un sistema de videovigilancia inteligente como parte de mi trabajo. Aproveché soluciones sencillas open source para implementar visionado artificial y seguir observando elementos de interés. Mi investigación ha demostrado la viabilidad de adquirir una solución de este tipo por un precio moderado y tunearla para que se adapte a las necesidades específicas de una organización particular en términos de rendimiento y configuración. He analizado diversas opciones tecnológicas y he llevado a cabo pruebas de rendimiento para garantizar que mi sistema funcione correctamente incluso en condiciones de baja visibilidad o tras diversos cambios en las condiciones ambientales. También comento los aspectos relevantes de mi elección de componentes, incluidas consideraciones relacionadas con la fiabilidad y la reducción de costos, algo fundamental si se recurre a hardware de segmentos inferiores y/o software open source. Me centraré en cómo esta información respalda mis ideas sobre la rentabilidad de la investigación y desarrollo en el contexto de un entorno similar al de Ecuador. (Gutiérrez Meneses, 2021)

En este estudio, se explica cómo funciona el hardware y cómo se capturan y procesan las imágenes de video. Se menciona cómo utiliza el uso de modelos para detección precisa de eventos en áreas educativas, detalla la integración de componentes de almacenamiento, transmisión de datos, sistemas de alertas, evaluando su impacto de consumo y estabilidad del sistema. La investigación concluye que el uso de hardware especiales reduce costos de mantenimiento de alto nivel de precisión en los registros. El antecedente evidencia el desarrollo exitoso de proyectos similares en Ecuador, validando la técnica de la propuesta aplicada en locales.

b) "Sistema de videovigilancia IP para la seguridad de la Quinta Nápoles"

Este proyecto integrador fue desarrollado en la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, por el estudiante Tipán Pérez Kevin Alexander, como requisito para obtener el título de Ingeniero en Tecnologías de la Información. La investigación se centró en diseñar e implementar un sistema de videovigilancia IP para garantizar la seguridad de la

Quinta Nápoles, aplicando criterios técnicos de selección de cámaras megapíxel, almacenamiento local mediante tarjetas SD y opciones de NVR para entornos más complejos. Dicho trabajo resalta la importancia de la eficiencia energética y el aprovechamiento de recursos, evidenciando una correcta distribución de cámaras y diseño de cableado disminuye los costos y mejora el área de cobertura. A pesar de no integrar inteligencia artificial su enfoque en la arquitectura de gestión de video es la base para futuras escalabilidades. (Tipán Pérez, 2025)

La propuesta técnica profundiza la ubicación estratégica de los dispositivos de seguridad física del hardware, la división de redes lógicas y sistemas de contingencia para asegurar la continuidad operativa. Al incluir estrategias de retención de video y planes de mantenimiento el proyecto asegura un sistema confiable. Esto radica en validar las decisiones de diseño arquitectónico tomadas en este proyecto, sirviendo como referencia de que en Ecuador existe implementaciones de videovigilancia IP exitosas y aplicables a laboratorios academicos.

c) "Implementación de un sistema de vigilancia mediante cámaras, sensores y alarmas para el campus del complejo universitario"

Esta tesis se hizo en la Universidad Estatal del Sur de Manabí en la carrera de Ingeniería en Tecnología de la Información. Los autores Castro Delgado y Caicedo Plúa diseñaron un sistema de vigilancia para el campus universitario en el año 2022. El objetivo principal del sistema es fortalecer la seguridad dentro del entorno universitario ya implementado específicamente en el complejo académico de Jipijapa, cubriendo áreas estratégicas como acceso principal, pasillos y zonas comunes. La implementación destacó por el uso de criterios técnicos para la colocación de dispositivos, gestión de alertas y de redes logrando una cobertura integral y mitigando los riesgos en tiempo real. Este caso de estudio evidencia el desarrollo exitoso de soluciones de seguridad tecnológica en el entorno universitario ecuatoriano. (Castro Delgado y Caicedo Plúa, 2022)

Las autoras ofrecen al lector una descripción exhaustiva del funcionamiento del sistema: detallan los tipos de sensores, analizan su funcionamiento e identifican las medidas necesarias para garantizar que se active el sistema de alerta. Para comprobar que el sistema funciona correctamente, las autoras someten el mismo equipo a pruebas en condiciones reales mediante la simulación de intentos de piratería y el análisis de la respuesta del sensor ante dichos intentos. Finalmente, también evalúan otras formas de optimizar el rendimiento del sistema, como sus

características de mantenimiento, alimentación y gestión de datos, para garantizar su fiabilidad durante su periodo de uso previsto. Todo ello demuestra hasta qué punto el sistema propuesto - que combina cámaras de videovigilancia y sensores - es eficaz a la hora de proteger cualquier instalación frente a posiblespiratas. Dado que dicho sistema ya ha sido instalado y puesto en marcha en un centro universitario del Ecuador, su estudio resulta especialmente relevante para la presente investigación, demostrando de forma tangible la eficacia de dichas medidas de protección.

b) “Diseño e implementación de un sistema inteligente de seguridad con respuesta en tiempo real mediante la integración de cámaras y sensores usando AIoT”

Quiñones Cuenca, Cuenca Maldonado y Maza Merchán realizaron una tesis en la Universidad Técnica Particular de Loja **(**UTPL**)** en el año 2021. El trabajo abordo un diseño de un sistema de seguridad inteligente mediante el uso de cámaras y sensores conectados a través de AloT, una plataforma se centró en detectar situaciones de riesgos y automatizar notificaciones en tiempo real para el personal de control. Los resultados del proyecto demostraron una mejora significativamente en tiempo de reacción ante eventos críticos logrando una gestión de seguridad mucho más eficiente y oportuna en el ámbito institucional. Los autores concluyeron que el uso de tecnologías accesibles y escalables facilita la implementación de sistemas de videovigilancia eficientes en organizaciones de tamaño medio.

En esta investigación se aplicará el método estadístico con el propósito de ordenar, procesar y examinar la información recopilada mediante encuestas y entrevistas, permitiendo convertir los datos en resultados precisos y comprensibles. Para el análisis se emplearán porcentajes y medidas de tendencia central, con el fin de reconocer patrones relacionados con la percepción de la seguridad institucional. Posteriormente, los resultados serán representados a través de tablas y gráficos que contribuyan a una mejor interpretación de la información y apoyen la toma de decisiones. (Sánchez Quirola, 2021)

2.3 Definiciones conceptuales

2.3.1 Videovigilancia

2.3.1.1 Evolución de la videovigilancia

La videovigilancia ha evolucionado de sistemas de circuito cerrado (CCTV) analógicos a plataformas digitales que incluyen cámaras IP y gestores de video (VMS). Huang, Chen y Su (2024) indican que el sector ha aumentado en cuanto a publicaciones y aplicaciones,

enfatizando lo relevante que es la incorporación de tecnologías de análisis de datos y el cambio hacia sistemas inteligentes con inteligencia artificial.

Por otro lado, el sistema de videovigilancia (VSS) con herramientas de monitoreo pasiva se han convertido en un apoyo fundamental en las ciudades inteligentes, integrando el aprendizaje profundo (Deep Learning), Edge Computing y cadena de bloqueo (Blockchain). Según Myagmar y Kim (2023) los sistemas modernos permiten reconocer automáticamente las acciones humanas y detectar anomalías en tiempo real para optimizar la seguridad y reduciendo los delitos.

2.3.1.2 Arquitecturas distribuidas y edge computing

Como el Edge Computing posibilita que se procesen los datos cerca de la fuente, mejorando así la eficacia y disminuyendo la latencia, este se ha vuelto un elemento clave en los sistemas actuales de videovigilancia. El sistema AiWatch, que se basa en gemelos digitales e inteligencia artificial y reparte el procesamiento entre la nube y el borde, es sugerido por Ferone y otros autores (Ferone et al., 2025)

De forma adicional, diseñaron un sistema de videovigilancia inteligente que se basa en la computación en el borde, lo cual muestra que esta estructura permite una mejor capacidad de reacción y disminuye la carga del servidor central; por ello es una solución posible para las instituciones educativas. (Cob Parro et al., 2021)

2.3.1.3 Aplicaciones de IA en control de acceso

Idrobo Vivar (2023) creo un sistema de videovigilancia con inteligencia artificial para gestionar accesos en su tesis de maestría en la Universidad Israel, en Ecuador. Su estudio evidencia que es factible implementar análisis de comportamiento y reconocimiento facial en entidades educativas.

De forma parecida, Yao (2024) examinó un sistema de videovigilancia inteligente con inteligencia artificial en espacios comunitarios y determinó que la incorporación de algoritmos para detectar anomalías aumenta la seguridad en instituciones y zonas públicas.

2.3.1.4 Inteligencia artificial aplicada a seguridad institucional

Los sistemas de seguridad institucional se están integrando con la IA representando cambios en el futuro y mejorando la vigilancia. Con estos avances ha mejorado la videovigilancia inteligente integrados para mejorar el rendimiento con el aprendizaje profundo,

redes neuronales convolucionales (CNN), las aplicaciones visión artificial, detección y clasificación de objetos (Olaniyi et al., 2023).

En su informe técnico acerca del estado de la inteligencia artificial en la videovigilancia, la institución Axis Communications (2025) sostiene que implementar algoritmos inteligentes no solo incrementa la seguridad, sino que además brinda eficacia operacional y análisis de negocio dentro de las instituciones.

2.3.1.5 Videovigilancia en instituciones educativas

En la actualidad es crucial una supervisión constante en las instituciones educativas debido a incidentes o impactos que afecten, es un beneficio no solo para los estudiantes, sino que permite a la institución tener un control adecuado sin afectaciones o buscar soluciones a dichas acciones.

Un sistema de cámaras de circuito cerrado de televisión (CCTV) ha demostrado ser una herramienta eficiente y eficaz para la seguridad fisca con el objetivo de fortalecer y garantizar una supervision constante, asi mejorando la respuesta de cualquier incídete. Además, se enfoca en la formación académica para incentivar la creación de nuevas tecnologías para un entorno seguro y creativo (Checa et al., 2025).

2.3.1.6 Videovigilancia y criminología: prevención situacional del delito

En la actualidad, la seguridad se ha consolidado como un pilar fundamental para los delitos y garantizar entornos protegidos. Para lograr se debe conocer dos pasos críticos: uno es la videovigilancia mediante sistemas inteligentes diseñado para optimizar la accesibilidad y el monitoreo constante. Por otro lado, la criminología que aporta el análisis de información necesario para comprender los delitos. Ambas permiten no solo reaccionar ante incidentes, sino establecer una estrategia de protección efectiva y sostenible.

El delito sigue creciendo y unos de los beneficios fundamentales es la prevención a través de la gestión de la información, así se recolecta y analiza los datos permitiendo tener un modelo de prevención estratégica. En Ecuador las instituciones como es el Departamento de Análisis de Información del Delito (DAID) han demostrado que a través de tecnología de vigilancia ser capaces para identificar patrones y comportamientos criminales, facilitando la toma de decisiones con evidencias claras y precisas, reduciendo las oportunidades de delitos en espacios institucionales y públicos (Torresano Melo y Calles López, 2018).

2.3.1.7 Componentes tecnológicos de la videovigilancia moderna

Un sistema de videovigilancia moderno es un conjunto interconectado de dispositivos diseñados para capturar y analizar datos, estos son fundamentales para que el sistema se una con las cámaras de red, medios de transmisión y sistemas de gestión de video (VMS) permitiendo la administración centralizada en la información. Ahora se almacenan en grabadores de video en red (NVR) que ofrecen una mayor escalabilidad y son capaces de integrarse con herramientas de análisis inteligentes en comparación de sistemas analógicos tradicionales (Senstar Corporation, 2025).

2.3.1.8 Cámaras IP y sistemas NVR

Las cámaras IP son capaces de capturar y procesar videos digitales y en este ámbito digital las NVR han construido un núcleo de almacenamiento y gestión de datos a diferencia de los sistemas tradicionales. Un NVR captura transmisiones de video que fueron procesados por cámaras IP a través de red local. Las tecnologías destacan por su capacidad de manejar altas resoluciones y facilidad de instalaciones, permitiendo conexión inalámbrica como por cable Ethernet (PoE) (Contributed by, 2025).

2.3.1.9 Videovigilancia y energética en sistemas tecnológicos

Un sistema tecnológico ha evolucionado con el trascurso de los años mostrando una sostenibilidad en el diseño de infraestructura crítica y en los sistemas modernos de videovigilancia garantiza la protección y optimización de recursos tecnológicos para una operatividad continua. un sistema de videovigilancia energético se divide en estos componentes y sus prácticas técnicas:

- Tecnología PoE permitiendo la trasmisión de energía y datos a través de un solo cable, reduciendo otras fuentes alimentarias externas y optimizadas para el consumo eléctrico de la red.
- Los sensores de imágenes de bajo consumo en las cámaras IP modernas incorporan sensores para operar en condiciones de poca luz, mejorando con la visión nocturna.
- La IA permite que el sistema grabe o porcese los datos en alta resolución para detectar movimientos o anomalías.

2.3.1.10 Gestión de vídeo: monitorización y grabación

Se puede utilizar una variedad de plataformas de software para administrar transmisiones de video. Las plataformas pueden basarse en servidores web integrados en

elementos del sistema (cámaras, servidores de vídeo) o en el uso de un sistema de gestión basado en Windows o tecnología web. A diferencia del software libre las soluciones del software de gestión de video (VMS) operan mayormente bajo licencias comerciales, el costo del sistema se compone en una tasa fija en la plataforma y una licencia por nodo (cámara o fuente de video) validando a través de direcciones MAC del hardware. Como los proveedores suelen estructurar costos adicionales para cubrir el soporte técnico, actualizaciones y aplicaciones complementarias. (García Mata, 2010)

2.3.2 Gestión de seguridad

2.3.2.1 Principios de seguridad industrial y prevención de riesgos laborales

Proteger la salud física y mental del personal dentro de los entornos productivos es el eje de central de la seguridad industrial. Este apartado analiza las pautas esenciales para identificar, evaluar y controlar a tiempo los riesgos derivados de la actividad laboral, transformando la prevención en una práctica sistemática y preventiva. Estos principios minimizan accidentes y enfermedades ocupacionales, así como fomentan una cultura preventiva, el cumplimiento normativo y asegura en condiciones de trabajo dignas y seguras. (Silva Frey, 2021)

La prevención constituye un elemento fundamental para garantizar la protección de la vida, la salud y la integridad de los trabajadores, debido a que implica la identificación de los peligros. Como resultado, se crean condiciones laborales seguras y se disminuye la frecuencia de riesgos en el trabajo. Asimismo, se fortalece la reducción de riesgos y se garantizan condiciones seguras en el ámbito laboral, en concordancia con los fines del derecho laboral y penal para salvaguardar la vida y la salud de los trabajadores. (Organización Internacional del Trabajo, 2022)

2.3.2.2 Prevención como eje central

La prevención es un aspecto clave en la seguridad laboral y en el manejo de los riesgos en el trabajo, ya que incluye el reconocimiento de amenazas, la valoración de riesgos y la implementación de estrategias de control destinadas a prevenir o disminuir los posibles daños que puedan surgir de las condiciones laborales. Hacer de la prevención un pilar en la gestión en el entorno laboral implica establecer procedimientos seguros y protocolos de respuesta, capacitar al equipo humano y promover una cultura organizativa que priorice la salud y el bienestar de los trabajadores. De este modo, se protege al personal, se incrementa la eficiencia,

se reducen los costos relacionados con accidentes y se garantiza el cumplimiento de las normativas establecidas. (Instituto Nacional de Seguridad y Salud , 2023)

La prevención garantiza la protección de la vida, salud e integridad de los trabajadores, ya que supone reconocer los peligros, evaluar el riesgo y controlarlo en las fases de la actividad laboral. Como resultado, se crean condiciones laborales seguras y se disminuye la frecuencia de riesgos en el trabajo. Asimismo, se fortalece la reducción de riesgos y se garantizan condiciones seguras en el ámbito laboral, en concordancia con los fines del derecho laboral y penal para salvaguardar la vida y la salud de los trabajadores. (Silva Frey, 2021)

2.3.2.3 Eliminación del riesgo en su origen

La eliminación del riesgo desde su origen constituye un principio fundamental de la seguridad industrial y la prevención de riesgos laborales, debido a que busca suprimir los peligros antes de que puedan afectar la salud y la integridad de los trabajadores. Esto se logra mediante el diseño de procesos, la sustitución de materiales peligrosos o la automatización de tareas críticas. Al eliminar el peligro de raíz se reduce la probabilidad de accidentes y consolidan entornos de trabajo seguros y sostenibles. (Organización Internacional de Normalización, 2025)

Según Dyreborg et al. (2022), las intervenciones de seguridad orientadas a prevenir accidentes laborales son más efectivas cuando actúan sobre las condiciones que originan el riesgo. Estas abarcan transformaciones a nivel estructural en los ambientes laborales, alteraciones en las leyes y regulaciones, así como la aplicación de controles técnicos y físicos que evitan que los riesgos se presenten antes de perjudicar a los empleados. Por ejemplo, cambios estructurales en las instalaciones, como barreras de seguridad o el perfeccionamiento del diseño de tareas, para erradicar peligros desde su origen y así obtener una prevención más eficaz y sostenible.

2.3.2.4 Sistema de gestión de la seguridad y salud en el trabajo

El 1 de junio de 2017 comenzó a regir para todas las empresas públicas y privadas establecidas en el país, definitivamente, después de varios plazos fijados desde el año 2014, el Sistema de Gestión de la Seguridad y la Salud en Trabajo- SGSST-, en reemplazo del Programa de Salud Ocupacional - PSO-, de acuerdo con las definiciones del artículo 1 de la Ley 1562 de 2012: "Programa de Salud Ocupacional: en lo sucesivo se entenderá como el Sistema de Gestión de la Seguridad y Salud en el Trabajo SGSST. Este Sis- tema consiste en el desarrollo de un proceso lógico y por etapas, basado en la mejora continua y que incluye la política, la

organización, la planificación, la aplicación, la evaluación, la auditoría y las acciones de mejora con el objetivo de anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y salud en el trabajo". (Arnulfo Cifuentes Orlarte, 2017)

En Colombia, el 31 de mayo de 2017, se encontraba en efecto la Resolución 1016 del 31 de marzo de 1989, que delineaba las normas, operatividad y estructura del Programa de Salud Ocupacional. Este programa abarcaba la planificación, organización, implementación y revisión de actividades relacionadas con Medicina Preventiva, Medicina Laboral, Higiene Industrial y Seguridad en el Trabajo, con el objetivo de proteger, mantener y mejorar la salud individual y colectiva de los empleados en sus labores. Estas actividades debían llevarse a cabo de manera integral y con un enfoque interdisciplinario en los lugares de trabajo. (Ministerio de Trabajo y Seguridad Social, 2025)

2.3.2.5 Gestión del riesgo: ¿Concepto rígido o en construcción?

El objetivo del presente escrito es contribuir al análisis de los elementos situacionales y los actores involucrados en la identificación de vulnerabilidades y la formulación de soluciones ajustadas a las necesidades y capacidades de la región latinoamericana. Estas soluciones se pueden lograr a través de la cooperación internacional entre países y organizaciones internacionales, gubernamentales y civiles. En especial, se pretende resaltar el cambio en la conciencia general de los actores, quienes ven la necesidad de protegerse conjuntamente de los riesgos y de las amenazas emergentes, producto de la actual época tecnológica y económica. Solo a través de este tipo de ejercicios de reflexión se hace una contribución sustancial a la formulación y el moldeamiento de sistemas de gestión de riesgo (Yuber Rico Venegas, 2020).

El texto está organizado de manera que se esclarecen las formas de gestión del riesgo y las instituciones e intereses involucrados. En el primer apartado, se hace un recuento teóricodescriptivo de la gestión de los riesgos y de las amenazas a la seguridad de los Estados y las sociedades. Después de haber identificado los conceptos pertinentes, y en concordancia con ellos, se procede a caracterizar y a cuestionar la gobernabilidad y la posibilidad de un nuevo multilateralismo. En el último apartado, se busca en el enfoque basado en procesos el funcionamiento agencial y organizacional de un sistema de gestión de riesgos para América Latina. (Yuber Rico Venegas, 2020)

2.3.2.6 El Departamento de seguridad informática en la empresa

El éxito de la implementación y continuidad del funcionamiento de un departamento de seguridad dependerá del apoyo brindado por la dirección, del personal asignado y su capacitación, y de las herramientas disponibles.

2.3.2.6.1 Los objetivos básicos de esta Unidad son:

- Controlar el acceso y uso de los recursos informáticos de la empresa.
- Detectar e investigar todas las brechas relacionadas con la seguridad e integridad de los sistemas informáticos.
- Asegurar a la dirección que sus recursos informáticos están adecuadamente protegidos y que la empresa cumple con todas las normas internas o legislaciones externas vigentes en materia de seguridad informática.

2.3.2.6.2 El número de personas a asignar a la Unidad dependerá de

- Número de perfiles a gestionar. • Número de ordenadores diferentes a gestionar.
- La complejidad de cada ordenador. ·
- La complejidad del software de seguridad utilizado. ·
- La complejidad de las normas y legislación de seguridad que se deben cumplir.
- Tareas asignadas al dispositivo.

2.3.3 Metodología Scrum

La metodología Scrum en trabajos ágil resultan fundamentales para el desarrollo del software, lo que permite gestionar un proyecto de manera iterativa a través de ciclos cortos llamados Sprints lo que facilita una organización eficiente en la información, priorizando tareas y adaptando de forma flexible los cambios durante todo el proceso de construcción del sistema.

Scrum es un marco de trabajo basado en ciclos cortos e iterativos donde la experiencia el criterio son fundamentales, pero deben completarse con la evidencia empírica para la toma de decisiones. Además, promueve un entorno colaborativo que atiende y comprende a las personas de forma coherente. Todo esto ayuda a minimizar los riesgos del proyecto logrando un equilibrio eficaz entre la explotación de problemas, la entrega continua y la validación constante de resultados. (Coleman et al., 2025)

Los Sprints son fundamentales siendo el motor principal dentro de la metodología scrum, se define por ciclos cortos temporales de duración fija donde un equipo multifuncional transforma los requerimientos en un incremento de producto potencialmente utilizable. Su

objetivo es centrarse en mantener un ritmo de trabajo sostenible, minimizar la incertidumbre del proyecto y permitir inspecciones y adaptaciones continuas. Al limitar el tiempo de cada iteración se fomenta la concentración en objetivos claros, facilitando la entrega de valor constante y el control riguroso de la calidad antes de avanzar hacia la siguiente etapa del desarrollo (Rehkopf, 2026).

Para comprender visualmente la dinámica de trabajo empleada a continuación se presenta la figura que ilustra el ciclo de vida de un sprint. Este esquema detalla las etapas iterativas que estructuran el desarrollo del software, permitiendo una gestión organizada, revisiones periódicas y una mejora continua orientada a cumplir con los objetivos planteados:

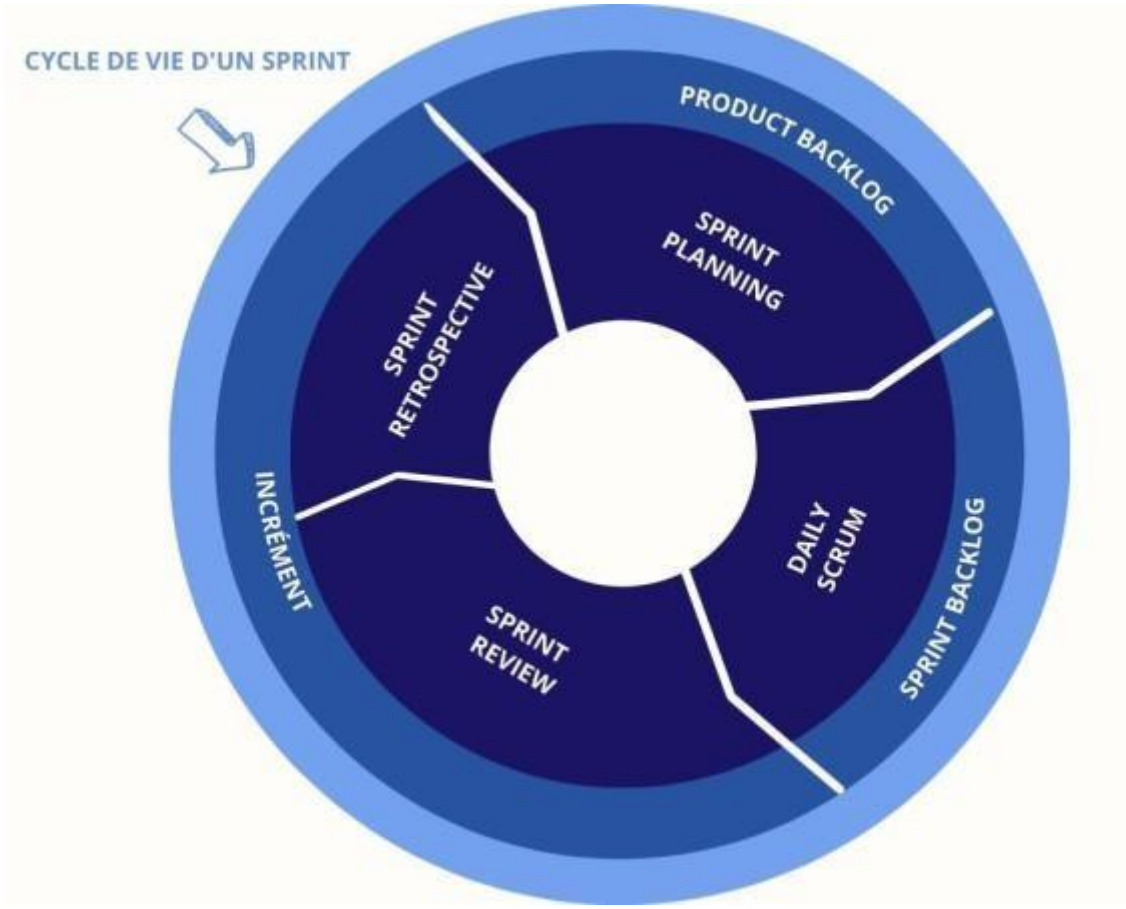


Ilustración 2Ciclos de vida de un Sprint. Fuente: https://www.qrpinternational.fr/blog/glossaire/quest-ce-quunsprint-dans-scrum-definition-etapes-caracteristiques-et-outils/

A continuación, se detalla cada uno de los componentes y fases del ciclo de vida de un sprint según se observa en el esquema:

2.3.3.1 Daily Scrum

El método consiste en organizar una reunión corta - de unos quince minutos - a diario, con la duración máxima expresada en minutos exactos, que tienen lugar a la misma hora cada día. Esta reunión tiene como objetivo principal facilitar la colaboración interactiva entre los miembros del equipo y obtener contestaciones satisfactorias a las tres preguntas fundamentales: ¿Qué hemos hecho?/¿Qué debemos hacer?/¿Qué nos impide hacerlo?, lo que contribuye considerablemente a minimizar el volumen de información necesaria para llevar a cabo un intercambio rápido de mensajes relacionado con el progreso del proyecto actual sin alterar el equilibrio temporal habitual necesario para el funcionamiento del sistema como whole.. (ENIUN, 2025)

Aunque en la práctica los términos «reunión de pie» y «Daily Scrum» suelen utilizarse como sinónimos, son conceptos distintos. La reunión de pie es una expresión genérica que

describe una breve reunión diaria de un equipo para intercambiar actualizaciones sobre su trabajo. Por otro lado, el Daily Scrum es un evento concreto dentro del marco Scrum. La única diferencia entre ambos conceptos es que el Daily Scrum es oficialmente una reunión breve, por lo que la expresión «reunión de pie» se ha adoptado como término habitual para este tipo de reuniones..

Un gran error que cometen muchos es tratar la reunión diaria simplemente como una rutina mecánica. Claro, hay tres preguntas que deben hacerse tanto al presentador como al escuchador (¿Lo lograste ayer? ¿Qué harás hoy? ¿Encuentras alguna impedimento?), pero los objetivos principales son revisar las acciones previstas para este día con respecto al objetivo del ciclo actual y realizar ajustes si hubo dificultades durante la jornada anterior. Al tomar estos en cuenta, la reunión diaria no puede limitarse únicamente a dar información, sino que también debe centrarse en organizar a la squad según estos objetivos para garantizar el éxito del sello.. (Zhezherau, 2025)

Para profundizar en la naturaleza y el propósito del Daily Scrum más allá de su simple mecánica, a continuación se presenta una figura que resume sus principios fundamentales. Este esquema destaca la flexibilidad de la reunión, el enfoque central en el objetivo del sprint y el rol colaborativo de los desarrolladores, elementos clave para mantener la auto-organización y la toma de decisiones ágil dentro del proyecto:

Ilustración 3 Guía de Daily Scrum. Fuente: https://discoveryfast.com/dailyscrum-guia2020/

2.3.3.2 Sprint Review

Esta fase constituye un espacio colaborativo fundamental donde el equipo de desarrollo presente de forma práctica el incremento de producto logrado a los staeholders o interesados.

Más allá de ser una reunión de carácter informal, representa una instancia de inspección altamente valiosa para validar el funcionamiento del sistema, evaluar el cumplimiento de los objetivos planteados y recibir retroalimentación directa. Este intercambio permite ajustar el rumbo desde desarrollo, garantizar la alineación con las expectativas reales de los usuarios y asegurar que las futuras iteraciones respondan de manera precisa a las necesidades del proyecto. (Donetonic, 2022)

2.3.3.3 Sprint Retrospective

La retrospectiva del sprint constituye un evento de análisis fundamental que se lleva a cabo de forma obligatoria al concluir cada ciclo de trabajo. Su finalidad principal es propiciar un espacio de diálogo reflexivo donde los miembros del equipo evalúan detalladamente el desarrollo de las actividades, identificando tanto los aciertos obtenidos como los aspectos susceptibles de optimización de cara a las siguientes iteraciones. Esta práctica de mejora continua resulta vital dentro de la gestión ágil, ya que no solo permite refinar los procesos técnicos y operativos del sistema, sino que también fomenta la cohesión del equipo y la adaptabilidad ante futuros requerimientos del proyecto. (MacNeil, 2026)

Como se ilustra en el diagrama superior, el ciclo de trabajo en Scrum no es lineal, sino un proceso de aprendizaje constante representado gráficamente en forma de infinito. La fase de «Sprint», enfocada en la construcción y el incremento del producto, alimenta directamente a la «Retrospectiva». En este espacio, el equipo se reúne para analizar su desempeño, recopilar datos, decidir acciones de mejora y preparar el terreno, incorporando estos aprendizajes y experimentos de vuelta al inicio del siguiente ciclo.

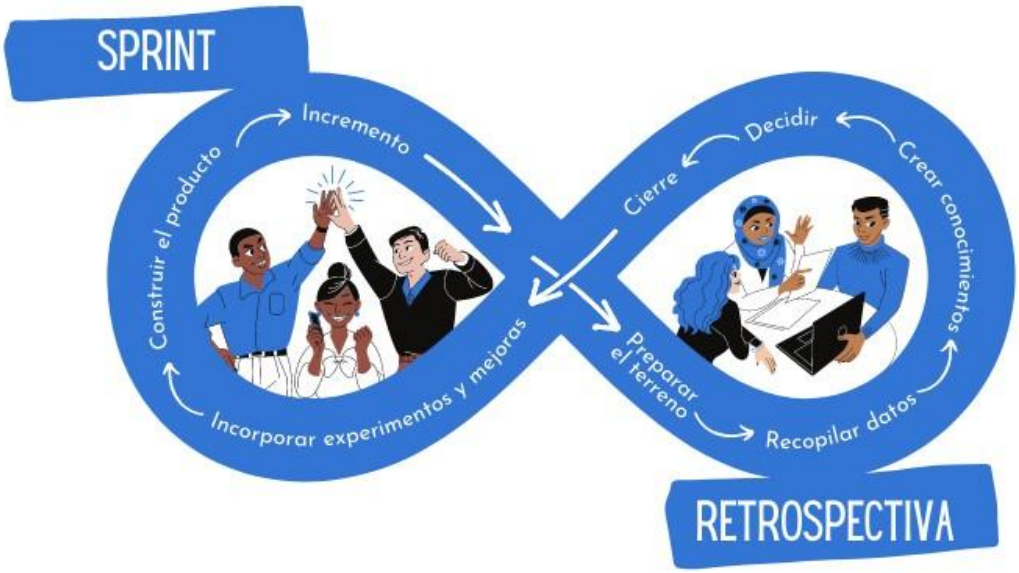


Ilustración 4Diseño de Sprint Retrospective. Fuente: https://www.scrummanager.com/blog/2022/10/sprintretrospective-ejemplo-preparacion-y-puesta-en-practica/

2.3.3.4 Sprint Planning

La reunión de planificación constituye el primer paso para iniciar cualquier ciclo. Su objetivo es establecer y organizar las responsabilidades y las iniciativas que deben llevarse a cabo durante el proceso con la participación de todo el equipo. El periodo de dicha reunión depende de la duración prevista del sello; por lo tanto, si el equipo cuenta con una iteración mensual, el tiempo asignado debe acortarse hasta unas 8 horas. Esta reunión de planificación puede dividirse, en general, en dos partes. La primera parte se centra en el «qué»: el propietario del producto presentará sus intenciones y priorizaciones, y el equipo analizará su viabilidad desde una perspectiva de competencias técnicas y eficiencia. En la segunda fase, el equipo debatirá sobre el «cómo»: cómo conseguirlo, teniendo en cuenta las obligaciones del Sprint Backlog y proponiendo un conjunto específico de enfoques para alcanzar los objetivos planteados.. (Donetonic, 2022)

Como síntesis del marco metodológico aplicado, el diagrama superior ilustra de forma integral el ciclo de vida completo de Scrum en el desarrollo del sistema. Desde la recolección inicial de requerimientos por parte del Product Owner y la planificación colaborativa (Sprint Planning), hasta la ejecución de iteraciones acotadas, las reuniones de seguimiento diario (Daily Scrum), la revisión de resultados (Review) y la evaluación interna (Retrospective), este flujo garantiza una gestión estructurada, transparente y orientada.

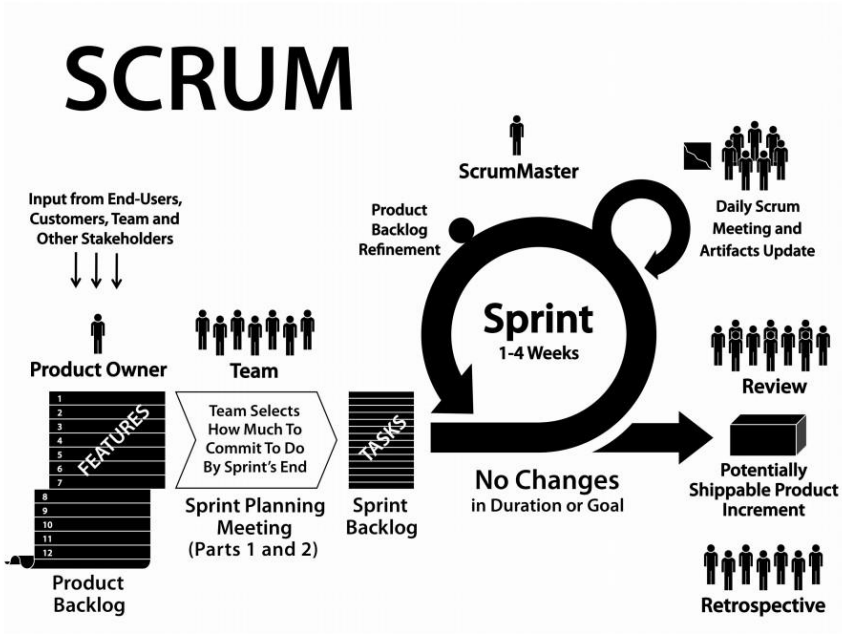


Figure 1. Scrum

Ilustración 5 Flujo general del marco de trabajo Scrum. Fuente: https://testingbaires.com/metodologias-agilesscrum/

2.4 Conclusiones

En teoría el desarrollo muestra la trasformación radical en los sistemas de seguridad de cómo se va evolucionando desde el CCTV hacia los ecosistemas digitales, La IA es un avance para los sistemas NVR y PoE que permiten guardar y visualizar el registro de eventos, comportamientos y anomalías en tiempo real, Las revisiones bibliográficas conforman que la tecnología optimiza la gestión de datos y la eficiencia energética para las demandas de alta disponibilidad y precisión operativa.

Asimismo, demuestran que la implementación de videovigilancia inteligente en el entorno educativo es esencial y productivo para una seguridad constante, La criminología y la ingeniería de tecnología de la información permiten establecer protocolos de prevención para las situaciones de delitos y comportamientos extraños, Por otro lado, un sistema basado con IA para el laboratorio de Electromecánica no solo es necesario para la seguridad de la institución, sino que mejora la transformación digital y sostenibilidad tecnológica en el área educativa.

Sobre el diseño del sistema siguiendo el método PPDIOO: usar el ciclo de vida PPDIOO ayudó a crear una red que es estable y que se puede ampliar. Esto asegura que cada parte tecnológica se elige basándose en su compatibilidad y eficiencia. El diseño lógico que utiliza la segmentación de red (VLAN) garantiza que el tráfico de datos del sistema de videovigilancia no afecte las actividades administrativas de la universidad, logrando así un balance entre la seguridad física y el rendimiento de la infraestructura de TI.

Capítulo III

3 Marco investigativo

3.1 Introducción

El presente capitulo se presentará la metodología para el diseño e implementación del sistema de videovigilancia inteligente en el laboratorio de Electromecánica de la ULEAM Extensión El Carmen. Se fundamenta en recopilar información a través de un enfoque mixto, cualitativo y cuantitativo para proporcionar una documentación rígida. Además, se desarrolla la metodología PPDIOO mostrando las fases del ciclo de vida de la red para cumplir los estándares de la universidad.

3.2 Tipo de investigación

3.2.1 Investigación aplicada

Esta investigación se centra en el conocimiento que se aplica en resolver problemas prácticos y en el entorno social, al destacar este enfoque porque toma la base teórica y la transforma en soluciones, impulsa al proceso ser eficiente y mejora de calidad de los usuarios (Lozada, 2014).

Se utiliza este tipo de investigación porque no solo representa el estudió teórico sobre la IA, sino como una herramienta tecnológica. Al implementar este enfoque en el Laboratorio de Electromecánica de la ULEAM se logró solucionar conceptos importantes de la seguridad del sistema, esto permite que la universidad este protegido con un sistema moderno, mejorando y impulsando a las nuevas tecnologías.

3.2.2 Investigación descriptiva

Esta investigación se compone principalmente en estudiar la descripción, en registros y el análisis de información presente. La actividad esencial es detallar la realidad observada, las etapas desde el principio de definición hasta la recolección de datos y de ultimo el análisis de los resultados para establecer la conclusión (Rodríguez Moguel, 2005).

Esta investigación permitió documentar detalladamente desde la instalación hasta la terminación del proyecto, realizando un diagnóstico en la situación actual del laboratorio de Electromecánica. Se garantiza documentar cada proceso del sistema inteligente para cubrir las necesidades reales de seguridad.

3.2.3 Investigación de campo

Esta metodología consiste en obtener de datos directamente desde el lugar donde ocurren los hechos. Aunque suele asociarse en el estudio de fenómenos en entornos abiertos como su aplicación en laboratorios y otros entornos técnicos donde buscan controlar y comparar los resultados mediante la observación (Pérez León, 2023).

Esta técnica es un pilar importante que permite validar la propuesta en el laboratorio de Electromecánica. Es necesario para documentar el comportamiento de la red, verificar la eficiencia de la tecnología PoE y determinar la ubicación exacta de las cámaras. Además, se aplica la recolección de datos a través de encuesta y entrevista que me brinde datos reales sobre las necesidades de seguridad, facilitando la toma de decisiones basado en la realidad del laboratorio.

3.3 Método(s) de investigación

3.3.1 Hipotético-Deductivo

Este método se define por enlazar el razonamiento lógico con el emperico. Consiste en proponer una serie de hipótesis o teorías para validar o descartar mediante la experimentación de los hechos. Se presenta en ciclo que empieza en la observación, explicación y comprobación de la experiencia y teoría (Pérez, 2024).

Este método es fundamental para este proyecto al implementar un sistema de videovigilancia con IA. Permite mostrar una información clara y eficiente para seguir un orden mostrando la observación de fallas, diseño del sistema y las pruebas técnicas en el laboratorio de electromecánica. Es fundamental pasar de una idea técnica a una solución para el proyecto.

3.3.2 Analítico-Sintético

Este método se complementa por el analítico que permite descomponer un objeto de diversos componentes y propiedades para comprender cada parte, y la síntesis actúa como el proceso inverso integrando para identificar las relaciones generales y característica globales. A través de este método permite entender el sistema real distribuyendo detalladamente las partes y como se entrelaza (Rodríguez Jiménez y Pérez Jacinto, 2017).

Para el sistema de videovigilancia se divide el análisis para el estudio de la infraestructura de la red, el servidor para la IA y la ubicación física de las cámaras en el laboratorio. Para la síntesis se integra los componentes de solución del sistema. Es fundamental para asegurar el software de reconocimiento facial entre la comunicación del hardware y la red, logrando tener un sistema equilibrado y seguro para el funcionamiento.

3.3.3 Estadístico

Se define para procesos sistemático diseñado para el manejo, organización y análisis de datos tanto cualitativos como cuantitativo de la investigación. Principalmente se define por etapas críticas que son la recolección, recuento de información y presentación final. Su objetivo es transformar los datos numéricos en información exacta, permitiendo que los resultados sean tabulados y validados para facilitar la comprensión del estudio (Zamora, 2018).

En este presente estudio utilizaremos un enfoque cuantitativo. Esto nos permitirá analizar eficazmente los datos que obtenemos de encuestas y entrevistas. Queremos facilitar datos de una forma sencilla y clara. De esta forma podremos entender cómo perciben la seguridad las personas de nuestro grupo de estudio. Para lograrlo realizaremos cálculos básicos como calcular promedios y porcentajes. Estos cálculos nos ayudarán a identificar patrones y tendencias en los datos recopilados. Presentaremos los resultados en tablas y gráficos. Esto hará que los resultados sean más fáciles de entender y facilitará decisiones informadas de gestión de seguridad.

3.4 Fuentes de información de datos

3.4.1 Fuentes primarias

En esta investigación se recolecta datos de manera directa para asegurar el diseño del sistema inteligente respondiendo las necesidades reales. Se aplica una encuesta a los estudiantes centrada en el control de acceso y la percepción de vigilancia sobre la seguridad y la eficiencia que existe en el laboratorio de Electromecánica.

3.5 Estrategia operacional para la recolección de datos

Es importante tener información presente y precisa en este entorno, lo que nos facilita este paso a la recopilación de datos. Se centra en obtener información técnica y critica del laboratorio. Se aplica la encuesta a los estudiantes de Electromecánica que utilizan a menudo el laboratorio.

3.5.1 Población

La población del estudio está compuesta por 163 estudiantes que usan el laboratorio de manera directa o indirecta, con el laboratorio de electromecánica de la Universidad Laica Eloy Alfaro de Manabí, en la Extensión El Carmen. Asimismo, el movimiento de eventos de acceso, transmisiones de video y grabaciones digitales generados dentro del entorno de la red común de los laboratorios durante el periodo de evaluación del sistema se considera un conjunto de

datos desde una perspectiva puramente técnica. Para los efectos del análisis de impacto social, utilidad y seguridad, se define a la población humana como:

- Estudiantes: Personas inscritas en clases que usan con frecuencia los talleres y laboratorios de electromecánica.
- Docentes y técnicos: personas que trabajan dando clases prácticas y encargándose de manejar los equipos de laboratorio.
- Personal Administrativo y de Seguridad: Cargo encargado de manejar las tareas logísticas y garantizar la seguridad de los bienes pertenecientes a la institución en el campus.

3.5.2 Técnica de muestreo

En este proyecto se aplicó un método de muestreo aleatorio simple para seleccionar a los estudiantes que tomarían parte en la investigación acerca de la usabilidad, la aceptación y la percepción de seguridad del sistema inteligente de videovigilancia.

Este método asegura que cada uno de los 163 estudiantes que conforman a toda la población del Laboratorio de Electromecánica tenga la misma chance de ser seleccionado para realizar cuestionarios.

La base de datos de los estudiantes que están inscritos en los seminarios es un registro cerrado que solo puede ser conocido por la administración del programa, por lo que se puede asignar a cada estudiante un número que lo identifique.

3.5.3 Tamaño de la muestra

Se aplica una fórmula de cálculo para poblaciones pequeñas (menos de 100.000 personas) con el fin de encontrar el tamaño justo de muestra necesario para representar adecuadamente a un grupo de estudiantes, asegurando que los resultados de las encuestas sean estadísticamente válidos y que el margen de error se mantenga bajo control. La ecuación matemática se define a continuación:

$$n = \frac{Z^2 \cdot p \cdot q \cdot N}{E^2 \cdot (N-1) + Z^2 \cdot p \cdot q}$$

Si los parámetros y criterios estadísticos establecidos para el desarrollo de este estudio tecnológico cumplen:

- N (población total): 163 estudiantes que están legalmente inscritos y que usan con regularidad las instalaciones del laboratorio electromecánico.
- Z (nivel de confianza): 1.96, que representa un nivel de confianza del 95%, algo que se sigue como norma en proyectos de ingeniería y ciencias sociales.
- E (margen de error tolerable): 0,05, que es el porcentaje máximo de error que se permite al generalizar los resultados.
- P (probabilidad de éxito o ingreso): 0,50, lo que significa que hay un 50% de diversidad porque no hay estudios previos similares en esta facultad.
- Q (probabilidad de error): 0,50, se calcula con el complemento de p ($1 - p = 0,50$).

Planteamiento inicial:

$$n = \frac{(1.96)^2 \cdot 0.5 \cdot 0.5 \cdot 163}{(0.05)^2 \cdot (163 - 1) + (1.96)^2 \cdot 0.5 \cdot 0.5}$$

Resolución de potencias cuadráticas:

$$n = \frac{3.8416 \cdot 0.25 \cdot 163}{0.0025 \cdot 162 + 3.8416 \cdot 0.25}$$

Multiplicación de los componentes del numerador y denominador:

$$n = \frac{156.5452}{405 + 0.9604}$$

Adición de los términos del denominador:

$$n = \frac{156.5452}{1.3654}$$

Resultado de la división:

$$n = 114.65 \approx 115$$

Según el desarrollo estadístico mostrado, se estableció que el número mínimo de participantes necesario fue de 115 estudiantes. El uso de herramientas para recoger datos, como encuestas que miden la percepción del nivel de seguridad, usabilidad y aceptación de un sistema

basado en inteligencia artificial, aplicadas a un grupo seleccionado al azar, permitirá obtener información con un nivel de rigor científico que cumple con las regulaciones establecidas en el título.

3.5.4 Análisis de las herramientas de recolección de datos a utilizar

3.5.4.1 Encuesta – Entrevista - Observación / Otras

El presente proyecto contempla la recopilación de datos mediante el análisis de encuesta a los estudiantes de la carrera de Electromecánica y entrevista al docente con el fin de evaluar la percepción de seguridad actual, identificar los protocolos de acceso y reconocer la vulnerabilidad operativa del laboratorio. Para garantizar la validez estadística se determinó una muestra de 115 estudiantes y un docente para fundamentar la técnica de requisitos del sistema de videovigilancia inteligente propuesto.

3.5.4.2 Estructura de lo(s) instrumento(s) de recolección de datos aplicados

(Formato de entrevista y encuesta)

Para analizar con precisión el problema de seguridad en el laboratorio de Electromecánica se diseño este instrumento de recolección de datos con el propósito de cuantificar las debilidades y la frecuencia de incidentes. Ayudaría a derivar las consecuencias de seguridad y vulnerabilidad en horarios no laborables.

Componentes	Preguntas abiertas	Preguntas cerradas
Patrones de uso	¿Cuentan con reportes de ingreso al laboratorio?	¿Con que frecuencia utiliza el laboratorio de electromecánica a la semana? • Diariamente • 2 a 3 veces a la semana • Una vez por semana • Casi nunca
Protocolo de seguridad	¿Existe en la actualidad un protocolo oficial para el control de ingreso de los estudiantes?	¿Cuánto tiempo permanece en el laboratorio por práctica? • Menos de 1 hora • Entre 1 y 2 horas • Más de 2 horas

Capacitación técnica	¿Han importado capacitaciones sobre la seguridad del laboratorio en este ciclo académico?	¿Ha recibido usted alguna charla, inducción o capacitación sobre las normas de seguridad y el cuidado de las instalaciones del laboratorio? • Si

Componentes	Preguntas abiertas	Preguntas cerradas
		• Muy poco • No
Eficacia del registro	¿Considera que el registro manual actual es un método seguro para controlar el ingreso y salida de los estudiantes?	¿Considera que existe un control estricto para que se respeten los horarios de entrada y salida asignados? • Si • A veces • No
Necesidad tecnológica	¿Considera una mejor opción implementar un sistema de videovigilancia inteligente en el laboratorio?	¿Considera importante implementar un sistema de video vigilancia inteligente? • Muy importante • Importante • Poco importante • Nada importante
Impacto de la IA	¿Cree que se reduciría los incidentes en el laboratorio con un sistema de inteligencia artificial?	¿Crees que el uso de Inteligencia Artificial para monitorear el laboratorio reducirá los riesgos de seguridad? • Si • Probablemente • No creo que haya diferencia

Percepción de seguridad	¿Qué considera sobre la propuesta de un sistema inteligente para facilitar y agilizar el acceso del laboratorio?	¿Considera que al implementar este sistema de video vigilancia se siente más seguro? • Si • No • No estoy seguro
Componentes	Preguntas abiertas	Preguntas cerradas
Capacidad de respuesta	¿Cree que las medidas actuales permiten la rapidez de intervenir en algún incidente?	Ante una dificultad de riego en el laboratorio, ¿crees que el encargado se entera con la rapidez necesaria para intervenir? • Si • No • Tal vez

Tabla 1 Estructura de recolección de datos

3.5.5 Plan de recolección de datos

El presente plan de recolección de datos constituye una fase fundamental para el desarrollo del proyecto, permitiendo visualizar las vulnerabilidades existentes en el laboratorio de Electromecánica. Se asegura la obtención de información estructurada y transparente la cual será presentada a la Universidad Laica Eloy Alfaro de Manabí Ext El Carmen. Este proceso es para validar los requerimientos técnicos y garantizar la solución de la propuesta con las necesidades reales de seguridad en el entorno académico.

CRONOGRAMA DE ACTIVIDADES			
TÉCNICA	**RESPONSABLE**	**ENFOCADO**	**PERIODO DE EJECUCIÓN**
Entrevista	Miller Vera	Docente	
Encuesta	Miller Vera	Estudiantes de Electromecánica	09-06-2026 / 19-06-2026
Tabulación de datos	Miller Vera	Resultados obtenidos	20-06-2026

Tabla 2 Cronograma de instrumentos

3.6 Análisis y presentación de resultados

En este análisis se aplicará una investigación de enfoque mixta para garantizar los resultados obtenidos. Principalmente la cuantitativa mediante la encuesta esto permite medir la magnitud del problema, mientras la cualitativa para la entrevista y adicional la observación de campo proporcionando la descripción necesaria para identificar las vulnerabilidades especificas en la gestión del Laboratorio de Electromecánica. Así se mostrarán resultados fundamentales y aceptables en la propuesta de videovigilancia.

3.6.1 Tabulación y análisis de los datos (según encuesta y/o resultado(s) obtenidos de la(s) entrevistas, etc.)

Entrevista

El proceso de entrevista se aplicó al administrador y docente de la carrera de Electromecánica con el propósito de obtener una perspectiva técnica y administrativa sobre la situación actual del laboratorio. Esta técnica permitió identificar las necesidades prioritarias, protocolos de vigilancia y los puntos críticos de vulnerabilidad, proporcionando información de primer mano esencial para fundamentar el diseño e implementación de la propuesta del proyecto.

Preguntas	Coordinador	Docente	Análisis
¿Cuentan con reportes de ingreso al laboratorio?	No existe, en si cada docente lleva el control de quien ingresa al laboratorio por la lista de asistencia.	Actualmente no se lleva reportes solo con la lista de asistencia de cada horario de clases.	Ambos indican que no existe un reporte de ingreso, ingresan por el horario de clases.
¿Existe en la actualidad un protocolo oficial para el control de ingreso de los estudiantes?	No, solo el control de uso dependiendo del horario de clases.	No existe un protocolo de control para los estudiantes, cada uno ingresa al horario de clases.	Ambas respuestas son negativas al no contar con protocolos de ingresos.
¿Han importado capacitaciones sobre la seguridad del laboratorio en este ciclo académico?	No, cada docente al iniciar los primeros niveles se encarga de detallar los cuidados a los equipos de trabajo.	Se explica en las primeras clases el cuidado de su entorno de estudio.	Coinciden que las capacitaciones cada docente en primera clase explica el cuidado de sus equipos.

¿Considera que el registro manual actual es un método seguro para controlar el	No es método totalmente seguro, porque cada horario ingresa los estudiantes y	No es seguro porque si esta desocupada el aula ingresa cualquier estudiante.	Se aborda el problema de ingreso de cualquier personal.

Preguntas	Coordinador	Docente	Análisis
ingreso y salida de los estudiantes?	mientras no ocupe el aula pueden ingresar		
¿Considera una mejor opción implementar un sistema de videovigilancia inteligente en el laboratorio?	Considero un éxito porque permite un monitoreo y novedades de alertas en tiempo real.	Seria una medida positiva para controlar, mantener y prevenir problemas en el laboratorio.	Demuestran el mismo interés de importancia del sistema de videovigilancia inteligente.
¿Cree que se reduciría los incidentes en el laboratorio con un sistema de inteligencia artificial?	Si, con un sistema de vigilancia constante registra y alerta cada movimiento inadecuado en el laboratorio.	Si esta herramienta reduciría los incidentes para prevenir y evitar los incidentes.	Coinciden que un sistema inteligente ayudaría a reducir incidentes en el laboratorio.
¿Qué considera sobre la propuesta de un sistema inteligente para facilitar y agilizar el acceso del laboratorio?	Considero necesario para la infraestructura y un control de acceso seguro, optimizando los recursos.	Resulta sumamente beneficiosa para garantizar que solo estudiantes ingresen y un buen control.	Ambos mencionan que es necesario un sistema inteligente para el ingreso adecuado de clases.

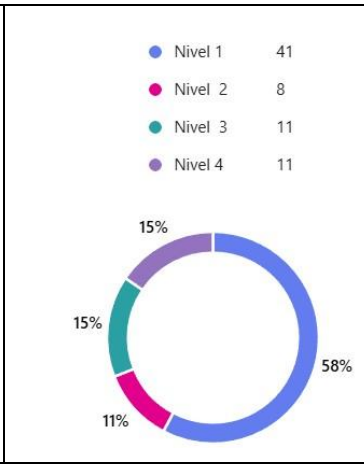
¿Cree que las medidas actuales permiten la rapidez de intervenir en algún incidente?	Realmente no, la gestión es lenta porque el control es manual.	No es rápida, solo depende que estemos en el aula para identificar al responsable.	Ambos coinciden que las medidas actuales son insuficientes.
¿Considera que al implementar un sistema inteligente impulsaría un mayor cuidado y	Definitivamente al saber que sus acciones están siendo monitoreadas será mucho más	Si ayuda bastante para recordar los valores de lo que utilizan, una responsabilidad para los estudiantes.	Sus respuestas no se justifican por la seguridad física, sino también promover la ética y cuidado de sus
Preguntas	**Coordinador**	**Docente**	**Análisis**
responsabilidad entre los estudiantes?	conscientes de sus actos.		herramientas de trabajo
¿Considera que un sistema de videovigilancia inteligente permite prevenir daños, usos indebidos o situaciones de riesgos?	Si es una ventaja con un monitoreo se puede detectar irregularidades ante daños o cualquier situación.	Por supuesto, el sistema detectaría un uso inadecuado para prevenir o evitar estas situaciones.	Coinciden que un sistema inteligente ayudaría a prevenir cualquier evento.

Tabla 3 Análisis de datos de la entrevista

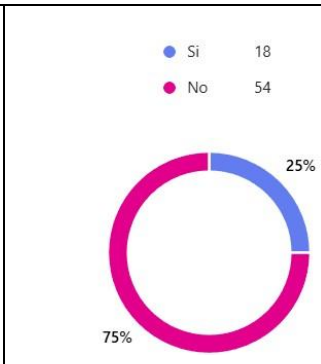
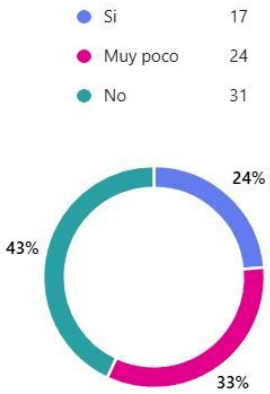
3.6.1.1 Encuesta

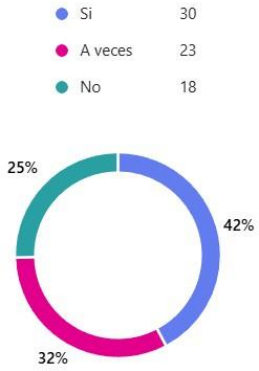
Para el levantamiento de información cuantitativa se aplicó la encuesta con una muestra de 113 estudiantes de la carrera de Electromecánica, seleccionados por su frecuente uso de la instalación. El objetivo fue conocer el estado actual de la seguridad, evaluar el riesgo y determinar las necesidades operativas para garantizar una propuesta de videovigilancia eficiente.

Preguntas	Grafico	Análisis

Seleccione el nivel de educación		Se observa una participación de estudiantes de Nivel 1 con un 58% lo que indica mayor parte de la muestra, mientras el nivel 2 y 3 se mantienen equitativa con un 15%.

Preguntas	Grafico	Análisis
¿Con que frecuencia utiliza el laboratorio de electromecánica a la semana?		El 49% indica que casi nunca utilizan el laboratorio, solo el 26% lo hace una vez por semana lo cual sugiere una baja frecuencia de uso.
¿Cuánto tiempo permanece en el laboratorio por práctica?		Con un 41% permanecen menos de 1 hora en el laboratorio y el 32% dedica más de 2 horas a sus prácticas.

¿Conoce la existencia de un protocolo para el control de ingreso al laboratorio?		Existe un desconocimiento sobre los protocolos de seguridad con un 75% y el 25% que si está al tanto de estas normas.
¿Ha recibido usted alguna charla, inducción o capacitación sobre las normas de seguridad y el cuidado de las instalaciones del laboratorio?		En la capacidad en seguridad el 43% no ha recibido ninguna charla, mientras el 33% si haber recibido muy poca información.

Preguntas	Grafico	Análisis
¿Considera que existe un control estricto para que se respeten los horarios de entrada y salida asignados?		Lo del control de horarios con un 42% crees que si existe un control estricto y el 32% cree que a veces.
¿Considera importante implementar un sistema de video vigilancia inteligente?		La existencia de alta valoración es positiva con el 43% considera necesario la implementación del sistema de videovigilancia inteligente.

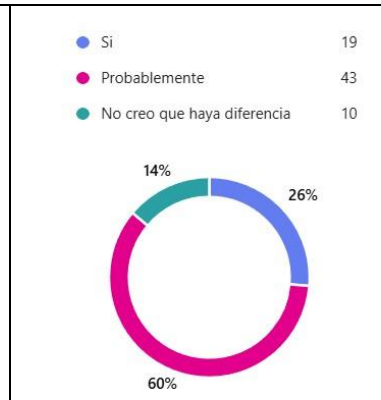
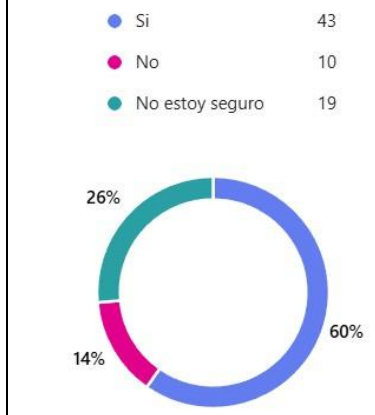
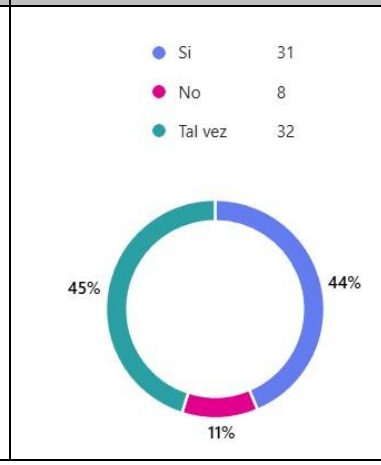
¿Crees que el uso de Inteligencia Artificial para monitorear el laboratorio reducirá los riesgos de seguridad?		La confianza en la IA es notable lo que el 60% opina que probablemente reducirá los riesgos y el 26% está convencido que sí.
¿Considera que al implementar este sistema de video vigilancia se siente más seguro?		Un 60% afirma que se sentiría más seguro y el 26% se mantiene neutral.
Preguntas	**Grafico**	**Análisis**
Ante una dificultad de riego en el laboratorio, ¿crees que el encargado se entera con la rapidez necesaria para intervenir?		Un 45% cree que el encargado se entera con rapidez, pero el 44% responde con tal ves lo que evidencia una incertidumbre.

Tabla 4Análisis de resultado de Encuesta

3.7 Introducción

En este capítulo se detalla el diseño y estructura del sistema inteligente de videovigilancia específicamente en los equipos para la detección y procesamiento de datos. El objetivo se centra en fortalecer la seguridad del Laboratorio mediante cámaras de alta resolución con algoritmos de inteligencia artificial para una supervisión automática. A través de este sistema se busca reducir los riesgos de perdida y daño, también optimizar la gestión del

entorno educativo con vigilancia continua y garantizando la integridad de los activos académicos.

3.7.1 Presentación y descripción de los resultados obtenidos

3.7.1.1 Análisis de resultados

- Respecto al uso de espacio en la pregunta 3, se determinó que el 41% de los estudiantes permanece menos de una hora en el laboratorio durante sus prácticas.
- El control de horario de la pregunta 6, el 42% indican que los horarios de entrada y salida si son respetados.
- En la percepción de seguridad de la pregunta 9, un 60% manifiesta que se sentirían más seguro.

3.7.1.2 Interpretación de resultados

- Relación entre la frecuencia de uso y ausencia de reportes: El análisis de los datos de los estudiantes mantiene un horario de menos una hora de practicas con un 41% lo que gestiona un mecanismo formal de registro[AM1] . Mientras en la entrevista (pregunta 1) menciona que al depender únicamente de la asistencia presencial del horario es insuficiente para documentar la ocupación real del espacio académico.
- Respeto de horarios y inseguridad de registro manual: En la encuesta los estudiantes indican un 42% si respetan las instalaciones. Mientras en la entrevista (pregunta 4) se dice que el registro manual no es un método seguro para permitir el acceso de entrada y salida de las personas.
- Seguridad y propuesta: Existe una alineación entre los estudiantes y la visión de la institución. La mayoría de los encuestados con un 60% mencionan una necesidad de mayor protección en el aula con un sistema inteligente. Lo que respalda la entrevista (pregunta 7) que afirman una necesidad de implementar un sistema de videovigilancia inteligente.

3.7.2 Informe final del análisis de los datos (conclusiones para el marco investigativo)

Aquí tienes el texto corregido y pulido según todas las observaciones planteadas en los comentarios, mejorando la redacción de la tercera sección para que resulte clara, fluida y precisa

Los datos recolectados durante la investigación permitieron confirmar las vulnerabilidades actuales del laboratorio de Electromecánica y la necesidad de intervenir. Los resultados obtenidos a través de entrevistas y encuestas reflejan una falta de control que resulta ineficaz para garantizar la trazabilidad de los ingresos, lo que deja expuesto el laboratorio al uso de personas no autorizadas en momentos de baja supervisión.

La comunidad estudiantil respalda la necesidad de modernizar la instalación mediante un sistema inteligente, sintiéndose más segura con la integración de herramientas de videovigilancia. Esta tecnología no es solo una cuestión de seguridad física, sino también una oportunidad de mejoramiento y práctica para futuros proyectos.

En definitiva, el análisis pone de manifiesto la urgencia de reemplazar los métodos tradicionales por un sistema avanzado. Dicha implementación no solo cubrirá las brechas en el control de identificación, sino que también mejorará la calidad y seguridad del entorno educativo. Asimismo, permitirá una gestión del laboratorio más transparente a través de procesos proactivos capaces de prevenir incidentes y fomentar un uso más eficiente de los recursos valiosos de la institución.

Capítulo IV

4 Marco propositivo

4.1 Descripción de la propuesta

El objetivo del proyecto es diseñar y desarrollar un programa de software de visión artificial para el Laboratorio que permita identificar a las personas que entren en él. El resultado final previsto es un sistema que sustituya el control de acceso manual por uno digital, de modo que se pueda registrar y archivar la entrada de cada persona. Para el desarrollo de este proyecto se ha elegido el enfoque ágil de Scrum, que permite planificar iteraciones, priorizar y comprobar el progreso, así como hacer ajustes constantes. El propio sistema es un conjunto de algoritmos que procesa imágenes de vídeo para identificar a los visitantes del Laboratorio y garantizar que se haya autorizado su entrada.

4.2 Determinación de recursos

El desarrollo de un programa de software para la construcción de una cámara virtual es el objetivo de esta propuesta. Es necesario elegir hardware y software tecnológicamente avanzados que garanticen el correcto funcionamiento del sistema de visión artificial. El ordenador debe poseer todas las cualidades necesarias para trabajar con imágenes en video y realizar los cálculos requeridos por los modelos entrenados en Roboflow. También deben seleccionarse sistemas de captura de imágenes y configuraciones de software compatibles con la estabilidad del programa en el laboratorio.

Se utilizará Python como lenguaje de programación general para escribir código utilizando el entorno de desarrollo de software Visual Studio. Asimismo, el proceso de diseño del software se analizará mediante una prueba de comportamiento (behavior-driven development). Este enfoque permitirá evaluar si las condiciones del trabajo se corresponden con la realidad. Los paquetes de python, los intérpretes y otros programas mencionados constituyen una base sólida sobre la que se construirá todo el proyecto. La elección de estas tecnologías garantiza resultados excelentes y automatización de la instrucción y el funcionamiento del sistema.

4.2.1 Humanos

La propuesta de esta idea radica en desarrollar un programa informático denominado «Software de Visión Artificial». Por consiguiente, para llevar a cabo dicha tarea, así como para garantizar el éxito del proceso, es necesario comprender qué dispositivos se utilizarán para que

el funcionamiento del Software de Visión Artificial se adapte al mejor nivel posible. Además, para crear dicho software y analizar su funcionamiento, hay que identificar las responsabilidades y establecer las funciones específicas de cada persona implicada en el proyecto. Los puestos más importantes relacionados con este tipo de trabajo son las siguientes figuras profesionales:

Cantidad	Nombre	Rol	Actividad	Tiempo estimado
1	Ing. Bladimir Mora	Coordinador de la carrera.	Gestión operativa del software en el laboratorio, control de accesos, equipos del funcionamiento diario y soporte local.	1 hora
1	Ing. Bladimir Mora	Tutor de tesis	Responsable del proceso de revisión.	16 horas
1	Miller Vera	Programadora	Encargada de la recolección de datos y del desarrollo del sistema de detección.	120 horas
153	Estudiantes	Encuestados	Se aplicaron encuestas a los estudiantes de la carrera de electromecánica.	1 hora por estudiante

Tabla 5 Recursos Humanos

Como se detalla en la tabla la distribución de los recursos humanos establece una información clara entre la ejecución técnica del desarrollo y la supervisión institucional. Los roles aseguran no solo la correcta programación de la arquitectura y el entrenamiento de los modelos de inteligencia artificial, sino también el respaldo metodológico y la futura operatividad del software dentro de las instalaciones de la ULEAM.

4.2.2 Tecnológicos

Para el diseño, desarrollo, entrenamiento y despliegue del sistema de visión artificial en el Laboratorio, se ha seleccionado un conjunto específico de herramientas tecnológicas que garantizan un rendimiento óptimo, escalabilidad y precisión en el control de accesos. Estas tecnologías se dividen en los siguientes componentes:

4.2.3 Entornos de Desarrollo y Lenguaje de Programación:

Como núcleo del sistema se utiliza el lenguaje Python, elegido por su versatilidad, su amplia comunidad y su potente ecosistema enfocado en inteligencia artificial y análisis de datos. Como entorno de desarrollo integrado (IDE) principal se emplea Visual Studio, el cual facilita la escritura, depuración y organización estructurada del código fuente y de los scripts encargados de procesar la transmisión de vídeo.

Para esquematizar la interacción lógica entre el lenguaje base, el entorno de programación y los módulos operativos del software dentro del laboratorio de la ULEAM, se presenta el siguiente diagrama conceptual de arquitectura:

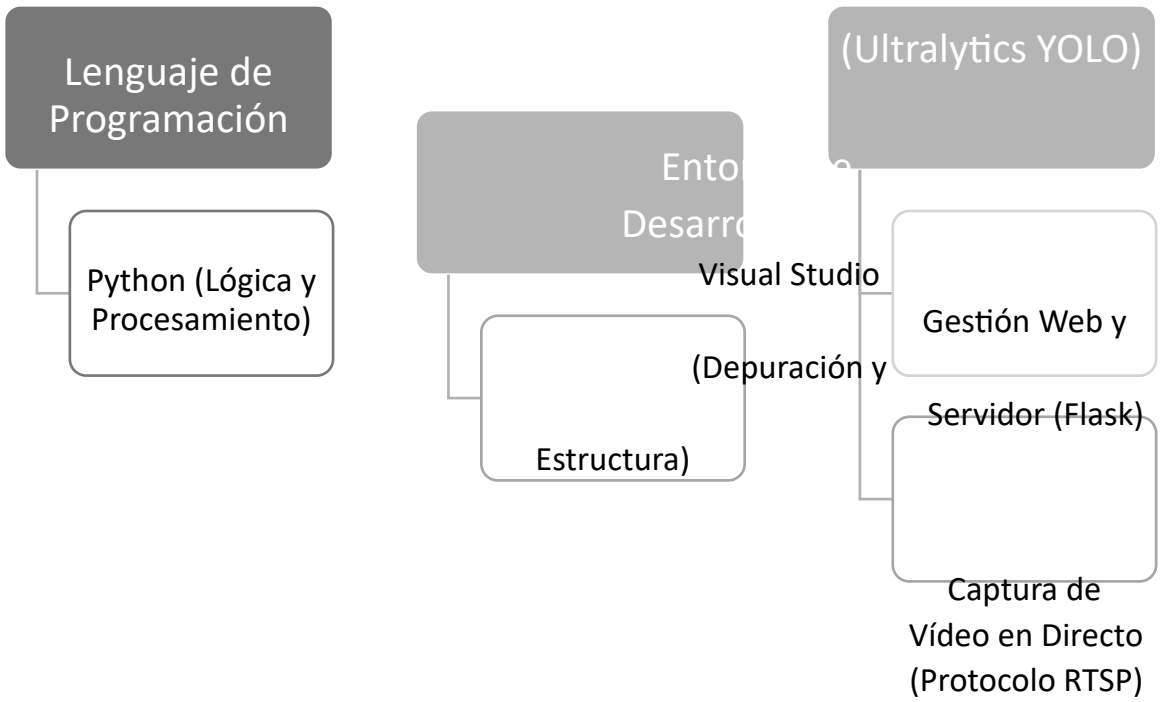


Ilustración 6 Diagrama de arquitectura del entorno de desarrollo y componentes tecnológicos centrales. Fuente: Elaboración propia (2026).

Como se visualiza en el esquema anterior, el Python como núcleo lógico y Visual Studio como plataforma de desarrollo estructurado permite centralizar la gestión operativa del sistema de videovigilancia. Esta arquitectura modular no solo optimiza la escritura, depuración y

mantenimiento del código fuente, sino que establece una base tecnológica sólida, limpia y escalable. Gracias a esta integración el sistema garantiza un flujo de trabajo eficiente para ejecutar de manera simultánea los algoritmos de detección de objetos, la interfaz web y la captura de vídeo en directo, asegurando un rendimiento óptimo y una alta fiabilidad durante la supervisión continua del laboratorio.

4.2.3.1 Plataforma de Inteligencia Artificial y Visión Computacional:

Para la gestión, etiquetado y entrenamiento de los modelos de detección y reconocimiento de rostros o personas se hace uso de Roboflow. Esta plataforma en la nube optimiza el flujo de trabajo de visión artificial, permitiendo preparar los conjuntos de datos, aplicar aumento de datos (data augmentation) y exportar los modelos entrenados listos para su integración local.

Para ilustrar de manera esquemática el ciclo de procesamiento que realiza esta plataforma en la nube, se presenta el siguiente esquema:

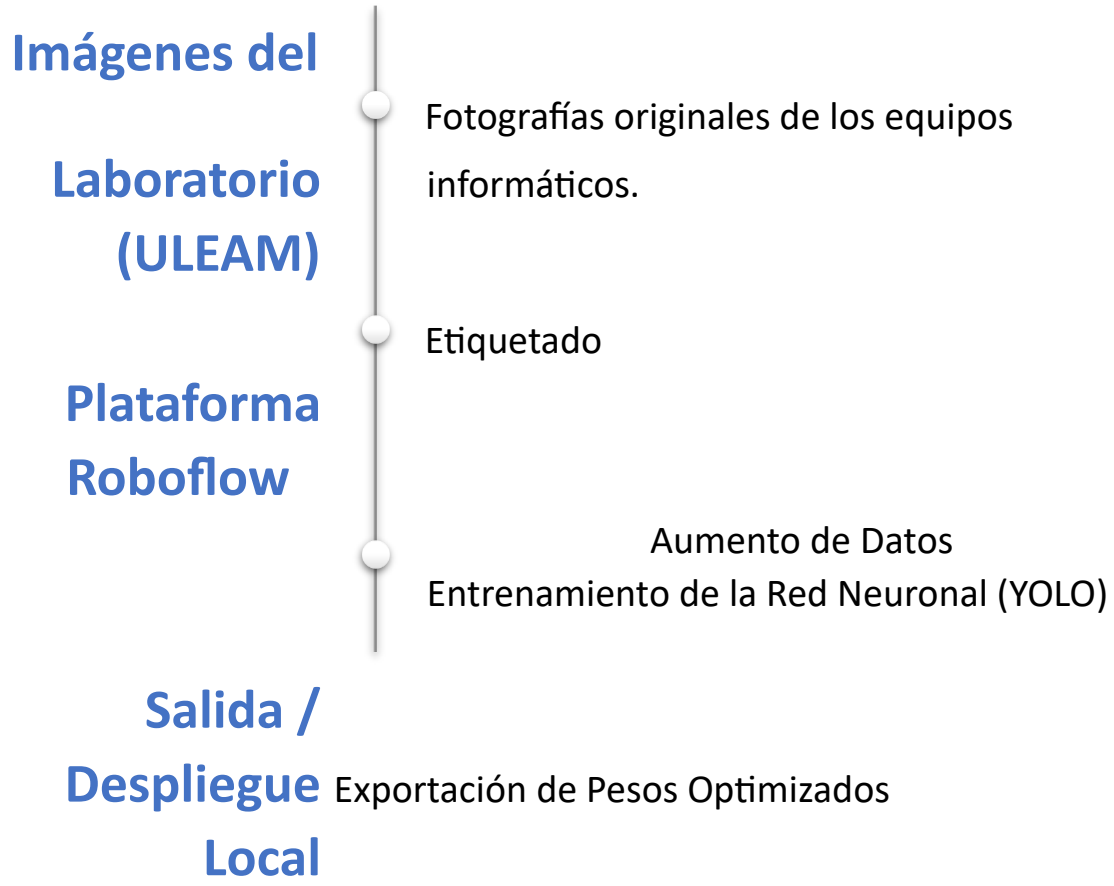


Ilustración 7 trabajo y entrenamiento en la plataforma. Fuente: Elaboración propia (2026).

Como se visualiza en el esquema anterior la integración de Roboflow dentro de la arquitectura del proyecto estandariza cada etapa del desarrollo del modelo de IA. Desde la carga inicial de las imágenes del laboratorio de la ULEAM y su respectivo etiquetado, hasta la aplicación de técnicas de aumento de datos para mitigar problemas de iluminación, la plataforma gestiona el entrenamiento de forma automatizada. Este proceso culmina con la exportación de los pesos optimizados del modelo, garantizando que el sistema cuente con una base neuronal precisa y lista para operar en el entorno local.

4.2.3.2 Metodología de Pruebas y Calidad:

Con el fin de asegurar que el software cumpla con los requerimientos funcionales esperados y funcione de manera predecible, se implementa un enfoque de desarrollo guiado por el comportamiento (BDD). Esto permite estructurar casos de prueba legibles tanto para el equipo técnico como para los evaluadores validando las reglas de acceso del laboratorio.

Para esquematizar visualmente el ciclo de validación de los escenarios de comportamiento dentro del sistema de monitoreo de la ULEAM, se presenta el siguiente diagrama conceptual:

Escenario de Negocio	**Acción del Sistema (Cuándo)**	**Resultado Esperado (Entonces)**
Dado que el equipo está activo en el laboratorio	Cuando la cámara deja de detectarlo por 3 imágenes consecutivos	El sistema confirma la ausencia y registra la alerta en la base de datos.

Ilustración 8 Diagrama de flujo del modelo de pruebas. Fuente: Elaboración propia (2026).

Como se visualiza en el esquema anterior, la metodología BDD establece un puente de comunicación directo entre los requerimientos del usuario y la lógica de programación del backend. Al estructurar las pruebas bajo un formato de especificación ejecutable, se garantiza que cada regla operativa como la confirmación de la presencia de los equipos en el laboratorio y el disparo correcto de las alertas ante anomalías sea rigurosamente validada. Este enfoque sistemático no solo reduce el margen de fallos lógicos, sino que asegura que la plataforma cumpla con los estándares de robustez, confiabilidad y calidad técnica exigidos para la supervisión automatizada de las instalaciones.

4.2.3.3 Infraestructura de Hardware

Se requiere una computadora o servidor local con capacidad de procesamiento gráfico y de cálculo adecuada para soportar la ejecución continua de los modelos de visión artificial, además de una cámara o sistema de captura de vídeo estratégicamente ubicado en el ingreso al recinto para garantizar una óptima iluminación y visibilidad.

Para ilustrar la distribución física y la interconexión de los componentes de hardware que conforman la infraestructura del sistema, se presenta la siguiente ilustración:

Ilustración 9 interconexión de la infraestructura de hardware y captura de vídeo. Fuente: Elaboración propia (2026).

Como se visualiza la infraestructura de hardware se compone de elementos físicos clave que operan de manera sincronizada. En primer lugar la Cámara de Vídeo / IP se encuentra situada estratégicamente en el acceso al Laboratorio de la ULEAM, capturando el flujo visual bajo condiciones óptimas. Esta información se transmite mediante el Flujo RTSP (Red Local) hacia la Servidor / Computadora Local la cual cuenta con la potencia de cálculo necesaria para ejecutar los modelos de visión artificial y el backend en Python, garantizando una supervisión estable, continua y libre de interrupciones técnicas para los operadores.

Cantidad	Recurso	Descripción y Requisitos
1	Computadora	Utilizada para el desarrollo y ejecución del software. Requisitos: Procesador Intel Core i5, 8 GB de RAM, 6 GB de almacenamiento libre.
1	Visual Studio Code	Entorno de desarrollo integrado (IDE) para C#

1	XAMPP v8.0.30	Es necesario contar con espacio disponible en el disco duro (mínimo 85 MB), 256 MB de memoria RAM y un procesador Pentium o de mayor capacidad. Versión 8.0.30 / PHP 8.0.30
1	Conexión a Internet	Es esencial para el correcto funcionamiento del sistema. Se sugiere una velocidad de conexión que esté entre 8 y 10 Mbps.
1	Servidor HP PROLONT	Esencial para gestionar y distribuir información de forma eficiente.
1	Roboflow	Plataforma integral de visión por computadora diseñada para que desarrolladores y empresas gestionen todo el ciclo de vida de sus modelos de Inteligencia Artificial

Tabla 6 Recursos tecnológicos

4.2.4 Económicos (presupuesto)

Para la ejecución y puesta en marcha del sistema de visión artificial en el Laboratorio se ha realizado una estimación de los recursos económicos necesarios. Esto incluye la valoración de los equipos de hardware disponibles, tiempo y otras herramientas así como los costos operativos asociados al desarrollo del software. A continuación, se detalla el presupuesto estimado del proyecto en la siguiente tabla:

Cantidad	Descripción	Precio U.	Subtotal
1	Cable Utp Dahua Dh-Pfm9201-6un Cat6 305mt 100% Cu Int	$113.00	$113.00
1	Extensor Hdmi Por Cable De Red Hasta 60mt	$15.90	$15.90
1	Cámara	$70,00	$70,00
1	NVR Hikision DS-2CD1123G2-LIU 2MP PoEcom audio y luz hibrida	$130,00	$130,00
384	Horas De Trabajo	$5	$1,920
1	Computadora	$800	$800

TOTAL GENERAL	**Total**	3,048.90

Tabla 7 Recursos Económicos

Como se puede observar en la tabla el desglose financiero refleja una inversión equilibrada y realista para la materialización del sistema de monitoreo en el laboratorio de la ULEAM. Las horas de desarrollo e ingeniería concentran la mayor parte del presupuesto debido al esfuerzo técnico invertido en el diseño de los algoritmos de inteligencia artificial, los costos asociados al hardware como el cableado UTP, los extensores y la cámara de seguridad representan recursos indispensables pero accesibles. Esta estimación económica demuestra que el proyecto no solo es viable desde una perspectiva estrictamente técnica y operativa, sino también financieramente sostenible, optimizando los recursos disponibles para garantizar una solución de seguridad automatizada de alto impacto y bajo coste de implementación.

4.3 Etapas de acción para el desarrollo de la propuesta (software)

Llevar a cabo el desarrollo de este sistema de visión artificial requirió seguir una ruta de trabajo organizada, donde cada paso se planificó de forma metódica para garantizar que el software funcionara de manera estable en el Laboratorio. En lugar de improvisar dividimos el proceso en etapas claras alineadas con los ciclos de Scrum permitiendo construir, probar y ajustar el programa iterativamente.

Todo comenzó con la fase de análisis y levantamiento de requerimientos donde definimos exactamente qué necesitaba el sistema para identificar los accesos de forma automatizada. Posteriormente, pasamos al diseño de la arquitectura lógica y a la configuración de las herramientas tecnológicas como la preparación de los conjuntos de datos en Roboflow para entrenar los modelos de inteligencia artificial. Con el núcleo del sistema programado en Python mediante Visual Studio, avanzamos hacia las etapas de integración y validación, asegurándonos de que cada funcionalidad cumpliera con las expectativas del proyecto a través de pruebas guiadas por comportamiento (BDD). De este modo, cada etapa representó un avance seguro hacia la solución final implementada.

Para estructurar de manera sistemática la ejecución del software, el desarrollo se dividió en sprints, cuyas etapas de acción se resumen a continuación:

Sprint	**Componente**	**Actividades**	**Herramientas**
Sprint 1	Autenticación y control de acceso.	Diseño de la interfaz inicial de login.	Python y Visual Studio,

Sprint 2	Visión Artificial y Procesamiento	Configuración de la captura de vídeo, etiquetado de datos, entrenamiento del modelo de IA y	Roboflow, Python y Visual Studio
Sprint	**Componente**	**Actividades**	**Herramientas**
		conexión con el núcleo lógico.	
Sprint 3	Sistema de Alertas y Pruebas BDD	Programación del módulo de detección de anomalías (perdida de PC), envío automatizado de correos y pruebas de aceptación-	Python y BDD

Tabla 8 Etapas del proyecto de software. Fuente: Elaboración propia (2026).

A continuación, se presentarán detalladamente cada uno de los sprints desarrollados, desglosando la lógica técnica, los fragmentos de código implementados y los resultados obtenidos en cada fase para consolidar el funcionamiento integral del sistema de seguridad en el laboratorio.

4.3.1 Sprint 1: Autenticación y Control de Acceso

Este ciclo de desarrollo constituyó en la base fundamental del proyecto de visión artificial implementado en el Laboratorio. Dado que la seguridad y la correcta identificación de los usuarios son críticas para la operatividad del sistema, este sprint se centró en establecer los mecanismos de autenticación, la gestión de privilegios y la infraestructura inicial de almacenamiento de datos.

4.3.2 Planificación

Al iniciar este sprint se explicará detalladamente a la aplicación y se cumplirá los siguientes objetivos:

- Diseñar y programar una interfaz de acceso intuitiva y segura.

- Establecer unos roles para diferenciar a los usuarios comunes del personal administrador.
- Configurar la base de datos local para el registro persistente de las credenciales de entrada.

4.3.3 Diagrama UML

Caso de uso del sistema de videovigilancia

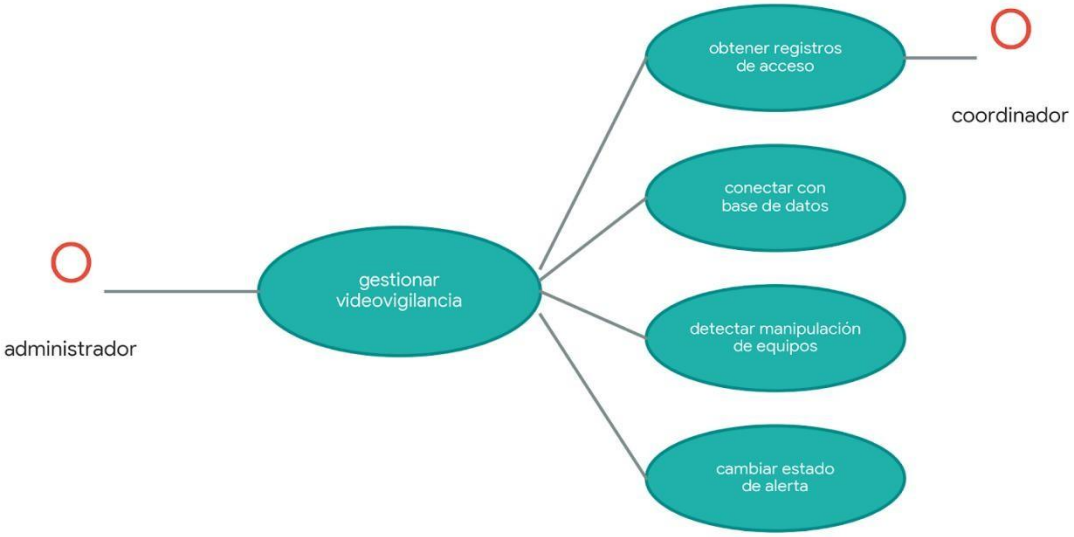


Ilustración 10 Caso de uso de videovigilancia

Caso de uso de ingreso al sistema

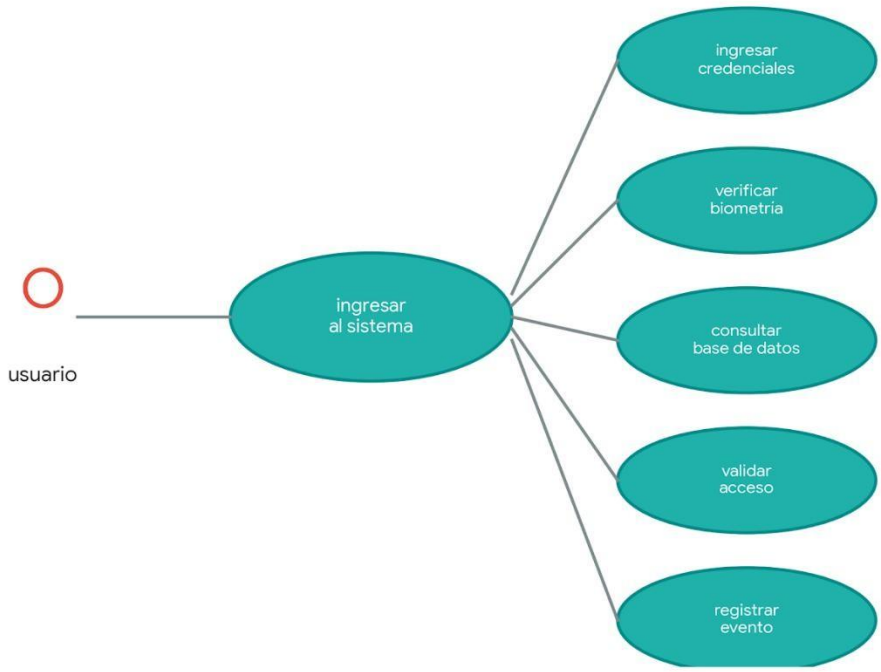


Ilustración 11 Caso de uso de ingreso al sistema

4.3.4 Desarrollo del Módulo de Autenticación

La codificación de este módulo se llevó a cabo utilizando Python como lenguaje principal y Visual Studio como entorno de desarrollo integrado. Se implementaron scripts encargados de validar las entradas del usuario frente a los registros almacenados, asegurando que las credenciales erróneas o el acceso no autorizado sean bloqueados de inmediato.

- **Validación de credenciales *y gestión de sesiones:*** El programa recibe información en formato de texto procedente de otro servidor a través de una cadena http_segura. Los datos introducidos deben cumplir con las credenciales del usuario
- **Control de roles (Roles y Permisos):** Operaciones» es un perfil estándar que tiene acceso únicamente a la vista de estado del Laboratorio. El rol de administrador, por su parte, puede realizar cambios en las alertas, acceder al historial y ajustar la máquina de visión artificial.El sistema gestiona la interfaz de inicio de sesión en la ruta raíz (/), permitiendo tanto la renderización de la vista HTML mediante el método GET como la captura de credenciales a través del envío de formularios mediante el método POST.

Cuando se reciben los datos el script valida los parámetros ingresados (username y password). Si la verificación es exitosa se establecen los parámetros de control en el servidor

(session['logged_in'] = True), otorgando acceso directo a la interfaz principal de monitoreo (prueba). En caso contrario la aplicación recarga la vista de login notificando el error de credenciales inválidas.

El siguiente fragmento de código muestra el diccionario de credenciales base y la ruta de autenticación gestionada en el archivo principal app.py:

```python
@app.route('/', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        username = request.form['username']
        password = request.form['password']

        if username in USUARIOS and USUARIOS[username] == password:
            session['logged_in'] = True
            session['username'] = username
            return redirect(url_for('prueba'))
        else:
            return render_template('login.html', error='Credenciales inválidas')

    return render_template('login.html')
```

Ilustración 12 Interfaz gráfica del login del sistema. Fuente: Elaboración propia (2026).

Como se observa en la figura anterior la interfaz de inicio de sesión solicita las credenciales correspondientes, permitiendo el acceso seguro al panel de control y monitoreo de los equipos del laboratorio.

4.3.5 Infraestructura de Datos y Estructura de la Vista de Acceso

Para complementar la lógica operativa del backend y garantizar una experiencia de interacción fluida, la interfaz de autenticación fue desarrollada utilizando HTML5 junto con un diseño adaptable (responsive), logrando integrarse de manera directa con el microframework Flask. Esta vista actúa como el punto de entrada principal al sistema de monitoreo estructurando de forma limpia y organizada los campos de entrada para el usuario y la contraseña, lo que permite asegurar un control de acceso estrictamente restringido al personal autorizado del laboratorio.

La estructura visual se diseñó priorizando la simplicidad y la usabilidad, permitiendo que los operadores accedan con rapidez a la plataforma de supervisión desde cualquier dispositivo conectado a la red local sin comprometer la seguridad de las credenciales institucionales.

A continuación, se muestra el fragmento de código HTML implementado para la renderización de la interfaz de acceso:

templates > login.html > html

```
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Login - Sistema de Monitoreo ULEAM</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}">

    <style>
        body {
            font-family: Arial, sans-serif;
            margin: 0;
            padding: 0;
            height: 100vh;
            display: flex;
            justify-content: center;
            align-items: center;
            background-image: url('{{ url_for("static", filename="portada.png") }}');
            background-size: cover;
            background-position: center;
            background-repeat: no-repeat;
        }

        .login-container {
            width: 100%;
            height: 100%;
            display: flex;
            justify-content: center;
            align-items: center;
            padding: 0 20px;
        }


        .login-box {
            background: rgba(255, 255, 255, 0.92);
            padding: 2rem;
            border-radius: 10px;
```

Ilustración 13 Código HTML de la interfaz de acceso

login.html | app.py | .env | . env | prueba.html | data.yaml | captura_20260727_155117

templates > login.html > html

```
<html lang="es">
<head>
    <style>
        .university-logo {
            margin-bottom: 1rem;
        }

    </style>
</head>
<body>
    <div class="login-container">
        <div class="login-box">
            <img src="{{ url_for('static', filename='logo.jpg') }}" alt="Logo Universidad" class="university
            <h2>Acceso al Sistema</h2>
            <form method="POST">
                <div class="input-group">
                    <label for="username">Usuario</label>
                    <input type="text" id="username" name="username" placeholder="Ingrese su usuario" requir
                </div>
                <div class="input-group">
                    <label for="password">Contraseña</label>
                    <input type="password" id="password" name="password" placeholder="Ingrese su contraseña"
                </div>
                <button type="submit" class="login-button">Ingresar</button>
            </form>
            {% if error %}
            <p class="error">{{ error }}</p>
            {% endif %}
        </div>
    </div>
</body>
</html>
```

Ilustración 14 Segunda Codificación del HTML de la interfaz de acceso

- *La gestión de recursos estáticos con Flask:* Mediante la función url_for('static', filename='...'), la plantilla enlaza de forma segura las hojas de estilo y las imágenes institucionales (como el logotipo de la universidad), asegurando la compatibilidad de rutas en el servidor local.
- *Envío de credenciales vía POST:* El formulario está configurado mediante <form method="POST">, lo que permite que los datos ingresados en los campos de texto (username y password) viajen de manera oculta al servidor para su validación inmediata.
- *Control de errores condicional:* {% if error %} la interfaz es capaz de renderizar mensajes dinámicos de alerta en caso de que el usuario ingrese credenciales incorrectas, mejorando la experiencia del operador en el laboratorio de electromecánica.

4.3.6 Sprint 2: Visión Artificial y Procesamiento de Imágenes

Esta fase se desarrolla por el software que se utilizara para replantear cómo la cámara de vigilancia dejaría de ser un simple dispositivo pasivo para convertirse en una herramienta activa de inteligencia artificial.

El objetivo principal de este ciclo fue conectar la captura de vídeo en directo con los modelos entrenados. Para lograrlo dividimos el trabajo en tres metas concretas: configurar las imágenes mediante Python, estructurar el flujo de datos en la plataforma Roboflow y asegurar que el sistema pudiera procesar las imágenes en tiempo real sin saturar los recursos locales del equipo.

4.3.7 Captura automatizada de imágenes mediante Python

Para alimentar de manera eficiente el conjunto de datos (dataset) que posteriormente se utilizaría en Roboflow, se desarrolló un script en Python utilizando la librería OpenCV. Este programa se conectó directamente a la transmisión en directo de la cámara de la universidad mediante el protocolo RTSP.

En lugar de realizar capturas imágenes de forma completamente manual el sistema fue programado para extraer imágenes del flujo de vídeo a intervalos de tiempo controlados, organizándolos de manera estructurada en un directorio local *(C:/xampp/htdocs/equipos/capturas)*. El script incorporó una lógica automatizada para alternar entre imágenes a color y versiones en escala de grises (blanco y negro) enriqueciendo la variedad visual del material recopilado para el entrenamiento de la inteligencia artificial.

A continuación, se muestra el fragmento de código implementado para esta captura periódica de las imágenes:

```
# --- INICIO: Implementación para guardar una captura cada 10 minutos ---
try:
    ahora = time.time()
    if ahora - last_capture_time >= CAPTURA_INTERVAL:
        # construir nombre de archivo con timestamp
        timestamp = datetime.now().strftime("%Y%m%d_%H%M%S")
        # Patrón: 3 capturas color, 1 captura blanco y negro
        try:
            if captures_saved % 4 == 3:
                # guardar en blanco y negro
                gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
                filename = os.path.join(CAPTURAS_DIR, f"captura_{timestamp}_bn.jpg")
                cv2.imwrite(filename, gray)
                print(f"✅ Captura B/N guardada: {filename}")
            else:
                # guardar en color
                filename = os.path.join(CAPTURAS_DIR, f"captura_{timestamp}.jpg")
                cv2.imwrite(filename, frame)
                print(f"✅ Captura color guardada: {filename}")
            captures_saved += 1
            last_capture_time = ahora
        except Exception as e:
            print(f"❌ Error guardando captura (color/BN): {e}")
except Exception as e:
    print(f"❌ Error guardando captura periódica: {e}")
# --- FIN: Implementación de captura periódica ---
```

Ilustración 15 Captura periódica de las imágenes. Fuente: Elaboración propia (2026).

Como se evidencia en la lógica del script, la utilización de temporizadores y contadores de guardado (captures_saved) permite automatizar por completo la recolección de muestras sin saturar el almacenamiento local ni requerir la intervención constante del operador. De esta forma cada imagen procesada es evaluado de manera síncrona dentro del hilo principal de ejecución antes de ser volcado en el directorio del servidor local.

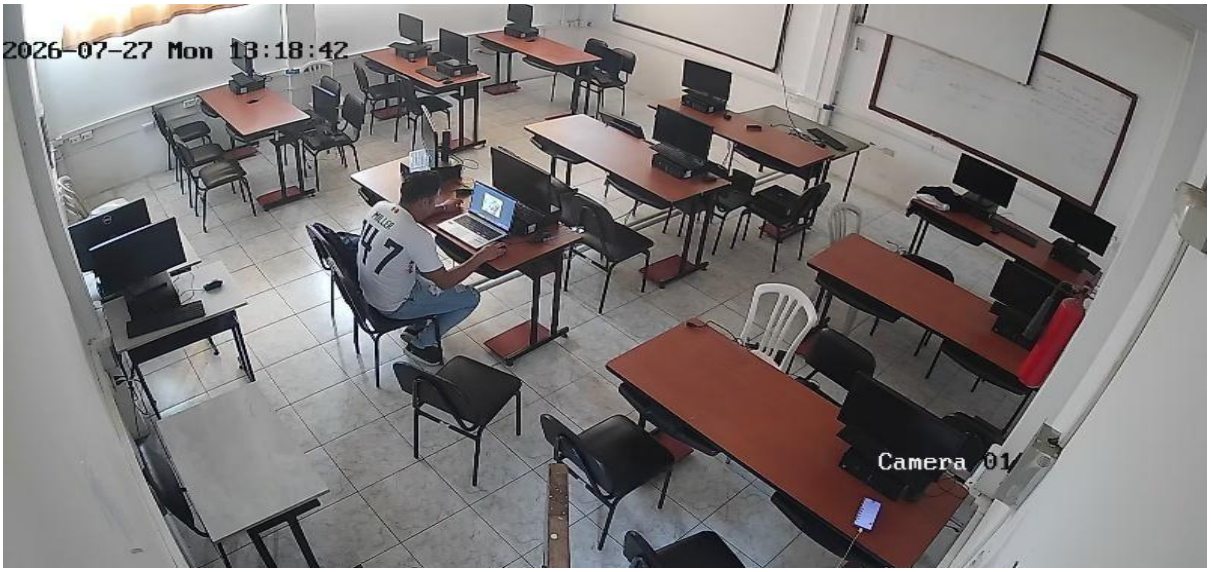


Ilustración 16 Ejecución del script en Python capturando. Fuente: Elaboración propia (2026).

Como se observa en la figura anterior, el entorno de ejecución muestra el funcionamiento en consola de la rutina automatizada, evidenciando el registro y almacenamiento exitoso de la extracción de imágenes directamente desde el flujo RTSP, facilitando la recolección masiva de muestras reales para el entrenamiento del modelo.

4.3.8 Entrenamiento y Gestión de Datos en Roboflow

El corazón de la visión artificial radica en la calidad de los datos. En esta etapa el proceso no se trata principalmente de programar, sino de entrenar al sistema para reconocer con precisión los equipos de computación.

4.3.9 Recolección y etiquetado

Una vez recolectadas y etiquetadas las muestras de imágenes bajo distintas condiciones de iluminación dentro del laboratorio, el conjunto de datos (dataset) fue procesado y entrenado utilizando la plataforma en la nube Roboflow. Este proceso permitió configurar las épocas de entrenamiento y optimizar el reconocimiento de los equipos informáticos.

En la siguiente figura se muestran los resultados del proceso de entrenamiento del modelo dentro de la plataforma Roboflow, donde se visualizan las métricas de rendimiento y las curvas de aprendizaje obtenidas durante el proceso de optimización.

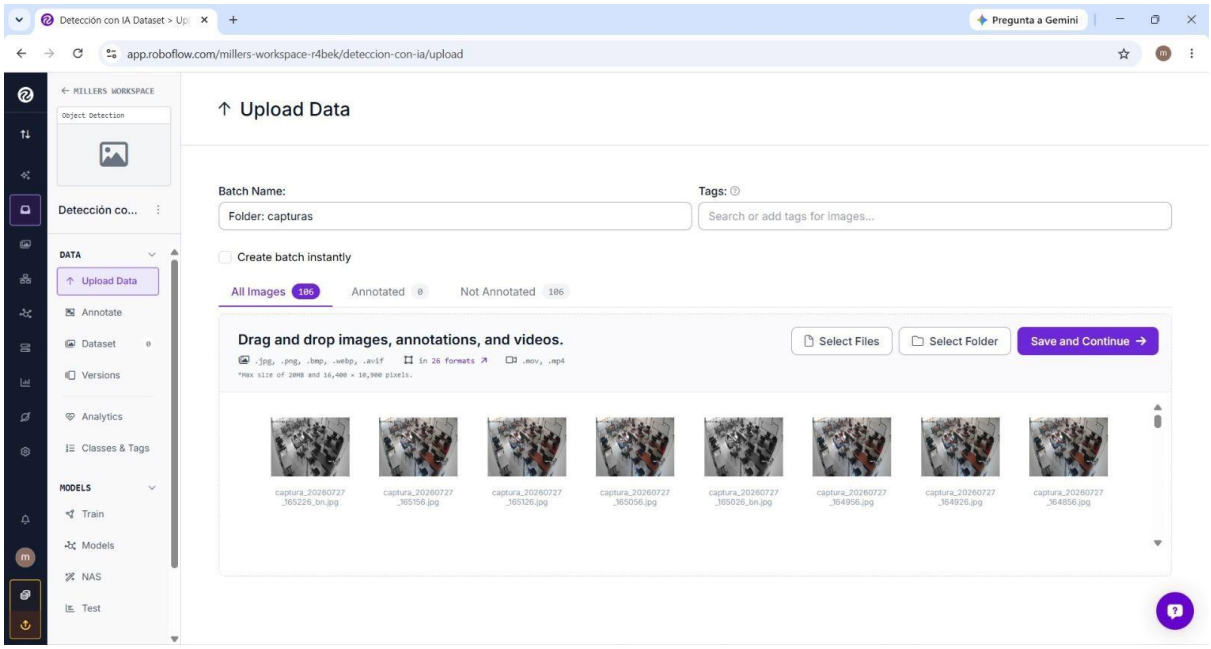


Ilustración 17 Panel de métricas y resultados del entrenamiento del modelo en Roboflow. Fuente: Elaboración propia (2026).

Como se observa en la figura anterior, la interfaz de Roboflow detalla el progreso y las gráficas de convergencia del modelo entrenado, permitiendo validar la eficacia del algoritmo de visión artificial antes de exportar el archivo de pesos optimizado (best.pt) para su integración local en el sistema.

La plataforma centraliza la gestión del dataset permitiendo visualizar la distribución cuantitativa de las imágenes procesadas, asegurando un porcentaje mayoritario destinado al entrenamiento del modelo y el resto para su validación iterativa.

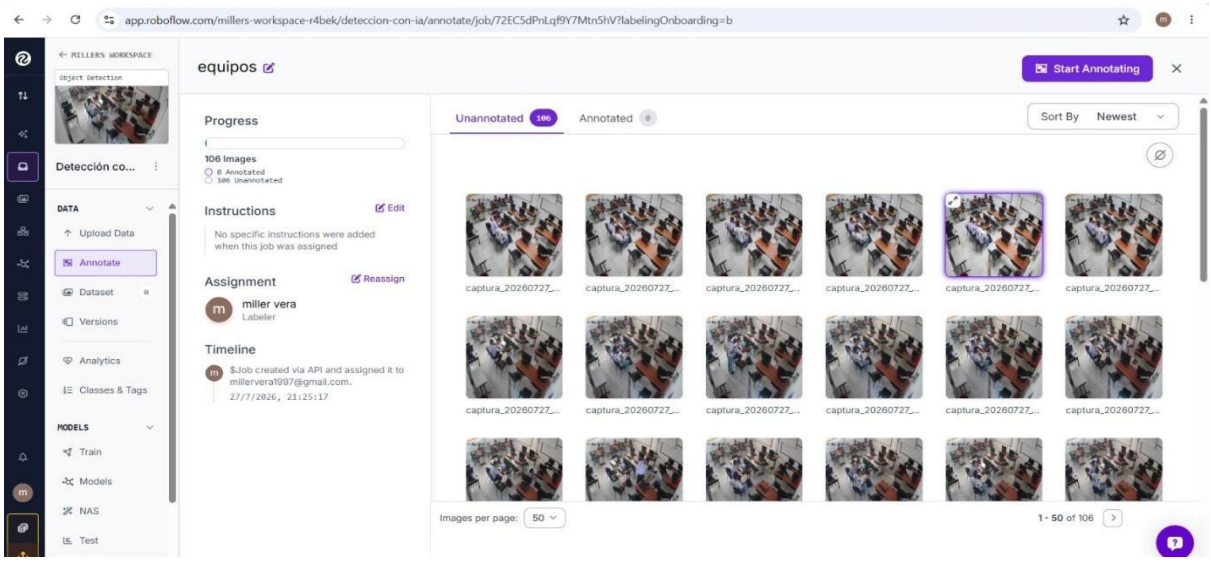


Ilustración 18 Interfaz de distribución del modelo con 106 imágenes en Roboflow. Fuente: Elaboración propia (2026).

Como se observa en la ilustración anterior, el panel de Roboflow detalla el total de 106 imágenes que conforman el conjunto de datos definitivo, desglosando de manera gráfica la partición porcentual establecida para el entrenamiento, validación y prueba de la red neuronal de visión artificial encargada de detectar los equipos del laboratorio.

En este proceso se muestra la anotación manual, donde cada equipo ha sido delimitado mediante una caja cuadrada (Bounding Box), asignándole una etiqueta única. Esta configuración guía el aprendizaje supervisado con inteligencia artificial para que el modelo reconozca la presencia o ausencia de los dispositivos en tiempo real.

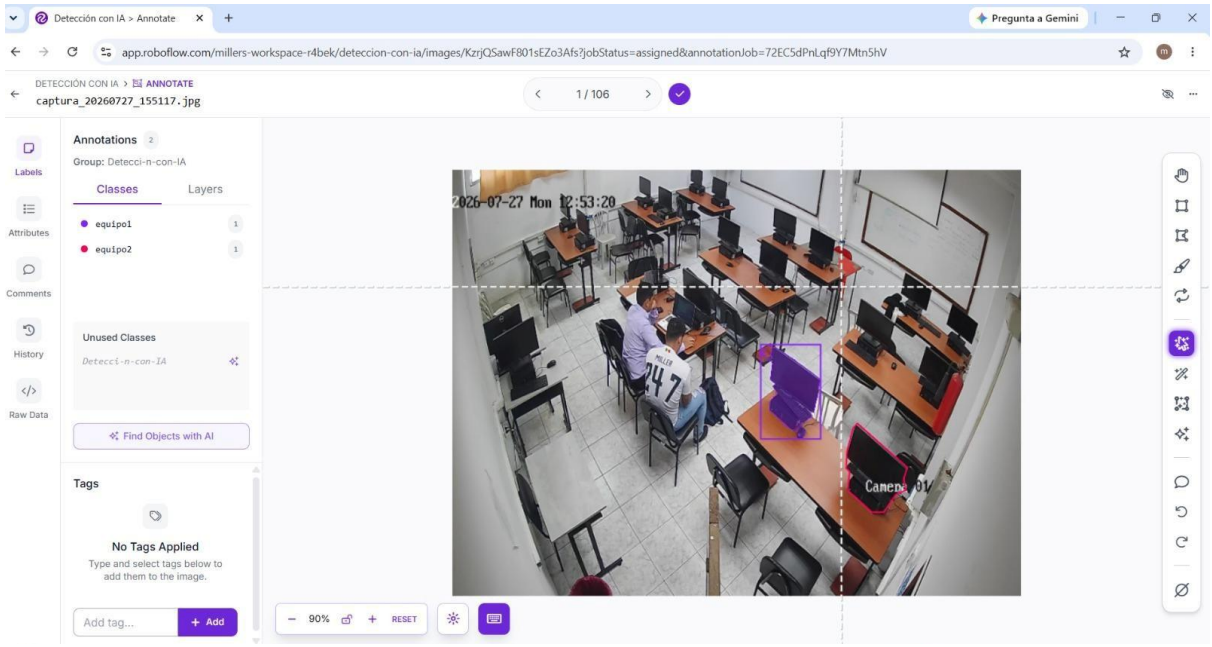


Ilustración 19 Proceso de etiquetado manual y delimitación de equipos en Roboflow. Fuente: Elaboración propia (2026).

Como se observa en la ilustración anterior la interfaz de Roboflow detalla la delimitación geométrica de los equipos dentro del laboratorio mediante cajas de selección, garantizando la precisión de las coordenadas espaciales que interpretará el algoritmo de YOLOv8.

Con el fin de mejorar el modelo ante condiciones no controladas en el laboratorio (como variaciones de luz o sombras), se aplicaron técnicas de aumento de datos (Data Augmentation). Estas transformaciones permiten simular variaciones del entorno real sin necesidad de recolectar físicamente miles de imágenes adicionales, incrementando artificialmente la diversidad y robustez del dataset.

4.3.9.1.1 Aumento de datos

Los mayores desafíos en el sistema de visión artificial aplicados a entornos reales es la variabilidad del entorno como la iluminación natural y artificial a lo largo del día o los diferentes ángulos desde los equipos que pueden aproximarse a su área de vigilancia.

4.3.9.1.2 Exportación del modelo

Uno de los mayores desafíos al implementar un sistema de visión artificial enfocado en la seguridad física de los equipos es que el entorno del laboratorio cambia constantemente. Los equipos están fijos en sus escritorios, pero la iluminación varía a lo largo del día como las sombras se desplazan, a veces hay reflejos en las pantallas o en las carcasas de las mesas. Para evitar que el modelo sufra de sobreajuste o que falle al intentar detectar si un equipo sigue en su lugar se aplica las técnicas avanzadas de aumento de datos dentro de la plataforma Roboflow.

El aumento de datos nos permitió multiplicar de forma inteligente el volumen del conjunto de entrenamiento original sin necesidad de tomar miles de fotos manuales adicionales. Mediante la automatización en la nube el sistema aplicó transformaciones matemáticas controladas a cada una de las imágenes etiquetadas, generando variaciones críticas para robustecer el sistema. Entre las principales operaciones configuradas se encuentran:

Modificaciones de brillo y exposición: Se simularon escenarios con luz natural directa entrando por las ventanas del laboratorio y escenarios oscuros o nocturnos. Esto le enseña al modelo a reconocer las computadoras y sus espacios incluso cuando la iluminación es deficiente o cambia de golpe.

Ilustración 20 Modificaciones de conjunto de color. Fuente: Elaboración propia (2026).

Como se observa en la figura anterior la misma estación de trabajo es procesada bajo diferentes niveles de iluminación. Esto le enseña al modelo a no depender de una iluminación estática, permitiéndole identificar y proteger el equipo de manera eficiente sin importar la hora del día.

Variaciones de ángulo y perspectiva: Aunque la cámara IP del Laboratorio se encuentra instalada en una posición fija las vibraciones leves de la estructura o los factores ambientales pueden generar variaciones milimétricas en el encuadre de los escritorios. Por esta razón durante la fase de entrenamiento en Roboflow se configuraron rotaciones controladas y cambios de perspectiva simulados, asegurando que el modelo sea tolerante a estas desviaciones físicas y que la ubicación exacta de cada equipo y se mantenga siempre dentro del rango de monitoreo del software en Python.

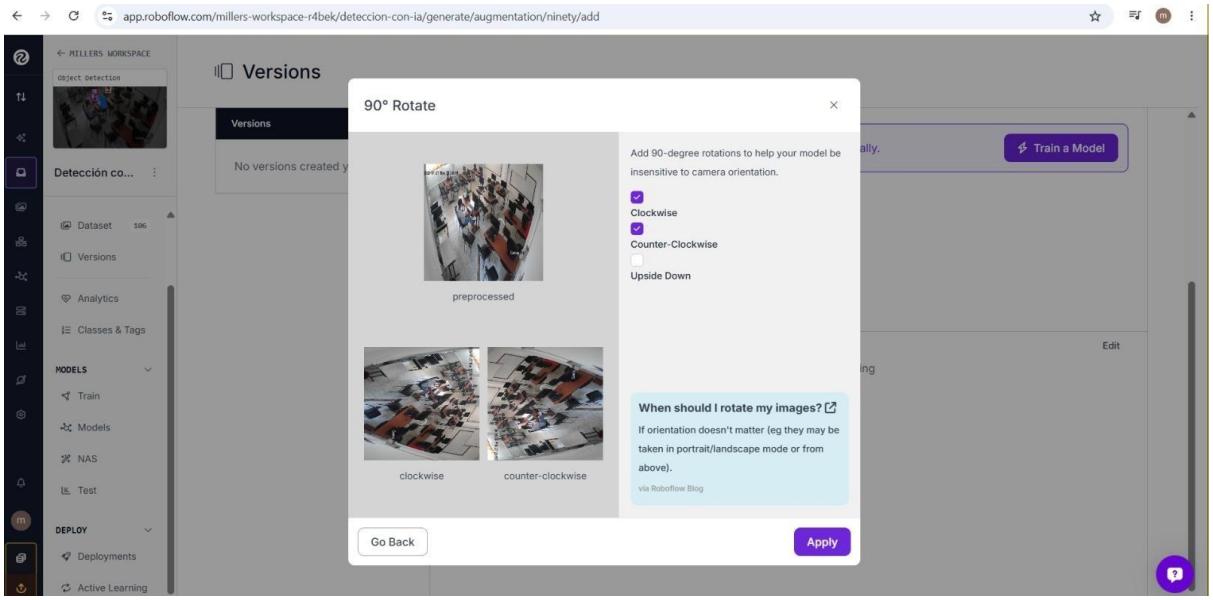


Ilustración 21 Variaciones de ángulo en Roboflow. Fuente: Elaboración propia (2026).

Adición de ruido digital y simulación de oclusión parcial: En un entorno real de laboratorio la transmisión de vídeo puede sufrir imperfecciones técnicas o interferencias momentáneas que generan ruido digital en la imagen. Asimismo, es común que una persona pase temporalmente frente a un equipo bloqueando la visibilidad directa por unos segundos. Para asegurar que el modelo entrenado no active falsas alarmas ni pierda el seguimiento ante estos eventos cotidianos se incorporaron patrones de ruido y oclusiones parciales controladas durante el entrenamiento en la plataforma Roboflow.

Para evidenciar de forma gráfica cómo se estructuró y configuró este entorno en la nube, se presenta la siguiente captura del panel de entrenamiento:

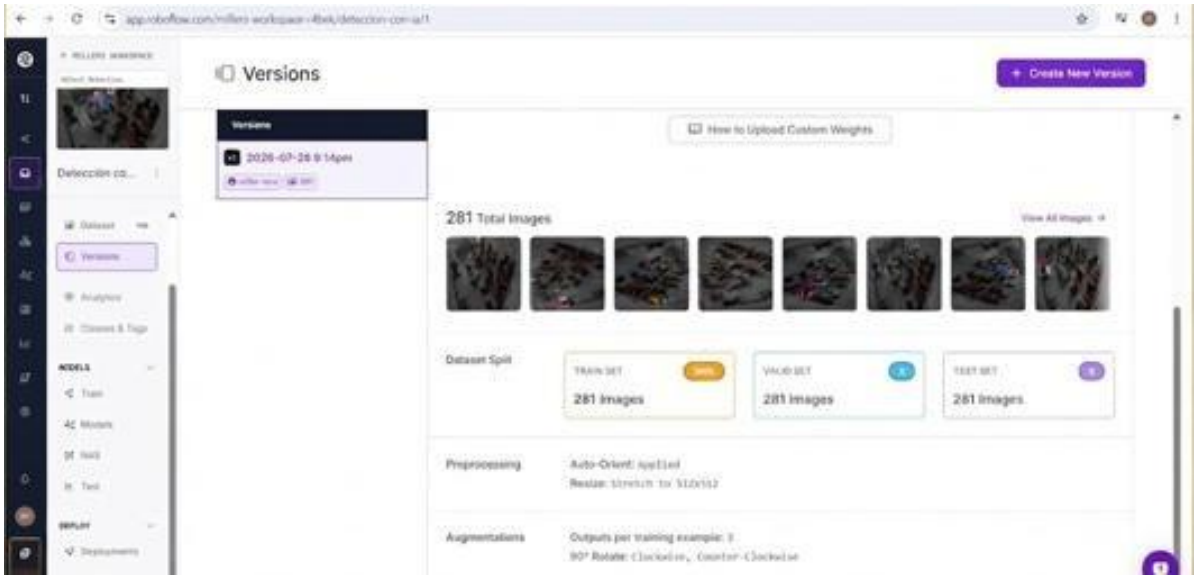


Ilustración 22 Panel de gestión y estado del entrenamiento del modelo en Roboflow. Fuente: Elaboración propia (2026).

Como se visualiza en la figura anterior la interfaz de Roboflow centraliza todo el ciclo de vida del modelo de visión artificial desde la categorización de las clases hasta la consolidación de las versiones entrenadas. El uso de esta plataforma en la nube facilitó la aplicación masiva de técnicas de aumento de datos, permitiendo que la red neuronal adquiera mayor robustez frente a variaciones de iluminación y perspectiva en el laboratorio de la ULEAM. Gracias a esta integración el proyecto asegura un flujo de trabajo estandarizado que culmina en la obtención de pesos optimizados y listos para su despliegue en el backend local.

4.3.9.1.3 Archivo de configuración del dataset

Una vez completado el entrenamiento del modelo en la plataforma de Roboflow y realizada la exportación de los pesos optimizados, se genera automáticamente el archivo de configuración data.yaml. Este archivo es fundamental para que el script de Python basado en YOLO conozca la estructura de las carpetas de entrenamiento (train), validación (val) y prueba (test), así como el número total de clases (nc) y las etiquetas correspondientes a cada equipo del laboratorio.

A continuación, se muestra el contenido estructurado del archivo de configuración utilizado en el proyecto:

deteccion > ! data.yaml

```yaml
train: ../train/images
val: ../valid/images
test: ../test/images

nc: 20
names: ['equipo1', 'equipo10', 'equipo11', 'equipo12', 'equipo13', 'equipo14', 'equipo15', 'equipo16', 'equipo17', 'equipo18', 'equipo19', 'equipo2'

roboflow:
  workspace: millers-workspace-r4bek
  project: deteccion-con-ia
  version: 1
  license: Private
  url: https://app.roboflow.com/millers-workspace-r4bek/deteccion-con-ia/1
```

Ilustración 23 el archivo de configuración data.yaml. Fuente: Elaboración propia (2026).

Rutas relativas del dataset: Define de forma estandarizada dónde se encuentran las imágenes para que el motor de inferencia local pueda evaluar el flujo de vídeo de manera eficiente.

Definición de clases (nc = 20$): Establece el universo de los elementos monitoreados en el laboratorio.

Trazabilidad del proyecto: Incluye los metadatos de Roboflow, lo que garantiza la reproducibilidad del entrenamiento en caso de requerir futuras actualizaciones o reentrenamientos de la red neuronal.

4.3.9.1.4 Organización y estructuración del dataset de entrenamiento

Para garantizar que el modelo de inteligencia artificial procese la información de manera ordenada, las imágenes capturadas del laboratorio de la ULEAM se estructuraron previamente en tres directorios principales: entrenamiento (train), validación (val) y prueba (test). Esta distribución estándar permite que el algoritmo aprenda a reconocer los patrones de los equipos sin sobreajustarse.

A continuación, se muestra la organización de los archivos dentro de la carpeta correspondiente al conjunto de entrenamiento:

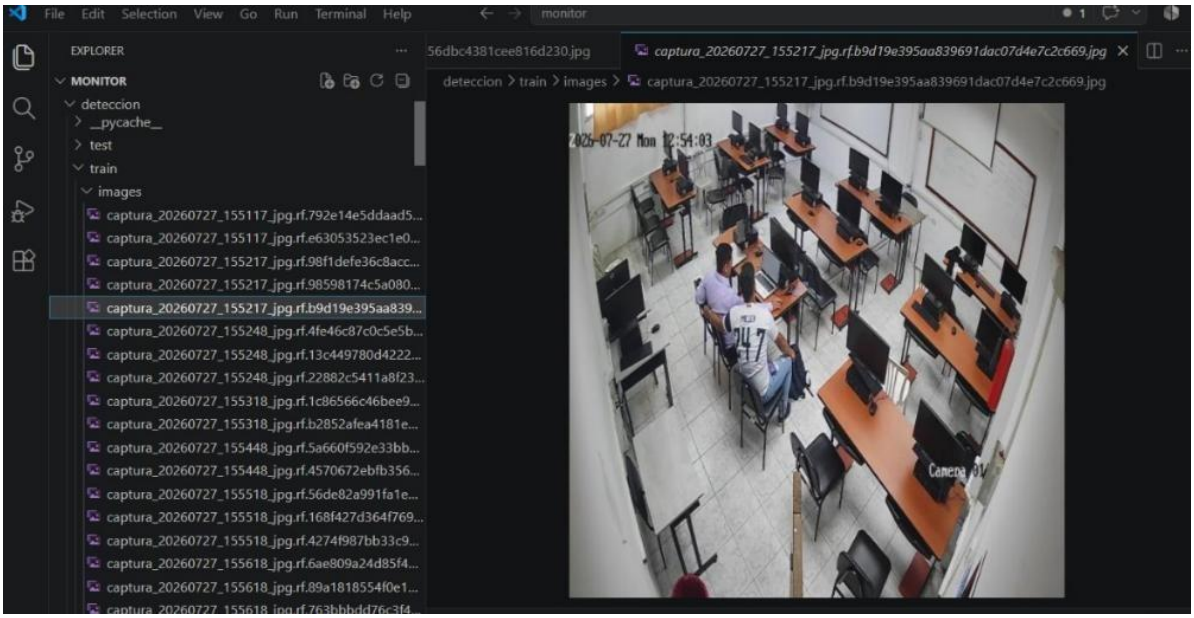


Ilustración 24 Estructura de directorios y almacenamiento de imágenes en el conjunto de entrenamiento (train). Fuente: Elaboración propia (2026).

Como se observa en la figura anterior el directorio de entrenamiento almacena de forma jerárquica las fotografías utilizadas para que la red neuronal reconozca los dispositivos del laboratorio bajo distintas perspectivas y condiciones de iluminación.

A su vez, cada imagen se encuentra vinculada a su respectivo archivo de etiquetas:

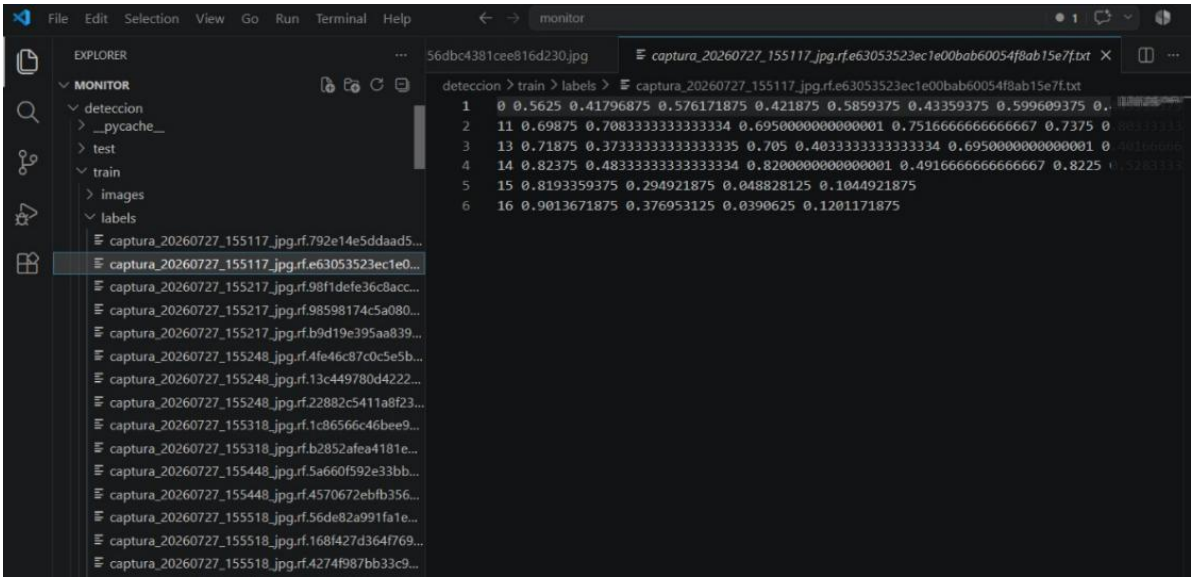


Ilustración 25Visualización de etiquetas correspondientes en el dataset. Fuente: Elaboración propia (2026).

En esta ilustración se expone el contenido detallado de las carpetas de datos, evidenciando que cada fotografía va acompañada de su respectivo archivo de marcado. Esto asegura que el sistema identifique con precisión milimétrica la ubicación exacta de cada equipo informático delimitado durante la fase de etiquetado en Roboflow.

4.3.9.2 Integración del modelo con Python y Visual Studio

Una vez que el modelo de inteligencia artificial fue entrenado y exportado exitosamente desde la plataforma Roboflow, el siguiente paso crítico consistió en integrarlo al entorno de desarrollo local mediante Python y Visual Studio. Para lograr una arquitectura robusta, escalable y capaz de gestionar múltiples procesos concurrentes (como la captura de vídeo, la inferencia de inteligencia artificial y la interfaz web), se empleó el microframework Flask en conjunto con bibliotecas especializadas de visión artificial.

4.3.9.2.1 Librerías utilizadas y técnica

La correcta selección de librerías fue fundamental para asegurar el rendimiento en tiempo real sin saturar los recursos de hardware del equipo local:

Ultralytics (YOLO): Se utilizó para cargar el modelo personalizado (best.pt), permitiendo ejecutar la inferencia de forma rápida sobre cada imagen capturado para la detección precisa de los equipos.

cv2 (OpenCV): Es la librería central para el procesamiento digital de imágenes. Permite la lectura de la transmisión de vídeo, el redimensionamiento de las imágenes, la conversión de formatos de color y la manipulación de la matriz gráfica de la cámara.

threading y queue: Esenciales para manejar la concurrencia. Permiten ejecutar el bucle pesado de detección de la inteligencia artificial en un hilo en segundo plano, evitando que la interfaz web o la visualización en vivo se congelen o sufran retrasos.

mysql.connector: Utilizada para establecer la persistencia de los datos, conectando el script de Python directamente con la base de datos local para registrar el estado, las alertas de los equipos y coordinar el aviso final mediante un mensaje de WhatsApp automatizado.

4.3.9.2.2 Conexión a la cámara de seguridad

Para vincular el sistema con el dispositivo de seguridad del Laboratorio se configuró el vídeo mediante el protocolo RTSP (Real-Time Streaming Protocol). Este protocolo permite acceder al flujo de vídeo en directo de la cámara IP de manera remota y continua.

A continuación, se muestra el fragmento de código correspondiente a la inicialización segura de los recursos y la conexión con la cámara de la universidad:

```python
import cv2
from ultralytics import YOLO
import threading
import queue

RTSP_URL = os.getenv("RTSP_URL", "rtsp://admin:Uleam123@172.17.141.6:554/Streaming/Channels/501")model = None
video_capture = None
lock = threading.Lock()

def inicializar_recursos():
    """Inicializa el modelo YOLO y la conexión con la cámara RTSP de forma segura"""
    global model, video_capture

    try:
        # Cargar el modelo de IA entrenado
        if model is None:
            model = YOLO("best.pt")
            print ("Modelo YOLO cargado correctamente")

        # Inicializar la captura de vídeo mediante RTSP con búfer optimizado
        with lock:
            if video_capture is None or not video_capture.isOpened():
                video_capture = cv2.VideoCapture(RTSP_URL)
                video_capture.set(cv2.CAP_PROP_BUFFERSIZE, 1)
                print ("Cámara RTSP inicializada exitosamente desde la red")

    except Exception as e:
        print (f"Error inicializando recursos: {e}")
        return False
    return True
```

Ilustración 26 Inicialización segura de los recursos y la conexión con la cámara de la universidad. Fuente: Elaboración propia (2026).

Como se observa en la ilustración anterior, el entorno de desarrollo refleja la correcta ejecución de la rutina de enlace con el protocolo RTSP, validando la carga del modelo de inteligencia artificial y la disponibilidad de la cámara en la red local.

4.3.9.2.3 Procesamiento de vídeo en segundo plano

Para asegurar que el sistema evalúe la presencia de los equipos de manera continua sin bloquear la aplicación se programó un hilo en segundo plano. Este script procesa las imágenes por intervalos optimizados y utiliza un algoritmo de consistencia temporal para evitar falsas alarmas ante movimientos momentáneos:

```
def proceso_deteccion():
    """Proceso principal de detección que se ejecuta en segundo plano"""
    global deteccion_activa, model, last_capture_time, captures_saved

    if not inicializar_recursos():
        print("❌ No se pudieron inicializar los recursos para detección")
        return
    deteccion_activa = True
    frame_count = 0
    print("✅ Iniciando proceso de detección en segundo plano...")

    while deteccion_activa:
        try:
            # Obtener frame de forma segura
            with lock:
                if video_capture is None or not video_capture.isOpened():
                    inicializar_recursos()
                    time.sleep(2)
                    continue

                success, frame = video_capture.read()
```

Ilustración 27 Inicialización del modelo YOLO y declaración de variables globales. Fuente: Elaboración propia (2026).

Como se observa en la primera parte del fragmento de código, se importan las librerías esenciales como OpenCV y Ultralytics YOLO, estableciendo además la URL de conexión RTSP para la cámara del laboratorio. Garantiza una gestión segura y concurrente de los recursos del sistema durante la transmisión en directo.

```
            if not success:
                print("❌ Error leyendo frame, reintentando...")
                time.sleep(2)
                continue

            frame = cv2.resize(frame, (800, 600))
            frame_count += 1

            # --- INICIO: Implementación para guardar una captura cada 10 minutos ---
            try:
                ahora = time.time()
                if ahora - last_capture_time >= CAPTURA_INTERVAL:
                    # construir nombre de archivo con timestamp
                    timestamp = datetime.now().strftime("%Y%m%d_%H%M%S")
                    # Patrón: 3 capturas color, 1 captura blanco y negro
                    try:
                        if captures_saved % 4 == 3:
                            # guardar en blanco y negro
                            gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
                            filename = os.path.join(CAPTURAS_DIR, f"captura_{timestamp}_bn.jpg")
                            cv2.imwrite(filename, gray)
                            print(f"✅ Captura B/N guardada: {filename}")
                        else:
                            # guardar en color
                            filename = os.path.join(CAPTURAS_DIR, f"captura_{timestamp}.jpg")
                            cv2.imwrite(filename, frame)
                            print(f"✅ Captura color guardada: {filename}")
                        captures_saved += 1
                        last_capture_time = ahora
```

Ilustración 28 Función de carga segura del modelo de IA y conexión al flujo de vídeo. Fuente: Elaboración propia (2026).

En la continuación del script establece la captura de vídeo mediante el protocolo RTSP configurando lo que previene el retraso en la transmisión y asegura que el monitoreo del laboratorio de la ULEAM se realice en tiempo real y sin interrupciones técnicas.

Como se evidencia en la lógica del bucle implementado, la decisión de ejecutar la inferencia del modelo YOLO de manera fraccionada y mediante hilos concurrentes permite aligerar notablemente la carga sobre el procesador. De esta manera, el servidor web local mantiene una respuesta fluida y evita cualquier tipo de bloqueo o retardo visual en la interfaz de supervisión del laboratorio.

4.3.9.3 Algoritmo de consistencia temporal **y control de estados**

En los sistemas de videovigilancia basados en inteligencia artificial uno de los principales retos es la presencia de interferencias visuales momentáneas, como una persona caminando temporalmente frente a la cámara o variaciones de sombra que podrían hacer que el modelo pierda de vista un equipo por un solo imagen. Para evitar falsas alarmas y garantizar la estabilidad del sistema se programó un algoritmo de consistencia temporal basado en umbrales de confirmación y recuperación:

- ***Umbral de confirmación (UMBRAL_CONFIRMACION = 3):*** El sistema no genera una alerta de ausencia de manera inmediata al primer fotograma perdido. Requiere que un equipo no sea detectado durante al menos 3 imágenes consecutivos antes de dar por sentado que ha sido desplazado o sustraído de su puesto.
- ***Umbral de recuperación (UMBRAL_RECUPERACION = 2):*** De igual forma, al reaparecer el equipo en su posición asignada, el sistema exige una persistencia mínima de 2 detecciones consecutivas para restablecer su estado normal a activo, evitando fluctuaciones erráticas en la interfaz.

A continuación, se muestra el fragmento de código que gestiona esta lógica de consistencia en el backend:

```
def verificar_equipos_con_consistencia(detecciones):
    """Verifica equipos con consistencia temporal y detecta cambios"""
    global ZONAS_EQUIPOS

    for i in range(1, 23):
        ZONAS_ EQUIPOS [i]["detectado_ahora"] = 0

    if detecciones is not None:
        for det in detecciones:
            x1, y1, x2, y2 = map(int, det.xyxy[0])
            centro_x = (x1 + x2) // 2
            centro_y = (y1 + y2) // 2

            for i in range(1, 23):
                pos_x, pos_y = ZONAS_ EQUIPOS [i]["posicion"]
                distancia = ((centro_x - pos_x)**2 + (centro_y - pos_y)**2)**0.5

                if distancia < 50:
                    ZONAS_ EQUIPOSorgenitores[i]["detectado_ahora"] = 1 if 'ZONAS_ EQUIPOS in globa
                    ZONAS_ EQUIPOS [i]["detectado_ahora"] = 1
                    break

    # Evaluación de contadores temporales para evitar falsos positivos
    for i in range(1, 23):
        detectado_ahora = ZONAS_ EQUIPOS [i]["detectado_ahora"]
        estado_actual = ZONAS_ EQUIPOS [i]["estado_real"]

        if detectado_ahora:
            if estado_actual == 0:
                ZONAS_ EQUIPOS [i]["contador"] += 1
                if ZONAS_ EQUIPOS [i]["contador"] >= UMBRAL_RECUPERACION:
                    ZONAS_ EQUIPOS [i]["estado_real"] = 1
                    ZONAS_ EQUIPOS [i]["contador"] = 0
            else:
```

```
                ZONAS_ EQUIPOS [i]["contador"] = 0
        else:
            if estado_actual == 1:
                ZONAS_ EQUIPOS [i]["contador"] += 1
                if ZONAS_ EQUIPOS [i]["contador"] >= UMBRAL_CONFIRMACION:
                    ZONAS_ EQUIPOS [i]["estado_real"] = 0
                    ZONAS_ EQUIPOS [i]["contador"] = 0
            else:
                ZONAS_ EQUIPOS [i]["contador"] = 0
```

Ilustración 29 Parámetros lógicos del algoritmo de consistencia temporal. Fuente: Elaboración propia (2026).

Como se aprecia en la implementación de la función, el uso de contadores condicionales por cada zona permite filtrar el ruido visual del entorno en tiempo real. Esta lógica asegura que el sistema de monitoreo sea altamente confiable, reduciendo drásticamente los falsos positivos antes de registrar cualquier cambio de estado en la base de datos o disparar una notificación.

```
# ==================== CAPTURAS PERIÓDICAS (IMPLEMENTACIÓN) ====================
# Directorio donde se guardarán las capturas (solicitado):
CAPTURAS_DIR = r"c:/xampp/htdocs/equipos/capturas"
# Intervalo en segundos entre capturas (10 minutos):
CAPTURA_INTERVAL = 0.5 * 60
# Tiempo de la última captura guardada
last_capture_time = 0
# Contador de capturas guardadas (para patrón 3 color + 1 B/N)
captures_saved = 0
# --- FIN: constantes de implementación ---
```

Ilustración 30 Representación lógica del algoritmo de consistencia temporal en el monitoreo. Fuente: Elaboración propia (2026).

Como se aprecia tanto en la implementación del script como en la estructura visual de la figura anterior, el uso de contadores condicionales y umbrales por cada zona permite filtrar con gran eficacia el ruido ambiental y las oclusiones momentáneas en el laboratorio de la ULEAM. Esta lógica computacional actúa como un filtro inteligente que previene cambios de estado prematuros, asegurando que la plataforma mantenga una alta robustez operativa. De este modo, se eliminan los falsos positivos antes de registrar cualquier modificación de inventario en el sistema o de activar los despachos automáticos de alerta, garantizando una supervisión confiable, continua y libre de interferencias técnicas para los operadores.

4.3.9.4 Validación y Pruebas (BDD)

Una vez integrado el modelo YOLO, la transmisión RTSP y el algoritmo de consistencia temporal, se realizaron pruebas de estrés y validación funcional en el entorno local de desarrollo para comprobar el rendimiento del sistema de visión artificial:

- ***Prueba de latencia y fluidez:*** Se corroboró que el procesamiento del flujo de vídeo mediante hilos en segundo plano (threading) permitiera mantener una tasa de refresco estable en la interfaz web sin provocar bloqueos (freezes) en la aplicación Flask
- ***Prueba de oclusión y falsas alarmas***: Se simuló el paso de personas frente a los equipos de los escritorios del laboratorio. Los resultados demostraron que gracias al umbral de confirmación configurado en 3 fotogramas, el sistema ignoró con éxito las interferencias momentáneas y evitó emitir alertas erróneas.
- ***Prueba de detección de ausencia:*** Al retirar de manera simulada o física un equipo de su posición delimitada, el sistema identificó el cambio de estado de manera precisa tras cumplirse el intervalo de validación temporal.

4.3.9.5 Integración del panel de control principal y visualización en tiempo real

Una vez que el backend procesa el flujo de vídeo de la cámara y evalúa los estados de los equipos mediante los hilos en segundo plano es necesario unificar toda esa información en una interfaz gráfica intuitiva para el usuario. Para lograrlo se diseñó la vista principal del sistema la cual combina el streaming de vídeo en directo, una tabla dinámica con el estado de los equipos y un sistema de notificaciones flotantes.

A continuación, se presenta el fragmento de código correspondiente a la estructura central y los scripts de actualización asíncrona de la vista:

```
<div class="container mt-4">
  <div class="row">
    <div class="col-12">
      <!-- Video ocupa todo el ancho superior -->
      <div class="video-container">
        <img src="{{ url_for('video_feed') }}" class="video-feed" />
      </div>
    </div>
  </div>

  <div class="row mt-3">
    <!-- Columna izquierda: Tabla Detallada (ahora ocupa todo el ancho) -->
    <div class="col-lg-12">
      <div class="table-card">
        <div class="table-header">
          <i class="fas fa-list me-2"></i>Detalle de Equipos
        </div>
        <div class="table-responsive">
          <table class="table table-hover mb-0 table-dark-custom" id="tablaDetallada">
            <thead class="table-light">
              <tr>
                <th>ID</th>
                <th>Nombre</th>
                <th>Estado</th>
                <th>Ubicación</th>
              </tr>
            </thead>
            <tbody></tbody>
          </table>
        </div>
      </div>
    </div>
```

Ilustración 31 Estructura central y los scripts del index.html. Fuente: Elaboración propia (2026).

Como complemento al funcionamiento del sistema, la interfaz incluye un panel lateral de navegación que facilita el acceso rápido a los diferentes apartados de control del laboratorio. Este menú lateral agrupa de manera intuitiva las secciones de supervisión en tiempo real, los registros de actividad y los parámetros generales del software, garantizando que el operador pueda navegar entre las distintas vistas de forma fluida y sin interrumpir el flujo continuo de videovigilancia.

```
    <!-- Estado General eliminado -->
  </div>
</div>

<!-- Notificación de WhatsApp enviado (oculta inicialmente) -->
<div id="whatsappNotification" class="whatsapp-notification" style="display: none;">
  <i class="fas fa-paper-plane"></i>
  <div class="whatsapp-notification-content">
    <h6>✅ WhatsApp Enviado</h6>
    <p id="whatsappNotificationText">Alerta enviada correctamente</p>
  </div>
</div>
```

Ilustración 32 Segunda Estructura central y los scripts del index.html. Fuente: Elaboración propia (2026).

Sincronización del streaming: La etiqueta de imagen con la ruta {{ url_for('video_feed') }} incrusta de forma continua el vídeo que el hilo de Python está procesando con el modelo YOLO.

Actualización asíncrona: Mediante la función setInterval junto con peticiones fetch('/data'), la interfaz consulta el estado de los equipos cada dos segundos, permitiendo que la tabla cambie de color y muestre "Presente" o "Ausente" en tiempo real sin congelar la pantalla del operador.

Respuesta visual de alertas: Este entorno web también se encuentra preparado para recibir las notificaciones flotantes (mediante librerías de avisos y eventos de WhatsApp), cerrando el círculo entre la detección de IA y la respuesta del sistema.

4.3.10 Sprint 3: Gestión de Alertas y Notificaciones Automatizadas

El desarrollo de este proyecto se enfocó en cerrar el ciclo de seguridad mediante la automatización de la respuesta ante incidentes. En los Sprints anteriores logramos que el sistema viera y analizara el laboratorio a través de la inteligencia artificial, pero un sistema de videovigilancia no es completamente útil si la información se queda estancada en una pantalla local que nadie está observando todo el tiempo. Por esta razón el Sprint 3 tuvo como misión principal la aplicación de una memoria persistente para registrar los eventos críticos y sobre todo un puente de comunicación proactivo que le avise de manera inmediata al personal encargado cuando un equipo del Laboratorio sufra alguna alteración, permitiendo una intervención rápida y eficaz sin depender de la supervisión humana constante.

4.3.10.1 Persistencia de eventos en la Base de Datos

El sistema requiere registrar formalmente dicha incidencia para mantener un historial auditable. Para cumplir con esto la aplicación se conecta de manera local a una base de datos relacional en MySQL, generando y verificando de forma automatizada una tabla estructurada para almacenar cada alerta:

```
CREATE TABLE IF NOT EXISTS alertas_equipos(
    idINT AUTO_INCREMENT PRIMARY KEY,
    fecha_horaDATETIME,
    equipos_idINT(11),
    nombre_equiposVARCHAR(100),
    ubicacion_xINT(11),
    ubicacion_yINT(11),
    estadoVARCHAR(20),
    created_atTIMESTAMP DEFAULT CURRENT_TIMESTAMP
)
```

Ilustración 33 Creación de la Base de Datos. Fuente: Elaboración propia (2026).

Cada vez que el algoritmo detecta un cambio crítico de estado (por ejemplo, el paso de un equipo de activo 1 a inactivo 0), el script inserta una nueva fila especificando la fecha, la hora exacta, el identificador del equipo afectado y las coordenadas de su posición dentro del laboratorio.

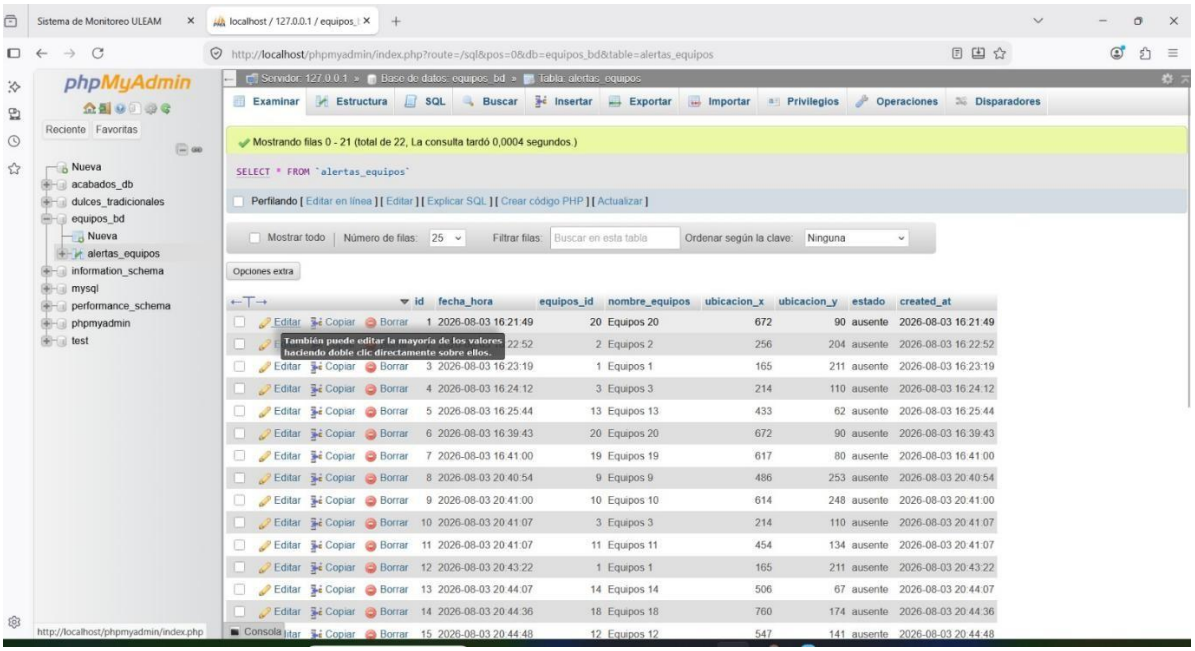


Ilustración 34 Ejecución de registros en MySQL Fuente: Elaboración propia (2026).

Como se visualiza tanto en el código de inserción como en la estructura de la base de datos de la figura anterior, el sistema asegura una persistencia de datos robusta y confiable. Este registro automatizado en MySQL al Laboratorio de la ULEAM de un historial auditable y permanente, permitiendo que los administradores consulten eventos pasados, analicen patrones de seguridad y verifiquen con absoluta precisión temporal cualquier anomalía o posible pérdida de equipos dentro de las instalaciones.

4.3.10.2 Control de intervalos y mitigación de spam de alertas

En un escenario real de seguridad si un equipo permanece ausente o si el sistema detecta intermitencias prolongadas, existe el riesgo de que el software genere docenas de registros e intente enviar notificaciones de manera masiva, saturando tanto la base de datos como los canales de comunicación de los administradores.

Para solucionar este inconveniente y garantizar una gestión eficiente de los avisos, se programó un mecanismo de control de intervalos temporales (INTERVALO_ALERTAS = 30 * 60), configurado para cumplirse en un rango de 30 minutos:

Restricción de frecuencia: El sistema evalúa el tiempo transcurrido desde la última notificación enviada. Si una anomalía persiste o se repite dentro de la misma ventana de tiempo de 30 minutos, el evento se registra internamente en la base de datos para fines de auditoría, pero se bloquea el envío masivo de nuevos avisos hacia el exterior.

Optimización operativa: Esta técnica evita la saturación de notificaciones innecesarias en los dispositivos móviles de los encargados del Laboratorio, asegurando que solo reciban alertas oportunas y espaciadas ante incidencias verdaderamente relevantes.

4.3.10.3 Integración de mensajería automatizada (WhatsApp)

Para cerrar de manera proactiva la arquitectura de seguridad del proyecto, el sistema no solo almacena la anomalía en la base de datos local, sino que dispara un mensaje de alerta instantáneo hacia los dispositivos móviles de los administradores del Laboratorio. Para lograr esta conectividad en la nube de forma segura y confiable, se integró la infraestructura de comunicación de Twilio.

4.3.10.3.1 ¿Qué es Twilio y su rol en el sistema?

Twilio es una plataforma de comunicación en la nube basada en API (Application Programming Interface) que permite a los desarrolladores integrar de forma programática servicios de mensajería SMS, voz y aplicaciones de mensajería instantánea como WhatsApp.

Su rol fundamental en este proyecto radica en actuar como un intermediario confiable y oficial que elimina la necesidad de desarrollar código personalizado o librerías no oficiales para conectarse con WhatsApp. Gracias a su infraestructura Twilio se encarga automáticamente de aspectos complejos como la autenticación, la seguridad de los tokens, el enrutamiento de los mensajes y la confirmación de entrega (generando registros y logs de estado), permitiendo que el backend del sistema se enfoque únicamente en la lógica de detección y alerta.

4.3.10.3.2 Configuración y puesta en marcha del entorno Sandbox de WhatsApp

Para poner en marcha esta pasarela de mensajería sin complicaciones durante el desarrollo del proyecto, seguimos una serie de pasos prácticos utilizando el entorno de pruebas (Sandbox) que ofrece la plataforma:

Creación de cuenta y activación: Tras registrarnos en la plataforma de Twilio, accedimos al menú lateral de mensajería (Messaging -> Try it out -> WhatsApp Sandbox), donde se nos asignó un número oficial de prueba (+14155238886). Para habilitar la comunicación bidireccional, vinculamos nuestro número personal enviando un mensaje predeterminado desde WhatsApp al número del Sandbox (por ejemplo, join <código>).

Gestión de credenciales: Desde el panel principal (Dashboard) obtuvimos los parámetros críticos de seguridad: el Account SID y el Auth Token, los cuales sirven como llaves de acceso para que nuestra aplicación pueda comunicarse con la API de Twilio.

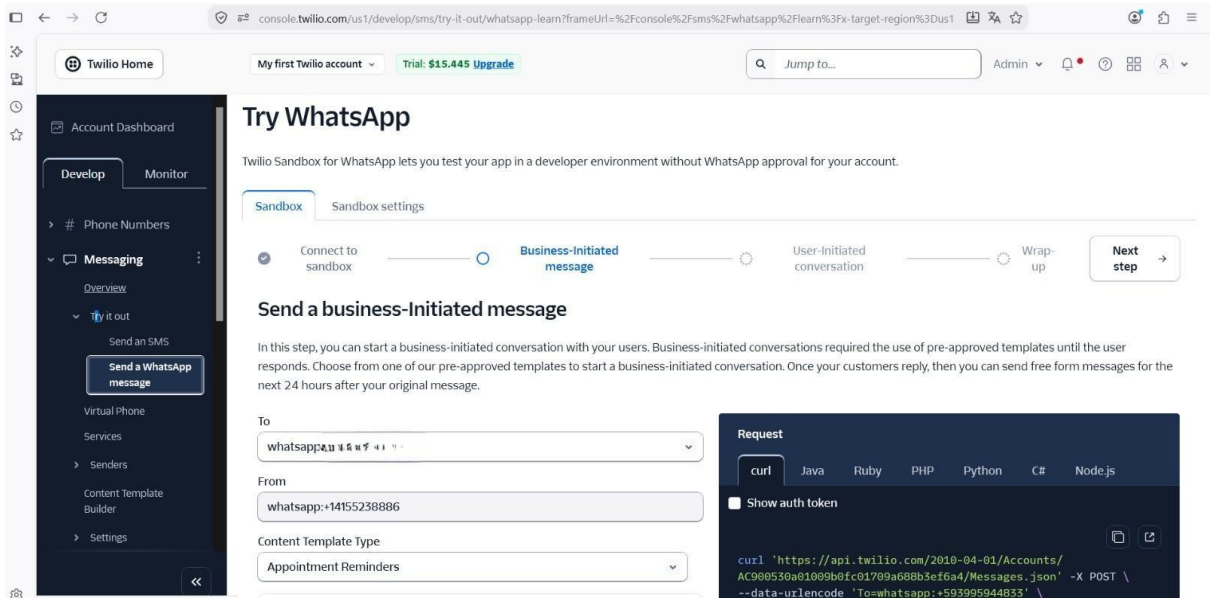


Ilustración 35Panel de configuración y pruebas del entorno Sandbox de WhatsApp en Twilio. Fuente: Elaboración propia (2026).

Como se observa en la ilustración anterior el entorno de desarrollo (Sandbox) en el panel de control de Twilio facilita la simulación y prueba del envío de notificaciones automatizadas a través de WhatsApp antes de pasar a un entorno institucional definitivo.

4.3.10.3.3 Variables de entorno y código de integración en Python

Para mantener la seguridad del código fuente y evitar exponer las credenciales directamente en los scripts, la configuración de Twilio y los números de destino se centralizaron

mediante un archivo de variables de entorno (.env), facilitando además la adaptabilidad del software tanto en entornos de pruebas locales como en las PCs del laboratorio de la universidad.

```
#. env
TWILIO_ACCOUNT_SID=AC900530a01009b0fc01709a688b3ef6a4
TWILIO_AUTH_TOKEN=daeb927d05ea08d5c1958fbfbaddb52b
TWILIO_FROM=whatsapp:+14155238886
WHATSAPP_TO_NUMBER=whatsapp:+593995944833
MODO=local
```

Ilustración 36 Variables de entorno para notificaciones

Una vez definidas las variables, la implementación dentro del script de Python se realizó de manera directa utilizando la librería oficial de cliente de Twilio. Cada vez que el sistema detecta una anomalía o la pérdida de un equipo, la función procesa el envío del mensaje de alerta de la siguiente manera:

```python
from twilio.rest import Client
import os


def enviar_alerta(mensaje):
    """Envía un mensaje de alerta automatizado a través de la API de WhatsApp de
    Twilio"""
    try:
        client = Client(
            os.getenv("TWILIO_ACCOUNT_SID"), os.getenv("TWILIO_AUTH_TOKEN")
        )
        client.messages.create(
            body=mensaje,
            from_=os.getenv("TWILIO_FROM"),
            to=os.getenv("WHATSAPP_TO_NUMBER"),
        )
        print("Alerta de WhatsApp enviada exitosamente.")
    except Exception as e:
        print(f"Error al enviar la notificación por WhatsApp: {e}")
```

Ilustración 37 Codificación de notificación de Twilio. Fuente: Elaboración propia (2026).

La ilustración anterior muestra la estructura lógica de la función programada en Python, encargada de empaquetar el mensaje de alerta y despacharlo de manera segura hacia la API en la nube de Twilio.

Una vez completada la vinculación de los números y configuradas las credenciales, el sistema quedó listo para realizar pruebas de recepción. La siguiente ilustración muestra cómo se visualizan las notificaciones automatizadas de alerta dentro de la aplicación de mensajería en el dispositivo móvil vinculado:

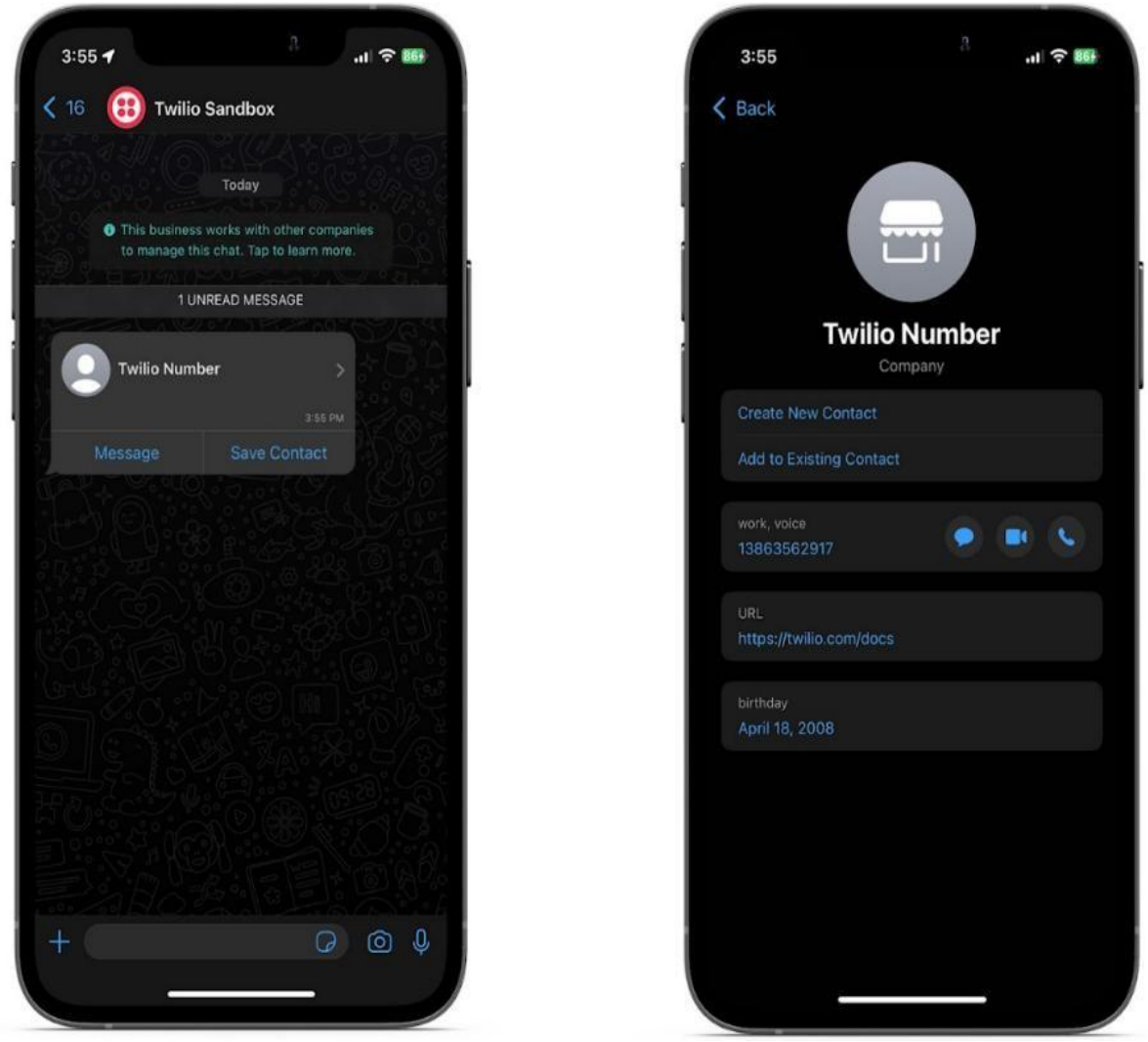


Ilustración 38 isualización de alertas automatizadas de ausencia de equipos en el entorno Sandbox de WhatsApp. Fuente: Elaboración propia (2026).

Como se observa en la ilustración anterior muestra la interfaz del dispositivo móvil, el entorno de desarrollo (Sandbox) en el panel de control de Twilio facilita la simulación y prueba del envío de notificaciones automatizadas a través de WhatsApp. Esta etapa de validación visual es crucial, ya que permite confirmar que el mensaje de alerta con el nombre del equipo y la hora exacta de la incidencia llega correctamente al administrador del laboratorio de la ULEAM antes de proceder a la implementación institucional definitiva, asegurando la efectividad del sistema de monitoreo.

Una vez completada la configuración de la pasarela y vinculadas las credenciales en el script de Python, el siguiente paso fundamental fue validar la comunicación bidireccional. La siguiente ilustración muestra la captura de pantalla en el dispositivo móvil donde se confirma exitosamente la suscripción al entorno de pruebas de Twilio:

Ilustración 39 Notificación automatizada recibida mediante la pasarela de Twilio. Fuente: Elaboración propia (2026).

Como se visualiza en la pantalla del dispositivo móvil, la recepción del mensaje "You are all set" confirma que la conexión entre la aplicación de monitoreo y la API de Twilio se ha establecido correctamente. Este paso de validación visual es crucial en el proceso de desarrollo, ya que asegura que el sistema está técnicamente capacitado para enviar notificaciones de alerta en tiempo real. De esta manera, se garantiza que ante cualquier anomalía o sustracción de equipos en el Laboratorio de Electromecánica de la ULEAM el administrador recibirá una notificación inmediata, validando la operatividad de la pasarela de mensajería antes de su implementación definitiva en un entorno de producción institucional..

4.4 Conclusión

En este capítulo se estructuró y diseñó la propuesta técnica del sistema inteligente de videovigilancia, estableciendo las bases metodológicas y operativas necesarias para su despliegue en el laboratorio de la ULEAM. Mediante la aplicación del marco de trabajo Scrum se organizó el desarrollo iterativo del software, garantizando una planificación ordenada y una adecuada adaptabilidad frente a los requerimientos técnicos del entorno académico.

Se definieron de manera integral los recursos humanos, tecnológicos y económicos requeridos, destacando la selección del lenguaje Python, el entorno Visual Studio y la plataforma Roboflow para el entrenamiento del modelo de visión artificial. La integración de

estos componentes tecnológicos permitió consolidar una arquitectura sólida optimizada para el procesamiento eficiente de imágenes y la gestión automatizada de la seguridad de los equipos.

Finalmente el desglose de los sprints de desarrollo permitió evidenciar la implementación práctica de los módulos de autenticación segura, captura de vídeo mediante RTSP y procesamiento por hilos en segundo plano. Estas fases demostraron la viabilidad técnica de la propuesta, estableciendo un sistema automatizado, confiable y capaz de responder de forma oportuna ante cualquier incidencia detectada en el recinto.

Capítulo V

5 Evaluación de resultados

5.1 Introducción

En este capítulo se evalúa el rendimiento operativo y la efectividad del sistema inteligente de videovigilancia implementado en el Laboratorio de la ULEAM. A través de métricas cuantitativas y cualitativas, se analiza la precisión del modelo de visión artificial (YOLO), la estabilidad del streaming de vídeo mediante el protocolo RTSP y la eficiencia en el envío de alertas automatizadas a través de Twilio. El propósito es contrastar el funcionamiento del software frente a los problemas iniciales de control manual de activos.

5.2 Presentación y monitoreo de resultados

Durante la fase de pruebas operativas en el laboratorio, el sistema se ejecutó de forma continua bajo diferentes escenarios de iluminación y flujo de usuarios. Los resultados obtenidos se reflejan en el comportamiento del panel web en tiempo real y sus funciones.

5.2.1 Validación visual del módulo de autenticación y acceso

Como parte de la evaluación operativa del sistema, se verificó el correcto despliegue de la interfaz gráfica de inicio de sesión desarrollada en el primer ciclo del proyecto. El diseño

cumple con los estándares de usabilidad y seguridad establecidos, garantizando que el usuario deba autenticarse obligatoriamente antes de tener acceso al panel de control principal del laboratorio.

El desarrollo de este módulo se integró de forma sincronizada con la base de datos y la lógica de control, permitiendo que el sistema valide credenciales de manera inmediata y bloquee accesos no autorizados. A continuación, se presenta el resultado visual obtenido durante la ejecución local de la aplicación:

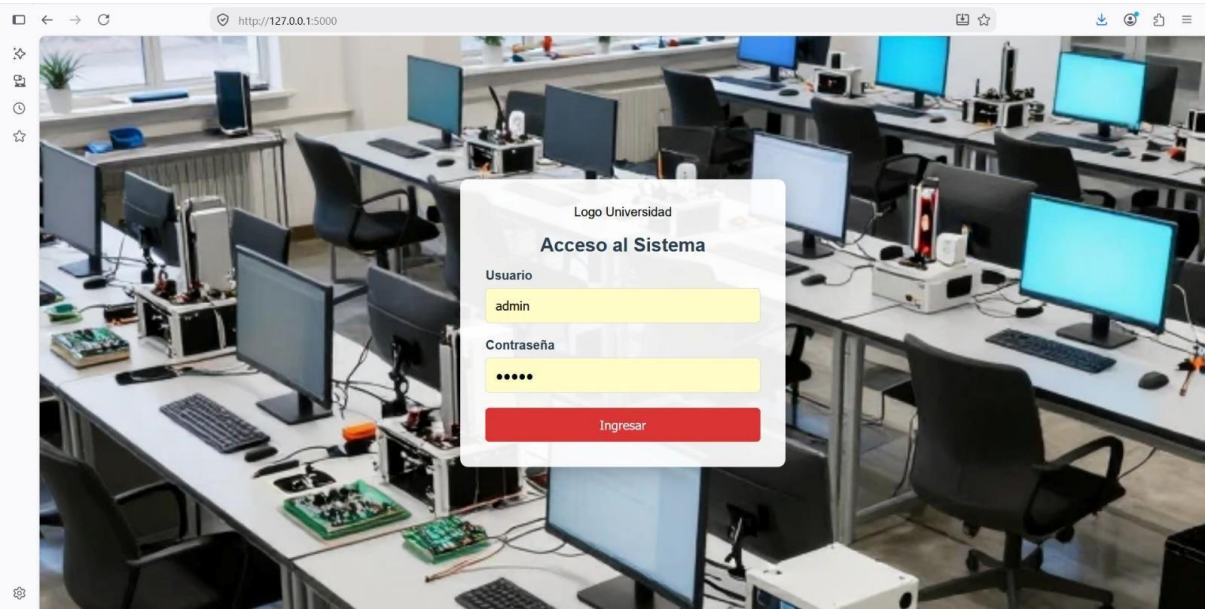


Ilustración 40 Interfaz gráfica del login del sistema. Fuente: Elaboración propia (2026).

La ilustración anterior evidencia la interfaz de acceso final operando en el entorno web local. Como se observa, el sistema solicita de manera limpia y estructurada las credenciales correspondientes, permitiendo un ingreso seguro y diferenciado para el administrador del laboratorio de la ULEAM.

5.2.2 Eficiencia en la Detección de Objetos

El modelo entrenado en Roboflow con 20 clases (total de equipos) logró identificar de manera consistente la presencia y ubicación de los equipos informáticos. Gracias a las técnicas de aumento de datos el sistema mantuvo una tasa de acierto estable incluso ante variaciones de luz natural y sombras proyectadas a lo largo del día.

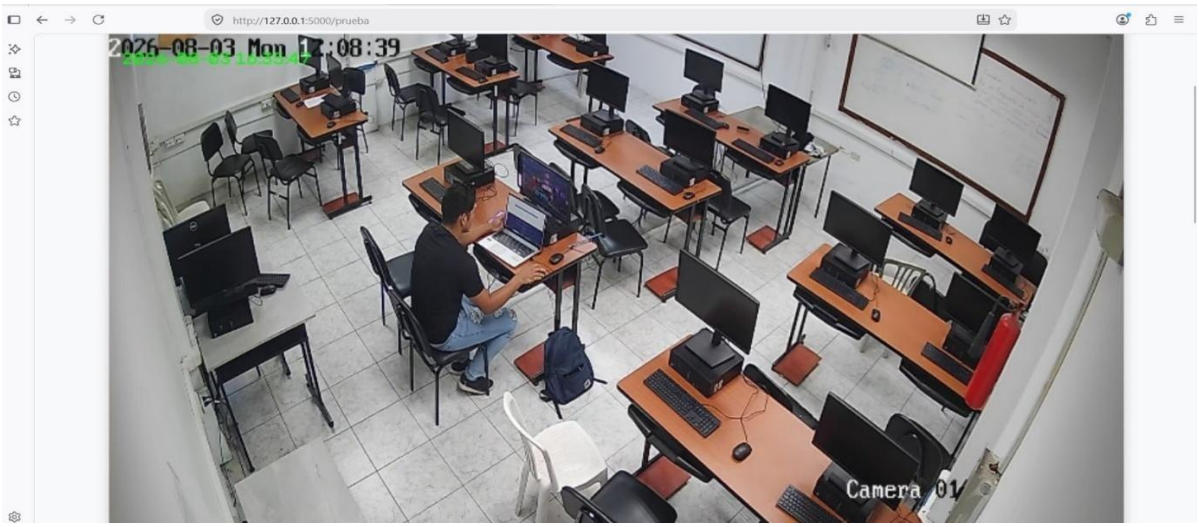


Ilustración 41 Visualización de la detección de equipos en tiempo real mediante el modelo de IA. Fuente: Elaboración propia (2026).

5.2.3 Estabilidad en el Monitoreo Asíncrono

La actualización de la interfaz mediante solicitudes fetch cada dos segundos permitió reflejar el estado real de los equipos ("Presente" o "Ausente") sin generar latencia ni congelamientos en el navegador del operador.

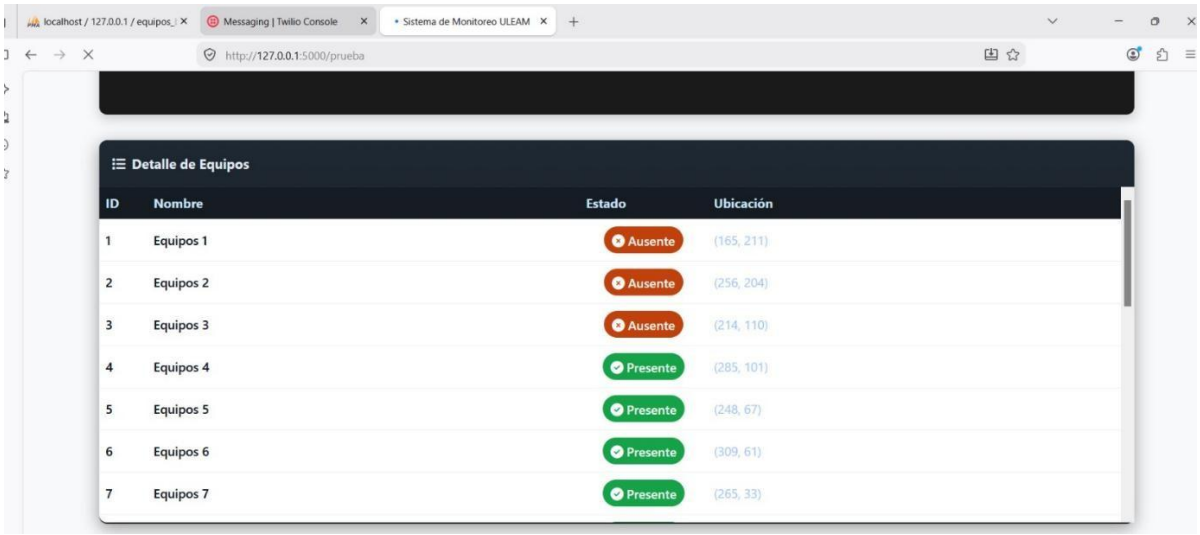


Ilustración 42Registro en consola del monitoreo y procesamiento asíncrono en segundo plano. Fuente: Elaboración propia (2026).

La ilustración anterior muestra la traza de ejecución en el entorno de desarrollo evidenciando la estabilidad del núcleo lógico al procesar de forma automatizada las imágenes del laboratorio sin afectar el rendimiento operativo de la plataforma web.

5.2.4 Respuesta del Sistema de Alertas

El algoritmo de consistencia temporal evitó falsas alarmas ante oclusiones momentáneas (como el paso fugaz de un estudiante), asegurando que las notificaciones de

emergencia y los mensajes de WhatsApp por ausencia de equipos se despacharan únicamente cuando la incidencia superaba el umbral de persistencia establecido.

Durante las pruebas de validación, el sistema demostró una alta efectividad, enviando las alertas de texto de forma automatizada y sin demoras significativas una vez superado el umbral de persistencia de la incidencia.

Ilustración 43 Notificación de alerta automatizada recibida vía WhatsApp. Fuente: Elaboración propia (2026).

La ilustración anterior evidencia la recepción en tiempo real de la alerta generada por el software. Se aprecia el mensaje automatizado con el detalle de la incidencia detectada, confirmando el cierre exitoso del ciclo de seguridad y monitoreo en el laboratorio.

Para evidenciar el comportamiento operativo de la plataforma bajo escenarios reales de prueba en el laboratorio de la ULEAM, se presenta a continuación el registro de salida de las notificaciones enviadas:

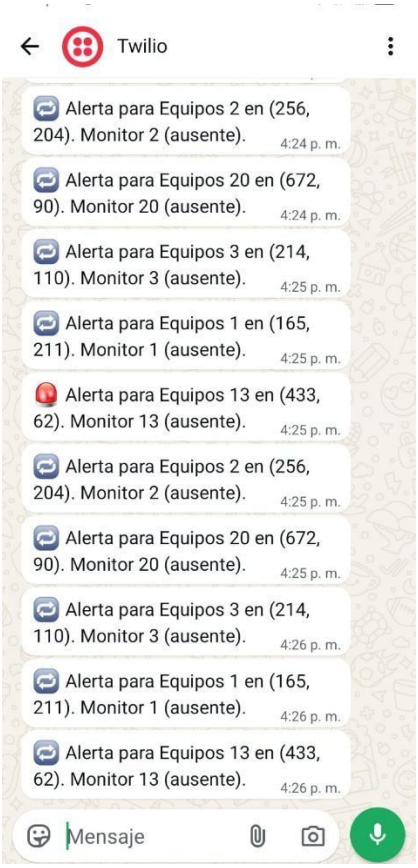


Ilustración 44 Historial de notificaciones de alerta automatizadas recibidas vía WhatsApp durante la ejecución del sistema. Fuente: Elaboración propia (2026).

Como se observa en la ilustración anterior el panel de chat refleja la recepción fluida y consecutiva de las alertas generadas por el software de monitoreo. En cada mensaje automatizado se detallan con absoluta precisión los datos de la incidencia, tales como el identificador del equipo afectado (por ejemplo, Monitor 2 o Monitor 13) y sus respectivas coordenadas espaciales dentro de las instalaciones. Esta evidencia confirma el cierre exitoso del ciclo de seguridad desde la detección mediante visión artificial y el filtrado por el algoritmo de consistencia temporal, hasta el despacho efectivo de los avisos en tiempo real al dispositivo del administrador, validando la robustez operativa de todo el proyecto.

5.3 Interpretación objetiva

Los resultados demuestran que la automatización del control de inventario y seguridad mediante inteligencia artificial supera significativamente al sistema manual anterior. La reducción de riesgos de pérdida y el registro automatizado de movimientos validan la hipótesis del proyecto. El uso de hilos en segundo plano (threading) garantizó que el procesamiento pesado de la red neuronal no afectara el rendimiento general del servidor local, confirmando la viabilidad técnica y operativa del software implementado en la ULEAM.

Ilustración 45 Vista general e integración del sistema operando en el entorno web. Fuente: Elaboración propia (2026).

La ilustración anterior sintetiza el funcionamiento integral de la propuesta desarrollada. Se visualiza la plataforma web consolidada, donde confluyen de manera síncrona el streaming de vídeo en tiempo real, el control dinámico del estado de los equipos y las notificaciones automáticas, validando con éxito el cumplimiento de los objetivos planteados en la investigación.

5.3.1 Diseño y estructuración del pie de página

Como parte del desarrollo integral de la interfaz de usuario, se cuidó minuciosamente la identidad visual institucional correspondiente a la Universidad Laica Eloy Alfaro de Manabí (ULEAM). Para ello, se incorporó un pie de página (footer) estructurado de manera profesional en la vista principal del sistema.

Este componente no solo otorga una presentación formal y alineada a los estándares de la carrera de Tecnologías de la Información, sino que delimita de forma estética el espacio de trabajo del operador en el laboratorio, integrando los principios institucionales dentro del diseño web adaptativo.

Ilustración 46 Diseño y estructura del pie de página institucional en la interfaz. Fuente: Elaboración propia (2026).

Capítulo VI

6 Conclusiones y recomendaciones

6.1 Conclusiones

Se cumplió a cabalidad con el diagnóstico de la problemática en el Laboratorio de la ULEAM, identificando que el control de acceso manual y la falta de supervisión automatizada de los equipos incrementaban el riesgo de vulnerabilidades y pérdidas, justificando la necesidad de una solución tecnológica.

Se cumplió con el diseño y desarrollo de la propuesta mediante la metodología ágil Scrum, integrando un modelo de visión artificial entrenado en Roboflow y un núcleo lógico en Python con Flask, logrando un software robusto, estructurado y adaptado a los requerimientos del laboratorio.

Se cumplió con la implementación exitosa del sistema de alertas automatizadas y pruebas de comportamiento demostrando a través de la evaluación de resultados que la plataforma es capaz de monitorear en tiempo real, evitar falsas alarmas y notificar incidencias de forma oportuna.

6.2 Recomendaciones

Se recomienda la adopción institucional de este sistema de videovigilancia con IA como herramienta oficial de control de activos en los laboratorios de la extensión El Carmen, promoviendo su escalabilidad hacia otras áreas académicas de alta concurrencia de equipos tecnológicos.

Se sugiere incorporar en futuras versiones del software un módulo de reconocimiento facial mediante Deep Learning para identificar de manera nominal al personal o estudiantes que interactúan directamente con los equipos, complementando la detección estática actual de los dispositivos.

Se aconseja realizar reentrenamientos periódicos del modelo en Roboflow (incorporando nuevas muestras de imágenes ante posibles cambios físicos en la distribución del mobiliario) y realizar mantenimientos preventivos en la red local para asegurar la estabilidad del flujo RTSP de la cámara de seguridad.

7 Bibliografía

Ariel, G. D. (2023). *Videovigilancia comunitaria.* Buenos Aires: Editorial Autores De Argentina.

Arnulfo Cifuentes Orlarte, C. A. (2017). *Sistema de gestión de la seguridad y salud en el trabajo.* Bogota: Edicion de la U.

Castro Delgado, A. J., y Caicedo Plúa, C. R. (2022). *Implementación de un sistema de vigilancia mediante cámaras, sensores y alarmas para el campus del complejo universitario.*

Checa, M., Torres, J., Valencia, F., y Jácome, P. (2025). Fortalecimiento de la seguridad con el uso de cámaras CCTV en institutos de educación superior. *The thinker's Journal, 1*(1).

Cob Parro, A. C., Losada Gutiérrez, C., Marrón Romera, M., Gadel Vicente, A., y Bravo Muñoz, I. (2021). Smart video surveillance system based on edge computing. *Sensors, 21*(9). https://doi.org/10.3390/s21092958

Coleman, J., Jocham, R., Sutherland, J., Ballarin, A., y Briceño, K. (11 de Junio de 2025). *Paquete de expansión de la Guía Scrum*. https://scrumexpansion.org/es/scrum-guideexpanded/2025.6/

Communications, Axis. (2025). *The state of AI in video surveillance.* Methodology.

Contributed by. (2025). *¿Qué es un NVR? Todo explicado de forma clara*. eufy: https://www.eufy.com/eu-es/blogs/security-camera/what-is-an-nvr

Dardour, A. E. (2025). Video Surveillance and Artificial Intelligence for Urban Security in Smart Cities: A Review of Empirical Studies (2018–2024). *Computer Sciences & Mathematics Forum*.

Donetonic. (2022). *¿Qué es el Sprint Planning?* https://donetonic.com/es/que-es-el-sprintplanning/

Dyreborg, J., Lipscomb, H., Nielsen, K., Törner, M., Rasmussen, K., y Frydendall, K. (2022). Intervenciones de seguridad para la prevención de accidentes laborales: una revisión sistemática. *Revisiones sistemáticas de Campbell, 2*(18), 54-56. https://doi.org/https://doi.org/10.1002/cl2.1234

ENIUN. (24 de Abril de 2025). *Metodología Scrum para el desarrollo de software ágil.* https://www.eniun.com/metodologia-scrum-desarrollo-softwareagil/#51_Daily_stand-up_tambien_llamada_daily_meeting_o_reunion_diaria

Evany Anne, M. B. (2025). Advancing intelligent surveillance: A comprehensive hybrid deep learning framework for anomaly detection, violence recognition, and person reidentification. *Multimedia Tools and Applications*.

Evany Anne, M. B. (2025). Advancing intelligent surveillance: A comprehensive hybrid deep learning framework for anomaly detection, violence recognition, and person reidentification. *Multimedia Tools and Applications*.

Ferone, A., Maratea, A., Camastra, F., Ciaramella, A., Staiano, A., Lettiero, M., . . . Spoleto, A. (2025). AiWatch: A distributed video surveillance system using artificial intelligence and digital twins technologies. *Technologies, 13*(5). https://doi.org/10.3390/technologies13050195

García Mata, F. J. (2010). *videovigilancia:CCTV usando videos IP.* vertice.

Gutiérrez Meneses, D. (2021). *Sistema de videovigilancia basado en visión artificial para espacios institucionales.*

Huang, F.-L., Chen, K.-Y., y Su, W.-H. (2024). Knowledge development trajectories of intelligent video surveillance domain. *Sensors, 24*. https://doi.org/10.3390/s24072240

Idrobo Vivar, Á. A. (2023). *Inteligencia artificial para videovigilancia y control de acceso.* Universidad Tecnológica Israel.

IEEE Access . (2024). Intelligent video surveillance system. *IEEE Access*.

Instituto Nacional de Seguridad y Salud . (26 de Octubre de 2023). *Identificación y control de los riesgos laborales en pymes.* INSST: https://www.insst.es/documentacion/materialtecnico/documentos-tecnicos/identificacion-y-control-de-los-riesgos-laborales-enpymes-2023

Li, X. &. (2020). Evolution of video surveillance systems: From CCTV to intelligent monitoring. *IEEE Access*.

Lozada, J. (2014). Inves tigación Aplicada: Definición, Propiedad Intelectual e Indus tria. *Dialnet, 3*, 47-50.

MacNeil, C. (7 de Febrero de 2026). *Guía de retrospectiva Scrum: qué es y cómo hacerla*. https://asana.com/es/resources/sprint-retrospective

Ministerio de Trabajo y Seguridad Social. (2025). *Resolución 1016 de 1989, por la cual se reglamenta la organización, funcionamiento y forma de los Programas de Salud Ocupacional que deben desarrollar los patronos o empleadores en el país.* Decreto Único Reglamentario del Sector Trabajo.

Myagmar, Y., y Kim, W. (2023). A Survey of Video Surveillance Systems in Smart City. *Electronics, 12*(17). https://doi.org/10.3390/electronics12173567

Olaniyi, O., Ganiyuo, S., y Akam, S. (2023). Intelligent Video Surveillance Systems: A. *Copyright © INESEG, 1*(1).

Organización Internacional de Normalización. (2025). *Seguridad en el trabajo: una guía para proteger la salud de las personas en el trabajo.* ISO: https://www.iso.org/es/sst/seguridad-trabajo

Organización Internacional del Trabajo. (2022). *Principios fundamentales de seguridad y salud en el trabajo.*

Pérez León, G. (18 de Abril de 2023). *Ejemplo de la investigación de campo*. GPL Research: https://gplresearch.com/investigacion-de-campo/

Pérez, A. (10 de Julio de 2024). *En qué consiste el método hipotético-deductivo*. Tesis Doctorales Online: https://tesisdoctoralesonline.com/en-que-consiste-el-metodohipotetico-deductivo/#Que_es_el_metodo_hipotetico-deductivo

Rehkopf, M. (2026). *Sprints de scrum*. ATLASSIAN: https://www.atlassian.com/es/agile/scrum/sprints

Rodríguez Jiménez, A., y Pérez Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Scielo*(82), 179-200. https://doi.org/https://doi.org/10.21158/01208160.n82.2017.1647

Rodríguez Moguel, E. (2005). *Metodología de la Investigación.* México: Universidad Juárez Autonoma de Tabasco. https://doi.org/968-5748-66-7

San Román Lana, I. (2019). Sistema context-aware de videovigilancia inteligente bajo el paradigma edge-computing. *Tesis doctoral*.

Sánchez Quirola, D. A. (2021). *Diseño de un plan de acción para la mejora de procesos del departamento de Calidad de importaciones de una empresa de Agenciamiento de aduana ubicada en la ciudad de Guayaquil.*

Senstar Corporation. (2025). *Componentes de los sistemas de videovigilancia*. SENSTAR: https://senstar.com/es/senstarpedia/componentes-de-los-sistemas-de-videovigilancia/

Silva Frey, F. F. (2021). *Gestión de riesgos laborales: estrategias organizacionales, fundamentos físicos, metodologías e innovación preventiva* . BRiobamba, Ecuador: Universidad Nacional de Chimborazo.

Tipán Pérez, K. A. (2025). *Sistema de videovigilancia IP para la seguridad de la Quinta Nápoles.* Proyecto Integrador.

Torresano Melo, M., y Calles López, J. (2018). *La gestión de la información para la prevención del delito.* Escuela de Gobierno del IDE Business School.

Yao, S. (2024). *INTEGRATING AI INTO CCTV SYSTEMS: A COMPREHENSIVE EVALUATION OF SMART VIDEO SURVEILLANCE IN COMMUNITY SPACE WITH ONLINE ANOMALY TRAINING.* University of North Carolina at Charlotte.

Yuber Rico Venegas, D. E. (2020). *Enfoques y gestión en seguridad.* Bogota: Escuela de Postgrados Fuerza Aérea Colombiana.

Zamora, B. (14 de Abril de 2018). *El Método Estadístico*. scribd: https://es.scribd.com/document/376315097/El-Metodo-Estadistico#google_vignette

Zhezherau, A. (25 de Septiembre de 2025). *Daily Scrum: Qué es, agenda y patrones que se deben evitar*. https://www.wrike.com/scrum-guide/daily-scrum/

Anexos

Anexo Aprobación de tema

Outlook

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

Desde NOTIFICACIONES TITULACION <notificaciones.titulacion@uleam.edu.ec>
Fecha Vie 15/08/2025 14:02
Para MORA MARCILLO ALEX BLADIMIR <alex.mora@uleam.edu.ec>
CC VERA LOOR MILLER EFRAIN <e1351912348@live.uleam.edu.ec>; REASCOS PINCHAO RAUL SAED <raul.reascos@uleam.edu.ec>

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Universidad Laica Eloy Alfaro de Manabí

Periodo 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 DE VIDEOVIGILANCIA CON IA PARA LA GESTIÓN DE SEGURIDAD EN EL LABORATORIO DE ELECTROMECÁNICA DE ULEAM 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.

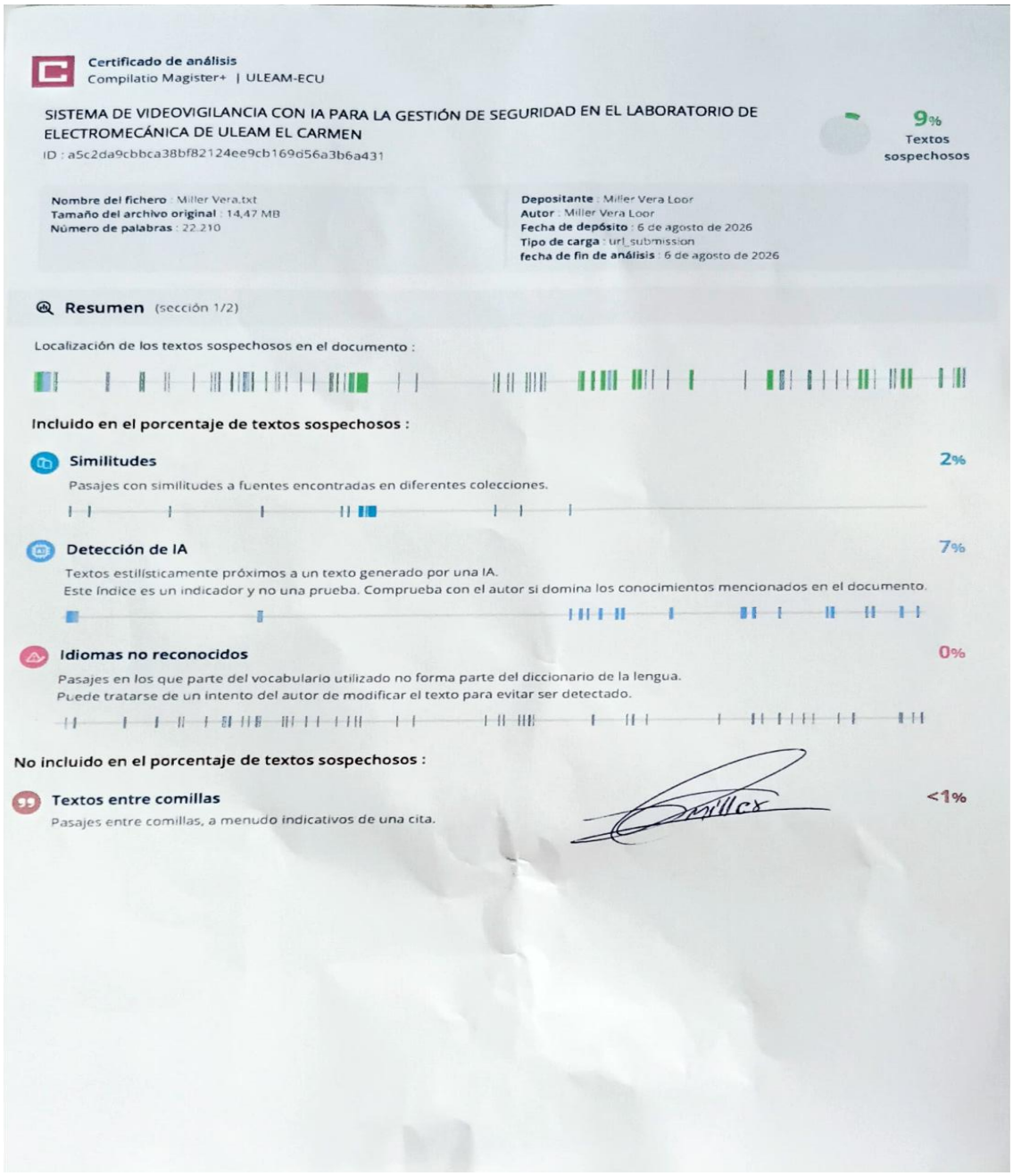
Apellidos y nombres del tutor asignado: MORA MARCILLO ALEX BLADIMIR

Apellidos y nombres del estudiante: VERA LOOR MILLER EFRAIN

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2025-2

Anexo BInstrumento de entrevista



Certificado de análisis
Compilatio Magister+ | ULEAM-ECU

SISTEMA DE VIDEOVIGILANCIA CON IA PARA LA GESTIÓN DE SEGURIDAD EN EL LABORATORIO DE ELECTROMECÁNICA DE ULEAM EL CARMEN

ID : a5c2da9cbbca38bf82124ee9cb169d56a3b6a431

9% Textos sospechosos

Nombre del fichero : Miller Vera.txt
Tamaño del archivo original : 14,47 MB
Número de palabras : 22.210

Depositante : Miller Vera Loor
Autor : Miller Vera Loor
Fecha de depósito : 6 de agosto de 2026
Tipo de carga : url_submission
fecha de fin de análisis : 6 de agosto de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :

Incluido en el porcentaje de textos sospechosos :

Similitudes 2%
Pasajes con similitudes a fuentes encontradas en diferentes colecciones.

Detección de IA 7%
Textos estilísticamente próximos a un texto generado por una IA.
Este índice es un indicador y no una prueba. Comprueba con el autor si domina los conocimientos mencionados en el documento.

Idiomas no reconocidos 0%
Pasajes en los que parte del vocabulario utilizado no forma parte del diccionario de la lengua.
Puede tratarse de un intento del autor de modificar el texto para evitar ser detectado.

No incluido en el porcentaje de textos sospechosos :

Textos entre comillas <1%
Pasajes entre comillas, a menudo indicativos de una cita.

Anexo Reporte sistema antiplagio

La presente entrevista está dirigida al administrador con el propósito de conocer la situación actual del laboratorio, sus procesos operativos y las principales dificultades que enfrenta en su gestión diaria. A continuación, se detallan las interrogantes planteadas:

1. ¿Cuentan con reportes de ingreso al laboratorio?
2. ¿Existe en la actualidad un protocolo oficial para el control de ingreso de los estudiantes?
3. ¿Han importado capacitaciones sobre la seguridad del laboratorio en este ciclo académico?
4. ¿Considera que el registro manual actual es un método seguro para controlar el ingreso y salida de los estudiantes?
5. ¿Considera una mejor opción implementar un sistema de videovigilancia inteligente en el laboratorio?
6. ¿Cree que se reduciría los incidentes en el laboratorio con un sistema de inteligencia artificial?
7. ¿Qué considera sobre la propuesta de un sistema inteligente para facilitar y agilizar el acceso del laboratorio?
8. ¿Cree que las medidas actuales permiten la rapidez de intervenir en algún incidente?

Anexo C Instrumento encuesta

Anexo D Fotografías de los materiales utilizados

Cable UTP Dahua Cat6 (305m): Cable de red de categoría 6 compuesto 100% de cobre, diseñado para instalaciones de alta exigencia y transmisión de datos a alta velocidad. Es

ideal para interconectar cámaras de seguridad, sistemas de videovigilancia y equipos de red, garantizando un rendimiento óptimo en largas distancias.

Extensor HDMI por cable de red (hasta 60 metros): Dispositivo electrónico que permite extender la señal de video y audio en alta definición (HDMI) utilizando un cable UTP convencional. Facilita la conexión entre fuentes de video y pantallas o proyectores ubicados a distancias prolongadas de hasta 60 metros sin pérdida significativa de calidad.

Anexo E Factura

COMPUFENIX S.A.

Emisor: TECHNOLOGY IMPORT COMPUFENIX S.A
RUC: 1792364094001
Matriz: LA MAGDALENA / CABO LUIS MINACHO S11-193 Y ALONSO DE ANGULO
Correo: facturacion@compufenix.com
Teléfono: 02 2617 441
Obligado a llevar contabilidad: SI
Contribuyente Especial: 1027E

FACTURA **No.001-100-000091820**

Número de Autorización:
0308202601179236409400120011000000918204451942917

Fecha y hora de Autorización:
03/08/2026 15:22:45

Ambiente: PRODUCCION
Emisión: NORMAL
Clave de Acceso:

0308202601179236409400120011000000918204451942917

Razón Social: VERA LOOR MILLER EFRAIN
Dirección: S/N
Fecha Emisión: 03/08/2026

RUC/CI: 1351912348
Teléfono: 099 594 4833
Correo: millervera1997@gmail.com

Código Principal	Cantidad	Descripción	Detalles Adicionales	Precio Unitario	Descuento	Total
CABLEDAH002	1.00	CABLE UTP DAHUA DH-PFM920I-6UN CAT6 305MT 100% CU INT		113.0000	$0.00	$113.00
EXTENSOR004	1.00	EXTENSOR HDMI POR CABLE DE RED HASTA 60MT		15.9000	$0.00	$15.90
TRANSPORTE2	1.00	LOGISTICA-TRANSPORTE		11.0000	$0.00	$11.00

Información Adicional

Descripción	RETIRA SERVIENTREGA EL CARMEN

Formas de pago

Otros con Utilización del Sistema Financiero	$160.88	0 días

Subtotal Sin Impuestos:	$139.90
Subtotal 15%:	$139.90
Subtotal 5%:	$0.00
Subtotal 0%:	$0.00
Subtotal No Objeto IVA:	$0.00
Descuentos:	$0.00
ICE:	$0.00
IVA 15%:	$20.98
IVA 5%:	$0.00
Servicio %:	$0.00
Valor Total:	$160.88

Recepción de retenciones:

retencionesclientes@compufenix.com

SINCHIGUANO CHIRIBOGA CESAR AUGUSTO

ROBOTIA

Dirección Matriz: Barrio: LOTIZACION JARAMILLO Calle: CORONEL VICTOR ASTUDILLO Numero: S/N Interseccion: SALUSTIO GILER

Dirección Sucursal: Barrio: LOTIZACION JARAMILLO Calle: CORONEL VICTOR ASTUDILLO Numero: S/N Interseccion: SALUSTIO GILER

OBLIGADO A LLEVAR CONTABILIDAD NO

R.U.C.: 1720659406001

FACTURA

No. 001-100-000000219

NÚMERO DE AUTORIZACIÓN

0308202601172065940600120011000000002191543402316

FECHA Y HORA DE AUTORIZACIÓN: 03/08/2026 20:48:16

AMBIENTE: PRODUCCIÓN

EMISIÓN: NORMAL

CLAVE DE ACCESO

0308202601172065940600120011000000002191543402316

Razón Social / Nombres y Apellidos: VERA LOOR MILLER EFRAIN

Identificación 1351912348

Fecha 03/08/2026 Placa / Matrícula: Guía

Direccion:

Cod. Principal	Cod. Auxiliar	Cantidad	Descripción	Detalle Adicional	Precio Unitario	Subsidio	Precio sin Subsidio	Descuento	Precio Total
CÁMARAS		1.00	HOLA VISIÓN		173.913	0.00	0.00	0.00	173.91

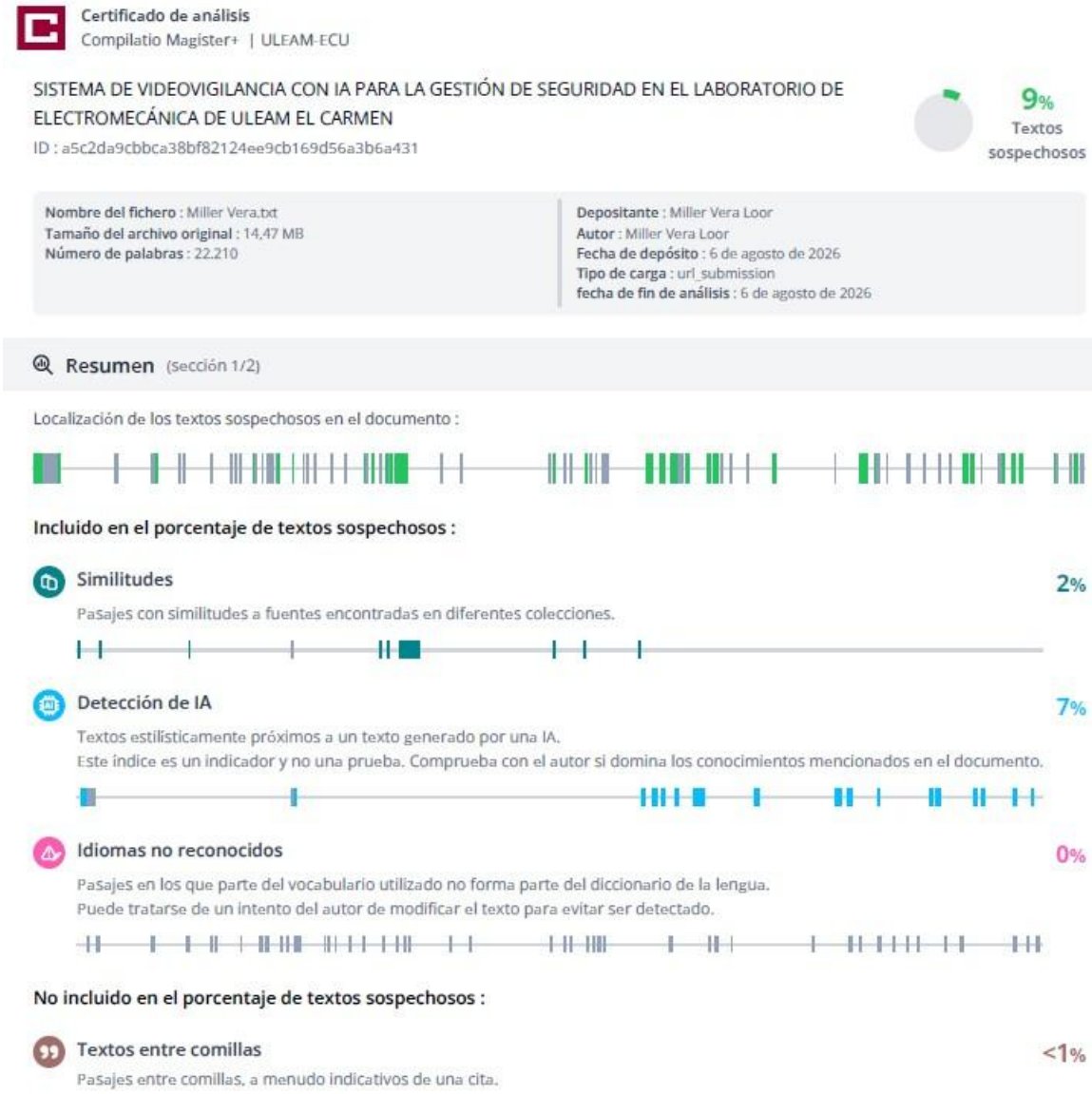
Información Adicional	
Email:	millervera1997@gmail.com

Forma de pago	Valor
01 - SIN UTILIZACION DEL SISTEMA FINANCIERO	200.00

SUBTOTAL 15%	173.91
SUBTOTAL NO OBJETO DE IVA	0.00
SUBTOTAL EXENTO DE IVA	0.00
SUBTOTAL SIN IMPUESTOS	173.91
TOTAL DESCUENTO	0.00
ICE	0.00
IVA 15%	26.09
IRBPNR	0.00
PROPINA	0.00
VALOR TOTAL	200.00

VALOR TOTAL SIN SUBSIDIO	0.00
AHORRO POR SUBSIDIO: (Incluye IVA cuando corresponda)	0.00

Anexo A Certificado de coincidencia académica



Certificado de análisis
Compilatio Magister+ | ULEAM-ECU

SISTEMA DE VIDEOVIGILANCIA CON IA PARA LA GESTIÓN DE SEGURIDAD EN EL LABORATORIO DE ELECTROMECÁNICA DE ULEAM EL CARMEN

ID : a5c2da9cbbca38bf82124ee9cb169d56a3b6a431

9% Textos sospechosos

Nombre del fichero : Miller Vera.txt
Tamaño del archivo original : 14,47 MB
Número de palabras : 22.210

Depositante : Miller Vera Loor
Autor : Miller Vera Loor
Fecha de depósito : 6 de agosto de 2026
Tipo de carga : url_submission
fecha de fin de análisis : 6 de agosto de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :

Incluido en el porcentaje de textos sospechosos :

Similitudes 2%
Pasajes con similitudes a fuentes encontradas en diferentes colecciones.

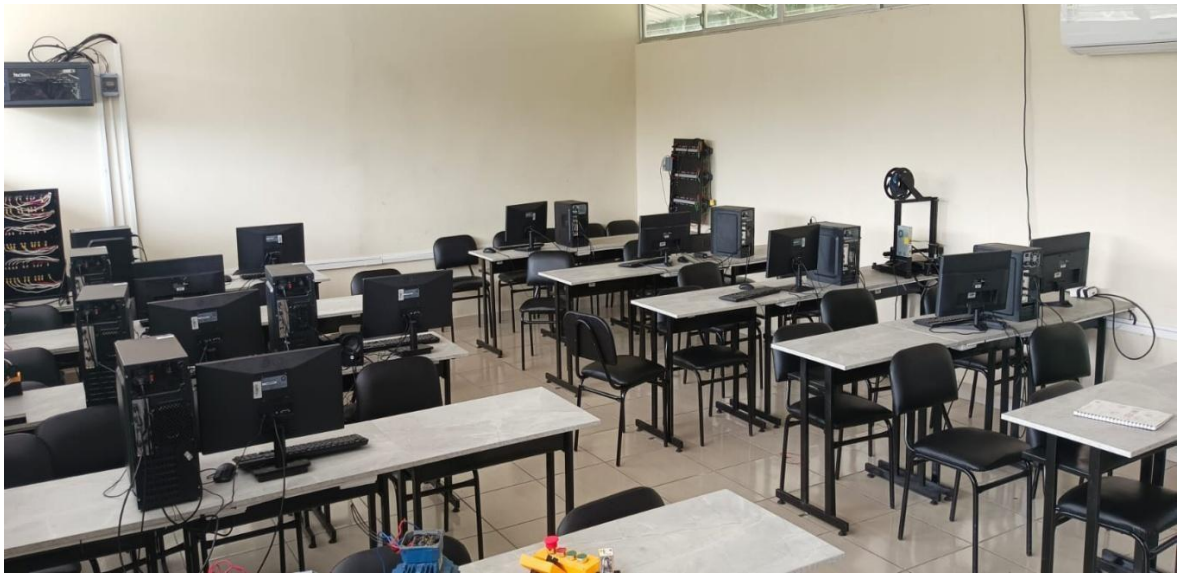
Detección de IA 7%
Textos estilísticamente próximos a un texto generado por una IA.
Este índice es un indicador y no una prueba. Comprueba con el autor si domina los conocimientos mencionados en el documento.

Idiomas no reconocidos 0%
Pasajes en los que parte del vocabulario utilizado no forma parte del diccionario de la lengua.
Puede tratarse de un intento del autor de modificar el texto para evitar ser detectado.

No incluido en el porcentaje de textos sospechosos :

Textos entre comillas <1%
Pasajes entre comillas, a menudo indicativos de una cita.

Anexo G Laboratorio 1 de la carrera electromecánica



Glosario

A

Algoritmo de consistencia temporal: Imagínate que es como un filtro inteligente que le enseña a la cámara a no asustarse ni disparar falsas alarmas por un movimiento rápido de un segundo (como una sombra o un insecto), asegurándose de que lo que ve sea real antes de reportarlo.

B

Backlog (Pila de producto): En los equipos de trabajo modernos, es la lista de pendientes o deseos donde se anota todo lo que hay que hacer y construir paso a paso para terminar el proyecto.

C

CCTV (Circuito Cerrado de Televisión): Los abuelitos de las cámaras de seguridad actuales; son sistemas tradicionales donde las cámaras se conectaban por cables directamente a monitores o grabadoras de cinta para vigilar de forma pasiva.

D

Dataset (Conjunto de datos): Es como el álbum de fotos o la biblioteca de entrenamiento que se le da a la inteligencia artificial para que aprenda a reconocer rostros, personas u objetos a base de verlos muchas veces.

E

Edge Computing (Computación en el borde):Es el truco tecnológico de hacer que la computadora o la cámara procesen la información ahí mismo donde están (en el borde), sin mandar todo a un servidor lejano, logrando así una velocidad impresionante.

Endpoint (Punto final): Es como la última parada de un viaje o el destino final de la información; puede ser la pantalla donde el guardia ve la cámara o el dispositivo móvil que recibe una alerta de seguridad.

F

Flask: Es una herramienta de programación en un lenguaje llamado Python que sirve para armar la estructura básica de páginas web de forma rápida y sencilla.

Frames per Second (Fotogramas por segundo): Imagina un libro de monitos que al pasar las páginas rápido da la sensación de movimiento; los FPS son la cantidad de "fotografías" estáticas que una cámara toma y muestra por cada segundo de video para que se vea fluido.

G

Git: Es como una máquina del tiempo y un diario de trabajo digital que usamos los ingenieros para guardar cada cambio que le hacemos al código, permitiendo volver atrás si algo sale mal o trabajar en equipo sin perder nada.

H

Hardware: Son todas las piezas físicas y tangibles que puedes tocar con tus manos; en este proyecto, se refiere a las cámaras, los cables, las computadoras y los soportes metálicos.

I

Inferencia: Es el momento exacto en que la inteligencia artificial, después de haber estudiado mucho, mira una situación nueva en la vida real y dice con seguridad: Ah, esto que veo aquí es tal cosa.

J

JSON (JavaScript Object Notation): Es un formato de texto muy sencillo y limpio que usan los programas y las páginas web para entenderse entre sí y pasarse datos de forma rápida (como cuando un programa le dice a otro: "Aquí está la lista de cámaras activas").

K

KPI (Indicador Clave de Rendimiento): Es como el tablero de un carro que te dice a qué velocidad vas o cuánta gasolina te queda; en un proyecto, son las métricas que usamos para saber si el sistema está funcionando bien y cumpliendo sus metas.

L

Latencia: Es el pequeño retraso o demora que ocurre desde que pasa algo frente a la cámara hasta que la computadora lo procesa y lo muestra en la pantalla.

M

Metadatos: Son como la "etiqueta invisible" o los datos sobre los datos; por ejemplo, cuando una foto guarda automáticamente la hora exacta en la fecha en que fue tomada, la cámara y el lugar exacto.

N

NVR (Network Video Recorder): Es el grabador de video en red; la evolución moderna de las viejas videograbadoras, que recibe las señales de las cámaras a través de internet o cables de red y la guarda de forma digital.

O

ONVIF: Es como un idioma universal o un acuerdo entre diferentes marcas de cámaras de seguridad del mundo para que, sin importar quién la fabricó, puedan entenderse y conectarse sin problemas a un mismo sistema.

P

Pipeline: Es como una línea de ensamblaje en una fábrica, pero de datos y código; un proceso por el cual la información pasa de una etapa a otra de forma ordenada hasta terminar una tarea.

PoE (Power over Ethernet): Una tecnología muy limpia y cómoda que permite enviar la corriente eléctrica y los datos de internet a través de un solo cable de red, evitando enredos de cables.

Q

Query (Consulta): Es la pregunta o la orden que le envías a una base de datos de manera técnica para que busque, ordene y te devuelva una información específica (por ejemplo: "Muéstrame los eventos de movimiento de ayer a las 3 PM").

R

Roboflow: Es una plataforma digital en la nube que ayuda a organizar, recortar, etiquetar y entrenar modelos de visión artificial de forma visual y guiada.

RTSP (Real-Time Streaming Protocol): Es el protocolo o caminito digital especializado que permite transmitir video en vivo y en tiempo real a través de una red local o de internet.

S

Sprint: Es un periodo corto de tiempo (por ejemplo, una o dos semanas) en el que un equipo se pone una meta fija para avanzar y entregar una parte funcional del proyecto.

T

Trazabilidad: Es la capacidad de poder seguir la pista o el rastro de algo; en este sistema, sirve para saber exactamente quién entró, a qué hora lo hizo y qué movimientos realizó en el laboratorio.

U

UI (User Interface / Interfaz de Usuario): Es el diseño, los botones, los colores y las pantallas con las que una persona interactúa de forma visual al usar un programa o una página web.

V

VLAN (Red de Área Local Virtual): Es una división lógica dentro de una misma red física de computadoras que sirve para separar el tráfico; por ejemplo, para que los videos de las cámaras de seguridad no saturen el internet que usan las oficinas administrativas.

W

WebSocket: Es una tecnología de comunicación súper rápida que permite que una página web y un servidor estén conversando en tiempo real y sin interrupciones, ideal para ver transmisiones de video en vivo o alertas instantáneas.

X

XML (Extensible Markup Language): Imagina que es como un idioma escrito estructurado con "etiquetas" (como pequeños rótulos que dicen dónde empieza y termina cada

cosa) que sirve para que diferentes programas de computadora compartan información ordenada, muy parecido a cómo guardamos documentos o configuraciones complejas.

Y

YAML: Es un formato de escritura muy ordenado y fácil de leer para los humanos, que los ingenieros utilizamos para configurar y dar instrucciones a los programas sobre cómo deben comportarse.

Z

Zero-day (Vulnerabilidad de día cero): Es como un escondite secreto o una debilidad en un programa o cámara que nadie conocía (ni siquiera sus creadores), y que los ciberdelincuentes descubren antes de que se pueda poner un parche de seguridad, representando un riesgo temporal hasta que se repara.