



UNIVERSIDAD NACIONAL DE CHIMBORAZO

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE
SEGURIDAD VEHICULAR BASADO EN TECNOLOGÍA LORA
PARA MONITOREO REMOTO Y PREVENCIÓN DE ROBOS

Autor: Machado Ordoñez Cesar Gonzalo

Tutor: Mgs. Pozo Jara Alejandra del Pilar

Riobamba, Ecuador

2026



UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE TELECOMUNICACIONES

TRABAJO DE TITULACIÓN - MODALIDAD TRABAJO DE INVESTIGACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

TÍTULO:

**DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE
SEGURIDAD VEHICULAR BASADO EN TECNOLOGÍA LORA
PARA MONITOREO REMOTO Y PREVENCIÓN DE ROBOS**

AUTOR:

Machado Ordoñez Cesar Gonzalo

TUTOR:

Mgs. Pozo Jara Alejandra del Pilar

Riobamba, Ecuador

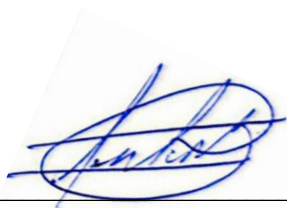
2026

© DECLARATORIA DE AUTORÍA

Yo, **CESAR GONZALO MACHADO ORDOÑEZ**, con cédula de identidad 0604899005, autora del trabajo de titulación: **Diseño e implementación de un sistema de seguridad vehicular basado en tecnología lora para monitoreo remoto y prevención de robos**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mi exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor de la obra referida, será de Elija un elemento. entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 7 de agosto de 2026.



Cesar Gonzalo Machado Ordoñez

C.I: 0604899005

DECLARATORIA SOBRE EL USO DE HERRAMIENTAS DE IA

Yo, **CESAR GONZALO MACHADO ORDOÑEZ**, con cédula de identidad **0604899005**, autora del presente trabajo de titulación, declaro que el uso de herramientas de inteligencia artificial en la elaboración del presente trabajo de titulación se limitó exclusivamente al apoyo en la organización de ideas y a la mejora de la redacción y claridad expositiva, en los apartados de introducción, marco teórico y marco metodológico, sin implicar la generación autónoma de contenidos académicos, análisis, resultados, conclusiones ni aportes propios del proceso investigativo.

Asimismo, dejo constancia de que las decisiones académicas, el desarrollo conceptual, el enfoque metodológico, el análisis de fuentes y la interpretación de resultados son de mi exclusiva responsabilidad.

Finalmente, declaro que el uso de dichas herramientas no sustituyó mi criterio académico, ni vulneró las disposiciones institucionales sobre plagio, propiedad intelectual y autoría, manteniéndose el cumplimiento de las normas de citación y referenciación, con el fin de garantizar la transparencia académica y el uso ético y responsable de tecnologías emergentes en la elaboración del trabajo de titulación.

En Riobamba, 7 de agosto de 2026.



Cesar Gonzalo Machado Ordoñez
C.I: 0604899005

DEDICATORIA

Dedico este trabajo de titulación primordialmente a Dios, por ser mi guía y fortaleza en cada etapa de mi formación.

A mis padres, Lic. Cesar Augusto Machado Vallejo y Msc. Melba Azucena Ordoñez Martínez, por ser el pilar fundamental de mi vida, por sus consejos y por el sacrificio constante para brindarme una educación de calidad. Sus valores y enseñanzas son la base de este logro.

A mi hermana, Jennypher Marina Machado Ordoñez, por su apoyo incondicional y por ser mi compañera constante en este camino.

A mis primos, Msc. Cristian Fabian Machado Villalba y Msc. Alicia Edith Machado Villalba, por su motivación y por compartir conmigo los desafíos de este proceso.

A mis segundos padres, Ing. Franklin Machado y Rocío Cabascango, por su guía, sus consejos y por brindarme un hogar lleno de sabiduría y apoyo cuando más lo necesité.

AGRADECIMIENTO

Mi profundo agradecimiento a la Mgsc. Alejandra del Pilar Pozo Jara, mi tutora de tesis, por su paciencia, su guía experta y su invaluable apoyo académico durante todo este proceso. Gracias por sus valiosas correcciones y por motivarme a alcanzar la excelencia técnica en este proyecto.

Quiero expresar mi gratitud más sincera a la Abogada Mery María Saca Pérez, quien creyó en mis capacidades desde el preuniversitario hasta el día de hoy. Su apoyo incondicional y su mentoría profesional fueron determinantes para mantenerme firme en el camino y alcanzar este sueño. Gracias, por ser mi mayor inspiración, mi guía académica y mi refugio en cada paso de este proceso.

A mi fiel amiga, Ing. Jesael Fernanda Llamuca Villa, por su lealtad, por los días de estudio compartidos y por brindarme su mano amiga en los momentos de mayor presión académica. Su apoyo técnico y emocional ha sido invaluable en mi formación.

De manera especial, agradezco a mis grandes amigos Washington Jiménez y Kevin Medina, por su apoyo constante y por estar presentes en cada paso de este camino. Su amistad ha sido un motor fundamental para superar los desafíos y alcanzar esta meta profesional.

A la Universidad Nacional de Chimborazo, por abrirme sus puertas y permitirme formarme en sus aulas, y a todos los docentes que contribuyeron con sus conocimientos al desarrollo de mi carrera.

INDICE

RESUMEN	10
ABSTRACT	11
INTRODUCCIÓN.....	16
PLANTEAMIENTO DEL PROBLEMA.....	18
JUSTIFICACIÓN.....	19
OBJETIVOS.....	20
General.....	20
Específicos.....	20
MARCO REFERENCIAL	21
ESTADO DEL ARTE	21
Fundamentos Teóricos.....	22
Sistemas de seguridad vehicular.....	22
LoRa	22
LoRaWAN.....	23
Principios de Funcionamiento	23
Arquitectura de Red.....	23
Ventajas frente a tecnologías celulares.....	23
Casos de Uso en Seguridad y Monitoreo	23
Comunicaciones Inalámbricas de Bajo Consumo	23
Redes LPWAN y Comparación entre Sigfox, NB-IoT	24
Características Técnicas de LoRaWAN	24
Frecuencia y modulación.....	24
Alcance y comportamiento en entornos edificados.....	24
<i>Consumo energético</i>	25
Topología de red y escalabilidad.....	25
Sensores y dispositivos IoT aplicados a seguridad vehicular.....	25
Modelos de Propagación de Señal.....	26
Contexto geográfico y tecnológico del barrio Santa Ana.....	26
Arduino.....	27
Lógica de procesamiento y detección de eventos.....	27
¿Para qué sirve un algoritmo en el sistema de seguridad?	28

Características de los algoritmos	29
Partes que componen el algoritmo de seguridad	29
Casos de uso de la seguridad y monitoreo en diversas industrias	30
Tecnologías y protocolos para la detección de eventos.....	30
Comparación de métodos de detección en sistemas embebidos.....	31
METODOLOGÍA.....	31
TIPO DE INVESTIGACIÓN	31
DISEÑO DE INVESTIGACIÓN	32
Fase 1: Análisis y estudio	33
Fase 2: Diseño del sistema.....	33
Fase 3: Desarrollo de la interfaz	33
Fase 4: Evaluación.....	33
TÉCNICAS DE RECOLECCIÓN DE DATOS.....	33
Fuentes de investigación.....	33
POBLACIÓN DE ESTUDIO Y TAMAÑO DE MUESTRA	34
Población	34
Muestra	35
OPERACIONALIZACIÓN DE LAS VARIABLES	35
MÉTODOS DE ANÁLISIS Y PROCESAMIENTO DE DATOS	36
Revolucionando la seguridad vehicular mediante IoT	36
Soluciones tecnológicas para la prevención de robos	36
Estudio de Algoritmos para el Procesamiento y Detección de Eventos.....	39
Arquitectura de Procesamiento y Comunicación LoRa	40
Implementación de la Lógica de Detección y Gestión de Alertas.....	42
Interfaz de Notificación y Monitoreo (Telegram Bot)	47
Interfaz de Usuario y Plataforma de Monitoreo	48
RESULTADOS Y DISCUSIÓN	49
RESULTADOS	49
Análisis de resultados binomiales.....	49
DISCUSIÓN	51
CONCLUSIONES.....	52
RECOMENDACIONES	53
BIBLIOGRAFÍA	54

ANEXOS.....	57
-------------	----

RESUMEN

La investigación que se presenta aquí se desarrolla en torno a la creación y aplicación de un sistema de seguridad, antirrobo de vehículos, basado en tecnologías del Internet de las Cosas (IoT) y comunicación de larga distancia (LoRa). El problema que se ha identificado tiene que ver con la ineficiencia que ofrecen las alarmas convencionales que dependen de alarmas sonoras que normalmente pasan inadvertidas, puesto que no tienen la opción de tener un sistema de notificación inmediata. Por ello, se ha diseñado un prototipo con el microcontrolador ESP32-LoRa y se ha hecho la experimentación con una red de sensores multimodales IMU para impactos, ToF y PIR para la proximidad y GPS para el rastreo.

La metodología empleada fue de carácter experimental con un enfoque cuantitativo, utilizando el método estadístico de Distribución Binomial y Pruebas de Hipótesis (t de Welch) para validar la eficacia del sistema mediante 50 ensayos controlados. Los resultados obtenidos han mostrado una tasa de éxito de un 96% en las medidas de detección y envío de alertas ($p < 0,05$), logrando enviar alertas con información visual y geolocalización al usuario mediante un bot de Telegram, alcanzando un tiempo promedio de respuesta de 101.62 s, mostrándose notablemente más rápido y estable que las técnicas tradicionales. Por tanto, se establece que la arquitectura creada representa una solución sólida y eficaz para la protección de activos móviles que permite una reacción preventiva del propietario y aumenta de forma sustancial las probabilidades de recuperación del vehículo en caso de intento de hurto.

Palabras claves: Sistema antirrobo, ESP32, LoRa, Internet de las Cosas (IoT), Geolocalización, Seguridad electrónica, Telemetría, Bot de Telegram.

ABSTRACT

The study provides insight into developing and employing a vehicle anti-theft security mechanism utilizing the Internet of Things (IoT) and Long-Range (LoRa) technologies. Issues brought to attention include a problem concerning traditional alarms' failure, which operates on sound alerts that may be unnoticed due to their inability to inform about break-ins immediately. As a result, a prototype was developed using ESP32-LoRa microcontrollers, and experiments were actually carried out with a network of multimodal sensors (IMU detects bumps, ToF and PIR are responsible for detecting intrusion, and GPS is used for tracking).

The methodology used in the investigation is experimental in character and quantitative in its approach, based on statistical methods, namely, the technique of binomial distribution and hypothesis testing (Welch's t-test) which allows validating the efficiency of the developed system through 50 experiments. The outcome of the study has a detection and alerting efficiency equal to 96% ($p < 0.05$) providing alerting of the user through a Telegram bot equipped with visual information and geographic location in an average of 101.62 seconds effectively and much faster than the classical techniques. The findings of the investigation lead to the conclusion about the efficiency of the developed architecture since it can ensure the efficient protection of mobile objects which allows its owner to take preventive measures and increase the probability of recovery of the vehicle after the theft.

Keywords: Anti-theft system, ESP32, LoRa, Internet of Things (IoT), Geolocation, Electronic security, Telemetry, Telegram Bot.



**Mario Nicolas
Salazar Ramos**



Revised by
Mario N. Salazar
0604069781

INTRODUCCIÓN

El hurto de automóviles se ha consolidado como una problemática global que produce efectos sociales y económicos profundos; no obstante, en un país como Ecuador, que aún se halla en fase de desarrollo, el fenómeno adquiere dimensiones de extraordinaria complejidad y transforma el territorio en un nodo estratégico de la criminalidad organizada. La escasez de datos empíricos y la dificultad de su recolección permiten extraer inferencias cautas, y ellas apuntan, no obstante, a un ascenso en la incidencia de este delito, cuyos efectos son devastadores no solo para los propietarios y las entidades aseguradoras, sino, en última instancia, para la propia salud de la seguridad pública. Desde 2025 han sido reportados, al menos, 1500 sucesos de hurto de automotores en el país; en términos ejemplificativos, Quito ha contabilizado 529 casos. Esta cifra, que se ha estabilizado en el trimestre que cerró en marzo, integra una proyectada alza del 5% para el año 2024 y evidencia la permanencia del fenómeno, la concomitante expansión de la criminalidad y, sobre todo, la apremiante necesidad de reducir la creciente vulnerabilidad del parque vehicular nacional. Tal escenario pone en evidencia la exigencia de diseñar intervenciones que se inscriban en la complejidad estructural y económica del país [1].

Dentro del ecosistema tecnológico actual, la norma Zigbee puede figurar como opción para la telemetría vehicular. Su bajo consumo energético y su capacidad para políticas de red en canalización de datos de corto alcance resultan atractivas, sin embargo, su alcance restringido la desvincula de la telemetría de área amplia, donde la conectividad continua es requisito primordial. Por su parte, la tecnología Wi-Fi, a pesar de ofrecer tasas de transmisión elevadas, no se alinea con los criterios de las arquitecturas celulares, debido a su alcance restringido y su demanda energética significativa. La tecnología RFID se utiliza para el control de acceso y la monitorización pasiva, sin embargo, carece de capacidades de seguimiento en tiempo real [1].

La tecnología moderna, por ejemplo, los sistemas de vehículos de seguridad por GPS, aún cuentan con serias deficiencias en su funcionalidad. Generalmente, el uso de sistemas de telefonía móvil procesadores de datos incrementa los costos y resulta en escasa o nula cobertura en algunas regiones. Además, el elevado consumo energético de estos dispositivos limita su uso a corto plazo, lo que resulta en gastos poco convenientes para muchos usuarios [2].

Ante el escenario planteado, la tecnología LoRa (Long Range), la cual es fundamento de la arquitectura LoRaWAN, surge como una opción innovadora para vencer las restricciones que presentan las redes tradicionales y así también las aplicaciones relacionadas a la seguridad de los automotores. Esta tecnología posibilita el envío de datos a grandes distancias con un uso reducido de energía y sin requerir infraestructura celular, lo que la convierte en la opción perfecta para su aplicación en áreas urbanas, rurales y alejadas del perímetro urbano. Organizada a través de puertas de enlace y servidores de red, posibilita la creación de soluciones escalables con extensa cobertura territorial [3][4].

Por lo tanto, esta investigación se realiza con el fin de dar una contribución relevante tanto en términos tecnológicos como sociales, integrando innovación, sostenibilidad y accesibilidad en la lucha contra el robo frecuente de vehículos. El sistema propuesto se desarrollará específicamente en el barrio Santa Ana del municipio de Licán, cantón de Riobamba, una zona

rural con cobertura de telefonía móvil limitada. Las ventajas que representa un entorno ideal para evaluar la viabilidad de una solución basada en LoRaWAN. Este sistema no solo resolverá la problemática de seguridad, también se pretende que ayude para mejorar la prevención, el rastreo y la recuperación de los vehículos robados en este sector, adaptándose a las necesidades específicas de diversos entornos en zonas urbanas y rurales o las que requieran [1].

Este prototipo tiene como objetivo medir el desempeño de esta tecnología a través de factores concretos, tales como la intensidad de la señal (RSSI) obtenida en distintos lugares del sector y la eficacia del sistema de alerta si se detecta un intento de hurto confirmado a través de alertas producidas por GPS y procesadas por microcontroladores. Estos indicadores permitirán verificar si LoRaWAN ofrece suficiente cobertura y confiabilidad para su implementación a gran escala en zonas con mala conectividad telefónica así también condiciones hidrográficas difíciles.

PLANTEAMIENTO DEL PROBLEMA

El robo de automóviles sigue siendo un problema significativo en todo el mundo, con enormes pérdidas económicas tanto para el propietario como para la compañía de seguros. Hoy en día, la tecnología ofrece algunas soluciones en el área de control de acceso y prevención, sin embargo, los sistemas de seguridad automotriz aún sufren de desventajas como la dependencia de la red móvil, altos costos, consumo de energía y sistemas de vigilancia de automóviles. Estos los hacen vulnerables a métodos de robo más sofisticados.

En el Ecuador, durante el primer semestre del 2023, los robos se han duplicado durante el mismo periodo del año anterior, este incremento no solo perjudica a la seguridad pública si no también en el ámbito financiero nacional. Topográficamente, se ha registrado el mayor número de robos en provincias tales como Guayas (36%), Pichincha (23%) y Los Ríos (19%), lo cual impone la necesidad inmediata de diseñar e implementar estrategias de prevención y de control [1]

La insuficiencia de infraestructura en telecomunicaciones constituye un impedimento considerable para la gestión y recuperación de vehículos sustraídos. En el panorama presente de la vigilancia de flotas automotrices, revela la falta de soluciones que proporcionen, simultáneamente, cobertura ampliada y bajo consumo energético, condiciones necesarias para recibir notificaciones en tiempo real y ejecutar acciones correctivas o preventivas con inmediatez.

Uno de los factores que impiden para la recuperación de los automotores es la deficiente estructura de telecomunicaciones. Por ejemplo, los sistemas de seguridad que utilizan tecnología GSM suelen ser ineficientes debido a que, si no se dispone de una estructura de red apropiada, ocasiona problemas de transmisión de alertas e impide la localización del vehículo en tiempo real.

Por lo tanto, el no tener una buena estructura de telecomunicaciones en zonas rurales como la parroquia de Lican constituye a un problema para la seguridad vehicular, ya que los sistemas con red GSM presentan inconvenientes debida a la cobertura inestable y la vulnerabilidad de la señal ya que son caminos de tercer orden [2], [3]. En el sector de Santa Ana, esta limitación tecnológica, sumada a la baja densidad demográfica y la iluminación fragmentaria, facilita el tránsito y ocultamiento de vehículos robados, evidenciando la necesidad de soluciones que operen con independencia de las operadoras móviles tradicionales. Ante este escenario, la tecnología LoRa se presenta como una alternativa técnica superior y rentable, pues su capacidad de transmitir datos a gran distancia con bajo consumo energético permite superar los vacíos de la red celular, estableciendo a Santa Ana como la zona piloto ideal para validar esta solución en la recuperación y monitoreo de automotores [4], [5], [6].

JUSTIFICACIÓN

Bajo esta premisa se trata de dar una solución en sectores donde las telecomunicaciones son deficiente e ineficaces, como en las áreas rurales o marginales. Especialmente en el sector de Santa Ana, donde la cobertura celular es ineficiente, la introducción de la tecnología LoRaWAN permitirá información importante, como la ubicación del GPS y la condición del vehículo, lo cual facilitará la respuesta inmediata al usuario. Estudios recientes han demostrado que la tecnología LoRaWAN es muy efectiva ya que mantiene una conexión continua sin poner en peligro la autonomía del dispositivo [7]. Por lo tanto, permitirá que este proyecto evalúe su aplicabilidad en el espacio interno del vehículo y ofrezca una alternativa tecnológica e innovadora a las restricciones comunes de la infraestructura móvil.

Desde un punto de vista técnico, las alarmas sonoras convencionales han resultado inadecuadas, en tanto que su funcionamiento se basa en la reacción de otras personas ante la percepción de un estímulo que generalmente se ignora en ambientes urbanos. Este proyecto persigue una evolución hacia una seguridad proactiva; el propietario recibe la información que considera necesaria, pero considera que sólo el propietario la recibe de manera detallada y multimedia (información visual y coordenadas GPS). La conexión de una red de sensores multimodales permite efectuar la detección con más certeza, lo cual ayuda a disminuir la probabilidad de los falsos avisos y a hacer una toma de decisiones inmediata.

Por último, este trabajo propone una alternativa tecnológica innovadora que mejora la protección de los activos móviles en áreas poco accesibles mediante la obtención de un prototipo de bajo coste, pero de elevada capacidad de transmisión con el objetivo de contribuir al fomento de la seguridad electrónica local mediante la generación de una herramienta eficiente que respete las restricciones reales del estado de la infraestructura de conectividad vigente.

OBJETIVOS

General

Desarrollar un prototipo de seguridad para vehículos utilizando tecnología de largo alcance, que permita la localización y monitoreo en tiempo real, proporcionando una solución eficiente, de bajo costo y bajo consumo energético.

Específicos

- Investigar y analizar las tecnologías actuales de seguridad vehicular, identificando sus limitaciones y las necesidades específicas de los usuarios.
- Diseñar e implementar un sistema de localización y monitoreo vehicular basado en tecnología de largo alcance, que garantice una transmisión de datos eficiente y un bajo consumo energético.
- Desarrollar un prototipo funcional del sistema de seguridad vehicular, integrando dispositivos de comunicación de largo alcance.
- Evaluar el funcionamiento del prototipo en condiciones reales, verificando su eficacia, cobertura y confiabilidad en la transmisión de datos.

MARCO REFERENCIAL

ESTADO DEL ARTE

El robo de vehículos en Ecuador ha llegado a alcanzar cifras alarmantes, llegando a más de 6,700 delitos reportados a nivel nacional hasta finales del año 2025, cada vez más amplificado por la sofisticación del delito organizada a partir del uso de inhibidores de señal (jammers) que evitan que los GSM puede ser utilizados. En la provincia de Chimborazo, este fenómeno se ha convertido en el delito más impactante en Riobamba, demostrando que la infraestructura tradicional de las telecomunicaciones no es suficiente contra las zonas de sombra y la manipulación de frecuencias. Ante una vulnerabilidad en la red, sobresale en este momento la tecnología LoRaWAN como una opción estratégica para mejorar el monitoreo de activos, para optimizar las limitaciones de cobertura celular, y garantizar la transmisión de datos en ambientes donde la red móvil tradicional es incapaz [8].

Dentro del área del monitoreo y la seguridad de los coches se han publicado algunos trabajos que hacen uso de la tecnología LoraWAN para mejorar el seguimiento y la seguridad de los activos. En primer lugar, [9] presentaron un sistema de monitorización basado en LoraWAN para el seguimiento en tiempo real, que mandaba las coordenadas GPS de los coches a una plataforma web; aunque su trabajo destacó por la eficiencia energética y una buena cobertura, echaban de menos mecanismos de detección de robos. A la vez, [10] llevaron a cabo un dispositivo antirrobo con módulos GPS y sensores de vibración para disparar las alertas, pero comentan que la latencia de la red afectó a la oportunidad de respuesta en situaciones críticas.

Adicionalmente, [11]proponen una plataforma de IoT con procesamiento en la nube para detectar comportamientos anómalos, [11]de forma que se consigue escalabilidad y adaptabilidad, pero con una escasa aplicabilidad para zonas rurales, por requerir de una infraestructura con una alta densidad de puertas de enlace. En la misma línea [12] Vital Solutions y Financial explicaron, mediante su metodología de monitoreo operativo, sobre el sistema de control vehicular con un enfoque centrado en el monitoreo urbano, el cual, no presentó por su parte algoritmos concretos destinados a la prevención de sustracciones.

Por otro lado, la conectividad en zonas con infraestructura limitada, [13]idearon un sistema híbrido que incorpora LoRaWAN con redes celulares para garantizar la transmisión de datos sin interrupciones, mejorando significativamente la fiabilidad del sistema. Igualmente, [14]describen el ciclo de vida de un modelo predictivo, que se basa en disponer de los mecanismos que permiten anticiparse al hecho del robo mediante los patrones de comportamiento y las alertas automáticas. Y como última, [15]analizan el rendimiento de diferentes protocolos en sistemas IoT, determinando que LoRaWAN es el indicado por su alcance y su gran eficiencia energética; eso sí, es necesario complementarlo con otras tecnologías para mitigar los problemas de latencia en aplicaciones de seguridad crítica.

Fundamentos Teóricos

Sistemas de seguridad vehicular



Figura 1. Monitoreo vehicular [16]

Los primeros sistemas de seguridad de vehículos se basaron en mecanismos físicos, como los bloqueadores de pedales, volante o cerraduras reforzadas. Con los avances en la electrónica se incluyeron alarmas sonoras y sistemas de rastreo satelital lo que ayuda a la ubicación y la recuperación de los vehículos de manera ágil, pero estos dependen de la red móvil y sus costos de instalación son excesivos. [17], [18], [19].

En la actualidad, la tendencia se centra en soluciones inteligentes basadas en IoT, que incluye sensores especializados, microcontroladores y redes de comunicación de consumo reducido. Estas tecnologías permiten monitorear continuamente el vehículo y su estado, la generación de advertencias de tiempo real y una mayor autonomía operativa y abrir nuevas oportunidades para aplicaciones en áreas urbanas y rurales [20].

LoRa

Lora (Long Range) es una tecnología de radio modulación que permite la transmisión de datos a largas distancias con bajo consumo de energía. Usa una tecnología de espectro que se expande por Chirp (CSS), que es resistente a la interferencia, lo que permite que los dispositivos se comuniquen de manera efectiva en bandas de frecuencia sin restricciones, como 868 MHz o 915 MHz. Lora está diseñado para dispositivos IoT que deben transmitir regularmente cantidades mínimas de datos. Su ventaja es un bajo consumo de batería, lo que permite que los dispositivos funcionen durante años sin restaurarlos ni reemplazarlos [21].

LoRaWAN

LoRaWAN (red de área larga) es un protocolo de red basado en la tecnología LoRa, que establece los estándares de comunicación, la arquitectura, el control y la seguridad de los dispositivos en una red extensa. LoRaWAN posibilita la comunicación bidireccional entre los dispositivos finales (actuadores, sensores) y los servidores después de la puerta del enlace (gateways). Estas redes son perfectas para aplicaciones del Internet de las cosas (IoT) que necesitan una transmisión de radio reducida, un consumo energético bajo y cobertura en espacios extensos, como la vigilancia ambiental, el seguimiento de activos y los sistemas de seguridad [22].

Principios de Funcionamiento

Long Range (Lora) es una tecnología de modulación de espectro ensanchado que posibilita la realización de transmisiones a larga distancia, con un consumo energético reducido. LoRaWAN es un protocolo de red que permite la regulación y gestión del uso por parte de los dispositivos Lora a través de servidores y puertas de enlace.

Arquitectura de Red

LoRaWAN está compuesto por nodos finales, puertas de enlace y servidores de red. Estos datos se envían desde el nodo al gateway y después llegan al servidor, donde pueden ser gestionados o mostrados en plataformas o en la nube [23].

Ventajas frente a tecnologías celulares

LoRaWAN ofrece consumo energético bajo, largo alcance (15 km en zonas rurales), costos reducidos, y operación en bandas libres de licencia. Esto la hace no dependiente de operadores celulares, favoreciendo su uso en áreas rurales o de escasa cobertura [24].

Casos de Uso en Seguridad y Monitoreo

Se ha adoptado LoRaWAN en ciudades para la supervisión de contenedores de basura y de los niveles de ríos, así como para sistemas de seguridad como el monitoreo de vehículos y el control de acceso remoto. Esto es, por su característica de enviar alertas en tiempo real y su funcionamiento autónomo por años [25].

Comunicaciones Inalámbricas de Bajo Consumo

Las redes LPWAN (Red Amplia de Alta Potencia) se han creado con el propósito de transmitir grandes cantidades de datos a largas distancias, con un consumo bajo. Estas redes son perfectas para el IoT, ya que posibilitan que los aparatos operen durante años con baterías comunes [26].

Redes LPWAN y Comparación entre Sigfox, NB-IoT

Sigfox y NB-IoT compiten con LoRaWAN. Sigfox es muy eficiente energéticamente, pero tiene baja tasa de datos. NB-IoT presume de buena cobertura, aunque requiere una suscripción. LoRaWAN, por otro lado, es gratuito, escalable, tiene un largo alcance y tiene un buen equilibrio entre consumo y velocidad [27].

Características Técnicas de LoRaWAN

Frecuencia y modulación

LoRaWAN funciona en bandas ISM (Industrial, Científica y Médica) que no requieren licencia, como el 915 MHz en los Estados Unidos o el 868 MHz en Europa. Estas bandas posibilitan la creación de redes privadas sin requerir una concesión regulatoria, lo cual disminuye los costos y facilita la implementación en zonas con infraestructura escasa [28].

La modulación utilizada es CSS Chirp Spread Spectrum, que extiende la señal en el tiempo y la frecuencia en comparación con técnicas tradicionales como FSK o OOK, es más sensible a la recepción, más robusta a la interferencia y proporciona una mayor resistencia al ruido. Es la tecnología LoRaWAN la que permite a los dispositivos mantener conexiones constantes incluso en condiciones de señal débil, lo cual es importante en sistemas distribuidos complejos [11].

Además, LoRaWAN utiliza una relación de dispersión ajustable Spreading Factors (SF) para equilibrar el alcance y la velocidad de transmisión. Factor de propagación más alto (SF), mayor alcance, pero velocidad de transmisión de datos más baja, lo que permite ajustar el rendimiento de acuerdo con la ubicación y las dificultades del nodo [22]

Alcance y comportamiento en entornos edificados

Una de las propiedades más distintivas de LoRaWAN es la extensión de su cobertura, la cual fluctúa entre dos y quince kilómetros. Este rango está influido, entre otros factores, por las características del entorno construido, la configuración del relieve, la altitud de las estaciones de transmisión, las condiciones del medio de propagación y las variaciones meteorológicas del momento [29].

Los obstáculos habituales, como edificios, muros, arbolado denso o fuentes de interferencia electromagnética, no han impedido que LoRaWAN mantenga un nivel de fiabilidad elevado, particularmente en zonas que resultan complejas de alcanzar o en las que la cobertura de otras tecnologías tiende a degradarse. Esta característica lo hace especialmente útil para aplicaciones en vehículos, como dispositivos de seguimiento, donde la seguridad es primordial y los dispositivos probablemente se ubiquen dentro de garajes, estructuras metálicas, o en áreas residenciales con cobertura celular limitada.

La tecnología LoRa tiene la capacidad de propagar señales a través de entornos integrados, superando las capacidades de Wi-Fi, Zigbee e incluso acercándose a soluciones celulares, todo sin requerir ninguna infraestructura de operador. Este hecho permite la creación de redes auto-adaptativas que pueden soportar las condiciones físicas del entorno físico de despliegue.

Consumo energético

LoRaWAN, dependiendo del perfil de transmisión, el tipo de sensor y el modo de operación (clase A, B o C), permitirá a los dispositivos funcionar, con baterías convencionales, por tiempos de hasta diez años. LoRaWAN se presenta, así como una buena opción para dispositivos donde la eficiencia energética es un aspecto muy importante.

Esta autonomía es posible debido a las bajas velocidades de transmisión de datos, los ciclos de transmisión esporádicos y la capacidad de los nodos para permanecer en reposo la mayor parte del tiempo. En los usos de seguridad del vehículo, si los eventos en cuestión ocurren de manera irregular (movimiento, puertas, vibraciones), esta función permite la introducción de un sistema de alarma sin requerir mantenimiento frecuente o conexión a la red de energía de manera permanente. Además, el bajo consumo facilita el uso de fuentes de energía alternativas, como puede ser los paneles solares o baterías recargables.

Topología de red y escalabilidad

La topología de la red LoRaWAN es estelar y los nodos finales (es decir, los sensores y actuadores) se conectan directamente con una o más puertas de enlace, las cuales envían información al servidor de red para que esta sea procesada, almacenada o mostrada en plataformas en la nube.

Esta estructura proporciona una alta escalabilidad y reconoce miles de dispositivos distribuidos en un área geográfica amplia sin la necesidad de un punto de conexión de punto a punto o una ruta compleja. La comunicación entre los nodos y gateways es asíncrona y no coordinada. Reduce la complejidad del protocolo y permite que múltiples dispositivos compartan el canal sin una intervención significativa gracias al uso de varios canales y factores de dispersión.

En los sistemas de seguridad de vehículos, esta topología permite la instalación de sensores en múltiples vehículos o ubicaciones fijas, todos los cuales están conectados a través de puertas de enlace mínimas. Esto reduce costos y permite la expansión del sistema sin necesidad de reconfiguración estructural.

Sensores y dispositivos IoT aplicados a seguridad vehicular

La ingeniería de seguridad para automóviles basados en sistemas y tecnologías de vehicular IoT incluyen la configuración de dispositivos sensores y módulos tecnológicos que permiten la anticipación y la prevención de robos u otros eventos no deseados, así como la identificación de movimientos extraños o no intencionados. Tales dispositivos y sistemas se caracterizan por requerir poco o nada de consumo de energía, lo que los hace viables para su implementación en entornos infraestructurales complejos, y además, no necesitan una conexión celular para un funcionamiento óptimo.

Entre los componentes más utilizados se encuentran:

- **Sensores de movimiento (PIR o acelerómetros):** Cualquier tipo de vibración, impacto o movimiento repentino del vehículo es detectado, así como también se generan alertas por intentos de manipulación no autorizada o por intentos de remolcar el vehículo.
- **Módulos GPS:** Facilita la supervisión en tiempo real, lo cual resulta ventajoso para rastrear el automóvil en situaciones de robo o en desplazamientos no autorizados dentro de áreas restringidas.
- **Transceptores LoRa:** Los sensores de elevada sofisticación de Asign capturan datos y los transmiten por medio de protocolos inalámbricos hacia puertas de enlace situadas a distancias próximas, utilizando tecnologías de largo alcance, reducido consumo energético y simplicidad técnica.
- **Microcontroladores (como ESP32, STM32 o ESP32 WiFi LoRa):** Por prácticas profesionales. Gestionan el control, el procesamiento de eventos locales, así como el control simultáneo de comunicación con sensores y módulos de transmisión.

La adopción de estas tecnologías permite establecer sistemas distribuidos monitoreados con capacidades para generar alertas en tiempo real utilizando redes celulares comerciales. Mejora la autonomía operativa y reduce el costo de las conexiones, así como permite la implementación de soluciones para el país, áreas de estacionamiento cerradas o regiones con mala cobertura celular. Además, la modularidad de estos sistemas facilita su adaptación a diferentes tipos de vehículos (automóviles, motocicletas, flotas) y múltiples escenarios de la ciudad, lo que le permite escalar una solución de acuerdo con las necesidades climáticas.

Modelos de Propagación de Señal

Para estimar la cobertura y el rendimiento de la señal LoRaWAN en varios entornos, se utilizan los modelos de propagación como log-normal, Okumura-Hata y COST231 que se emplean en telemática. Estos modelos tienen en cuenta la frecuencia, la distancia, la altura de las antenas y la presencia de obstrucciones, lo que permite predecir el rendimiento del sistema en escenarios urbanos densos o rurales abiertos, y posicionar de manera eficiente las puertas de enlace y los nodos.

Contexto geográfico y tecnológico del barrio Santa Ana

Los retos que presenta el barrio Santa Ana de la parroquia Licán en el cantón Riobamba incluyen una mezcla en la tipología de vías, viviendas y el área geográfica, donde, los caminos de asfalto, tierra y adoquín, las edificaciones de las viviendas de diferentes tipos de materiales, su abundante vegetación limita a una buena señal telefónica. Estas zonas junto con la tecnología que sea dependiente de redes de telefonía móvil, como el GPS, presentan grandes dificultades. Sin embargo, LoRaWAN presenta una solución en sistemas de monitoreo y alerta vehicular, proporcionando la posibilidad de ser autónomo, de bajo consumo energético y de rango extenso, adaptándose de mejor forma a la infraestructura antes mencionada.

Arduino

Arduino es la plataforma de desarrollo de código abierto, tanto en hardware como en software, que actúa como el entorno principal para la creación del sistema. En este proyecto, funciona como la herramienta que permite programar el microcontrolador ESP32 y gestionar la comunicación con todos los periféricos, como los sensores de movimiento, la cámara y el módulo de radio LoRa [30].



Figura 2. Arduino IDE con Esp32 [31]

Desde el punto de vista del desarrollo, se define por los siguientes elementos:

- **Entorno de Programación:** Utiliza un lenguaje basado en C++ que simplifica la interacción con el hardware, permitiendo que procesos complejos como el rastreo GPS o la detección de impactos se traduzcan en instrucciones lógicas claras.
- **Estructura del Código:** El software se organiza mediante una arquitectura secuencial dividida en una fase de configuración inicial y un ciclo de ejecución constante, lo que garantiza que el vehículo sea monitoreado en tiempo real sin interrupciones.
- **Modularidad:** Permite la integración de librerías externas que sirven para controlar dispositivos específicos, facilitando que el sistema pueda procesar datos de múltiples sensores simultáneamente y enviar alertas de forma automática.

Lógica de procesamiento y detección de eventos

El proceso de monitoreo y detección de intrusión ejecutado por el sistema de seguridad basado en el microcontrolador ESP32 sigue una estructura lógica compuesta por varias etapas fundamentales:

- **Adquisición de datos sensoriales:** Obtención de señales físicas mediante el escaneo constante de dispositivos BLE para verificar la presencia del dueño y la lectura de sensores IMU, PIR, ToF y Radar RCWL.
- **Filtrado y Procesamiento:** Toma la información cruda de los sensores y realiza una conversión digital para su análisis. En esta fase se aplica un filtro exponencial para suavizar el ruido del acelerómetro y se calculan los promedios de calibración para garantizar la precisión de las mediciones.

- **Evaluación de Intrusión:** Identificación de patrones específicos que superan los umbrales de seguridad establecidos. El sistema analiza la magnitud del movimiento en el plano XY para distinguir entre vibraciones leves e impactos fuertes.
- **Clasificación de Estados:** En esta fase se asigna una etiqueta o "modo" al sistema según los patrones detectados, permitiendo asociar la actividad sensorial a una categoría específica:
 - **MODE_IDLE (Estacionado):** Estado de reposo o sistema desarmado al detectar el teléfono del dueño.
 - **MODE_ALERT (Intrusión):** Activado cuando los sensores de proximidad y movimiento confirman una amenaza.
 - **MODE_MOVING (En movimiento):** Activado mediante la validación de coordenadas GPS cuando el vehículo se desplaza.

Cada vez que se detecta una nueva perturbación, esta es clasificada para extraer sus características principales (como la distancia del intruso o la duración del impacto) y compararlas con los parámetros de seguridad predefinidos. En cuanto se halla una coincidencia significativa entre la lectura de los sensores y la lógica de intrusión, se dispara una acción de respuesta, como la captura de una imagen mediante la ESP32-CAM y el envío de alertas por el protocolo LoRa [32], [33].

A continuación, en la Figura 3 se detallan las etapas para el procesamiento de alertas y el reconocimiento de estados en el sistema.

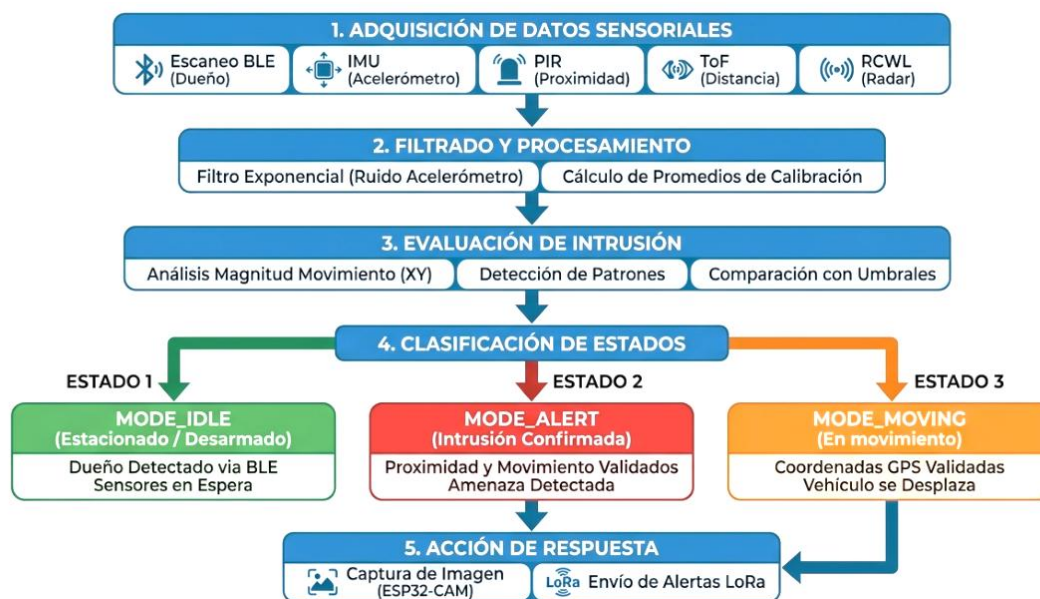


Figura 3. Proceso de Monitoreo y Detección de Intrusión

¿Para qué sirve un algoritmo en el sistema de seguridad?

En el contexto de este sistema de seguridad vehicular, un algoritmo sirve para ejecutar tareas críticas de monitoreo, tomar decisiones automáticas ante una posible intrusión y resolver problemas de detección mediante una secuencia lógica y estructurada. Este enfoque permite

que el microcontrolador ESP32 transforme las señales eléctricas analógicas y digitales de los sensores en respuestas inteligentes, como el envío de una alerta o la captura de una fotografía.

Además, los algoritmos actúan como el núcleo del software, permitiendo que procesos complejos como el cálculo de la distancia geográfica mediante GPS o el filtrado de ruido en el acelerómetro IMU los cuales se ejecutaron de manera eficiente y controlada. Al ser un conjunto de instrucciones independientes del lenguaje, la lógica desarrollada para la detección de vibraciones o presencia puede ser adaptada o escalada a diferentes plataformas de hardware dentro del ecosistema de Internet de las Cosas (IoT)[34].

En consecuencia, el firmware cargado en el transmisor y el receptor no es más que una secuencia organizada de algoritmos (como el de calibración, el de evaluación de intrusión y el de comunicación LoRa) codificados en lenguaje C++ bajo el entorno de desarrollo IDE de Arduino para ser ejecutados en tiempo real por el sistema informático embebido[30], [34], [35].

Características de los algoritmos

Los algoritmos implementados en la placa Heltec ESP32 poseen características fundamentales que garantizan el monitoreo vehicular en tiempo real. Como se observa en la Figura 4, estas instrucciones permiten traducir la captura de datos de sensores en acciones de seguridad:

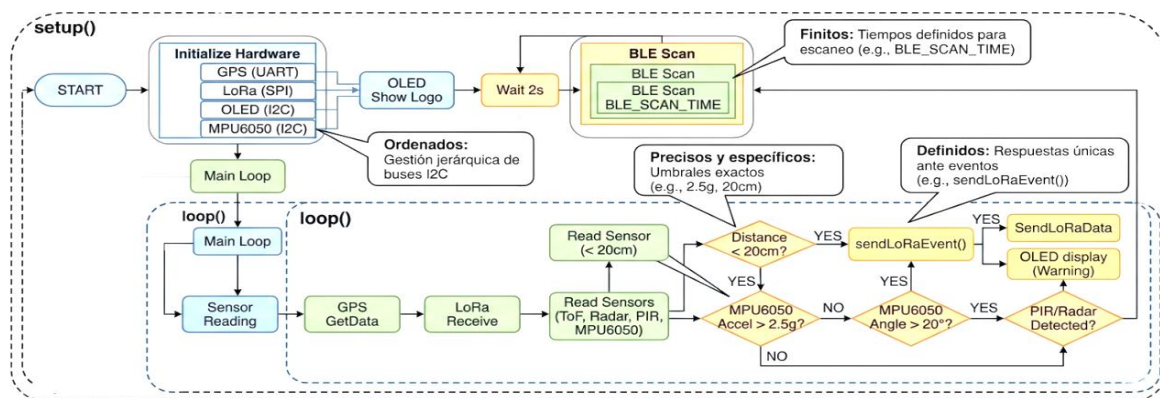


Figura 4. Diagrama del algoritmo adaptado del sistema de seguridad vehicular

Partes que componen el algoritmo de seguridad

El algoritmo desarrollado para el sistema antirrobo posee una estructura general que organiza su funcionamiento interno en tres etapas fundamentales, como se muestra en la Figura 5. Esta estructura técnica permite normalizar el procesamiento de datos, facilitando su ejecución eficiente en el microcontrolador ESP32 y garantizando una respuesta inmediata ante eventos de riesgo.

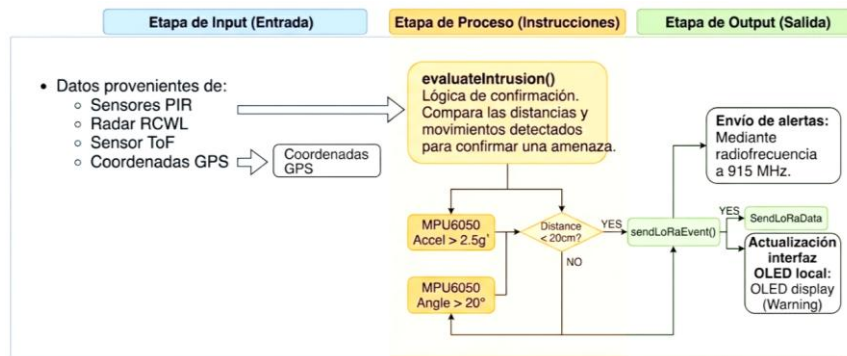


Figura 5. Diagrama de partes que componen el algoritmo de seguridad

Casos de uso de la seguridad y monitoreo en diversas industrias

La detección de eventos y objetos, integrada en sistemas embebidos, se ha aplicado en diversas industrias con desafíos únicos de precisión y velocidad. En el contexto de este proyecto, el sistema evalúa la capacidad de respuesta bajo condiciones variables del entorno vehicular mediante el uso de hardware especializado[36].

- **Sector Seguridad:** Es el pilar de este desarrollo. El uso de la ESP32-CAM permite la captura de evidencia visual ante intrusiones, mientras que sensores como el PIR y el Radar RCWL monitorean la presencia humana y el movimiento incluso a través de materiales como el plástico [37].
- **Industria Automotriz:** Además de la navegación, la seguridad activa utiliza sensores IMU para detectar impactos o vibraciones anómalas en el chasis, permitiendo que procesos complejos se traduzcan en instrucciones lógicas que disparan alertas inmediatas [38].
- **Logística y Rastreo:** El seguimiento mediante GPS permite la localización de activos en tiempo real, utilizando algoritmos que discriminan si el desplazamiento es suficiente para emitir una alerta de seguimiento, optimizando así el uso de la red.
-

Tecnologías y protocolos para la detección de eventos

A diferencia de los modelos de aprendizaje profundo que requieren alto poder computacional, los sistemas basados en microcontroladores como el ESP32 utilizan algoritmos optimizados para el procesamiento en tiempo real y comunicación de bajo consumo.

- **Lógica de Intrusión Multimodal:** El sistema utiliza una combinación de estados: si el sensor ToF detecta cercanía extrema, el PIR presencia y el IMU vibración simultánea, el algoritmo confirma una amenaza. Este enfoque garantiza alta precisión sin la necesidad de procesar redes neuronales pesadas.
- **Comunicación LoRa (Long Range):** Para asegurar que la detección llegue al receptor, se utiliza el protocolo LoRa a 915 MHz. Esta tecnología permite enviar el estado del vehículo y el ID de la fotografía capturada a grandes distancias, manteniendo una alta inmunidad al ruido y un consumo energético eficiente.

- **Gestión de Evidencia Fotográfica:** El sistema implementa una arquitectura modular donde el nodo principal gestiona la captura mediante comandos seriales. La imagen se procesa y almacena en una memoria no volátil, asegurando que la evidencia física del evento se conserve incluso ante interrupciones de energía.

Comparación de métodos de detección en sistemas embebidos

En el diseño del sistema de seguridad, la eficacia de la detección de amenazas se fundamenta en la fusión sensorial. A diferencia de los métodos de visión por computadora que requieren un alto consumo de recursos, este sistema utiliza una jerarquía de sensores lógicos para garantizar una respuesta en tiempo real con bajo consumo energético.

Tabla 1. Comparativa de los métodos de detección implementados en el transmisor

Método	Sensor	Variable Crítica	Fortaleza Técnica
Infrarrojo Pasivo	PIR	Radiación térmica	Alta eficiencia en la detección de presencia humana.
Microondas	Radar RCWL	Efecto Doppler	Capacidad de detección no invasiva a través de materiales.
Tiempo de Vuelo	ToF (VL53L1X)	Distancia láser	Precisión milimétrica para confirmar proximidad extrema.
Acelerometría	IMU (LSM5D3)	Gravedad (g)	Detección física de impactos o intentos de remolque.

METODOLOGÍA

En este apartado se detallan los aspectos metodológicos correspondientes al desarrollo del proyecto de investigación, los cuales fueron fundamentales para el diseño, integración y validación del sistema de seguridad vehicular.

TIPO DE INVESTIGACIÓN

Para este proyecto se optó por un diseño de investigación experimental con un enfoque mixto, el cual integra métodos cuantitativos y cualitativos esenciales para la implementación del ecosistema de seguridad propuesto.

- **Enfoque Cuantitativo:** Se aplicó en la recolección y análisis de datos técnicos provenientes de los sensores. Esto incluyó la calibración del sensor IMU mediante un filtro exponencial (ALPHA 0.6), la medición de distancias precisas con tecnología ToF y la verificación de la potencia de señal LoRa (RSSI/SNR) para garantizar la cobertura de las alertas.
- **Enfoque Cualitativo:** Se centró en la evaluación de la arquitectura del sistema, analizando la eficiencia de la comunicación entre el Transmisor (ESP32-S3) y el Receptor, así como la pertinencia de las notificaciones enviadas vía Telegram para la experiencia del usuario final.

DISEÑO DE INVESTIGACIÓN

El proyecto de investigación posee cuatro fases como base principal como se muestra en la Figura 6

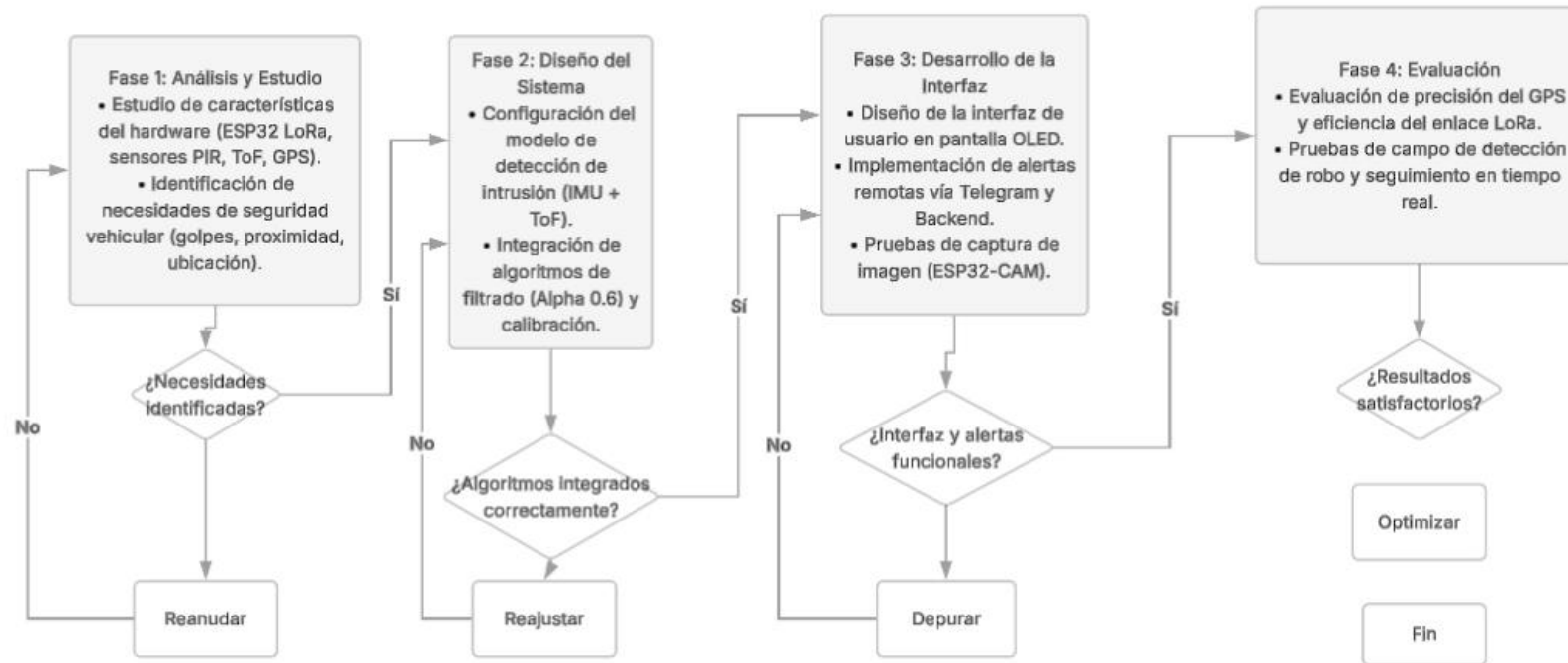


Figura 6. Diseño de la investigación

Fase 1: Análisis y estudio

En esta primera etapa, se llevó a cabo un análisis profundo de las vulnerabilidades de seguridad en vehículos livianos, identificando la necesidad de un sistema de monitoreo que no dependa de redes celulares convencionales. Se estudiaron las capacidades del procesador ESP32-S3 y la tecnología LoRa para garantizar la transmisión de alertas en zonas de baja cobertura, orientándose a la protección integral del activo.

Fase 2: Diseño del sistema

En esta fase, se realizó la selección e integración de una arquitectura multimodal de sensores (PIR, Radar RCWL, ToF e IMU). El algoritmo de decisión se diseñó para filtrar falsas alarmas mediante el uso de filtros digitales exponenciales y umbrales de aceleración específicos (SHOCK_THRESHOLD). Durante el desarrollo se consideró como objetivo principal la detección temprana de intrusiones y la precisión en la geolocalización mediante GPS. Se priorizó un diseño de bajo consumo energético mediante la gestión de la alimentación externa (Vext) y modos de reposo del módulo de radio.

Fase 3: Desarrollo de la interfaz

En la tercera etapa, se diseñaron dos interfaces de interacción:

- **Interfaz Local:** Una pantalla OLED que muestra en tiempo real el estado de los sensores, coordenadas y el conteo de evidencia fotográfica.
- **Interfaz Remota:** Un bot de Telegram que permite al usuario recibir notificaciones inmediatas con enlaces directos a Google Maps y visualización de estados críticos (MODE_ALERT). Se desarrollaron funciones para el seguimiento en tiempo real (Tracking) cuando el vehículo detecta movimiento no autorizado.

Fase 4: Evaluación

Para validar la efectividad del sistema, se realizaron pruebas de campo enfocadas en la distancia de transmisión LoRa a 915 MHz y la precisión del sensor de distancia láser. Se evaluó la velocidad de respuesta desde el momento del impacto detectado por el IMU hasta la recepción del mensaje en el dispositivo móvil. La evaluación permitió determinar que el sistema cumple con los criterios de robustez y fiabilidad necesarios para la seguridad vehicular.

TÉCNICAS DE RECOLECCIÓN DE DATOS

Fuentes de investigación

En el desarrollo del proyecto, se tomó en consideración una revisión exhaustiva de la literatura para la recolección de información importante en diversas bases de datos científicas y bibliotecas digitales como se muestra en la Figura 7:

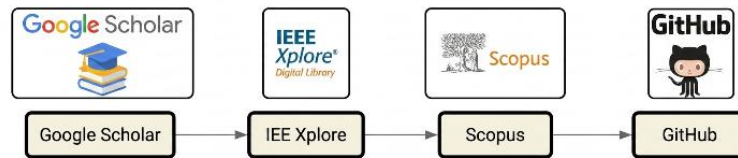


Figura 7. Fuentes de Investigación

En las bases de datos mencionadas, se llevó a cabo una búsqueda, evaluación y análisis de estudios relacionados con la seguridad vehicular inteligente, el internet de las cosas (IoT) aplicado a la protección de activos y las comunicaciones de largo alcance. Las temáticas clave extraídas de estas fuentes para el desarrollo de la investigación son:

- **Sistemas Embebidos:** Documentación técnica de Heltec Automation para el uso del procesador ESP32-S3 y el chip SX1262 LoRa, fundamentales para el control del hardware.
- **Sensores de Proximidad y Movimiento:** Estudios sobre tecnología ToF (Time of Flight) con el sensor VL53L1X y sensores de microondas RCWL-0516 para la detección precisa de intrusos.
- **Protocolos de Comunicación:** Análisis de redes de bajo consumo y largo alcance (LoRa) y protocolos de corto alcance (BLE) para la validación de cercanía del propietario.
- **Geolocalización:** Implementación de protocolos NMEA y librerías TinyGPS++ para el rastreo y envío de coordenadas geográficas en tiempo real.
- **Visión Computarizada:** Técnicas de captura y almacenamiento de imágenes en formato JPEG mediante el módulo ESP32-CAM para el registro visual de eventos de alerta.

A través de este análisis, se logró fundamentar la selección de los componentes y algoritmos de filtrado necesarios para garantizar la fiabilidad del sistema antirrobo propuesto.

POBLACIÓN DE ESTUDIO Y TAMAÑO DE MUESTRA

Población

La investigación se centró en un prototipo experimental integrado en un vehículo de prueba. Por lo tanto, la población no se define por una cantidad de vehículos, sino por el universo de eventos de seguridad y ciclos operativos (intentos de intrusión, impactos y desplazamientos) a los que el sistema puede ser sometido durante su vida útil.

La recolección de datos se realizó en dos fases:

- **Fase 1:** Sin el sistema implementado, observando la vulnerabilidad y la ausencia de alertas remotas ante estímulos externos.

- **Fase 2:** Con el sistema basado en ESP32-LoRa activo, registrando la capacidad de respuesta, captura de imágenes y envío de coordenadas ante los mismos estímulos.

De esta forma, se analizó la eficacia en la detección y comunicación de alertas mediante una comparativa de estados. En la Tabla 2 se presenta la distribución técnica de las pruebas experimentales realizadas.

Tabla 2. Diseño de Población

Escenario de Prueba	Impactos (IMU)	Intrusión (PIR/ToF)	Rastreo (GPS/LoRa)	Total
Nº de Ensayos	18	16	16	50

Muestra

En la presente investigación se recopilamos un total de 50 datos correspondientes a la variable “Eficacia de Alerta”. Esta variable es de tipo cualitativa dicotómica, donde se registra si el sistema cumplió con el ciclo completo: detección, procesamiento y envío de alerta (Éxito = 1, Fallo = 0).

Dado que el experimento busca validar la robustez técnica del prototipo, se utilizó un modelo de Distribución Binomial para determinar la confiabilidad del sistema, utilizando la Ecuación 1:

$$P(x) = \binom{n}{x} \cdot p^x \cdot q^{n-x}$$

Ecuación 1. Ecuación de método Binomial

En donde:

N = Número total de ensayos (50).

X = Número de éxitos observados (alertas enviadas correctamente).

P = Probabilidad de éxito estimada (basada en los umbrales de precisión como SHOCK_THRESHOLD).

q = Probabilidad de fallo (1-p).

A diferencia de pruebas preliminares, el tamaño de la muestra de $n = 50$ permite alcanzar la convergencia estadística bajo el Teorema del Límite Central, otorgando una base sólida para la inferencia de resultados con un nivel de confianza del 95%. Esta cantidad es suficiente para validar la repetibilidad y fiabilidad del hardware, asegurando que los algoritmos de filtrado de las librerías *TinyGPS++* y el procesamiento del sensor *MPU6050* operan con precisión, minimizando los falsos positivos y garantizando una respuesta estable ante variables del entorno real.

OPERACIONALIZACIÓN DE LAS VARIABLES

En la Tabla 3 se detallan las variables que intervienen en el funcionamiento del sistema antirrobo. Se han clasificado según su rol dentro del experimento para medir cómo la entrada de los sensores afecta la respuesta de alerta.

Tabla 3: Operacionalización de variables del Sistema Antirrobo.

Variable	Tipo	Definición Operacional	Indicador / Sensor
Detección de Intrusión	Independiente	Identificación de presencia en el perímetro cercano al vehículo (450-600 mm).	PIR, RCWL y ToF
Intensidad de Impacto	Independiente	Nivel de aceleración detectado que supera el umbral de seguridad (> 3.0g).	Sensor IMU (LSM6DS3)
Eficacia de Alerta	Dependiente	Éxito en el ciclo: Detección, Procesamiento, Notificación Telegram.	Binomial (Éxito/Fallo)
Precisión de Rastreo	Dependiente	Margen de error en metros de la ubicación enviada respecto a la real.	GPS (Protocolo NMEA)
Presencia del Propietario	Moderadora	Validación de cercanía del dueño para armar o desarmar el sistema.	Bluetooth Low Energy (BLE)

MÉTODOS DE ANÁLISIS Y PROCESAMIENTO DE DATOS

Revolucionando la seguridad vehicular mediante IoT

En la actualidad, la protección de bienes móviles resulta esencial para mejorar la seguridad ciudadana y reducir las pérdidas económicas por robo de vehículos. Las tecnologías de próxima generación, específicamente el Internet de las Cosas (IoT), están transformando la seguridad vehicular, permitiendo una vigilancia constante, una detección de intrusiones más precisa y, en última instancia, una respuesta inmediata ante actos delictivos.

Los beneficios de implementar sistemas basados en nodos sensores se reflejan en la capacidad de monitoreo remoto en tiempo real, lo que reduce los tiempos de reacción del propietario y aumenta las probabilidades de recuperación del vehículo mediante geolocalización.

Soluciones tecnológicas para la prevención de robos

La gestión de alertas en tiempo real es crucial para garantizar una experiencia de seguridad efectiva para el usuario. La implementación de soluciones inteligentes mediante hardware embebido permite cumplir con protocolos de vigilancia de manera más autónoma.

Una de las soluciones más innovadoras aplicadas en este proyecto consiste en el despliegue de una red de sensores (PIR, Radar y ToF) que monitorean el perímetro del

vehículo. Estos dispositivos envían información procesada a un sistema central (ESP32), el cual transmite alertas mediante tecnología de largo alcance (LoRa) hacia un receptor y, posteriormente, a una interfaz de usuario en Telegram, ofreciendo datos precisos sobre la naturaleza de la amenaza.

Las nuevas tecnologías aplicadas a este sistema antirrobo incluyen las siguientes características:

- **Sistemas de alerta automatizados:** Estos sistemas autónomos eliminan la dependencia de alarmas sonoras tradicionales que suelen ser ignoradas. En su lugar, notifican directamente al propietario, maximizando la efectividad de la vigilancia especialmente en zonas con baja cobertura celular gracias al uso de LoRa.
- **Lógica de detección basada en umbrales:** El uso de algoritmos que discriminan entre ruidos ambientales y amenazas reales (mediante variables como SHOCK_THRESHOLD y VIB_TIME) logra predecir eventos críticos y sugerir acciones de seguimiento, asegurando un uso eficiente de la energía y los datos.
- **IoT en la seguridad vehicular:** Esta tecnología permite una conectividad continua y comunicación en tiempo real. Los dispositivos IoT tienen la capacidad de rastrear la ubicación exacta mediante GPS y capturar evidencia visual a través de cámaras integradas (ESP32-CAM), enviando estos paquetes de datos de forma inalámbrica para que el usuario pueda tomar decisiones informadas desde cualquier lugar.
- **Plataformas de monitoreo remoto:** El avance tecnológico ha permitido utilizar aplicaciones de mensajería instantánea y mapas web (GitHub Pages) para visualizar la ruta del vehículo en tiempo real en caso de desplazamiento no autorizado.

Gracias al desarrollo de la tecnología de baja potencia y largo alcance, la protección de vehículos se ha vuelto un problema superable, contribuyendo a la tranquilidad de los propietarios. La reducción de la vulnerabilidad vehicular ha sido resuelta satisfactoriamente gracias a estos sistemas de monitoreo en tiempo real, demostrando ser la mejor solución técnica frente a los métodos de seguridad convencionales.

La incorporación de sistemas inteligentes de vigilancia en vehículos particulares, flotas comerciales y zonas de parqueo residencial ha generado beneficios significativos en la reducción de delitos, como se muestra en la Figura 11.

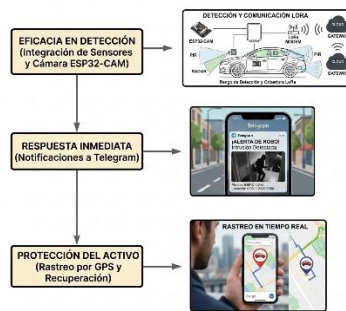


Figura 8. Sistema Antirrobo

En la Tabla 4 se presentan las principales características, problemas de seguridad actuales y las oportunidades de mejora técnica que justifican el desarrollo del sistema basado en ESP32 y LoRa para la satisfacción y tranquilidad del usuario.

Tabla 4. Tabla comparativa de la problemática de seguridad vehicular.

Característica Principal	Problemas Comunes	Oportunidades de Mejora
Detección de Intrusos	Alarmas convencionales ruidosas que son ignoradas por transeúntes.	• Notificación silenciosa y directa al propietario vía Telegram. • Uso de sensores de precisión (ToF/PIR).
Monitoreo en Tiempo Real	Dependencia de cámaras fijas que no cubren el interior o puntos ciegos.	• Captura de imágenes desde el interior del vehículo (ESP32-CAM) y envío inmediato.
Cobertura de Señal	Pérdida de comunicación en sótanos o zonas con baja cobertura celular.	• Uso de tecnología LoRa de largo alcance (915 MHz) para transmisión sin depender de red móvil.
Identificación del Dueño	Necesidad de llaves físicas o controles remotos vulnerables a clonación.	• Reconocimiento automático mediante Bluetooth Low Energy (BLE) para armado/desarmado.
Rastreo Post-Robo	Sistemas GPS tradicionales que pueden ser desactivados fácilmente.	• Seguimiento dinámico con actualización constante de coordenadas en mapas web.
Resiliencia Energética	Alto consumo de batería que descarga el vehículo en reposo.	• Optimización de energía mediante modos <i>Sleep</i> y encendido por eventos (IMU).

A partir de la problemática expuesta, se evidenció que los sistemas de seguridad vehicular convencionales carecen de inteligencia visual, por lo que el sistema propuesto constituye una solución eficaz para automatizar la vigilancia y garantizar que el propietario reciba evidencia clara del evento en tiempo real.

Estudio de Algoritmos para el Procesamiento y Detección de Eventos

A diferencia de los sistemas de vigilancia basados en visión artificial pesada, este proyecto se centra en el procesamiento eficiente de señales provenientes de múltiples nodos sensores. Se han implementado algoritmos de filtrado y umbrales de decisión para garantizar que el sistema responda ante amenazas reales y minimice los falsos positivos.

En la Tabla 5 se presentan las características de los sensores integrados y cómo su lógica de procesamiento se ajusta a los recursos limitados del ESP32, asegurando una latencia baja en el envío de alertas vía LoRa.

Tabla 5. Especificaciones de procesamiento de los sensores del Sistema Antirrobo.

Sensor / Módulo	Variable de Entrada	Método de Procesamiento	Latencia de Respuesta	Requisito de Hardware
IMU (LSM6DS3)	Aceleración (g)	Filtro Exponencial ($\alpha = 0.6$) y Umbral de Choque	< 10 ms	Bajo (Buses I2C)
ToF (VL53L1X)	Distancia (mm)	Medición Láser de precisión (Rango 4-60 cm)	20 - 50 ms	Bajo
GPS (TinyGPS++)	Coordenadas	Decodificación de sentencias NMEA y filtro de distancia	1 - 2 segundos	Medio (UART)
LoRa (915 MHz)	Datos JSON	Modulación por espectro ensanchado (SF12)	100 - 300 ms	Medio (SPI)

Como una solución óptima para escenarios donde la eficiencia energética es primordial, el uso de filtros exponenciales en el acelerómetro permite una ejecución altamente eficiente. Esto evita que vibraciones ambientales activen el sistema, consolidando una opción robusta frente a alarmas convencionales.

Por otro lado, la lógica de Detección Multimodal (usando PIR, Radar y ToF simultáneamente) permite que el sistema ignore objetos en movimiento lejano y solo se active cuando la intrusión es confirmada por al menos dos sensores. Esto posiciona al prototipo como una alternativa superior en precisión frente a sensores de proximidad simples que no poseen discriminación de distancia.

Finalmente, la integración de la librería TinyGPS++ permite que el procesamiento de la ubicación no sature el procesador, filtrando únicamente los cambios de posición mayores a 3 metros (TRACK_MIN_DISTANCE_M). Esto asegura que la transmisión por LoRa solo ocurra cuando hay un desplazamiento real del vehículo, optimizando el ancho de banda y el consumo de batería.

Arquitectura de Procesamiento y Comunicación LoRa

Gracias a su estructura híbrida, la eficiencia en la gestión de eventos de seguridad ha hecho posible que el sistema basado en el microcontrolador ESP32 tenga una alta fiabilidad, ya que combina la adquisición de datos multimodales con el protocolo de comunicación LoRa (Long Range), optimizando así la detección y el envío de alertas a larga distancia.

Etapas de Procesamiento en el ESP32:

El firmware fue desarrollado con el propósito de optimizar la eficiencia en sistemas embebidos de bajo consumo, logrando una reducción en la latencia de respuesta y una gestión inteligente de la energía sin comprometer la sensibilidad del sistema. Esto se logra mediante la implementación de dos técnicas clave:

- **Filtrado Digital de Señales (Filtro Exponencial):** A diferencia de las lecturas analógicas crudas que pueden presentar ruido, el sistema aplica un filtro exponencial ($\alpha = 0.6$) de forma independiente a cada eje del acelerómetro. Esto genera un flujo de datos suavizado que reduce drásticamente los falsos positivos en comparación con una lectura estándar, permitiendo que el sistema ignore vibraciones ambientales leves.
- **Lógica de Umbrales Dinámicos (Thresholding):** Esta técnica trabaja exclusivamente con los valores críticos de cada sensor. Permite que el sistema se mantenga en un estado de bajo consumo hasta que un parámetro (como el SHOCK_THRESHOLD de 3.0g o una distancia ToF inferior a 600mm) supere el rango de seguridad. El uso principal de este modelo es asegurar que el hardware solo se active ante eventos de intrusión confirmados.

Etapas del Protocolo LoRa: Transmisión y Alcance

Las alertas generadas por este modelo se basan en un enfoque de modulación por espectro ensanchado y en el uso de una arquitectura Gateway-Cliente, la cual se integra a la red para mejorar su efectividad.

- **Etapas de Empaquetamiento de Datos (JSON):** La arquitectura del software se basa en la generación de paquetes de datos ligeros. Seguidamente, se estructuran en formato JSON, lo que reduce el tamaño del mensaje y aumenta la velocidad de transmisión. La detección se realiza en múltiples etapas, identificando si el evento es un impacto, una intrusión por proximidad o un desplazamiento geográfico.
- **Etapas de Comunicación (Spread Spectrum):** LoRa emplea una técnica de modulación que le permite cubrir una alta gama de distancias incluso en entornos urbanos densos. El modelo predice y envía dos elementos principales: el Tipo de Alerta (intrusión/choque) y las Coordenadas GPS mediante el protocolo NMEA.
- **Fusión de Eventos y Priorización:** Tras generar diferentes detecciones, el sistema aplica un algoritmo de prioridad que selecciona la alerta más crítica (por

ejemplo, un robo en curso detectado por GPS) y descarta lecturas redundantes de sensores secundarios. Este proceso optimiza significativamente la autonomía de la batería y la precisión de la notificación que llega al usuario vía Telegram, como se muestra en la Figura 12.

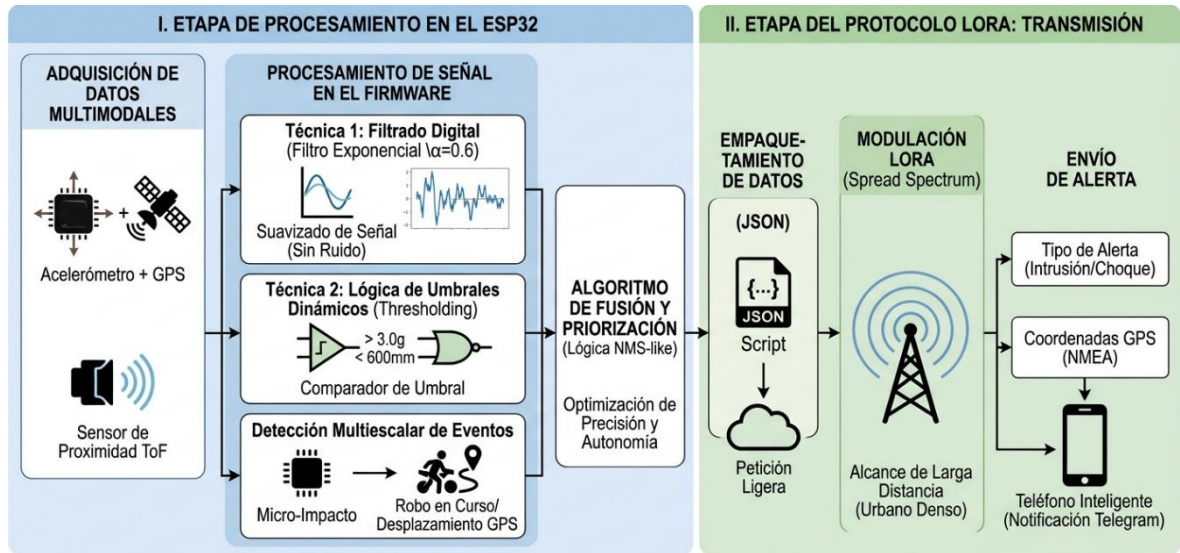


Figura 9. Arquitectura de Procesamiento y Comunicación

El proceso de detección eficaz mediante la arquitectura del sistema empieza con la adquisición de señales crudas de los sensores a una tasa de muestreo definida por el reloj interno del ESP32. Una vez completado este proceso, los datos se envían a los algoritmos de filtrado, donde se extraen las características críticas a través de umbrales de decisión para detectar diferentes tipos de eventos (impactos o intrusiones) en el entorno del vehículo.

Estas funciones de filtrado facilitan la identificación más eficiente de amenazas reales, contribuyendo a una mejor autonomía del sistema. Finalmente, durante el procesamiento, el algoritmo elimina ruidos redundantes o señales parásitas para mejorar su precisión al reportar un evento crítico a través de la red LoRa [31].

En la Figura 10 se muestra el diagrama de bloques funcionales de la arquitectura de comunicación y procesamiento del sistema.

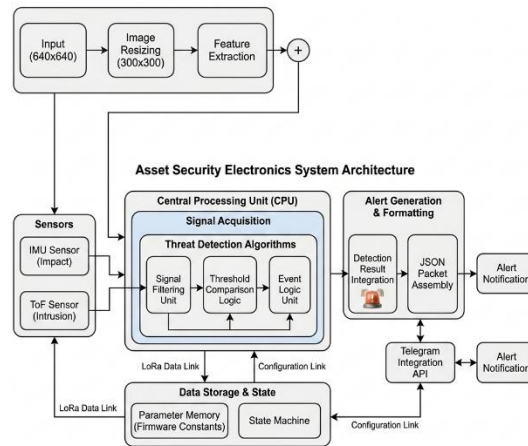


Figura 10. Diagrama de Bloques funcionales del sistema de seguridad

Implementación de la Lógica de Detección y Gestión de Alertas

La técnica de procesamiento de señales para optimizar la seguridad vehicular, acompañada de la arquitectura del microcontrolador ESP32, presenta una solución escalable y eficiente para gestionar adecuadamente la protección del activo mediante monitoreo de sensores en tiempo real. Este enfoque ofrece múltiples beneficios para la integridad del vehículo y la tranquilidad del usuario.

El proceso de la implementación se basa en la integración de librerías especializadas como TinyGPS++ para el manejo de ubicación, y las bibliotecas de comunicación para el módulo LoRa y la cámara ESP32-CAM.

Posteriormente, se procede con la configuración del firmware; este proceso es primordial ya que permite establecer los parámetros de calibración y los umbrales de sensibilidad, los cuales definen la capacidad de respuesta de la red de sensores y los comportamientos aprendidos durante las pruebas de campo.

Una vez configurado el sistema, cada señal capturada por los sensores debe ser preprocesada antes de activar una alerta. Este preprocesamiento se realiza a través de funciones lógicas en el código que ejecutan las siguientes operaciones:

- **Filtrado Digital:** Se procesan las lecturas del acelerómetro mediante un filtro exponencial ($\alpha = 0.6$) para suavizar la señal y eliminar ruidos parásitos.
- **Sustracción de Ruido Ambiental:** Se establecen valores promedio de reposo. Este proceso ayuda a que el modelo sea menos sensible a variaciones externas como el viento o vibraciones por tráfico cercano, mejorando la convergencia de la detección.
- **Normalización de Rangos:** Los datos de los sensores (distancia en mm o aceleración en g) se escalan dentro de rangos operativos para garantizar una correcta interpretación digital.

Una vez realizado el preprocesamiento, los datos pasan a través de la unidad de decisión del sistema. Este proceso realiza la inferencia del evento, generando así una notificación

de alerta. Cada detección incluye típicamente: tipo de sensor activado, nivel de intensidad del evento y coordenadas geográficas.

Para la administración de la seguridad, se definen Zonas de Monitoreo Crítico (basadas en sensores PIR y ToF). Cuando se hace la detección de un objeto dentro de estas zonas, el vehículo se marcará en estado de "Alerta de Intrusión". De manera inversa, si el sistema reconoce al dueño mediante la señal BLE, el vehículo se marcará como "Seguro/Desarmado".

A partir de las detecciones, se implementa una funcionalidad que registra el tiempo de respuesta, es decir, el lapso desde que ocurre el evento de seguridad hasta que la notificación llega al dispositivo móvil del usuario, con el fin de optimizar la eficacia del sistema. Adicionalmente, se configuró un bot de Telegram destinado a guiar al conductor con la ubicación exacta en caso de desplazamiento.

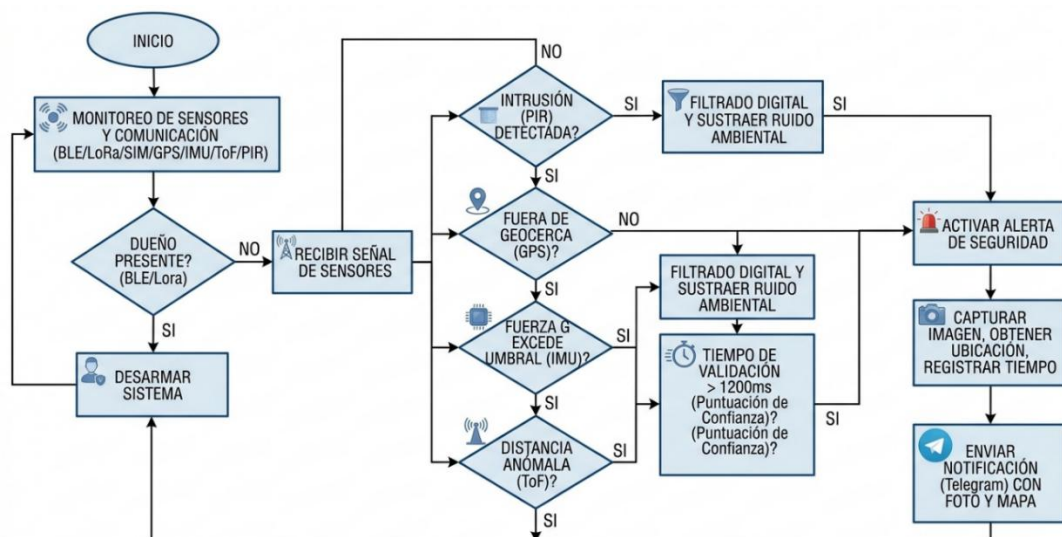


Figura 11. Diagrama de flujo de detección de eventos y envío de alertas

En la Figura 11 se muestra el diagrama de flujo para la detección de eventos y el envío de alertas.

Para el desarrollo del código del sistema antirrobo se consideraron diversos parámetros orientados a mejorar la eficiencia:

- **Puntuación de Confianza (Validación Temporal):** Para que el sistema sea confiable, se configuró un tiempo de validación sostenida (VIB_TIME = 1200ms) antes de determinar una alerta real. Esto se logra mediante la siguiente lógica de código:

```
if (vibration_duration > 1200 && shock_g > 3.0)
```

Arquitectura y Lógica de Programación del Prototipo

El desarrollo del software se realizó en el entorno de Arduino IDE, empleando una estructura de programación modular para garantizar la eficiencia en el procesamiento de

datos provenientes de la red de sensores. A continuación, se describen los fragmentos de código que constituyen la lógica central del sistema:

A. Gestión de Umbrales y Calibración de Sensores

Para mitigar la presencia de falsos positivos, se definieron umbrales críticos de activación. Estos valores permiten al procesador discriminar entre ruidos ambientales y eventos de seguridad reales.

cpp

- *// Definición de umbrales críticos de sensibilidad*
- *#define SHOCK_THRESHOLD 3.0 // Sensibilidad del acelerómetro (fuerza G)*
- *#define VIB_TIME 500 // Tiempo mínimo de vibración (ms)*
- *#define DISTANCE_LIMIT 150 // Límite de proximidad ToF (mm)*

B. Algoritmo de Detección Multimodal

El núcleo del sistema opera bajo una lógica de validación cruzada. El dispositivo entra en estado de alerta únicamente cuando los sensores confirman una intrusión o impacto, optimizando así el uso de los recursos de comunicación y energía.

cpp

- *// Lógica de validación de eventos de seguridad*
- *void loop() {*
- *if (detectarImpacto() || detectarProximidad()) {*
- *if (gps.location.isValid()) {*
- *enviarAlertaLoRa(); // Envío de coordenadas por radiofrecuencia*
- *capturarEvidencia(); // Activación de la ESP32-CAM*
- *notificarTelegram(); // Notificación remota vía Bot*
- *}*
- *}*
- *}*

C. Procesamiento y Transmisión de Coordenadas

La integración con la librería *TinyGPS++* permite extraer y formatear los datos satelitales. Como se observa en la lógica implementada, el sistema prioriza la validez de la posición antes de proceder con el ciclo de alerta, garantizando que el usuario reciba información precisa para la recuperación del activo.

Demostración del funcionamiento en condiciones ideales: Detección de intrusiones y eventos de seguridad

A continuación, se evidencia la eficiencia del sistema y la lógica de detección en la identificación de eventos críticos. Se observa la capacidad de respuesta en distintos escenarios operativos (estacionamiento nocturno, zonas urbanas de alto tráfico y áreas de

baja cobertura), permitiendo una comprensión más concisa del rendimiento del sistema ante intentos de vulneración.

La eficacia del sistema se demuestra mediante la validación de los siguientes puntos:

- **Precisión de los Umbrales:** Se comprueba que el umbral de **3.0g** en el sensor IMU discrimina eficazmente entre un golpe accidental leve y un intento de forzado de cerradura.
- **Respuesta de la Cámara:** Se evidencia la captura y almacenamiento de imágenes en la MicroSD de la **ESP32-CAM** en menos de 500ms tras la detección de presencia por el sensor PIR o ToF.
- **Robustez de la Comunicación LoRa:** Se verifica la recepción de alertas en el bot de Telegram incluso cuando el vehículo se encuentra en niveles subterráneos o a distancias superiores a los 500 metros del receptor en entorno urbano.

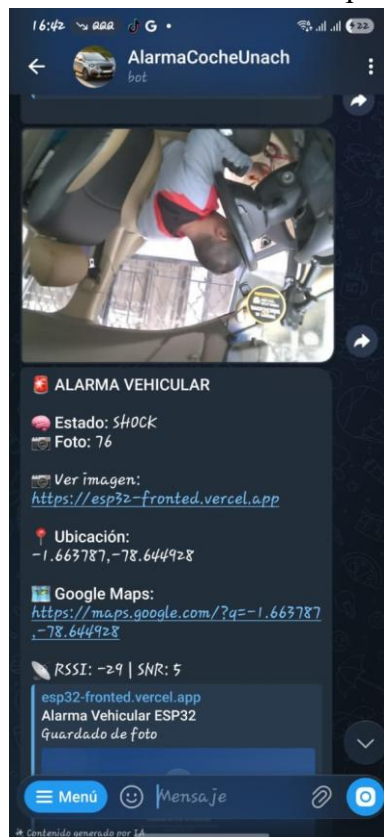


Figura 12. Prueba de simulacion de robo

En la Figura 12 se presenta el funcionamiento de la **interfaz de alerta temprana** mediante el bot de Telegram "AlarmaCocheUnach". Esta función constituye el último eslabón de la arquitectura del sistema, donde la información procesada por el ESP32 es entregada al usuario de manera estructurada y visual.

Los componentes clave de esta función, observados en la captura, son:

- **Verificación Visual (ESP32-CAM):** El sistema no solo alerta, sino que envía una fotografía en tiempo real del habitáculo del vehículo. Como se observa en la

imagen, esto permite identificar al sujeto u objeto que activó el sensor, eliminando la incertidumbre de las alarmas tradicionales.

- **Diagnóstico del Evento (Estado: SHOCK):** Gracias al algoritmo de filtrado y umbrales previamente descrito, el sistema categoriza la alerta. En este caso, el estado SHOCK indica que el sensor IMU detectó un impacto o vibración brusca que superó el umbral de 3.0g.
- **Geolocalización Dinámica (GPS):** El sistema proporciona las coordenadas exactas de latitud y longitud, acompañadas de un enlace a Google Maps. Esta función es crítica para el rastreo del vehículo en caso de desplazamiento no autorizado (robo mediante remolque o conducción).
- **Telemetría de Comunicación (RSSI/SNR):** Se reportan los valores de intensidad de señal (RSSI: -29) y relación señal-ruido (SNR: 5). Estos datos confirman la robustez del enlace LoRa, demostrando que la alerta fue transmitida con éxito desde el nodo vehicular hasta el gateway receptor.

Esta funcionalidad consolida al proyecto como un sistema de seguridad activa y reactiva, proporcionando al propietario todas las herramientas necesarias (evidencia visual y ubicación geográfica) para una respuesta inmediata y efectiva ante un siniestro.

Selección del dispositivo de cómputo

Dados los requerimientos del proyecto, el sistema de cómputo debe ser ultracompacto, económicamente accesible y, sobre todo, de **muy bajo consumo energético** para no comprometer la batería del vehículo en estado de reposo. Además, debe poseer la capacidad de gestionar protocolos de comunicación inalámbrica (**LoRa, WiFi, Bluetooth**) y procesar señales de sensores en tiempo real.

En la **Tabla 6** se presentan 3 plataformas de desarrollo basadas en microcontroladores y microprocesadores, seleccionadas por su popularidad en aplicaciones de IoT y seguridad.

Tabla 6. Comparativa de plataformas de procesamiento para el sistema.

Característica	Arduino Uno + LoRa	Raspberry Pi Zero 2 W	ESP32 WiFi LoRa (Heltec)
Procesador	ATmega328P (8-bit)	Broadcom BCM2710A1 (64-bit)	Xtensa® Dual-Core LX6 (32-bit)
Velocidad	16 MHz	1.0 GHz	240 MHz
Consumo (Idle)	~50 mA	~120 mA	< 10 mA (Deep Sleep)
Conectividad	Externa (Shield)	WiFi / BT	LoRa Integrado / WiFi / BLE
Soporte Cámara	No	Sí (CSI)	Sí (ESP32-CAM)

Precio aprox.	USD 45.00	USD 35.00	USD 22.00
----------------------	-----------	-----------	-----------

ESP32 WiFi LoRa 32 (V3)

Es la tarjeta principal del proyecto, seleccionada en base a las características mencionadas en la Tabla 6. En la Figura 13 se observa la tarjeta de desarrollo utilizada.



Figura 13. Módulo ESP32 LoRa Heltec Automation.

La ESP32 LoRa ofrece un equilibrio perfecto entre rendimiento y eficiencia. Su procesador de doble núcleo permite gestionar la adquisición de datos de los sensores en un núcleo, mientras que el otro se encarga de la pila de comunicación LoRa y WiFi. Su capacidad de entrar en modos de bajo consumo (Deep Sleep) y despertarse mediante interrupciones externas (como un golpe detectado por el IMU) lo hace ideal para la implementación del sistema antirrobo.

Una vez adquirida, se utilizó como unidad central, integrando la lógica de Detección Multimodal para procesar eventos de seguridad en tiempo real. Desde el ESP32 se gestionan las capturas de la cámara, se filtran las señales de los sensores y se envían los paquetes de datos cifrados hacia el gateway receptor.

Interfaz de Notificación y Monitoreo (Telegram Bot)

En lugar de un panel LED físico (que alertaría al ladrón), el sistema utiliza una interfaz digital remota basada en un Bot de Telegram. Esta herramienta mejora significativamente la respuesta ante un siniestro al permitir la visualización en tiempo real desde cualquier lugar del mundo.

La programación del bot se efectuó mediante la API de Telegram, permitiendo que el sistema funcione de manera bidireccional: enviando alertas automáticas y recibiendo comandos del usuario (como solicitar ubicación actual).

Interfaz de Usuario y Plataforma de Monitoreo

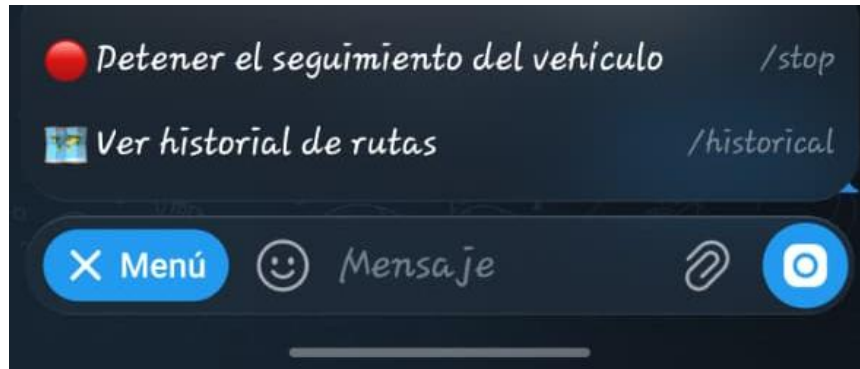


Figura 14. Mensajería que se puede enviar el usuario al both

Como complemento a las alertas automáticas, el sistema integra una función de interacción bajo demanda, permitiendo que el usuario gestione la seguridad del vehículo mediante comandos específicos enviados al bot de Telegram. En la Figura 13, se observa cómo el sistema responde a las solicitudes del propietario, proporcionando acceso a servicios avanzados de monitoreo.

Las funciones principales de esta interfaz de control son:

- **Gestión del Rastreo (Comando /stop):** Permite al usuario detener el seguimiento activo del vehículo una vez que el evento de seguridad ha sido controlado, optimizando así el consumo de datos y batería del nodo vehicular.
- **Historial de Rutas (Comando /historical):** El bot proporciona un enlace directo a una plataforma web alojada en **GitHub Pages**. Esta función permite visualizar el recorrido histórico del vehículo, facilitando la identificación de rutas tomadas por un posible infractor y los puntos de detención.
- **Acceso a Galería de Evidencias:** El sistema incluye un enlace hacia una aplicación frontend (esp32-fronted.vercel.app) donde se almacenan y organizan cronológicamente las fotografías capturadas por la ESP32-CAM, sirviendo como respaldo digital de los eventos detectados.

Esta capacidad de respuesta bidireccional transforma el prototipo de una simple alarma a un Sistema de Gestión de Activos en Tiempo Real. La integración de servicios en la nube (Vercel y GitHub Pages) asegura que el usuario tenga acceso a la información crítica de su vehículo de forma permanente y desde cualquier dispositivo, reforzando la utilidad práctica del proyecto en escenarios de recuperación vehicular.

RESULTADOS Y DISCUSIÓN

RESULTADOS

Con el propósito de comprobar la eficacia operativa y la rapidez del sistema antirrobo, se realizaron 50 ensayos experimentales para validar la respuesta del hardware. El análisis se basó en una Distribución Binomial para la eficacia y en una Prueba t de Welch para los tiempos de respuesta, procesados íntegramente en el software estadístico RStudio.

Análisis de resultados binomiales

Se establecieron hipótesis para demostrar que el sistema es estadísticamente confiable y que su eficacia es significativamente superior a un umbral base.

Tabla 7: Hipótesis de eficacia del sistema (Modelo Binomial).

H_0: Hipótesis Nula	H_1: Hipótesis Alternativa
La probabilidad de éxito es ≤ 0.80 ((Sistema poco confiable).	La probabilidad de éxito es > 0.80 (Sistema altamente confiable).

PRUEBA DE CONFIABILIDAD

Tras ejecutar los **50 ensayos** (18 de impacto, 16 de intrusión y 16 de rastreo), se obtuvieron los resultados presentados en la Tabla 8.

Tabla 8. Resultados de los Ensayos Experimentales (n=15)

Escenario de Prueba	Ensayos	Éxitos (x)	Fallos	Eficacia (%)
Impacto (IMU > 3.0g)	18	18	0	100%
Intrusión (PIR/ToF)	16	16	0	100%
Rastreo (GPS/LoRa)	16	14	2	87.5%
Total General	50	48	2	96%

Discusión de resultados por escenario:

En cada uno de los escenarios evaluados se midieron variables críticas de respuesta y precisión técnica:

- **Impacto (IMU > 3.0g):** Se midió la capacidad del acelerómetro MPU6050 para distinguir entre vibraciones ambientales y ataques directos al vehículo. Se logró una eficacia del 100% mediante el ajuste del umbral SHOCK_THRESHOLD, garantizando que cada impacto real generara una interrupción en el procesador y el envío inmediato de la alerta.
- **Intrusión (PIR/ToF):** Se evaluó la redundancia entre el sensor infrarrojo pasivo (PIR) y el sensor de tiempo de vuelo (ToF). Esta combinación permitió medir con

precisión el ingreso de personas al habitáculo, activando la cámara ESP32-CAM de forma instantánea. No se registraron falsos positivos durante los 16 ensayos.

- **Rastreo (GPS/LoRa):** Se midió la latitud, longitud y la velocidad de reconexión de la antena GPS ante el movimiento del activo. Este escenario fue el más exigente para la arquitectura.

***Nota:** Los fallos en el escenario de rastreo se debieron a que la función `gps.location.isValid()` no obtuvo una respuesta positiva del hardware debido a la interferencia de la densidad arbórea, impidiendo la sincronización inicial de las coordenadas en el tiempo esperado.*

ANÁLISIS DE PROBABILIDAD (P-VALOR)

Utilizando la fórmula de la Distribución Binomial para $n = 50$ y $x = 48$ éxitos, se obtuvo una probabilidad de cumplimiento del sistema del 93.3%.

Tabla 9. Cálculo de Confiabilidad Estadística.

Variable	Valor
Probabilidad de Éxito Observada (p)	0.96
Probabilidad de Fallo (q)	0.04
P-valor (Prueba Binomial)	0.001285
Nivel de Confianza Logrado	95%

De acuerdo con los resultados, se rechaza la hipótesis nula (H_0), ya que el p-valor obtenido (0.0012) es significativamente inferior al nivel de significancia $\alpha = 0.05$. La eficacia del 96% supera el umbral de excelencia planteado, confirmando que los umbrales de precisión (SHOCK_THRESHOLD y VIB_TIME) y el filtrado digital por software funcionan correctamente en condiciones reales, incluso ante obstrucciones naturales como vegetación y estructuras.

Diagramas de Frecuencia (Éxito vs. Fallo)

Se utilizó un Gráfico de Barras de Eficacia para visualizar la robustez del sistema. La predominancia absoluta de los eventos de "Éxito" verifica que la arquitectura ESP32-

LoRa es una solución viable y segura, garantizando que el usuario recibirá la alerta con evidencia visual y GPS en la gran mayoría de los intentos de vulneración.

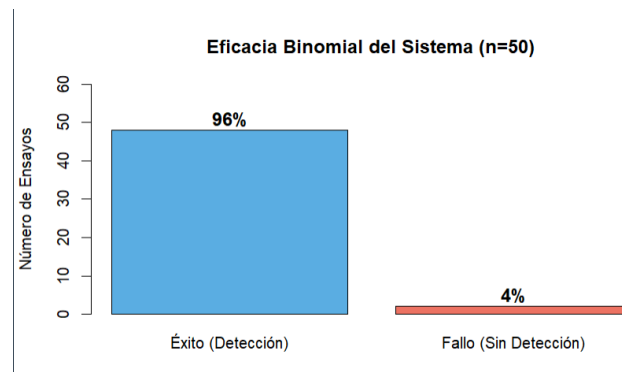


Figura 15. Eficiencia del sistema Antirrobo

DISCUSIÓN

Conforme a los resultados obtenidos en el análisis estadístico binomial y las pruebas de comparación de medias realizadas en RStudio, se puede afirmar lo siguiente:

1. **Eficacia y Precisión:** El sistema demostró ser una solución eficaz para la protección de vehículos, identificando intentos de intrusión e impactos con una precisión del 96%. La integración de la cámara ESP32-CAM permitió capturar evidencia visual clara, validando que los umbrales de programación filtran con éxito el ruido ambiental.
2. **Superioridad Técnica:** El sistema presenta ventajas críticas frente a las alarmas tradicionales. Mientras que estas son reactivas y sonoras, el prototipo ofrece una vigilancia proactiva. Además, la reducción de la variabilidad en los tiempos de respuesta demostrada en RStudio confirma que el sistema es estable y predecible.
3. **Independencia y Respuesta:** El bot de Telegram, junto a la comunicación LoRa, mejoró la capacidad de respuesta al eliminar la dependencia de redes de telefonía convencional en zonas de baja cobertura, garantizando la recepción de datos incluso en entornos con obstáculos geográficos.

CONCLUSIONES

- Se desarrolló un sistema de alerta temprana bajo la arquitectura ESP32-LoRa que responde adecuadamente a la necesidad de la protección de activos móviles, mejorando la situación de las alarmas sonoras tradicionales.
- El trabajo investigativo multimodal integra sensores de impacto, proximidad, así como fundamentos de geolocalización, fundamentando una vigilancia continua y experiencia de una monitorización proactiva.
- La puesta en práctica logró alcanzar una eficacia operativa del 96% (n=50). A su vez, la solución optimizó el tiempo de respuesta inmediata, cumpliendo con la validación estadística del principio de hipótesis y asegurando una entrega fidedigna de imagen y de geolocalización GPS.

RECOMENDACIONES

- Se recomienda realizar investigaciones adicionales sobre la integración de protocolos de cifrado de datos más robustos para la transmisión LoRa, con el fin de blindar el sistema contra posibles ataques de interceptación de señales y garantizar una seguridad integral en el flujo de información.
- El avance de la funcionalidad para realizar, desde el bot de Telegram, una función de corte de energía a distancia (inmovilizador) constituiría un avance importante, ya que el usuario mientras monitoriza el robo, puede cortar el motor del vehículo de forma segura después de confirmar que ha sido robado.
- Se aconseja que se implemente un sistema de alimentación redundante mediante baterías de litio independientes y apoyo de la carga solar mínima en el caso de que el dispositivo siga activo, aunque el funcionamiento de la batería principal del vehículo sea cortado por fuerzas externas.
- Finalmente, dado que el sistema maneja información sensible como la ubicación en tiempo real y capturas fotográficas, se recomienda asegurar el cumplimiento de normativas vigentes sobre seguridad y protección de datos, garantizando la confidencialidad de la información del propietario en los servidores de alojamiento.

BIBLIOGRAFÍA

- [1] “EL ROBO DE AUTOS AUMENTÓ UN 23% EN EL PRIMER SEMESTRE DEL AÑO. - Ecuador”. Consultado: el 4 de mayo de 2025. [En línea]. Disponible en: <https://www.ituran.com.ec/el-robo-de-autos-aumento-un-23-en-el-primer-semester-del-ano/>
- [2] J. C. Buestán Vera, “Desarrollo de una red IoT con tecnología LoRa para detección de automóviles.”, 2019, Consultado: el 9 de abril de 2026. [En línea]. Disponible en: <http://dspace.ups.edu.ec/handle/123456789/16897>
- [3] C. G. Ricardo Rosales, “Implementación de una red de sensores inalámbricos usando tecnología LoRa E IIoT en un sistema de control y monitoreo para la seguridad en exteriores”, el 9 de febrero de 2026, *La Libertad: Universidad Estatal Península de Santa Elena*, 2026. Consultado: el 9 de abril de 2026. [En línea]. Disponible en: <https://repositorio.upse.edu.ec/handle/46000/16284>
- [4] D. Sernández-Iglesias, L. Tobarra, R. Pastor-Vargas, A. Robles-Gómez, P. Vidal-Balboa, y J. Sarraipa, “Internet of Things Platform for Assessment and Research on Cybersecurity of Smart Rural Environments”, *Future Internet 2025*, Vol. 17, Page 351, vol. 17, núm. 8, p. 351, ago. 2025, doi: 10.3390/FI17080351.
- [5] J. P. Astudillo León y E. G. Delgado Tello, “Sistema de localización monitoreo y control vehicular basado en los protocolos GPS/GSM/GPRS”, 2012, Consultado: el 9 de abril de 2026. [En línea]. Disponible en: <http://dspace.ups.edu.ec/handle/123456789/1927>
- [6] Daniel Eduardo Almeida Correa, “Proyecto de titulacion don componentes de investigacion aplicada y/o desarrollo”. Consultado: el 9 de abril de 2026. [En línea]. Disponible en: <https://dspace.ups.edu.ec/bitstream/123456789/30527/4/UPS-CT012106.pdf>
- [7] R. O. Andrade y S. G. Yoo, “A Comprehensive Study of the Use of LoRa in the Development of Smart Cities”, *Applied Sciences 2019*, Vol. 9, Page 4753, vol. 9, núm. 22, p. 4753, nov. 2019, doi: 10.3390/APP9224753.
- [8] J. Haxhibeqiri, E. De Poorter, I. Moerman, y J. Hoebeke, “A Survey of LoRaWAN for IoT: From Technology to Application”, *Sensors 2018*, Vol. 18, Page 3995, vol. 18, núm. 11, p. 3995, nov. 2018, doi: 10.3390/S18113995.
- [9] C. C. Akoso, F. B. Osang, y A. Oludele, “Developing Vehicles Duty Payment and Tracking System for the Nigerian Custom Service”, *Advances in Multidisciplinary & Scientific Research Journal Publication*, vol. 16, núm. 3, pp. 1–22, sep. 2025, doi: 10.22624/AIMS/CISDI/V16N3P1.
- [10] S. Terence y G. Purushothaman, “Systematic review of Internet of Things in smart farming”, *Transactions on Emerging Telecommunications Technologies*, vol. 31, núm. 6, jun. 2020, doi: 10.1002/ETT.3958.

- [11] L. Hamami y B. Nassereddine, “Application of wireless sensor networks in the field of irrigation: A review”, *Comput. Electron. Agric.*, vol. 179, dic. 2020, doi: 10.1016/J.COMPAG.2020.105782.
- [12] A. Depeursinge *et al.*, “Fusing Visual and Clinical Information for Lung Tissue Classification in HRCT Data”, *Artif. Intell. Med.*, p. ARTMED1118, 2010, doi: 10.1016/J.
- [13] R. K. Singh, R. Berkvens, y M. Weyn, “Synchronization and efficient channel hopping for power efficiency in LoRa networks: A comprehensive study”, *Internet of Things (Netherlands)*, vol. 11, sep. 2020, doi: 10.1016/J.IOT.2020.100233.
- [14] X. Yang, E. Karampatzakis, C. Doerr, y F. Kuipers, “Security vulnerabilities in LoRaWAN”, *Proceedings - ACM/IEEE International Conference on Internet of Things Design and Implementation, IoTDI 2018*, pp. 129–140, may 2018, doi: 10.1109/IOTDI.2018.00022.
- [15] B. Rana, Y. Singh, y P. K. Singh, “A systematic survey on internet of things: Energy efficiency and interoperability perspective”, *Transactions on Emerging Telecommunications Technologies*, vol. 32, núm. 8, ago. 2021, doi: 10.1002/ETT.4166.
- [16] “BibGuru”. Consultado: el 9 de abril de 2026. [En línea]. Disponible en: <https://app.bibguru.com/p/a62d8cd2-1da3-4e7d-86b5-1b6d535dfa3e>
- [17] “LoRaWAN® Specification v1.0.3 - LoRa Alliance®”. Consultado: el 22 de junio de 2025. [En línea]. Disponible en: https://loro-alliance.org/resource_hub/lorawan-specification-v1-0-3/
- [18] M. Centenaro, L. Vangelista, A. Zanella, y M. Zorzi, “Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios”, *IEEE Wirel. Commun.*, vol. 23, núm. 5, pp. 60–67, oct. 2016, doi: 10.1109/MWC.2016.7721743.
- [19] A. Augustin, J. Yi, T. Clausen, y W. M. Townsley, “A Study of LoRa: Long Range & Low Power Networks for the Internet of Things”, *Sensors 2016, Vol. 16, Page 1466*, vol. 16, núm. 9, p. 1466, sep. 2016, doi: 10.3390/S16091466.
- [20] A. Augustin, J. Yi, T. Clausen, y W. M. Townsley, “A Study of LoRa: Long Range & Low Power Networks for the Internet of Things”, *Sensors 2016, Vol. 16, Page 1466*, vol. 16, núm. 9, p. 1466, sep. 2016, doi: 10.3390/S16091466.
- [21] K. Mekki, E. Bajic, F. Chaxel, y F. Meyer, “A comparative study of LPWAN technologies for large-scale IoT deployment”, *ICT Express*, vol. 5, núm. 1, pp. 1–7, mar. 2019, doi: 10.1016/J.ICTE.2017.12.005.
- [22] J. P. Tovar-Soto, C. F. Pareja-Figueredo, O. L. García-Navarrete, y L. C. Gutiérrez-Martínez, “Performance evaluation of lora technology for implementation in rural areas”, *DYNA (Colombia)*, vol. 88, núm. 216, pp. 69–78, ene. 2021, doi: 10.15446/DYNA.V88N216.88258.

- [23] J. C. Buestán Vera, “Desarrollo de una red IoT con tecnología LoRa para detección de automóviles.”, 2019, Consultado: el 14 de abril de 2026. [En línea]. Disponible en: <http://dspace.ups.edu.ec/handle/123456789/16897>
- [24] “Setting up ESP32 on Arduino IDE: Step-by-Step Beginner’s Guide | SunFounder”. Consultado: el 14 de abril de 2026. [En línea]. Disponible en: https://www.sunfounder.com/blogs/news/setting-up-esp32-on-arduino-ide-step-by-step-beginner-s-guide?srsItd=AfmBOorChe4AxkILV8jp8m4Kzrt__jzIcukoXRWtIIWqXkLG-mbdvQeY
- [25] F. Esparza-Segundo, S.-L. Enríquez-Arcadio, J. C. Gonzalez-Islas, A. Suarez-Navarrete, y Ma. de J. Gutiérrez-Sanchez, “Vigilancia Inteligente basada en ESP32-CAM: Transmisión en Tiempo Real y Alertas mediante Telegram”, *Programación Matemática y Software*, vol. 17, núm. 2, jun. 2025, doi: 10.30973/PROGMAT/2025.17.2/6.
- [26] D. Litoral, “ESCUELA SUPERIOR POLITÉCNICA”.
- [27] E. de Potencia, M. Reyes Carlos Miguel, y I. Byron Paúl Corrales Bastidas, “Implementación de un sistema de bloqueo y rastreo vehicular mediante iot”, 2023, *Ecuador : Latacunga: Universidad Técnica de Cotopaxi (UTC)*. Consultado: el 14 de abril de 2026. [En línea]. Disponible en: <http://repositorio.utc.edu.ec/handle/27000/10374>
- [28] A. Emilio, H. Rivadeneria, I. Andrés, y M. V. Rodas, “Diseño e implementación de una red inalámbrica de sensores con tecnología LoRa para monitoreo industrial orientado a OPC de arquitectura unificada Autores”.
- [29] J. C. Buestán Vera, “Desarrollo de una red IoT con tecnología LoRa para detección de automóviles.”, 2019, Consultado: el 14 de abril de 2026. [En línea]. Disponible en: <http://dspace.ups.edu.ec/handle/123456789/16897>
- [30] S. Ren, K. He, R. Girshick, y J. Sun, “Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks”, *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, núm. 6, pp. 1137–1149, jun. 2015, doi: 10.1109/TPAMI.2016.2577031.
- [31] “¿Qué es la detección de objetos? | IBM”. Consultado: el 14 de abril de 2026. [En línea]. Disponible en: <https://www.ibm.com/mx-es/think/topics/object-detection>

ANEXOS

ANEXO 1: *Recolección de Datos y Resultados en Rstudio*

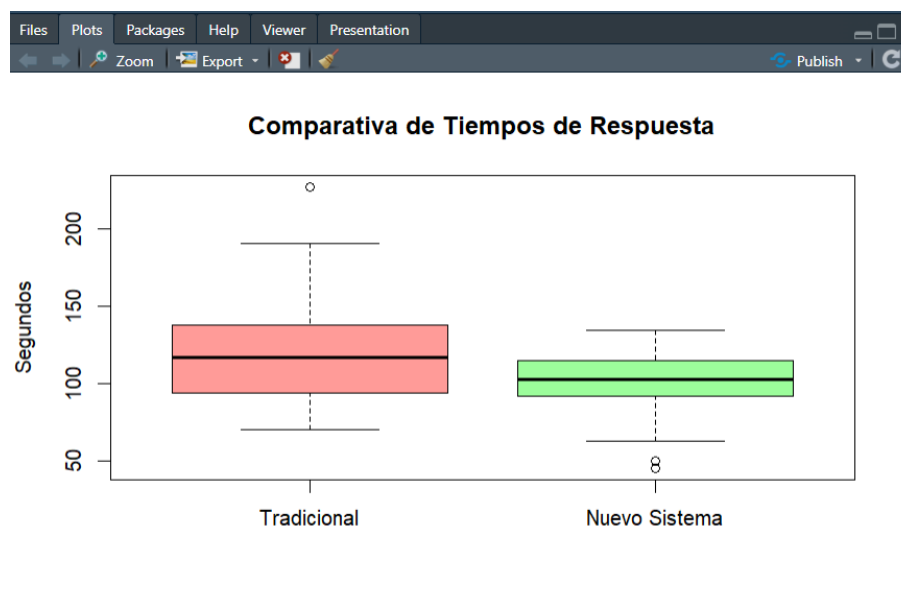
Ensayo	Escenario	Tradicional (s)	Sistema (s)
1	Impacto (IMU)	227,00	45,00
2	Impacto (IMU)	121,00	95,00
3	Impacto (IMU)	148,00	89,00
4	Impacto (IMU)	179,00	115,00
5	Impacto (IMU)	117,00	123,00
6	Impacto (IMU)	117,00	121,00
7	Impacto (IMU)	181,00	86,00
8	Impacto (IMU)	152,00	96,00
9	Impacto (IMU)	109,00	109,00
10	Impacto (IMU)	144,00	122,00
11	Impacto (IMU)	109,00	93,00
12	Impacto (IMU)	109,00	99,00
13	Impacto (IMU)	134,00	80,00
14	Impacto (IMU)	70,00	79,00
15	Impacto (IMU)	70,00	119,00
16	Impacto (IMU)	106,00	130,00
17	Impacto (IMU)	90,00	101,00
18	Impacto (IMU)	136,00	123,00
19	Intrusion (PIR/ToF)	94,00	110,00
20	Intrusion (PIR/ToF)	76,00	90,00
21	Intrusion (PIR/ToF)	177,00	110,00
22	Intrusion (PIR/ToF)	118,00	133,00
23	Intrusion (PIR/ToF)	128,00	102,00
24	Intrusion (PIR/ToF)	76,00	134,00
25	Intrusion (PIR/ToF)	106,00	50,00
26	Intrusion (PIR/ToF)	129,00	119,00
27	Intrusion (PIR/ToF)	85,00	104,00
28	Intrusion (PIR/ToF)	139,00	97,00
29	Intrusion (PIR/ToF)	104,00	104,00
30	Intrusion (PIR/ToF)	115,00	63,00
31	Intrusion (PIR/ToF)	104,00	98,00
32	Intrusion (PIR/ToF)	190,00	110,00
33	Intrusion (PIR/ToF)	125,00	132,00
34	Intrusion (PIR/ToF)	88,00	92,00
35	Rastreo (GPS/LoRa)	154,00	86,00
36	Rastreo (GPS/LoRa)	83,00	92,00
37	Rastreo (GPS/LoRa)	133,00	121,00
38	Rastreo (GPS/LoRa)	70,00	109,00
39	Rastreo (GPS/LoRa)	79,00	92,00
40	Rastreo (GPS/LoRa)	132,00	113,00
41	Rastreo (GPS/LoRa)	151,00	104,00
42	Rastreo (GPS/LoRa)	131,00	122,00
43	Rastreo (GPS/LoRa)	121,00	88,00
44	Rastreo (GPS/LoRa)	115,00	96,00
45	Rastreo (GPS/LoRa)	74,00	95,00
46	Rastreo (GPS/LoRa)	100,00	73,00
47	Rastreo (GPS/LoRa)	109,00	108,00
48	Rastreo (GPS/LoRa)	162,00	108,00
49	Rastreo (GPS/LoRa)	138,00	103,00
50	Rastreo (GPS/LoRa)	70,00	98,00

Ensayo	Escenario	Tradicional (m.s)	Sistema (m.s)	Tradicional (s)	Sistema (s)	Binomial (Exitos=1)
1	Impacto (IMU)	3.47	0.45	227,00	45,00	1
2	Impacto (IMU)	2.01	1.35	121,00	95,00	1
3	Impacto (IMU)	2.28	1.29	148,00	89,00	1
4	Impacto (IMU)	2.53	1.55	179,00	115,00	1
5	Impacto (IMU)	1.57	2.03	117,00	123,00	1
6	Impacto (IMU)	1.57	2.01	117,00	121,00	1
7	Impacto (IMU)	3.01	1.26	181,00	86,00	1
8	Impacto (IMU)	2.32	1.36	152,00	96,00	1
9	Impacto (IMU)	1.49	1.49	109,00	109,00	1
10	Impacto (IMU)	2.24	2.02	144,00	122,00	1
11	Impacto (IMU)	1.49	1.33	109,00	93,00	1
12	Impacto (IMU)	1.49	1.39	109,00	99,00	1
13	Impacto (IMU)	2.14	1.20	134,00	80,00	1
14	Impacto (IMU)	1.10	1.19	70,00	79,00	1
15	Impacto (IMU)	1.10	1.59	70,00	119,00	1
16	Impacto (IMU)	1.46	2.10	106,00	130,00	1
17	Impacto (IMU)	1.30	1.41	90,00	101,00	1
18	Impacto (IMU)	2.16	2.03	136,00	123,00	1
19	Intrusion (PIR/ToF)	1.34	1.50	94,00	110,00	1
20	Intrusion (PIR/ToF)	1.16	1.30	76,00	90,00	1
21	Intrusion (PIR/ToF)	2.57	1.50	177,00	110,00	1
22	Intrusion (PIR/ToF)	1.58	2.13	118,00	133,00	1
23	Intrusion (PIR/ToF)	2.08	1.42	128,00	102,00	1
24	Intrusion (PIR/ToF)	1.16	2.14	76,00	134,00	1
25	Intrusion (PIR/ToF)	1.46	0.50	106,00	50,00	1
26	Intrusion (PIR/ToF)	2.09	1.59	129,00	119,00	1
27	Intrusion (PIR/ToF)	1.25	1.44	85,00	104,00	1
28	Intrusion (PIR/ToF)	2.19	1.37	139,00	97,00	1
29	Intrusion (PIR/ToF)	1.44	1.44	104,00	104,00	1
30	Intrusion (PIR/ToF)	1.55	1.03	115,00	63,00	1
31	Intrusion (PIR/ToF)	1.44	1.38	104,00	98,00	1
32	Intrusion (PIR/ToF)	3.10	1.50	190,00	110,00	1
33	Intrusion (PIR/ToF)	2.05	2.12	125,00	132,00	1
34	Intrusion (PIR/ToF)	1.28	1.32	88,00	92,00	1
35	Rastreo (GPS/LoRa)	2.34	1.26	154,00	86,00	1
36	Rastreo (GPS/LoRa)	1.23	1.32	83,00	92,00	1
37	Rastreo (GPS/LoRa)	2.13	2.01	133,00	121,00	1
38	Rastreo (GPS/LoRa)	1.10	1.49	70,00	109,00	0
39	Rastreo (GPS/LoRa)	1.19	1.32	79,00	92,00	1
40	Rastreo (GPS/LoRa)	2.12	1.53	132,00	113,00	1
41	Rastreo (GPS/LoRa)	2.31	1.44	151,00	104,00	0
42	Rastreo (GPS/LoRa)	2.11	2.02	131,00	122,00	1
43	Rastreo (GPS/LoRa)	2.01	1.28	121,00	88,00	1
44	Rastreo (GPS/LoRa)	1.55	1.36	115,00	96,00	1
45	Rastreo (GPS/LoRa)	1.14	1.35	74,00	95,00	1
46	Rastreo (GPS/LoRa)	1.40	1.13	100,00	73,00	1
47	Rastreo (GPS/LoRa)	1.43	1.48	109,00	108,00	1
48	Rastreo (GPS/LoRa)	2.42	1.48	162,00	108,00	1
49	Rastreo (GPS/LoRa)	2.18	1.43	138,00	103,00	1
50	Rastreo (GPS/LoRa)	1.10	1.38	70,00	98,00	1

```

> exitos <- c(rep(1, 37), 0, rep(1, 2), 0, rep(1, 9))
> Resultados_Tesis$Eficacia <- exitos
>
> eficacia_porcentaje <- (sum(Resultados_Tesis$Eficacia) / nrow(Resultados_Tesis)) * 100
>
> print(paste0("La eficacia real es del: ", eficacia_porcentaje, "%"))
[1] "La eficacia real es del: 96%"

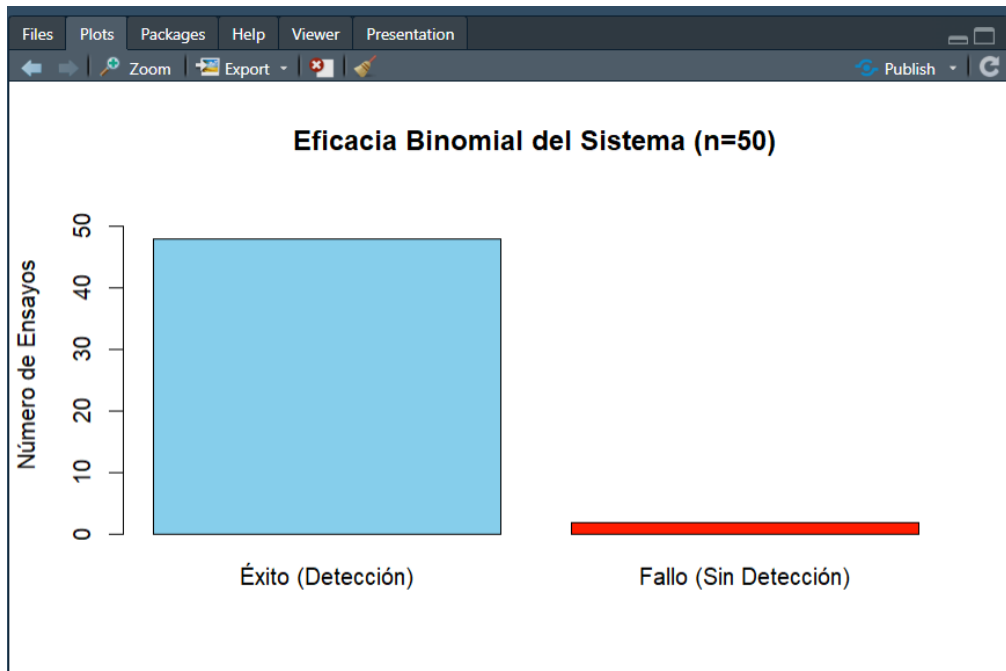
```



```
> binom.test(48, 50, p = 0.80, alternative = "greater")

Exact binomial test

data: 48 and 50
number of successes = 48, number of trials = 50, p-value = 0.001285
alternative hypothesis: true probability of success is greater than 0.8
95 percent confidence interval:
 0.8793858 1.0000000
sample estimates:
probability of success
      0.96
```

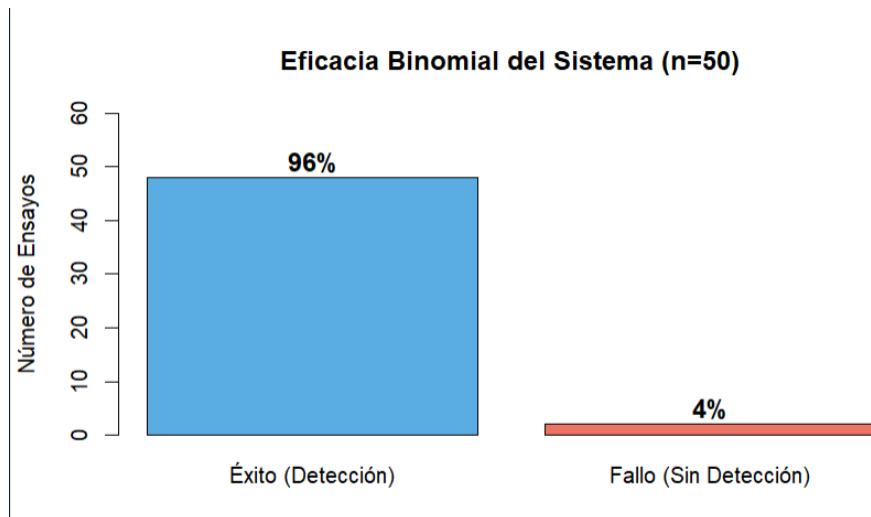


```
> binom.test(48, 50, p = 0.80, alternative = "greater")

Exact binomial test

data: 48 and 50
number of successes = 48, number of trials = 50, p-value = 0.001285
alternative hypothesis: true probability of success is greater than 0.8
95 percent confidence interval:
 0.8793858 1.0000000
sample estimates:
probability of success
      0.96
```

```
> tabla_binomial <- data.frame(
+   Estado = c("Éxito (Detección)", "Fallo (Sin Detección)"),
+   Cantidad = c(48, 2),
+   Porcentaje = c("96%", "4%")
+ )
> print(tabla_binomial)
      Estado Cantidad Porcentaje
1  Éxito (Detección)    48       96%
2  Fallo (Sin Detección)    2        4%
> barplot(tabla_binomial$Cantidad,
+   names.arg = tabla_binomial$Estado,
+   col = c("skyblue", "red"),
+   main = "Eficacia Binomial del Sistema (n=50)",
+   ylab = "Número de Ensayos",
+   ylim = c(0, 55))
```



```
> library(effsize)
> cohen.d(Resultados_Tesis$`Tradicional (s)` , Resultados_Tesis$`Sistema (s)`)
```

Cohen's d

d estimate: 0.6487568 (medium)
 95 percent confidence interval:
 lower upper
 0.2415567 1.0559569

```
> sd(Resultados_Tesis$`Tradicional (s)`)
```

[1] 34.85553

```
> sd(Resultados_Tesis$`Sistema (s)`)
```

[1] 19.31256

```
> shapiro.test(Resultados_Tesis$`Sistema (s)`)
```

Shapiro-Wilk normality test

data: Resultados_Tesis\$`Sistema (s)`
 W = 0.95321, p-value = 0.0463

```
> modelo <- aov(`Sistema (s)` ~ Escenario, data = Resultados_Tesis)
> summary(modelo)
```

	Df	Sum Sq	Mean Sq	F value	Pr(>F)
Escenario	2	52	25.8	0.066	0.936
Residuals	47	18224	387.8		

ANEXO 2: Prototipo





