

## Trabajo Fin de Grado

### Diseño de una Red Distribuida de Sensores Inteligentes con redundancia Multisensorial y Gestión *IoT* en Escenarios de Baja Conectividad

Jose Óscar Villalba Puertas

Director académico: Miguel Ángel Guillomía San Bartolomé

Director militar: Laura Herranz López

Centro Universitario de la Defensa-Academia General Militar





## Agradecimientos

En primer lugar, expresar mi agradecimiento a mi familia, por el apoyo incondicional recibido a lo largo de mi vida. Sin vuestra comprensión, ánimo y valores que me habéis inculcado, nunca habría escogido este camino.

A *Javier Fernández González*, gracias a quien tuve la oportunidad de involucrarme en actividades que originaron este trabajo y que me permitió conocer a mis tutores, pilares fundamentales durante estos meses.

A mi tutora militar, *Laura Herranz López* por su comprensión y respaldo frente al cambio de enfoque del proyecto. Destacando su disposición para afrontar los nuevos retos que este entrañaba y su ayuda constante en la elaboración del mismo.

Finalmente, un agradecimiento especial a mi tutor académico, *Miguel Ángel Guillomía San Bartolomé*, por la atención, paciencia y dedicación que demuestra hacia el alumnado. Sin su guía y el interés que despertó en mí hacia esta materia, jamás habría propuesto la temática de este TFG.

A todos vosotros, gracias por vuestra cercanía y trato humano. Ha sido un placer y un honor trabajar a vuestro lado.



## RESUMEN

Este Trabajo Fin de Grado aborda el diseño y validación conceptual de una red distribuida de sensores inteligentes con redundancia multisensorial y gestión *IoT*, orientada a escenarios de baja conectividad y alta interferencia electromagnética, como los generados por guerra electrónica. El problema identificado radica en la ausencia de soluciones prácticas que integren detección fiable, autonomía energética y comunicación segura en entornos donde las infraestructuras convencionales son inoperantes o vulnerables. La propuesta responde a la necesidad de garantizar información crítica para operaciones militares, vigilancia perimetral y misiones tácticas, minimizando la dependencia de redes centralizadas.

El objetivo principal consiste en diseñar y validar mediante simulación un nodo sensor autónomo, capaz de detectar movimiento mediante la fusión de datos de cámara y sensor PIR, y transmitir alertas mediante una red *LoRa* robusta y de bajo consumo. Entre los objetivos secundarios se incluyen la definición de requisitos funcionales, la selección de hardware, el diseño del protocolo de comunicación con cifrado ligero (XOR) y pseudo salto de frecuencia, así como la evaluación de la fiabilidad, latencia y autonomía del sistema.

La metodología adoptada combina un enfoque descriptivo-aplicativo con técnicas cuantitativas y cualitativas. Se realizó una revisión bibliográfica sobre *IoT*, *LoRa* y sistemas embebidos, seguida del diseño de la arquitectura hardware. El algoritmo de integración multisensorial se modeló en Bizagi y se validó mediante simulaciones en NS-3 y entornos como *Wokwi* y *Python*. Se implementaron pruebas de comunicación cifrada y pseudo salto de frecuencia, además de simulaciones de escalabilidad con hasta 35 nodos emisores. Finalmente, se evaluaron métricas clave como latencia, tasa de entrega y consumo energético.

Los resultados obtenidos demuestran la viabilidad técnica del sistema en entornos simulados: tasa de entrega del 100%, latencia promedio de 11,5 ms en pruebas iniciales y 104 ms en escenarios ampliados, sin penalización significativa por el cifrado XOR. El algoritmo de fusión redujo falsos positivos y garantizó la generación coherente de alertas. La autonomía estimada, basada en cálculos y pruebas de consumo, alcanza aproximadamente 48 horas con baterías externas de 50.000 mAh. Estos resultados cumplen los objetivos planteados, validando la propuesta a nivel conceptual y funcional.

En conclusión, el trabajo aporta una solución innovadora y escalable para la vigilancia autónoma en entornos hostiles, integrando tecnologías de bajo coste y alta resiliencia. Aunque la validación se limita a simulaciones, el diseño constituye una base sólida para futuros desarrollos orientados al prototipado físico, optimización energética y despliegue en condiciones reales. Su aplicación se extiende al ámbito militar y civil, incluyendo seguridad perimetral, monitoreo ambiental y protección de infraestructuras críticas.

**PALABRAS CLAVE:** LoRa, IoT, RED DISTRIBUIDA, SENSORES INTELIGENTES



## ABSTRACT

This Final Degree Project addresses the design and conceptual validation of a distributed network of intelligent sensors with multisensor redundancy and IoT management, aimed at low-connectivity environments with high electromagnetic interference, such as those caused by electronic warfare. The identified problem lies in the lack of practical solutions that combine reliable detection, energy autonomy, and secure communication in scenarios where conventional infrastructures are inoperative or vulnerable. The proposed system seeks to ensure critical information for military operations, perimeter surveillance, and tactical missions, minimizing dependence on centralized networks.

The main objective is to design and validate through simulation an autonomous sensor node capable of detecting movement using data fusion from a camera and a PIR sensor, and transmitting alerts via a robust, low-power LoRa network. Secondary objectives include defining functional requirements, selecting hardware, designing a communication protocol with lightweight encryption (XOR) and pseudo-frequency hopping, and evaluating system reliability, latency, and autonomy.

The methodology combines a descriptive-applied approach with quantitative and qualitative techniques. A literature review on IoT, LoRa, and embedded systems was followed by the design of the hardware architecture. The multisensor integration algorithm was modeled in Bizagi and validated through simulations in NS-3 and environments such as Wokwi and Python. Communication tests with encryption and pseudo-frequency hopping were implemented, along with scalability simulations involving up to 35 transmitting nodes. Key metrics such as latency, packet delivery rate, and energy consumption were analyzed.

Results confirm the technical feasibility of the system in simulated environments: 100% packet delivery rate, average latency of 11.5 ms in initial tests and 104 ms in extended scenarios, with no significant penalty from XOR encryption. The fusion algorithm reduced false positives and ensured coherent alert generation. Estimated autonomy, based on consumption calculations and tests, reaches approximately 48 hours using 50,000 mAh external batteries. These results meet the stated objectives, validating the proposal at a conceptual and functional level.

In conclusion, this work provides an innovative and scalable solution for autonomous surveillance in hostile environments, integrating low-cost, resilient technologies. Although validation is limited to simulations, the design offers a solid foundation for future developments focused on physical prototyping, energy optimization, and real-world deployment. Its applicability extends to both military and civilian domains, including perimeter security, environmental monitoring, and critical infrastructure protection.

**KEYWORDS :** LoRa, IoT, DISTRIBUTED NETWORK, INTELLIGENT SENSORS



# INDICE DE CONTENIDO

|                                                               |             |
|---------------------------------------------------------------|-------------|
| <b>AGRADECIMIENTOS .....</b>                                  | <b>I</b>    |
| <b>RESUMEN.....</b>                                           | <b>II</b>   |
| <b>ABSTRACT .....</b>                                         | <b>III</b>  |
| <b>INDICE DE CONTENIDO .....</b>                              | <b>IV</b>   |
| <b>INDICE DE FIGURAS.....</b>                                 | <b>VI</b>   |
| <b>INDICE DE TABLAS .....</b>                                 | <b>VII</b>  |
| <b>ABREVIATURAS, SIGLAS Y ACRÓNIMOS .....</b>                 | <b>VIII</b> |
| <b>DECLARACIÓN DE USO DE INTELIGENCIA ARTIFICIAL .....</b>    | <b>X</b>    |
| <b>1. INTRODUCCIÓN .....</b>                                  | <b>1</b>    |
| 1.1. Justificación .....                                      | 1           |
| 1.2. Ámbito de aplicación.....                                | 2           |
| 1.3. Contextualización.....                                   | 2           |
| 1.4. Estructura de la memoria y plan de trabajo .....         | 3           |
| <b>2. OBJETIVOS Y METODOLOGÍA.....</b>                        | <b>4</b>    |
| 2.1. OBJETIVOS.....                                           | 4           |
| 2.1.1. Objetivo principal .....                               | 4           |
| 2.1.2. Objetivos secundarios .....                            | 4           |
| 2.2. ALCANCE .....                                            | 4           |
| 2.3. METODOLOGÍA .....                                        | 6           |
| <b>3. ANTECEDENTES Y MARCO TEÓRICO.....</b>                   | <b>7</b>    |
| 3.1. Antecedentes .....                                       | 7           |
| 3.2. Bases teóricas .....                                     | 7           |
| 3.2.1. <i>LoRa</i> .....                                      | 7           |
| 3.2.2. Detección de movimiento e imagen por cámara .....      | 9           |
| 3.3. Estado del arte.....                                     | 10          |
| 3.3.1. Tecnología actual .....                                | 10          |
| 3.3.2. Avances recientes .....                                | 10          |
| 3.3.3. Comparación crítica.....                               | 11          |
| 3.4. Amenazas de la Guerra Electrónica .....                  | 11          |
| 3.5. Introducción a sistemas embebidos .....                  | 12          |
| 3.6. <i>Raspberry Pi</i> , <i>ESP32</i> y el <i>IoT</i> ..... | 13          |
| <b>4. DESARROLLO: ANÁLISIS Y RESULTADOS .....</b>             | <b>14</b>   |
| 4.1. Definición de requisitos.....                            | 14          |
| 4.2. Selección de hardware .....                              | 15          |
| 4.2.1. Elección de componentes comerciales .....              | 15          |



|           |                                                                 |           |
|-----------|-----------------------------------------------------------------|-----------|
| 4.2.2.    | Cálculo de la autonomía del sistema.....                        | 19        |
| 4.2.3.    | Carcasa protectora .....                                        | 21        |
| 4.3.      | Integración hardware .....                                      | 23        |
| 4.3.1.    | Integración del dispositivo emisor .....                        | 23        |
| 4.3.2.    | Integración del dispositivo receptor .....                      | 25        |
| 4.4.      | Diseño de red <i>LoRa</i> y protocolo de comunicación .....     | 26        |
| 4.5.      | Validación de red y protocolo de comunicación .....             | 30        |
| 4.6.      | Diseño y validación de algoritmo de integración .....           | 31        |
| 4.6.1.    | Diseño del proceso .....                                        | 31        |
| 4.6.2.    | Validación de algoritmo de integración mediante simulación..... | 32        |
| 4.6.3.    | Validación prototipada .....                                    | 34        |
| 4.7.      | Análisis DAFO.....                                              | 35        |
| 4.8.      | RESULTADOS.....                                                 | 37        |
| <b>5.</b> | <b>CONCLUSIONES .....</b>                                       | <b>38</b> |
| 5.1.      | Líneas de investigación futuras .....                           | 39        |
| 5.2.      | Conclusión final.....                                           | 40        |
|           | <b>REFERENCIAS BIBLIOGRÁFICAS.....</b>                          | <b>41</b> |
|           | <b>ANEXO I.....</b>                                             | <b>48</b> |
|           | <b>ANEXO II.....</b>                                            | <b>50</b> |
|           | <b>ANEXO III.....</b>                                           | <b>51</b> |
|           | <b>ANEXO IV .....</b>                                           | <b>55</b> |
|           | <b>ANEXO V .....</b>                                            | <b>56</b> |



## INDICE DE FIGURAS

|                                                                                                      |    |
|------------------------------------------------------------------------------------------------------|----|
| Figura 1. Diagrama de Gannt. Fuente: elaboración propia.....                                         | 4  |
| Figura 2. Medición de consumo del prototipo. Fuente: elaboración propia. ....                        | 20 |
| Figura 3. Concepto de carcasa protectora. Fuente: elaboración propia.....                            | 22 |
| Figura 4. Pesaje de conjunto sensor. Fuente: elaboración propia.....                                 | 23 |
| Figura 5. Pesaje de prototipo de Gateway. Fuente: elaboración propia.....                            | 23 |
| Figura 6. Conexionado del nodo sensor. Fuente: elaboración propia. ....                              | 25 |
| Figura 7. Prototipo para detección de movimiento y transmisión LoRa. Fuente: elaboración propia..... | 25 |
| Figura 8. Conexionado Gateway. Fuente: elaboración propia.....                                       | 26 |
| Figura 9. Prototipo Gateway. Fuente: elaboración propia. ....                                        | 26 |
| Figura 10. Arquitectura de red LoRa. Fuente: [16].....                                               | 27 |
| Figura 11. Arquitectura de Thingsboard. Fuente:[91] .....                                            | 29 |
| Figura 12. Protocolo y procesado de los mensajes en Gateway. Fuente: elaboración propia...           | 30 |
| Figura 13. Resultados primera simulación. Fuente: elaboración propia.....                            | 30 |
| Figura 14. Simulación de funcionamiento del PIR. Fuente: elaboración propia. ....                    | 33 |
| Figura 15. Simulación de funcionamiento de detección de imagen. Fuente: elaboración propia.<br>..... | 34 |
| Figura 16. Detección simultanea mediante prototipo. Fuente: elaboración propia.....                  | 35 |
| Figura 17. Detección de vehículo militar mediante prototipo. Fuente: elaboración propia.....         | 35 |
| Figura 20. Interfaz web local. Fuente: elaboración propia. ....                                      | 55 |
| Figura 21. Interfaz Thingsboard. Fuente: elaboración propia. ....                                    | 55 |
| Figura 22. Diagrama de flujo. Fuente: elaboración propia. ....                                       | 56 |





## INDICE DE TABLAS

|                                                                                                                  |    |
|------------------------------------------------------------------------------------------------------------------|----|
| Tabla 1. Resultados de simulación de proceso. Fuente: elaboración propia. ....                                   | 32 |
| Tabla 2. Estimación de alcance y retardo estimado. Fuente: elaboración propia. ....                              | 49 |
| Tabla 3. Dimensiones de los componentes. Fuente: elaboración propia en base a componentes ya referenciados. .... | 50 |
| Tabla 4. Simulación de escalabilidad. Fuente: elaboración propia. ....                                           | 52 |
| Tabla 5. Simulación de colisiones. Fuente: elaboración propia. ....                                              | 52 |
| Tabla 6. Fiabilidad detección mediante PIR. Fuente: elaboración propia. ....                                     | 53 |
| Tabla 7. Fiabilidad detección cámara. Fuente: elaboración propia. ....                                           | 53 |
| Tabla 8. Fiabilidad detección acumulada. Fuente: elaboración propia. ....                                        | 54 |



## ABREVIATURAS, SIGLAS Y ACRÓNIMOS

|               |                                                                               |
|---------------|-------------------------------------------------------------------------------|
| <b>AI</b>     | Artificial intelligence (inteligencia artificial)                             |
| <b>AT</b>     | Attention Command (comando de configuración en módulos de comunicación serie) |
| <b>BW</b>     | Bandwidth (Ancho de banda)                                                    |
| <b>CAM</b>    | Cámara                                                                        |
| <b>COMINT</b> | Inteligencia de las comunicaciones                                            |
| <b>CSS</b>    | Chirp Spread Spectrum (espectro ensanchado por chirp)                         |
| <b>CR</b>     | Coding rate (tasa de codificación)                                            |
| <b>CRC</b>    | Cyclic Redundancy Check (verificación de redundancia cíclica)                 |
| <b>CUD</b>    | Centro Universitario de la Defensa                                            |
| <b>C2</b>     | Mando y control                                                               |
| <b>DAFO</b>   | Debilidades, Amenazas, Fortalezas y Oportunidades                             |
| <b>DID</b>    | Decentralized Identifier (identificador descentralizado)                      |
| <b>DoD</b>    | Depth of Discharge (profundidad de descarga)                                  |
| <b>EM</b>     | Electromagnético                                                              |
| <b>ELINT</b>  | Inteligencia electrónica                                                      |
| <b>EW</b>     | Electronic warfare (Guerra electrónica)                                       |
| <b>GPRS</b>   | General Packet Radio Service                                                  |
| <b>GPS</b>    | Global Positioning Sistem (Sistema de posicionamiento Global)                 |
| <b>h</b>      | Hora                                                                          |



|               |                                                                             |
|---------------|-----------------------------------------------------------------------------|
| <b>IA</b>     | Inteligencia Artificial                                                     |
| <b>IEC</b>    | International Electrotechnical Commission                                   |
| <b>IH</b>     | Implicit Header (cabecera implícita)                                        |
| <b>IoBT</b>   | Internet of Battlefield Things (Internet de las cosas del campo de batalla) |
| <b>IoT</b>    | Internet of Things (internet de las cosas)                                  |
| <b>IP</b>     | Internet Protocol                                                           |
| <b>LoRa</b>   | Long Range (largo alcance)                                                  |
| <b>LPWA</b>   | Low Power Wide Area (área amplia de baja potencia)                          |
| <b>mAh</b>    | Miliamperios hora                                                           |
| <b>MHz</b>    | Megahercios                                                                 |
| <b>MOV</b>    | Movimiento                                                                  |
| <b>ms</b>     | Milisegundos                                                                |
| <b>OSINT</b>  | Inteligencia de fuentes abiertas                                            |
| <b>PETG</b>   | Tereftalato de polietileno glicolizado                                      |
| <b>PIR</b>    | Passive Infrared Sensor (sensor infrarrojo pasivo)                          |
| <b>SF</b>     | Spreading Factor (factor de expansión)                                      |
| <b>SIGINT</b> | Inteligencia de las señales (EM)                                            |
| <b>TFG</b>    | Trabajo de Fin de Grado                                                     |
| <b>USB</b>    | Universal Serial Bus                                                        |
| <b>WiFi</b>   | Wireless Fidelity                                                           |
| <b>XOR</b>    | Exclusive OR (operación lógica exclusiva O)                                 |



# DECLARACIÓN DE USO DE INTELIGENCIA ARTIFICIAL

Durante la elaboración del Trabajo Fin de Grado se empleó la herramienta *Microsoft Copilot* (que implementa el motor GPT-5) como apoyo en diferentes fases del desarrollo. Su utilización se centró en la asistencia técnica para la comprensión y aplicación de conceptos relacionados con la simulación de redes *LoRa* en entornos como *NS-3* y *OMNeT++*, así como en la definición de estrategias para la implementación en dispositivos Raspberry Pi 5 y ESP32-S3. Además, se recurrió a la herramienta para la generación y optimización de fragmentos de código en lenguajes como Python y C++, orientados a la simulación y comunicación mediante *LoRa*. También se empleó para mejorar la redacción del documento, garantizando la claridad y coherencia del lenguaje, y para organizar la estructura general del trabajo, incluyendo la descripción técnica de los prototipos. Además, se ha utilizado la herramienta de generación de imágenes para la mejora de la calidad visual de aquellas imágenes originales de las que no se observaba bien su contenido.

Durante la elaboración del presente Trabajo Fin de Grado se ha utilizado la herramienta de inteligencia artificial *ChatGPT*, basada en el modelo GPT-5 de *OpenAI*, con el objetivo de optimizar el proceso de redacción, análisis y estructuración del documento. Su uso se ha centrado en tareas de apoyo relacionadas con la mejora del estilo y la coherencia del texto, la reformulación de este para lograr una redacción más clara y técnica, la elaboración de resúmenes y conclusiones a partir de contenidos previamente desarrollados por el autor, así como en la organización y presentación de la información de manera más uniforme y precisa. En ningún caso la herramienta ha intervenido en la definición de la metodología, el análisis de los resultados ni en la interpretación de los datos, funciones que corresponden íntegramente al autor del trabajo.

Se ha hecho uso de la versión Pro de Gemini para el análisis de datos obtenidos durante el transcurso del proyecto para la elaboración de tablas, así como se ha utilizado su motor de creación de imágenes NaNo Banana Pro para mejorar la claridad de esquemas realizados por el autor.

El uso de inteligencia artificial se ha limitado, por tanto, a un papel complementario de asistencia en la redacción, manteniéndose en todo momento la autoría, el criterio técnico y la responsabilidad final del contenido por parte del estudiante. En todo momento, los datos introducidos en la herramienta se limitaron a información técnica del proyecto y a fragmentos del texto del TFG, sin incluir datos personales ni información confidencial, asegurando así la integridad y seguridad de la información utilizada.



# 1. INTRODUCCIÓN

El avance tecnológico experimentado en las últimas décadas ha transformado la naturaleza de los entornos operativos militares, caracterizados actualmente por una elevada densidad informativa y una dependencia creciente de las tecnologías CIS [1]. En este contexto, la toma de decisiones rápidas y precisas requiere disponer de información fiable y actualizada, lo que ha impulsado el desarrollo de tecnologías que integran la adquisición, procesamiento y transmisión de datos de manera autónoma y segura en el menor tiempo posible.

La aplicación de conceptos derivados del *IoT* al ámbito de defensa denominado *IoBT* se presenta como una respuesta a estas necesidades. El *IoBT* busca aprovechar la conectividad y capacidad de procesamiento de dispositivos inteligentes para crear redes distribuidas capaces de operar de manera cooperativa en entornos adversos y con infraestructuras de comunicación limitadas. Sin embargo, la literatura técnica muestra un vacío significativo en la implementación de soluciones prácticas que integren sensores heterogéneos, redundancia multisensorial y protocolos de comunicación de bajo consumo adaptados a escenarios tácticos degradados.

Esta necesidad de investigación y desarrollo fue reflejada en 2018 por el Ministerio de Defensa de España en su publicación "Entorno Operativo 2035" [2]. Es por esto que el presente TFG tratará de dar ideas de implementación de *IoBT* para su aplicación en un sistema de vigilancia y mando haciendo uso de la una red *LoRa*. El concepto de *IoBT* es demasiado amplio como para explorarlo en un único TFG de modo que este se centrará en una de las principales tecnologías usadas en la automatización de la industria civil (*LoRa*) aplicada al ámbito militar.

## 1.1. Justificación

El presente Trabajo de Fin de Grado se justifica por su contribución al desarrollo de sistemas de vigilancia y sensado autónomos capaces de operar bajo condiciones de baja conectividad y alta interferencia electromagnética. Estos sistemas resultan de especial interés para operaciones militares, misiones de inteligencia, vigilancia de perímetros o control de fronteras, donde la fiabilidad de la información es determinante para la seguridad operativa.

Desde el punto de vista práctico, el trabajo propone una arquitectura basada en sensores inteligentes interconectados mediante tecnología *LoRa*, que destaca por su bajo consumo energético, su alcance extendido y su robustez frente a interferencias. Este enfoque permite ofrecer una solución de bajo coste y alta resiliencia frente a los sistemas tradicionales de comunicación o vigilancia, generalmente dependientes de redes centralizadas o infraestructura de telecomunicaciones preexistente.

Además, la investigación aborda la fusión de datos provenientes de sensores ópticos y térmicos, mejorando la precisión de la detección y reduciendo los falsos positivos. La combinación de estas tecnologías contribuye a cerrar un vacío existente en la literatura, donde la mayoría de los estudios tratan de forma aislada las problemáticas de sensorización, conectividad o autonomía energética.

A partir del análisis de la literatura, se evidencian vacíos relevantes que sustentan la realización de este trabajo. En primer lugar, no se han encontrado estudios que integren en un único nodo emisor, basado en Raspberry Pi, la detección de imagen y movimiento junto con la transmisión mediante *LoRa*, incorporando además procesamiento local y autonomía energética. Asimismo, la exploración de enlaces *LoRa* multipunto que empleen cifrado XOR y mecanismos de pseudo salto de frecuencia resulta escasa, especialmente en escenarios tácticos o de guerra electrónica donde estas características son críticas. Finalmente, se observa la ausencia de soluciones que contemplen el almacenamiento local de mensajes ante la falta de conectividad *LoRa*, un aspecto fundamental para garantizar la operatividad en entornos con conectividad intermitente.

Desde una perspectiva académica, este trabajo aporta conocimiento al campo de los



sistemas embebidos, el *IoT* aplicado al entorno militar y las estrategias de comunicación seguras en escenarios degradados. De igual modo, sienta las bases para futuras investigaciones orientadas a la validación experimental y al despliegue de redes distribuidas de sensores autónomos en condiciones reales.

Finalmente, desde un punto de vista personal, la elección del tema responde al interés por integrar los ámbitos de la ingeniería electrónica, las telecomunicaciones y la defensa, aportando soluciones innovadoras que contribuyan al desarrollo tecnológico de las Fuerzas Armadas españolas en consonancia con los objetivos definidos en el documento “Entorno Operativo 2035” del Ministerio de Defensa [2].

## **1.2. Ámbito de aplicación**

El sistema diseñado está concebido para su aplicación en entornos operacionales caracterizados por la baja o nula conectividad, interferencias electromagnéticas y condiciones ambientales adversas. Estos escenarios comprenden tanto operaciones militares en zonas sin infraestructura de comunicaciones como misiones de observación o respuesta ante desastres naturales, donde las redes convencionales resultan insuficientes o inoperativas.

La principal aportación práctica del trabajo radica en el desarrollo de una red de sensores inteligentes capaces de recopilar información de manera autónoma, procesarla localmente y transmitir alertas mediante una red de comunicación de largo alcance y bajo consumo. Los resultados del estudio pueden aplicarse al diseño de sistemas de vigilancia perimetral, detección de intrusiones o monitorización de actividad en áreas críticas, garantizando la continuidad operativa incluso en presencia de interferencias o intentos de inhibición de señales.

El público objetivo incluye unidades militares de reconocimiento y vigilancia, cuerpos de seguridad y equipos de emergencia que operen en entornos sin infraestructura establecida. El uso de componentes comerciales de bajo coste y libre disponibilidad permite además que la tecnología desarrollada sea accesible y adaptable a distintos niveles operativos, implementando despliegues en campo según necesidad.

No obstante, el estudio presenta limitaciones inherentes a su carácter de simulación. La validación de la red y del algoritmo de integración multisensorial se realiza en un entorno virtual que reproduce condiciones de conectividad degradada, pero no incluye pruebas físicas ni exposición prolongada a factores ambientales. Estas restricciones pueden afectar a la aplicabilidad directa de los resultados, aunque no comprometen su validez teórica ni su utilidad como base para futuros desarrollos experimentales.

En términos de impacto práctico, los resultados de esta investigación pueden contribuir a la optimización de sistemas de comunicación descentralizados en defensa y seguridad, fomentando el uso de arquitecturas distribuidas más seguras y energéticamente sostenibles. Asimismo, su extrapolación al ámbito civil podría favorecer el desarrollo de soluciones de monitoreo ambiental, agricultura de precisión o protección de infraestructuras críticas en zonas rurales o aisladas.

## **1.3. Contextualización**

El entorno operativo que motiva este trabajo se enmarca en un escenario de transformación digital de las Fuerzas Armadas, donde la interoperabilidad, la autonomía y la resiliencia de los sistemas tecnológicos son elementos clave para mantener la superioridad informativa. La creciente sofisticación de las capacidades de guerra electrónica y cibernética obliga a desarrollar soluciones que minimicen la dependencia de infraestructuras vulnerables y permitan mantener el flujo de información incluso bajo condiciones de interferencia o degradación del espectro



electromagnético.

Dentro de este contexto, el uso de redes distribuidas de sensores constituye una estrategia esencial para mejorar la capacidad de vigilancia y reconocimiento. La integración de sensores ópticos y térmicos, junto con algoritmos de fusión de datos y protocolos de comunicación *LoRa*, permite conformar sistemas flexibles y escalables, capaces de operar de manera autónoma en zonas extensas sin supervisión continua.

El presente trabajo se desarrolla en el marco del Centro Universitario de la Defensa, alineado con las líneas de investigación orientadas a la modernización tecnológica del Ejército de Tierra y la aplicación de principios de ingeniería al ámbito táctico y operativo. En este contexto institucional, la investigación contribuye a explorar la viabilidad técnica de un modelo de red *IoT* militar, basada en redundancia multisensorial y comunicación segura, que responda a los requisitos definidos en los escenarios futuros de operaciones previstos para 2035.

De este modo, la contextualización del estudio se sitúa en la confluencia entre la ingeniería de sistemas embebidos, la tecnología *IoT* y las necesidades estratégicas de defensa, proporcionando una solución aplicable a la vigilancia autónoma y resiliente en entornos de baja conectividad.

## 1.4. Estructura de la memoria y plan de trabajo

La memoria se organiza conforme a la estructura establecida por el Centro Universitario de la Defensa [3], articulándose en cinco apartados principales. En el primero, se expone la justificación y contextualización que motivan la realización del proyecto. El segundo apartado desarrolla la metodología empleada para alcanzar los objetivos propuestos. El tercero presenta las bases teóricas y conceptuales que sustentan el trabajo, sirviendo de fundamento para el cuarto capítulo, en el que se lleva a cabo el desarrollo técnico y el análisis de la propuesta. Finalmente, el quinto apartado recoge las conclusiones derivadas del estudio y las aportaciones más relevantes del proyecto. El trabajo desarrollado se ha estructurado en las siguientes etapas:

**Etapas 0.** Definición del alcance, cronograma y recursos. Se establecieron los objetivos específicos, el alcance técnico y temporal, así como los recursos materiales y software necesarios. La planificación se realizó con *Excel* y *Canva* [4], siguiendo las directrices del CUD.

**Etapas 1.** Estudio del marco teórico y análisis de sistemas similares. Se efectuó una revisión bibliográfica sobre *IoT*, sistemas embebidos y redes *LoRa* aplicadas al ámbito militar, comparando soluciones del Ejército de Tierra y del sector civil. Se empleó *Zotero* [5] para la gestión de referencias y *Word* para la síntesis documental.

**Etapas 2.** Diseño de la arquitectura hardware, algoritmo y protocolo. Se desarrolló el diseño del nodo sensor inteligente, la selección de componentes electrónicos y el algoritmo de fusión multisensorial. Asimismo, se definieron los parámetros del protocolo *LoRa* e implementaron medidas de protección frente a interferencias electrónicas.

**Etapas 3.** Simulación y modelado. Se validó el diseño mediante simulaciones en *NS-3*, analizando distintas topologías y condiciones de conectividad. El algoritmo de fusión se modeló con *Bizagi Modeler* y *Visual Studio Code* (Python y C++).

**Etapas 4.** Desarrollo del prototipo e implementación del *firmware*. Se integraron los componentes seleccionados y se diseñó la carcasa para impresión 3D. El *firmware* se programó en Python y C++, verificando la interoperabilidad y comunicación de los módulos *LoRa* y sensores.

**Etapas 5.** Análisis de resultados y evaluación DAFO. Se analizaron los datos de simulación con *Excel* y Python, comprobando el cumplimiento de los requisitos. Se elaboró un análisis DAFO para determinar la viabilidad técnica y estratégica del sistema.

**Etapas 6.** Redacción de la memoria. Finalmente, se estructuró la memoria en función de las experiencias y resultados de las fases previas, integrando resultados obtenidos y conclusiones.



Figura 1. Diagrama de Gannt. Fuente: elaboración propia

## 2. OBJETIVOS Y METODOLOGÍA

### 2.1. OBJETIVOS

#### 2.1.1. Objetivo principal

El objetivo principal será diseñar y validar mediante simulación un prototipo de nodo sensor autónomo y resistente, capaz de detectar movimiento de forma fiable mediante fusión de datos de cámara y láser, y transmitir las alertas mediante una red de comunicación *LoRa* segura y robusta, específicamente diseñada para operar en escenarios de baja conectividad y bajo la amenaza de interceptación propia de la guerra electrónica.

#### 2.1.2. Objetivos secundarios

- Definir los requisitos de alto nivel del sistema, centrándose en la fiabilidad de la detección, la autonomía energética, la capacidad de operar en entornos con conectividad intermitente y la resistencia a técnicas de interceptación y *jamm*ing.
- Diseñar la estrategia de redundancia multisensorial y el algoritmo de fusión de datos que permita, a nivel de nodo, discriminar falsos positivos y confirmar detecciones de movimiento mediante la corroboración entre el sensor de cámara y el sensor láser.
- Diseñar el protocolo de comunicación para la red *LoRa*, el cual deberá ser de bajo consumo y permitir el almacenamiento y reenvío de datos a la vez que incorporar técnicas de ofuscación y cifrado ligero para minimizar el riesgo de detección e interceptación.
- Diseñar la arquitectura hardware del dispositivo sensor, seleccionando los componentes críticos (microcontrolador, módulo *LoRa*, sensores, fuente de alimentación) que cumplan con los requisitos de consumo, coste y resistencia a factores medioambientales.
- Validar el diseño mediante simulación software de los protocolos de comunicación y del algoritmo de fusión de sensores, evaluando métricas de fiabilidad sobre detección, latencia de la red, consumo energético y resistencia a interferencias.

### 2.2. ALCANCE

El presente Trabajo de Fin de Grado se enfoca en el diseño conceptual y la validación mediante simulación de un nodo sensor autónomo, robusto y energéticamente eficiente, destinado a la detección fiable de movimiento en entornos hostiles. El sistema propuesto integra





técnicas de fusión de datos provenientes de una cámara digital y un sensor láser, con el objetivo de mejorar la precisión en la detección de presencia humana o actividad relevante. La transmisión de alertas se realiza a través de una red de comunicación *LoRa*, configurada con mecanismos de seguridad como cifrado XOR y pseudo salto de frecuencia, para garantizar la integridad y confidencialidad de los datos en escenarios de baja conectividad y alta interferencia electromagnética, como los generados por guerra electrónica.

La relevancia de este trabajo radica en su aplicabilidad a contextos donde las infraestructuras de comunicación convencionales son inoperantes o vulnerables, como zonas de conflicto, operaciones militares, o entornos de desastre natural. La propuesta busca contribuir al desarrollo de sistemas de vigilancia autónomos que puedan operar de forma resiliente ante condiciones adversas, minimizando la dependencia de redes centralizadas y fuentes de energía convencionales.

El estudio se circunscribe a un entorno simulado que representa escenarios operacionales militares, caracterizados por conectividad intermitente, presencia de interferencias electrónicas intencionadas y condiciones ambientales extremas. No se contempla la realización de pruebas en campo ni en situaciones reales de combate, limitándose a simulaciones controladas en laboratorio que emulan condiciones representativas. El alcance temporal del trabajo abarca exclusivamente las fases de diseño, simulación y validación virtual del prototipo, sin incluir etapas posteriores de producción industrial ni despliegue operativo.

Dentro del marco del estudio se abordarán los siguientes aspectos técnicos:

- Diseño del nodo sensor con enfoque en bajo consumo energético y autonomía operativa.
- Integración de sensores ópticos y láser para la detección de movimiento.
- Implementación de protocolos de comunicación *LoRa* con seguridad básica.
- Simulación del comportamiento del sistema en entornos degradados mediante herramientas como NS-3.
- Evaluación de la viabilidad técnica del sistema en condiciones simuladas de guerra electrónica.

Aunque el sistema no está orientado a una población civil específica, su diseño está pensado para ser utilizado por unidades militares, cuerpos de seguridad o equipos de respuesta ante emergencias que operen en zonas de difícil acceso o con infraestructura comprometida.

Las principales limitaciones del trabajo derivan de su enfoque simulado. Al no realizarse pruebas en entornos de combate reales, la validez de los resultados depende directamente de la fidelidad de los modelos de simulación empleados. Asimismo, no se contempla la fabricación física del prototipo ni su integración en sistemas operativos existentes, lo que limita la extrapolación directa de los resultados a aplicaciones prácticas inmediatas.

Quedan fuera del alcance del estudio los siguientes aspectos:

- Desarrollo de interfaces gráficas de usuario para el sistema.
- Evaluación de impacto económico o logístico del despliegue del sistema.
- Integración con plataformas de inteligencia artificial para análisis avanzado de imágenes.
- Validación en redes *LoRaWAN* comerciales o infraestructura de telecomunicaciones existente.

Se espera que este trabajo proporcione una base sólida para el desarrollo de sistemas de vigilancia autónomos en entornos hostiles, demostrando su viabilidad técnica mediante simulación. El prototipo virtual validado podrá servir como punto de partida para futuras investigaciones orientadas a su implementación física, optimización energética y adaptación a escenarios operativos reales. Además, se pretende fomentar el uso de tecnologías de bajo coste



y alta resiliencia en aplicaciones críticas de seguridad y defensa.

## 2.3. METODOLOGÍA

El proyecto se enmarca dentro de un enfoque descriptivo-aplicativo, ya que busca no solo describir y explorar tecnologías como *LoRa*, detección de señales y cifrado, sino también explicar cómo interactúan estos elementos en un entorno operativo concreto. El objetivo es comprender las causas y efectos de las decisiones de diseño técnico en el rendimiento del sistema, especialmente en contextos de comunicación segura y detección remota. Este enfoque permite establecer relaciones causales entre variables como el tipo de cifrado, la frecuencia de transmisión y la eficiencia energética.

Se empleará un método mixto, con predominancia del método deductivo, ya que el desarrollo parte de principios teóricos consolidados como la teoría de comunicaciones, la teoría de detección de señales y fundamentos de criptografía para derivar un diseño específico. A partir de estos marcos teóricos, se formularán hipótesis sobre el rendimiento del sistema, que serán posteriormente validadas mediante pruebas experimentales. El componente inductivo se incorpora en la fase inicial, donde se analiza el entorno operativo y se ajustan los requisitos técnicos a las condiciones reales del campo de aplicación.

La metodología será híbrida, integrando elementos cuantitativos y cualitativos.

- En la fase cualitativa, se realizará una revisión exhaustiva de literatura científica, manuales técnicos y documentación de estándares, además de un análisis del entorno operativo (por ejemplo, condiciones del terreno, interferencias, necesidades tácticas), con el fin de identificar requisitos técnicos y operativos.
- En la fase cuantitativa, se aplicarán simulaciones y pruebas experimentales para medir el rendimiento del sistema, incluyendo métricas como latencia, tasa de pérdida de paquetes, consumo energético y robustez frente a interferencias. Esta metodología mixta permite garantizar tanto la validez conceptual como la validez empírica del diseño propuesto.

Para el desarrollo y validación del proyecto se emplearán diversas herramientas técnicas, entre ellas:

- Software de simulación: NS-3 para simular redes *LoRa* con salto de frecuencia y cifrado XOR.
- Plataformas de diseño: *Visual Studio Code* para el desarrollo de código en Python y C++, y herramientas de modelado como *Fritzing* o *KiCad* para el diseño de prototipos electrónicos.
- Hardware: *Raspberry Pi 5*, ESP32-S3 zero, sensores PIR AM 312, módulos *LoRa* RYLR998 y batería de 50000 mAh.
- Plataformas de visualización: *ThingsBoard* para la visualización remota de datos, y una interfaz web local accesible por IP.



## 3. ANTECEDENTES Y MARCO TEÓRICO

### 3.1. Antecedentes

El desarrollo de sistemas de comunicación inalámbrica de bajo consumo energético y alta resiliencia ha cobrado especial relevancia en el contexto de aplicaciones tácticas, vigilancia autónoma y entornos degradados. En este marco, la tecnología *LoRa* (*Long Range*), basada en modulación *Chirp Spread Spectrum* (CSS), se ha consolidado como una solución eficaz para enlaces punto a punto, permitiendo la transmisión de datos a larga distancia sin necesidad de infraestructura de red ni servidores intermedios [6].

Diversos trabajos han abordado el uso de *LoRa* en sistemas de comunicación directa. Por ejemplo, en un estudio se desarrolló una red punto a punto con tecnología *LoRa* y servidor web, demostrando su viabilidad en aplicaciones de sensado distribuido sin necesidad de *LoRaWAN* [7]. De forma complementaria, Martos Núñez (2021) diseñó un sistema *IoT* basado en *LoRa* punto a punto para monitoreo ambiental en ganadería, utilizando *Raspberry Pi* como nodo emisor, lo que evidencia la aplicabilidad de esta arquitectura en entornos rurales y aislados [8].

En el ámbito de la detección de movimiento e imagen, múltiples investigaciones han validado el uso de *Raspberry Pi* como plataforma de procesamiento local. El proyecto PiVision Lab [9] ha demostrado la capacidad de la *Raspberry Pi* 4 y 5 para ejecutar modelos de inteligencia artificial en tiempo real mediante cámaras IMX500, permitiendo la detección de objetos sin necesidad de procesamiento en la nube. Asimismo, se describe cómo implementar un sistema de detección de movimiento con *Raspberry Pi* y Python, utilizando técnicas de comparación de imágenes sucesivas para activar alarmas o grabaciones [10].

En cuanto a la integración de sensores PIR y cámaras en *Raspberry Pi*, se propuso un sistema de seguridad escolar que utiliza sensores PIR y cámaras conectadas a una *Raspberry Pi*, transmitiendo alertas mediante *Telegram* [11]. Aunque el sistema no emplea *LoRa*, demuestra la viabilidad de la arquitectura basada en procesamiento local y sensores múltiples [12].

La seguridad en redes *LoRa* punto a punto ha sido objeto de estudio en trabajos como el de Martínez Calle (2023) [13], quien identificó vulnerabilidades críticas en la capa física del protocolo *LoRa*, incluyendo ataques de inhibición y suplantación de mensajes con una efectividad del 93%. Estos hallazgos evidencian la necesidad de implementar mecanismos de protección adicionales, como el cifrado XOR y el pseudo salto de frecuencia, especialmente en aplicaciones sensibles y entornos hostiles.

Rojas Giraldo (2024) [14] realizó pruebas de seguridad en el espectro de 915 MHz, validando la posibilidad de capturar y manipular paquetes *LoRa* mediante hardware básico, lo que refuerza la importancia de diseñar sistemas con medidas de seguridad en la capa física.

Por tanto, el presente TFG propone el diseño, implementación y validación virtual de un sistema de detección autónomo que integra sensores PIR, cámara y transmisión segura por *LoRa*, con simulación detallada de su comportamiento en entornos hostiles. Esta contribución busca avanzar en el desarrollo de soluciones resilientes, escalables y de bajo coste para aplicaciones de seguridad y vigilancia en condiciones extremas.

### 3.2. Bases teóricas

#### 3.2.1. *LoRa*

*LoRa* [15] es un sistema de telecomunicaciones inalámbrico de largo alcance, bajo consumo y baja tasa de bits, promovido como una solución de la infraestructura del internet de las cosas. Los dispositivos finales utilizan *LoRa* a través de un salto inalámbrico para comunicarse con las puertas de enlace conectadas a Internet, que actúan como puentes transparentes y retransmiten



mensajes entre estos dispositivos finales y un servidor de red central [16].

*LoRa* es una tecnología perteneciente a la empresa *Semtech* [17], la capa física de *LoRa* se fundamenta en la modulación por espectro ensanchado (CSS), lo cual le permite alcanzar distancias de varios kilómetros con un consumo energético reducido y es por eso que es ampliamente usado en escenarios de monitorización ambiental, ciudades inteligentes y sistemas industriales.

Complementando lo anterior, es importante destacar que la tecnología *LoRa* no solo se caracteriza por su eficiencia en la capa física, sino también por el modelo de red que posibilita su escalabilidad y fiabilidad en entornos con un gran número de nodos. [15] *LoRa* permite establecer topologías de red tipo estrella, en las que los nodos finales se comunican directamente con uno o varios *Gateways* sin necesidad de saltos intermedios. Esta arquitectura simplifica el diseño y reduce la latencia de comunicación, ya que las puertas de enlace se encargan únicamente de retransmitir los paquetes hacia el servidor o la aplicación final, manteniendo el consumo energético de los dispositivos remotos en niveles mínimos. La combinación de su largo alcance y bajo consumo energético convierte a *LoRa* en una alternativa especialmente adecuada para aplicaciones donde los dispositivos operan de forma autónoma durante largos periodos, como el monitoreo agrícola, la gestión de recursos hídricos o el control de infraestructuras urbanas inteligentes.

Asimismo, *LoRa* presenta mecanismos internos que optimizan la coexistencia de múltiples nodos en un mismo canal. La modulación CSS otorga una alta inmunidad al ruido y permite la coexistencia de transmisores con distintos factores de expansión, posibilitando que múltiples dispositivos transmitan de manera simultánea sin colisiones significativas. [18] Esta característica, junto con la capacidad de configurar parámetros como el ancho de banda y la tasa de codificación, proporciona a *LoRa* una gran versatilidad operativa en comparación con otras tecnologías LPWAN. A nivel práctico, esta flexibilidad se traduce en un control más preciso del equilibrio entre alcance, robustez y velocidad de transmisión, permitiendo adaptar el rendimiento del enlace a las condiciones ambientales o topográficas del entorno de despliegue. Gracias a ello, *LoRa* puede integrarse tanto en redes privadas, donde se requiere control total sobre la infraestructura, como en entornos mixtos con distintos niveles de cobertura y densidad de nodos.

La modulación CSS utiliza señales de frecuencia creciente o decreciente de manera lineal en el tiempo, para codificar la información. Esto le confiere robustez frente a interferencias y variaciones de frecuencia así como inmunidad al efecto *Doppler* [19]. Además, permite que transmisores de bajo costo operen sin requerir osciladores de alta precisión [20].

La capa física de *LoRa* opera principalmente en bandas ISM no licenciadas (433, 868 y 915 MHz) [21], con tasas de datos que van desde los cientos de bps hasta aproximadamente 50 kbps. Su sensibilidad de recepción puede alcanzar valores de hasta -136 dbm, lo que la hace altamente eficiente para enlaces de largo alcance.

La flexibilidad de *LoRa* proviene de tres parámetros configurables [22]. El primero, el ancho de banda que determina la tasa y rendimiento global de transmisión. El segundo, el factor de expansión, a mayor SF (factor de expansión), mayor sensibilidad y alcance, pero menor velocidad de datos. Por último, la tasa de codificación que introduce redundancia mediante códigos de corrección de errores mejorando la resistencia a interferencias. El compromiso entre estos parámetros permite adaptar la comunicación según las necesidades: alcance máximo, mayor robustez o velocidad de transmisión.

Pruebas experimentales han demostrado que *LoRa* puede mantener enlaces estables en entornos urbanos de hasta 3 km y en áreas rurales de hasta 15 Km, dependiendo del factor de expansión utilizado [23]. El aumento del SF (Anexo I ) mejora significativamente la cobertura, a costa de reducir la velocidad de transmisión [24]. Aumentar el SF incrementa el número de chips por símbolo, lo que mejora la sensibilidad del receptor y permite alcanzar distancias mayores o superar obstáculos en entornos complejos, como áreas urbanas o forestales. Sin embargo, este beneficio en cobertura se obtiene a costa de una reducción significativa en la tasa de datos, ya



que los símbolos requieren más tiempo para transmitirse. Diversos estudios académicos han confirmado esta relación inversa entre SF y velocidad, destacando que una asignación adecuada del SF es esencial para optimizar el rendimiento de la red según las necesidades específicas de cada aplicación [25].

Los receptores *LoRa* destacan por su sensibilidad, que supera la de modulaciones tradicionales como FSK. Esto permite que dispositivos con potencias de transmisión reducidas logren cubrir grandes áreas siempre que haya distancia visual entre emisor y receptor. Los ensayos de Augustin et al. (2016) muestran que, con un salto SF alto (12), se consigue una tasa de entrega superior al 80% a distancias cercanas a 3 km en entornos urbanos densos [16].

En comparación con otras tecnologías LPWAN, como *Sigfox* o *NB-IoT*, *LoRa* ofrece mayor flexibilidad de configuración, lo que facilita adaptarse a diversos escenarios. Mientras que *Sigfox* se limita a mensajes muy pequeños y *NB-IoT* requiere infraestructura celular, *LoRa* permite despliegues privados con control total sobre la red física [26].

En resumen, la capa física de *LoRa* constituye un núcleo tecnológico que permite comunicaciones inalámbricas de largo alcance y bajo consumo. Su diseño basado en CSS, junto con parámetros ajustables (BW, SF, CR), proporciona una versatilidad única frente a interferencias y condiciones adversas de propagación. Estos aspectos la posicionan como una solución sólida para aplicaciones *IoT* que demandan autonomía energética, bajo costo y conectividad en zonas extensas.

### 3.2.2. Detección de movimiento e imagen por cámara

La *Raspberry Pi 5* [27] representa una evolución significativa en capacidad de procesamiento, permitiendo la ejecución de algoritmos de visión por computador en tiempo real. Gracias a su compatibilidad con cámaras como la IMX500 y librerías como *OpenCV*, es posible implementar sistemas de detección de movimiento e identificación de objetos sin necesidad de procesamiento en la nube [28].

Esta capacidad ha sido ampliamente validada en la literatura técnica. Por ejemplo, un estudio [29] destaca que la *Raspberry Pi 5*, en combinación con algoritmos optimizados como YOLO y bibliotecas como *OpenCV*, permite realizar detección de objetos en tiempo real directamente en el borde (*edge computing*), reduciendo la latencia y eliminando la dependencia de redes externas. Esta arquitectura mejora la privacidad, la eficiencia energética y la robustez del sistema, aspectos clave en aplicaciones de vigilancia, robótica y sistemas autónomos.

Asimismo, ha sido desarrollado un sistema de reconocimiento facial basado en *Raspberry Pi*, demostrando que esta plataforma es capaz de procesar flujos de vídeo en tiempo real con alta precisión, incluso bajo condiciones operativas reales [30]. El sistema utilizó modelos preentrenados y bibliotecas como *OpenCV*, *Dlib* y *Picamera2*, optimizados para las limitaciones de hardware de la *Raspberry Pi*, logrando un equilibrio entre rendimiento y consumo de recursos.

A. L. Zekovic [31] también subraya que la integración de visión por computador en sistemas *IoT* basados en *Raspberry Pi* ha permitido el desarrollo de soluciones inteligentes en áreas como seguridad, agricultura, salud y ciudades inteligentes. La combinación de procesamiento local, sensores y algoritmos de inteligencia artificial ha demostrado ser una estrategia eficaz para implementar sistemas autónomos, escalables y de bajo coste.

La detección de movimiento en sistemas embebidos puede abordarse desde múltiples enfoques. Uno de los más comunes es el análisis de imágenes sucesivas mediante visión por computadora, donde se aplican técnicas como la sustracción de fondo, el cálculo de diferencias de píxeles y la generación de máscaras binarias para identificar cambios significativos en la escena. Este enfoque, aunque potente, puede verse limitado en condiciones de baja visibilidad o iluminación deficiente. Por ello, es habitual complementar la detección visual con sensores de tipo térmico, como los sensores PIR, que permiten detectar la presencia de cuerpos humanos o animales a partir de la radiación infrarroja que emiten.



Los sensores PIR se basan en el principio de detección de radiación infrarroja emitida por cuerpos con temperatura superior al cero absoluto. Todo objeto con temperatura emite radiación electromagnética en el espectro infrarrojo, y los sensores PIR están diseñados para captar las variaciones de esta radiación cuando un objeto entra o sale de su campo de visión [32].

El componente central de un sensor PIR es un sensor piroeléctrico, fabricado con materiales que generan una carga eléctrica cuando se exponen a cambios en la radiación infrarroja. Esta señal eléctrica, de muy baja intensidad, es amplificada y procesada por un circuito comparador que genera una salida digital cuando se detecta un cambio significativo en la radiación [32]. Para mejorar la sensibilidad y cobertura, los sensores PIR incorporan una lente de Fresnel, que divide el campo de visión en múltiples zonas. Esto permite detectar el movimiento de un cuerpo al pasar de una zona a otra, generando una señal de activación más precisa y reduciendo las falsas alarmas.

### 3.3. Estado del arte

El desarrollo de sistemas embebidos para la detección de movimiento en exteriores ha cobrado relevancia en el contexto de aplicaciones de vigilancia autónoma, agricultura de precisión, y monitoreo ambiental. Estos sistemas integran tecnologías de monitoreo, procesamiento local, comunicación inalámbrica y almacenamiento energético, optimizadas para operar en condiciones variables y con restricciones de consumo energético.

#### 3.3.1. Tecnología actual

Los sensores PIR se emplean ampliamente en la detección de movimiento por su bajo consumo energético y simplicidad de integración. En entornos exteriores, su desempeño depende de factores como la sensibilidad térmica, el diseño óptico y la capacidad de filtrado de interferencias ambientales. Estudios recientes destacan la necesidad de sensores PIR con mayor robustez frente a variaciones de temperatura y radiación solar, así como una mejor adaptación a plataformas como *Raspberry Pi* mediante interfaces digitales estables [33].

La visión artificial, aplicada mediante sistemas embebidos como *Raspberry Pi*, ha demostrado ser eficaz en tareas de reconocimiento de objetos, clasificación y seguimiento en tiempo real. Investigaciones han validado el uso de bibliotecas como *OpenCV* y *TensorFlow Lite* para ejecutar modelos de aprendizaje automático en dispositivos de bajo coste, logrando una detección precisa en condiciones de iluminación variable. La combinación de sensores PIR y visión artificial permite mejorar la fiabilidad del sistema, reduciendo falsos positivos y optimizando la respuesta ante eventos relevantes.

En cuanto a la comunicación, la tecnología *LoRa* se ha consolidado como una solución de largo alcance y bajo consumo para entornos sin infraestructura de red. Su modulación de espectro ensanchado tipo CSS permite transmisiones robustas en presencia de ruido y obstáculos físicos. Investigaciones han explorado el uso de cifrado ligero, como XOR, en sistemas *LoRa* para mejorar la seguridad sin comprometer la eficiencia energética, especialmente en aplicaciones donde los recursos computacionales son limitados [34].

#### 3.3.2. Avances recientes

Los avances en sensores PIR para exteriores han mejorado la capacidad de detección en condiciones adversas mediante el uso de lentes ópticas optimizadas y algoritmos de compensación térmica. Asimismo, la visión artificial ha evolucionado hacia modelos de inferencia optimizados para hardware limitado, permitiendo la ejecución de redes neuronales convolucionales en tiempo real sobre plataformas como *Raspberry Pi*.

En el ámbito de la comunicación, se han propuesto esquemas de mecanismos de seguridad complementarios en redes *LoRa*, especialmente en aplicaciones donde la implementación de *LoRaWAN* resulta inviable por coste o complejidad [35].





Por otro lado, el uso de baterías de gran capacidad ha permitido extender la autonomía de sistemas embebidos en exteriores, facilitando su operación continua sin necesidad de recarga frecuente. La literatura enfatiza la necesidad de seleccionar materiales sostenibles y eficientes para los componentes internos de las baterías, considerando también la sostenibilidad de la cadena de suministro [36].

### 3.3.3. Comparación crítica

En comparación con soluciones comerciales de videovigilancia, los sistemas embebidos basados en *Raspberry Pi* presentan ventajas en términos de flexibilidad, coste y personalización. Sin embargo, enfrentan desafíos relacionados con la robustez frente a condiciones ambientales, la seguridad de la transmisión y la gestión energética.

Los sensores PIR convencionales pueden presentar limitaciones en exteriores, mientras que los modelos optimizados para ambientes abiertos ofrecen mayor fiabilidad a costa de un incremento en el consumo y el coste. La visión artificial mejora la precisión, pero requiere una gestión eficiente de los recursos computacionales.

La tecnología *LoRa*, aunque eficaz en términos de alcance y consumo, presenta limitaciones en ancho de banda y seguridad. El uso de cifrado ligero como XOR es adecuado para aplicaciones de bajo riesgo, pero no sustituye protocolos criptográficos robustos como AES [34].

Finalmente, las baterías de alta capacidad permiten una autonomía prolongada, pero requieren una gestión térmica adecuada y una integración eficiente con el sistema embebido para evitar degradación prematura [37].

Entre los medios en dotación del ET tecnológicamente más afines al sistema desarrollado en este trabajo destacan los sistemas de localización acústica de lanzamiento/impacto, representados por soluciones comerciales como SORAS 6E [38] y HALO [39]. Ambos sistemas emplean una red de sensores acústicos (micrófonos de alta sensibilidad) distribuidos sobre el área de interés y conectados a una unidad de procesamiento que estima parámetros balísticos para determinar la posición de impacto de un proyectil o el origen de un disparo (posición del lanzador).

Desde el punto de vista arquitectónico, la diferencia principal entre ambos radica en el método de comunicación de la red de sensores: SORAS 6E utiliza enlaces cableados para la transmisión de datos hacia la unidad de cálculo, mientras que HALO emplea comunicación inalámbrica. Esta última característica puede implicar ventajas en rapidez de despliegue y flexibilidad operacional, si bien, en implementaciones reportadas, el tiempo medio de respuesta de sistemas inalámbricos comparables se sitúa en torno a los 15 segundos. En cualquier caso, la eficacia global depende de la sincronización temporal de los sensores, la precisión de los modelos balísticos empleados y las condiciones ambientales [40].

## 3.4. Amenazas de la Guerra Electrónica

La EW comprende el conjunto de acciones militares destinadas a controlar o explotar el espectro electromagnético, afectando directamente a los sistemas que operan mediante radiofrecuencia (RF). Las comunicaciones por RF, que constituyen la base de los sistemas de radar, enlace de datos, navegación y mando y control, resultan especialmente vulnerables a las operaciones de guerra electrónica.

El ataque electrónico busca degradar, denegar o destruir las capacidades del adversario mediante la emisión deliberada de energía electromagnética. Las técnicas de *jamming* (interferencia intencionada) son su principal herramienta. Estas pueden clasificarse en *jamming* de ruido, que incrementa el nivel de ruido en el receptor del enemigo hasta saturarlo, y *jamming* de engaño (*deception jamming*), que introduce señales falsas imitando las emisiones originales para confundir los sistemas receptores. El *barrage jamming* cubre amplias porciones del espectro



con baja densidad de potencia, mientras que el spot *jamming* concentra energía en una frecuencia específica, aumentando su eficacia, pero reduciendo el ancho de banda cubierto. Las variantes más avanzadas combinan ambas estrategias para contrarrestar sistemas de radar o comunicaciones con agilidad de frecuencia. La eficacia de las técnicas depende principalmente de la relación entre la potencia de interferencia y la de la señal (*J/S ratio*). Cuando el valor de *J/S* supera la unidad, el receptor no puede distinguir la información útil, provocando la pérdida o distorsión de los datos. Sin embargo, a medida que el transmisor legítimo incrementa su potencia o reduce la distancia al receptor se consigue que la señal supere al ruido y se restablezca la comunicación efectiva [41].

Por otro lado, la interceptación es la capacidad pasiva para detectar, capturar y analizar emisiones electromagnéticas ajenas con el fin de obtener información útil para la inteligencia, planificación y la conducción de operaciones. Dentro del marco de la EW, la interceptación se enmarca principalmente en el apoyo electrónico (ES) y en las disciplinas de inteligencia técnica SIGINT, que incluye COMINT y ELINT. De manera simplificada, la EW contempla las siguientes fases: detección de la emisión, caracterización (frecuencia, ancho de banda, modulación, etc.), localización (dirección y/o posición del emisor) y explotación (demodulación, decodificación, análisis de contenido y metadatos) [41].

Las limitaciones técnicas incluyen la sensibilidad del receptor, ancho de banda de vigilancia, capacidad de procesamiento en tiempo real, efectos de propagación y contramedidas como agilidad de frecuencia, FHSS, espectro ensanchado y robusto cifrado que aumentan la complejidad de detección, sincronización y decodificación.

### 3.5. Introducción a sistemas embebidos

Un sistema embebido es un sistema informático especializado que se integra dentro de un dispositivo más grande, desempeñando una función específica y dedicada. A diferencia de las computadoras de propósito general, estos sistemas están diseñados para ejecutar una o varias tareas concretas bajo condiciones de operación definidas y, en la mayoría de los casos, presentan restricciones en cuanto al consumo energético, tamaño, costo y rendimiento. Un ejemplo representativo de este tipo de sistemas son las *Raspberry Pi*, ESP32, NodeMCU etc. ampliamente utilizadas en entornos de desarrollo y prototipado para la interconexión de dispositivos mediante diversos estándares de comunicación dentro del ámbito del *IoT*. La función principal de un sistema embebido en un entorno *IoT* consiste en la adquisición, procesamiento y transmisión de datos hacia servidores o plataformas en la nube. Por ejemplo, un sistema embebido puede recibir información de sensores de gas y remitirla a un sitio web a través de un canal inalámbrico, permitiendo así la supervisión remota en tiempo real [42] [43] [44].

Los sistemas embebidos se caracterizan por integrar tanto el hardware como el software en una misma arquitectura, lo que les permite ejecutar funciones autónomas y específicas sin requerir intervención humana constante. Estos sistemas suelen incorporar un microcontrolador o microprocesador que gestiona las operaciones internas [45], junto con componentes de memoria, interfaces de comunicación y elementos de entrada/salida adaptados al propósito del dispositivo. El software embebido se desarrolla habitualmente en lenguajes de bajo nivel, como C o ensamblador, optimizados para garantizar eficiencia, fiabilidad y respuesta determinista en tiempo real.

De acuerdo con la definición [46], los sistemas embebidos pueden clasificarse en función de su criticidad y tiempo de respuesta, abarcando desde sistemas de tiempo real —donde el cumplimiento de los plazos de ejecución es esencial, como en la automatización industrial o la aviación— hasta sistemas de propósito general embebido, empleados en dispositivos de consumo, como electrodomésticos inteligentes, cámaras digitales o sistemas multimedia. En estos últimos, el equilibrio entre costo, consumo y rendimiento adquiere especial relevancia, priorizando la estabilidad operativa frente a la potencia de procesamiento.

Además, la proliferación del *IoT* ha impulsado la evolución de los sistemas embebidos hacia





arquitecturas más complejas y conectadas, capaces de comunicarse mediante protocolos como Wi-Fi, BLE, *LoRa* o *ZigBee*, integrando funcionalidades de análisis local o *edge computing* para reducir la dependencia de servidores centrales. Esta tendencia amplía el papel de los sistemas embebidos, que dejan de ser simples controladores para convertirse en nodos inteligentes dentro de redes distribuidas de sensorización y control.

### 3.6. *Raspberry Pi*, ESP32 y el *IoT*

La *Raspberry Pi* es un SBC de bajo costo y tamaño reducido, creado por la Fundación *Raspberry Pi* en el Reino Unido. Se ha consolidado como una herramienta accesible y flexible para estudiantes, investigadores y desarrolladores interesados en computación, automatización y, especialmente, en aplicaciones relacionadas con el *IoT*.

La primera versión apareció en 2012, desde entonces los modelos han mejorado en capacidades y lo más interesante, tiene la capacidad de incorporar periféricos mediante puertos USB 2.0, 3.0, conectividad HDMI y soporte para módulos de sensores a través de pines GPIO. Estas características permiten su integración en proyectos de monitoreo, control y procesamiento distribuido.

El *IoT* se define como la interconexión de dispositivos físicos, sensores y actuadores capaces de recopilar, procesar y transmitir información en tiempo real a través de internet. Su importancia radica en la automatización de procesos, el aumento de la eficiencia y la capacidad de tomar decisiones basadas en datos [47].

Las aplicaciones de *Raspberry Pi* en *IoT* son diversas. En el sector transporte, se han desarrollado sistemas de asistencia al conductor, gestión de estacionamiento, monitorización de vehículos mediante sensores y comunicación en la nube. En agricultura su uso supone optimización de recursos, detección de enfermedades a la par que en el ámbito de la sanidad es usado en combinación de sensores biométricos permite el monitoreo remoto de pacientes.

En el ámbito de la seguridad, la *Raspberry Pi* puede integrarse con sensores de movimiento, cámaras, detectores de gas y geolocalización mediante GPS para crear sistemas de vigilancia en tiempo real. Estos sistemas envían notificaciones instantáneas a los usuarios mediante aplicaciones de mensajería como *Telegram*, alertando sobre intrusiones, incendios o fugas de gas [48]. Este tipo de soluciones combina bajo costo, escalabilidad y la capacidad de operar en cualquier lugar con acceso a internet.

Los beneficios de usar *Raspberry Pi* en *IoT* son su bajo costo y accesibilidad. A lo que se añade su bajo consumo energético y compatibilidad con gran variedad de sensores y módulos. Además de facilidad de programación y amplia documentación disponible.

El ESP32 es un microcontrolador de bajo coste con Wi-Fi 802.11n y Bluetooth 4.2/BLE integrados, dual-core de hasta 240 MHz, 520 KB de SRAM y múltiples GPIOs, ADC y DAC, lo que lo convierte en una solución ideal para el desarrollo de aplicaciones *IoT* que requieren procesamiento local y conectividad inalámbrica. Su arquitectura ofrece un óptimo ratio coste-rendimiento, permitiendo despliegues fiables en entornos domésticos, industriales, de salud o entornos agrónomos [49].

Los artículos de aplicación práctica subrayan su versatilidad en entornos reales. Desde el desarrollo de un sistema de automatización doméstica inteligente [50], integrando sensores de temperatura/humedad, gas y riego con control Wi-Fi y aplicaciones móviles. Hasta el diseño de una estación de monitorización ambiental con sensores de calidad del aire que transmiten datos a *Blynk* [51] [52]. Además, su integración es apta en sistemas descentralizados con IOTA, demostrando su uso en arquitecturas distribuidas avanzadas [53].

En síntesis, el ESP32 destaca por su conectividad Wi-Fi/Bluetooth, eficiencia energética, flexibilidad en protocolos y amplia compatibilidad con periféricos. Su implantación en edificación



inteligente, automatización industrial, monitoreo ambiental, e incluso *edge computing* y *blockchain* ligero, está ampliamente documentada. Estos estudios hacen del ESP32 una piedra angular sólida y contrastada para sistemas *IoT*.

## 4. DESARROLLO: ANÁLISIS Y RESULTADOS

### 4.1. Definición de requisitos

Antes de proceder con el diseño de la red distribuida de sensores, es indispensable establecer los requisitos que deben cumplirse para garantizar la viabilidad del sistema en un escenario real. La correcta definición de estos requisitos no solo facilita el proceso de diseño, sino que además asegura que la solución propuesta se adapte a las condiciones y limitaciones del entorno de aplicación.

Con el fin de estructurar adecuadamente esta fase, los requisitos se han dividido en dos grandes categorías: requisitos derivados del entorno y requisitos técnicos.

- Requisitos derivados del entorno.

En un contexto de operación militar o de combate real, el sistema de sensores debe cumplir una serie de condiciones específicas orientadas principalmente a garantizar la supervivencia, seguridad y discreción de la red.

Uno de los aspectos más críticos es la minimización de la posibilidad de ser detectado. La exposición del sistema ante medios de guerra electrónica representa un riesgo elevado, dado que estos medios son capaces de interceptar, alterar o anular las comunicaciones transmitidas mediante el espectro electromagnético. La amenaza más significativa se concentra en el dispositivo receptor, ya que se encuentra vinculado al puesto de mando y, en consecuencia, su localización podría comprometer la integridad de la operación.

En paralelo, la detección o captura de un dispositivo emisor también constituye un riesgo considerable, pues podría proporcionar información sensible al enemigo y comprometer tanto la seguridad de la red como la validez de las comunicaciones.

De estas consideraciones se derivan los siguientes requisitos:

1. **Minimización de la comunicación:** La comunicación debe ser estrictamente unidireccional, desde el emisor hacia el receptor, reduciendo al máximo el volumen de información transmitida para preservar la seguridad del puesto de mando.
2. **Protección de la comunicación:** La transmisión de datos debe estar protegida frente a interceptaciones mediante técnicas de ofuscación y cifrado ligero, de modo que, en caso de ser interceptada, la información no pueda ser explotada de manera inmediata.
3. **Capacidad de reconfiguración:** Los parámetros de seguridad de la red deben ser reconfigurables, permitiendo modificar claves y protocolos en caso de que un dispositivo sea capturado por fuerzas enemigas.

Además de las amenazas electrónicas, el sistema debe adaptarse a las condiciones físicas y medioambientales del entorno operativo. Los dispositivos emisores pueden ser transportados tanto en vehículos como por los propios combatientes, y en muchos casos se prevé que sean desplegados y abandonados en el teatro de operaciones para la recolección de información.

En este sentido, se establecen los siguientes requisitos adicionales:

4. Los dispositivos deben contar con una **carcasa protectora** capaz de soportar impactos, vibraciones, exposición solar, humedad, lluvia y polvo.



5. El **tamaño y peso** de cada unidad debe reducirse al mínimo de manera que su transporte sea discreto y compatible con el equipamiento habitual de un combatiente. En particular, debe poder almacenarse en una mochila estándar sin comprometer el espacio destinado a otros elementos críticos para la misión.
- Requisitos técnicos.  
Además de los condicionantes derivados del entorno, el sistema debe cumplir con una serie de requisitos técnicos que aseguren un rendimiento adecuado y la fiabilidad del conjunto. Entre los más relevantes se destacan:
  6. **Tiempo de comunicación:** La literatura especializada en sistemas embebidos y aplicaciones de monitoreo sugiere que, para que una alerta se considere en tiempo real en sistemas de bajo coste y recursos limitados, el tiempo total desde la detección hasta la recepción de la alerta debe ser inferior a 5 segundos [54], garantizando así una respuesta rápida y útil en escenarios dinámicos.
  7. **Autonomía energética:** Las baterías deben ser recargables y de fácil sustitución, de modo que se asegure la continuidad operativa de los sensores incluso en entornos donde no sea posible disponer de infraestructura de carga prolongada.
  8. **Capacidad de procesamiento:** El procesador de cada dispositivo debe ser capaz de ejecutar de forma simultánea un algoritmo de reconocimiento de imagen y otro de detección de movimiento, combinando ambos resultados para incrementar la fiabilidad de la detección antes de transmitirlo.
  9. **Fiabilidad:** La precisión tanto del sistema de cámara como del algoritmo de detección de movimiento debe alcanzar un nivel mínimo del 98% de acierto de forma independiente. La razón de la combinación de ambas fuentes es la reducción de falsos positivos y falsos negativos.
  10. **Tecnología de comunicación:** La red de sensores debe implementarse empleando tecnologías de *IoT* que ofrecen bajo consumo energético, escalabilidad y facilidad de integración.
  11. **Escalabilidad de la red:** El sistema debe ser capaz de soportar al menos 30 dispositivos emisores de modo que sea viable el transporte por una SERECO (sección de reconocimiento) [55] de infantería, conectados simultáneamente a un único receptor sin degradar su rendimiento.

## 4.2. Selección de *hardware*

Antes de exponer las diferentes selecciones, se establece que los criterios seguidos para la elección de estos vienen dados principalmente por la facilidad de integración que presentan entre sí, fiabilidad, rendimiento, coste, relativo bajo consumo, amplia variedad de modelos de software libre sobre los que iniciar un proyecto partiendo de una base sólida junto con la existencia de una amplia comunidad de desarrolladores [56] que permite el intercambio de conocimiento a la hora de consultar documentación; Además de características que los hacen idóneos para su aplicación en un escenario de combate real.

### 4.2.1. Elección de componentes comerciales

De este modo, los componentes seleccionados han sido previamente comparados con sus homólogos en el mercado siendo los elegidos finales:

#### **Raspberry Pi 5**

Para el núcleo de procesamiento principal del sistema propuesto, se ha seleccionado la *Raspberry Pi 5* [57], una plataforma de computación embebida de última generación que



representa un avance significativo respecto a sus predecesoras en términos de rendimiento, capacidad de expansión y eficiencia operativa. Esta elección se fundamenta en su arquitectura moderna, su capacidad de procesamiento mejorada y su compatibilidad con periféricos avanzados, lo que la convierte en una solución adecuada para aplicaciones de detección, análisis de imágenes y transmisión de datos en tiempo real.

La *Raspberry Pi 5* incorpora un procesador Broadcom BCM2712 con arquitectura Arm Cortex-A76 de 64 bits, compuesto por cuatro núcleos que operan a 2,4 GHz, lo que permite ejecutar algoritmos de procesamiento intensivo con mayor rapidez y eficiencia que versiones anteriores. Este SoC, fabricado en tecnología de 16 nm, proporciona un rendimiento de CPU entre 2 y 3 veces superior al de la *Raspberry Pi 4* [58], además de una mejora sustancial en el rendimiento gráfico gracias a su GPU *VideoCore VII* [59], compatible con OpenGL ES 3.1 [60] y *Vulkan 1.2* [61] [62].

En cuanto a la memoria, se dispone de configuraciones de 4 GB y 8 GB de RAM LPDDR4X, lo que permite la ejecución simultánea de múltiples procesos en entornos multitarea, manteniendo la estabilidad del sistema incluso bajo carga elevada. Esta capacidad resulta especialmente relevante en aplicaciones que combinan detección por sensores PIR, procesamiento de imágenes y transmisión *LoRa*.

Desde el punto de vista de conectividad, la *Raspberry Pi 5* incluye Wi-Fi de doble banda (802.11ac), Bluetooth 5.0/BLE y Gigabit Ethernet, lo que facilita la integración en redes locales o remotas, así como la comunicación con dispositivos periféricos. Aunque la conectividad inalámbrica no constituye el foco principal del presente estudio, su disponibilidad amplía las posibilidades de implementación en escenarios futuros.

La placa también incorpora puertos USB 3.0 y 2.0, salidas micro-HDMI duales con soporte para resolución 4K a 60 Hz, y un bus GPIO [63] de 40 pines, lo que permite la conexión directa de sensores, actuadores y módulos de expansión. Además, se ha añadido una interfaz PCIe 2.0 x1, que habilita la conexión de unidades SSD NVMe y otros periféricos de alto rendimiento.

En términos de consumo energético, la *Raspberry Pi 5* requiere una alimentación de 5V DC a 5A, lo que representa un incremento respecto a la *Raspberry Pi 4* (5V/3A), pero justificado por el aumento en capacidad de procesamiento y ancho de banda de entrada/salida. Este consumo sigue siendo compatible con sistemas alimentados por baterías de alta capacidad, como los considerados en el presente proyecto.

En comparación con la *Raspberry Pi 4* Modelo B, la *Raspberry Pi 5* ofrece mejoras sustanciales en todos los aspectos clave: mayor frecuencia de CPU (2.4 GHz vs. 1.8 GHz), GPU más potente (800 MHz vs. 500 MHz), memoria RAM más rápida (LPDDR4X-4267 vs. LPDDR4-3200), y mayor ancho de banda en puertos USB y microSD. Aunque el consumo energético es ligeramente superior (hasta 12 W frente a 8 W), el rendimiento obtenido compensa esta diferencia en aplicaciones que requieren procesamiento intensivo y respuesta rápida.

La elección de la *Raspberry Pi 5* se justifica por su mayor capacidad de cómputo, mejor eficiencia en tareas de visión artificial, y compatibilidad con periféricos modernos, lo que la convierte en una opción más adecuada que modelos anteriores para el sistema de detección y alerta propuesto en este TFG.

### **Microprocesador ESP32-S3**

El ESP32-S3 [64] de *Espressif Systems* [65] se incorpora como un módulo auxiliar encargado de la gestión de comunicación inalámbrica de bajo nivel y control de periféricos. Su selección responde a su excelente relación entre prestaciones, flexibilidad y bajo consumo energético, características esenciales en sistemas distribuidos o de recolección de datos remota.



Este microprocesador integra un procesador *dual-core Xtensa LX7* de 32 bits a 240 MHz, con 512 KB de SRAM y 384 KB de ROM, suficientes para ejecutar tareas de sensorización, transmisión *LoRa* y control local. Dispone de una amplia variedad de interfaces (UART, SPI, I<sup>2</sup>C, I<sup>2</sup>S, PWM, ADC, etc.) que permiten conectar y gestionar numerosos dispositivos externos.

El ESP32-S3 mantiene la conectividad Wi-Fi 802.11 b/g/n y Bluetooth 5.0 LE, lo que posibilita la comunicación tanto con redes locales como con dispositivos móviles o nodos de una red *IoT*. Además, incluye mecanismos avanzados de seguridad (arranque seguro, cifrado AES/rsa y generador de números aleatorios por hardware) que garantizan la integridad de la información transmitida.

Su capacidad para operar en modos de bajo consumo, junto con un coprocesador ULP (*Ultra-Low Power*), que permite reducir significativamente la demanda energética en períodos de inactividad.

### **Módulo de cámara Arducam OV5647 IR-CUT2**

Para las tareas de captura y procesamiento de imagen en el sistema propuesto, se ha seleccionado el módulo Arducam OV5647 IR-CUT [66], plenamente compatible con la *Raspberry Pi 5* mediante interfaz CSI. Esta elección responde a la necesidad de disponer de un sistema de visión que funcione de forma fiable tanto en condiciones de iluminación diurna como nocturna, sin comprometer la calidad de imagen ni la eficiencia energética a la vez que proporciona un alcance efectivo de identificación de objetivos de 30 m.

El módulo incorpora un sensor Omnivision OV5647 [67] de tipo CMOS con obturador rolling shutter, resolución nativa de 5 megapíxeles (2592 × 1944 píxeles) y tamaño de píxel de 1.4 μm × 1.4 μm, lo que permite capturar imágenes de alta definición con buena sensibilidad en condiciones de baja luz. Además, soporta grabación de vídeo en 1080p a 30 fps, 720p a 60 fps y 480p a 90 fps, lo que lo hace adecuado para aplicaciones de detección de movimiento y análisis visual en tiempo real [68].

Una de las características distintivas de este módulo es la inclusión de un filtro IR-CUT motorizado, que se activa o desactiva automáticamente en función de la iluminación ambiental. Este mecanismo permite obtener imágenes con fidelidad cromática durante el día y mejorar la visibilidad en la oscuridad mediante el uso de iluminación infrarroja integrada (LEDs IR de 850 nm). Esta funcionalidad elimina la necesidad de intervención manual o de componentes externos para cambiar entre modos de visión, lo que simplifica la operación del sistema en entornos autónomos.

El módulo presenta un campo de visión horizontal de 85°, lente tipo M12 con distancia focal de 2.25 mm, y enfoque manual ajustable, lo que permite adaptar la captura a diferentes escenarios de vigilancia o monitoreo ambiental, lo que proporciona una cobertura adecuada para tareas de vigilancia perimetral. En combinación con modelos de detección como YOLOv5 o YOLO-NAS, optimizados para dispositivos de bajo consumo como la *Raspberry Pi*, se ha demostrado que es posible detectar figuras humanas a distancias de 12 metros con una tasa de precisión aceptable, dependiendo de las condiciones de iluminación, resolución configurada y calidad del enfoque. En entornos nocturnos, el sistema se apoya en iluminación infrarroja activa mediante LEDs IR integrados, lo que permite mantener la capacidad de detección en ausencia de luz visible, siempre que el objeto se encuentre dentro del rango efectivo de iluminación (habitualmente hasta 7 metros) [69]. Sus dimensiones compactas (36 × 36 mm) y peso reducido facilitan su integración en sistemas embebidos portátiles, sin afectar la estructura física del dispositivo.

La conexión mediante interfaz CSI de 15 pines garantiza una transmisión de datos directa y de alta velocidad hacia el procesador principal, minimizando la latencia en la captura y procesamiento de imágenes. Esta característica es especialmente relevante en sistemas que requieren respuesta rápida ante eventos detectados por sensores PIR.





### Sensor PIR AM 312

Para la detección de movimiento en el sistema propuesto, se ha seleccionado el sensor AM312 [70] por su eficiencia energética al ser un sensor pasivo, compatibilidad directa con la *Raspberry Pi* 5 y adecuación a entornos exteriores protegidos mediante el empleo de una carcasa protectora [71]. Este módulo opera con un voltaje de alimentación de 2.7 V a 12 V DC, y presenta un consumo en reposo inferior a 0.1 mA, lo que lo convierte en una solución óptima para sistemas alimentados por batería.

El AM312 ofrece una salida digital de 3.3 V, compatible con los niveles lógicos de los pines GPIO de la *Raspberry Pi*, y un modo de disparo repetible, manteniendo la señal activa mientras se detecte movimiento. Su distancia de detección es de hasta 12 metros, con un ángulo de cobertura de hasta 100°, lo que proporciona una cobertura eficaz en aplicaciones de vigilancia perimetral [70].

En comparación con sensores como el HC-SR501 [72], el AM312 destaca por su tamaño más compacto, menor consumo energético y mayor simplicidad de integración, aunque no dispone de ajustes de sensibilidad ni tiempo de retención. Estas características lo hacen especialmente adecuado para sistemas embebidos autónomos que operan en exteriores, siempre que se instale en una carcasa que lo proteja de la intemperie.

### Módulo *LoRa* RYLR998

Para la comunicación a larga distancia se ha seleccionado el módulo de transceptor *LoRa* RYLR998 [73] del fabricante *REYAX Technology* [74]. Este componente utiliza el chipset *LoRa* de *Semtech* [75], operando en frecuencias entre 868 y 915 MHz, y ofrece alcances de transmisión de hasta 20 Km, lo que lo convierte en una solución idónea para aplicaciones de *IoT* distribuidas en áreas extensas.

El módulo presenta una alta sensibilidad de recepción (-129 dBm) y bajo consumo de corriente, factores determinantes en el diseño de sistemas alimentados por batería. La comunicación se realiza mediante UART y comandos AT, lo que simplifica su integración con la *Raspberry Pi* 5.

La robustez frente a interferencias y la eficiencia energética del protocolo *LoRa* garantizan una transmisión estable y segura incluso en entornos con ruido electromagnético elevado (como puede ser el uso de *jamming* a frecuencias distintas a la *LoRa* por parte del enemigo).

El módulo, ofrece mecanismos básicos de seguridad como:

- Asignación de direcciones únicas a cada nodo (AT+ADDRESS).
- Identificador de red (AT+NETWORKID) para segmentar grupos de dispositivos.
- Cifrado de datos mediante soporte para cifrado simétrico AES-128, configurable mediante comandos AT.

El RYLR998 se configura mediante comandos AT, lo que simplifica su uso en sistemas embebidos como la *Raspberry Pi* 5. Además, permite definir parámetros clave como frecuencia, el canal, la latencia, el *Spreading Factor* (SF), el ancho de banda y la tasa de codificación, así como la potencia de transmisión, lo que facilita la adaptación del sistema a distintos entornos operativos.

La arquitectura de red soportada por el módulo *LoRa* RYLR998 permite establecer comunicaciones punto a punto, punto a multipunto y multipunto a multipunto mediante la asignación de direcciones únicas a cada nodo emisor mediante el comando AT+ADDRESS, con un rango de valores de 0 a 255. Esta capacidad teórica de direccionamiento habilita la integración de hasta 255 dispositivos emisores en una misma red lógica, siempre que compartan el mismo AT+NETWORKID y estén configurados con parámetros de frecuencia, factor de expansión (SF), ancho de banda (BW) y tasa de codificación (CR) compatibles. La



viabilidad práctica de esta configuración depende de la gestión del tráfico en la red, ya que *LoRa* no implementa control de acceso al medio en su capa física. En aplicaciones de bajo volumen de datos y transmisión esporádica, como sistemas de alerta por detección de movimiento, esta limitación no representa un impedimento significativo, lo que hace viable la implementación de una red con hasta 255 nodos emisores y un *Gateway* receptor utilizando el RYLR998 [76] [77].

### Conjunto de alimentación

La elección de una batería recargable ion litio de 12 V y 50 Ah [78] integrada y de un módulo convertidor DC-DC *step-down* [79] de 12 V a 5 V responde directamente a los requisitos eléctricos del sistema, el cual opera a 5 V y 2 A de forma estable. La batería seleccionada proporciona un nivel de tensión superior al requerido por la electrónica principal, lo que permite aumentar la versatilidad del sistema y asegurar una autonomía adecuada. No obstante, esta tensión debe ser acondicionada para garantizar la correcta alimentación de los componentes, especialmente de la Raspberry Pi 5, que presenta una sensibilidad elevada a variaciones de voltaje.

Para ello, se integra un convertidor *step-down* regulable que permite obtener de forma precisa una salida estabilizada de 5 V, manteniendo la corriente necesaria para el funcionamiento continuo del conjunto. Dicho módulo presenta una eficiencia elevada, lo que minimiza las pérdidas energéticas y contribuye a prolongar la autonomía de la batería. Además, su capacidad de regulación facilita la adaptación del sistema a futuras modificaciones o ampliaciones sin necesidad de sustituir la fuente de alimentación principal.

La combinación de ambos elementos —batería integrada y convertidor DC-DC— ofrece así una solución compacta, eficiente y adecuada para garantizar la alimentación estable del sistema, asegurando simultáneamente la compatibilidad con todos los módulos electrónicos que requieren una tensión nominal de 5 V. Esta configuración permite prescindir de alternativas menos eficientes, como las *powerbanks* comerciales, proporcionando un mayor control sobre el flujo energético y optimizando el rendimiento global del dispositivo.

Por otro lado, se considera el uso de baterías AA NiMH de 4,8 V y 5000 mAh [80] para el dispositivo *Gateway* debido a la compatibilidad con los componentes, reducido tamaño, peso y facilidad de sustitución y carga que se considera para este dispositivo al deber estar cercano al puesto de mando para la explotación de la información proporcionada por el sistema.

#### 4.2.2. Cálculo de la autonomía del sistema

Dispositivo sensor:

Para estimar la autonomía del sistema se ha considerado una batería de ion-litio recargable de 12 V y 50 000 mAh (50 Ah), cuya capacidad nominal equivale a 600 Wh, según las especificaciones técnicas del fabricante. A partir de las mediciones empíricas realizadas durante el funcionamiento del sistema, se ha obtenido un consumo medio de 8,7 W (ver Figura 2) en condiciones normales de operación con los sensores activos, no obstante, para la realización de cálculos se utilizará un consumo de 10,28 W pues es el que se llega a alcanzar en picos de trabajo. Dado que el sistema realiza envíos de datos de forma aleatoria y poco frecuente, se ha incorporado un margen adicional del 10 % para contemplar posibles picos de consumo asociados a dichas transmisiones, alcanzando así un consumo total estimado de 11,308 W.

$$P_{out} = 10,28 \text{ W} \times (1 + 0,10) = 10,28 \times 1,10 = 11,308 \text{ W}$$

El sistema se alimenta a través de un convertidor DC-DC tipo *step-down*, encargado de reducir la tensión de salida de la batería (12 V) hasta los 5 V necesarios para el funcionamiento de los componentes. Estos convertidores presentan pérdidas por disipación que dependen de su eficiencia, la cual suele oscilar entre el 80 y el 95 % según el diseño y las condiciones de carga. Para este cálculo se ha adoptado una eficiencia del 90 %, valor representativo y conservador para módulos comerciales de este tipo. Considerando esta eficiencia, la potencia demandada a



la batería se obtiene dividiendo el consumo de salida entre la eficiencia del convertidor, resultando en aproximadamente 12,564 W.

$$P_{in} = \frac{P_{out}}{\eta} = \frac{11,308 \text{ W}}{0,90} = 12,564 \text{ W}$$

A partir de la capacidad energética nominal de la batería (600 Wh) y la potencia total demandada (12,564 W), la autonomía teórica máxima del sistema sería de unas 47,75 horas, equivalente a aproximadamente 2 días de funcionamiento continuo. Sin embargo, en la práctica, no se recomienda agotar completamente la carga de las baterías de ion-litio, ya que las descargas profundas reducen de forma significativa su vida útil. Por este motivo, se considera una profundidad de descarga (DoD) del 80 %, valor habitualmente empleado en estimaciones conservadoras. Aplicando este criterio, la energía útil se reduce a 480 Wh, lo que sitúa la autonomía realista del sistema en torno a 38,2 horas, equivalentes a aproximadamente 1,59 días de funcionamiento continuo.

Autonomía (horas) = energía disponible (Wh) / potencia demandada (W):

$$t_{teórico} = \frac{E_{nominal}}{P_{in}} = \frac{600 \text{ Wh}}{12,564 \text{ W}} \approx 47,75 \text{ h}$$

Equivalente en días:

$$47,75 \approx 2 \text{ días}$$

Energía utilizable conservadora:

$$E_{usable} = E_{nominal} \times 0,80 = 600 \text{ Wh} \times 0,80 = 480 \text{ Wh}$$

Autonomía conservadora:

$$t_{conservador} = \frac{E_{usable}}{P_{in}} = \frac{480 \text{ Wh}}{12,564 \text{ W}} \approx 38,2 \text{ h} \approx 1,59 \text{ días}$$

En resumen, con las condiciones de consumo medidas, un margen adicional del 10 % por envíos ocasionales y una eficiencia del 90 % en el convertidor, la batería seleccionada proporcionaría una autonomía estimada de entre 38,2 y 47,7 horas, en función del nivel de descarga permitido. Este cálculo se ha realizado siguiendo criterios técnicos habituales en el dimensionamiento energético de sistemas autónomos, considerando tanto las pérdidas por conversión como las prácticas recomendadas para el uso de baterías de ion-litio.



Figura 2. Medición de consumo del prototipo. Fuente: elaboración propia.

Dispositivo Gateway:

Para estimar la autonomía del sistema se ha considerado una batería de ion-litio recargable de 4,8 V y 5000 mAh, cuya capacidad nominal equivale a 24 Wh. Teniendo un consumo en reposo (a la espera de recibir las alertas) de 196 mA, la autonomía esperada es:

$$t_{teórico} = \frac{E_{nominal}}{P_{in}} = \frac{24 \text{ Wh}}{0,196 \text{ W}} \approx 122,44 \text{ h}$$





En resumen, con las condiciones de consumo medidas, un margen adicional del 10 % por envíos ocasionales y una eficiencia del 90 % en el convertidor, la batería seleccionada proporcionaría una autonomía estimada de entre 38,2 y 47,7 horas, en función del nivel de descarga permitido mientras que el *Gateway* consigue una autonomía de 122,44 h. Este cálculo se ha realizado siguiendo criterios técnicos habituales en el dimensionamiento energético de sistemas autónomos, considerando tanto las pérdidas por conversión como las prácticas recomendadas para el uso de baterías de ion-litio.

#### 4.2.3. Carcasa protectora

El sistema electrónico desarrollado para este proyecto está destinado a operar en entornos exteriores, donde puede estar expuesto a condiciones adversas como lluvia, polvo, radiación solar y variaciones térmicas. Para garantizar la integridad funcional de los componentes, se debe construir una carcasa protectora la cual seguirá los estándares internacionales de protección IP definidos por la norma IEC 60529 [71] para asegurar su idoneidad.

Según la normativa IEC 60529, se recomienda una carcasa con clasificación IP67 o superior para garantizar protección total contra polvo (primer dígito 6) y resistencia a inmersión temporal en agua hasta 1 metro durante 30 minutos (segundo dígito 7) [71]. Esto asegura la operatividad del sistema en condiciones de lluvia intensa, humedad elevada y ambientes polvorientos, como zonas rurales o industriales.

El sistema desarrollado requiere una carcasa protectora destinada a alojar y proteger los componentes electrónicos principales, formados por una *Raspberry Pi 5*, un módulo *LoRa RLYR998*, una cámara *Arducam OV5647 IR-CUT2*, un sensor *PIR AM312* y conjunto de alimentación formado por una batería recargable y un convertidor *step-down*. La función principal de la carcasa es proporcionar protección mecánica y ambiental, asegurando la integridad de los dispositivos frente a agentes externos como humedad, radiación solar, polvo e impactos accidentales, al mismo tiempo que permite la correcta operación de los sensores ópticos y de movimiento. Las medidas de los componentes junto con imágenes de estos pueden ser consultadas en: Anexo II .

Tras analizar las condiciones de uso y las recomendaciones técnicas, se selecciona PETG [81](Tereftalato de polietileno glicolizado) como material principal de fabricación. Este polímero termoplástico ofrece una combinación óptima entre resistencia mecánica, facilidad de impresión y durabilidad frente a la intemperie, siendo especialmente adecuado para entornos exteriores. Su resistencia al agua y a la humedad evita la degradación del material, mientras que su mayor resistencia frente a los rayos ultravioleta, comparado con el PLA, permite un uso prolongado sin deterioro significativo de sus propiedades estructurales. Además, el PETG presenta una temperatura de trabajo comprendida entre -40 °C y 80 °C, lo que garantiza la operatividad del conjunto en condiciones ambientales extremas.

Para optimizar la resistencia frente a la radiación solar, se recomienda el uso de PETG con aditivos estabilizadores UV, complementado con una capa de barniz acrílico protector (por ejemplo, *Rust-Oleum Clear Gloss*), aplicada tras el proceso de impresión, con el fin de prolongar la vida útil de la carcasa y evitar la degradación superficial por exposición prolongada al sol.

La carcasa se concibe con un diseño hermético y modular, compuesto por una base principal y una tapa superior fijada mediante tornillos de acero inoxidable y arandelas de goma, garantizando la estanqueidad en los puntos de unión. Las paredes externas tendrán un grosor de entre 2 y 3 mm, suficiente para asegurar la rigidez estructural y absorber vibraciones o pequeños impactos. En la unión entre la tapa y la base se incorpora una junta de silicona para impedir la entrada de agua y polvo, mientras que los puntos de ventilación estarán protegidos mediante rejillas con malla de aluminio o filtros Gore-Tex, que permiten el intercambio de aire sin comprometer la estanqueidad.



La disposición de los elementos internos (Figura 7) se organiza de forma que se reduzcan las interferencias y se optimice la disipación térmica. La *Raspberry Pi 5* se ubica en la zona central de la carcasa, fijada mediante separadores plásticos y anclajes roscados, dejando espacio lateral para el módulo *LoRa* RLYR998, cuya antena puede sobresalir a través de un conector estanco tipo PG7. En la parte frontal se reserva un espacio específico para la cámara Arducam OV5647 IR-CUT2 y el sensor PIR AM312, alineados de modo que ambos compartan el mismo eje de visión. Esta disposición garantiza una cobertura visual y de detección coherente. Para evitar la incidencia directa del sol, se incorpora un visor o parasol frontal, diseñado como una prolongación superior de la carcasa que proyecta sombra sobre ambos sensores, evitando falsos positivos del PIR y reduciendo el deslumbramiento en el módulo óptico.

El sistema debe prever una adecuada disipación térmica, especialmente debido a la generación de calor por parte de la *Raspberry Pi 5*. Para ello, se contempla la inclusión de rejillas laterales protegidas. De este modo, se facilita la convección del aire sin comprometer la hermeticidad del conjunto. Además, los componentes electrónicos se montan sobre una placa soporte de aluminio anodizado, que contribuye a la disipación pasiva del calor.

Las uniones mecánicas se realizan con tornillería de acero inoxidable A2, acompañada de arandelas de goma para sellar los orificios de fijación. Los pies de goma situados en la base permiten aislar la carcasa de la superficie de apoyo, evitando la absorción de humedad por capilaridad. Los cables de alimentación y comunicación se conducen por el interior de modo que la batería queda en el extremo de la carcasa donde se ubica una pestaña que permite la sustitución de esta. Esta abertura cuenta con una junta de goma que garantiza el sellado y protegen las conexiones frente a la humedad. En el proceso de ensamblaje final se aplica un sellador epóxico (por ejemplo, Araldite) en los puntos críticos para reforzar la estanqueidad y la resistencia estructural.

El conjunto formado por los dispositivos principales presenta unas dimensiones aproximadas de  $180 \times 120 \times 80$  mm, considerando el espacio necesario para la batería, la placa base y los módulos adicionales. Teniendo en cuenta un espesor medio de las paredes de 2,5 mm y el volumen de material empleado, se estima un volumen total de la carcasa de alrededor de 1,5 litros. El peso final del conjunto, incluyendo los componentes internos, se aproxima a 500 g debido al peso añadido del conjunto de alimentación (no incluido en Figura 4). Estas cifras sitúan el sistema dentro de un rango manejable y fácilmente instalable en entornos exteriores.

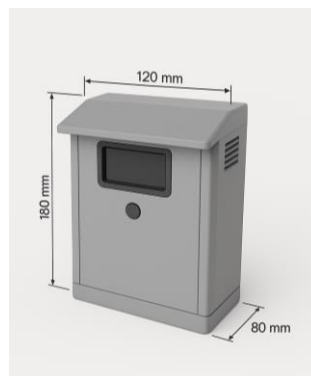


Figura 3. Concepto de carcasa protectora. Fuente: elaboración propia



*Figura 4. Pesaje de conjunto sensor. Fuente: elaboración propia.*

De la misma manera, se considera una carcasa similar para la protección del Gateway teniendo en cuenta que no requiere de la protección que el dispositivo sensor que estará expuesto a la intemperie. La carcasa fue desarrollada en la AALOG41 [82] mediante un diseño propio empleando ONIX sin refuerzo de carbono. El peso de este dispositivo es de 216 g tal y como muestra la Figura 5.



*Figura 5. Pesaje de prototipo de Gateway. Fuente: elaboración propia.*

En conjunto, la arquitectura hardware definida ofrece un equilibrio óptimo entre rendimiento computacional, bajo consumo y versatilidad, requisitos esenciales para el correcto desarrollo del proyecto.

### 4.3. Integración *hardware*

La integración hardware constituye un aspecto esencial en el diseño de sistemas embebidos y dispositivos *IoT*, ya que garantiza la correcta interacción entre los distintos módulos electrónicos que conforman el conjunto. En el presente proyecto, se desarrolla un sistema para la detección de movimiento y transmisión mediante *LoRa*, a la vez que el sistema para recepción de dicha transmisión empleando una combinación de plataformas de desarrollo y sensores interconectados de forma coherente y energéticamente eficiente.

#### 4.3.1. Integración del dispositivo emisor

La arquitectura hardware se organiza en torno a la *Raspberry Pi 5*, que actúa como unidad de procesamiento principal dedicado a la captura de imágenes y lectura del PIR para la detección de movimiento. Además, esta unidad se encarga del control del módulo de transmisión *LoRa*, conformando así una estructura distribuida que optimiza los recursos de cómputo y reparte la carga del sistema.

Una vez definida la carga de trabajo de la unidad de procesamiento y asignados los periféricos, se procede a la interconexión de los componentes. La cámara Arducam OV5647 IR-CUT, se conecta a la *Raspberry* mediante la interfaz CSI (Camera Serial Interface), que permite una comunicación de alta velocidad y baja latencia, imprescindible para el procesamiento eficiente de imágenes en tiempo real [83]. Los focos infrarrojos integrados en la cámara se



activan automáticamente en condiciones de baja luminosidad, garantizando la detección en entornos nocturnos.

El sensor PIR AM312 se conecta a uno de los pines GPIO de la *Raspberry Pi* para la lectura digital del estado de detección. Su alimentación se obtiene del regulador de 3,3 V, ya que el consumo del PIR es mínimo y compatible con esta tensión.

Para la transmisión de datos, se emplea el módulo *LoRa* RYLR998, que se comunica con la *Raspberry Pi* mediante la interfaz UART (pines TX y RX). Este módulo requiere alimentación a 3,3 V, por lo que se utiliza un convertidor DC-DC tipo *buck* conectado a uno de los puertos de la batería. El *buck* convierte los 5 V suministrados por la batería en 3,3 V estables para el *LoRa* y el PIR.

El sistema se alimenta mediante una batería de ion-litio recargable de 12 V y 50 000 mAh (50 Ah), seleccionada por su alta densidad energética, estabilidad y portabilidad. Esta batería ofrece una capacidad nominal de 600 Wh, lo que garantiza un suministro energético prolongado y adecuado para el funcionamiento continuo del conjunto de sensores y del microcontrolador. Su configuración interna proporciona un equilibrio óptimo entre tensión, capacidad y seguridad, permitiendo su integración directa en aplicaciones electrónicas de baja potencia.

Para adaptar la tensión de salida de la batería a los requerimientos de los distintos módulos, se incorpora un convertidor DC-DC tipo regulador reductor, encargado de transformar los 12 V de entrada en una tensión continua estabilizada de 5 V. Este componente asegura una alimentación constante y eficiente a los dispositivos electrónicos, evitando fluctuaciones que puedan afectar al rendimiento del sistema. Los convertidores de este tipo alcanzan habitualmente eficiencias superiores al 90 %, reduciendo las pérdidas por disipación y mejorando el aprovechamiento de la energía disponible en la batería.

El empleo de esta configuración resulta más eficiente que la utilización de una *powerbank* comercial, ya que elimina los múltiples procesos internos de conversión presentes en estos dispositivos. Las *powerbanks* suelen integrar etapas de carga, regulación y protección que incrementan las pérdidas eléctricas y limitan la capacidad útil disponible para el sistema. En cambio, el uso directo de una batería de ion-litio junto con un convertidor DC-DC de alta eficiencia permite optimizar la entrega de energía, minimizar las pérdidas térmicas y disponer de un control más preciso sobre los parámetros eléctricos de alimentación.

En términos mecánicos y de diseño conceptual, las dimensiones de los componentes permiten su integración en una carcasa compacta de 180 x 120 x 80 mm, manteniendo una distribución óptima para la disipación térmica y el acceso a los conectores. Se considera ubicar la alimentación en la base del conjunto, la *Raspberry Pi* en el centro y los módulos periféricos en las zonas laterales para favorecer la ventilación y minimizar la interferencia electromagnética entre antena y sensores tal y como se muestra en Figura 7, el interconexiónado se realizará según Figura 6. Dado a la no posibilidad de materializar el diseño propuesto con los materiales definidos en este, el prototipo se ha construido adaptando los bloques de manera compacta para realizar las pruebas de funcionamiento.



#### ESQUEMA CONEXIÓN RPÍ5 CON DISPOSITIVOS

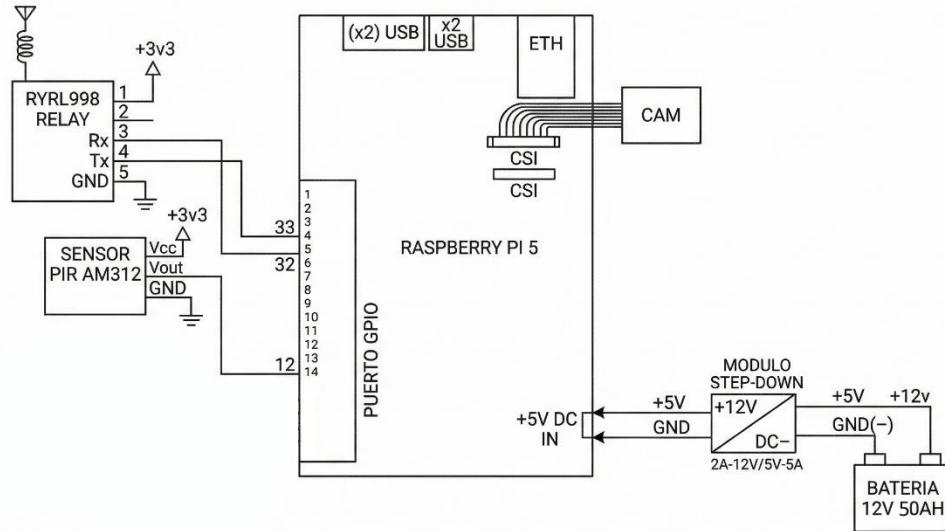


Figura 6. Conexión del nodo sensor. Fuente: elaboración propia.

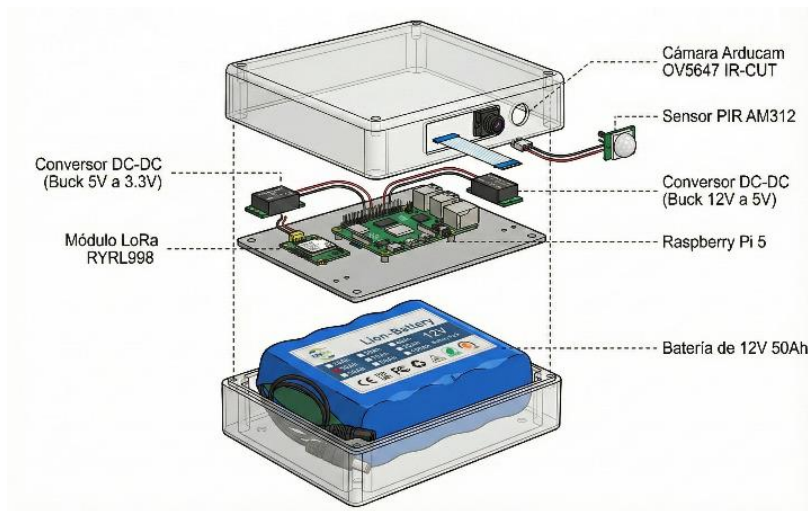


Figura 7. Prototipo para detección de movimiento y transmisión LoRa. Fuente: elaboración propia.

#### 4.3.2. Integración del dispositivo receptor

El dispositivo receptor (Figura 9) tiene la misión de permanecer de manera continuada a la escucha sin necesidad de integrar ningún periférico a parte del módulo *LoRa* el cual se comunicará con el ESP32-S3 mediante UART de la misma forma en que lo hace en el apartado anterior con el Raspberry. En cuanto a la alimentación, un paquete de baterías AA NiMH de 4,8V, 5000mAh de capacidad [84] que la anterior descrita ya que no supone un consumo energético tan elevado como si lo hace la *Raspberry Pi* en su función de reconocimiento de imagen, resultando en un dispositivo de menor tamaño y consumo que el anterior, el interconexión se realizará según Figura 8.

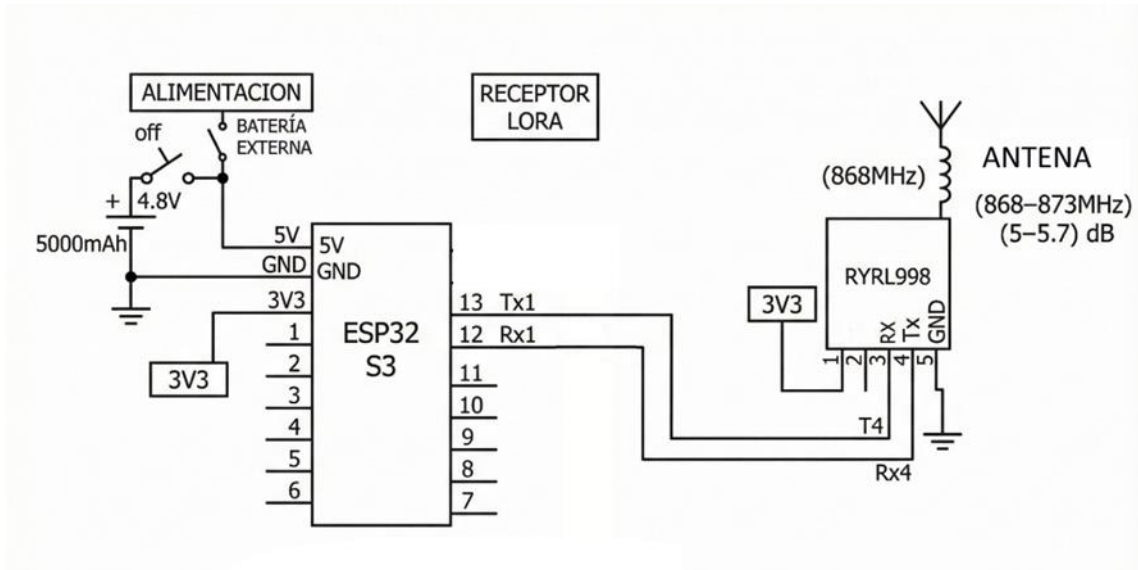


Figura 8. Conexión Gateway. Fuente: elaboración propia.

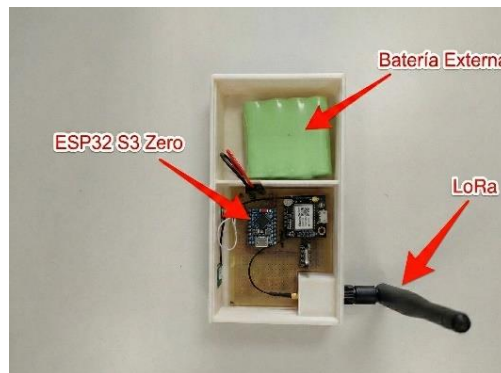


Figura 9. Prototipo Gateway. Fuente: elaboración propia.

#### 4.4. Diseño de red LoRa y protocolo de comunicación

El modelo elegido para la red de comunicación entre sensores será mediante radio *LoRa*, dado que estamos en Europa, la banda de frecuencia a utilizar es la 868 MHz. Posteriormente, la comunicación con el dispositivo de mando final será mediante IP por *Wifi* o por cable.

Cada elemento sensor (dispositivo final) constará de un sensor y una antena mediante la cual transmitirá la información a un *Gateway*, que será el dispositivo que utilice el mando y a través del cual, dependiendo de la situación táctica (si es ambiente electrónicamente degradado o no) podrá obtener la información a través de una página web a través de Internet o conectarse por cable al *Gateway* para acceder a esta.

De este modo, la red (Figura 10) estará compuesta por dos elementos principales:

- Emisor (*end device*): en el caso de este proyecto serán los conjuntos de sensores en base a *Raspberry* con los transmisores *LoRa*.
- Receptor (*Gateway*): puerta de enlace que se comunica con los transmisores de los sensores, escucha los mensajes enviados y permite servir los datos al operador y subirlos a la plataforma de visualización de datos. Los datos son leídos e interpretados por el operador conectando bien un ordenador, tablet o móvil al servidor web integrado en el ESP-32 bien a través de *WiFi* o por cable o bien a través de *Thingsboard* [85] en escenarios en los que es viable el uso de Internet.



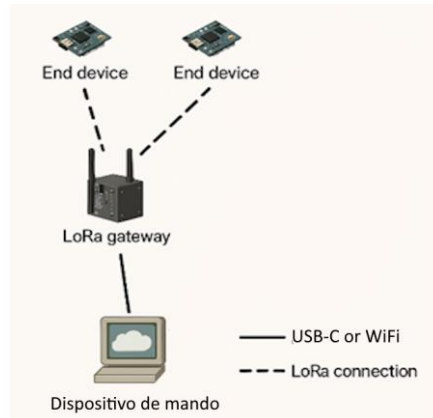


Figura 10. Arquitectura de red LoRa. Fuente: [16]

La comunicación entre emisor y receptor *LoRa* debe ofrecer garantía de que no va a ser fácilmente interceptable por el enemigo. Primeramente, se minimizará el número de envíos de información que se realizarán por parte de los emisores teniendo un tiempo de emisión definido por el tiempo que tarde en enviar un texto plano (ver Anexo I ). De esta manera, el único dispositivo detectable mediante guerra electrónica sería el emisor, por lo que el receptor que sería el utilizado en el puesto de mando permanecería en silencio la mayor parte del tiempo garantizando la supervivencia de este.

En la actualidad, no es posible garantizar la no interceptación de una emisión por un medio no guiado. Uno de los principales retos en la implementación de sistemas de comunicación basados en tecnología *LoRa* es la limitación de ciertos módulos comerciales para realizar cambios dinámicos de frecuencia durante la operación [86]. El módulo RYLR998, ampliamente utilizado por su simplicidad y bajo consumo, permite modificar la frecuencia únicamente mediante comandos AT [87].

Para definir una estrategia de pseudo-salto de frecuencia se propone que el evento de cambio se active cuando el *Gateway* acumule un umbral de  $N$  mensajes recibidos procedentes de cualquiera de los emisores. Esta elección se fundamenta en tres aspectos técnicos principales [88]. Primero, al usar el número de mensajes como métrica, el salto se adapta dinámicamente al tráfico real de la red; lo que permite una mayor frecuencia de saltos en periodos de alta actividad y una menor frecuencia cuando la red está menos activa, optimizando el equilibrio entre seguridad y eficiencia. Segundo, el conteo de mensajes requiere una carga computacional y de comunicación mínima en el *Gateway*, sin necesidad de complejos cálculos temporales o sincronización de relojes, lo que es coherente con los entornos de bajo consumo. Tercero, teniendo en cuenta que las intervenciones de salto implican una interrupción (temporal) de la transmisión, ajustar  $N$  permite amortizar ese coste y evitar saltos innecesarios en momentos de baja actividad.

La relación entre el umbral  $N$ , la tasa media de mensajes recibidos  $R$  (mensajes por unidad de tiempo) y el objetivo de intervalo de salto  $T_{obj}$  puede expresarse como:

$$N = \lceil T_{obj} \cdot R \rceil$$

De esta forma, si por ejemplo  $R = 1$  mensajes/minuto y se desea un salto aproximadamente cada  $T_{obj} = 10$  minutos, se obtendría  $N \approx 10$ . Esta metodología proporciona una base cuantitativa para ajustar el parámetro en función de la carga real de la red.

Una condición operativa esencial es que el *Gateway* verifique la conectividad con todos los emisores antes de proceder al salto de frecuencia. Este paso es crítico para garantizar que ningún nodo quede desconectado o desincronizado como consecuencia del cambio. Para realizar esta comprobación con el menor coste posible en términos de ancho de banda y consumo energético, se considera la utilización de tramas de aplicación de tipo “ping ligero” (*payload* mínimo, trama confirmada). Esta técnica permite verificar la bidireccionalidad del enlace





sin recurrir a protocolos de alto *overhead* (como ICMP sobre IP) que no resultan adecuados en entornos LPWAN [89]. Si un emisor no responde tras 2 intentos, el *Gateway* lo marca como no verificado y continua con la comprobación de dispositivos emisores. Una vez finalizado, inicia rondas de reintento hasta un máximo de 5 intentos por dispositivo no verificado. Esta política asegura que el salto solo proceda cuando todos los emisores se hayan verificado, garantizando la coherencia de la red al cambiar de frecuencia.

Una vez superada la verificación, el *Gateway* procede al anuncio y coordinación del salto de frecuencia el cual comunicará a todos los emisores.

Este mecanismo garantiza la sincronía entre los nodos y el *Gateway*, reduce la ventana de inconsistencia y minimiza la posibilidad de que un nodo quede descolgado tras el salto.

La política adoptada establece que no se ejecutará el salto hasta que todos los emisores hayan respondido satisfactoriamente. Sin embargo, para evitar bloqueos indefinidos se considera implementar un límite de intentos  $R_{\max} = 5$  y una temporización máxima de espera. Si tras estas rondas aún existen emisores sin respuesta, el sistema debe posponer el salto, generar una alarma pertinente y registrar los nodos implicados de manera que se alerta la no operatividad de estos.

Este procedimiento, aunque no constituye un salto de frecuencia real en tiempo de transmisión, incrementa la dificultad de interceptación y reduce la vulnerabilidad frente a ataques de escucha pasiva, sin necesidad de incorporar hardware especializado ni modificar el *firmware* del módulo. La solución propuesta se integra de manera eficiente en el sistema, aprovechando la capacidad de la *Raspberry Pi* para gestionar tanto el control de los sensores como la lógica de comunicación, garantizando así la sincronización entre actualización de parámetros de frecuencia.

Por otro lado, y complementando al salto de frecuencia, se incluirá un cifrado lógico XOR para el mensaje de alerta enviado consistente en una clave conocida tanto por emisor como por receptor. El cifrado XOR se basa en la operación lógica *Exclusive OR* que trabaja bit a bit sobre dos entradas. La operación devuelve un uno únicamente cuando los bits de entrada son distintos, y un 0 cuando son iguales. Su principal ventaja es que es reversible: si se aplica XOR entre un mensaje y una clave, basta con volver a aplicar XOR con la misma clave para recuperar el mensaje original. Cuando un texto se transmite, primero se convierte en una secuencia de bytes. A cada uno de los bytes se le aplica la operación con un byte de la clave. Si la clave tiene varios bytes, se van usando uno a uno y, si es más corta que el mensaje, suele repetirse.

Por último, es necesario asegurar el envío de todos los mensajes a transmitir por lo que surge la necesidad de crear un *buffer* que almacene y envíe los mensajes que por algún casual no hayan sido enviados con éxito (ej. El salto de frecuencia ha interrumpido el envío, etc.). Se implementa un *buffer* de reintentos para el envío de mensajes, cuya función es asegurarse de que los mensajes no se pierdan si en el momento de transmitirlos ocurre algún fallo. El mecanismo funciona de la siguiente manera, cuando llega un nuevo mensaje, primero se intenta enviarlo directamente. Si el envío falla, en lugar de descartarlo, el mensaje se guarda en el *buffer* en la posición que indica el orden de prioridad por el que debe ser reenviado en caso de haber varios, que actúa como un puntero circular de tamaño diez. Esto significa que el *buffer* va almacenando hasta diez mensajes pendientes y, si se llena, el índice vuelve al inicio sobrescribiendo los más antiguos dado que el objetivo del dispositivo es advertir de eventos que ocurren en tiempo real perdiendo relevancia eventos captados en el pasado frente a los modernos.

Más tarde se recorre todo el *buffer* con un ciclo *for*. Para cada posición que contenga un mensaje pendiente, se vuelve a intentar enviarlo. Si en ese intento la función devuelve éxito, el mensaje se borra de la posición correspondiente, liberando espacio. De este modo, el *buffer* funciona como un sistema de cola de retransmisión: asegura que los mensajes que no pudieron enviarse en el primer lugar se conserven temporalmente y se sigan reintentando



hasta que finalmente logren transmitirse, evitando la pérdida de información en comunicaciones poco fiables.

Como hito final al protocolo de comunicación, es necesario añadir un método de interpretación de los diferentes mensajes que llegan al dispositivo receptor y presentarlos mediante una interfaz que sea amigable de tipo página web Anexo IV. La solución para esta necesidad adopta dos métodos, dependiendo de la situación táctica en que se pretendan utilizar los dispositivos.

- Ambiente electrónicamente degradado: la transmisión de datos se realizará por cable y se accederá a un servidor web local ubicado en el dispositivo receptor al cual se accederá mediante su dirección IP.
- Supremacía electrónica: siempre y cuando se considere seguro, se podrá habilitar al dispositivo receptor comunicar los mensajes a una página web por WiFi en local y una página web remota privada de haber GPRS, facilitando el acceso a la información que los sensores nos ofrecen. En este caso concreto se ha usado la *Community Edition* [90] la cual es gratuita y completamente de fuente abierta, su arquitectura está diseñada para ser escalable, robusta y eficiente a la vez que adaptable y duradera. La estructura básica de *Thingsboard* [85] se muestra en la Figura 11. Esta plataforma permite recopilar procesar y visualizar datos provenientes de dispositivos conectados y será utilizada para ubicar en un plano las alertas provenientes de los diferentes dispositivos facilitando la acción de C2 (mando y control).

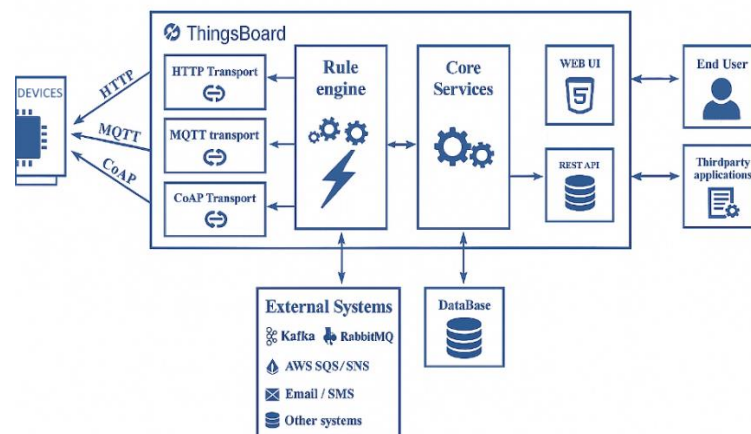


Figura 11. Arquitectura de Thingsboard. Fuente:[91]

El protocolo de comunicación que se aprecia en la Figura 12 muestra el procesamiento de los mensajes en el *Gateway* en el caso de que un dispositivo sensor envíe una alerta en la que se identifica al sensor que la está enviando y se recibe el mensaje cifrado por XOR para ser descifrado con la clave simétrica correspondiente dentro del *Gateway*. Los datos enviados en el mensaje son: identificador de dispositivo sensor para el conocimiento de la ubicación donde se ha producido la detección junto con la correspondiente alerta atendiendo al tipo de detección permaneciendo cifrada hasta su procesamiento.



```

59.906 -> Msj Recibido: +RCV=2,ALERT,03:12 ← MENSAJE ENVIADO DE NODO SENSOR
59.999 -> Num_Sensor: 2 Tipo de detección: ALERT Hora: 03:12
59.999 -> ----- ENVIO DATOS NODO SENSOR A THINGSBOARD
59.999 -> ¡Dato actualizado de SLAVE en WEBSEVER!
59.999 -> Enviando Mensaje SLAVE: {"RECEP2": [{"detection-type": "ALERT", "time": "03:12"}]}
59.999 -> Datos enviados correctamente!
59.999 -> -----
59.999 -> Enviando Mensaje MASTE{"detection-type": "ALERT", "time": "03:12"} ACTUALIZACION DE DATOS WEBSEVER ESP32-S3
59.999 -> Datos enviados correctamente!
59.999 -> -----
04.146 -> ENVIO DATOS GATEWAY A THINGSBOARD

```

Figura 12. Protocolo y procesado de los mensajes en Gateway. Fuente: elaboración propia.

## 4.5. Validación de red y protocolo de comunicación

El primer paso para realizar la validación del protocolo de comunicación es la elección de procedimiento de actuación para la realización de esta. El método elegido es la simulación mediante software especializado, específicamente NS-3.

NS-3 (*Network simulator 3*) es un simulador de redes de comunicación muy utilizado en investigación y en entornos académicos para estudiar, diseñar y evaluar el comportamiento de redes de computadoras sin necesidad de montar físicamente toda la infraestructura lo cual permite la depuración y corrección de errores antes de pasar a una posterior fase de producción.

Funciona como una herramienta de software libre y de código abierto, escrita principalmente en C++, que permite crear escenarios virtuales en los que se modelan nodos, enlaces, protocolos y aplicaciones de red.

Del protocolo diseñado en el apartado 4.4 es importante saber en qué modo afecta a la transmisión de datos el uso de cifrado XOR y el salto de frecuencia. Para una primera simulación se ha medido la transmisión de cinco paquetes cifrados de los que se obtiene un resultado de rendimiento óptimo. Destacando:

- Tasa de entrega del 100%: todos los paquetes enviados fueron recibidos correctamente, sin pérdidas.
- Latencia promedio de 11,5 ms: adecuada para aplicaciones de alerta o monitoreo en tiempo real.
- Tiempo total de transmisión de 8 s (toda la simulación): consistente con el intervalo de envío de paquetes.

```

Flow 1 (10.1.1.1 -> 10.1.1.2)
Tx Packets: 5
Rx Packets: 5
Lost Packets: 0
Delivery Ratio: 100 %
Average Delay: 0.011504 s
Total Transmission Time: 8.01301 s
Flow 2 (10.1.1.2 -> 10.1.1.1)
Tx Packets: 5
Rx Packets: 5
Lost Packets: 0
Delivery Ratio: 100 %
Average Delay: 0.011504 s
Total Transmission Time: 8.01301 s

```

Figura 13. Resultados primera simulación. Fuente: elaboración propia.<sup>1</sup>

<sup>1</sup> Los valores de latencia y tiempo de transmisión en la Figura 13 no se aproximan a los reales dado que en esta prueba se simula exclusivamente la lógica de la comunicación.



Estos datos demuestran que el sistema propuesto es fiable, eficiente y tolerante a cambios de frecuencia, lo que valida su viabilidad para aplicaciones de bajo consumo y comunicación segura en entornos distribuidos. Además, el uso de cifrado XOR no introdujo penalizaciones significativas en la entrega ni la latencia, confirmando su idoneidad para el presente sistema embebido. Además, los cálculos para tiempo de vuelo y alcance estimados quedan reflejados en Anexo II.

Una vez completada la simulación de la comunicación básica entre un emisor y un receptor, se procede a la fase de validación de la escalabilidad del sistema. En esta etapa se busca evaluar el comportamiento de la red cuando aumenta el número de nodos transmisores y el volumen de mensajes intercambiados, con el objetivo de determinar los límites operativos y la robustez del sistema en situaciones de mayor carga.

Para esta prueba se amplía la simulación al envío de un mensaje tipo “fechahora, ALERT”, (ejemplo para el 04/10/25 a las 13:49 → “041349 ALERT”) que corresponde al formato de mayor longitud previsto para las comunicaciones dentro del sistema propuesto. Este mensaje representa el caso más desfavorable en cuanto a tamaño de trama y consumo de ancho de banda, por lo que resulta adecuado para validar la eficiencia de la comunicación en escenarios exigentes.

La red simulada se compone de 35 dispositivos emisores (número superior al objetivo propuesto en 4.1 Definición de requisitos), dispuestos linealmente a una distancia de 500 metros entre cada nodo. De esta forma, el primer dispositivo corresponde al receptor principal y el último emisor se ubica a 17.500 m (500m x 35) respecto al receptor. Esta configuración permite analizar el comportamiento de la red a lo largo de una extensión considerable, bajo condiciones ideales de propagación.

Los resultados de esta simulación son favorables dado el carácter aleatorio y poco frecuente de los casos en los que se prevé la comunicación entre los dispositivos obteniéndose una latencia media de 104.35 ms incluyendo el soporte de cifrado de mensaje sin que la red se sature por el envío de paquetes entre los dispositivos. La tabla resumen con los datos obtenidos puede consultarse en Anexo III.

## 4.6. Diseño y validación de algoritmo de integración

### 4.6.1. Diseño del proceso<sup>2</sup>

Se entiende como algoritmo de integración a aquel que permitirá el procesamiento de las señales recibidas por los componentes periféricos del dispositivo emisor, es decir, recibirá la señal producida por el PIR en la detección de movimiento y la de la cámara en la detección de los elementos que se consideran de interés. A continuación, se procede a definir las interacciones que se deben dar entre estos y cómo debe proceder el algoritmo para el correcto funcionamiento del aparato emisor.

El estado del PIR cuando no detecte movimiento será LOW, pasando a transmitir la señal HIGH cuando lo detecte.

- La cámara estará constantemente observando y cuando detecte como elemento de interés a personas o vehículos, enviará una señal al procesador para que sepa que se ha detectado movimiento (se parte de la base de que en el momento de la instalación de la cámara no tendrá ninguno de los anteriores elementos delante).
- Cuando se detecte movimiento con el PIR y un elemento de interés con la cámara se

---

<sup>2</sup> Dado que en el apartado 4.4 Diseño de red *LoRa* y protocolo de comunicación ya se ha definido el protocolo de comunicación, este se obviará para este apartado.



generará el mensaje “fecha-hora-ALERT”.

- Cuando se detecte movimiento exclusivamente con el PIR, se generará el mensaje “fecha-hora-MOV”.
- Cuando se detecte movimiento exclusivamente con la cámara, se generará el mensaje “fecha-hora-CAM”.
- El algoritmo estará continuamente leyendo los sensores a la espera de recibir las respectivas señales.

El diagrama presentado en el Anexo V ha sido elaborado mediante la herramienta *Bizagi Modeler* [92], estudiada en la asignatura Sistemas de Información para la Dirección. Esta aplicación permite no solo validar los procesos diseñados, sino también realizar simulaciones ajustando parámetros específicos, con el fin de aproximar el escenario modelado a condiciones lo más cercanas posible a la realidad.

Para la simulación realizada, se establecieron los siguientes parámetros: una probabilidad de error en la detección de los sensores del 2%. En cuanto a los tiempos de ejecución, se consideró un tiempo estimado de 1,5 minutos para el arranque de los sensores, dado que el dispositivo PIR requiere un periodo de adaptación a la radiación reflejada en el área de vigilancia. Para el resto de las tareas (generación, almacenamiento y envío de mensajes) se definió un tiempo de ejecución de un segundo.

Con estos parámetros se llevaron a cabo 1000 simulaciones. Los resultados obtenidos (Tabla 1), resumidos en la tabla correspondiente, permiten extraer las siguientes conclusiones:

De los 1000 procesos simulados<sup>3</sup> en los que se detecta movimiento en todos se alcanza el objetivo final consistente en el envío de los correspondientes mensajes. De este millar de mensajes, 954 corresponden a mensajes ALERT, correspondientes al correcto funcionamiento del algoritmo y ambos sensores, y 23 mensajes CAM y 23 MOV resultado del posible fallo de uno de los dos sensores sin fallar ambos simultáneamente de manera prolongada en el tiempo pues constantemente el algoritmo lee las señales de estos.

| Nombre                          | Tipo             | Instancias completadas |
|---------------------------------|------------------|------------------------|
| ENCENDIDO                       | Evento de inicio | 1000                   |
| Establecimiento de comunicación | Tarea            | 1000                   |
| Arranque de sensores            | Tarea            | 1000                   |
| Lectura de sensores             | Tarea            | 1000                   |
| ¿PIR detecta mov?               | Compuerta        | 1000                   |
| ¿Cámara detecta elemento?       | Compuerta        | 977                    |
| ¿Cámara detecta elemento?       | Compuerta        | 23                     |
| Generar mensaje 'CAM'           | Tarea            | 23                     |
| Generar mensaje 'MOV'           | Tarea            | 23                     |
| Generar mensaje 'ALERT'         | Tarea            | 954                    |
| Envío de mensajes               | Tarea            | 1000                   |

Tabla 1. Resultados de simulación de proceso. Fuente: elaboración propia.

#### 4.6.2. Validación de algoritmo de integración mediante simulación

Una vez verificado el correcto funcionamiento lógico del proceso desarrollado, se

<sup>3</sup> Nota: para estas simulaciones no se han tenido en cuenta procesos aleatorios como el paso de animales o movimiento generado por caída de árboles que podrían introducir nuevos mensajes, acotando la simulación al paso exclusivo de personas y vehículos.





procede a la validación funcional del algoritmo antes de iniciar la fase de montaje físico y producción del sistema. Con este propósito, se han realizado dos simulaciones diferenciadas, ambas derivadas del código original, que ha sido modificado parcialmente con el fin de adaptarlo a las limitaciones inherentes de los entornos de simulación utilizados.

La primera simulación se ha llevado a cabo utilizando la plataforma *Wokwi* [93], un entorno de desarrollo y simulación en línea diseñado para la emulación de microcontroladores y sistemas embebidos. *Wokwi* permite la ejecución de programas y la visualización del comportamiento de diferentes dispositivos electrónicos, entre los que se incluyen placas basadas en ESP32, Arduino o *Raspberry Pi Pico*, así como diversos sensores y periféricos digitales.

Este simulador ofrece un espacio virtual en el que es posible probar la lógica del código, depurar errores y analizar señales de entrada y salida sin necesidad de disponer de hardware físico, lo que resulta especialmente útil en las etapas preliminares del desarrollo. Además, proporciona herramientas de visualización de pines, terminal serial y depuración paso a paso, facilitando la verificación de la lógica programada y la detección temprana de posibles errores en el algoritmo. A pesar de sus ventajas, presenta ciertas limitaciones a la hora de simular sistemas complejos, como la ausencia de soporte para módulos de comunicación *LoRa* o periféricos de captura de imagen, además de restricciones en la gestión temporal de eventos simultáneos. No obstante, su empleo en este proyecto resulta altamente conveniente, ya que permite verificar el funcionamiento lógico del algoritmo de control, comprobar la gestión de interrupciones y validar la detección de movimiento mediante un sensor PIR, aspectos fundamentales para garantizar la estabilidad del sistema antes de su implementación real.

En la simulación, el código original ha sido adaptado para sustituir las funciones de transmisión *LoRa* por la emulación del envío de mensajes mediante texto en consola, indicando en el momento exacto en que se produciría la transmisión real. Asimismo, se ha omitido la lógica asociada al procesamiento de la cámara, al no ser posible su integración en este entorno.

```
#define PIR_PIN 13

const char* xorKey = "clave123";
const long freqs[] = {868100000, 868300000, 868500000};
int freqIndex = 0;

String bufferMensajes[10];
int bufferIndex = 0;

// Cifrado XOR
String xorEncrypt(String msg, const char* key) {
    String result = "";
    for (int i = 0; i < msg.length(); i++) {
        result += char(msg[i] ^ key[i % strlen(key)]);
    }
    return result;
}

// Simular configuración de frecuencia LoRa
void configurarFrecuencia(long freq) {
    Serial.println("Configurando frecuencia LoRa: " + String(freq));
}
```

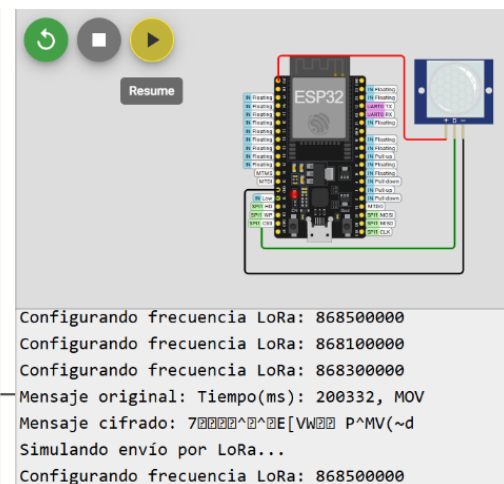


Figura 14. Simulación de funcionamiento del PIR. Fuente: elaboración propia.

Tal y como se muestra en la Figura 14, el algoritmo implementa un cambio de frecuencia predefinido establecido para la simulación. A continuación, se ha incluido la detección de movimiento aproximando un objeto frente al sensor PIR. Este evento genera un mensaje con el formato "fechahora, MOV", que indica la detección de movimiento en el instante de tiempo correspondiente. Dicho mensaje es posteriormente cifrado antes de ser enviado.

Durante la simulación se ha verificado que, tras la detección y cifrado del mensaje, el envío simulado se ejecuta correctamente sin afectar al proceso de salto de frecuencia, lo que confirma la independencia funcional de ambos procesos dentro del algoritmo.

La segunda simulación tiene por objeto la validación del algoritmo de integración con el



periférico que falta en la anterior simulación en sustitución del PIR, la cámara. Dado que esta fase antecede a la adquisición de material físico, se ha optado por adaptar el módulo de detección de imagen a un entorno de simulación en Python, utilizando la webcam del equipo de desarrollo en sustitución de la cámara prevista para la implementación final.

El programa desarrollado en Python (Figura 15) permite realizar detección de movimiento y reconocimiento básico de vehículos en tiempo real, generando un mensaje cifrado cada vez que se detecta un evento relevante. Al igual que en la simulación anterior, la transmisión LoRa ha sido emulada mediante mensajes de texto, debido a las limitaciones del entorno de simulación. No obstante, se ha mantenido la lógica de cifrado y de selección aleatoria de frecuencias de transmisión, replicando con fidelidad el comportamiento esperado del sistema real.

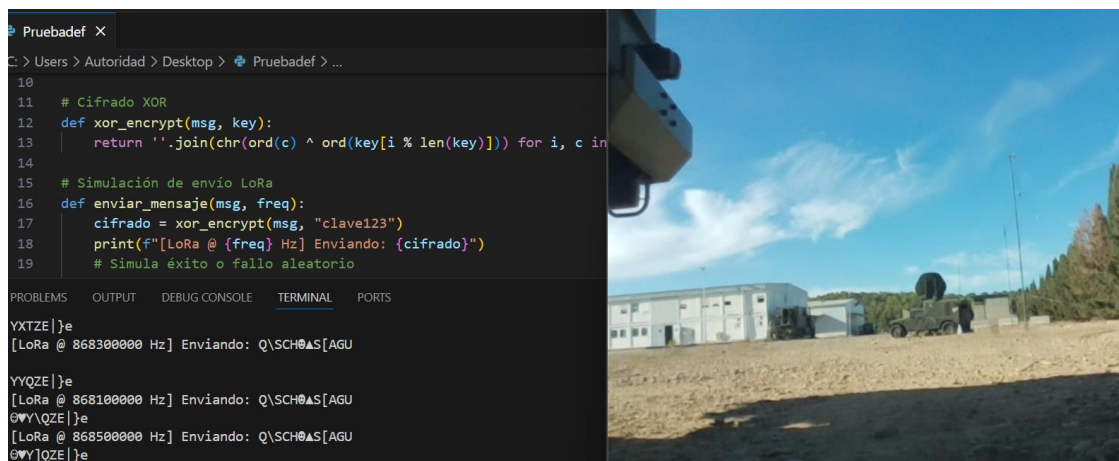


Figura 15. Simulación de funcionamiento de detección de imagen. Fuente: elaboración propia.

Durante la ejecución, se ha observado que, al detectar la presencia de vehículo, el sistema genera un mensaje cifrado que se “envía” a través de la frecuencia activa en ese momento. Para comprobar la eficacia del mecanismo de salto de frecuencia, se han realizado múltiples pruebas en diferentes instantes de tiempo en los que se ha modificado la frecuencia, verificando que el envío del mensaje y el cambio de frecuencia se ejecutan sin interferencias mutuas.

Los resultados obtenidos (Anexo III) en ambas simulaciones permiten validar la coherencia y estabilidad funcional del algoritmo desarrollado, demostrando que la lógica de detección, cifrado y transmisión opera conforme a las especificaciones de diseño establecidas. En consecuencia, se considera que el sistema se encuentra en condiciones adecuadas para avanzar hacia la fase de implementación física y pruebas experimentales, con una base de software previamente verificada y depurada.

#### 4.6.3. Validación prototipada

Una vez demostrada la validez del algoritmo se procede a su implementación en un prototipo compuesto principalmente por la Raspberry Pi 5 con cámara los cuales han sido utilizados para la detección de personas y vehículos tanto de manera aislada como simultánea en espacios abiertos consiguiendo una detección fiable a 25 m como se muestra en la Figura 16 y Figura 17.



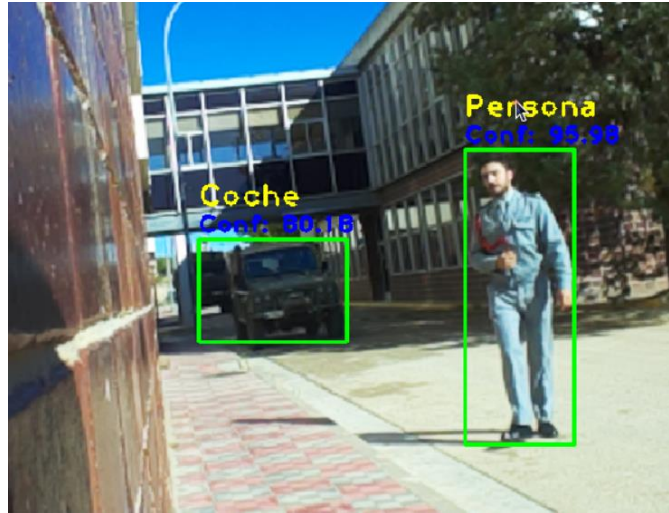


Figura 16. Detección simultanea mediante prototipo. Fuente: elaboración propia.



Figura 17. Detección de vehículo militar mediante prototipo. Fuente: elaboración propia.

## 4.7. Análisis DAFO

El análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades) permite evaluar de forma estructurada los factores internos y externos que afectan al desarrollo y aplicación del sistema propuesto. En este caso, el sistema de detección distribuido basado en sensores ópticos e infrarrojos con comunicación *LoRa* cifrada y arquitectura de red modular se orienta a su implementación en entornos militares, donde la fiabilidad, la discreción y la robustez resultan determinantes.

### Fortalezas

1. Diseño modular escalable: la arquitectura basada en la combinación de *Raspberry Pi 5*, microcontrolador ESP32-S3 y sensores periféricos permite una distribución funcional eficiente entre procesamiento, sensorización y comunicación, favoreciendo la escalabilidad de la red. Esta estructura facilita la incorporación de nuevos nodos o módulos de detección sin necesidad de rediseñar el sistema completo.
2. Comunicación segura y discreta: el empleo de tecnología *LoRa* en la banda de 868 MHz proporciona gran alcance de transmisión con bajo consumo energético, mientras que la inclusión de mecanismos de cifrado XOR y pseudosalto de frecuencia reduce la probabilidad de interceptación o rastreo por medios de guerra electrónica. Esto incrementa significativamente la supervivencia electrónica de la red en escenarios



hostiles.

3. Autonomía y eficiencia energética: el uso de baterías externas de alta capacidad y la optimización del consumo mediante activación por eventos permiten una autonomía aproximada a 24 horas de operación continua, un valor adecuado para misiones de reconocimiento o vigilancia táctica.
4. Compatibilidad con condiciones ambientales adversas: la carcasa protectora, fabricada en PETG, garantiza la resistencia frente a polvo, humedad e impactos. Este nivel de protección hace viable el despliegue del sistema en entornos exteriores o zonas de combate sin comprometer la funcionalidad de los componentes electrónicos.
5. Validación mediante simulación y metodología rigurosa: la verificación del sistema mediante entornos especializados (*Wokwi*, *NS-3*, *Bizagi Modeler*) ha permitido validar la lógica de detección, el protocolo de comunicación y la escalabilidad de la red antes de la implementación física, reduciendo los riesgos y asegurando una base técnica sólida para la posterior implementación del prototipo.

#### Debilidades

1. Dependencia de componentes comerciales: la arquitectura se basa en hardware de propósito general (*Raspberry Pi 5*, *ESP32-S3*, sensores PIR comerciales), lo que puede limitar la robustez ante interferencias electromagnéticas extremas o condiciones climáticas prolongadas, en comparación con equipos de grado militar certificados. Además de comprometer la adquisición de estos componentes a empresas ajenas a la industria militar española ya que la negativa de una sola empresa proveedora de un componente específico pondría en riesgo la construcción del sistema.
2. Capacidad de procesamiento limitada en tiempo real: aunque la *Raspberry Pi* y la *ESP32-S3* ofrecen buen rendimiento para aplicaciones civiles, el procesamiento simultáneo de algoritmos puede reducir la velocidad de respuesta o incrementar la latencia bajo cargas elevadas.
3. Carencia de redundancia en la red: el sistema actual no contempla rutas alternativas de transmisión ni nodos repetidores. La pérdida o destrucción de un nodo crítico como el receptor pondría en riesgo el funcionamiento del sistema.
4. Ausencia de integración de criptografía avanzada: el uso de cifrado XOR, aunque ligero y eficiente, presenta limitaciones en cuanto a nivel de seguridad criptográfica frente a sistemas más sofisticados como AES o RSA, lo que podría comprometer la confidencialidad de la información ante ataques persistentes.
5. Mantenimiento y sustitución manual de baterías: la autonomía del sistema depende de la sustitución física de las baterías, lo que supone un riesgo logístico en operaciones prolongadas o en zonas de difícil acceso.

#### Oportunidades

1. Aplicaciones en entornos de defensa y seguridad: el sistema posee alto potencial de integración en operaciones de vigilancia táctica, reconocimiento avanzado o protección perimetral, tanto en bases fijas como en despliegues temporales, ampliando su campo de aplicación más allá del uso experimental.
2. Evolución hacia redes inteligentes de sensores: su arquitectura modular lo convierte en un candidato idóneo para evolucionar hacia una red de *IoT* militar (*IoMT* o *IoBT*), permitiendo la integración futura de sistemas de mando y control o con redes de comunicaciones seguras cifradas.
3. Optimización mediante inteligencia artificial: la incorporación de modelos de detección



y clasificación de objetos basados en *Deep learning* podría incrementar la precisión del sistema, reduciendo falsos positivos y permitiendo priorizar amenazas según tipo o distancia.

4. Miniaturización y producción de bajo coste: el uso de componentes de bajo consumo y reducido coste facilita la fabricación a gran escala y el despliegue masivo en entornos distribuidos, lo que puede suponer una ventaja estratégica en misiones donde el reemplazo rápido y económico sea prioritario.

#### Amenazas

1. Interferencia y guerra electrónica enemiga: en escenarios militares reales, el enemigo podría utilizar sistemas de *jamming* o *spoofing* para anular las comunicaciones *LoRa*, dificultando la transmisión de datos y comprometiendo la efectividad operativa del sistema.
2. Captura o sabotaje de nodos: la posibilidad de que un dispositivo emisor sea capturado físicamente por fuerzas enemigas representa un riesgo crítico, ya que podría revelar información sobre las claves de cifrado o la topología de la red si no se aplican medidas de autodestrucción o reconfiguración inmediata.
3. Vulnerabilidades en software de código abierto: la dependencia de librerías y entornos de desarrollo de fuente abierta implica el riesgo de vulnerabilidades no detectadas que podrían ser explotadas para manipular el sistema o interceptar datos pese a que se puedan mitigar mediante ofuscadores de código como *Pyarmor* [94] una vez capturado un dispositivo aplicando ingeniería reversa.
4. Limitaciones regulatorias en el espectro de radiofrecuencia: el uso de la banda *LoRa* de 868 MHz se encuentra sujeto a restricciones legales en algunos países o contextos operativos, lo que podría limitar el uso del sistema en misiones interinstitucionales.
5. Obsolescencia tecnológica: la rápida evolución de las plataformas de hardware y protocolos de comunicación puede provocar que, en un corto plazo, algunos componentes o tecnologías (como *LoRa* o determinados microcontroladores) queden superados, requiriendo una actualización del sistema.

El análisis global refleja que el sistema propuesto posee una base técnica sólida y adaptable, con un elevado potencial de aplicación en operaciones de defensa que requieren despliegue rápido, autonomía y comunicación discreta. Sus principales fortalezas se centran en la modularidad, la eficiencia y la seguridad funcional, mientras que las debilidades identificadas se relacionan con la robustez frente a ataques electrónicos y la dependencia de componentes comerciales.

Las oportunidades del desarrollo tecnológico y militar, especialmente en el ámbito del *IoT* y la integración con sistemas de inteligencia artificial, mientras que las amenazas subrayan la necesidad de reforzar la ciberseguridad y la resiliencia del sistema frente a interferencias y capturas.

## 4.8. RESULTADOS

A nivel de la comunicación en simulaciones en las que se ha forzado la interrupción y el envío simultáneo de paquetes de manera aleatoria, se demuestra un aumento en la fiabilidad de envío del 4,5% aproximando la fiabilidad al 100% reduciendo drásticamente la pérdida. Si bien, por otro lado, aumenta ligeramente las colisiones en aire y aumenta ligeramente la latencia sin llegar a producir saturación.

Por otro lado, las simulaciones de sensorización resultan en el aumento y aproximación al 100% de fiabilidad al aplicar la redundancia de sensores para la detección de movimiento siendo



la menor fiabilidad proporcionada por la fusión de los sensores de un 98,74%. Si bien este se reduce al alcanzar el límite de alcance de uno de los sensores, en este caso el PIR cuyo límite de detección está en los 12 m.

Finalmente, el envío de datos a la plataforma *Thingsboard* permite la fácil interpretación de las alertas enviadas por los sensores y su ubicación teniendo de respaldo la web local en el ESP32 para su explotación en escenarios en los que el uso de Internet no sea viable. Dado la viabilidad del uso de GPS en escenarios de guerra convencional [95], se ha considerado la introducción de los datos de posicionamiento de manera manual en las interfaces web mediante la función “Añadir sensor” en la que habría que relacionar cada sensor con la ubicación en la que será colocado previo planeamiento.

## 5. CONCLUSIONES

Tras el análisis y experimentación realizada a partir del modelo propuesto en el presente TFG se redacta este apartado en el que se discuten los resultados obtenidos y se relacionan con el cumplimiento de los objetivos propuestos al inicio en el apartado 2.1.

El presente TFG ha propuesto y validado, mediante modelado y simulación, una arquitectura de nodo sensor autónomo orientada a la detección fiable de movimiento en escenarios de baja conectividad y alta interferencia electromagnética. La propuesta integra redundancia multisensorial, procesamiento local y comunicación por radio *LoRa* con mecanismos de protección ligera, aportando una solución técnica coherente. La contribución más relevante del trabajo es la delineación completa de un flujo de diseño (requisitos → arquitectura hardware → algoritmo de fusión → protocolo → validación por simulación) que puede servir como referencia para desarrollos posteriores orientados a prototipado físico y ensayo en campo. El estudio ha identificado y documentado vacíos técnicos y operativos en la literatura y en soluciones existentes (p. ej. integración multisensorial con almacenamiento local y reenvío en redes *LoRa* punto-a-punto), justificando la necesidad y la pertinencia del presente desarrollo.

A continuación, se enumeran los objetivos formulados en el proyecto y la conclusión asociada que explica en qué grado se ha alcanzado cada uno.

**Objetivo principal.** Se considera alcanzado. Se ha diseñado la arquitectura del nodo sensor y receptor junto con un algoritmo de fusión multisensorial adaptado al entorno operativo; además el sistema de comunicación fue modelado y evaluado mediante simulaciones que apuntan a una operatividad viable en condiciones de conectividad degradada. No obstante, la validación se limita a entornos simulados: la implementación física del sistema completo junto con pruebas experimentales en campo con medios reales de EW quedan fuera del alcance del proyecto. Por tanto, el diseño está validado a nivel conceptual, pero requiere prototipado y ensayos experimentales para considerarse plenamente verificado.

De los objetivos secundarios (2.1.2)

**Objetivo 1.** Se considera alcanzado. Se establecieron y justificaron requisitos funcionales y no funcionales (tiempos de respuesta, métricas de fiabilidad, criterios de autonomía, protección mecánica y límites operativos) (4.1). Estos requisitos guiaron la selección de componentes y las decisiones de diseño. La comprobación del cumplimiento se realizó sobre modelos de simulación, análisis teórico además de realizarse la validación empírica de autonomía, resultados recogidos en Anexo III.

**Objetivo 2.** Se considera alcanzado a nivel conceptual y de simulación. Se definió un algoritmo de fusión (Anexo V) que prioriza la correlación temporal entre detección PIR/cámara y una regla de decisión basada en umbrales y confirmación cruzada. Las simulaciones de funcionamiento y las pruebas de lógica muestran una reducción proyectada de falsos positivos respecto a detección única aumentando la fiabilidad de detección en el rango de alcance de ambos sensores (PIR y cámara) desde un 82% hasta 98,74% (Anexo III, Tabla 8); sin embargo,



la eficacia real frente a escenarios complejos (iluminación adversa, movimiento de vegetación, firmas térmicas variables, etc.) requiere de ensayo físico y ajuste de parámetros.

Objetivo 3. Se considera alcanzado funcionalmente en modelo. Se definieron estructuras de mensajes, políticas de retransmisión (*store-and-forward*) y mecanismos de ofuscación (cifrado ligero tipo XOR) y pseudo-salto de frecuencia aplicable a módulos comerciales. Las simulaciones con NS-3 muestran que la política de minimización de envíos y el *buffering* local mejoran la disponibilidad de alertas en condiciones intermitentes aumentando la fiabilidad de la comunicación de un 95,16% al 99,66% (Anexo III, Tabla 5). No obstante, se reconoce que los mecanismos de seguridad implementados son soluciones de compromiso (ligeras) y no sustituyen criptografía robusta (p. ej. AES) o saltos de frecuencia reales cuando la amenaza así lo exija; su adecuación depende del análisis de riesgo operacional y de la capacidad del hardware.

Objetivo 4. Se considera alcanzado. Se seleccionaron y justificaron componentes (*Raspberry Pi 5*, ESP32-S3, Arducam OV5647, AM312, RYLR998, conjunto de alimentación) y se propuso un diseño la carcasa protectora según criterios IP y térmicos adecuados para integrar el sistema. El diseño (Figura 7) contempla las interfaces eléctricas y la distribución energética. La viabilidad práctica del conjunto se infiere por cálculo de autonomía mediante medición prototipada y por la compatibilidad entre módulos.

Objetivo 5. Alcanzado en el ámbito de simulación. Las simulaciones realizadas en NS-3 y los modelos desarrollados en Python/C++ permitieron evaluar el comportamiento de la red y del algoritmo en escenarios parametrizados (topologías, niveles de interferencia, tasas de emisión). Los resultados anteriores sugieren la viabilidad técnica del diseño y permiten identificar parámetros de configuración recomendables [frecuencias utilizables entre 869,4-869,65 (habiendo más frecuencias, pero siendo estas las más óptimas a la par que legales en Europa), SF 12, ancho de banda 125 kHz, CR 4/5, potencia 22dBm], necesidad de planificación previa del despliegue del sistema. Sin embargo, la correspondencia exacta entre simulación y comportamiento real requiere calibración empírica. Además, el haber realizado mediciones de consumo reales (Figura 2) ha permitido estimar la autonomía del sistema además de implementar métricas de fiabilidad de la detección para la comprobación de esta.

## 5.1. Líneas de investigación futuras

El presente Trabajo Fin de Grado ha contribuido al estudio y desarrollo de soluciones tecnológicas vinculadas *IoT*, centradas en la integración de sistemas embebidos, la comunicación entre dispositivos y la gestión eficiente de datos en entornos operativamente exigentes. No obstante, el rápido avance tecnológico en este campo abre múltiples líneas de investigación que, en el futuro próximo, permitirán consolidar y ampliar los logros obtenidos.

En relación con el objetivo de diseño e implementación de sistemas embebidos adaptados al *IoT*, una línea prioritaria de investigación se orienta hacia el desarrollo de arquitecturas distribuidas basadas en *edge e fog computing*. Estas permitirán aumentar la capacidad de procesamiento local, reducir la latencia y mejorar la autonomía de los nodos de red, aspectos críticos en operaciones donde la conectividad con infraestructuras centrales puede ser limitada o intermitente.

Respecto al objetivo de garantizar la comunicación segura y eficiente entre dispositivos, las futuras investigaciones apuntan al empleo de tecnologías de *blockchain*, criptografía poscuántica y autenticación basada en identidades distribuidas (DID). Estos enfoques reforzarán la integridad y confidencialidad de la información transmitida, al tiempo que facilitarán la trazabilidad de los eventos dentro del sistema *IoT*. Además, el uso de inteligencia artificial aplicada a la detección de intrusiones y la respuesta autónoma a ciberataques constituye una de las tendencias más prometedoras en materia de ciberseguridad táctica.

En relación con la optimización de la eficiencia energética y la sostenibilidad operativa de los dispositivos desplegados, se prevé un auge en el estudio de sistemas de gestión energética





inteligentes y fuentes de energía híbridas o autoalimentadas mediante recolección de energía ambiental (*energy harvesting*) así como se deberá complementar con pruebas físicas que impliquen exposición prolongada a factores ambientales. Estas soluciones buscan incrementar la autonomía de los sensores y unidades de comunicación, reduciendo la necesidad de mantenimiento en escenarios de difícil acceso.

Desde una perspectiva más futurista, el *IoT* evolucionará hacia ecosistemas donde la inteligencia colectiva y los enjambres autónomos (*swarm intelligence*) permitirán la coordinación de múltiples agentes robóticos o humanos para la ejecución cooperativa de misiones como ya lo es *EagleEye* [96] de Anduril [97]. La investigación en algoritmos de consenso distribuido, aprendizaje multiagente y toma de decisiones descentralizada resultará esencial para alcanzar este objetivo.

En conjunto, las líneas de investigación futuras del *IoT*, directamente relacionadas con los objetivos de este trabajo, se orientan hacia la creación de un entorno operativo más autónomo, inteligente, seguro y resiliente, capaz de adaptarse a condiciones extremas y responder de forma dinámica ante amenazas emergentes. Estas tendencias consolidarán el papel del *IoT* como pilar tecnológico en la transformación digital del ámbito militar y de defensa.

## 5.2. Conclusión final

En conclusión, el desarrollo de este Trabajo Fin de Grado ha permitido analizar y materializar los principios fundamentales del *IoT*, abordando el diseño, implementación y evaluación de sistemas embebidos orientados a la comunicación y gestión inteligente de información en entornos operativamente críticos. A través del cumplimiento de los objetivos propuestos, se ha demostrado la viabilidad técnica de integrar tecnologías de sensorización, conectividad y procesamiento distribuido en escenarios tácticos, garantizando al mismo tiempo la seguridad y eficiencia en la transmisión de datos. Los resultados obtenidos evidencian el potencial del sistema propuesto como herramienta estratégica para la mejora de la coordinación, la autonomía y la toma de decisiones en contextos de defensa, sentando las bases para futuras investigaciones centradas en la optimización energética, la ciberseguridad avanzada y la incorporación de inteligencia artificial distribuida en sistemas de próxima generación.

En conjunto, el sistema presenta un alto grado de madurez conceptual, siendo técnicamente viable y estratégicamente relevante, aunque requiere evolución hacia versiones más seguras redundantes y criptográficamente robustas para su aplicación real en entornos o emergencias reales.



## REFERENCIAS BIBLIOGRÁFICAS

- [1] Ministerio de Defensa, «Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa», Boletín Oficial del Estado, n.º 295, sec. I, p. 116898, 10 de diciembre de 2015. [En línea]. Disponible en: [https://www.boe.es/eli/es/o/2015/12/03/def2639\\*\\*](https://www.boe.es/eli/es/o/2015/12/03/def2639**)
- [2] Centro Conjunto de Desarrollo de Conceptos (CCDC), «ENTORNO OPERATIVO 2035 PRIMERA REVISIÓN», Ministerio de Defensa, Secretaría General Técnica, 2019. Accedido: 4 de noviembre de 2025. [En línea]. Disponible en: <https://publicaciones.defensa.gob.es/entorno-operativo-2035-primera-revision-libros-pdf.html>
- [3] Ministerio de Defensa, «Centros Universitarios de Defensa». Accedido: 5 de noviembre de 2025. [En línea]. Disponible en: <https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Presentacion/OrganizacionID/Paginas/CentrosUniversitarios.aspx>
- [4] Canva, «Plantillas», Canva. Accedido: 5 de noviembre de 2025. [En línea]. Disponible en: <https://www.canva.com/templates>
- [5] Corporation for Digital Scholarship, «Zotero | Your personal research assistant». Accedido: 5 de noviembre de 2025. [En línea]. Disponible en: <https://www.zotero.org/>
- [6] IOTROUTER, «LoRa Esquema de Transmisión Punto a Punto Vs. LoRaWAN - IOTROUTER». Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://en.iotrouter.com/es/lora-point-to-point-transmission-scheme-vs-lorawan/>
- [7] «Desarrollo de interfaz Web para red LoRa», Documento técnico, 2020. Accedido: 10 de octubre de 2025.
- [8] M. M. Núñez y A. S. M. Sala, «Diseño e implementación de una red de sensores LoRa para la monitorización de ganado vacuno», trabajo Fin de Máster, Universitat Politècnica de Catalunya, Barcelona, España, 2021. Accedido: 12 de octubre de 2025.
- [9] Raspberry Pi Foundation, «Presentando PiVision Lab: Detección de Objetos en Tiempo Real con la Raspberry Pi AI Camera », Raspberry Pi Forums. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://forums.raspberrypi.com/viewtopic.php?t=385522>
- [10] Marcombo, «Cómo crear un sistema de detección de movimiento con Raspberry Pi», Marcombo. Libros técnicos, de arte, formación y científicos. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://www.marcombo.com/archivo/como-crear-un-sistema-de-deteccion-de-movimiento-con-raspberry-pi/>
- [11] Telegram FZ-LLC, «Telegram: una nueva era de mensajería», Telegram. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://telegram.org/>
- [12] A. G. López y J. C. Martínez, «Propuesta de un sistema de seguridad con cámaras y sensores usando tecnología Raspberry-Pi, en el colegio Bautista de la Concepción, Masaya en el año 2020», Tesis de Grado, Universidad Nacional Autónoma de Nicaragua, Managua, 2020. Accedido 5 de octubre de 2025.
- [13] D. M. Calle, «Seguridad en Dispositivos IoT para Redes LoRa», Trabajo de fin de grado, Universidad de los Andes, Bogotá, 2024. [En línea]. Disponible en:





<https://hdl.handle.net/1992/74229>

[14] M. A. R. Giraldo, «Pruebas de seguridad a nivel de radio (Espectro 915 MHz), en dispositivos LPWA (LoRa)», Trabajo de Grado, Universidad Piloto de Colombia, Bogotá, 2024.

[15] R. Carrillo, «Qué es LoRa, cómo funciona y características principales», Venco Electrónica. Accedido: 1 de noviembre de 2025. [En línea]. Disponible en: <https://www.vencoel.com/que-es-lora-como-functiona-y-caracteristicas-principales/>

[16] A. Augustin, J. Yi, T. Clausen, y W. Townsley, «A Study of LoRa: Long Range & Low Power Networks for the Internet of Things», *Sensors*, vol. 16, n.º 9, p. 1466, sep. 2016, doi: 10.3390/s16091466.

[17] Semtech Corporation, «Home», Semtech (formerly Sierra Wireless). Accedido: 20 de octubre de 2025. [En línea]. Disponible en: <https://www.sierrawireless.com/>

[18] Catsensors, «Tecnología LoRA y LoRAWAN - Catsensors». Accedido: 1 de noviembre de 2025. [En línea]. Disponible en: <https://www.catsensors.com/es/lorawan/tecnologia-lora-y-lorawan>

[19] Tecnore Sound Systems, «Efecto Doppler: Qué Es, Cómo Funciona Y Aplicaciones Reales | Tecnore®». Accedido: 1 de noviembre de 2025. [En línea]. Disponible en: <https://www.tecnore.com/es/article/efecto-doppler/>

[20] A. Berni y W. Gregg, «On the Utility of Chirp Modulation for Digital Signaling», *IEEE Trans. Commun.*, vol. 21, n.º 6, pp. 748-751, jun. 1973, doi: 10.1109/TCOM.1973.1091721.

[21] Y. K. Huang, «¿Cuál es la tecnología detrás de la frecuencia LoRa? - MOKOSmart», MOKOSmart. Accedido: 28 de octubre de 2025. [En línea]. Disponible en: <https://www.mokosmart.com/es/lora-frequency/>

[22] E. F. Silva *et al.*, «Adaptive Parameters for LoRa-Based Networks Physical-Layer», *Sensors*, vol. 23, n.º 10, p. 4597, may 2023, doi: 10.3390/s23104597.

[23] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, y M. Pettissalo, «On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology», en *2015 14th International Conference on ITS Telecommunications (ITST)*, Copenhagen, Denmark: IEEE, dic. 2015, pp. 55-59. doi: 10.1109/ITST.2015.7377400.

[24] M. Asad Ullah, J. Iqbal, A. Hoeller, R. D. Souza, y H. Alves, «K-Means Spreading Factor Allocation for Large-Scale LoRa Networks», *Sensors*, vol. 19, n.º 21, p. 4723, ene. 2019, doi: 10.3390/s19214723.

[25] P. Maurya, A. Singh, y A. A. Kherani, «A review: spreading factor allocation schemes for LoRaWAN», *Telecommun. Syst.*, vol. 80, n.º 3, pp. 449-468, jul. 2022, doi: 10.1007/s11235-022-00903-4.

[26] 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, n.º 5, pp. 60-67, oct. 2016, doi: 10.1109/MWC.2016.7721743.

[27] R. P. Ltd, «Buy a Raspberry Pi 5», Raspberry Pi. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://www.raspberrypi.com/products/raspberry-pi-5/>

[28] Raspberry Pi Foundation, «Presentando PiVision Lab: Detección de Objetos en Tiempo



Real con la Raspberry Pi AI Camera », Raspberry Pi Forums. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://forums.raspberrypi.com/viewtopic.php?t=385522>

[29] T. Dhake, V. D. Chaudhari, H. T. Ingale, H. V. Dhande, y M. N. Patil, «Literature Review and Methods for Real Time Object detection using Raspberry Pi», *Int. J. Innov. Eng. Sci.*, vol. 10, n.º 7, pp. 30-34, jun. 2025, doi: 10.46335/IJIES.2025.10.7.7.

[30] Lviv Polytechnic National University, R. Diachok, I. Tepliako, M. Lapko, A. I. Popov, y Institute of Solid State Physics University of Latvia, «Efficiency and accuracy: comparison of PIR, OpenCV with a webcam, and Raspberry Pi», *Adv. Cyber-Phys. Syst.*, vol. 10, n.º 1, pp. 77-82, may 2025. [En línea]. Disponible en: <https://science.lpnu.ua/acps/all-volumes-and-issues/volume-10-number-1-2025/efficiency-and-accuracy-comparison-pir-opencv>

[31] A. L. Zekovic, «Hardware and Software of Computer Vision IoT Solutions Leveraging Raspberry Pi Boards» *Telfor Journal*, vol. 17, n.º 1. Accedido 30 de septiembre de 2025. [En línea]. Disponible en: [https://journal.telfor.rs/Published/Vol17No1/Vol17No1\\_A1.pdf](https://journal.telfor.rs/Published/Vol17No1/Vol17No1_A1.pdf)

[32] EMS, «HC-sr505: A Complete Guide», EMS. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://electronicmanufacturingservice.org/hc-sr505-a-complete-guide/>

[33] Universidad Nacional del Centro del Perú, «Edificios Inteligentes y Sensores PIR - Monografía de Ingeniería 2025», Studocu. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://www.studocu.com/pe/document/universidad-nacional-del-centro-del-peru/matematicas-i/edificios-inteligentes-y-sensores-pir-monografia-de-ingenieria-2025/142182050>

[34] J. D. R. Munca, «Dispositivo LoRa de comunicación a largo alcance y bajo consumo energético para aplicaciones del ámbito del desarrollo», Trabajo Fin de Grado, Universidad Distrital Francisco José de Caldas, Bogotá, 2019.

[35] J. D. O. Auza, «Estudio sobre las características del protocolo de transmisión de LoRa», Trabajo de fin de grado, Universitaria Agustiniiana, Bogotá, 2020. [En línea]. Disponible en: <https://repositorio.uniagustiniana.edu.co/items/909f5466-55e7-4066-8a11-df42f3f1eb06>

[36] W. Pantoja, J. Perez-Taborda, A. Ávila, y J. de, «Materiales Sostenibles para Baterías con Alta Capacidad de Energía», *Revista Colombiana de Materiales*, no. 15, pp. 1-10

[37] Universidad Técnica de Cotopaxi Ecuador, E. J. Jácome Espinoza, F. R. Romero Bedón, Universidad Técnica de Cotopaxi Ecuador, A. D. Paredes Anchatipán, y Universidad Técnica de Cotopaxi Ecuador, «Revisión de la Literatura para Gestión de Sistemas de Almacenamiento de Energía por Medio de Baterías para Determinar su Eficiencia», *Polo Conoc.*, vol. 9, n.º 7, pp. 1478-1495, jul. 2024, doi: 10.23857/pc.v9i7.7579.

[38] U.S Army «SORAS 6 Sound Ranging System» en Worldwide Equipment Guide (WEG), vol. 1: Ground Systems, U.S. Army TRADOC Intelligence Support Activity, 2015, pp. 6-12. Accedido 20 de octubre de 2025[En línea]. Disponible en: <https://odin.tradoc.army.mil/WEG/Asset/cbfb8966ae59c186539a80350d72377>

[39] «LDO\_UK25\_01362 HALO - Hostile Artillery LLocation System - Datasheet\_LQ».

[40] Academia de Artillería, «Memorial de Artillería» n.º 160-2, Ministerio de Defensa, Madrid, diciembre de 2004. Accedido 4 de noviembre de 2025. [En línea]. Disponible en: <https://publicaciones.defensa.gob.es/memorial-de-artiller-a-160-2.html>

[41] U.S Air Force, «Electronic Warfare Fundamentals» Nellis Air Force Base, NV: 57th Wing,



noviembre de 2000 Accedido 4 de noviembre de 2025. [En línea]. Disponible en: [https://archive.org/details/electronicwarfarefundamentals\\_201908](https://archive.org/details/electronicwarfarefundamentals_201908)

[42] O. J. Salcedo-Parra y N. G. Agudelo-Cristancho, «Desempeño RSSI de nodos sensores LoRa, BLE y WiFi en un sistema IoT interoperable», *Aibi Rev. Investig. Adm. E Ing.*, vol. 9, n.º 2, pp. 19-32, ago. 2021. [En línea]. Disponible en: <https://revistas.udes.edu.co/aibi/article/view/2490>

[43] A. Maroşan, G. Constantin, C. E. Gîrjob, A. L. Chicea, M. Crenganiş, y F. Morariu, «Real-time data acquisition with ESP32 for IoT applications using open-source MQTT brokers» *Proceedings in Manufacturing Systems*, vol. 19, n.º 2, pp. 61-68, 2024. [En línea]. Disponible en: <https://journals.indexcopernicus.com/publication/4181158>

[44] P. Rahman y S. Mehnaz, «International Journal for Multidisciplinary Research (IJFMR)», *SSRN Electron. J.*, 2024, doi: 10.2139/ssrn.5054029.

[45] Ceupe, «Sistema embebido: Qué es, características y componentes», Ceupe. Accedido: 1 de noviembre de 2025. [En línea]. Disponible en: <https://www.ceupe.com/blog/sistema-embebido.html>

[46] «Sistema embebido», *Wikipedia, la enciclopedia libre*. 13 de abril de 2025. Accedido: 1 de noviembre de 2025. [En línea]. Disponible en: [https://es.wikipedia.org/w/index.php?title=Sistema\\_embebido&oldid=166810655](https://es.wikipedia.org/w/index.php?title=Sistema_embebido&oldid=166810655)

[47] K. M. Hosny, A. Magdi, A. Salah, O. El-Komy, y N. A. Lashin, «Internet of things applications using Raspberry-Pi: a survey», *Int. J. Electr. Comput. Eng. IJECE*, vol. 13, n.º 1, p. 902, feb. 2023, doi: 10.11591/ijece.v13i1.pp902-910.

[48] I. G. M. N. Desnanjaya y I. N. A. Arsana, «Home security monitoring system with IoT-based Raspberry Pi», *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, n.º 3, p. 1295, jun. 2021, doi: 10.11591/ijeecs.v22.i3.pp1295-1302.

[49] A. P. Pangarkar, P. G. Gawande, y S. Shabadi, «A Comprehensive Analysis of ESP32 Microcontroller for IoT Applications», *International Journal of Research in Applied Science and Engineering Technology* vol. 10, n.º 10, 2025. [En línea]. Disponible en: <https://ijnrd.org/papers/IJNRD2510255.pdf>

[50] D. Ahmed, S. Z. Ali, F. B. Khan, y M. H. Faruki, «Design And Implementation Of An ESP32-Based Smart Home Automation System With Environmental Monitoring And Automated Controls», *IOSR J. Electron. Commun. Eng.*, vol. 19, n.º 6, pp. 23-28, dic. 2024, doi: 10.9790/2834-1906012328.

[51] Blynk, «Blynk: Low-Code IoT Platform». Accedido: 20 de noviembre de 2025. [En línea]. Disponible en: <https://blynk.io>

[52] N. Omkar, S. Rahul, R. Vijaykrishna, N. Swapna, y M. R. Sura, «Smart Environmental Monitoring Using Esp32 Microcontroller», *International Journal of Scientific Research in Science and Technology*, 2024.

[53] C. E. Romero y A. Elustondo, «Análisis de la capacidad de la placa ESP32 para integrar sistemas IoT descentralizados», *Elektron*, vol. 6, n.º 1, may 2022, doi: 10.37537/rev.elektron.6.1.142.2022.

[54] P. A. García, «Sistemas embebidos de tiempo real con aplicaciones en bioingeniería», Tesis Doctoral en Ingeniería, Universidad Nacional de La Plata, 2019. doi: 10.35537/10915/74734.



- [55] Academia de Infantería «Memorial de Infantería» n.º 86, Ministerio de Defensa, Toledo, junio de 2023. Accedido 4 de noviembre de 2025. [En línea]. Disponible en: <https://publicaciones.defensa.gob.es/memorial-de-infanteria-86-revistas-pdf.html>
- [56] ForoRaspberry.es, «Inicio», ForoRaspberry.es. Accedido: 23 de octubre de 2025. [En línea]. Disponible en: <https://www.fororaspberry.es/>
- [57] R. P. Ltd, «Buy a Raspberry Pi 5», Raspberry Pi. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://www.raspberrypi.com/products/raspberry-pi-5/>
- [58] R. P. Ltd, «Buy a Raspberry Pi 4 Model B», Raspberry Pi. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://www.raspberrypi.com/products/raspberry-pi-4-model-b/>
- [59] CPU-Monkey, «Broadcom VideoCore VII Benchmarks & Specs». Accedido: 22 de octubre de 2025. [En línea]. Disponible en: [https://www.cpu-monkey.com/en/igpu-broadcom\\_videocore\\_vii](https://www.cpu-monkey.com/en/igpu-broadcom_videocore_vii)
- [60] Android Developers, «OpenGL ES | Views», Android Developers. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://developer.android.com/develop/ui/views/graphics/opengl/about-opengl?hl=es-419>
- [61] F. Ayala, «Raspberry Pi 5: Nueva arquitectura, mejor rendimiento.», UNIT Electronics. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://blog.uelectronics.com/tarjetas-desarrollo/raspberry-pi-5-nueva-arquitectura-mejor-rendimiento/>
- [62] Xataka, «Raspberry Pi 5: características, precio y ficha técnica». Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://www.xataka.com/ordenadores/raspberry-pi-5-caracteristicas-precio-ficha-tecnica>
- [63] Transfer Multisort Elektronik (TME), «GPIO - definición | Distribuidor de componentes electrónicos. Tienda en línea: Transfer Multisort Elektronik España», TME. Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://www.tme.eu/es/news/library-articles/glossary/page/61888/gpio-general-purpose-inputoutput-definicion/>
- [64] Espressif Systems, «ESP32-S3 Wi-Fi & BLE 5 SoC | Espressif Systems». Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://www.espressif.com/en/products/socs/esp32-s3>
- [65] Espressif Systems, « Repositorio Oficial de GitHub», GitHub. Accedido: 23 de octubre de 2025. [En línea]. Disponible en: <https://github.com/espressif>
- [66] Arducam, «Arducam 5MP OV5647 Camera Module Motorized IR-CUT Filter for Daylight and Night vision for Raspberry Pi». Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://www.arducam.com/arducam-for-raspberry-pi-noir-5mp-ov5647-camera-module-motorized-ir-cut-filter-for-daylight-and-night-vision-support-pi-4-zero-pi-3.html>
- [67] OmniVision Technologies, «OV5647 Color CMOS QXGA (5-megapixel) Image Sensor Datasheet», versión 1.2 . Accedido 1 de octubre de 2025. [En línea]. Disponible en: [https://cdn.sparkfun.com/datasheets/Dev/RaspberryPi/ov5647\\_full.pdf](https://cdn.sparkfun.com/datasheets/Dev/RaspberryPi/ov5647_full.pdf)
- [68] Arducam, «5MP OV5647 - Arducam Wiki». Accedido: 22 de octubre de 2025. [En línea]. Disponible en: <https://docs.arducam.com/Raspberry-Pi-Camera/Native-camera/5MP-OV5647/>
- [69] Cytron, «AI CCTV with Raspberry Pi 5 | Human Detection CCTV», <https://www.cytron.io/tutorial>. Accedido: 23 de octubre de 2025. [En línea]. Disponible en:



<https://www.cytron.io/tutorial/create-ai-cctv-camera-with-human-detection-using-raspberry-pi-5>

[70] Nanyang Senba Optical & Electronic Co., Ltd., «AM312: Digital Intelligent PIR Sensor Datasheet» Accedido 1 de octubre de 2025. [En línea]. Disponible en: <https://www.alldatasheet.com/datasheet-pdf/view/1179499/ETC2/AM312.html>

[71] International Electrotechnical Commission, «IEC 60529: Degrees of protection provided by enclosures (IP Code)», 1989.

[72] Micropik, «HC-SR501 PIR Motion Sensor Module», Datasheet, rev. 1.0. [En línea]. Disponible: <https://www.micropik.com/PDF/HCSR501.pdf>

[73] Reyax Technology, «RYLR998 LoRa Module Datasheet», [En línea]. Disponible: <https://reyax.com/products/RYLR998>

[74] Reyax Technology, «IoT Solution Provider | Modules, Wireless Solution & IoT Connectivity». Accedido: 23 de octubre de 2025. [En línea]. Disponible en: <https://reyax.com/>

[75] Semtech Corporation, «Home», Semtech (formerly Sierra Wireless). Accedido: 23 de octubre de 2025. [En línea]. Disponible en: <https://www.sierrawireless.com/>

[76] Proyecto Correcaminos, «Cómo Usar Módulos LoRa con ESP32. – Proyecto Correcaminos». Accedido: 23 de octubre de 2025. [En línea]. Disponible en: <https://proyectocorrecaminos.com/como-usar-modulos-lora-con-esp32/>

[77] Reyax Technology Co., Ltd., «RYLR998 UART Interface 868/915 MHz LoRa Antenna Transceiver Module Datasheet», Accedido: 20 de octubre de 2025. [En línea]. Disponible en: <https://reyax.com/products/RYLR998>

[78] HJGHY, «Batería Litio 3S2P 12V con BMS Incorporado y Cargador para Dispositivos eléctricos», Especificaciones del producto B0CC51S743. Accedido: 20 de noviembre de 2025. [En línea]. Disponible en: <https://www.amazon.es/HJGHY-Recargable-Incorporado-Dispositivos-el%C3%A9ctricos/dp/B0CC51S743>

[79] RUNCCI-YUN, «DC-DC 9V/12V/24V a 5V 5A Step Down Fuente de alimentación Buck Converter Ajustable», Especificaciones del producto B0F59TDVBG. Accedido: 20 de noviembre de 2025. [En línea]. Disponible en: <https://www.amazon.es/RUNCCI-YUN-alimentaci%C3%B3n-Converter-Ajustable-Step-Down/dp/B0F59TDVBG>

[80] Tienda Fotovoltaica, «Batería recargable 3,6V 1300 mAh», Especificaciones del producto 901021. Accedido: 20 de noviembre de 2025. [En línea]. Disponible en: <https://www.tiendafotovoltaica.es/Bateria-recargable-36V-1300-mAh>

[81] Filament2Print, «¿Qué es el PETG?», Filament2Print. Accedido: 24 de octubre de 2025. [En línea]. Disponible en: <https://filament2print.com/es/blog/filament2print.com/es/blog/petg?slug=petg&module=smartblog>

[82] Ejército de Tierra, «Agrupación de Apoyo Logístico nº 41 (AALOG 41)». Accedido: 28 de noviembre de 2025. [En línea]. Disponible en: <https://ejercito.defensa.gob.es/unidades/Zaragoza/aalog41/>

[83] G. E. Upton y G. Halfacree, «Raspberry Pi User Guide, Eben Upton and Gareth Halfacree.





- [84] AliExpress, «Batería recargable AA NiMH 4.8V 5000mAh para juguetes RC, coches, tanques y robots». Especificaciones del producto 1005008790006145. Accedido: 28 de noviembre de 2025. [En línea]. Disponible en: <https://www.aliexpress.com/item/1005008790006145.html>
- [85] Thingsboard, «Open-source IoT Platform», ThingsBoard. Accedido: 23 de octubre de 2025. [En línea]. Disponible en: <https://thingsboard.io/>
- [86] Netline Communication Technologies, «LoRa Protocol and the challenge it raises for Counter IEDs», Netline Communication Technologies. Accedido: 29 de octubre de 2025. [En línea]. Disponible en: <https://netlinetech.com/lora-protocol-and-the-challenge-it-raises-for-counter-ieds/>
- [87] LoRa Alliance, «LR-FHSS Allows Longer Range, Longer Payloads», (2 de octubre de 2023). Accedido: 27 de octubre de 2025. [En línea Video]. Disponible en: <https://resources.lora-alliance.org/home/lr-fhss-allows-longer-range-longer-payloads>
- [88] D. Basu, T. Gu, y P. Mohapatra, «Security Issues of Low Power Wide Area Networks in the Context of LoRa Networks», 30 de junio de 2020, *arXiv*: arXiv:2006.16554. doi: 10.48550/arXiv.2006.16554.
- [89] S. Farrell, «Low-Power Wide Area Network (LPWAN) Overview», Internet Engineering Task Force, Request for Comments RFC 8376, may 2018. doi: 10.17487/RFC8376.
- [90] Thingsboard, «ThingsBoard Community Edition», ThingsBoard. Accedido: 23 de octubre de 2025. [En línea]. Disponible en: <https://thingsboard.io/docs/>
- [91] L. O. Aghenta, M. Tariq Iqbal, «Design and implementation of a low-cost, open source IoT-based SCADA system using ESP32 with OLED, ThingsBoard and MQTT protocol», *AIMS Electron. Electr. Eng.*, vol. 4, n.º 1, pp. 57-86, 2020, [En línea]. Disponible en: <https://www.aimspress.com/article/doi/10.3934/ElectrEng.2020.1.57>
- [92] Bizagi, «Software de modelado de procesos: Bizagi Modeler». Accedido: 23 de octubre de 2025. [En línea]. Disponible en: <https://www.bizagi.com/es/plataforma/modeler>
- [93] Wokwi «Wokwi - World's most advanced ESP32 Simulator». Accedido: 23 de octubre de 2025. [En línea]. Disponible en: <https://wokwi.com/>
- [94] Dashingsoft, «Pyarmor - Obfuscating Python Scripts». Accedido: 20 de noviembre de 2025. [En línea]. Disponible en: <https://pyarmor.dashingsoft.com/>
- [95] M. Dahlgren, «Countermeasures, Penetration Aids, and Missile Defense», Missile Threat, Center for Strategic and International Studies (CSIS). Accedido: 29 de noviembre de 2025. [En línea]. Disponible en: <https://missilethreat.csis.org/countermeasures-penetration-aids-and-missile-defense/>
- [96] «Anduril». Accedido: 5 de noviembre de 2025. [En línea]. Disponible en: <https://www.anduril.com/eagleeye/>
- [97] Anduril Industries, «EagleEye: Superpowers for Superheroes!». Accedido: 5 de noviembre de 2025. [En línea]. Disponible en: <https://www.anduril.com/eagleeye/>





## Anexo I

En sistemas de comunicación LoRa, conocer la latencia de transmisión es fundamental para evaluar el rendimiento y la viabilidad de aplicaciones IoT, especialmente cuando se requiere un equilibrio entre alcance y tiempo de respuesta. La latencia depende directamente de parámetros como el Spreading Factor (SF), el ancho de banda y la longitud del mensaje. Por ello, es necesario calcular el Time on Air (ToA), que representa el tiempo que el canal permanece ocupado durante la transmisión del paquete.

Un SF más alto “expande” la señal de forma más extensa, lo que aumenta la sensibilidad del receptor y, por tanto, el alcance de la transmisión. Por ende, un SF más bajo permite que la señal transmita más datos en el mismo período de tiempo, resultando en una mayor velocidad de datos.

El cálculo del ToA se basa en la fórmula definida por *Semtech* para *LoRa*:

$$T_{\text{sym}} = \frac{2^{SF}}{BW}$$
$$N_{\text{payload}} = 8 + \max \left( \left\lceil \frac{8 \cdot PL - 4 \cdot SF + 28 + 16 \cdot CRC - 20 \cdot IH}{4 \cdot (SF - 2 \cdot DE)} \right\rceil \cdot (CR + 4), 0 \right)$$

$$T_{\text{packet}} = (\text{Preamble} + 4.25) \cdot T_{\text{sym}} + N_{\text{payload}} \cdot T_{\text{sym}}$$

Donde se han usado los valores por defecto del módulo RYLR998:

- **BW** = 125 kHz,
- **CR** = 4/5,
- **Preamble** = 8 símbolos,
- **Payload** = 9 bytes (mensaje “0459ALERT”),
- **CRC** habilitado,
- **Low Data Rate Optimization** activado para  $SF \geq 11$ .

Estos parámetros son estándar en aplicaciones *LoRa* y permiten estimar la latencia realista para cada SF. La Tabla 2 muestra cómo el aumento del SF incrementa significativamente la latencia, pero también mejora la sensibilidad y el alcance, lo que es crucial para aplicaciones que requieren cobertura de hasta 15–20 km.



| SF | Alcance estimado (km) | ToA (ms) |
|----|-----------------------|----------|
| 7  | 2                     | 41.22    |
| 8  | 4                     | 72.19    |
| 9  | 7                     | 144.38   |
| 10 | 10                    | 247.81   |
| 11 | 15                    | 495.62   |
| 12 | 20                    | 991.23   |

*Tabla 2. Estimación de alcance y retardo estimado. Fuente: elaboración propia.*



## Anexo II

En la siguiente tabla se puede observar la imagen de los componentes principales elegidos para el proyecto junto con sus dimensiones.

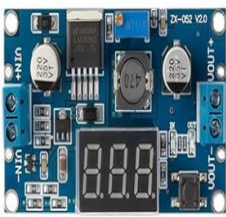
|                                                                                     |                                                                                      |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
|    |    |
| RLYR 998: 32 x 12 x 2,2 mm                                                          | ESP 32-S3: 18 x 23,5 x 2,5 mm                                                        |
|    |    |
| Batería 3,7 V: 50 x 43 x 14 mm                                                      | PIR AM 312: 10 x 8 x 10 mm                                                           |
|  |  |
| Step-down: 10 x 27 x 10 mm                                                          | Raspberry Pi 5: 85 x 56 x 20 mm                                                      |
|  |                                                                                      |
| Batería 12 V: 116 x 66 x 20 mm                                                      |                                                                                      |

Tabla 3. Dimensiones de los componentes. Fuente: elaboración propia en base a componentes ya referenciados.



## Anexo III

**Resultados de simulaciones:** En las siguientes tablas se muestran los datos recogidos tras las diferentes simulaciones y pruebas llevadas a cabo para identificar la viabilidad del sistema propuesto.

Simulación en la que se demuestra la viabilidad de la introducción de 35 nodos sensores conectados a un *Gateway*.

| Emisor | Enviados | Recibidos | Fiabilidad(%) | LatenciaProm(ms) |
|--------|----------|-----------|---------------|------------------|
| 1      | 100      | 100       | 100           | 100,39           |
| 2      | 100      | 100       | 100           | 100,12           |
| 3      | 100      | 100       | 100           | 100,79           |
| 4      | 100      | 100       | 100           | 101,01           |
| 5      | 100      | 100       | 100           | 101,00           |
| 6      | 100      | 100       | 100           | 101,00           |
| 7      | 100      | 100       | 100           | 101,00           |
| 8      | 100      | 100       | 100           | 102,00           |
| 9      | 100      | 100       | 100           | 102,00           |
| 10     | 100      | 100       | 100           | 102,00           |
| 11     | 100      | 100       | 100           | 103,10           |
| 12     | 100      | 100       | 100           | 103,79           |
| 13     | 100      | 100       | 100           | 103,22           |
| 14     | 100      | 100       | 100           | 103,56           |
| 15     | 100      | 100       | 100           | 104,11           |
| 16     | 100      | 100       | 100           | 104,23           |
| 17     | 100      | 100       | 100           | 104,67           |
| 18     | 100      | 100       | 100           | 104,78           |
| 19     | 100      | 100       | 100           | 105,00           |
| 20     | 100      | 100       | 100           | 105,34           |
| 21     | 100      | 100       | 100           | 105,54           |
| 22     | 100      | 100       | 100           | 105,88           |
| 23     | 100      | 100       | 100           | 106,23           |
| 24     | 100      | 100       | 100           | 106,28           |



|    |     |     |     |        |
|----|-----|-----|-----|--------|
| 25 | 100 | 100 | 100 | 106,44 |
| 26 | 100 | 100 | 100 | 106,79 |
| 27 | 100 | 100 | 100 | 107,05 |
| 28 | 100 | 100 | 100 | 107,12 |
| 29 | 100 | 100 | 100 | 107,35 |
| 30 | 100 | 100 | 100 | 107,45 |
| 31 | 100 | 100 | 100 | 108,00 |
| 32 | 100 | 100 | 100 | 108,30 |
| 33 | 100 | 100 | 100 | 108,56 |
| 34 | 100 | 100 | 100 | 108,73 |
| 35 | 100 | 100 | 100 | 108,84 |

Tabla 4. Simulación de escalabilidad. Fuente: elaboración propia.

Simulación en la que se ha forzado la colisión de paquetes para comprobar la efectividad del buffer.

| Métrica                      | Sin Buffer | Con Buffer |
|------------------------------|------------|------------|
| Paquetes Generados           | 1200       | 1200       |
| Paquetes Recibidos (Gateway) | 1142       | 1196       |
| PDR (Packet Delivery Ratio)  | 95.16%     | 99.66%     |
| Pérdida de Paquetes (PLR)    | 4.84%      | 0.34%      |
| Colisiones en el Aire        | 58         | 72         |
| Latencia Promedio            | 95.6 ms    | 106,7 ms   |
| Uso del Canal (Duty Cycle)   | 0.8%       | 0.95%      |

Tabla 5. Simulación de colisiones. Fuente: elaboración propia.



Fiabilidad de detección de movimiento del sensor PIR en función de la distancia a la que se pretende efectuar la detección.

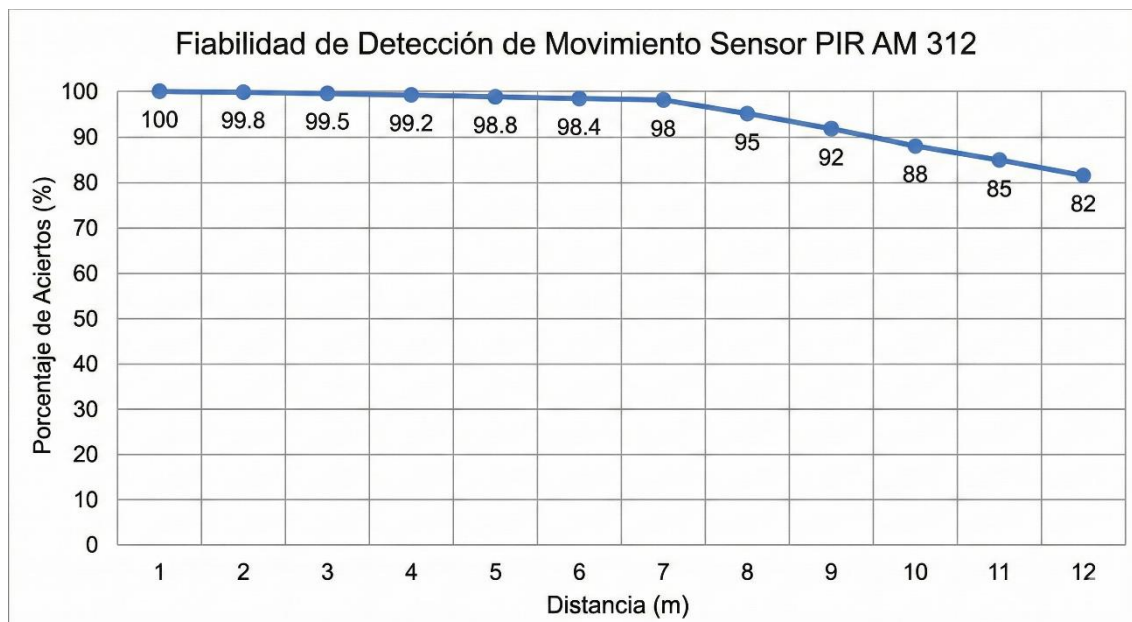


Tabla 6. Fiabilidad detección mediante PIR. Fuente: elaboración propia.

Fiabilidad del algoritmo de reconocimiento de imagen en función de la distancia a la que se coloca la persona o vehículo que se pretende detectar.

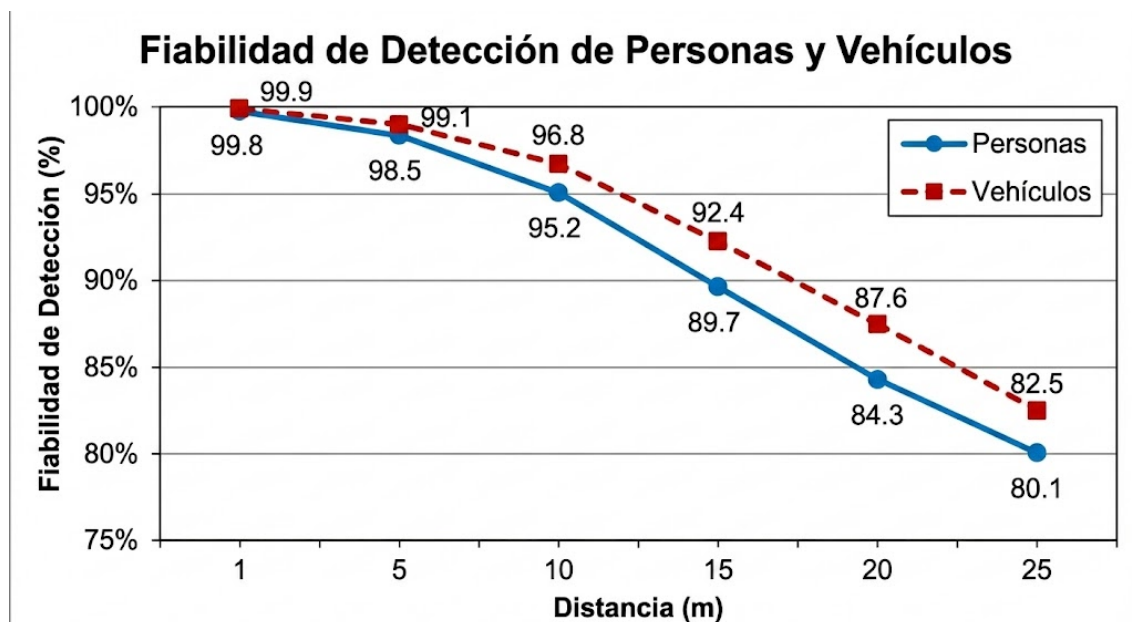


Tabla 7. Fiabilidad detección cámara. Fuente: elaboración propia.

Resultado de la redundancia multisensorial ampliando la fiabilidad de detección al combinar ambos métodos de detección.



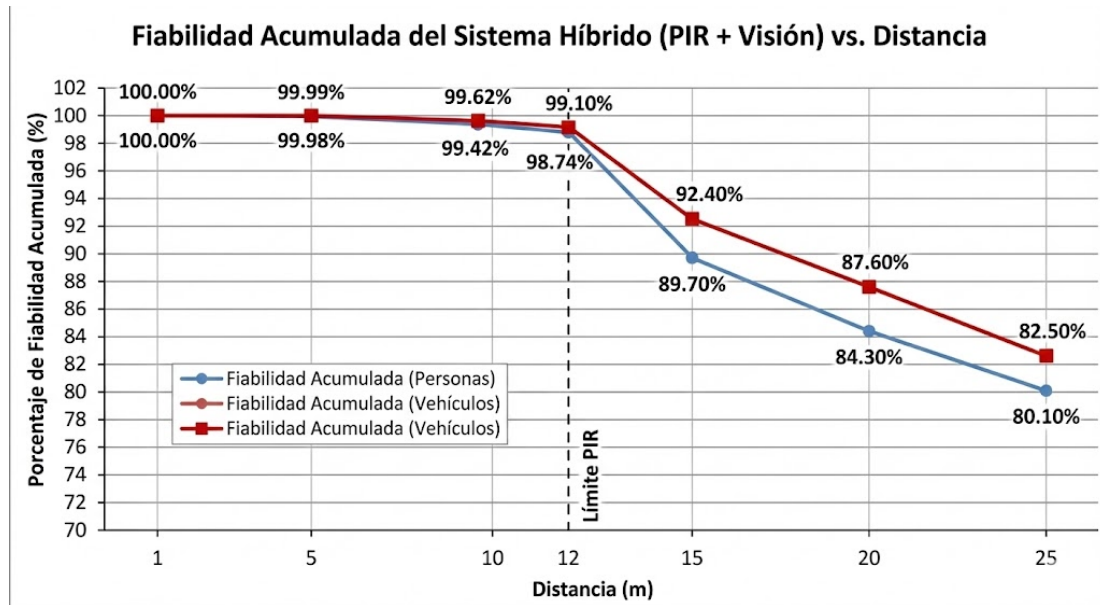


Tabla 8. Fiabilidad detección acumulada. Fuente: elaboración propia.



## Anexo IV

A continuación, se muestran las interfaces local (Figura 18) y de *Thingsboard* (Figura 19) para la presentación de la información al usuario final.



Figura 18. Interfaz web local. Fuente: elaboración propia.

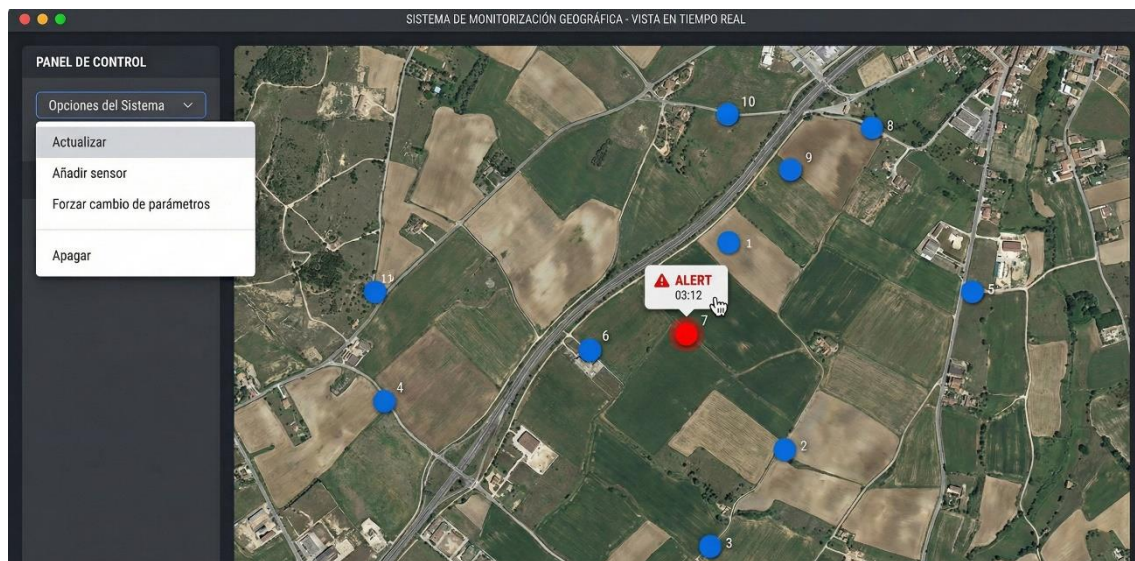


Figura 19. Interfaz Thingsboard. Fuente: elaboración propia.



## Anexo V

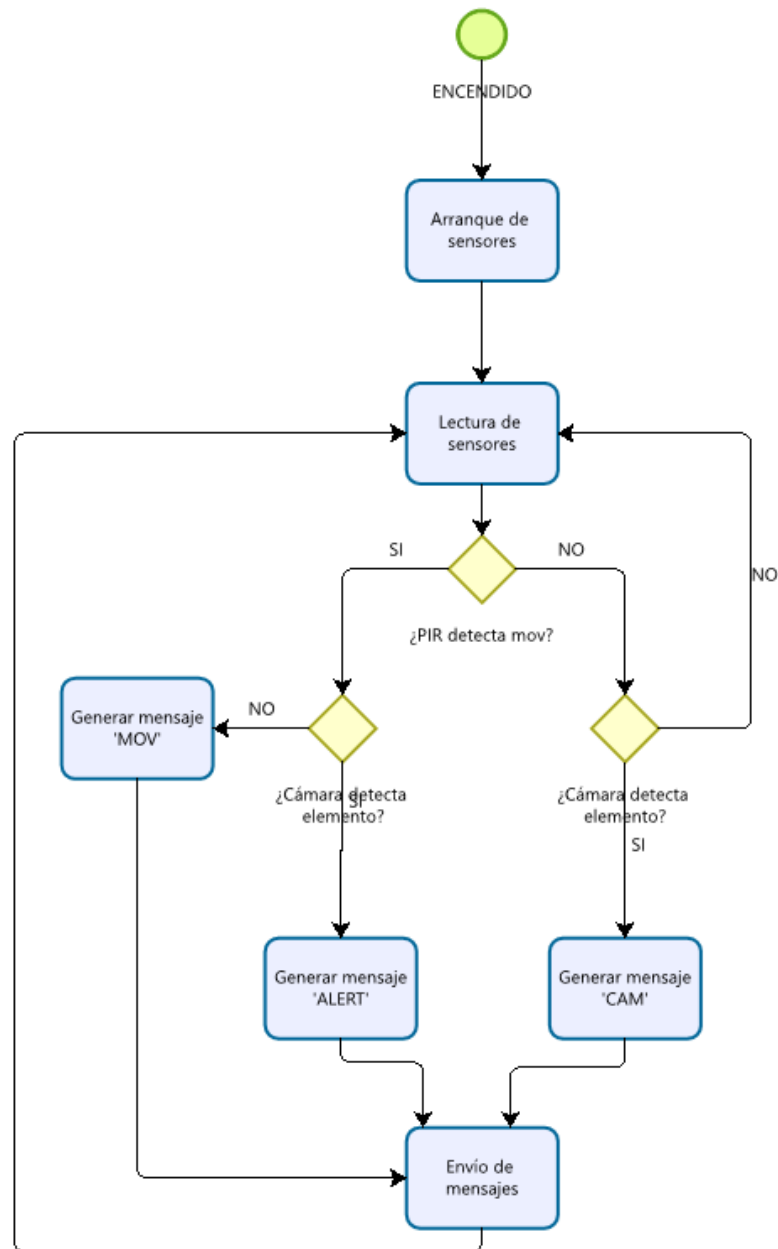


Figura 20. Diagrama de flujo. Fuente: elaboración propia.