



1859

UNL

Universidad
Nacional
de Loja

Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Carrera de Ingeniería en Telecomunicaciones

Sistema de seguridad comunitaria antiextorsión utilizando sistemas embebidos en el casco urbano de la ciudad de Loja

Trabajo de Integración Curricular,
previo a la obtención del título de
Ingeniero en Telecomunicaciones.

AUTOR:

Carlos Daniel Briceño Ledesma

DIRECTOR:

Ing. Diego Vinicio Orellana Villavicencio. Mg. Sc.

Loja – Ecuador

2024

Certificación

Loja, 20 de noviembre de 2024

Ing. Diego Vinicio Orellana Villavicencio. Mg. Sc.

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Integración Curricular denominado: **Sistema de seguridad comunitaria antiextorsión utilizando sistemas embebidos en el casco urbano de la ciudad de Loja.**, previo a la obtención del título de **Ingeniero en Telecomunicaciones**, de la autoría del estudiante **Carlos Daniel Briceño Ledesma**, con **cédula de identidad Nro. 1150197307**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa.

Ing. Diego Vinicio Orellana Villavicencio. Mg. Sc

DIRECTOR DEL TRABAJO DE TITULACIÓN

Autoría

Yo, **Carlos Daniel Briceño Ledesma**, declaro ser autor del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Integración Curricular, en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma:



Cedula: 1150197307

Fecha: 20/11/2024

Correo electrónico: carlos.d.briceno@unl.edu.ec

Celular: 0995968614

Carta de autorización por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica del texto completo del Trabajo de Integración Curricular.

Yo **Carlos Daniel Briceño Ledesma**, declaro ser autor Trabajo de Integración Curricular denominado: **Sistema de seguridad comunitaria antiextorsión utilizando sistemas embebidos en el casco urbano de la ciudad de Loja**, como requisito para optar el título de **Ingeniero en Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, suscribo, en la ciudad de Loja, a los veinte días del mes de noviembre de dos mil veinticuatro.



Firma:

Autora: Carlos Daniel Briceño Ledesma

Cédula: 1150197307

Dirección: Republica dominicana y Chile

Correo electrónico: carlos.d.briceno@unl.edu.ec

Celular: 0995968614

DATOS COMPLEMENTARIOS:

Director de tesis: Ing. Diego Vinicio Orellana Villavicencio. Mg. Sc.

Dedicatoria

A mi madre querida, Cecilia Ledesma, por ser mi guía y mi mayor fuente de creatividad. Eres mi ejemplo a seguir en cada paso que doy. Tu amor y apoyo incondicional han sido la guía de mi camino. Gracias por la confianza que siempre tuviste en mí, sin ti, nada de esto sería posible.

A mi padre, Juan Briceño, por ser la motivación constante en mi vida y por su apoyo inquebrantable. Me enseñaste que las cosas complicadas son las más satisfactorias de terminar. Gracias por cada consejo y sacrificio que has hecho para verme cumplir mis metas. Gracias por ser mi guía y mi amigo.

A mi hermano Juan, por formar parte en cada paso de este viaje. En las buenas y malas siempre estás a mi lado, brindándome fuerza y aliento. Te agradezco cada risa compartida hermano.

A mi hermana Mara, por enseñarme el valor de la valentía. Por creer en mis capacidades y por alentarme a alcanzar mis metas. Tu apoyo ha sido parte de mi fortaleza en este camino.

A mis amigos, por estar ahí en los momentos difíciles. Por el apoyo incondicional durante toda la carrera y por estar a mi lado en cada decisión. Siempre que necesité un amigo, estuvieron ahí sin dudarlo.

Este logro no es solo mío, sino de todos ustedes. Especialmente quiero expresar mi profundo agradecimiento a mis padres. Con todo mi amor y gratitud, les dedico este logro.

Carlos Daniel Briceño Ledesma

Agradecimiento

Primeramente, quiero agradecer a mis padres por permitirme estar aquí y alcanzar una de mis tantas metas. Por brindarme fortaleza, perseverancia y sobre todo por ser mis guías en todo momento. También quiero extender mi agradecimiento a la Universidad Nacional de Loja especialmente a la carrera de Telecomunicaciones, y a su planta docente por impartirme los conocimientos necesarios y contribuir en mi formación académica.

Un agradecimiento especial a mi director de integración curricular, Diego Orellana, por su guía en cada paso de este proceso. Cuya dedicación, compromiso y apoyo, así como su experiencia, han enriquecido mi proceso de aprendizaje y han sido fundamentales para la realización de este trabajo de titulación.

Agradezco profundamente a mi familia por ser el pilar de mi vida. Cada palabra de aliento, motivación y consejo que me han brindado ha sido importante para mí crecimiento personal y mi formación académica. Gracias a cada uno de ustedes, he encontrado la fuerza de superarme y seguir adelante siempre con la frente en alto.

Gracias a mis amigos por el apoyo que me brindaron en cada momento que los necesité. Cada risa compartida, cada palabra de ayuda y cada momento juntos, los cuales hicieron una diferencia en mi vida.

Carlos Daniel Briceño Ledesma

Índice de contenidos

Portada	i
Certificación	ii
Autoría	iii
Carta de autorización	iv
Dedicatoria	v
Agradecimiento	vi
Índice de contenidos	vii
Índice de tablas:	ix
Índice de ilustraciones:	x
Índice de anexos:.....	xi
1. Título	1
2. Resumen	2
Abstract	3
3. Introducción	4
4. Marco Teórico	6
4.1. Conceptos básicos de IoT	6
4.1.1 ¿Qué es IoT?	6
4.1.2 Despliegue de IoT en el sector de la agricultura.....	6
4.1.3 Aplicaciones de IoT con móviles integrados	7
4.1.4 Eficiencia energética por medio de IoT	7
4.1.5 Seguridad y vigilancia apoyada por IoT	8
4.1.6 El uso de IoT en ciudades inteligentes.....	8
4.1.7 La industria potenciada por IoT	8
4.2. Sistemas de notificación de emergencias.....	9

4.2.1	Definición y arquitectura de los sistemas de notificación para emergencias.....	9
4.3.	Aplicaciones y usos.....	10
4.4.	Tecnologías de comunicación.....	13
4.4.1.	Wi-Fi.....	14
4.4.2.	LoRA.....	15
4.4.3.	Zigbee	15
4.5.	Trabajos relacionados	16
5.	Metodología	18
5.1.	Determinación de los requerimientos del equipo.....	18
5.2.	Selección de componentes electrónicos.....	19
5.2.1	Componentes del sistema de transmisión de datos	20
5.2.2	Componentes del sistema de respaldo energético.....	21
5.3.	Diseño del sistema de respaldo energético y sistema de transmisión de datos.....	24
5.3.1.	Sistema de transmisión	24
5.3.2.	Sistema de respaldo energético	25
5.4.	Evaluación del desempeño del prototipo	28
6.	Resultados.....	30
6.1.	Construcción del prototipo.....	30
6.2.	Análisis del desempeño del sistema de transmisión antiextorsión	32
6.3.	Análisis del sistema energético.....	35
6.4.	Análisis Económico	36
7.	Discusión	37
8.	Conclusiones	39
9.	Recomendaciones	40
10.	Bibliografía	41
11.	Anexos	45

Índice de tablas:

Tabla 1. Datos de requerimientos	19
Tabla 2. Tabla de elementos según el sistema propuesto	20
Tabla 3. Especificaciones técnicas del módulo ESP32	20
Tabla 4. Especificaciones técnicas módulo SIM800L	21
Tabla 5. Componentes del sistema de respaldo energético.....	21
Tabla 6. Especificaciones técnicas del módulo regulador de voltaje.....	22
Tabla 7. Especificaciones técnicas del módulo cargador de baterías	22
Tabla 8. Especificaciones técnicas del módulo conmutador de emergencia	23
Tabla 9. Detalle del análisis económico.....	36

Índice de figuras:

Figura 1. Ecosistema de IoT	6
Figura 2. Arquitectura básica de sistemas de notificación para emergencia	9
Figura 3. Comparativas de tecnologías de comunicación.....	14
Figura 4. Segmentación de metodología.....	18
Figura 5. Diagrama de flujo del sistema de transmisión.....	24
Figura 6. Interconexión de los sistemas internos del sistema antiextorsión.	25
Figura 7. Diagrama de conexiones del sistema de respaldo energético.....	26
Figura 8. Diseño del circuito para el sistema de respaldo energético.....	26
Figura 9. Diseño 3D del gabinete	27
Figura 10. Mapa de la ciudad de Loja y zonas de pruebas	28
Figura 11. Sistema de respaldo energético	30
Figura 12. Ensamblaje del sistema antiextorsión.....	31
Figura 13. Lugares donde se hicieron pruebas de funcionamiento.....	32
Figura 14. Resultados según las zonas de estudio en la ciudad de Loja.....	34
Figura 15. Análisis de datos del sistema energético	35

Índice de anexos:

Anexo 1. Código diseñado para en los diferentes prototipos 45

Anexo 2. Interfaz de la aplicación WDSservice 48

Anexo 3. Certificado de traducción del resumen..... 49

1. Título

Sistema de seguridad comunitaria antiextorsión utilizando sistemas embebidos en el casco urbano de la ciudad de Loja.

2. Resumen

Actualmente el Internet de las cosas (IoT) permite integrar eficazmente dispositivos y sistemas a la red, facilitando la transmisión de datos y la automatización de tareas. En la agricultura, por ejemplo, se usa para el monitoreo y control de cultivos; en medicina, para monitorear pacientes; en la industria, para gestionar material en tiempo real, en transporte público, para optimizar su gestión, entre otros.

IoT es una tecnología adaptable y versátil, con la capacidad de crear soluciones a diferentes necesidades presentes en la cotidianidad. En este proyecto, nos enfocamos en los sistemas de notificación de emergencias, y los beneficios generados cuando enviamos alertas sobre eventos críticos por medio de mensajes, siendo muy útiles dentro de escenarios como catástrofes ambientales, emergencias médicas, gestión de vialidad, fallos industriales, entre otros.

El objetivo de este estudio es desarrollar un sistema de notificación de emergencia antiextorsión utilizando sistemas embebidos en el casco urbano de la ciudad de Loja. El sistema propuesto combina la tecnología IoT y el sistema global de comunicaciones móviles (GSM), al incluir dos medios de comunicación aseguramos la transmisión de las alertas en casos den los que alguno de los medios de transmisión falle. Además, considerando la crisis energética que atraviesa el país, se diseñó e implementó un sistema de respaldo energético de aproximadamente 6 horas. Y así mitigar en cierta medida el incremento de inseguridad debido a los apagones.

Finalmente, es importante resaltar que analizamos el desempeño del sistema en varios sectores de la ciudad y bajo diferentes escenarios de uso, proporcionando una fiabilidad mayor al 90%, ofreciendo una solución accesible, de bajo costo y de fácil implementación ante el aumento de la delincuencia y la inseguridad en el país.

Palabras clave: GSM, IoT, Sistemas de emergencia, sistema energético.

Abstract

Nowadays, the Internet of Things (IoT) allows devices and systems to be efficiently integrated into the network, facilitating the transmission of data and the automation of tasks. In agriculture, for example, it is used to monitor and control crops; in medicine, to monitor patients; in industry, to manage material in real time; in public transport, to optimise its management, among others.

IoT is an adaptable and versatile technology, with the ability to create solutions to different everyday needs. In this project, we focus on emergency notification systems, and the benefits generated when we send alerts about critical events through messages, being very useful in scenarios such as environmental catastrophes, medical emergencies, road management, industrial failures, among others.

The objective of this study is to develop an anti-extortion emergency notification system using embedded systems in the urban area of the city of Loja. The proposed system combines IoT technology and the global system of mobile communications (GSM), by including two means of communication we ensure the transmission of alerts in cases where one of the means of transmission fails. In addition, considering the energy crisis that the country is going through, an energy backup system of approximately 6 hours was designed and implemented. This will mitigate to a certain extent the increase in insecurity due to blackouts.

Finally, it is important to highlight that the performance of the system was analysed in several sectors of the city and under different usage scenarios, providing a reliability of more than 90%, offering an accessible, low-cost and easy-to-implement solution to the increase in crime and insecurity in the country.

Keywords: GSM, IoT, emergency systems, energy system.

3. Introducción

En los últimos años el rápido avance de IoT ha abierto nuevas oportunidades para el despliegue de sistemas de seguridad que se ajustan a diferentes áreas de trabajo, sin embargo, a menudo los sistemas comerciales se sobredimensionan resultando en costos elevados. Este trabajo de titulación se enfoca en el diseño y construcción de un sistema de notificación de emergencia comunitario usando tecnología IoT, específicamente diseñado para abordar el problema de extorsión que atraviesa el sector comercial.

Un sistema de notificación de emergencia permite alertar de forma instantánea a personas o grupos de personas sobre una emergencia. Este tipo de sistemas son útiles en gran variedad de escenarios, por ejemplo: en la agricultura, el control de alimentos; dentro la medicina, el monitoreo de pacientes; para la industria, el control de material en tiempo real; en cuanto a vialidad, la gestión del transporte público; sobre la seguridad, el monitoreo de edificios con sensores; en los servicios de emergencia, la alerta de incendios, robos o accidentes automovilísticos.

La extorsión es un problema que afecta a diferentes zonas del país, preocupando a la ciudadanía, en cambio, el sector comercial busca trabajar con un buen sistema de seguridad. Los métodos de seguridad tradicionales se enfocan en resguardar la información y defender zonas restringidas de intrusos.

El sistema propuesto en este trabajo aprovecha la tecnología IoT para generar una red de diferentes nodos, que comuniquen por medio de Telegram y servicio de mensajes cortos (SMS) sobre un posible acto de extorsión, enviando un mensaje personalizado a un grupo en Telegram y un SMS a un número de teléfono particular.

Nuestro sistema está conformado por los siguientes componentes principales:

- Módulo ESP32 Arduino
- Módulo GSM GPRS SIM 8001
- Sistema de respaldo energético

El encargado de coordinar el funcionamiento de los diferentes componentes es el módulo ESP32 Arduino, además de ser el encargado de enviar el mensaje por Telegram vía Wi-Fi, el módulo GSM GPRS SIM 8001 es el destinado a realizar la comunicación de SMS por la red GSM. En este proyecto se utilizó la red desplegada por Claro, por último, el sistema de respaldo energético es el encargado de defender el sistema contra los cortes de energía, permitiendo el uso de nuestro sistema durante la escases energética.

Se puede deducir que delitos como la extorsión o similares son el objetivo de este proyecto, donde por objetivo principal tiene “Desarrollar un sistema de seguridad antiextorsión orientado al sector comercial de la ciudad de Loja”. En primer lugar, se revisará y analizará información relacionada al tema planteado y se comparará sistemas con un objetivo similar, de esta forma cumplir el primer objetivo específico “Identificar las características, ventajas y desventajas de las tecnologías de comunicación inalámbricas actuales, para seleccionar la que más se adapte a las necesidades del proyecto”.

El siguiente paso será adquirir los componentes electrónicos necesarios para un prototipo funcional, teniendo en cuenta las tecnologías de comunicación que se lleguen a implementar en conjunto a GSM. Lo siguiente, es elaborar el código que permita ejecutar las funciones que busque cumplir nuestro sistema, cumpliendo el segundo objetivo específico “Construir un prototipo del sistema antiextorsión enfocado en funcionamiento de tecnologías de mensajería instantánea y SMS.

Por último, se realizará pruebas de funcionamiento analizando las principales variables y realizar correcciones de ser necesario, así finalizando con el ultimo objetivo específico “Analizar la eficiencia del sistema antiextorsión en base a parámetros de comunicación”.

La estructura del trabajo se organiza de la siguiente manera: primero, se presenta la introducción del tema que contextualiza los objetivos, problemática y justificación del trabajo realizado. Posteriormente, se hace una descripción del marco teórico aquí revisaremos conceptos relevantes con la temática del proyecto. Luego describiremos detalladamente la metodología utilizada y se presentan los resultados obtenidos. Finalmente, se presenta la discusión de los resultados analizando la relación con los objetivos, se presentan las conclusiones y recomendaciones.

4. Marco Teórico

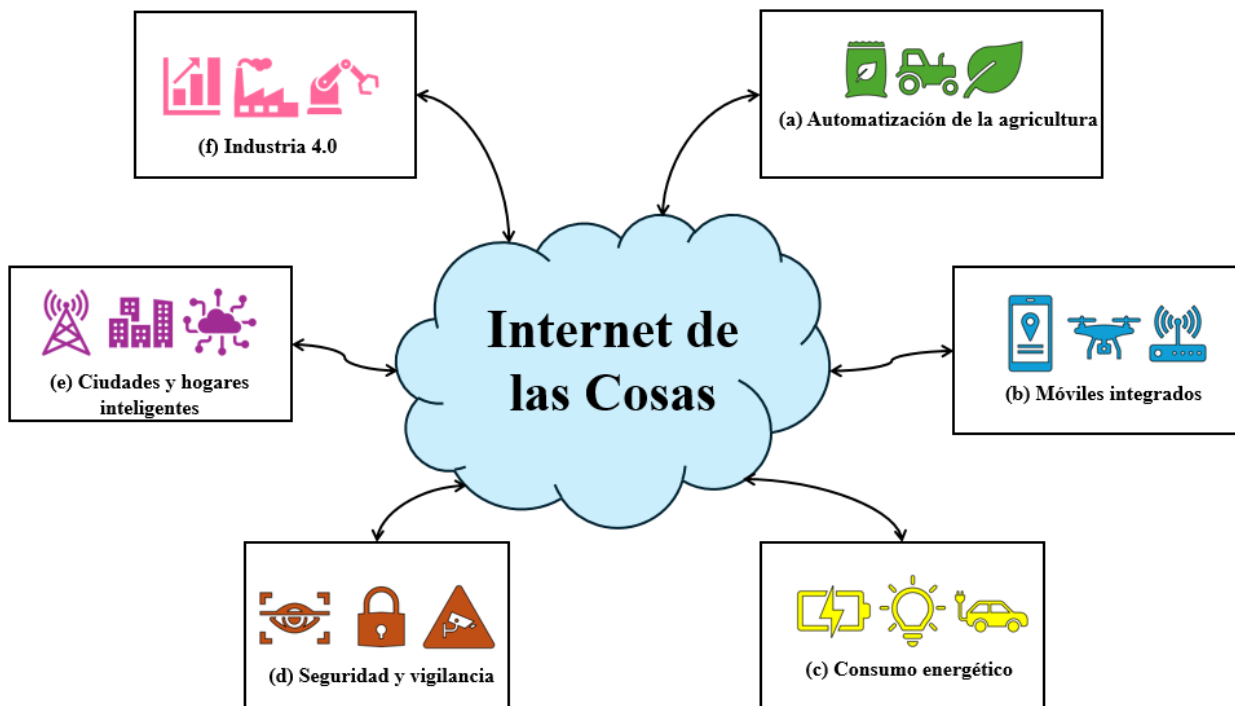
4.1. Conceptos básicos de IoT

4.1.1 ¿Qué es IoT?

Internet de las cosas se refiere a la idea de conectar cosas a la red de internet, especialmente objetos cotidianos, que son legibles, reconocibles, localizables, direccionables a través de un dispositivo sensor de información y/o controlables a través de Internet, independientemente del medio de comunicación (ya sea mediante RFID, LAN inalámbrica, redes de área amplia, u otros medios) (Patel et al., 2016).

Por lo tanto, IoT es una tecnología que busca integrarse en todas las cosas que utiliza el ser humano, esto con la finalidad de mejorar su funcionamiento, adquirir información, automatizar acciones y mejorar la calidad de vida.

Figura 1
Ecosistema de IoT



Nota. Autor

4.1.2 Despliegue de IoT en el sector de la agricultura

Una de las aplicaciones que más ha ganado popularidad en los años recientes es la que se conoce como agricultura de precisión ilustrada en la figura 1 (a). “En este ámbito, se despliegan

las redes IoT para optimizar la gestión de cultivos y ganado, lo que genera un incremento en la productividad y mejora las tácticas que pueden utilizar los agricultores” (Jaiganesh et al., 2017)

El uso de Redes de sensores inalámbricos (WSN) en conjunto con IoT mejora significativamente los métodos tradicionales de agricultura. Según Quy et al. (2022), las WSN son ideales para la automatización de la agricultura debido a las capacidades de autoorganización, autoconfiguración, autoestabilización y autorrecuperación.

En resumen, por medio de IoT y WSN Hace que el sector agrícola sea más eficiente, se adapte mejor y se ajuste a los retos tecnológicos actuales.

4.1.3 *Aplicaciones de IoT con móviles integrados*

La Aplicación de IoT junto a la movilidad que entrega los celulares como se observa en la figura 1 (b). “Esto hace referencia a la capacidad de combinar diferentes tecnologías en un dispositivo móvil como es el caso de teléfonos inteligentes, vehículos aéreos no tripulados (UAV), relojes inteligentes, entre otros.” (Barthold et al., 2011).

Usos como la detección de accidentes automovilísticos por medio sensores presentes en teléfonos inteligentes o el envío de datos médicos son aplicaciones innovadoras dentro de este sector. Como describe Yang et al. (2022) modernizar los sistemas médicos con IoT facilita la prevención, detección y tratamiento de enfermedades utilizando sensores de salud dedicados

Por lo tanto, el uso conjunto de IoT con los dispositivos móviles actuales facilita la recopilación de información y mejora la calidad de datos.

4.1.4 *Eficiencia energética por medio de IoT*

El sector energético es un área de gran interés para el despliegue de IoT figura 1 (c). “Mediante la aplicación de sensores IoT, los dispositivos conectados a Internet son capaces de distinguir cualquier fallo en el funcionamiento o disminución anormal de la eficiencia energética, alertando de la necesidad de mantenimiento.” (Motlagh et al., 2020)

Una de las principales ventajas que IoT se observan por medio de sensores orientados a la mejora energética, como a la capacidad de monitorear el consumo energético de las máquinas. Según Rao et al. (2020), El uso de microcontroladores en sistemas de monitoreo contribuye al ahorro energético.

De esta manera, el uso de WSN dentro del sector energético mejora la eficiencia al reducir el consumo de maquinarias y sistemas.

4.1.5 *Seguridad y vigilancia apoyada por IoT*

El uso de IoT en seguridad y vigilancia se ilustra en la figura 1 (d). Aunque temas relacionados a la seguridad y sus aplicaciones se detallan más adelante en este documento, es importante comentar que la integración de IoT ha mejorado los sistemas de seguridad.

Por ejemplo, Made et al. (2021) “describe un sistema de vigilancia usando un espejo inteligente, este sistema tiene la capacidad de notificar al propietario sobre la presencia de un intruso”. De igual manera, la seguridad a gran escala se mejora con el uso de IoT, como lo comenta Fatima et al. (2021), “donde por medio de cámaras de vigilancia e imágenes térmicas se logra detectar intrusos en áreas fronterizas y alertar a los funcionarios en caso de emergencia.”

En resumen, IoT potencia la seguridad y la vigilancia al añadir funcionalidades o mejorando sistemas existentes.

4.1.6 *El uso de IoT en ciudades inteligentes*

El enfoque de IoT en ciudades inteligentes se identifica en la figura 1 (e). Donde se plantea la capacidad que tiene IoT para interconectar, censar, analizar y medir eventos o variables importantes en las ciudades u hogares, de esta manera (Sánchez-Corcuera et al., 2021) comenta:

En el contexto de las ciudades inteligentes, IoT permite que los sensores recopilen y envíen datos sobre el estado de la ciudad a una nube central, que luego se extraen o procesan para la extracción de patrones y la toma de decisiones.

Dentro de las ciudades inteligentes existen propuestas de hogares inteligentes, como lo describe Salman et al. (2016), donde por medio de simulación y análisis de un hogar inteligente expresan como es energéticamente eficiente.

Podemos resumir que IoT busca ser implementado en las estructuras actuales de las diferentes ciudades y hogares, así medir variables que beneficien este sector.

4.1.7 *La industria potenciada por IoT*

En la figura 1 (f) se muestra el sector industrial, esta área puede ser una de las más beneficiadas de usar IoT, Khan et al. (2022) analiza cómo la industria 4.0 ayuda a crear fábricas inteligentes, donde usando correctamente IoT se mejora la eficiencia y la fabricación se realiza con menos costos y errores.

Sin embargo, no todo siempre es fácil de implementar. Frank et al. (2019), realiza una encuesta a 92 empresas manufactureras y describe los desafíos que se producen durante la

transición hacia la industria 4.0, temas como big data y el análisis de datos aún son retos presentes en las empresas encuestadas.

Por lo tanto, se puede concluir que la implementación de IoT dentro de la industria es un reto para cada empresa y una vez aplicada con éxito se llega a mejorar la eficiencia de la industria además de reducir costos y minimizar riesgos en la operación industrial.

4.2. Sistemas de notificación de emergencias

4.2.1 Definición y arquitectura de los sistemas de notificación para emergencias

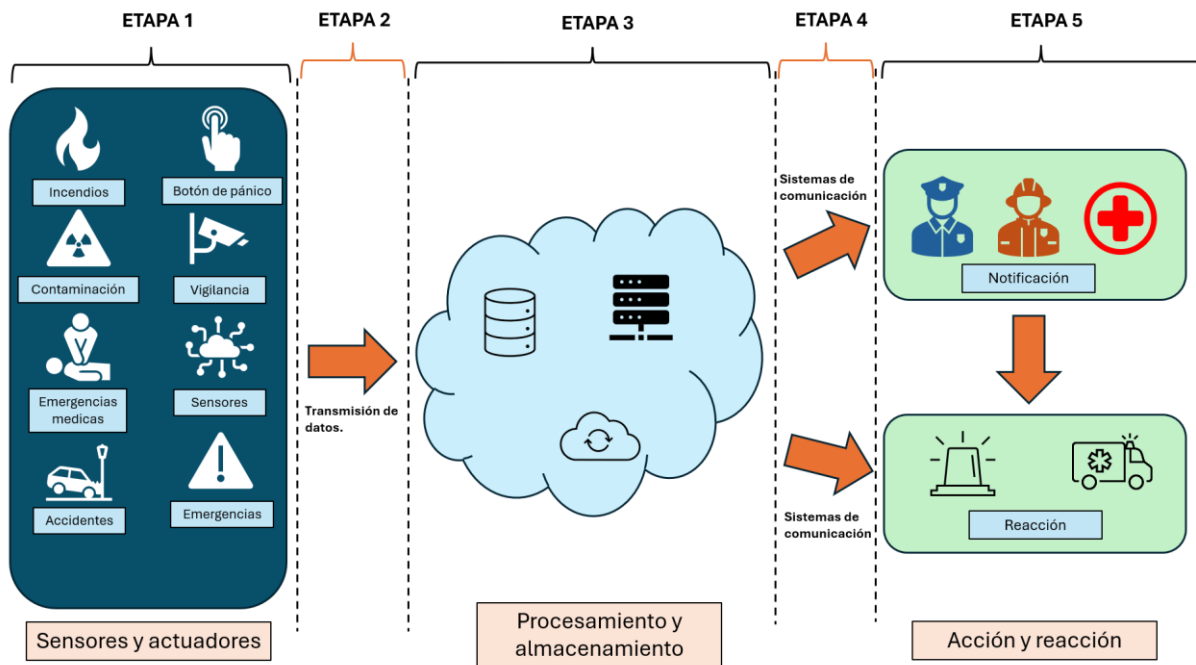
Se puede definir a un sistema de notificación como el conjunto de dispositivos interconectados con el propósito de enviar un mensaje o una señal a un controlador, el mismo que tiene la capacidad de entender el mensaje enviado. Estos mensajes se deben enviar cuando se produzca una acción crítica que aun tenga solución. De esta manera salvaguardar la integridad de los elementos que cubra el sistema de notificación.

Arquitectura más usada

Las arquitecturas que utilizan los sistemas de notificación para emergencias varían según sus funciones y de los datos que se estudien. Sin embargo, todas esas arquitecturas tienen un punto en común que funciona como una base para desarrollar nuevos sistemas.

Figura 2

Arquitectura básica de sistemas de notificación para emergencia



Nota. Autor

La capacidad de transmitir información de alguna emergencia, procesar la información y transmitirla a se observa en la figura 2, en donde se logra identificar cinco etapas principales.

1. Etapa 1 – Sensores y Actuadores: Esta etapa se engloban los diferentes sensores y dispositivos que permiten detectar diferentes tipos de emergencias, como incendios, contaminación, vigilancia, emergencias médicas, accidentes y diferentes situaciones que se presenten riesgosas. Estos sensores envían alertas al sistema cuando detectan una condición crítica.
2. Etapa 2 – Transmisión de Datos: Los datos que han sido capturados por los sensores son enviados a través de un canal de comunicación. Esta transmisión permite que la información generada llegue al sistema y se procesen los datos producidos por los sensores.
3. Etapa 3 – Procesamiento y Almacenamiento: En esta fase, los datos recibidos se almacenan y procesan. Aquí se realiza el análisis de los datos producidos por los sensores y se gestiona la información para determinar la naturaleza de la emergencia.
4. Etapa 4 – Comunicación: Luego del procesamiento de datos, el sistema se comunica con los diferentes equipos de respuesta (policía, bomberos y servicios médicos) para notificar sobre la emergencia. Se utilizan los sistemas de comunicación para transmitir el mensaje de manera rápida y eficaz.
5. Etapa 5 – Acción y Reacción: Finalmente, los equipos de respuesta reciben la notificación y reaccionan en consecuencia, donde movilizan los recursos necesarios para mitigar la situación reportada.

Estas cinco etapas muestran el seguimiento de acciones que se dan en un sistema de notificación y se logra identificar el objetivo de este tipo de sistemas, que es la optimización de los equipos de respuesta ante emergencias.

4.3. Aplicaciones y usos

Las diferentes aplicaciones de los sistemas de notificación basados en IoT surgen a partir de la necesidad de notificar una urgencia en diferentes ámbitos laborales. Con la gran variedad de sensores y de dispositivos inteligentes disponibles, los posibles usos de este tipo de sistemas se adaptan a los requerimientos de las personas o de empresas, mejorando la capacidad de alertar a los equipos de respuesta.

En esta sección se revisarán diferentes sistemas de notificación apoyados con IoT y como han sido aplicados en diferentes áreas de estudio. De esta manera analizar las problemáticas en la que se aplicaron y extraer ideas claves que puedan aplicarse a nuestro proyecto.

Sistemas de notificación de emergencias medicas

IoT y los sistemas de notificaciones dentro de la salud se expandió significativamente en los años de la pandemia de COVID-19. Sabukunze et al. (2021) comenta que “la salud potenciada por Internet de las cosas (IoT) es útil para el seguimiento eficaz de los pacientes con COVID-19, mediante el uso de una red conectada”.

Otra aplicación de IoT en el campo de la salud es el aviso de incidentes que requieran asistencia médica urgente. Utilizando una arquitectura cliente-servidor las agencias gubernamentales pueden notifiquen de manera rápida y eficiente a los usuarios dentro del rango de peligro en caso de ocurrencia de un desastre a través de SMS o notificaciones pulsadas en la aplicación móvil o al reloj inteligente (Ghazal et al., 2016).

Notificación de emergencia en desastres naturales

Los eventos que requieren un envío de mensajes urgentes ocurren a diario y en diferentes escenarios. Por ejemplo, ámbitos marítimos “un sistema de notificación de emergencia de IoT que puede rescatar rápidamente a personas que se ahogan” (Gong, 2022). Según el autor, “el servidor de IoT de emergencia envía un mensaje de notificación de emergencia al rescatista y le permite responder” (Gong, 2022).

En caso de accidentes automovilísticos, estos pueden ser detectados tanto por sensores dentro del vehículo como por teléfonos inteligentes. Las plataformas iPhone y Google Android pueden detectar automáticamente accidentes de tráfico usando acelerómetros y datos acústicos, notificando inmediatamente a un servidor central de despacho de emergencia y proporcionar información sobre la situación mediante fotos, coordenadas GPS y VOIP (White et al., 2011).

Sistemas de notificación en el cuidado del adulto mayor

Los sistemas de notificación orientados al cuidado de personas mayores han experimentado grandes avances gracias a la integración de IoT. Un claro ejemplo de estos cambios lo presenta Chen et al. (2007), quienes describen un sistema que utiliza tecnologías de RFID, servicios de video 3G y funciones de radio para monitorear posibles incidentes. En caso de que ocurra una caída, este sistema notifica al usuario por SMS, imágenes y video, asegurando de esta manera una mejor respuesta por parte de los equipos de emergencia.

El uso de métodos de mensajería instantánea es la mejor manera eficaz para comunicar una emergencia. En este sentido, Goldwin et al. (2024) destacan un sistema que haciendo uso de acelerómetros, GPS y giroscopios detectan caídas y comunican la alerta por medio de Telegram. Esta solución permite tanto a cuidadores como a familiares tener información precisa sobre el estado del adulto mayor.

Este tipo de avances muestran cómo la aplicación de IoT optimiza la respuesta de diferentes sistemas y además incrementa la calidad de vida y la seguridad de las personas mayores, por medio de un monitoreo continuo y menos intrusivo.

Mensajería instantánea en conjunto a sistemas de notificación

En la actualidad métodos como las redes móviles y aplicaciones de mensajería instantánea son usados normalmente para realizar llamadas y mensajes por parte de diferentes entidades, sin embargo, la cobertura desplegada por esta tecnología es un factor importante para tomar en cuenta.

La mensajería instantánea es una de las aplicaciones que más uso tiene en la actualidad y utilizar estas herramientas para el uso de sistemas de seguridad es algo fundamental. Esto se ve reflejado a continuación.

Los datos del sensor se enviarían a la plataforma ThingSpeak IoT mediante el protocolo MQTT¹. Los datos se visualizarán en gráficos y también pueden desencadenar diversas actividades, como enviar mensajes de alerta a través de Twitter o alertar a otros hogares en función de diversas condiciones (Nettikadan & Raj, 2018).

Utilizamos la red móvil GSM que es la más confiable y madura en la actualidad para lograr un sistema de alarma comunitario. Y transmitirá directamente la noticia de la alarma en un mensaje corto o por teléfono al teléfono móvil del gerente (Wang et al., 2016).

Monitorea los factores ambientales (es decir, humo, gas explosivo) y alerta automáticamente a los residentes por teléfono al descubrir una posible emergencia, lo que les permite confirmar el evento y comunicarse con los despachadores de emergencia con el mínimo esfuerzo (Benson et al., 2015).

Teniendo en cuenta lo anterior se puede decir que en virtud de los usuarios la alerta puede ser personalizada según lo necesite el cliente.

El resultado de esta investigación es un dispositivo que hace sonar una alarma y envía notificaciones vía Telegram cuando hay una persona dentro del alcance del sensor PIR, reduciendo

¹ Protocolo de mensajería basado en reglas, que permite la comunicación entre dispositivos

así los problemas habituales de búsqueda que suelen producirse en los hogares mediante el método de investigación en cascada (Kurniawan & Hariyanto, 2023).

Partiendo de lo antes mencionado se observa que este tipo de sistemas se puede adaptar con facilidad a las necesidades que se presenten por parte de los diferentes usuarios. Haciendo uso de una herramienta de uso diario.

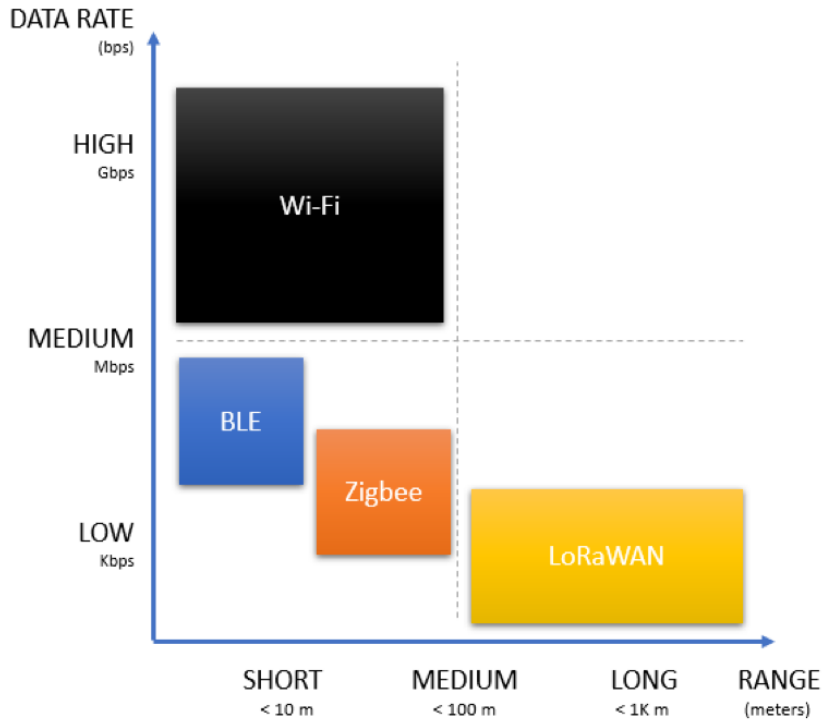
El desarrollo de las alarmas y alertas a través de las aplicaciones Telegrama y WhatsApp permiten que el sistema sea una herramienta funcional, ya que no se necesita la instalación de otras aplicaciones en los teléfonos de los usuarios, sino más bien aprovechar las redes sociales de uso cotidiano para el control y notificación de eventos delictivos que puedan suceder dentro y fuera del mercado. (Chicaiza Guachi, 2020)

El autor anterior nos emite una idea clara de un sistema de notificación que use mensajería instantánea y podemos afirmar que el uso de estas aplicaciones mejora en gran medida la versatilidad del sistema de notificación.

4.4. Tecnologías de comunicación

Las tecnologías de comunicación son aquellas que por medios guiados y no guiados permiten la transmisión de datos entre diferentes dispositivos interconectados entre sí, con esta premisa se realizó una comparativa con las tecnologías inalámbricas que más se relacionan con el desarrollo de este trabajo de titulación.

Figura 3
Comparativas de tecnologías de comunicación



Nota: obtenido de (Guest Blog: Wi-Fi, LoRaWAN, and IoT Convergence - Wireless Broadband Alliance, 2024)

4.4.1. Wi-Fi

La tecnología de Wi-Fi como se observa en la figura 3, permite la conexión a redes o internet con altas velocidades de transmisión, esta tecnología trabaja dentro del espectro radioeléctrico, donde por medio de ondas electromagnéticas transmite información de forma inalámbrica entre dispositivos.

Esta tecnología inalámbrica está basada en el estándar IEEE 802.11 en todas sus versiones, Wi-Fi fue desarrollada como alternativa del estándar cableado IEEE 802.3 (Ethernet). Opera en la banda ISM en 2.4 GHz y también en la banda de 5 GHz, esta última ofrece más canales y menor interferencia (Roa Parra, 2019).

Por lo tanto, Wi-Fi entrega altas velocidades de transmisión, con la banda de 5G la que optimiza este rendimiento, aunque a costa de reducir el rango de cobertura que puede alcanzar. Esta tecnología es la que más se ha globalizado y se ha vuelto la más accesible, lo que la convierte

en la principal tecnología que cumple con las demandas que genera el sector comercial y, en particular, las necesidades a cubrir en este proyecto.

De esta manera, la tecnología de Wi-Fi es la que más globalizada y accesible además de adaptarse a las necesidades del sector comercial y, por lo tanto, a las necesidades de nuestro proyecto.

4.4.2. LoRA

La figura 3 presenta la tecnología de LoRA y como es una forma de comunicación inalámbrica que permite establecer la comunicación inalámbrica a larga distancia con un bajo consumo de energía, ideal para aplicaciones de IoT. Según Ortiz Sosa, (2020) “LoRa es una técnica de modulación de la capa física desarrollada por Semtech, fundada en Chirp Spread Spectrum (CSS) con *señales robustas ante interferencias y ruidos.*”

El uso de LoRA se enfoca a escenarios donde las distancias son extensas siendo desde 10 a 20 km, además es una tecnología robusta que soporta interferencias. Por ello trabaja en frecuencias de 915Mhz, de esta forma logra mantener una comunicación constante, enfocada en mensajes de poco consumo de datos.

En comparación a Wi-Fi, LoRA entrega una seguridad de transmisión a largas distancias y una excelente protección contra ruidos que produzcan interferencias.

4.4.3. Zigbee

En cuanto a tecnologías “intermedias” la figura 3 nos muestra a Bluetooth y Zigbee en un mismo cuadrante, esto se debe a que Zigbee es una tecnología de comunicación inalámbrica que permite conectar dispositivos a poca distancia y con bajo consumo de energía, se usa principalmente en sectores como domótica, industria, y salud. Según (Castillo Imbaquingo, 2012) “Zigbee es una alternativa ideal para varios tipos de aplicaciones como una WSN, así como la monitorización del consumo energético, recopilación de datos y sistemas de automatización.”

En contraste con la tecnología de LoRA las distancias se ven reducidas, además de no mantener un sistema robusto enfocado a combatir el ruido, y a diferencia de Wi-Fi, las velocidades de envío de datos son menores. Sin embargo, logra ser una tecnología de alternativa en aplicaciones de: ciudades y hogares inteligentes, industria 4.0, el sector de la medicina, recopilación de datos, etc.

4.5. Trabajos relacionados

Introducción a los sistemas de notificación de emergencia

Los sistemas de notificación de emergencias son herramientas diseñadas para prevenir y mitigar los desastres, ya que permiten alertar a los usuarios del sistema de manera rápida y precisa. Este tipo de sistemas han cambiado desde métodos tradicionales que usan sirenas y mensajes transmitidos por radio y televisión, hasta soluciones actuales las mismas que aprovechan los teléfonos inteligentes y las redes de comunicación para alertar las emergencias.

Además, con los avances de la tecnología y la aplicación de IoT se han generado oportunidades para mejorar los sistemas de notificación desarrollados. Estas mejoras se ven reflejadas en la capacidad de geolocalización, la inteligencia artificial, la capacidad de alertar automáticamente sobre incidentes, entre otros.

Este proyecto se centra en desarrollar un prototipo para notificación de emergencia en caso de extorsión, de esta generar una nueva solución que permita reducir el problema de delincuencia que atraviesa el país.

Revisión de los tipos de sistemas de notificación

En el desarrollo de sistemas de notificación de emergencia se debe tener en cuenta las condiciones en donde será implementado, por lo tanto, generar un sistema lo más robusto posible no siempre es la mejor opción, pues el sobredimensionamiento de los sistemas es algo que ocurre frecuentemente.

Teniendo en cuenta lo anterior, un ejemplo de sobredimensionamiento se presenta con Cabezas Cortéz et al, (2017). Donde presenta un sistema de administración remota de una alarma comunitaria, donde el uso de raspberry pi 2 se usa para manejar un servidor web, activar una alarma y luces de emergencia. Optimizar el sistema hubiera sido la mejor prioridad, donde por medio de equipos adaptados a las necesidades de los usuarios se reduzcan costos y sea más accesible el sistema para la comunidad.

Para tener un sistema robusto tanto en procesamiento de datos como en respaldo de energía se debe tener claro los requerimientos de los usuarios y así cubrir sus necesidades.

En el ámbito de la seguridad personal, se han desarrollado diferentes dispositivos para que los usuarios logren notificar eventos delictivos. Por ejemplo, cuando una persona está en peligro y presiona el botón, se envía un mensaje de alerta a un número preestablecido Este sistema también puede activarse automáticamente en tres escenarios: cuando los sensores de presión y temperatura

alcanzan valores *elevados*, cuando el sensor de temperatura y frecuencia de pulso se vuelven *elevados* y el caso del sensor de frecuencia del pulso y presión se vuelven *elevados*. (Hyndavi et al., 2020)

El autor plantea un sistema orientado a mujeres, que envía una notificación de emergencia a un contacto específico al presionar un botón o en las condiciones antes mencionadas. Esta premisa a pesar de ser novedosa plantea problemas que suceden con los sensores, debido a la falta de capacidad de diferenciar entre agitación por actividad física y delitos. Estos falsos positivos afectarían negativamente a los usuarios, sin embargo, la portabilidad es una premisa interesante que se puede implementar en nuestro sistema.

Otros ámbitos en donde la notificación de emergencia es necesaria se encuentra en el área de ciudades inteligentes, más específicamente dentro de los hogares. (Rifat Yıldız et al., 2020) propone lo siguiente:

La solidez del sistema de seguridad IoT que proponemos depende de las tecnologías de comunicación inalámbrica integradas para ofrecer una solución de bajo coste con la máxima libertad de capacidad inalámbrica. Además, hemos utilizado un teléfono inteligente y un sistema de seguridad desarrollado con el módulo de cámara NoIR Pi y el sensor de movimiento PIR que son fáciles de usar y de instalar.

A través del uso de cámaras y sensores, el sistema logra detectar la presencia de intrusos en el hogar y de esta manera alertar por medio de una aplicación la posible amenaza a la seguridad.

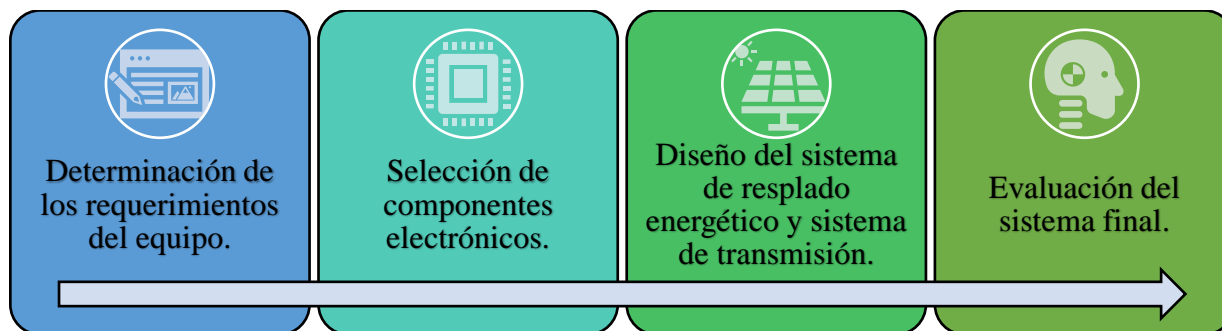
Los diferentes tipos de sistemas de notificación y la integración de IoT, no solo proporciona seguridad en tiempo real, sino que también facilita la implementación de soluciones accesibles y eficientes. Cumplir con los requerimientos principales permite a los usuarios mantener un control adecuado y un fácil dominio del sistema, este tipo de cualidades son las que se buscaron implementar en nuestro sistema.

5. Metodología

En esta investigación, titulada “Sistema de seguridad comunitaria antiextorsión utilizando sistemas embebidos en el casco urbano de la ciudad de Loja”, se propone una metodología estructurada en los siguientes bloques:

Figura 4

Segmentación de metodología



Nota. Autor

5.1. Determinación de los requerimientos del equipo

Para determinar las características del equipo y que responda a las necesidades observadas en el sector comercial del casco céntrico de la ciudad de Loja; se realizó una recopilación de información relacionada con la aceptación que tendría nuestro sistema de seguridad antiextorsión en los posibles usuarios y beneficiados. Los aspectos se detallan en el siguiente apartado:

- Pequeño y portátil.
- Al menos dos vías de comunicación independientes.
- Fácil de usar.
- Con respaldo de energía.
- Escalable.
- Desarrollo de bajo costo.
- Fácil de instalar.

Tabla 1
Datos de requerimientos

Pruebas	Sector	Respaldo energético	Posibles usuarios	Señal GSM	Señal Wi-Fi
1	Mercado Tebaida	Necesario	160	Buena	Buena
2	Mercado central	Necesario	180	Buena	Moderada
3	Mercado mayorista	Necesario	240	Buena	Moderada
4	Zona la banda	Necesario	190	Buena	Moderada
5	Zona UNL	Necesario	100	Buena	Buena

Nota. Autor

Con los requerimientos establecidos, se iniciaron las pruebas en las zonas de estudio, el orden y la ubicación se destalla en la tabla 1. Se contempló el sistema de respaldo energético en todos los lugares donde se realizaron los ensayos, dado que no existían equipos o sistemas que curvan esta necesidad.

Durante las pruebas del prototipo, se realizó una aproximación del promedio de usuarios potenciales del sistema en cada área de estudio. Además, se comprobó la disponibilidad de señal GSM y Wi-Fi en los lugares de pruebas. Los resultados mostraron una buena cobertura y desempeño de la señal GSM. Sin embargo, la red Wi-Fi presentó problemas de cobertura debido a la estructura de algunos edificios, lo que afectó negativamente a la transmisión de mensajes a través de la red.

5.2. Selección de componentes electrónicos

El sistema incluye dos bloques principales; el bloque de sistema de transmisión de datos y el sistema de respaldo energético. Con el objetivo de mantener un orden en el documento y una mejor comprensión, esta sección se divide en: componentes del sistema de transmisión y el sistema de respaldo energético. Además, es importante acotar que los dispositivos seleccionados aparte de cumplir con las especificaciones descritas en la tabla 1 deben permitir el desarrollo de un sistema escalable y asequible económicamente.

En la tabla 2 se puede identificar los diferentes componentes que se utilizaron en este proyecto.

5.2.1 Componentes del sistema de transmisión de datos

Tabla 2

Tabla de elementos según el sistema propuesto

Sistema de transmisión de datos
Módulo ESP32
Módulo SIM 8001
Resistencia 4.7k Ohm
Pulsador

Nota. Autor

En la tabla 2 se identifican los diferentes elementos que se interconecta en el sistema de transmisión de datos. A continuación, se detallan los principales componentes.

Tabla 3

Especificaciones técnicas del módulo ESP32

Equipo ESP32-WROOM-32



Categoría	Descripción	Características
Certificaciones	Wi-Fi	Wi-Fi Alliance
Wifi	Protocolos	802.11 b/g/n (802.11n velocidades de hasta 150 Mbps)
Hardware	Rango de frecuencia central del canal operativo	2412 – 2484 MHz
	Voltaje de funcionamiento	3.3V
	Corriente de funcionamiento	80mA
	Corriente mínima suministrada por la fuente de alimentación	500mA

Rango de temperatura ambiente de funcionamiento recomendado	-40°C a +85°C
Dimensiones	18mm x 28.5mm x 3.10mm

Nota. Tomado de (ESP32WROOM32 Datasheet, 2023)

Tabla 4
Especificaciones técnicas módulo SIM800L

Equipo Módulo SIM800L



Características	Descripción
Voltaje de entrada	3.4V – 4.4V
Corriente de entrada	0.7mA (ATM+CFUN=0)
Bandas de frecuencia	GSM 850, EGSM 900, DCS 1800, PCS 1900
Rango de temperatura	-40°C a +85°C
SMS	MT, MO, CB, texto y modo PDU
Dimensiones	15.8mm x 17.8mm x 2.4mm

Nota. Tomado de (SIM800L GSM Module Pinout, Datasheet, Equivalent, Circuit, and Specifications, 2024.)

5.2.2 Componentes del sistema de respaldo energético

Tabla 5
Componentes del sistema de respaldo energético

Sistema de respaldo energético
Módulo regulador de voltaje 5v DC
Módulo cargador de batería 7.4v DC
Módulo conmutador 5v, 12v, 24v
Batería de litio 7.4v DC

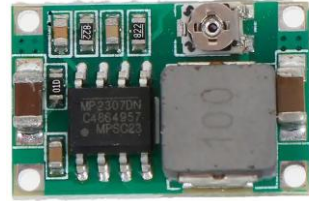
Nota. Autor

En la tabla 5 se identifican los diferentes elementos que se interconecta para generar el sistema de respaldo energético. A continuación, se detallan los principales componentes.

Tabla 6
Especificaciones técnicas del módulo regulador de voltaje

Equipo

Módulo regulador de voltaje Mini 360
MP2307

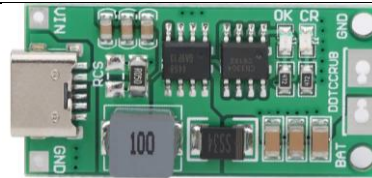


Características	Descripción
Voltaje de entrada	4.75 a 23V
Voltaje de salida	1 a 17V (Ajustable)
Corriente de salida máxima	3A (Depende del voltaje de salida)
Eficiencia de conversión	96% (más alta)
Frecuencia de conmutación	340 KHz
Ondulación de salida	30 mV (sin carga)
Regulación de la carga	±0.5%
Temperatura de funcionamiento	-40°C a +150°C
Dimensiones	17mm x 11mm x 4mm
Peso	3g

Nota. Tomado de (DC DC-Converters – Matt’s Electronics, 2024.)

Tabla 7
Especificaciones técnicas del módulo cargador de baterías

Equipo Módulo cargador baterías tipo litio
2s 2 celdas 7.4v 2a USB tipo C



Características	Descripción
Voltaje de entrada	3V – 6V (se recomienda 3.7V - 5V)
Corriente de entrada	2A
Voltaje de carga	8.4V
Corriente de carga	1.1 ^a
Temperatura de funcionamiento	-40°C a +85°C
Tamaño	39mm x 18mm x 6.3mm

Nota. Tomado de (Type C BMS 2S 2A 18650 21700 3.7V Lithium Battery Charge Board Step-Up Boost Li-Po Polymer USB C To 8.4V, 2024.)

Tabla 8
Especificaciones técnicas del módulo conmutador de emergencia

Equipo Módulo Conmutador de Emergencia de corte de energía con relé ups	
Características	Descripción
Voltajes permitidos	5V – 48V
Carga permitida	Hasta 10A
Mientras se encuentre conectada la alimentación DC, la batería se cargará al mismo tiempo que se entrega alimentación a la salida.	-
La conmutación se realiza de manera automática al desenergizar la entrada DC	-
El módulo prefiere predeterminadamente la fuente de alimentación DC mientras esté disponible	-
La conmutación posee un delay de 0.7 segundos por la demora del relé.	-
Dimensiones	61x30x18mm
Peso	23.9g

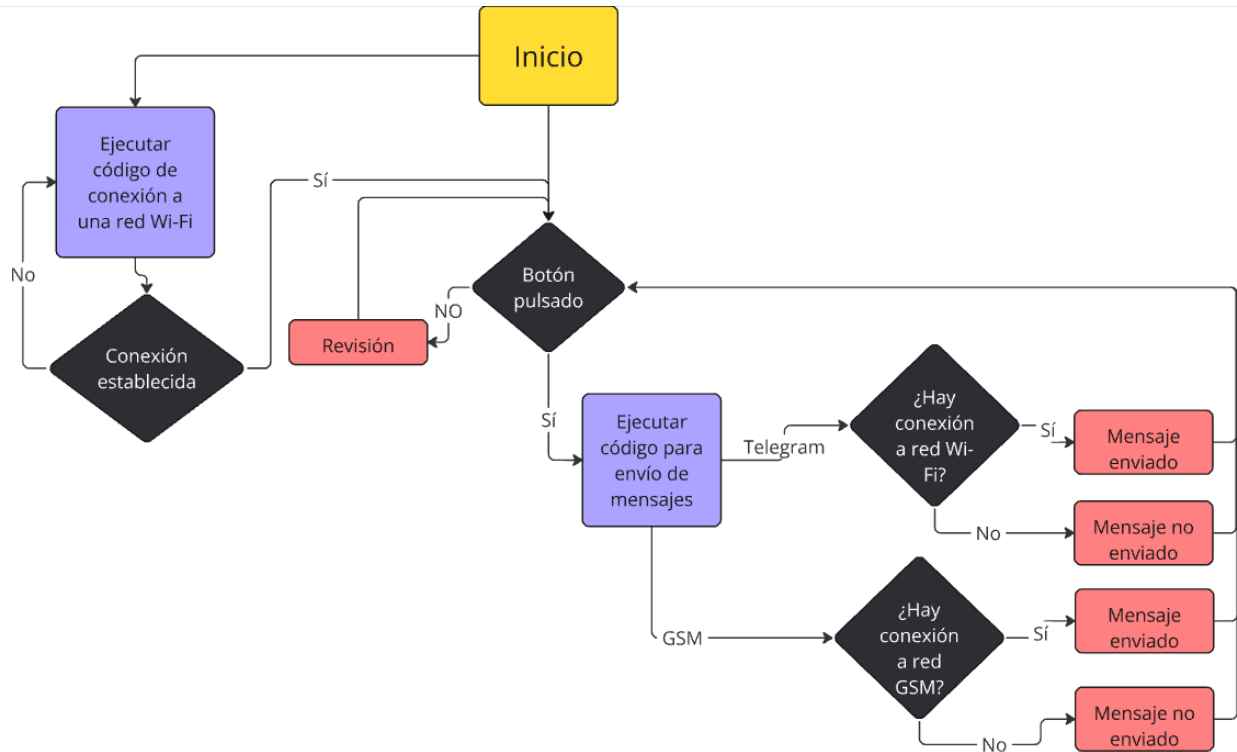
Nota. Tomado de (Power-OFF Protection Module Automatic Switching Module UPS Emergency Cut-off Battery Power Supply 12V to 48V Control Board, 2024.)

5.3. Diseño del sistema de respaldo energético y sistema de transmisión de datos

5.3.1. Sistema de transmisión

Figura 5

Diagrama de flujo del sistema de transmisión

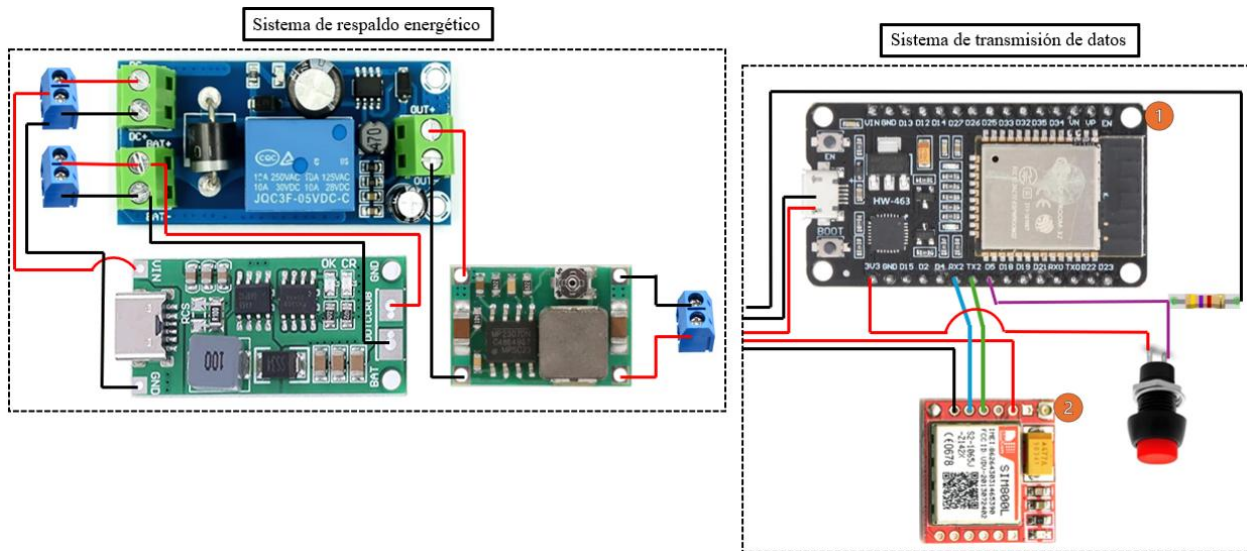


Nota. Autor

La parte lógica de nuestro sistema se desglosa dentro de la figura 5, una vez que el dispositivo se conecta a la red eléctrica lo primero que realiza son dos acciones simultáneas; la primera es ejecutar el código para conectarse a la red Wi-Fi, esto lo hará hasta tener un resultado positivo, la segunda acción es comprobar el estado del pulsador. Estas dos acciones paralelas se deben a que el sistema trabaja con dos vías de comunicación.

En caso de que se presione el pulsador se ejecuta el código encargado de enviar mensajes, tanto por la tecnología GSM y Wi-Fi, de esta manera asegurar la entrega del mensaje. Esta acción quedará en bucle hasta alterar nuevamente el estado del pulsado a uno de espera. En caso de accionar el pulsador cuando aún no se haya tenido una conexión a internet el mensaje será enviado solo por la red GSM.

Figura 6
Interconexión de los sistemas internos del sistema antiextorsión.



Nota. Autor

En la figura 6 se puede observar en la parte derecha el sistema de transmisión de datos, el mismo que se compone de los siguientes elementos:

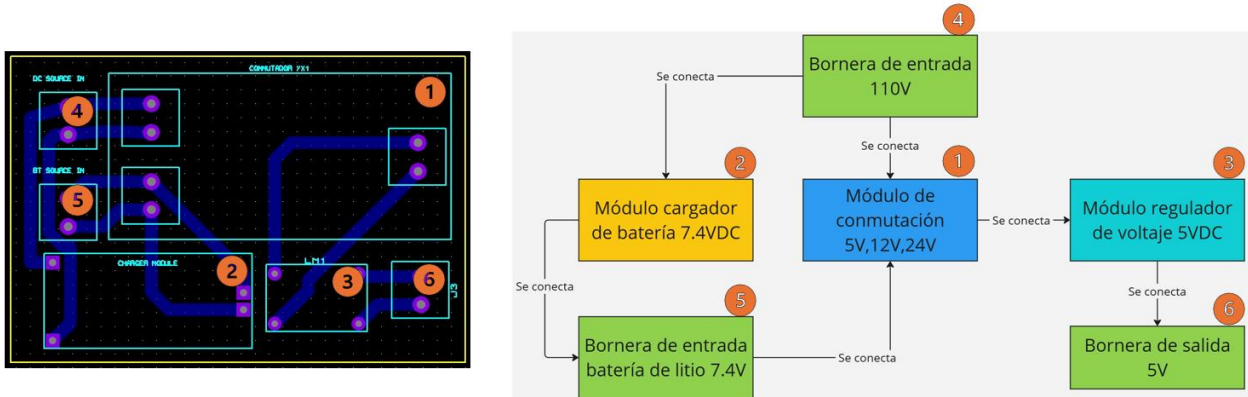
1. Módulo ESP32, es el encargado de ejecutar la parte lógica detectando el estado del pulsador y de acuerdo con el estado en el que se encuentre, enviar mensajes por GSM y Wi-Fi.
2. Módulo SIM 8001, es aquel elemento que nos permite enviar SMS por medio de la tecnología GSM.

El sistema de transmisión de datos se conecta a la salida del sistema de respaldo energético, de esta manera asegurar el funcionamiento del prototipo aun en casos de tener fallas en el suministro de energía. Los demás elementos que se encuentran en la parte derecha se describen en la tabla 2.

5.3.2. *Sistema de respaldo energético*

La función principal de este sistema es presentar una protección contra los cortes de energía, donde en el momento de no existir alimentación de la red eléctrica cambie de manera rápida al banco de baterías, de esta forma mantener el equipo funcionando en caso de fallar el suministro energético.

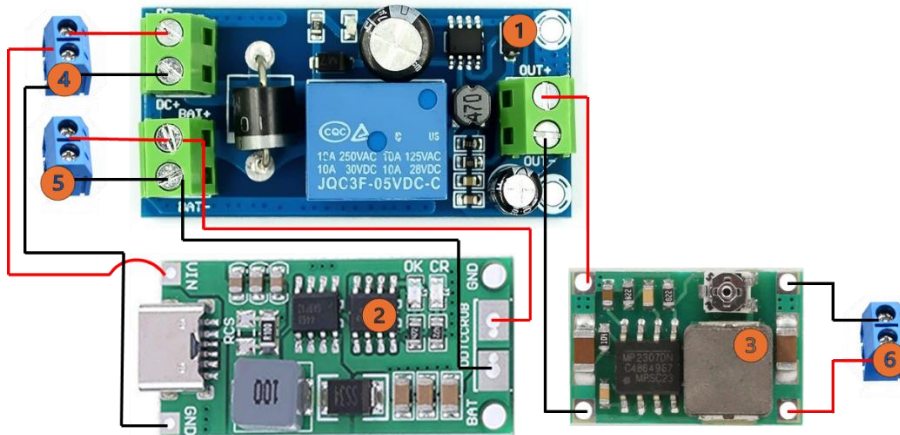
Figura 7
Diagrama de conexiones del sistema de respaldo energético



Nota. Autor

El diagrama de bloques y el modelo de la placa de circuito impreso se observa en la figura 7, donde se logra identificar la distribución de todos los componentes y como se interconectan dentro del sistema de respaldo energético.

Figura 8
Diseño del circuito para el sistema de respaldo energético



Nota. Autor

Cómo está distribuida la placa de circuito impreso del sistema de respaldo energético y como se interconectan entre los diferentes elementos que lo conforman se detallada en la figura 8. Además, estos componentes se mencionan a continuación:

1. Módulo de conmutación 5V, 12V, 24V
2. Módulo cargador de batería 7.4 VDC
3. Módulo regulador de voltaje 5VDC
4. Bornera de entrada 110V

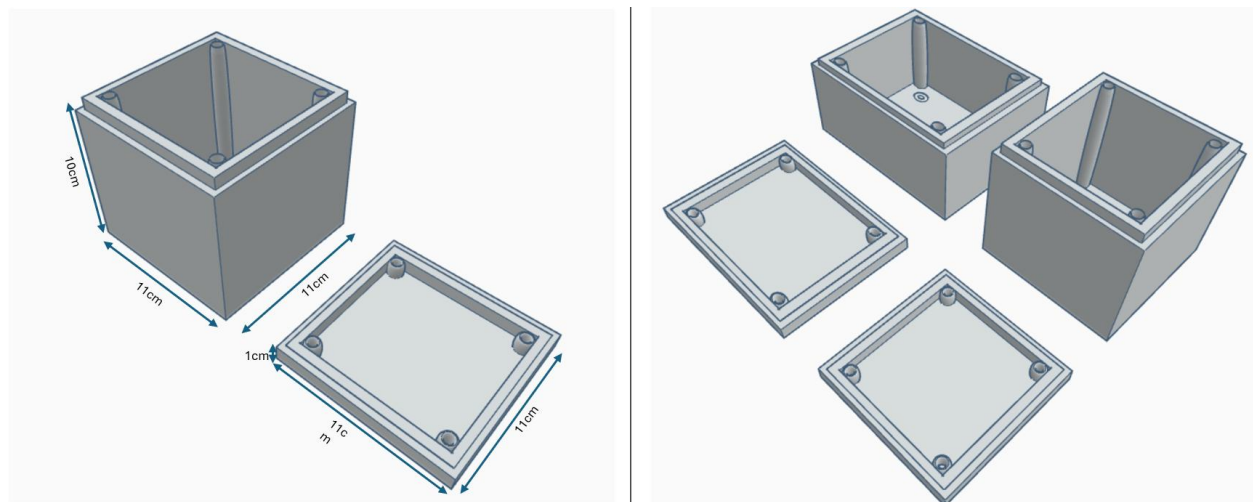
5. Bornera de entrada batería de litio 7.4V
6. Bornera de salida 5V

Las dimensiones que se generaron en la placa de circuito impreso del sistema de respaldo energético fueron de 10 x 7 cm, estas medidas se vieron reflejadas para la adquisición del gabinete contenedor.

Diseño y construcción del prototipo final

En cuanto al diseño del gabinete este se construyó usando la herramienta web Tinkercad, debido a la versatilidad y fácil uso de herramientas en 3D que entrega esta plataforma, además de tener experiencia previa usando el software.

Figura 9
Diseño 3D del gabinete



Nota. Autor

Los diferentes diseños 3D se los remarca en la figura 9. En esta se muestra la idea del gabinete con tapa a utilizar, el mismo se encuentra dividido en dos vistas. La primera a la izquierda, se observa el gabinete con dimensiones de 11 cm de ancho y largo, y 10 cm de alto. Las mismas dimensiones se aplican a la tapa, pero con una altura de 1 cm. Además, se logran identificar los puntos de apoyo dispuestos para la sujeción del gabinete.

En la segunda sección a la derecha de la imagen, se observa la variedad de gabinetes que se contemplaron en nuestro proyecto, en ellos se alteraron dimensiones para minimizar el tamaño a la más pequeña expresión. Sin embargo, por razones de disponibilidad, optimización de tiempo y costos, se optó por adquirir el gabinete que posea las medidas que se muestran en la figura 9. De

esta manera el diseño elaborado ayudo a tener una idea clara de las dimensiones necesarias para almacenar los diferentes elementos que conforman el sistema antiextorsión.

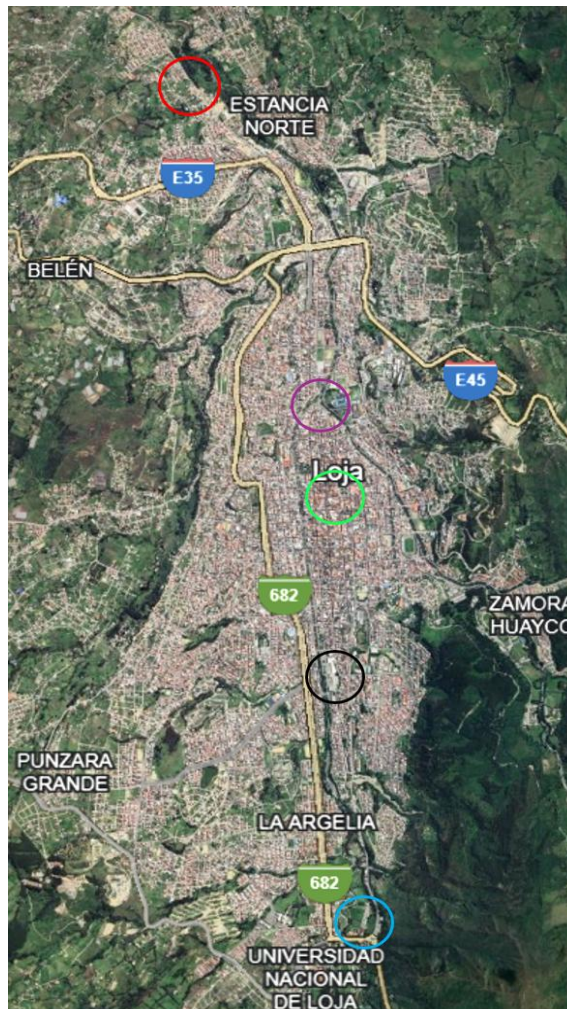
5.4. Evaluación del desempeño del prototipo

Lo evaluado en esta sección consiste en dos aspectos, primero la flexibilidad de transmitir datos por medio de dos tecnologías y analizar su desempeño en diferentes escenarios. En cuanto a las pruebas de funcionamiento, se enfocó medir los mensajes exitosos y fallidos tanto en Telegram como por SMS teniendo en cuenta la cobertura de red Wi-Fi como red GSM.

Las pruebas se enfocaron en las zonas cercanas a los principales puntos comerciales, de esta manera evaluar los siguientes datos: retraso del envío de mensajes, perdidas de mensajes, eficiencia del sistema e independencia energética.

Figura 10

Mapa de la ciudad de Loja y zonas de pruebas



Nota. Tomado de (MAPA INTERACTIVO ECUADOR, 2024)

En la figura 10 se observa diferentes zonas marcadas las mismas que se listan a continuación con orden superior a inferior:

- Zona de la banda (Rojo)
- Zona del mercado mayorista (Morado)
- Zona del mercado central (Verde)
- Zona del mercado de la Tebaida (Negro)
- Zona de la Universidad Nacional de Loja (Azul)

6. Resultados

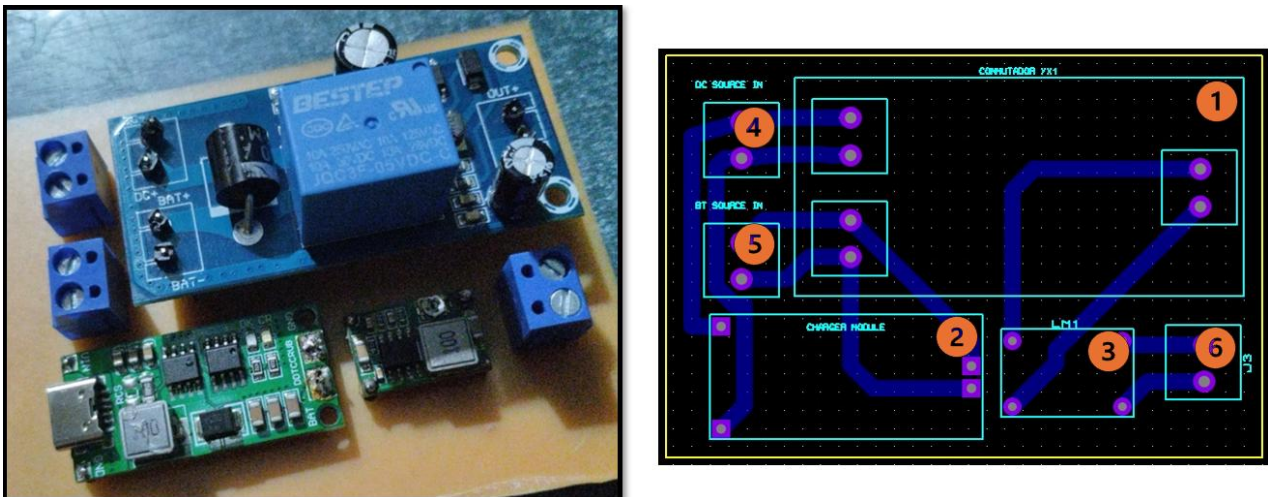
En esta sección se describen las diferentes fases desarrolladas durante la elaboración del sistema antiextorsión, teniendo en cuenta el análisis de los requerimientos y los datos recopilados en las zonas comerciales de la ciudad de Loja. Los resultados obtenidos incluyen un prototipo que cumple con las necesidades comunitarias identificadas en las áreas evaluadas, una evaluación del sistema de respaldo energético y la cotización parcial y total de los diferentes prototipos.

6.1. Construcción del prototipo

En cuanto al prototipo del sistema antiextorsión, se buscó materiales de bajo costo y de buenas prestaciones que sean de fácil acceso y remplazo. Siendo componentes como un ESP32, un módulo SIM800L, un sistema de respaldo energético, pulsador accionador, resistencia y un gabinete plástico los que conforman los dispositivos.

En cuanto al desarrollo del sistema de respaldo energético se hizo la adquisición de equipos genéricos, de esta manera mantenernos en el presupuesto destinado al sistema, para el desarrollo de la placa de circuito impreso se trabajó en el software Proteus. Seleccionamos este programa por la facilidad de trabajo, su versatilidad y la gran información que existe de este software en internet.

Figura 11
Sistema de respaldo energético

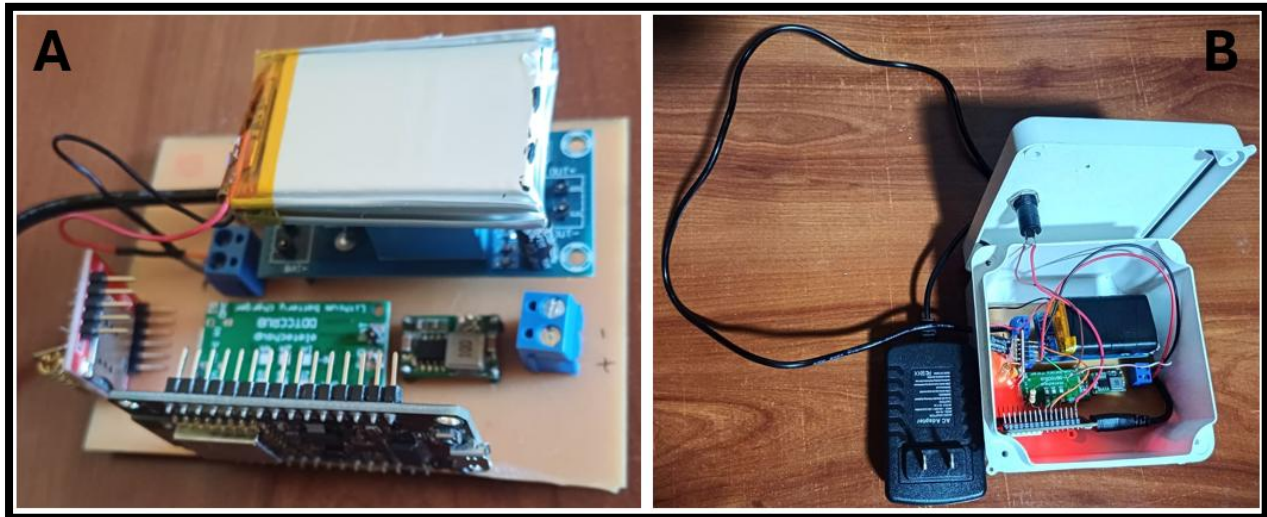


Nota. Autor

El sistema de respaldo energético culminado se observa a la izquierda de la figura 11, el orden de los componentes se puede apreciar de mejor manera en la figura 8. Una vez terminada la PCB se decidió dejar 5 cm de borde en la placa, de esta manera colocar los componentes del sistema de transmisión.

De esta manera, se buscó tener una disposición de los componentes que conforman el sistema de transmisión de datos en los bordes de la PCB, así reducir el espacio necesario de los dos sistemas mencionados en la sección 5.2 de este documento.

Figura 12
Ensamblaje del sistema antiextorsión



Nota. Autor

Observamos como será la posición final de los elementos que conforman el prototipo del sistema antiextorsión dentro de la figura 12 sección A, y se logra identificar que todos los componentes colocados en la parte interior de la placa corresponden al sistema de respaldo energético y los componentes orientados verticalmente forman parte del sistema de transmisión de datos.

Para colocar los diferentes elementos se buscó la forma más óptima y compacta, de manera que se reduzca al máximo el tamaño del prototipo y que se permita tener una fácil conexión entre los diferentes equipos. El tamaño del dispositivo puede variar tanto en ancho o en altura según la disposición de los elementos, logrando adaptar el tamaño y las dimensiones según las necesidades del usuario final. Además, en caso de utilizar dispositivos de montaje superficial (SMD) el tamaño del sistema de respaldo energético se puede reducir en gran medida.

En cambio, dentro de la figura 12 sección B se observa las dimensiones del dispositivo final, las cuales son de 11cm de ancho, 11cm de profundidad y 7 cm de alto. Estas corresponden a las medidas desarrolladas en los modelos 3D, dentro del gabinete observamos los sistemas de

transmisión de datos y el sistema de respaldo energético y adicional a ello el transformador que se conecta a la corriente eléctrica.

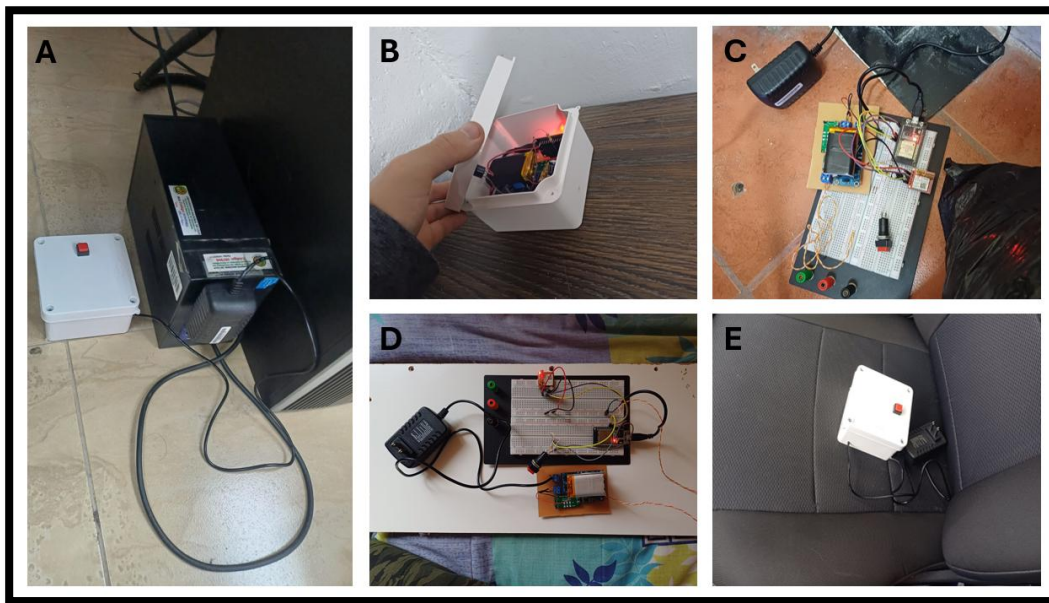
6.2. Análisis del desempeño del sistema de transmisión antiextorsión

Para recopilar los datos necesarios se hizo envíos de mensajes cada minuto durante horas, de esta manera identificar posibles fallos. En cuanto a la información necesaria del sistema de transmisión de datos, se recopiló durante 4 a 5 horas en cada zona propuesta, esto con la finalidad de trabajar la información y conocer el comportamiento de nuestro sistema en diferentes escenarios.

En las pruebas realizadas se observó que el retraso entre mensajes varía muy poco y con cifras muy pequeñas. Por lo tanto, la variabilidad entre mensajes puede ser despreciable.

Figura 13

Lugares donde se hicieron pruebas de funcionamiento



Nota. Autor

Dentro de la figura 13 se remarcan los lugares de pruebas en las diferentes zonas de la ciudad. Más adelante, se detallan los resultados obtenidos en cada uno de los sitios, exponiendo con mejor detalle los datos recopilados en las diferentes zonas de pruebas.

Dentro de la misma figura las zonas C, D y E son aquellas donde se utilizó el sistema de respaldo energético, por lo tanto, en estas zonas se recopiló datos para el sistema de respaldo energético. *Los datos recopilados por el sistema de respaldo energético se los presentará más adelante en esta misma sección.*

En cuanto a las pruebas de transmisión de datos, se realizaron enviando mensajes cada minuto durante horas. De esta manera tratar de almacenar la mayor cantidad de datos posible para un correcto análisis.

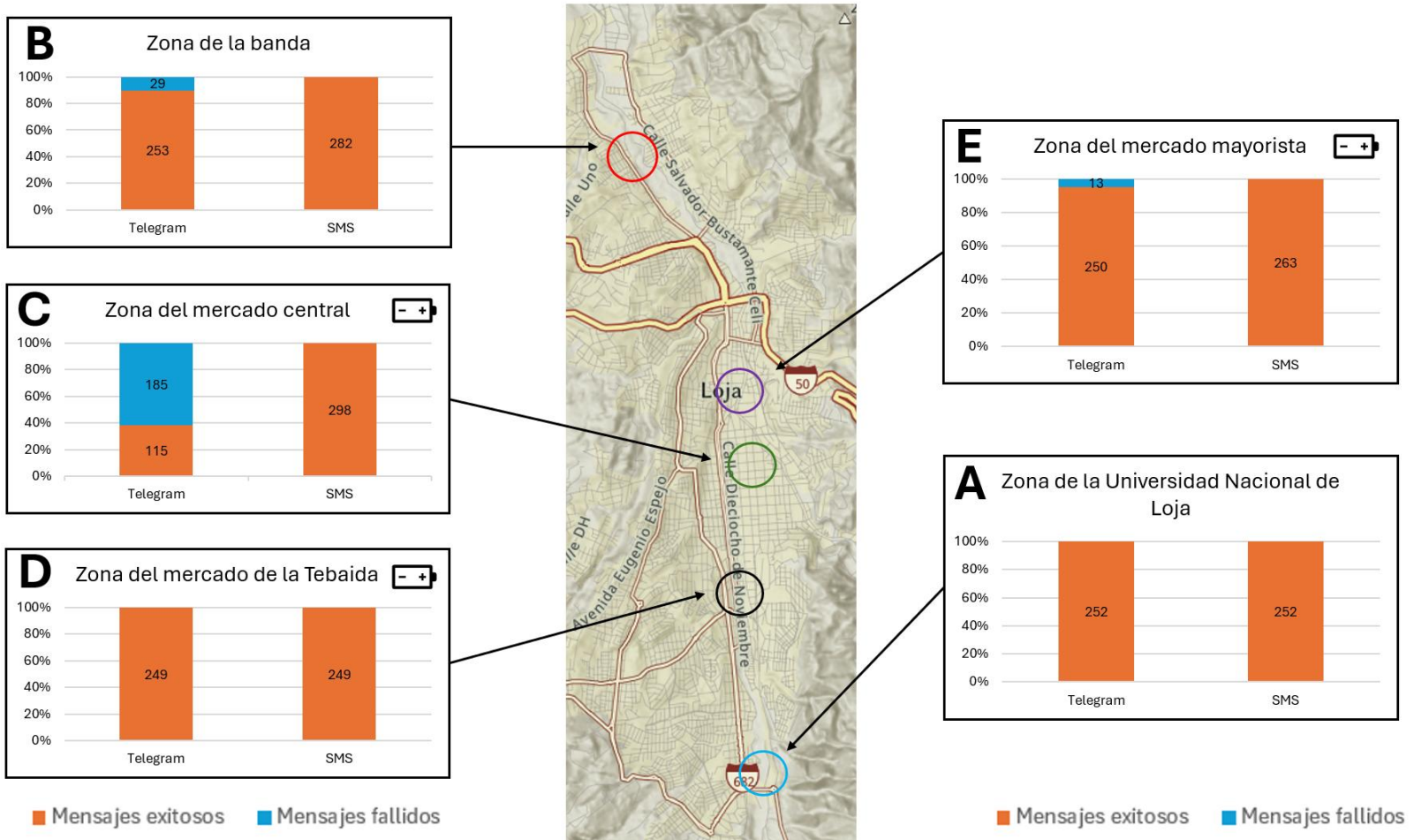
La distribución del mapa de la ciudad de Loja y el resultado de los datos analizados según la zona de estudio, junto a los éxitos y fallos presentes durante las pruebas, son reflejados en la figura 14.

Entre las zonas con mayor fallo se logra identificar que la zona del mercado central la cual tuvo el peor rendimiento, tener en cuenta que en esta prueba se buscó realizar el desarrollo del peor de los casos, por ello se seleccionó un edificio comercial con una infraestructura robusta, lo que dificultaría la emisión de señal Wi-Fi en su interior. En cambio, los mensajes errados usando Wi-Fi fueron correctamente entregados por GSM, con un total de 60% de mensajes vía Telegram fallados.

De igual manera en la zona de la banda se observa cómo un 10% de los mensajes se perdieron y en la zona del mercado mayorista cómo un 5% de los mensajes fallaron, sin embargo, fueron errores poco frecuentes, afectados únicamente por la calidad de señal Wi-Fi.

Para todas las otras zonas el envío de mensajes vía Telegram y SMS fueron del 100% de éxito, esto debido a una buena cobertura tanto de Wi-Fi como de la red GSM.

Figura 14
Resultados según las zonas de estudio en la ciudad de Loja



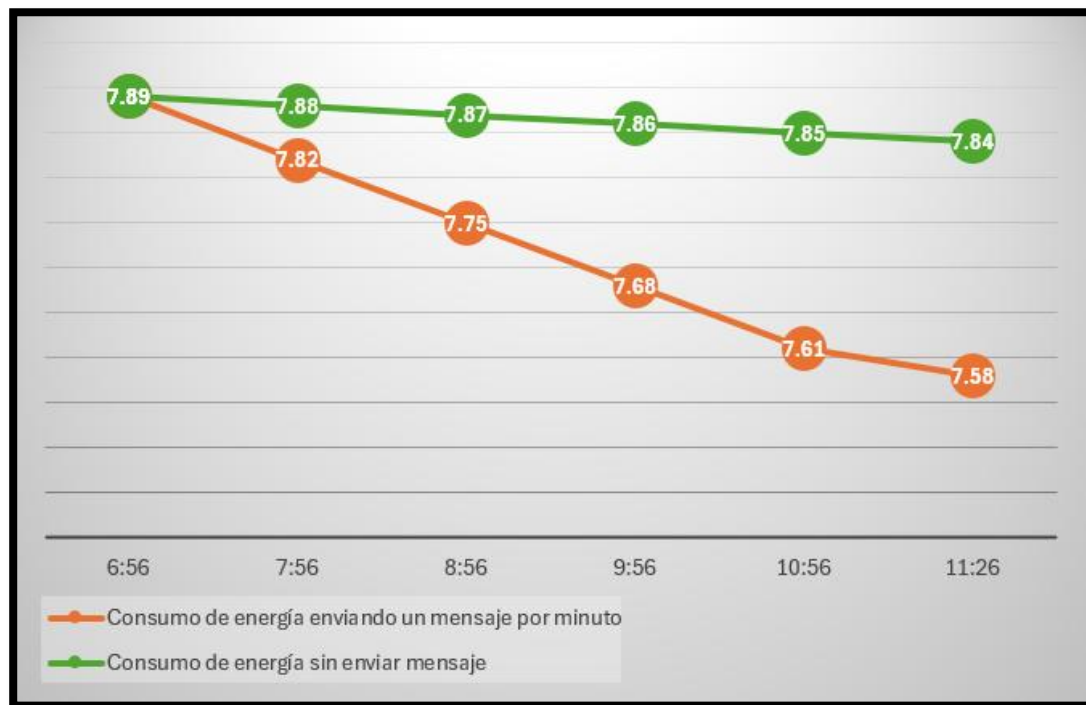
Nota. Autor

6.3. Análisis del sistema energético

El seguimiento del sistema energético se realizó en tres zonas remarcadas con una batería en la figura 14. Se decidió medir durante dos días en cada localización el desempeño de nuestro sistema; el primer día se buscaba presionar el sistema con envíos continuos en cada minuto, así mantener el sistema antiextorsión activo la mayor parte del tiempo. En el segundo día se contrastaba el desgaste de la batería con el sistema antiextorsión en modo espera.

De esta manera se midió el voltaje cada hora durante 5 horas, observando como nuestro sistema de respaldo energético entrega una autonomía considerable. Tener en cuenta que el envío de mensajes no será invasivo, se planteó utilizar mensajes cada 2, 3 o 5 minutos. Este tiempo varía en función de las necesidades del usuario y en consecuencia aumentará el tiempo de autonomía.

Figura 15
Análisis de datos del sistema energético



Nota. Autor

El análisis de los datos que corresponde al sistema de respaldo energético, su comportamiento se detalla en la figura 15, donde se observa la diferencia de funcionamiento. Marcado con color verde la variación de energía cuando el sistema **no** está enviando ningún mensaje. En cambio, el color naranja indica la variación de energía cuando el sistema **si** envía mensajes, para los casos de estudio se realizaron enviando mensajes cada minuto.

Se diferencia claramente que cuando el sistema está en espera el gasto de energía es mínimo, a diferencia del sistema en un consumo constante. En conclusión, se puede asegurar que la autonomía energética que entrega nuestro sistema es más que suficiente para cubrir una escases de energía prolongada.

6.4. Análisis Económico

Tabla 9

Detalle del análisis económico

Elementos	Costo
Módulo regulador de voltaje 5VDC	\$3.60
Módulo cargador de batería 7.4 VDC	\$12.00
Batería de Litio 7.4 VDC	\$25.00
Conmutador 5/12/24 VDC	\$8.60
Módulo ESP32	\$10.00
Módulo SIM8001	\$9.00
Switch / Pulsador	\$0.50
Componentes de conexión	\$10.00
Gabinete	\$1.40
TOTAL	\$80.10
TOTAL / Prototipo simple	\$30.90

Nota. Autor

En la tabla 9 se observa el gasto total realizado en el desarrollo de los dos diferentes prototipos; el total para el prototipo que utiliza el sistema de respaldo energético y el sistema de transmisión de datos fue de \$80.10 dólares y para el prototipo que solo utiliza el sistema de transmisión de datos fue de \$30.90 dólares.

En resumen, la construcción, distribución e implementación de nuestro sistema en diferentes comunidades comerciales es viable y ampliamente escalable.

7. Discusión

El sistema de seguridad comunitaria antiextorsión desarrollado presenta múltiples ventajas en comparación a sistemas similares o comerciales. La principal ventaja es el costo de fabricación. Esto se redujo al implementar un diseño reducido y compacto, ajustando el sistema a las necesidades analizadas, este enfoque nos permitió reducir los costos y evitar sobredimensionar las capacidades del sistema. Sistemas más elaborados y robustos como el desarrollado por (Majumder & Izaguirre, 2020) muestra un sistema de detección y monitoreo facial, el mismo que envía una notificación al usuario. Para nuestro sistema antiextorsión nos enfocamos principalmente en la notificación de emergencias, asegurándonos que el mensaje llegue correctamente.

El sistema antiextorsión desarrollado a pesar de no tener funciones tan complejas resulta ser muy versátil, esto debido a la capacidad de adaptación de acuerdo con las necesidades del cliente. Por ejemplo, en temas de seguridad personal, funciones como las que detalla (Hyndavi et al., 2020), donde se envía una alerta según factores cardiacos o por medio de la activación de un pulsador. pueden ser implementadas dentro de nuestro sistema antiextorsión.

En cuanto al desarrollo del hardware observamos como sistemas similares que cubren más factores en cuanto a seguridad puede ser más costoso, esto se debe a la cantidad de datos que se plantea enviar y de las necesidades del cliente. Sin embargo, sistemas como el que plantea (Ur Rehman et al., 2021) muestra la aplicación de sistemas de notificación de emergencia con un hardware reducido, donde usando un SIM800l envía mensajes en caso de accidentes. Sin embargo, en caso de accidentes o emergencias es mejor utilizar la mayor cantidad de vías de comunicación, de esta manera lograr acercar la información necesaria a los elementos de seguridad correspondientes. Por razones como esta, fue que se decidió utilizar más de una sola tecnología de comunicación.

Para el caso de seleccionar una aplicación de mensajería se buscó utilizar las más comerciales, seguras y que sean gratuitas, sistemas como el diseñado por (Made et al., 2021) donde por medio de una Raspberry Pi monitorea factores de seguridad en un hogar y envía una notificación por medio de Telegram. Son un claro ejemplo del objetivo que se tenía en mente, sin embargo, el uso de un sistema como una Raspberry Pi era sobredimensionar nuestro sistema. Por ello se usó componentes de bajo costo y que permitan una adecuada conexión con las aplicaciones de mensajería instantánea.

Por lo tanto, aplicaciones como WhatsApp, Telegram, Facebook y Twitter fueron las principales a tomar en cuenta. Para el caso de nuestro sistema se utilizó Telegram por la capacidad de ser implementado fácilmente con los componentes que conforman el sistema de transmisión de datos y además la aplicación posee un buen apartado en cuanto a seguridad de mensajes y cifrado de los mismos.

Un añadido a la aplicación de mensajería fue utilizar una aplicación de lectura de notificaciones, por ello se buscó y se probó diferentes aplicaciones, la aplicación que se utilizó en nuestro proyecto se llama WDSERVICE. Añadir esta función nos permite asegurar que el receptor de los mensajes siempre esté enterado de las notificaciones. Debido a que la aplicación antes mencionada realiza la lectura en voz alta de las notificaciones, incluso si el teléfono inteligente del receptor se encuentra en silencio.

Un sistema de respaldo energético es algo que no se contempla en los sistemas de seguridad comerciales, en nuestro sistema antiextorsión planteamos un sistema de respaldo energético, donde en caso de fallar la energía eléctrica el sistema continúe trabajando con normalidad. La independencia energética de nuestro sistema presentó excelentes resultados esto se debe al bajo consumo de energía que realiza el sistema propuesto.

Además, otro factor importante es el uso de diferentes tecnologías de comunicación, nuestro prototipo integra dos tipos de tecnología, esto con la finalidad de en caso de faltar una de ellas, tener la posibilidad de transmitir el mensaje de alerta por otro medio.

Por lo tanto, podemos decir que nuestro sistema es una alternativa confiable, que se ajusta a los requerimientos principales de seguridad. Además de presentar una mejora en cuestión de respaldo energético y capacidad de comunicación.

De este modo, se puede concluir que, mediante ajustes en los microprocesadores y modificando las dimensiones del gabinete nuestro sistema antiextorsión es adaptable a diversas necesidades y aplicable a diferentes áreas de trabajo. Esto demuestra que la escalabilidad de nuestro sistema es favorable y que las posibles aplicaciones dependerán de los requisitos específicos que tenga cada cliente.

8. Conclusiones

Este trabajo de titulación tuvo como objetivo principal el desarrollo de un sistema de seguridad antiextorsión orientado al sector comercial de la ciudad de Loja. Luego de analizar los resultados obtenidos, se permitió establecer las siguientes conclusiones:

- ✚ El sistema desarrollado cumple el propósito de esta investigación, se obtuvo un sistema capaz de enviar mensajes de alerta por medio de dos tecnologías de comunicación Wi-Fi y GSM, logrando un desempeño del 90% de eficacia en la entrega de mensajes durante las diferentes pruebas realizadas dentro de la ciudad de Loja.
- ✚ El sistema desarrollado demostró ser aplicable en diferentes tipos de trabajo, en los escenarios actuales del país nuestro sistema ayudaría a notificar incidentes como: incendios, riesgos de inundaciones, estado crítico de pacientes, entre otros.
- ✚ La elaboración de nuestro sistema antiextorsión presentó dos prototipos: el primero usando un sistema de transmisión de datos y un sistema de respaldo energético que costó un total de ochenta dólares con diez centavos; y el segundo usando únicamente el sistema de transmisión de datos costando un total de treinta dólares y noventa centavos. Realizar una producción en grandes cantidades reduciría aún más el valor de cada nodo de transmisión, llegando a ser un sistema de fácil adquisición para las comunidades y la población en general.
- ✚ En el mercado de nuestro país, existe una gran variedad de sistemas de seguridad. Sin embargo, esos sistemas incluyen muchas funcionalidades que en nuestro caso no son útiles. Estas funcionalidades encarecen los productos y por ende no son accesibles para los pequeños negocios. La solución propuesta aborda específicamente las necesidades del sector, logrando disminuir costos y a la vez mantener las especificaciones que se necesitan.
- ✚ Las pruebas realizadas demuestran que nuestro sistema es altamente escalable en la ciudad y en los diferentes sectores comerciales, además, la capacidad de adaptar este sistema con aplicaciones de mensajería (Telegram, WhatsApp, X) es una ventaja en cuanto a la versatilidad que posee nuestro sistema antiextorsión.
- ✚ Considerando la crisis energética que atraviesa el país podemos decir que el sistema desarrollado es una buena alternativa para la protección de bienes. Según el análisis

del desempeño del sistema de respaldo energético. El prototipo es capaz de brindar una independencia de 5 horas en el peor de los casos, aumentando esta cifra según se incremente el intervalo de tiempo entre mensajes.

9. Recomendaciones

A partir del desarrollo de este proyecto, se derivan las siguientes recomendaciones:

- ✚ El desempeño del sistema desarrollado se analizó usando tres prototipos y se lo probó en cinco sectores de la ciudad. Para un análisis más detallado se recomienda analizar el funcionamiento del equipo en más sectores de la ciudad.
- ✚ La selección de los componentes en nuestro sistema se realizó en base a criterios de costos y volumen de datos transmitidos. No obstante, en caso de aumentar el tráfico de datos se recomienda mejorar los componentes usados. En ese caso, placas como Raspberry, ASUS Thinker o LePotato son excelentes alternativas.
- ✚ Para reducir las dimensiones del sistema de respaldo energético y en consecuencia el de los prototipos en alrededor de 5cm. Es recomendable utilizar dispositivos de montaje superficial (SMD), debido a que estos elementos poseen un tamaño menor en comparación a la tecnología de agujero pasante (THT).
- ✚ Las tecnologías que se utilizaron en el desarrollo nuestro sistema fueron seleccionadas por la ubicación de las zonas de estudio, en caso de trasladar el sistema a zonas rurales es recomendable investigar las empresas que entreguen cobertura GSM y en caso de tener poca o nula cobertura utilizar sistemas de transmisión de alta penetración como sería la tecnología de LoRa.
- ✚ Al utilizar diferentes aplicaciones durante el desarrollo de este proyecto se demostró que elaborar una aplicación propia mejoraría aún más nuestro sistema. Esto se debe a las capacidades que se tendría como: la lectura del estado de red, mostrar la batería restante o generar estadísticas de alta prioridad. Optimizando la información que entrega el sistema.

10. Bibliografía

- Barthold, C., Pathapati Subbu, K., & Dantu, R. (2011). Evaluation of gyroscope-embedded mobile phones. *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, 1632–1638. <https://doi.org/10.1109/ICSMC.2011.6083905>
- Benson, K., Fracchia, C., Wang, G., Zhu, Q., Almomen, S., Cohn, J., D'Arcy, L., Hoffman, D., Makai, M., Stamatakis, J., & Venkatasubramanian, N. (2015). SCALE: Safe community awareness and alerting leveraging the internet of things. *IEEE Communications Magazine*, 53(12), 27–34. <https://doi.org/10.1109/MCOM.2015.7355581>
- Cabezas Cortéz, J. D., Bajaña Guevara, W. J., & Espol. (2017). *Diseño e implementación de un prototipo de telecontrol de la alarma comunitaria con interfaz web mediante uso de hardware y software libre*. <http://www.dspace.espol.edu.ec/handle/123456789/38862>
- Castillo Imbaquingo, D. X. (2012). *Diseño e implementación de un sistema de alarma comunitaria a base de módulos inalámbricos utilizando tecnología ZIGBEE*. <https://repositorio.utn.edu.ec/handle/123456789/1886>
- Chen, Y. C., & Wang, C. C. (2007). RFID emergency notification system for fall accidents at home. *HEALTHCOM 2007: Ubiquitous Health in Aging Societies - 2007 9th International Conference on e-Health Networking, Application and Services*, 323–326. <https://doi.org/10.1109/HEALTH.2007.381663>
- Chicaiza Guachi, K. G. (2020). *Sistema de alarma comunitaria para el mercado San Juan de la Ciudad de Santiago de Píllaro*. <https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/30709>
- DC DC-Converters – Matt's Electronics. (n.d.). Retrieved September 20, 2024, from <https://www.matts-electronics.com/dcdc-converters/ESP32WROOM32> Datasheet. (2023). <https://www.espressif.com/en/support/download/documents>.
- Fatima, N., Siddiqui, S. A., & Ahmad, A. (2021). IoT based Border Security System using Machine Learning. *ICCISc 2021 - 2021 International Conference on Communication, Control and Information Sciences, Proceedings*. <https://doi.org/10.1109/ICCISC52257.2021.9484934>

- Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics*, 210, 15–26. <https://doi.org/10.1016/J.IJPE.2019.01.004>
- Ghazal, M., Ali, S., Al Halabi, M., Ali, N., & Al Khalil, Y. (2016). Smart mobile-based emergency management and notification system. *Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016*. <https://doi.org/10.1109/W-FiCloud.2016.64>
- Goldwin, I., Gunadhi, A., Lestariningsih, D., Pranjoto, H., Angka, P. R., & Agustine, L. (2024). Fall detection and notification system to fast emergency management for the elderly. *E3S Web of Conferences*, 475, 02014. <https://doi.org/10.1051/E3SCONF/202447502014>
- Gong, D.-H. (2022). IoT notification system for marine emergencies. *International Journal of Internet, Broadcasting and Communication*, 14(1), 122–128. <https://doi.org/10.7236/IJIBC.2022.14.1.122>
- Guest Blog: Wi-Fi, LoRaWAN, and IoT Convergence - Wireless Broadband Alliance*. (n.d.). Retrieved July 27, 2024, from <https://wballiance.com/guest-blog-wi-fi-lorawan-and-iot-convergence/>
- Hyndavi, V., Nikhita, N. S., & Rakesh, S. (2020). *Smart Wearable Device for Women Safety Using IoT*. 459–463. <https://doi.org/10.1109/ICCES48766.2020.9138047>
- Jaiganesh, S., Gunaseelan, K., & Ellappan, V. (2017). IOT agriculture to improve food and farming technology. *2017 Conference on Emerging Devices and Smart Systems, ICEDSS 2017*, 260–266. <https://doi.org/10.1109/ICEDSS.2017.8073690>
- Khan, I. H., & Javaid, M. (2022). Role of Internet of Things (IoT) in Adoption of Industry 4.0. *Journal of Industrial Integration and Management*, 7(4), 515–533. <https://doi.org/10.1142/S2424862221500068/ASSET/IMAGES/LARGE/S2424862221500068FIGF2.JPEG>
- Kurniawan, H., & Hariyanto, S. (2023). Designing Home Security With Esp32-Cam and IoT-Based Alarm Notification Using Telegram. *Bit-Tech*, 6(2), 95–102. <https://doi.org/10.32877/BT.V6I2.932>
- Made, G., Desnanjaya, N., Nyoman, I., & Arsana, A. (2021). Home security monitoring system with IoT-based Raspberry Pi I Nyoman Alit Arsana Institut Agama Hindu Negeri Tampung Penyang Palangka Raya Home security monitoring system with IoT-based Raspberry Pi.

- Indonesian Journal of Electrical Engineering and Computer Science*, 22(3), 1295–1302.
<https://doi.org/10.11591/ijeecs.v22.i3.pp1295-1302>
- Majumder, A. J., & Izaguirre, J. A. (2020). A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition. *Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, 1065–1071.
<https://doi.org/10.1109/COMPSAC48688.2020.0-132>
- MAPA INTERACTIVO ECUADOR. (n.d.). Retrieved July 17, 2024, from
<https://www.arcgis.com/apps/View/index.html?appid=e0d96ec9f1ec40979afc8ba7eff55c7c>
- Motlagh, N. H., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of Things (IoT) and the Energy Sector. *Energies* 2020, Vol. 13, Page 494, 13(2), 494.
<https://doi.org/10.3390/EN13020494>
- Nettikadan, D., & Raj, S. (2018). Smart Community Monitoring System using Thingspeak IoT Platform. *Article in International Journal of Applied Engineering Research*, 13, 13402–13408. <http://www.ripublication.com>
- Ortiz Sosa, M. G. (2020). *Desarrollo de una red de sensores inalámbricos utilizando tecnología LoRa para el monitoreo de un sistema*. <http://dspace.ups.edu.ec/handle/123456789/18469>
- Patel, K. K., Patel, S. M., & Scholar, P. G. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Engineering Science and Computing*. <http://ijesc.org/>
- Power-OFF Protection Module Automatic Switching Module UPS Emergency Cut-off Battery Power Supply 12V to 48V Control Board*. (n.d.). Retrieved September 20, 2024, from
<https://www.icstation.com/mobile/power-protection-module-automatic-switching-module-emergency-battery-power-supply-control-board-p-13126.html>
- Quy, V. K., Hau, N. Van, Anh, D. Van, Quy, N. M., Ban, N. T., Lanza, S., Randazzo, G., & Muzirafuti, A. (2022). IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges. *Applied Sciences* 2022, Vol. 12, Page 3396, 12(7), 3396.
<https://doi.org/10.3390/APP12073396>
- Rao, B. N., & Sudheer, R. (2020). Energy Monitoring using IOT. *Proceedings of the 5th International Conference on Inventive Computation Technologies, ICICT 2020*, 868–872.
<https://doi.org/10.1109/ICICT48043.2020.9112426>

- Rifat Yıldız, E., Bitirim, Y., & Bitirim, Y. (2020). A Smart Emergency Notification System for Road Accident, Fire, and Injury Cases. *Journal of Imaging Science and Technology R*, 64(3), 30506–30507. <https://doi.org/10.2352/J.ImagingSci.Technol.2020.64.3.030506>
- Roa Parra, E. F. (2019). *Análisis de seguridad de tecnologías inalámbricas de comunicación basado en radio definida mediante software*. <http://dspace.utpl.edu.ec/jspui/handle/20.500.11962/25117>
- Sabukunze, I. D., Setyohadi, D. B., & Sulistyoningsih, M. (2021). Designing An Iot Based Smart Monitoring and Emergency Alert System for Covid19 Patients. *2021 6th International Conference for Convergence in Technology, I2CT 2021*. <https://doi.org/10.1109/I2CT51068.2021.9418078>
- Salman, L., Salman, S., Jahangirian, S., Abraham, M., German, F., Blair, C., & Krenz, P. (2016). Energy efficient IoT-based smart home. *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*, 526–529. <https://doi.org/10.1109/WF-IOT.2016.7845449>
- Sánchez-Corcuera, R., Nuñ Ez-Marcos, A., Sesma-Solance, J., Bilbao-Jayo, A., Mulero, R., Zulaika, U., Azkune, G., & Almeida, A. (2021). IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. *Smart Cities 2021, Vol. 4, Pages 429-475, 4(2)*, 429–475. <https://doi.org/10.3390/SMARTCITIES4020024>
- SIM800L GSM Module Pinout, Datasheet, Equivalent, Circuit, and Specifications*. (n.d.). Retrieved July 30, 2024, from <https://components101.com/wireless/sim800l-gsm-module-pinout-datasheet-equivalent-circuit-specs>
- Type C BMS 2S 2A 18650 21700 3.7V Lithium Battery Charge Board Step-Up Boost Li-Po Polymer USB C To 8.4V*. (n.d.). Retrieved September 20, 2024, from https://www.adeept.com/li-ion-battery-charger-m-2s2a_p0374.html
- Ur Rehman, S., Khan, S. A., Arif, A., & Khan, U. S. (2021). IoT-based Accident Detection and Emergency Alert System for Motorbikes. *AIMS 2021 - International Conference on Artificial Intelligence and Mechatronics Systems*. <https://doi.org/10.1109/AIMS52415.2021.9466055>
- Wang, Z., Wang, H., Liu, L., Song, W., & Lu, J. (2016). Community alarm system design based on MCU and GSM. *Proceedings of 2015 4th International Conference on Computer Science and Network Technology, ICCSNT 2015*, 859–862. <https://doi.org/10.1109/ICCSNT.2015.7490876>

- White, J., Thompson, C., Turner, H., Dougherty, B., & Schmidt, D. C. (2011). WreckWatch: Automatic traffic accident detection and notification with smartphones. *Mobile Networks and Applications*, 16(3), 285–303. <https://doi.org/10.1007/S11036-011-0304-8>
- Yang, Y., Wang, H., Jiang, R., Guo, X., Cheng, J., & Chen, Y. (2022). A Review of IoT-Enabled Mobile Healthcare: Technologies, Challenges, and Future Trends. *IEEE Internet of Things Journal*, 9(12), 9478–9502. <https://doi.org/10.1109/JIOT.2022.3144400>

11. Anexos

Anexo 1

Código diseñado para en los diferentes prototipos

```
#include <WiFi.h>
#include <HTTPClient.h>
#include <HardwareSerial.h>

// Definiciones para el módulo SIM800L
HardwareSerial SIM800(1); // Utilizamos el puerto serial 1 del ESP32
const int SIM800_RST_PIN = 4; // Pin de reset del SIM800L

// Definiciones de red WiFi
//ZONA LAS PITAS
#define WIFI_SSID "Nettplus Carlos Jimbo" // Nombre de la red WiFi
#define WIFI_PASSWORD "Zero*****@20jm" // Contraseña de la red WiFi
//ZONA TEBAIDA
#define WIFI_SSID "CELERITY_Briled" // Nombre de la red WiFi
#define WIFI_PASSWORD "JCclcb*****mb@435" // Contraseña de la red WiFi
//ZONA UNL
#define WIFI_SSID "Internet_UNL" // Nombre de la red WiFi
#define WIFI_PASSWORD "UNL18*****59WiFi" // Contraseña de la red WiFi
//ZONA PARQUE CENTRAL
#define WIFI_SSID "Velocity-Coopser_Loja" // Nombre de la red WiFi
#define WIFI_PASSWORD "SL1191*****001" // Contraseña de la red WiFi
//ZONA MERCADO MAYORISTA
#define WIFI_SSID "RYGO" // Nombre de la red WiFi
#define WIFI_PASSWORD "1234*****rygo" // Contraseña de la red WiFi

// Definiciones para el bot de Telegram
#define BOT_TOKEN "6534708030:AAFBCBKu-UKBv08BtPT7pYmFS_o_IkpMxsfo" // Token del bot de Telegram
#define CHAT_ID "-4247658582" // ID de chat de Telegram

// Definición del switch
const int SWITCH_PIN = 5; // Pin del switch
bool sendingMessages = false; // Estado de envío de mensajes
unsigned long lastMessageTime = 0; // Último tiempo de envío de mensajes

void setup() {
  // Inicializamos la comunicación serial para depuración
  Serial.begin(115200);

  // Inicializamos la comunicación serial con el SIM800L
  SIM800.begin(9600, SERIAL_8N1, 16, 17); // TX2, RX2

  // Inicializamos el pin de reset
  pinMode(SIM800_RST_PIN, OUTPUT);
  digitalWrite(SIM800_RST_PIN, HIGH);

  // Configuración del switch
  pinMode(SWITCH_PIN, INPUT_PULLUP);
```



```

// Conectamos a la red WiFi
connectWiFi();

// Inicializar el módulo SIM800L
resetSIM800L();
}

void loop() {
// Leer el estado del switch
if (digitalRead(SWITCH_PIN) == LOW) {
  if (!sendingMessages) {
    sendingMessages = true;
    lastMessageTime = 0; // Reiniciar el temporizador de mensajes
  }
} else {
  sendingMessages = false;
}

// Verificar si es tiempo de enviar un mensaje
if (sendingMessages && (millis() - lastMessageTime >= 60000)) { // Enviar mensajes cada 1 minuto
  sendSMS("+593939641374", "Hola Usuario 2, este es un mensaje enviado desde ESP32 con SIM800L!");
  sendTelegramMessage("Hola Usuario 2, este es un mensaje enviado desde ESP32 a través de un bot de Telegram!");
  lastMessageTime = millis(); // Actualizar el tiempo del último mensaje
}
}

void resetSIM800L() {
// Resetear el módulo SIM800L
digitalWrite(SIM800_RST_PIN, LOW);
delay(100);
digitalWrite(SIM800_RST_PIN, HIGH);
delay(3000); // Esperamos a que el módulo se reinicie
}

void sendSMS(String number, String text) {
// Esperamos a que el módulo esté listo
SIM800.println("AT");
delay(1000);

// Configuramos el modo de texto para SMS
SIM800.println("AT+CMGF=1");
delay(1000);

// Indicamos el número al que enviaremos el SMS
SIM800.print("AT+CMGS=\"");
SIM800.print(number);
SIM800.println("\"");
delay(6000);

// Enviamos el texto del SMS
SIM800.println(text);
delay(1000);

// Enviamos el caracter de finalización (Ctrl+Z)
SIM800.write(26);
delay(1000);

// Mostramos el mensaje de confirmación en el monitor serial
Serial.println("SMS enviado!");
}

void connectWiFi() {
// Conectar a la red WiFi
Serial.print("Conectando a ");
Serial.println(WIFI_SSID);

WiFi.begin(WIFI_SSID, WIFI_PASSWORD);

// Esperar hasta que se establezca la conexión

```

```

while (WiFi.status() != WL_CONNECTED) {
  delay(1000);
  Serial.print(".");
}

// Conexión establecida, mostrar detalles
Serial.println("");
Serial.println("WiFi conectado");
Serial.println("Dirección IP: ");
Serial.println(WiFi.localIP());
}

void sendTelegramMessage(String text) {
  // Enviar mensaje a Telegram si está conectado a WiFi
  if (WiFi.status() == WL_CONNECTED) {
    HTTPClient http;
    String url = "https://api.telegram.org/bot" + String(BOT_TOKEN) + "/sendMessage?chat_id=" + String(CHAT_ID) + "&text=" +
text;

    http.begin(url);
    int httpCode = http.GET();

    // Verificar el código de respuesta HTTP
    if (httpCode > 0) {
      String payload = http.getString();
      Serial.println("Respuesta de Telegram: ");
      Serial.println(payload);
    } else {
      Serial.println("Error al enviar el mensaje a Telegram");
    }

    http.end();
  } else {
    Serial.println("WiFi no conectado");
  }
}

```

Anexo 2
Interfaz de la aplicación WDSservice



Anexo 3

Certificado de traducción del resumen



UNL

Universidad
Nacional
de Loja

Loja, 30 de julio de 2024

Ph.D.

MARCIA ILIANA CRIOLLO VARGAS

**DOCENTE DE LA CARRERA DE PEDAGOGÍA DE LOS IDIOMAS
NACIONALES Y EXTRANJEROS- UNL**

C E R T I F I C O:

Que el resumen del Trabajo de Integración Curricular denominado "Sistema de seguridad comunitaria antiextorsión utilizando sistemas embebidos en el casco urbano de la ciudad de Loja", de la autoría de Carlos Daniel Briceño Ledesma, con cédula de identidad 1150197303, de la Carrera de Ingeniería en Telecomunicaciones; ha sido traducido al inglés y aprobado por mi persona en calidad de profesional especialista en idioma extranjero.



MARCIA ILIANA
CRIOLLO VARGAS

Marcia Iliana Criollo Vargas, Ph.D.

**DOCENTE DE LA CARRERA DE PEDAGOGÍA DE LOS IDIOMAS
NACIONALES Y EXTRANJEROS-UNL**