ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

"Análisis del Comportamiento Humano en Aglomeraciones de Estudiantes de FIEC: Una Perspectiva Integral usando tecnología de IoT y aprendizaje profundo (DetectGuard Pro)"

PROYECTO INTEGRADOR

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO EN TELEMÁTICA

Presentado por:
Jhonny Andres Zambrano Poma
Jorge Lucas Benavides

Guayaquil - Ecuador

AÑO 2023

Agradecimientos

Agradecemos de manera sincera y profunda a Dios, fuente de sabiduría y fortaleza, por habernos brindado la guía y la inspiración necesarias para llevar a cabo este estudio. Su gracia nos ha acompañado a lo largo de este proceso y nos ha permitido alcanzar nuestros objetivos Asimismo, queremos expresar nuestro agradecimiento a nuestros padres, cuyo apoyo inquebrantable y amor incondicional han sido un pilar fundamental en nuestra formación y desarrollo. Sus sacrificios y consejos han sido fundamentales en nuestra vida, y este logro es también un tributo a su dedicación. Extendemos nuestra gratitud a nuestros respetados profesores, quienes nos han brindado la educación y la orientación necesarias para adquirir los conocimientos y habilidades que hicieron posible la realización de este trabajo. Sus enseñanzas han sido invaluables. No podemos pasar por alto el agradecimiento a nuestro estimado tutor, el Ingeniero Durango Espinoza Rayner Stalyn, cuya orientación experta y apoyo constante fueron cruciales en la elaboración de este documento. Su dedicación, conocimiento y paciencia han sido esenciales para nuestro crecimiento académico y profesional. A todos los mencionados, les estamos eternamente agradecidos por ser parte integral de este logro. Sus contribuciones y apoyo han sido fundamentales en nuestro viaje hacia la culminación de este análisis del Comportamiento Humano en Aglomeraciones de Estudiantes de FIEC. Este trabajo no habría sido posible sin ustedes. Gracias por su constante aliento y confianza en nosotros.

Jorge Lucas Benavides

Agradecimientos

Quiero expresar mi más profundo agradecimiento a mi amada familia, quienes han sido el pilar fundamental durante mi travesía académica para completar esta tesis de grado. A mis padres, quienes desde el principio han sido una fuente inagotable de apoyo, aliento y sabiduría. Gracias por inspirarme con su ejemplo y por brindarme las bases que me permitieron alcanzar este logro. A mis hijos, quienes han compartido pacientemente su tiempo y comprensión mientras trabajaba en este proyecto. Su alegría y amor han sido mi motivación constante. En especial, quiero dedicar un agradecimiento especial a mi querida esposa. Tu apoyo incondicional, paciencia y comprensión han sido mi roca durante los desafíos de este camino académico. Gracias por estar a mi lado en cada paso y por ser mi fuente constante de inspiración. Este logro no solo es mío, sino de toda nuestra familia, que ha sacrificado y contribuido de manera invaluable para que este sueño se hiciera realidad.

Jhonny Zambrano Poma

Dedicatoria

Dedico este trabajo a mis amados padres, quienes a lo largo de los años han sido mi fuente inagotable de amor, apoyo y guía. Su sacrificio y dedicación inquebrantables han sido mi mayor inspiración y motor para seguir adelante. Cada logro que alcanzo es un reflejo de su amor y enseñanzas. Gracias por creer en mí y por ser la razón detrás de mi perseverancia. También dedico este trabajo a mis respetados profesores, quienes han sido faros de conocimiento en mi camino de aprendizaje. A través de su sabiduría, paciencia y dedicación, han iluminado mi camino, brindándome las herramientas y la orientación necesarias para crecer como estudiante y como individuo. Agradezco profundamente su influencia positiva en mi vida y en mi formación académica.

Jorge Lucas Benavides

Dedicatoria

Dedico este trabajo a mis amados padres, quienes a lo largo de los años han sido mi fuente inagotable de amor, apoyo y guía. Su sacrificio y dedicación inquebrantables han sido mi mayor inspiración y motor para seguir adelante. Cada logro que alcanzo es un reflejo de su amor y enseñanzas. Gracias por creer en mí y por ser la razón detrás de mi perseverancia.

Jhonny Zambrano Poma

Declaración Expresa

"La responsabilidad del contenido de este Trabajo Final de Graduación, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral."

(Reglamento de Graduación de la ESPOL)

Jorge Lucas Benavides
ESTUDIANTE DE LA MATERIA

Jhonny Andres Zambrano Poma
ESTUDIANTE DE LA MATERIA

Evaluadores

Firmado electrónicamente por:
IGNACIO MARIN GARCIA

Ing. Ignacio Marin
PROFESOR DE LA MATERIA

Firmado electrónicamente por:
RAYNER STALYN DURANGO ESPINOZA

Ing. Rayner Durango
PROFESOR TUTOR

Resumen

"La seguridad en la era moderna se ha convertido en una preocupación importante tanto en los entornos universitarios como en los entornos urbanos que siguen creciendo. El crecimiento constante de la población y la creciente densidad urbana han creado grandes desafíos en relación con el seguimiento y la prevención de actividades ilícitas, con especial atención a la prevención del robo",(Zavaleta y cols., 2012).

El crecimiento de las ciudades y la concentración de personas en campus y áreas urbanas plantea una serie de cuestiones críticas en materia de seguridad. El bienestar de estudiantes, profesores, residentes y visitantes se ha convertido en una máxima prioridad a medida que los riesgos de seguridad en la vida cotidiana se vuelven cada vez más evidentes (Hartjen, 2023). La necesidad de proteger la integridad y los bienes de la sociedad es innegable y urgente.

Queda clara la importancia de desarrollar soluciones efectivas para monitorear y prevenir actividades ilegales, especialmente robos, en aglomeraciones urbanas y entornos académicos. La adopción de tecnologías avanzadas y un enfoque de seguridad integral surgen como una estrategia fundamental para superar estos desafíos y garantizar un entorno más seguro para (fastercapital.com, 2024).

El enfoque en la seguridad en entornos urbanos y académicos resalta la necesidad de investigación y soluciones innovadoras que puedan abordar eficazmente estos riesgos emergentes. Este proyecto integrador pretende contribuir a la comprensión y mitigación de estos desafíos, centrándose en el análisis detallado del comportamiento humano en situaciones de hacinamiento y la aplicación de tecnologías avanzadas, como el sistema "DetectGuard Pro", para mejorar la seguridad. y ciudades en general. Esta investigación representa un paso importante hacia la optimización de la seguridad y el bienestar en la sociedad moderna.

Abstract

In today's world, the analysis of security and human behavior has become crucial in densely populated environments such as university campuses and urban areas. This study focuses on the comprehensive analysis of human behavior in groups of students from the Faculty of Electrical and Computer Engineering (FIEC) through the use of IoT technology and deep learning techniques via the innovative "DetectGuard Pro"system.

The growth of cities and the intensification of urban density present significant challenges in terms of monitoring and preventing illegal activities, particularly thefts. The objective of this research is to comprehensively understand how students behave in crowded situations, including aspects such as student flow, social activities, and ultimately, security. The "DetectGuard Pro"system is presented as an innovative tool for analyzing and preventing undesirable situations in academic and urban environments.

The fundamental goal of this work is to contribute to the understanding of human dynamics in academic and urban contexts and demonstrate how cutting-edge technology can play an essential role in optimizing the security and quality of life for students. With this comprehensive approach, we aim to make a valuable contribution to the educational community and society at large, envisioning a safer and more protected future.

Abreviatura

FIEC Facultad de Ingeniería Electrónica y Computación

Wi-Fi Wireless Fidelity

TCP Protocolo de Control de Transmisión

RTCP Real Time Transport Protocol

IP Protocolo de Internet

IA Artificial Intelligent

ESPOL Escuela Superior Politecnica del Litoral

IoT Internet of Thing

Índice

Índice de cuadros

Índice de figuras

Capítulo 1

1. Introducción

En la actualidad, la seguridad que impera en espacios públicos, tanto en universidades como en centros comerciales, es una prioridad ineludible. Específicamente, en contextos universitarios, ya sean urbanos o en áreas de expansión pública (Segovia, 2024), se evidencia un aumento demográfico y la densificación de las ciudades. Estos fenómenos han generado desafíos considerables en términos de vigilancia y prevención de actividades que se centran en comportamientos específicos, con especial atención en la disuasión de conductas que conducen a resultados ilícitos.

El bienestar estudiantil, tanto para profesores como para residentes y visitantes, se ve amenazado por riesgos de seguridad que atraviesan la vida cotidiana. Esto subraya la necesidad urgente de salvaguardar la integridad y los bienes de la sociedad (Ferrer, 2024). En este contexto, se evidencia la importancia crucial de desarrollar soluciones eficaces para la implementación de sistemas que puedan prevenir actividades ilícitas, priorizando la adopción de tecnologías avanzadas y un enfoque de seguridad integral como estrategia fundamental.

En este caso, la proyección de posturas y posiciones que estudian el comportamiento de las personas con posibles riesgos aborda el tema de la psicología de acuerdo a sus actos(A., 2008). Este estudio se centra en la imperante necesidad de investigar e implementar soluciones innovadoras capaces de abordar de manera efectiva los riesgos emergentes en entornos urbanos y académicos. Con un enfoque detallado en el análisis del comportamiento humano en situaciones de hacinamiento y la aplicación de tecnologías de vanguardia, como el sistema "DetectGuard Pro", esta investigación busca contribuir significativamente a la optimización de la seguridad y el bienestar en la sociedad moderna.

1.1. Estado del Arte

Evolución de sistemas a soluciones avanzadas. La evolución de los sistemas de seguridad y monitorización ha sufrido cambios importantes en los últimos años. Los enfoques tradicionales han dado paso a soluciones avanzadas que aprovechan el poder de la IoT y las tecnologías de aprendizaje profundo para obtener una comprensión más profunda y precisa del comportamiento humano en entornos abarrotados(Ruz, 2020). Este cambio de paradigma ha permitido aumentar la eficiencia en la detección de situaciones anómalas y responder más rápidamente a posibles amenazas.

El Internet de las cosas (IoT) ha revolucionado la forma en que se recopilan y transmiten datos. En el contexto de la seguridad, IoT permite la recopilación de información en tiempo real sobre el comportamiento humano en multitudes(latam.Kaspersky.com, 2024). Dispositivos como cámaras, sensores de movimiento y otros elementos de IoT proporcionan datos en tiempo real que son importantes para comprender y analizar la dinámica de las multitudes y las interacciones humanas.

El aprendizaje profundo, una rama de la inteligencia artificial, ha demostrado ser una herramienta poderosa para detectar comportamientos sospechosos. Al aplicar algoritmos de aprendizaje profundo a los datos recopilados a través de sistemas de IoT, se pueden identificar patrones de comportamiento que pueden ser indicativos de situaciones de riesgo(Fastercapital.com, 2024). Este sistema puede aprender a reconocer comportamientos normales y anómalos, aumentando así la precisión de la detección de amenazas.

La implementación de sistemas avanzados de análisis del comportamiento humano enfrenta desafíos importantes. La integración de dispositivos de IoT en entornos académicos y urbanos puede ser un desafío y requiere una planificación cuidadosa(Samaniego, 2019). Los costos asociados con la adquisición y el mantenimiento de tecnología avanzada también son un factor importante a considerar. Además, la privacidad humana y la gestión ética de datos son cuestiones clave que deben abordarse adecuadamente en estos sistemas.

A pesar de los desafíos, este enfoque para analizar el comportamiento humano en multitudes de estudiantes representa una oportunidad única. El desarrollo de un modelo de seguridad académica innovador mediante la integración de IoT y el aprendizaje profundo tiene el potencial de mejorar significativamente la seguridad en los campus universitarios y las áreas urbanas(Jitterbit, 2021). Esta innovación no sólo ayudará a proteger a estudiantes y residentes, sino que también puede servir como ejemplo para futuras implementaciones de seguridad en entornos similares.

1.2. Planteamiento del Problema

La seguridad en entornos urbanos y académicos es un desafío persistente en la sociedad moderna. El aumento de la densidad demográfica y de la densidad de población en determinadas zonas ha aumentado la necesidad de abordar las cuestiones de seguridad de forma eficaz. En este contexto, la detección temprana y la prevención pro-activa de amenazas se ha convertido en un objetivo importante para garantizar la seguridad de ciudadanos y estudiantes. La reducción de la delincuencia es fundamental para minimizar los impactos negativos en el ámbito de aplicación y, al mismo tiempo, mejorar la percepción de seguridad y calidad de vida de la sociedad en general. Además, la disponibilidad de herramientas de investigación que permitan la consulta y evidencia para el seguimiento judicial es esencial para el proceso legal y la resolución de casos relacionados con la seguridad A continuación, en la Figura 1, se presenta una toma de captura de la cámara de 360 grados en el estacionamiento de FIEC (ESPOL).

Figura 1: Toma de captura de cámara 360 grados estacionamiento de FIEC (ESPOL)

Para el uso e implementación de técnicas de seguridad e incluso dividir las acciones y observar posibles comportamientos sospechosos se ha implementado un sistema de detección temprana capaz de comparar diferentes poses y acciones las cuales nos pueden ayudar a identificar pro activamente un posible comportamiento sospechoso de tal manera que este pueda ser advertido antes de que suceda el delito, para esto se presenta los diferentes puntos importantes para arribar el problema:

La **detección temprana** significa la capacidad de identificar amenazas y comportamientos sospechosos de manera temprana, antes de que se conviertan en incidentes graves(Ahijon, 2023). Esto implica el uso de tecnologías avanzadas, como sistemas de análisis de datos en tiempo real, para advertir sobre riesgos potenciales.

La **prevención pro-activa** consiste en tomar medidas preventivas antes de que ocurran incidentes de seguridad. Esto puede incluir implementar políticas de seguridad, capacitar al personal de seguridad y colaborar con las autoridades para identificar y abordar amenazas potenciales(Bizkaia.eus, 2024).

La **reducción de la delincuencia** es un objetivo fundamental para garantizar la seguridad en las zonas urbanas y académicas(Alvarado, 2017). Esto significa implementar estrategias y tecnologías que puedan disuadir a los delincuentes y reducir la incidencia del crimen, lo que a su vez reduce el impacto en las áreas donde se implementan estas medidas.

La implementación de medidas de seguridad efectivas resultará en un **menor impacto en las regiones** donde se implementen(Oas.org, 2024). Esto significa un entorno más seguro para residentes, estudiantes y visitantes, así como una reducción de los incidentes de seguridad.

Las **herramientas de investigación** de seguridad son esenciales para facilitar la audiencia y el seguimiento de cuestiones relacionadas con la seguridad(Gov.co, 2024). Proporciona pruebas cruciales para el proceso legal y contribuye a la imparcialidad de la justicia y la resolución de casos.

Para garantizar que los infractores sean procesados y procesados adecuadamente, es esencial contar con una **herramienta que pueda brindar asesoramiento y confirmar pruebas para el seguimiento legal**(et al, 2024).

Los **beneficios sociales** de abordar eficazmente las cuestiones de seguridad son múltiples. Estos incluyen una mayor conciencia sobre la seguridad en la comunidad, lo que ayuda a mejorar la calidad de vida y el bienestar general de los residentes y estudiantes (doctorado en seguridad y prevención, 2024). Una mayor seguridad aumenta la confianza y la tranquilidad en la vida cotidiana.

1.3. Justificación del Problema

El proyecto se enfoca en mejorar la seguridad en el departamento de seguridad de ESPOL FIEC, con un énfasis específico en la optimización de la comunicación interna y la gestión de la red segura con fines académicos. Se propone la implementación de una estructura organizacional confiable que permita la clasificación detallada y comparación de la información y los marcos transmitidos. Un componente innovador y esencial del proyecto es la integración de inteligencia artificial (IA), que no solo resuelve alarmas físicas en situaciones potencialmente riesgosas, sino que también se adapta dinámicamente mediante API actualizadas. Esto asegura la estabilidad y adaptabilidad del sistema, incluso en condiciones de tráfico de datos reducido.

La justificación de este proyecto radica en varios aspectos fundamentales:

- La propuesta facilita la colaboración con los departamentos de seguridad de la ESPOL, mejorando la coordinación y el intercambio de información para lograr respuestas más rápidas ante posibles amenazas.
- La utilización de redes de cámaras y técnicas de aprendizaje profundo mejora la detección temprana de comportamientos sospechosos, fortaleciendo la seguridad en el departamento de estacionamiento
- Entrenamiento de Inteligencia Artificial: La IA, con su entrenamiento continuo, es esencial para la comparación de imágenes y vectores de posicionamiento, permitiendo una detección precisa y respuestas rápidas ante amenazas.
- El impacto de este proyecto se extiende a una variedad de departamentos y facultades en la ESPOL. Los departamentos beneficiados incluyen el Centro de Tecnología de Información, los Centros de Investigación para la Biotecnología Sustentable del Ecuador, y facultades como Ingeniería Marítima y Ciencias del Mar, Artes y Diseño, Comunicación Visual, Ciencias Sociales y Humanísticas, Ingeniería Mecánica y Ciencias de la Productividad. Además, los estacionamientos cercanos a la ESPOL también se beneficiarán al vincularse a este sistema, ampliando así el alcance de la seguridad en la comunidad académica y sus alrededores. El proyecto no solo promoverá la seguridad, sino que también contribuirá al bienestar y la calidad de vida de la comunidad académica y la población circundante. Para realizar nuestro propósito de una seguridad eficaz y eficiente es necesario conocer los diferentes espacios públicos que se puedan encontrar en el área académica de ESPOL, un ejemplo de esto son:
  - Plaza de Facultad de Ingeniería en Electricidad y Computación.
  - Plaza de Facultad de Ciencias Naturales y Matemáticas.
  - Plaza de Facultad de Ingeniería en Mecánica y Ciencias de la Producción.

1.4. Propuesta de solución

Para abordar los desafíos de seguridad en un entorno universitario, en el cual se pueda evidenciar un tráfico urbano, se propone implementar un sistema de seguridad integrado que combine tecnologías avanzadas con un enfoque psicológico. De esta manera, se pueda optimizar y entrenar automáticamente con un sistema de aprendizaje profundo, acompañado de la tecnología IoT. Ante esta solución integral, se busca optimizar la prevención y proponer actividades ilícitas, priorizando el bienestar estudiantil, de los profesores y visitantes.

Para la vigilancia e implementación tecnológica avanzada, se instalará una cámara inteligente con análisis de vídeo en tiempo real. Además, se dispondrán sensores de movimiento para capturar con monitoreo continuo un área específica. Una inteligencia artificial, con integración de algoritmos de análisis de comportamientos humanos, aislará la captura de pantalla. De esta manera, podrá compararla con múltiples imágenes y posiciones creadas previamente por el aprendizaje aplicado. Este proceso desarrolla patrones de conductas y compara las imágenes, fusionando datos de vigilancia tecnológica y análisis psicológicos. Esto permite implementar alertas automáticas ante comportamientos anómalos detectados.

1.5. Objetivos

Objetivo General

Desarrollar un sistema de seguridad integral basado en tecnología de IoT y aprendizaje profundo cuyo producto resultante se denominara (DetectGuard Pro) para el análisis del comportamiento humano en aglomeraciones de estudiantes de FIEC, con el fin de garantizar la prevención pro-activa de amenazas y la reducción de delitos en espacios públicos académicos en ESPOL, específicamente en la FIEC.

Objetivos Específicos

1. Implementar una red de cámaras de seguridad y sensores de movimiento en los espacios públicos masivos académicos de la FIEC en la ESPOL, con un enfoque inicial en los espacios públicos más concurridos y áreas de estacionamiento.

2. Desarrollar y probar algoritmos de aprendizaje profundo en el área piloto, con el objetivo de detectar comportamientos sospechosos y clasificar situaciones de riesgo en entornos académicos masivos.

3. Proporcionar una herramienta de investigación que permita la consulta y la evidencia sólida para casos relacionados con la seguridad en los espacios públicos masivos académicos de la FIEC en la ESPOL.

4. Realizar pruebas para evaluar la seguridad y la calidad de vida de la comunidad académica y los residentes de la FIEC en la ESPOL antes y después de la implementación del sistema de seguridad.

Capítulo 2

2. Metodología

La metodología se lleva a cabo en diversas fases y etapas clave. Cada fase está diseñada para lograr objetivos específicos y contribuir al éxito general del proyecto. A continuación, se detalla la metodología propuesta:

Fase 1: Investigación y Planificación
Esta primera fase contara con tres etapas. La Primera esta es la de Análisis de la situación actual, la segunda etapa es la de Identificación de Necesidades y Requisitos, Finalmente la tercera etapa es la de Recolección de datos.

Análisis de la Situación Actual: En esta etapa, se lleva a cabo un análisis exhaustivo de la situación actual en los espacios públicos masivos académicos de la FIEC. Esto incluye una revisión de los sistemas de seguridad existentes, áreas de riesgo y patrones de comportamiento.

Identificación de Necesidades y Requisitos: Se identifican las necesidades específicas de seguridad en el área piloto de la FIEC, así como los requisitos tecnológicos y de capacitación.

Recolección de Datos: Se recopilan datos sobre incidentes de seguridad anteriores, áreas de alta afluencia y horarios de mayor actividad.

Fase 2: Diseño del Sistema de Seguridad
Esta segunda fase contara con dos etapas. La Primera esta es la de Selección de Tecnología y Hardware, Finalmente la segunda etapa es la de Recolección de datos.

Selección de Tecnología y Hardware: En esta etapa, se seleccionan las tecnologías de seguridad, como cámaras, sensores y sistemas de comunicación, que se utilizan en el área piloto.

Desarrollo de Algoritmos de Aprendizaje Profundo: Se diseñan y desarrollan algoritmos de aprendizaje profundo específicos para la detección de comportamientos sospechosos en entornos académicos masivos.

Fase 3: Implementación en el Área Piloto
Esta tercera fase contara con dos etapas. La Primera esta es la de Instalación de Hardware y Tecnología,Finalmente la segunda etapa es la de Entrenamiento de la Inteligencia Artificial.

Instalación de Hardware y Tecnología: Se instalan cámaras de seguridad, sensores de movimiento y sistemas de comunicación en el área piloto de la FIEC.

Entrenamiento de la Inteligencia Artificial: Se lleva a cabo un proceso de entrenamiento intensivo para la inteligencia artificial, utilizando datos recopilados en el área piloto.

Fase 4: Evaluación y Ajustes

Pruebas en el Área Piloto: Se realizan pruebas exhaustivas del sistema de seguridad en el área piloto, evaluando su capacidad para detectar comportamientos sospechosos y

prevenir amenazas.

Recopilación de Datos de Percepción de Seguridad: Se recopilan datos sobre la percepción de seguridad y la calidad de vida de la comunidad académica en el área piloto antes y después de la implementación del sistema.

Ajustes y Optimización: Basados en los resultados de las pruebas y la retroalimentación de los usuarios, se realizan ajustes y optimizaciones al sistema.

Fase 5: Implementación Completa y Escalabilidad

Implementación en Espacios Públicos Masivos Académicos: Una vez que el sistema ha demostrado su eficacia en el área piloto, se procede a su implementación en otros espacios públicos masivos académicos de la FIEC en la ESPOL.

Fase 6: Capacitación y Documentación

Documentación del Sistema: Se crea documentación detallada sobre el sistema de seguridad, incluyendo manuales de uso y procedimientos de mantenimiento.

Fase 7: Monitoreo Continuo y Actualizaciones

Operación y Monitoreo Continuo: El sistema se mantiene en operación continua, con monitoreo constante para detectar y responder a amenazas en tiempo real.

Actualizaciones y Mejoras: Se realizan actualizaciones periódicas del sistema para adaptarse a las cambiantes dinámicas de seguridad y tecnológicas.

2.1. Marco Teórico

Leyes de Privacidad:
La implementación de un sistema de seguridad integral debe fluir en total consonancia con las leyes vigentes sobre privacidad. En este escenario, el Reglamento General de Protección de Datos (GDPR)"(GDPR, 2024), una regulación europea, se erige como un elemento esencial. Este reglamento establece principios cruciales para el procesamiento de datos personales, actuando como el guardián de la privacidad y los derechos individuales, pilares fundamentales para la aceptación y legalidad del sistema propuesto. No podemos dejar de lado las leyes locales de privacidad, entes que abordan aspectos específicos de la vigilancia y la recopilación de datos en entornos académicos y urbanos. Las normativas relacionadas con la videovigilancia son también determinantes, imponiendo restricciones y requisitos específicos para salvaguardar la privacidad.

Importancia de la Seguridad:
La seguridad en entornos académicos y urbanos trasciende la simple protección de bienes materiales; se torna esencial para resguardar vidas y forjar un entorno propicio para el aprendizaje y el trabajo. Imaginemos este concepto como el director de una sinfonía, contribuyendo de manera significativa al bienestar general de estudiantes, profesores y residentes. En un contexto más amplio, la seguridad efectiva desempeña un papel crucial en la prevención de amenazas emergentes, adaptándose de manera proactiva a los desafíos en constante evolución.

Uso de Materiales y Aprendizaje Profundo:
La selección de materiales, comparable a la conservación de una galería de arte, se basa en su capacidad para proporcionar datos precisos y actualizados, por ejemplo sobre obras maestras que registran comportamientos anómalos. La implementación de algoritmos de aprendizaje profundo aumenta el nivel de complejidad del sistema, permitiendo identificar patrones complejos en el comportamiento humano. Este enfoque avanzado mejora significativamente la capacidad del sistema para detectar eficazmente situaciones de riesgo. Además, la integración de tecnologías de Internet de las Cosas (IoT) facilita la comunicación entre dispositivos, permitiendo respuestas coordinadas y rápidas ante posibles amenazas.

Normativas de Uso:
Establecer políticas internas claras es fundamental para regular el acceso a los datos y determinar los propósitos del monitoreo. La transparencia en el uso de la tecnología y la obtención del consentimiento adecuado son prácticas éticas y legales esenciales para lograr la aceptación de la comunidad. "La implementación de prácticas de auditoría de sistemas y actualización continua es fundamental para el cumplimiento normativo y para garantizar la seguridad a largo plazo "(De, 2024). Estas medidas no sólo cumplen con los requisitos legales, sino que también promueven la confianza y aceptación entre la comunidad académica y los residentes.

2.2. Materiales

En este capítulo, se detallan los fundamentos teóricos de la solución propuesta, integrando la infraestructura de hardware y las herramientas de software clave. El enfoque principal se centra en la red de sensores y la definición de elementos esenciales para su implementación, los cuales se integran de manera coherente en el sistema.

La Raspberry Pi 3, la cámara IP de 2MP y el Enrutador MikroTik se destacan como componentes esenciales que conforman la base de la red de sensores, seleccionados estratégicamente para asegurar una implementación efectiva y precisa del proyecto.

En el ámbito del software, se emplean herramientas avanzadas como OpenCV, MediaPipe y TensorFlow para el procesamiento de imágenes y el análisis de comportamiento humano, permitiendo una comprensión profunda del entorno estudiantil.

Facilitando la comunicación entre estos componentes, se adopta el protocolo TCP/IP como método principal, asegurando una integración eficiente y confiable. Además, para gestionar el flujo de vídeo, se implementa el protocolo RTSP, optimizando la transmisión y recepción de datos en tiempo real. Esta elección estratégica se alinea directamente con los objetivos específicos del proyecto, centrados en el análisis del comportamiento humano en aglomeraciones estudiantiles.

La combinación de hardware y software delineada establece la base integral para el desarrollo e implementación exitosa del sistema, proporcionando una perspectiva completa sobre cómo la tecnología IoT y las herramientas de procesamiento de imágenes contribuyen al análisis de entornos estudiantiles.

Rasberry Pi 3

Concebida por la Raspberry Pi Foundation en 2012, representa una serie de computadoras de placa única que han desencadenado un impacto significativo en el ámbito de la tecnología (Pi, 2019b). Inicialmente desarrollada con el propósito de facilitar la enseñanza de programación y conceptos de informática en entornos educativos, la Raspberry Pi ha evolucionado hasta convertirse en una plataforma versátil y asequible para proyectos de bricolaje y aplicaciones de Internet de las cosas (IoT).

Desde el punto de vista técnico, las Raspberry Pi así como en la figura 2 el cual utilizaremos el protocolo TCP/IP para la comunicación entre la cámara y la laptop en general, incorporan procesadores ARM, con capacidades de memoria RAM que varían entre 1 GB y 8 GB, puertos USB, HDMI, Ethernet y GPIO para conectar periféricos y componentes electrónicos. La capacidad de almacenamiento principal se basa en tarjetas microSD, y la plataforma admite la instalación de varios sistemas operativos, siendo Raspbian, basado en Debian, el más común.

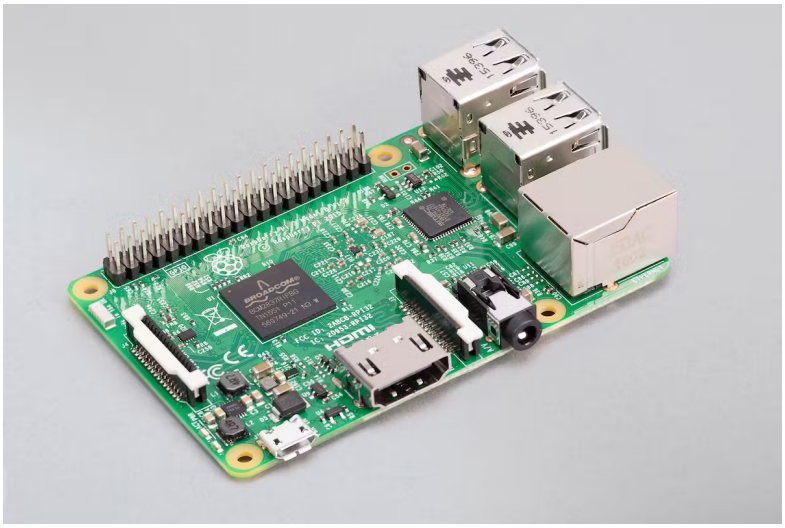


Figura 2: Raspberry Pi 3

Tensorflow

Es una biblioteca de código abierto dirigida al aprendizaje automático a través de una serie de tareas (Delgado, 2017). Ha sido desarrollado por Google para satisfacer las necesidades de sistemas capaces de construir y entrenar redes neuronales para detectar y descifrar patrones y correlaciones, análogos al aprendizaje y razonamiento usados por los humanos aso como se muestra en la figura 3. Actualmente es utilizado tanto para la investigación como para la producción de productos de Google, remplazando el rol de su predecesor de código cerrado.

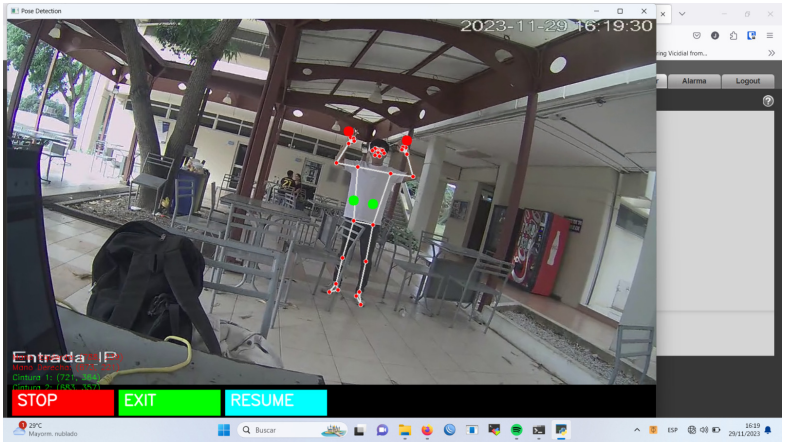


Figura 3: Implementación de sistema de MediaPipe por la biblioteca OpenCV y utilización del tensor Flow para entrenamiento por la foto capturada

Librería OpenCV

OpenCV es una librería libre tanto para proyectos comerciales o de investigación que se destaca en la visión artificial, OpenCV permite diseñar aplicaciones como: detección de movimiento, Reconocimiento de objetos, entre otros (V. M. Arévalo y Ambrosio, 2024). Siendo multiplataforma para los diferentes sistemas operativos existentes y para múltiples dispositivos de hardware, computadoras, celulares y Raspberry Pi (Howse.J, 2013). OpenCV es una biblioteca con demasiada eficiencia, principalmente orientada a objetos y desarrollada por el lenguaje de programación C++ pero permite incorporar conexiones con distintos lenguajes como: Python, Java, Matlab, Octave, Javascript, esto se puede evidenciar viendo un diagrama neuronal en la Figura 4

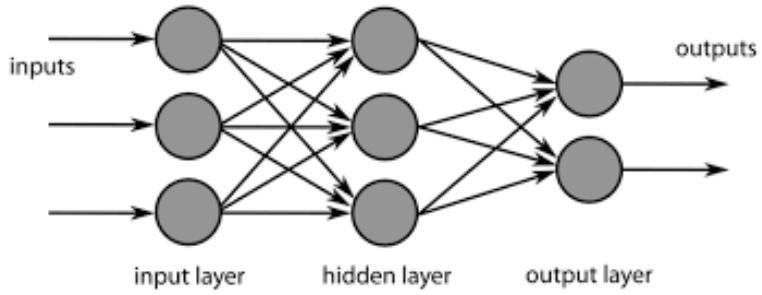


Figura 4: Diagramas neuronales básica como resultado de la utilización de tensorflow

Señal de Reloj

Señal que sólo refleja dos estados lógicos: ALTO ('1') y BAJO ('0') [4], representados con una onda cuadrada [5]. Se emplea para coordinar las acciones de dos o más circuitos (HeTPro-Tutoriales, 2015).

Node-RED

Node-RED es un marco de desarrollo visual de transmisión que facilita la conexión de dispositivos, API y servicios en Internet de las cosas (IoT)(Pickdata.net, 2020). Node-RED, desarrollado por IBM, proporciona una interfaz gráfica para crear flujos de trabajo conectando nodos predefinidos para realizar diversas acciones. Desarrollo de flujo visual donde Node-RED utiliza una interfaz gráfica basada en nodos, donde los usuarios pueden arrastrar y soltar nodos para crear flujos de trabajo. Cada nodo representa una acción o función específica y los usuarios pueden conectarlos para determinar una secuencia de eventos, se puede evidenciar un alto funcionamiento en la figura 5. para los ámbitos de Iot, Node-REd puede servir para diferentes medios:

- **Facilita la integración:** Node-RED es muy útil para la integración de sistemas y dispositivos heterogéneos(Sinelec, 2021). Puede conectarse a varios dispositivos y servicios, como bases de datos, servicios web, dispositivos IoT y más.
- **IoT (Internet de las cosas):** Node-RED es muy popular en proyectos de IoT debido a su capacidad para manejar fácilmente la conectividad y la lógica de flujo de trabajo para dispositivos de IoT.

- **Amplia biblioteca de nodos:** Node-RED tiene una extensa biblioteca de nodos predefinidos que realizan diversas funciones. Los usuarios pueden agregar sus propios nodos o instalar nodos adicionales según sea necesario.
- **Desarrollo rápido:** al ser visual, Node-RED permite el desarrollo rápido de prototipos y aplicaciones sin tener que escribir mucho código.
- **Expansibilidad:** si bien Node-RED tiene sus puntos fuertes, también es extensible. Puede incrustar funciones personalizadas utilizando código JavaScript en nodos específicos cuando se requiera funcionalidad adicional.

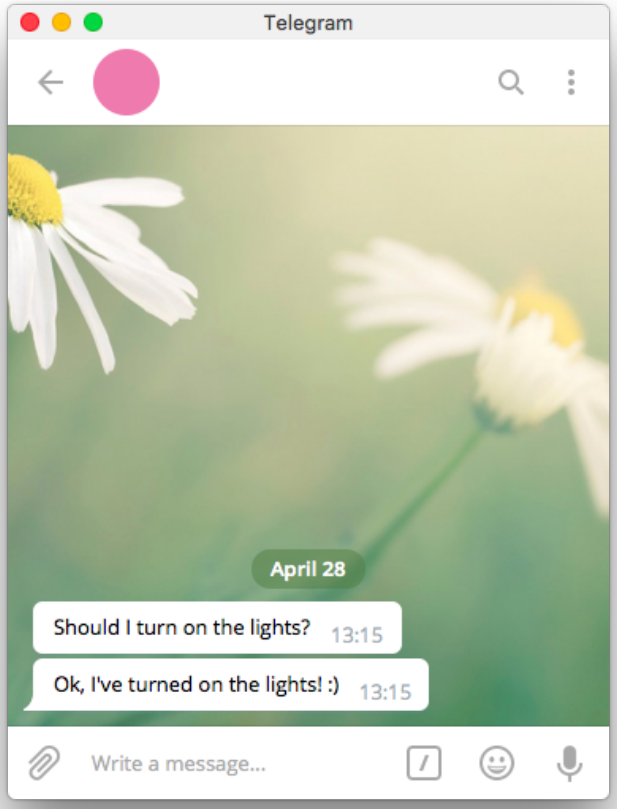


Figura 5: Ejemplo sobre un Bot desplegado con node-red

Sistema Operativo para Raspberri (Raspbian)

El sistema operativo Pi-OS (Raspbian), es un software completamente gratuito, basándose en el sistema operativo de Debian que se optimizo con el fin que pueda funcionar en el dispositivo Raspberry Pi(Pi, 2019a). Sin embargo, se lo conoce como un sistema operativo puro, incluyendo más de 35000 paquetes, a su vez posee software en un formato agradable, recompilado que permite tener facilidad en su instalación.

Lenguaje Python

Python es un lenguaje de nivel alto, que se orienta a objetos, enfocándose en su flexibilidad de uso. "Python es un lenguaje interpretado, flexible, multipropósito, y su sintaxis clara convirtiéndolo en un lenguaje muy productivo"(aula21 | Formación para la Industria, 2020) Python es un lenguaje que se caracteriza por tener distintas formas de usar, una de ellas es por las bibliotecas, permiten realizar atajos para algunos tipos de proyectos, por lo tanto, Python se lo puede usar desde cero, para inventar cualquier tipo de programa para el uso de bibliotecas o atajos (Chazallet, 2016).

Cámara de Seguridad DH-IPC-HDBW2230E-S-S2

La cámara de seguridad DH-IPC-HDBW2230E-S-S2 es otro modelo de cámara de red (IP) fabricado por Dahua Technology. según las tablas .Especificaciones de la cámara DH-IPC-HDBW2230E-S-S2ƶ "Detalles adicionales de la cámara DH-IPC-HDBW2230E-S-S2", las cuales son muy importantes para visualizar los componentes que convendrán a nuestro proyecto:

Tabla 1: Especificaciones de la cámara DH-IPC-HDBW2230E-S-S2 (Store, 2024)

Característica	**Descripción**
Resolución	2 megapíxeles (1080p), permite capturar imágenes de alta calidad
Sensor de imagen	CMOS de 1/2.7", contribuye a la claridad de la imagen y permite una mejor captura de detalles
Compresión de vídeo	H.265 y H.264 para optimizar el uso del ancho de banda y el almacenamiento
Visión nocturna	Iluminación infrarroja (IR) integrada, distancia de hasta 30 metros
Protección	Clasificación IP67 (resistente al polvo y al agua), clasificación IK10 de resistencia al vandalismo
Lente	Lente fija de 2.8 mm, proporciona un ángulo de visión amplio
Funciones de detección	Detección de movimiento, detección de rostros, detección de intrusos
Almacenamiento	Admite grabación en tarjeta microSD (no incluida), compatible con dispositivos de almacenamiento en red (NAS)
Conectividad	Conexión a la red a través de Ethernet (RJ45), protocolo de Internet IPv4/IPv6

Tabla 2: Detalles adicionales de la cámara DH-IPC-HDBW2230E-S-S2

Característica	**Descripción**
Modelo	DH-IPC-HDBW2230E-S-S2
Tipo	Cámara de red domo de focal fija IR Lite de 2 MP
Sensor de imagen	CMOS de 2 MP, 1/2.7", baja luminancia, alta definición de imagen
Resolución	2 MP (1920 × 1080) a 25/30 fps
Compresión de vídeo	Códec H.265, alta tasa de compresión, tasa de bits ultrabaja
Visión nocturna	LED IR incorporado, distancia IR máxima: 30 m
Funciones adicionales	ROI, SMART H.264+/H.265+, codificación flexible, modo de rotación, DWDR, 3D NR, HLC, BLC, marca de agua digital
Detección inteligente	Intrusión, cable trampa
Detección de anomalías	Detección de movimiento, manipulación de video, sin tarjeta SD, tarjeta SD llena, error de tarjeta SD, red desconectada, conflicto de IP, acceso ilegal, detección de voltaje
Almacenamiento	Máx. Tarjeta micro SD de 256GB
Fuente de alimentación	12 V CC/PoE
Protección	IP67, IK10

2.3. Topología

La topología representa la estructura de la red, tanto lógica como física, así como la disposición de nodos y enlaces topológicos que determinan la distribución de la red, tanto lógica como físicamente.

La topología de la red describe la disposición geométrica de los componentes de la red, definiendo cómo se conectan los nodos y cómo se transmiten las señales entre ellos. Esta configuración puede ser teórica o real, proporcionando la base que determina cómo interactúan los dispositivos.

En nuestro proyecto nos centramos en la topología física y lógica de una red en estrella conectada al servidor mediante nodos y sensores. Cada terminal establece conexiones tanto a nivel físico como lógico, respeta las topologías y gestiona eficientemente las comunicaciones que ocurren a través de redes extensas, independientemente de la distancia entre los componentes.

El diseño en estrella significa que cada nodo o sensor está conectado directamente al servidor central, lo que facilita la gestión y el seguimiento centralizados. Este enfoque permite una comunicación eficiente entre diferentes elementos de la red, incluso si están muy separados.

La implementación cuidadosa de topologías físicas y lógicas garantiza una comunicación fluida y confiable, permitiendo que la información fluya de manera eficiente desde los puntos finales al servidor central y viceversa. Este diseño el cual se ve en la figura 6 denota una topología en estrella el cual se ve que la Cámara TCP/IP va directamente hacia el router y está por medio de conexión wifi se conecta tanto el TensorFlow, Python, node-red, usuario y además dispositivos de tal manera que forman un canal directo hacia la Cámara inteligente ,estratégico ayudará a optimizar el rendimiento de la

red y mantener una conectividad sólida, lo cual es esencial para el éxito de nuestro proyecto.

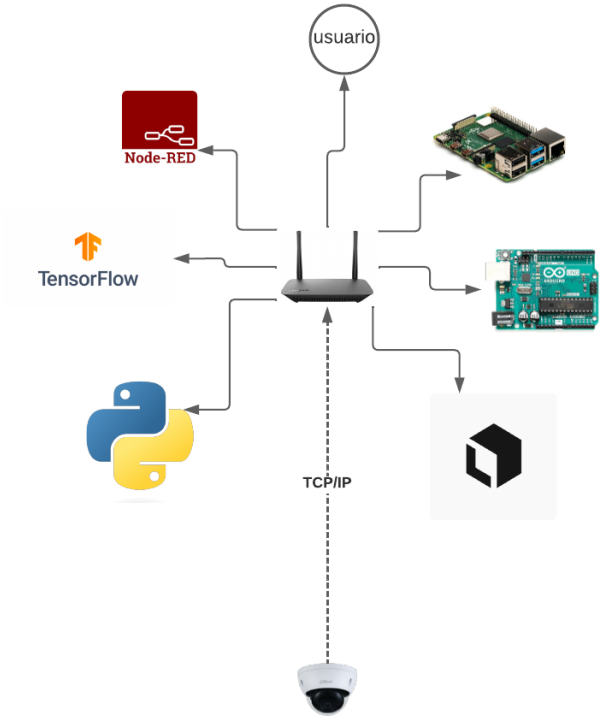


Figura 6: Diagrama topológico (estrella) del proyecto integrador utilizando un enrutador como punto principal

Wi-Fi 2.4 GHz

Una de las conexiones más populares y utilizadas en la actualidad es el Wi-Fi. Esta tecnología se ha vuelto importante e imprescindible tanto en el hogar como en las empresas y unidades académicas (C. Fernández, 2022). Proporciona mayor flexibilidad y acceso a la red de Internet sin tener que depender de una conexión física, lo que permite a los usuarios disfrutar de la conectividad a través de múltiples dispositivos de forma inalámbrica.

Wi-Fi no sólo elimina la necesidad de cables físicos, sino que también incorpora funciones y componentes inteligentes que pueden integrarse en las redes locales. Estos componentes inteligentes facilitan la comunicación y la colaboración entre dispositivos, optimizando la eficiencia de la conexión.

En un entorno doméstico, Wi-Fi permite a los residentes disfrutar de la conectividad a través de múltiples dispositivos, como teléfonos móviles, tabletas, computadoras portátiles y dispositivos domésticos inteligentes, sin restricciones de ubicación física. En un entorno empresarial, la tecnología Wi-Fi facilita la movilidad de los empleados, permitiéndoles acceder a los recursos de la empresa desde varias ubicaciones dentro de la organización.'

Protocolo de Comunicación Ethernet

El protocolo de comunicación Ethernet es un estándar ampliamente utilizado para la transmisión de datos a través de redes de área local (LAN). Basado en un esquema de acceso a medios de tipo contención, Ethernet define las reglas para el formato de la trama, la dirección física de cada dispositivo (dirección MAC) y los mecanismos de detección de colisiones (Guide, 2022). Las tramas de datos se envían de un dispositivo a otro dentro de la red mediante conmutación de paquetes a través de cables de cobre o fibra óptica. A lo largo de los años, Ethernet ha evolucionado para ofrecer velocidades de transmisión más altas. Variantes como Gigabit Ethernet y 10 Gigabit Ethernet desempeñan un papel fundamental en la conectividad de dispositivos en entornos locales e impulsan el desarrollo de tecnologías de redes.

Bot de Telegram

La aplicación de mensajería Telegram posee una herramienta denominada bots, permite la interacción con los usuarios a través de la plataforma de mensajería Telegram (Y. Fernández, 2020). Estos bots pueden realizar diversas funciones, desde proporcionar información hasta realizar determinadas tareas de forma automática. Los bots de Telegram están controlados por comandos y los desarrolladores pueden crearlos utilizando la API de Telegram.

Los bots se pueden utilizar para diversos fines, como proporcionar noticias, pronósticos meteorológicos, convertir moneda, jugar, configurar recordatorios y muchas otras funciones. Los usuarios pueden convocar bots usando comandos específicos y recibir respuestas automáticas o realizar acciones basadas en la programación del bot. Esto se puede ver claramente en nuestro proyecto integrador, reflejado en la figura 7

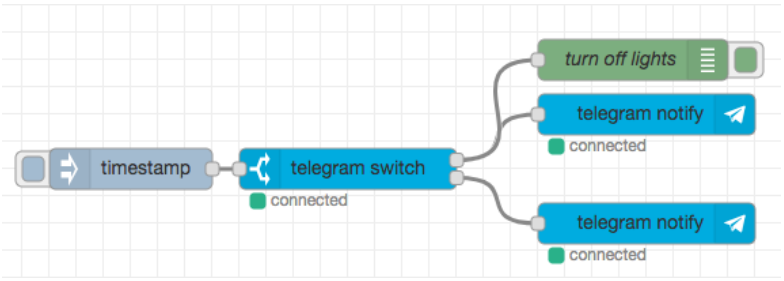


Figura 7: Entorno gráfico del proyecto integrador (programación) node red

Protocolo de comunicación Ethernet (TCP/IP)

El protocolo de comunicación Ethernet, más conocido como Internet Protocol (IP), se basa principalmente en comunicaciones TCP para la realización de configuraciones de dispositivos de forma automática (aula21, 2019). Puede utilizar hardware y software de forma colaborativa. Este protocolo clasifica los nodos dentro de tipos preferidos de dispositivos, lo que le permite asignar preferencias de manera consecutiva para la disposición de dispositivos específicos. Por otro lado, en el protocolo de red utilizado en nuestro proyecto, se apoyan controles de información mediante TCP y UDP para lograr una comunicación efectiva entre la cámara, la Raspberry y Node-RED.

Enrutador Mikrotik hAP ac lite

El enrutador tal como se ve en la figura **??**, que utiliza una conexión Wi-Fi en la banda de 2.4 gigahercios, es el dispositivo primordial en nuestra configuración de red en estrella para el proyecto integrador (Y. Fernández, 2023). Este enrutador facilita la comunicación principalmente con la Raspberry Pi y, a su vez, transmite información a la plataforma que alberga el bot de Telegram. Este bot es capaz de proporcionar información acerca de las notificaciones generadas por personas congregadas en la plazoleta de la FIEC.

Sensor de Movimiento PIR HC-SR501

Es un componente crucial para la eficiencia energética del sistema, ya que contribuye al ahorro de energía tanto en el funcionamiento de la cámara como en la comunicación de la Raspberry Pi. Su papel es esencial en la optimización del consumo, ya que, mediante la predeterminación de áreas específicas, el sensor de movimiento se activará cuando una persona transite por una zona calculada previamente, tal como se ve en la figura 8. Esta activación no solo impulsa la funcionalidad de la cámara, sino que también sincroniza otras operaciones relevantes, maximizando así la eficacia del sistema en su conjunto.

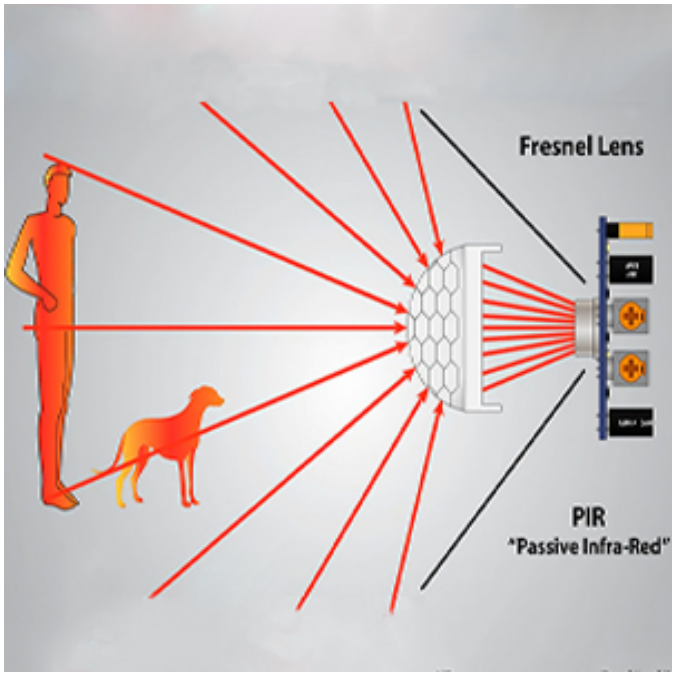


Figura 8: Sensor de Movimiento PIR HC-SR501, funcionamiento

Capítulo 3

3. Diseño de la solución

El diseño del prototipo para la detección de personas sospechosas en un espacio reducido y con aglomeración en instituciones académicas se enfocó principalmente en la seguridad de la Escuela Superior Politécnica Litoral (ESPOL), considerando el flujo de personas en una ubicación específica y la protección de las pertenencias y la seguridad de los estudiantes que transitan por esa área.

El sistema que tenemos en desarrollo nos permite conocer el numero estimado de personas que están en el sector, realiza un análisis de su comportamiento. Este análisis es realizado por un modelo de Inteligencia Artificial, que aprende los patrones de comportamiento de cada individuo, nuestro sistema constantemente analiza las imágenes provenientes del lugar a monitorear. Luego, si el sistema no detecta un comportamiento anómalo o sospecho, el sistema lo descarta. Sin embargo, si el comportamiento es detectado como sospechoso, el sistema emitirá una alerta, esta alerta será enviada por un Bot en Telegram, el Bot será agregado a un grupo, donde las personas interesadas deben unirse para recibir las notificaciones.

Además de la detección de personas sospechosas, el sistema puede proporcionar datos útiles sobre la densidad de personas en el área, ofreciendo insights valiosos para la gestión del flujo de personas y la seguridad en tiempo real. La implementación de tecnologías como la inteligencia artificial y la notificación instantánea a través de Telegram refuerzan la capacidad del sistema para mantener un entorno seguro y controlado en el campus universitario, se puede representar claramente en una maqueta digital de la plazoleta FIEC en la figura 9.

Figura 9: Esquemático de escenario implementado en illustrator donde la ceseta roja es la plazoleta FIEC y las lineas azules son el transito vial publico

Figura 10: Plazoleta FIEC

En la figura 13, se presenta el escenario real en el que implementaremos nuestro proyecto: un sistema de cámara inteligente para la identificación de comportamientos sospechosos utilizando aprendizaje profundo y tecnología IoT. Este sistema se desplegará en la plazoleta de la FIEC, ubicada en la FIEC vieja, un espacio amplio estratégicamente seleccionado con constante circulación de personas. La plazoleta cuenta con tres niveles de bajada y un quiosco donde los estudiantes realizan compras.

La elección de este lugar se basa en la alta afluencia de personal administrativo, profesores y estudiantes que transitan hacia sus respectivas clases. Además, la ubicación estratégica de la plazoleta presenta el riesgo de posibles situaciones de "bolsiqueo", un acto sutil de robo. Esta problemática puede ser relevante también en lugares concurridos fuera de la universidad, como la parada denominada "Garita"de la ESPOL.

Para la implementación de la cámara inteligente con aprendizaje profundo, se considerarán factores clave como la ubicación, la infraestructura y las condiciones climáticas. Estos elementos son cruciales para determinar el mantenimiento necesario de las cámaras, considerando aspectos como la opacidad o interferencias que podrían afectar el dispositivo, especialmente en condiciones climáticas adversas. Se han identificado espacios estratégicos expuestos, con zonas específicas para la colocación de cámaras de seguridad, abordando así la necesidad de una vigilancia efectiva en estas áreas.

4. Descripción del sistema

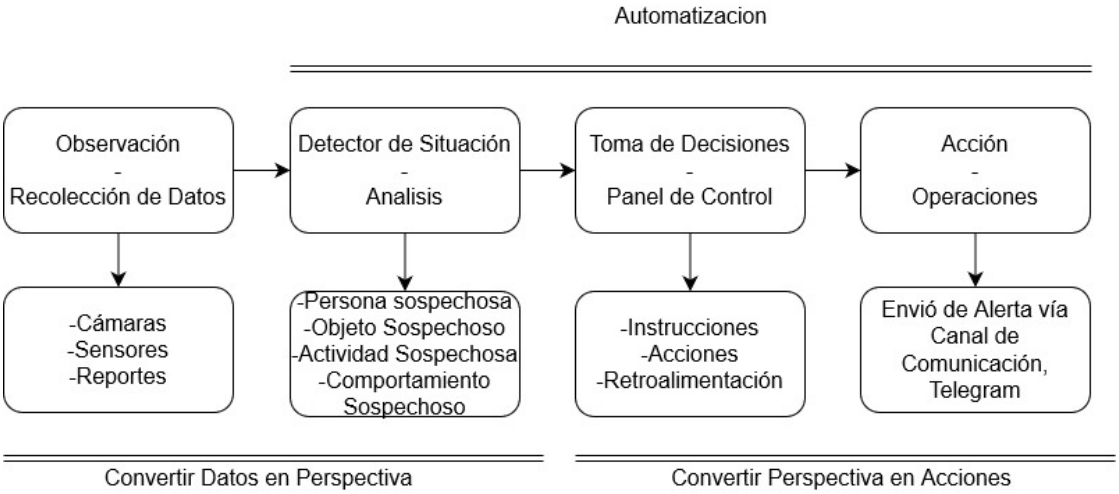


Figura 11: Secuencia de pasos ante un evento de seguridad

Para el desarrollo de sistemas que utilizan arquitectura con el protocolo RTSP, según lo mostrado en la figura 11, se emplea un sistema de información en el cual la inteligencia artificial compara imágenes con un cierto grado de similitud respecto a las imágenes almacenadas en la biblioteca en Python Media Pipe. Este sistema utiliza comunicación TCP/IP entre una computadora que contiene la inteligencia artificial y la Raspberry Pi que esta conectada a la cámara ip.

En el momento en que una persona pasa específicamente por el sensor de movimiento, este se activa, permitiendo que la cámara Ip junto con la Raspberry Pi comiencen a funcionar. En este proceso, la Raspberry Pi envía las imágenes capturadas hacia la computadora, donde son comparadas con imágenes previamente almacenadas bajo la supervisión de la inteligencia artificial.

Según la figura 12 donde se muestra el diagrama tecnológico ,el prototipo diseñado consta de partes representadas mediante diagramas de bloques, los cuales se encuentran detallados en la Figura 14. En este esquema, la cámara TCP, mediante la conexión a la Raspberry Pi y al Arduino, genera la señal para iniciar el funcionamiento de la cámara. De esta manera, las imágenes son dirigidas mediante protocolos TCP hacia una laptop que alberga la inteligencia artificial denominada TensorFlow.

Cuando la laptop envía las imágenes, estas son etiquetadas por Labo y comparadas bajo la supervisión de la inteligencia artificial con imágenes recopiladas previamente gracias a las posiciones en vectores, las cuales se utilizan con el protocolo de Bella Pipe. Además de esto, al compararlas, si resultan ser falsas, se descartan y eliminan. En caso de que la comparación sea verdadera y haya una similitud mayor al 70 por ciento , según la inteligencia artificial, estas imágenes son redirigidas nuevamente hacia la Raspberry Pi.

La Raspberry Pi, a su vez, envía una señal a través de la red para activar un bot

de Telegram, el cual envía notificaciones a las personas que han registrado el contacto mediante un código QR.

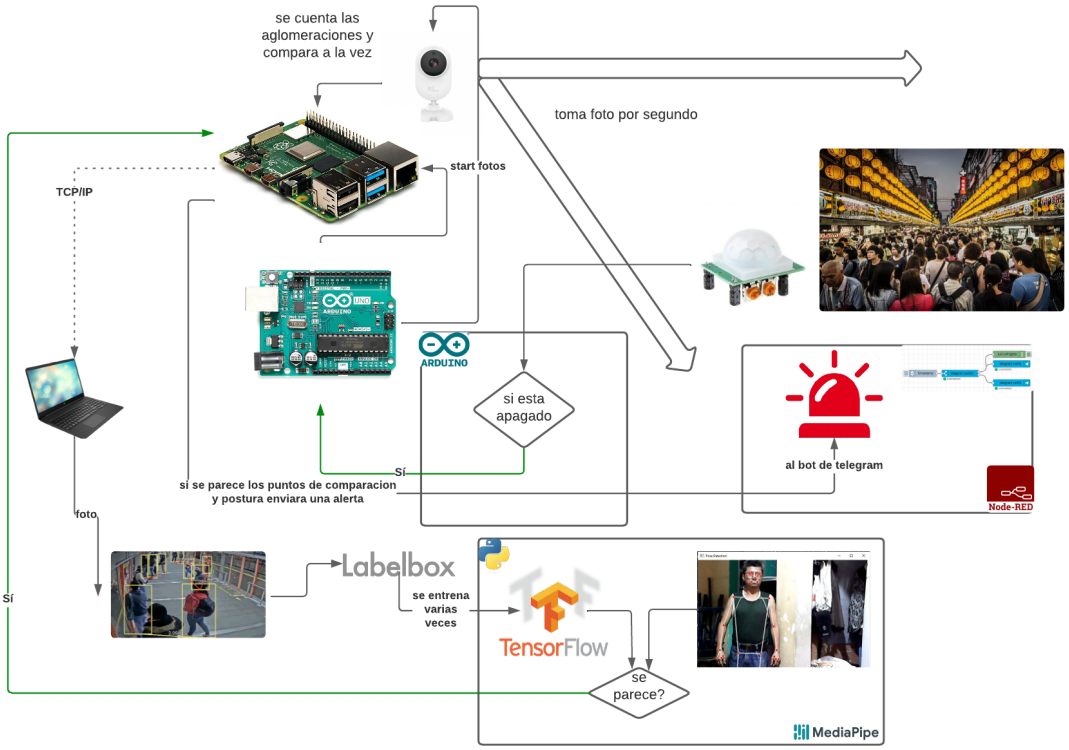


Figura 12: Diagrama tecnológico integrador con respecto a los procesos en la intervención física y digital de componentes tecnológicos usados

A continuación, se presentará en la figura 13 una versión más concisa las cuales se pueden ver en la figura 14, figura 15 y figura 16 e integradora del diagrama tecnológico, detallando cada uno de los bloques principales y sus respectivas secciones:

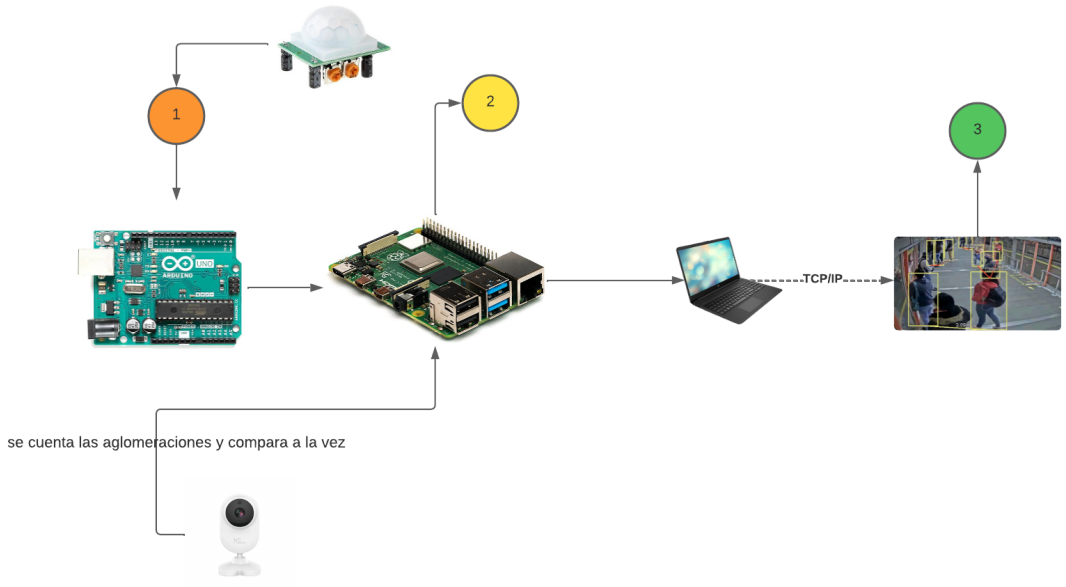


Figura 13: Diagrama tecnológico condensado por las cuales se presentan los procesos de forma individual

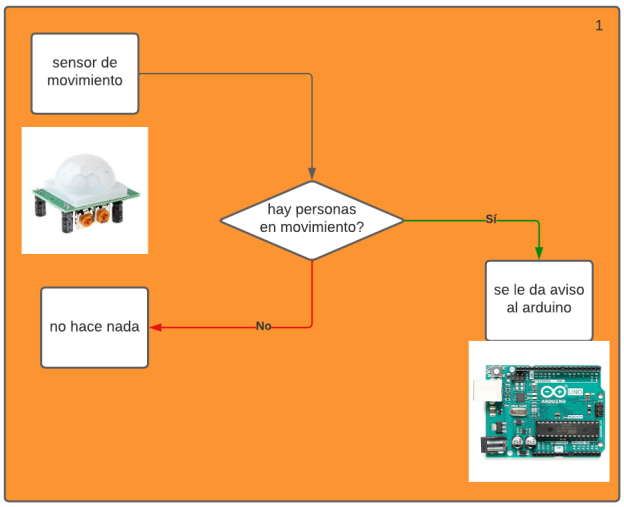


Figura 14: Primer bloque del diagrama tecnológico

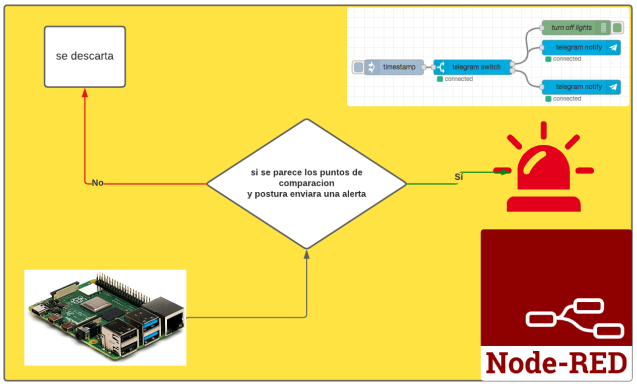


Figura 15: Segundo bloque del diagrama tecnológico

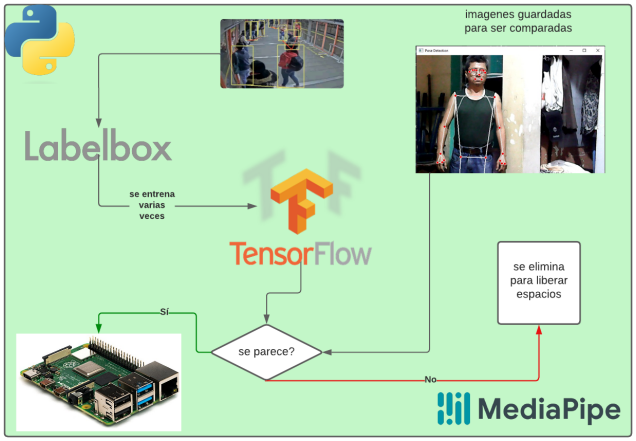


Figura 16: Tercero bloque del diagrama tecnológico

4.1. Planteamiento inicial

Las Raspberri Pi y la cámara serán colocadas en un lugar alto, que tenga la mejor vista para que se pueda abarcar el mayor espacio disponible. La Raspberry Pi actuará como el cerebro del sistema, gestionando la captura de imágenes de la cámara IP y enviándolas de forma segura a un servidor remoto para su almacenamiento y acceso remoto. Tanto las Rapsberri-pi como la cámara ip deben estar en el mismo segmento de red para que no tenga ningún problema de nivel de conectividad.

4.2. Diagramas de funcionamiento

Para obtener un concepto más claro, es necesario considerar tres partes interrelacionadas. Estas son el diagrama físico de retroalimentación y el virtual. En el diagrama físico, la implementación del conteo de personas es fundamental. Al activarse el sensor de movimiento, este detectará personas y las contará según la detección de capturas por la cámara TCP/IP hacia la computadora principal. Una vez que la imagen se dirige directamente hacia la computadora, la parte virtual toma la oportunidad, al igual que la página de retroalimentación.

El bloque de retroalimentación, el procesador de datos, que tiene las imágenes guardadas, utiliza las bibliotecas Keras y estimadores proporcionados por TensorFlow. Este utiliza estratégicamente los procesadores de la CPU, GPU y TPU respectivamente para obtener beneficios según la imagen. Estas imágenes, a través de los bots, serán etiquetadas y guardadas en una carpeta en el almacenamiento de la computadora principal. Luego, en el bloque virtual, se especifica directamente a TensorFlow JS como un medio para analizar los archivos, los cuales el diagrama físico envía directamente al virtual.

Dentro del diagrama de entrenamiento, que se encuentra en el bloque de virtualidad, se analizará con la biblioteca MediaPipe en Python para determinar si las coordenadas

guardadas indican si una persona es sospechosa o no. Si esta es correcta, se guarda la imagen y se aplica la etiqueta correspondiente. Luego, la imagen entra en el diagrama de retroalimentación para seguir con lo indicado anteriormente.

Cuando las imágenes se guardan, se ejecutan y leen una a una. No obstante, TensorFlow, compara el comportamiento de las imágenes principales de la cámara TCP/IP hacia todas las imágenes guardadas en el entrenamiento. Si la similitud es mayor al 75 por ciento, estas serán aisladas y guardadas. Se vuelve a analizar la implementación de sistemas y las coordenadas correspondientes, así como la fecha, hora y lugar donde se solicitó el atentado. Estos datos se guardarán en el sistema de Glitch, una base de datos utilizada para el sistema. Además, se envía una alerta a través de la voz de Telegram mediante la Raspberry Pi, específicamente a través de la red, para notificar a las personas correspondientes.

Capítulo 4

5. Resultados y análisis

Para comprobar la eficiencia y eficacia de nuestro sistema, el cual utilizará inteligencia artificial, se va a utilizar un cierto sector en la plazoleta de FIEC con suficientes personas para la implementación en nuestro proyecto. En el momento en que una persona pase del sensor de movimiento y sea captada como la primera persona, se procederá con la prueba pertinente.

Las pruebas a realizar son importantes en nuestro proyecto, por la cual podemos conocer el tiempo de respuesta de nuestro sistema ante algún peligro. Realizaremos una simulación de peligros en la plazoleta de FIEC, de tal manera que, en diferentes situaciones, ya sea con cambios climáticos o alguna perturbación en nuestras cámaras, nuestro sistema pueda adaptarse. Además, observaremos los puntos negativos y positivos de nuestro sistema para identificar errores y fallas, de modo que el Telegram pueda notificarnos si existe presencia de peligro en dicha área.

5.1. Implementación en diseño virtual

Inicialmente, el escenario seleccionado para la implementación de nuestro proyecto eran las instalaciones de estacionamientos en FIEC. Sin embargo, enfrentamos problemas con el uso de dichas instalaciones, así como con la duplicación de proyectos. Debido a estas complicaciones, tomamos la decisión de modificar nuestro enfoque y optamos por implementar un sistema de reconocimiento de comportamientos sospechosos de las personas.

Nos interesaba particularmente conocer cómo las personas actuarían en situaciones delictivas, donde la inteligencia artificial podría contrarrestar con tiempos de respuesta antes de la precipitación de un evento. En este contexto, decidimos utilizar la plazoleta de FIEC como escenario, dado el mayor número de estudiantes que transitan por esa área.

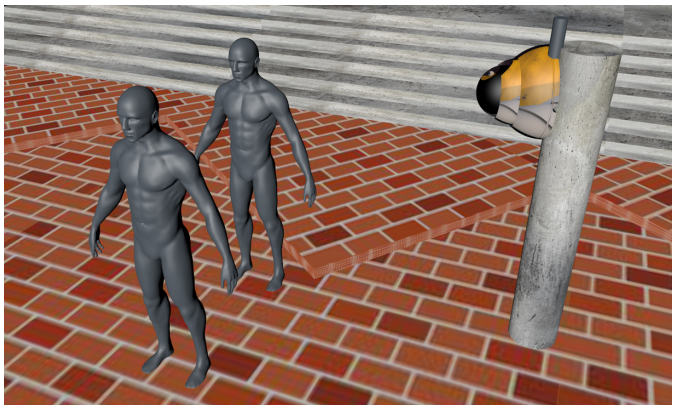


Figura 17: Maqueta diseñada para el escenario de implementación

A continuación, detallamos los procesos relacionados con la inteligencia artificial y la implementación del sensor de movimiento, así como el bot de Telegram que nos ayudará a

procesar la información de las notificaciones en conjunto con la Raspberry. En la Figura 17, se presenta la simulación de una persona caminando en la plazoleta de FIEC con otra persona detrás, la cual tiene intenciones delictivas.

Cuando la cámara es activada por la primera persona que pasa, analizará el comportamiento tanto de la primera como de la segunda persona. La primera, al no mostrar un comportamiento que requiera atención, permitirá que la cámara se enfoque en la siguiente persona. Sin embargo, si esta última presenta un comportamiento sospechoso desde el principio, se enviará una notificación a la Raspberry indicando la presencia de una situación inusual.

La Raspberry, a su vez, recibirá la captura por protocolo TCP/IP hacia una computadora cercana, la cual está equipada con inteligencia artificial. Esta analizará el comportamiento, comparándolo en tiempo récord con otras imágenes procesadas de delincuentes y personas con comportamientos delictivos, basándose en la posición de sus cuerpos convertida en vectores.

En el momento en que se detecte un comportamiento inusual, se enviará una notificación a través de un programa de red desde un bot de Telegram, y esta información se guardará en una base de datos denominada "Glitch". Este enfoque nos permitirá mejorar la seguridad en la plazoleta de FIEC y anticiparnos a posibles situaciones de riesgo.

5.2. Programación de la inteligencia artificial

Para la implementación de nuestro sistema, recurrimos a la inteligencia artificial mediante TensorFlow, lo cual fue fundamental para el desarrollo de la lógica de programación. En este proceso, se utilizaron diversas bibliotecas a través de Python, en particular, para la comparación de elementos. El objetivo era obtener un porcentaje de similitud, y para esto, se empleó la biblioteca MediaPipe.

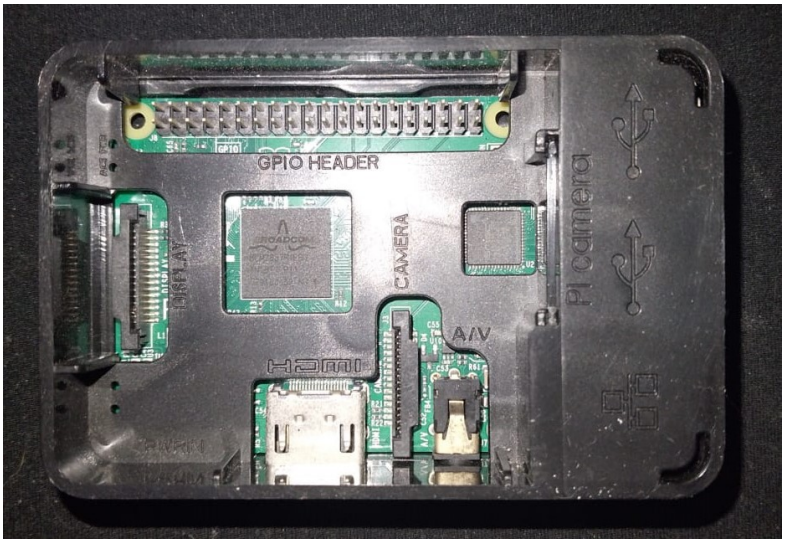


Figura 18: Rasberry el cual se usará para nuestro proyecto integrador

La lógica de programación se centra en realizar comparativas en tiempo real a partir de imágenes que el Raspberry tal como se ve en la figura 18 ,reenvía a la laptop automáticamente en intervalos definidos por el sensor de movimiento. Estas imágenes son almacenadas en el tensor de la computadora, proporcionando la base para la comparación necesaria en los siguientes pasos del procedimiento.

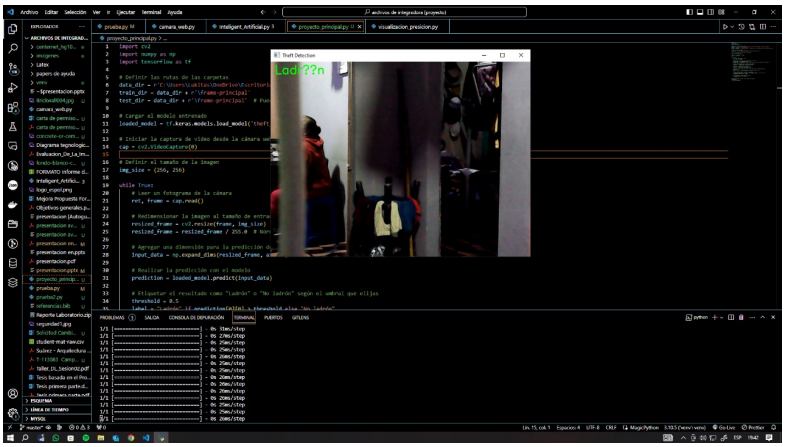


Figura 19: Inteligencia artificial detectando posible comportamiento según imágenes de ladrones

La figura 19 ilustra la implementación del sistema, donde la cámara TCP se utiliza como medio para establecer comparaciones directamente desde la máquina. Se aprovechan las comparativas de las imágenes almacenadas, utilizando variables acumulativas que, en última instancia, generan porcentajes que reflejan el comportamiento de una persona. Este enfoque nos permite evaluar el comportamiento en relación con la implementación de la cámara de seguridad TCP, proporcionando información valiosa para la toma de decisiones.

5.3. Programación del Bot de Telegram

Como se evidencia en los nodos de previsualización de Telegram, el bot que estamos utilizando recibe una entrada previa del usuario del bot. En nuestra aplicación, solicitamos la API basándonos en la disponibilidad numérica, cercana al área designada donde se presume que la persona sospechosa se encuentra. Cuando el bot recibe esta entrada, emite una alerta que contribuye a la recopilación de información sobre la persona en cuestión.

Este proceso se relaciona con determinar el porcentaje de sospechosos presentes y nos ayuda a prevenir cualquier tipo de inseguridad en áreas con aglomeración de personas. Como se ilustra en la figura 20, se pueden observar nodos que envían información, permitiendo al bot proporcionar notificaciones pertinentes en tiempo real. Estas notificaciones se envían a las personas en el área designada después de un escaneo previo del bot. Este escaneo se inicia cuando una persona se acerca al sensor de movimiento.

Durante las pruebas realizadas en la plaza, notamos que las notificaciones hacia el bot

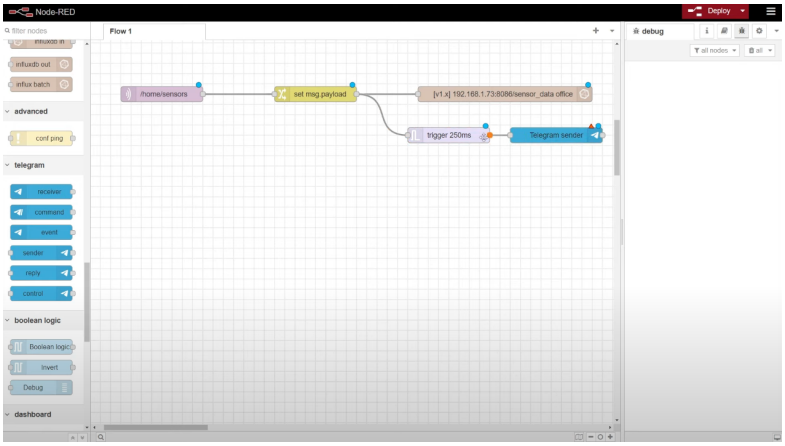


Figura 20: Implementación de node-red para envió de notificaciones en el bot de Telegram

de WhatsApp tardaron dos segundos en llegar, debido a retrasos generados por el análisis y la carga que la laptop experimentaba con la inteligencia artificial. Es relevante destacar que la conectividad de la red influye significativamente en el rendimiento del sistema. Las actualizaciones eficientes del Gateway, incluso con una conexión relativamente lenta, pueden verse afectadas por cargas en lecturas e interpretación de datos. Estos factores pueden ser tanto positivos como negativos, dependiendo de cómo la inteligencia artificial pueda previsualizar y comparar personas potencialmente sospechosas.

```
var opts = {
    reply_markut: JSON.stringify({
        "inline_keyboard": [[
            {
                "text" : "una persona sospechoza esta cerca del sector, tenga cuidado",
                "callback_data": "1"
            }
        ]]
    })
};
```

Figura 21: Configuración del bot con sus características

En la figura 21, se presentan las propiedades del canal y el mensaje previo que será enviado a las personas que contienen el bot. Este bot de Telegram permite a los usuarios obtener notificaciones en tiempo real sobre personas sospechosas cercanas, con el objetivo de prevenir situaciones delictivas.

5.4. Pruebas de Campo

Para los análisis de pruebas, se eligió la plazoleta de FIEC, ya que presentaba una mayor aglomeración, lo que proporcionaba un contexto más desafiante para el procesamiento del contador de personas y el rendimiento del procesador. Además, se buscaba un mejor campo visual que permitiera distinguir entre personas con comportamientos sospechosos y aquellas que simplemente transitaban de manera normal.

Figura 22: Toma de la detección de una persona con el software implementado

Figura 23: Detección de Gestos y puntos importantes

Con el objetivo de mejorar el campo visual, realizamos una reprogramación completa, centrándonos en la configuración de la cámara inalámbrica. Ajustamos tanto el alto como el ancho, ingresando en la configuración de la cámara y habilitando un campo visual más amplio de (1024 x 1945 píxeles), como se muestra en la figura 23 y la figura 22. Esta modificación nos permitió captar con mayor detalle el comportamiento de las personas en el área de prueba.

Figura 24: Cámara que se uso para las pruebas

La cámara de la figura 24, posteriormente, se conecto por cable a una computadora con inteligencia artificial. En esta configuración, llevamos a cabo pruebas a escala baja, haciendo pasar una o dos personas por el mismo sector. Este enfoque nos permitió observar cómo interactuaban entre sí y resultó beneficioso para la inteligencia artificial, ya que agilizó el procesamiento de comparativas entre las 12,500 imágenes en un corto período de tiempo.

Las pruebas se llevaron a cabo en un entorno real con una temperatura promedio de 27 grados y precipitaciones óptimas. La aglomeración en el área no fue masiva, pero sí apropiada para evaluar el desempeño del sistema y realizar mantenimientos necesarios. Este escenario proporcionó condiciones realistas para validar la efectividad y robustez del sistema implementado.

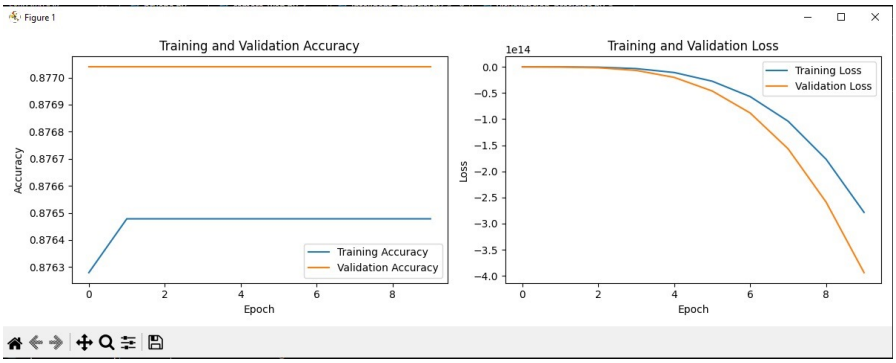


Figura 25: Estadísticas sobre la precisión en 20 pruebas exactas con el paso del tiempo para la Inteligencia artificial

En la Gráfica 25, que interpreta la precisión con respecto a las imágenes, se observa que inicialmente alcanza niveles elevados, pero a medida que progresa, se estabiliza. Sin embargo, al descender, se produce una estabilización que conduce a falsos positivos y a un porcentaje mínimo aceptable. Este último escenario permite que las imágenes se envíen directamente a la Raspberry, interpretadas como notificaciones emitidas por el bot de Telegram hacia las personas cercanas a las identificadas como sospechosas.

Tiempo de notificaciones transcurridos por datos enviados por la IA y porcentajes de precisión sobre comportamiento sospechoso					
Número de escenario por acumulación de personas	T1[S]	T2[S]	T3[S]	Prom[s]	Porcentaje de precisión de acuerdo a numero de personas sospechosas
4	1.52	1.73	1.71	1.65	59 %
9	1.95	1.24	1.86	1.68	55 %
12	0.59	1.39	1.46	1.15	71 %
16	0.84	1.14	0.66	0.88	57 %
19	0.77	1.42	1.25	1.15	73 %
20	0.27	1.73	0.31	0.77	67 %
24	1.57	1.61	1.44	1.54	59 %
26	1.60	1.26	0.60	1.15	56 %
28	0.36	0.59	0.34	0.43	74 %
30	0.76	1.99	0.62	1.12	55 %
34	1.42	0.97	1.76	1.38	63 %
36	0.35	1.28	0.82	0.82	71 %
39	1.09	0.93	1.88	1.30	73 %
40	0.38	1.63	0.71	0.91	69 %
42	1.22	1.76	0.29	1.09	51 %
46	0.90	1.97	0.74	1.20	55 %
48	1.29	1.99	1.43	1.57	65 %
50	0.80	0.18	0.02	0.34	55 %

Tabla 3: Tiempo de notificaciones transcurridos por datos enviados por la IA y porcentajes de precisión sobre comportamiento sospechoso

En la Tabla 3 se presentan los resultados de 20 pruebas realizadas, cada una con personas que exhibieron comportamientos sospechosos. Se incluye la precisión a lo largo del rango de comparativa, mostrando porcentajes y la exactitud alcanzada en relación con las imágenes comparadas directamente con las capturas enviadas por la cámara TCP a la inteligencia artificial. Estos datos proporcionan una representación gráfica en tiempo real de cómo evoluciona la comparativa de imágenes a lo largo del conteo de cada persona.

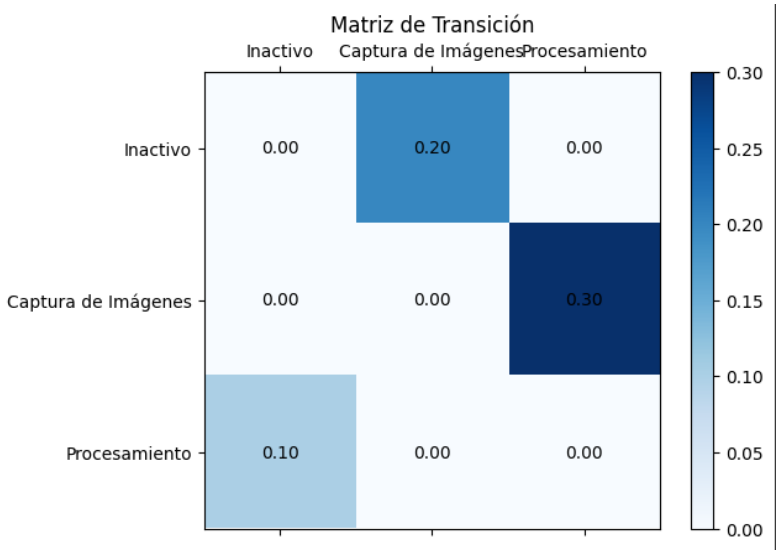


Figura 26: Matriz de procesamiento con respecto a datos obtenidos de la Inteligencia artificial

En la Figura 26, se presenta un cuadro representativo de todos los datos recopilados sobre la tabla 3, destacando la relación entre el tiempo, la precisión y el porcentaje de ambas fotos capturadas. Estos resultados son cruciales para evaluar el rendimiento y la eficacia del sistema, permitiendo ajustes y mejoras continuas con base en el análisis detallado de las pruebas realizadas.

5.5. Análisis de Costos

En esta sección se detallara el costo tanto de software como de hardware en la Tabla 4, el cual se pondrá en el mercado. La licencia sera por el numero de cámaras a usar con nuestro sistema y sera mediante suscripción mensual o anual. lo cual incluye el software, acceso a la aplicación y equipos, donde los entrégales serán un enrutador Mikrotik, Raspberri Pi 3.

- **Inversión inicial:** Representara el valor que se necesita para la implementación del proyecto, en esta se consideran los componentes de hardware, alquiler de servicios de software, así como la nomina del personal que programara el software dándonos un valor de $8226 dolares.
- **Capital de Trabajo:** Es un valor fijo que sera de $1000.00 dolares,este valor sera considerado para temas de comercialización, marketing y presentación del proyecto

Descripción	**P. unitario**	**Cant**	**Subtotal**
Servicio de Hosting	$60	12	$720
Programador	$600	12	$7200
Arduino	$12	1	$12
Sensor de Movimiento	$3	1	$3
Cable USB Tipo B	$3	1	$3
Raspberri Pi 3 Model B	$80	1	$80
Cable USB Tipo B	$3	1	$3
Caja para Proyectos 11x6.5x9.25cm	$15	1	$15
Mikrotik hAP ac lite	$95	1	$95
Camara Ip Domo 2Mp Dahua	$95	1	$95
INVERSIÓN INICIAL			$8226
CAPITAL DE TRABAJO			$1000

Tabla 4: Inversión inicial del sistema (incluye IVA)

Precio de Venta

Se trata de la totalidad de gastos que contribuyen a establecer un precio para el producto en fase de desarrollo, siendo este precio el umbral mínimo necesario para evitar pérdidas en la inversión realizada, como se ilustra en la ecuación 1

$$PV = ((CFT \times \%CF) + CVU) \times (1 + \%G) \tag{1}$$

Donde:

$$\begin{aligned} PV &= \text{Valor del producto} \\ CFT &= \text{Costos fijos totales} \\ \%CF &= \text{Porcentaje de costos fijos} \\ CVU &= \text{Costos variables unitarios} \\ \%G &= \text{Porcentaje de ganancia} \end{aligned}$$

- **Costos fijos totales:**Se refieren a los costos que permanecerán constantes durante toda la duración de la membresía, y dicho importe, equivalente a $306 dólares, se abonará en una única ocasión al momento de adquirir el producto.
- **Costo variable unitario:**Es una cantidad que experimentará cambios a lo largo del tiempo, dado que está sujeta a la fluctuación dependiente de un proveedor externo de servicios de alojamiento.
- **Porcentaje de costo fijo:**Se tomará como la proporción de los montos que deben abonarse de manera invariable al adquirir la membresía, y en nuestra situación específica, se manifestará como el 10 % de los Costos fijos, resultando en un total de $30,60 dólares por cámara.
- **Porcentaje de ganancia:**n el ámbito comercial, hay ciertos criterios que los negocios deben satisfacer para alcanzar una rentabilidad que garantice la estabilidad financiera del producto a largo plazo. Dadas las particularidades del producto propuesto y resaltando su carácter innovador, se sugiere una ganancia del 30 % sobre los costos totales.

Como se observa en la Tabla 5 El Precio de Venta estimado al público para una membresía anual es de...

Variable	Valor
CFT (Costos fijos totales)	1306.65
CVU (anual) (Costos variables unitarios)	600
%CF (Porcentaje de costos fijos)	0.15
%G (Porcentaje de ganancia)	0.3
PV (anual) (Precio de Venta)	1034.80

Tabla 5: Ingresos

Punto de equilibrio

También reconocido como el punto de equilibrio de una empresa, se refiere al nivel de ventas mínimo necesario para evitar tanto pérdidas como ganancias, es decir, alcanzar un equilibrio en el beneficio. Este valor se calcula mediante el uso de la ecuación 2

$$PE = \frac{CFT}{PVE - CVU} = \frac{CFT}{MC} \tag{2}$$

Donde:

$$CFT = \text{Costos fijos totales}$$
$$\%PVE = \text{Precio de venta unitario}$$
$$CVU = \text{Costos variables unitarios}$$
$$MC = \text{Margen de contribución}$$

- **Margen de contribución:**Se refiere a las ganancias de una empresa sin tener en cuenta los costos fijos asociados, representando esencialmente la disparidad entre el precio de venta y los costos variables unitarios.

Variable	Valor
Años	4
CF(periodo)	5226.60
PV (Precio de Venta)	1034.80
CVU (anual)	600
MC	434.80
PE	12.02
Membresías (unidades anuales)	14

Tabla 6: Gestos

Como se puede apreciar en la Tabla 6, la estimación anual del Punto de Equilibrio para el período de 4 años es de 12.02 unidades. Sin embargo, por razones prácticas, se ha fijado concretamente en 14 unidades.

Depreciación

La depreciación está vinculada a la duración efectiva de un producto o activo, durante la cual pierde su valor inicial con el paso del tiempo. Este concepto se aplica específicamente a los activos fijos. La Ecuación 3 nos proporciona el cálculo del valor de depreciación.

$$D = \frac{CT - VR}{VU} \tag{3}$$

Donde:

$CT =$ Costos totales
$VR =$ Valor residual
$VU =$ Vida útil

Modelo de negocio

Estimación de los costos mediante las membresías de alquiler

- **Depreciación de equipos**
- **Costo anual de mantenimiento**
- **Porcentaje de ganancia**

Capítulo 5

6. Conclusiones y recomendaciones

Conclusiones:

- En este trabajo se desarrolló el sistema de detección de comportamiento sospechoso, basado en inteligencia artificial el cual usa un modelo de aprendizaje automático y continuo que luego de entrenarlo tiene una tasa de detección del 59 % si existen 4 personas en la imagen e incluso una tasa de detección del 74 % si hay 28 personas en la imagen, por lo cual nuestro sistema cumple con el objetivo de este proyecto.
- En este trabajo se implemento una red de cámaras y sensores en el espacios público masivo de la FIEC, el mismo, esto nos permitió obtener información relevante para poder entrenar el modelo, y además para poder validar la efectividad del mismo, sin embargo una de los retos que tuvimos fue el tema de permisos de grabación por el aspecto de privacidad de terceros por lo cual a pesar de que nuestro sistema pueda ser beneficioso también debe cumplir con la reglamentación de privacidad vigente del área a vigilar.
- En este trabajo se desarrollo y se probó el algoritmo de aprendizaje profundo, el mismo que fue alimentado por diversas imágenes que fueron bajadas de internet, también las obtenidas por la grabación de la cámara, cabe recalcar que entrenar este modelo no fue fácil, ya que el mismo debía determinar si una persona era sospechosa y muchas veces el modelo no podía diferencia entre arma y otro objeto si la persona lo sostenía en la mano por lo cual tener un buen banco de imágenes es importante.

Recomendaciones:

- Se recomienda realizar actualizaciones periódicas del sistema "DetectGuard Pro"para adaptarse a las cambiantes dinámicas de seguridad y tecnológicas.
- Además, se sugiere considerar la implementación de herramientas de software y hardware clave que puedan mejorar la eficiencia y precisión del sistema, aprovechando las tecnologías de vanguardia disponibles en el mercado.

Bibliografía

Referencias

A., L. (2008, 21 de Octubre). *La intervenciÓn psicolÓgica: CaracterÍsticas y modelos.* Descargado de https://diposit.ub.edu/dspace/bitstream/2445/4963/1/IPCS%20caracter%C3%ADsticas%20y%20modelos.pdf

Ahijon, R. (2023, 03 de Octubre). *¿qué es la detección de incidentes? - msmk university.* Descargado de https://msmk.university/ciberseguridad/que-es-la-deteccion-de-incidentes-msmk-university

Alvarado, N. (2017, 30 de Noviembre). *"5 elementos esenciales para reducir la inseguridad desde lo local," seguridad ciudadana.* Descargado de https://blogs.iadb.org/seguridad-ciudadana/es/elementos-para-reducir-la-inseguridad/

aula21. (2019, 16 de Julio). *Qué es el protocolo ethernet industrial.* Descargado de https://www.cursosaula21.com/que-es-ethernet-industrial/

aula21 | Formación para la Industria. (2020, 08 de Octubre). *¿qué es python?* Descargado de https://www.cursosaula21.com/que-es-python/

Bizkaia.eus. (2024, 07 de Enero). *Modelo de prevencion de riesgo laboral.* Descargado de https://www.bizkaia.eus/Kultura/kirolak/pdf/Guia%20Modelo%20de%20Plan%20de%20Prevencion.pdf?hash=b53f100903f40c7acf33939d2a844ba3

De, L. . R. O. S. . n. (2024, 05 de Febrero). *Codigo organico de entidades de seguridad ciudadana y orden publico.* Descargado de https://www.igualdadgenero.gob.ec/wp-content/uploads/2018/05/C%C3%B3digo-Org%C3%A1nico-de-Entidades-de-Seguridad-Ciudadana-y-Orden-P%C3%BAblico.pdf

Delgado, D. O. (2017, 15 de Septiembre). *¿qué es tensorflow?* Descargado de https://openwebinars.net/blog/que-es-tensorflow/

doctorado en seguridad y prevención, P. D. (2024, 07 de Enero). *Universidad autónoma de barcelona," corteidh.or.cr. [online].* Descargado de https://www.corteidh.or.cr/tablas/r27406.pdf

et al, T. D. T. D. D. (2024, 08 de Enero). *"tribunales de tratamiento de drogas en las américas," oas.org. [online].* Descargado de https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=526&lang=2

fastercapital.com. (2024). *Abordar las preocupaciones de seguridad y privacidad* (1ra ed.). Naciones Unidas. Descargado 2024-02-05, de https://fastercapital.com/es/startup-tema/Abordar-las-preocupaciones-de-seguridad.html

Fastercapital.com. (2024, 04 de Febrero). *Aprendizaje automatico y aib revolucionar la deteccion de fraude en la banca.* Descargado de https://fastercapital.com/es/contenido/Aprendizaje-automatico-y-AIB--revolucionar-la-deteccion-de-fraude-en-la-banca.html

Fernández, C. (2022, 30 de Marzo). *¿qué es la tecnología wifi? características y cómo funciona.* Descargado de https://abamobile.com/web/tecnologia-wifi-que-es-y-caracteristicas/

Fernández, Y. (2020, 27 de Mayo). *Bots de telegram: qué son, cómo funcionan y 17 recomendados para empezar.* Descargado de https://www.xataka.com/basics/bots-telegram-que-como-funcionan-recomendados-para-empezar

Fernández, Y. (2023, 08 de Noviembre). *Wifi, guía a fondo de configuración: todo lo que tienes que saber para mejorar tu conexión.* Descargado de https://www.xataka.com/basics/wifi-guia-a-fondo-configuracion-todo-que-tienes-que-saber-para-mejorar-tu-conexion

Ferrer, E. (2024, 07 de Enero). *Cuadernillo de jurisprudencia de la corte interamericana de derechos humanos no 22: Derechos econÓmicos, sociales, culturales y ambientales.* Descargado de https://www.corteidh.or.cr/sitios/libros/todos/docs/cuadernillo22.pdf

GDPR. (2024, 05 de Febrero). *Lo que debes saber sobre el reglamento general de protección de datos. (n.d.).* Descargado de https://www.powerdata.es/gdpr-proteccion-datos#:~:text=El%20Reglamento%20General%20de%20Protecci%C3%B3n%20de%20Datos%20(GDPR)%20(Reglamento,la%20Uni%C3%B3n%20Europea%20(UE).

Gov.co. (2024, 08 de Enero). *Seguridad y privacidad de la informacion.* Descargado de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Guide, I. D. (2022, 08 de Diciembre). *¿qué es ethernet (ieee 802.3)?* Descargado de https://www.ionos.es/digitalguide/servidores/know-how/ethernet-ieee-8023/

Hartjen, R. (2023, 17 de Noviembre). *Lo que los profesores y el personal deben saber sobre la ciberseguridad.* Descargado 2024-02-05, de https://www.lightspeedsystems.com/blog/es/lo-que-los-profesores-y-el-personal-deben-saber-sobre-la-ciberseguridad/

HeTPro-Tutoriales. (2015, 05 de Abril). *Señal digital, características, frecuencia, ciclo de trabajo.* Descargado de https://hetpro-store.com/TUTORIALES/senal-digital/

Jitterbit. (2021, 22 de Deciembre). *3 desafíos de integración percibidos dentro de recursos humanos y 3 pasos útiles para garantizar una gestión adecuada.* Descargado de https://www.jitterbit.com/es/blog/three-perceived-integration-challenges-within-hr-and-3-helpful-steps-to-ensure-proper-management/

latam.Kaspersky.com. (2024, 18 de Enero). *¿qué es iot (internet de las cosas)?* Descargado de https://latam.kaspersky.com/resource-center/definitions/what-is-iot

Oas.org. (2024, 07 de Enero). *Estrategia institucional para la seguridad ciudadana: Plan nacional de vigilancia comunitaria por cuadrantes (pnvcc).* Descargado de https://www.oas.org/es/sap/dgpe/innovacion/banco/ANEXO%20I.%20PNVCC.pdf

Pi, R. (2019a, 14 de Febrero). *Software de,.* Descargado de https://raspberrypi.cl/software-de-raspberry/

Pi, R. (2019b, 14 de Febrero). *¿que es raspberry pi?* Descargado de https://raspberrypi.cl/que-es-raspberry/

Pickdata.net. (2020, 11 de Mayo). *Node-red, the visual programming tool for internet of things.* Descargado de https://www.pickdata.net/es/noticias/node-red-programacion-visual-iot

Ruz, C. (2020, 01 de Enero). *Evolución de los sistemas operativos.* Descargado de http://iic2333.ing.puc.cl/activities/history.html

Samaniego, J. (2019, 13 de Deciembre). *Detección de fraude utilizando ia en servicios financieros. grupo-novatech.com; grupo novatech.* Descargado de https://www.grupo-novatech.com/deteccion-de-fraude-utilizando-ia-en-servicios-financieros/#:~:text=Un%20algoritmo%20de%20aprendizaje%20autom%C3%A1tico,transacci%C3%B3n%20un%20puntaje%20de%20riesgo.

Segovia, O. (2024, 07 de Enero). Experiencias emblemáticas para la superación de la pobreza y precariedad urbana: espacio público [Manual de software informático]. Descargado de https://repositorio.cepal.org/server/api/core/bitstreams/b7a302c6-d2c9-49c0-bcf4-3894748aa964/content

Sinelec, E. G. (2021, 04 de Febrero). *¿qué es node-red y para qué sirve?* Descargado de https://blog.gruposinelec.com/actualidad/que-es-node-red-y-para-que-sirve/

Store, P. (2024, 15 de Enero). *Camara de seguridad dh-ipc-hdbw2230e-s-s2.* Descargado de https://www.premiumstore.cl/product/camara-de-seguridad-dh-ipc-hdbw2230e-s-s2

V. M. Arévalo, J. G., y Ambrosio, G. (2024, 09 de Enero). *La librerÍa de visiÓn artificial opencv aplicaciÓn a la docencia e investigaciÓn.* Descargado de https://mapir.isa.uma.es/varevalo/drafts/arevalo2004lva1.pdf

Zavaleta, J., Kessler, G., Paternaln, R., y Maldonado, S. (2012). *La inseguridad y la seguridad ciudadana en américa latina* (1ra ed.). Ciudad Autónoma de Buenos Aires: CLACSO.

Anexos

Anexo1. Código general de la cámara web TCP/IP con la PC y uso de MediaPipe (Python)

```python
import cv2
import mediapipe as mp

class PoseDetection:
    def __init__(self, ip, username, password):
        self.mp_pose = mp.solutions.pose
        self.pose = self.mp_pose.Pose()
        # La URL de la c mara IP en este formato: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0
        self.url = f"rtsp://{username}:{password}@{ip}/cam/realmonitor?channel=1&subtype=0"
        self.cap = cv2.VideoCapture(self.url)
        self.exit = False


    def draw_button(self, img, text, x, y, w, h, color):
        cv2.rectangle(img, (x, y), (x + w, y + h), color, -1)
        cv2.putText(img, text, (x + 10, y + 30), cv2.FONT_HERSHEY_SIMPLEX, 1, (255, 255, 255), 2, cv2.LINE_AA)

    def check_button(self, x, y, h):
        if 10 <= x <= 210 and (h + 10) <= y <= (h + 60):
            return 'STOP'
        elif 220 <= x <= 420 and (h + 10) <= y <= (h + 60):
            return 'EXIT'
        elif 430 <= x <= 630 and (h + 10) <= y <= (h + 60):
            return 'RESUME'
        return None

    def mouse_callback(self, event, x, y, flags, param):
        h = param
        if event == cv2.EVENT_LBUTTONDOWN:
            button = self.check_button(x, y, h)
            if button == 'STOP':
                for i in range(5, 0, -1):
                    frame = self.cap.read()[1]  # Obtener el marco actual
                    self.draw_button(frame, f'STOPPING IN {i} SECONDS', 10, h + 10, 200, 50, (0, 0, 255))
                    cv2.imshow('Pose Detection', frame)
                    cv2.waitKey(1000)  # Pausa de 1 segundo
                cv2.waitKey(0)  # Pausa
            elif button == 'EXIT':
                self.exit = True
            elif button == 'RESUME':
```

```
41                 pass  # No hacemos nada espec fico aqu , simplemente continuar  el bucle
42
43     def run(self):
44         cv2.namedWindow('Pose Detection')
45         cv2.resizeWindow('Pose Detection', 640, 480)
46
47         while self.cap.isOpened():
48             ret, frame = self.cap.read()
49             h, w, _ = frame.shape
50             cv2.setMouseCallback('Pose Detection', self.mouse_callback, h)
51
52             button_panel = 80  # Espacio adicional para los botones
53             frame = cv2.copyMakeBorder(frame, 0, button_panel, 0, 0, cv2.BORDER_CONSTANT)
54
55             # Convertir el color BGR de OpenCV a RGB para MediaPipe
56             image_rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
57             results = self.pose.process(image_rgb)
58
59             # Dibujar los puntos de la pose en el frame
60             if results.pose_landmarks:
61                 mp.solutions.drawing_utils.draw_landmarks(frame, results.pose_landmarks, self.mp_pose.POSE_CONNECTIONS)
62
63                 pose_landmarks = results.pose_landmarks.landmark
64
65                 # Obtener las coordenadas de las manos y puntos de la cintura
66                 mano_izquierda = pose_landmarks[mp.solutions.pose.PoseLandmark.LEFT_WRIST]
67                 mano_derecha = pose_landmarks[mp.solutions.pose.PoseLandmark.RIGHT_WRIST]
68                 cintura_1 = pose_landmarks[mp.solutions.pose.PoseLandmark.LEFT_HIP]
69                 cintura_2 = pose_landmarks[mp.solutions.pose.PoseLandmark.RIGHT_HIP]
70
71                 # Dibujar c rculos en las manos y puntos de la cintura
72                 cv2.circle(frame, (int(mano_izquierda.x * w), int(mano_izquierda.y * h)), 10, (0, 0, 255), -1)
73                 cv2.circle(frame, (int(mano_derecha.x * w), int(mano_derecha.y * h)), 10, (0, 0, 255), -1)
74                 cv2.circle(frame, (int(cintura_1.x * w), int(cintura_1.y * h)), 10, (0, 255, 0), -1)
```

```
75                  cv2.circle(frame, (int(cintura_2.x * w), int(
    cintura_2.y * h)), 10, (0, 255, 0), -1)
76
77                  # Mostrar la posici n de las manos y puntos de la
     cintura
78                  cv2.putText(frame, f"Mano Izquierda: ({int(
    mano_izquierda.x * w)}, {int(mano_izquierda.y * h)})", (10, h -
     50), cv2.FONT_HERSHEY_SIMPLEX, 0.5, (0, 0, 255), 1)
79                  cv2.putText(frame, f"Mano Derecha: ({int(
    mano_derecha.x * w)}, {int(mano_derecha.y * h)})", (10, h - 30)
    , cv2.FONT_HERSHEY_SIMPLEX, 0.5, (0, 0, 255), 1)
80                  cv2.putText(frame, f"Cintura 1: ({int(cintura_1.x
    * w)}, {int(cintura_1.y * h)})", (10, h - 10), cv2.
    FONT_HERSHEY_SIMPLEX, 0.5, (0, 255, 0), 1)
81                  cv2.putText(frame, f"Cintura 2: ({int(cintura_2.x
    * w)}, {int(cintura_2.y * h)})", (10, h + 10), cv2.
    FONT_HERSHEY_SIMPLEX, 0.5, (0, 255, 0), 1)
82
83              self.draw_button(frame, 'STOP', 10, h + 10, 200, 50,
    (0, 0, 255))
84              self.draw_button(frame, 'EXIT', 220, h + 10, 200, 50,
    (0, 255, 0))
85              self.draw_button(frame, 'RESUME', 430, h + 10, 200,
    50, (255, 255, 0))
86
87              cv2.imshow('Pose Detection', frame)
88
89              k = cv2.waitKey(1) & 0xFF
90              if k == ord('q'):
91                  break
92
93              if self.exit:
94                  break
95
96          self.cap.release()
97          cv2.destroyAllWindows()
98
99  if __name__ == '__main__':
100     # Cambia las credenciales y la direcci n IP seg n la
    configuraci n de tu c mara
101     ip_address = "192.168.1.6"
102     username = "admin"
103     password = "admin"
104
105     pd = PoseDetection(ip_address, username, password)
106     pd.run()
```

Anexo 2. Código de la cámara web RTCP/IP con la pc y uso de TensorFlow

```
import cv2
import dlib
import mediapipe as mp

class PoseDetection:
    def __init__(self, ip, username, password):
        # Inicializar detector de rostros
        self.detector = dlib.get_frontal_face_detector()

        # Inicializar detector de puntos clave de la pose
        self.mp_pose = mp.solutions.pose
        self.pose = self.mp_pose.Pose()

        # La URL de la c mara IP en este formato: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0
        self.url = f"rtsp://{username}:{password}@{ip}/cam/realmonitor?channel=1&subtype=0"
        self.cap = cv2.VideoCapture(self.url)
        self.exit = False
        self.people = []

    def run(self):
        cv2.namedWindow('Pose Detection')
        cv2.resizeWindow('Pose Detection', 640, 480)

        while self.cap.isOpened():
            ret, frame = self.cap.read()
            h, w, _ = frame.shape

            # Convertir el color BGR de OpenCV a RGB para MediaPipe
            image_rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
            results = self.pose.process(image_rgb)

            # Detecci n de rostros con dlib
            faces = self.detector(frame)

            # Dibujar los puntos de la pose en el frame
            if results.pose_landmarks:
                mp.solutions.drawing_utils.draw_landmarks(frame, results.pose_landmarks, self.mp_pose.POSE_CONNECTIONS)

                self.people = []
                for person_id, face in enumerate(faces):
                    x1, y1, x2, y2 = face.left(), face.top(), face
```

```
    .right(), face.bottom()
42                      self.people.append((person_id, x1, y1, x2, y2)
    )
43
44                      # Dibujar rect ngulo y etiqueta para cada
    persona
45                      cv2.rectangle(frame, (x1, y1), (x2, y2), (255,
     0, 0), 2)
46                      cv2.putText(frame, f'Persona {person_id + 1}',
     (x1, y1 - 10), cv2.FONT_HERSHEY_SIMPLEX, 0.5, (255, 0, 0), 1,
    cv2.LINE_AA)
47
48              cv2.imshow('Pose Detection', frame)
49
50              k = cv2.waitKey(1) & 0xFF
51              if k == ord('q'):
52                  break
53
54          self.cap.release()
55          cv2.destroyAllWindows()
56
57 if __name__ == '__main__':
58      # Cambia las credenciales y la direcci n IP seg n la
    configuraci n de tu c mara
59      ip_address = "192.168.1.6"
60      username = "admin"
61      password = "admin"
62
63      pd = PoseDetection(ip_address, username, password)
64      pd.run()
```

Anexo 3.Código general del procesamiento de la inteligencia artificial (TensorFlow) y el procesamiento de 12500 imágenes

```
1 import tensorflow as tf
2 from tensorflow.keras import layers, models
3 from tensorflow.keras.preprocessing.image import
    ImageDataGenerator
4 import matplotlib.pyplot as plt
5
6 # Definir las rutas de las carpetas
7 data_dir = r'C:\Users\Lukitas\OneDrive\Escritorio\archivos de
    integradora (proyecto)\imagenes'
8 train_dir = data_dir + r'\frame-principal'
9 test_dir = data_dir + r'\frame-principal'  # Puedes cambiar esto
    dependiendo de tu estructura de datos
10
```

```
# Configurar generadores de datos
batch_size = 32
img_size = (256, 256)

train_datagen = ImageDataGenerator(rescale=1./255,
    validation_split=0.2)
test_datagen = ImageDataGenerator(rescale=1./255)

train_generator = train_datagen.flow_from_directory(
    train_dir,
    target_size=img_size,
    batch_size=batch_size,
    class_mode='binary',  # O 'categorical' si hay m s de dos
    clases
    subset='training'
)

validation_generator = train_datagen.flow_from_directory(
    train_dir,
    target_size=img_size,
    batch_size=batch_size,
    class_mode='binary',
    subset='validation'
)

# Crear el modelo de red neuronal
model = models.Sequential()
model.add(layers.Conv2D(32, (3, 3), activation='relu', input_shape
    =(256, 256, 3)))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(64, (3, 3), activation='relu'))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(128, (3, 3), activation='relu'))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Flatten())
model.add(layers.Dense(128, activation='relu'))
model.add(layers.Dense(1, activation='sigmoid'))  # Salida binaria

# Compilar el modelo
model.compile(optimizer='adam',
              loss='binary_crossentropy',
              metrics=['accuracy'])

# Entrenar el modelo
history = model.fit(
    train_generator,
    epochs=10,  # Ajusta el n mero de  pocas  seg n sea
    necesario
    validation_data=validation_generator
```

```
)

# Visualizar las m tricas
# Obtener las m tricas de entrenamiento
accuracy = history.history['accuracy']
val_accuracy = history.history['val_accuracy']
loss = history.history['loss']
val_loss = history.history['val_loss']

# Crear gr ficas de precisi n
plt.figure(figsize=(12, 4))
plt.subplot(1, 2, 1)
plt.plot(accuracy, label='Training Accuracy')
plt.plot(val_accuracy, label='Validation Accuracy')
plt.title('Training and Validation Accuracy')
plt.xlabel('Epoch')
plt.ylabel('Accuracy')
plt.legend()

# Crear gr ficas de p rdida
plt.subplot(1, 2, 2)
plt.plot(loss, label='Training Loss')
plt.plot(val_loss, label='Validation Loss')
plt.title('Training and Validation Loss')
plt.xlabel('Epoch')
plt.ylabel('Loss')
plt.legend()

# Mostrar las gr ficas
plt.tight_layout()
plt.show()

# Guardar el modelo entrenado
model.save('theft_detection_model.h5')
```

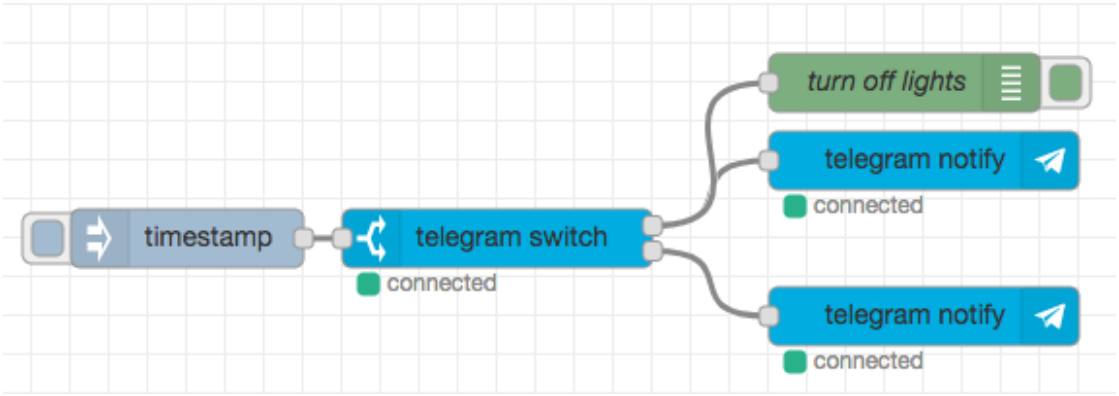
Anexo 4.Resultados estadísticos sobre la precisión con la que la cámara compara con las fotos guardadas usando inteligencia artificial

```
import tensorflow as tf
from tensorflow.keras import layers, models
from tensorflow.keras.preprocessing.image import
    ImageDataGenerator
import matplotlib.pyplot as plt

# Definir las rutas de las carpetas
```

```
data_dir = r'C:\Users\Lukitas\OneDrive\Escritorio\archivos de integradora (proyecto)\imagenes'
train_dir = data_dir + r'\frame-principal'
test_dir = data_dir + r'\frame-principal'  # Puedes cambiar esto dependiendo de tu estructura de datos

# Configurar generadores de datos
batch_size = 32
img_size = (256, 256)

train_datagen = ImageDataGenerator(rescale=1./255, validation_split=0.2)
test_datagen = ImageDataGenerator(rescale=1./255)

train_generator = train_datagen.flow_from_directory(
    train_dir,
    target_size=img_size,
    batch_size=batch_size,
    class_mode='binary',  # O 'categorical' si hay m s de dos clases
    subset='training'
)

validation_generator = train_datagen.flow_from_directory(
    train_dir,
    target_size=img_size,
    batch_size=batch_size,
    class_mode='binary',
    subset='validation'
)

# Crear el modelo de red neuronal
model = models.Sequential()
model.add(layers.Conv2D(32, (3, 3), activation='relu', input_shape=(256, 256, 3)))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(64, (3, 3), activation='relu'))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(128, (3, 3), activation='relu'))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Flatten())
model.add(layers.Dense(128, activation='relu'))
model.add(layers.Dense(1, activation='sigmoid'))  # Salida binaria

# Compilar el modelo
model.compile(optimizer='adam',
              loss='binary_crossentropy',
              metrics=['accuracy'])

```

```
# Entrenar el modelo
history = model.fit(
    train_generator,
    epochs=10,  # Ajusta el n mero de  pocas  seg n sea necesario
    validation_data=validation_generator
)

# Visualizar las m tricas
# Obtener las m tricas de entrenamiento
accuracy = history.history['accuracy']
val_accuracy = history.history['val_accuracy']
loss = history.history['loss']
val_loss = history.history['val_loss']

# Crear gr ficas de precisi n
plt.figure(figsize=(12, 4))
plt.subplot(1, 2, 1)
plt.plot(accuracy, label='Training Accuracy')
plt.plot(val_accuracy, label='Validation Accuracy')
plt.title('Training and Validation Accuracy')
plt.xlabel('Epoch')
plt.ylabel('Accuracy')
plt.legend()

# Crear gr ficas de p rdida
plt.subplot(1, 2, 2)
plt.plot(loss, label='Training Loss')
plt.plot(val_loss, label='Validation Loss')
plt.title('Training and Validation Loss')
plt.xlabel('Epoch')
plt.ylabel('Loss')
plt.legend()

# Mostrar las gr ficas
plt.tight_layout()
plt.show()

# Guardar el modelo entrenado
model.save('theft_detection_model.h5')
```

Anexo 5. Captura sobre funcionamiento del bot de Telegram



Anexo 6. Diagrama de proceso integrador con respecto a los procesos en la intervención física, virtual y de retroalimentación de componentes usados