UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

”DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE ALARMA DE INTRUSIÓN BASADO EN EL PROTOCOLO ESP-NOW DE INTERNET DE LAS COSAS”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

RUIZ SANDOVAL, JULIAN ANTONIO

Villa El Salvador

2020

DEDICATORIA

A mi familia por ser fuente inagotable de inspiración y motivación para afrontar los retos de la vida. De manera especial a mis padres Máximo y Haydeé y a mi hermana Mónica por sus consejos, infinito cariño y apoyo a lo largo de mi vida personal y universitaria.

AGRADECIMIENTO

Agradezco a Dios por brindarme la vida y la dicha de poder seguir mis sueños. A mi familia por apoyarme y no dejar que me rinda ante las dificultades. A mis verdaderos amigos por darme ánimos y palabras de aliento. A mi universidad por ser el lugar donde empecé mi vida profesional y he tenido gratos recuerdos que me acompañarán por el resto de mi vida.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

El internet de las cosas o mejor conocido por sus siglas en inglés (IoT) es una de las tecnologías de mayor auge a nivel mundial, debido a su gran versatilidad y múltiples usos. Uno de ellos es el desarrollo de prototipos para seguridad electrónica.

El objetivo a lograr con el desarrollo del sistema propuesto es brindar una alternativa de sistema de seguridad de bajo costo para hogares que no cuenten con un poder adquisitivo elevado. Cubriendo de esta manera la necesidad de seguridad en el hogar manteniendo la calidad de los sistemas comercializados en el mercado actual.

Para realizar la validación del sistema se usó de referencia la velocidad de respuesta de los nodos sensores y la central comunicadora. Los resultados obtenidos demuestran que el prototipo es totalmente funcional y no se presentaron pérdidas de información en el universo de pruebas realizadas.

Se pueden obtener resultados más favorables haciendo uso de procesos de ensamblaje de tarjetas electrónicas de precisión y con componentes superficiales que ocupen menor espacio. De esa manera lograr aminorar aún más los costos.

Palabras clave: IoT, Seguridad electrónica

INTRODUCCIÓN

PRESENTACIÓN

El presente trabajo cuyo nombre es ”Diseño e implementación de un sistema de alarma de intrusión basado en el protocolo ESP-NOW de internet de las cosas” detalla una alternativa de menor costo en contraste con sistemas de alarma de intrusión comerciales sin perder la efectividad y rendimiento. El sistema está compuesto de sensores electrónicos instalados en los puntos más vulnerables de una casa. La comunicación se realizará a través del protocolo ESP-NOW el cual es propiedad del fabricante ESPRESSIF. La comunicación con el usuario final se realiza vía una aplicación de mensajería instantánea llamada Telegram.

PLANTEAMIENTO DEL PROBLEMA

En los últimos años, las tasas e indicadores de seguridad ciudadana nos han mostrado cifras realmente alarmantes respecto a la cantidad de incidencias reportadas (INEI, 2020a). Ante ello las personas optan por recurrir a diversas maneras de cubrir la necesidad básica de seguridad en sus viviendas; de esta manera proteger sus bienes materiales y el bienestar de sus familias. Esto, debido a que muchas organizaciones criminales y/o delincuentes recurren a maneras violentas para lograr sus objetivos. Muchas instituciones de índole privada y estatal se dedican día tras día a intentar aplacar o disminuir los daños tanto materiales como psicológicos que ocasiona un robo. Sin embargo, el trabajo realizado no es suficiente por la gran cantidad de personas que son víctimas a diario de actos delincuenciales en sus viviendas. Esto sumado al poco resguardo policial que es percibido por la población y recopilado por el Instituto Nacional de Estadística e Informática (INEI, 2020a). La incidencia de delitos contra el patrimonio a nivel nacional se ha incrementado considerablemente a lo largo de los últimos años. Llegando al punto que el 85,7 %(INEI, 2020a) de la población nacional tiene la percepción de que sufrirá un robo. Esto se puede verificar en la Figura 1, donde el 11.9 %(INEI, 2020a) de las viviendas en el primer semestre del año 2020 sufrieron robo o un intento de robo. Esta cantidad

si se extrapola al espacio geográfico de la provincia de Lima, nos daría una cifra aproximada de 1,151,295.84 personas que han sufrido intrusiones a sus viviendas.

Semestre móvil	Robo o intento de robo en la vivienda			Robo en la vivienda			Intento de robo en la vivienda		
	Nacional urbano	Ciudades de 20 mil a más habitantes	Centros poblados urbanos entre 2 mil y menos de 20 mil habitantes	Nacional urbano	Ciudades de 20 mil a más habitantes	Centros poblados urbanos entre 2 mil y menos de 20 mil habitantes	Nacional urbano	Ciudades de 20 mil a más habitantes	Centros poblados urbanos entre 2 mil y menos de 20 mil habitantes
Indicadores semestrales									
Dic 2018 - May 2019	9,4	9,1	10,0	4,6	4,0	6,0	5,2	5,6	4,4
Ene 2019 - Jun 2019	9,6	9,3	10,3	4,6	3,9	6,3	5,4	5,7	4,6
Feb 2019 - Jul 2019	9,4	9,2	10,1	4,6	3,9	6,1	5,3	5,6	4,5
Mar 2019 - Ago 2019	9,5	9,5	9,5	4,5	4,0	5,7	5,3	5,8	4,2
Abr 2019 - Sep 2019	9,4	9,3	9,4	4,4	3,8	5,8	5,3	5,7	4,2
May 2019 - Oct 2019	9,7	9,6	10,1	4,6	3,9	6,2	5,5	5,9	4,5
Jun 2019 - Nov 2019	9,7	9,8	9,5	4,4	4,0	5,5	5,6	6,1	4,4
Jul 2019 - Dic 2019	9,3	9,3	9,5	4,4	3,9	5,4	5,3	5,6	4,4
Ago 2019 - Ene 2020	9,7	9,8	9,5	4,5	4,2	5,3	5,5	5,9	4,6
Sep 2019 - Feb 2020	10,1	10,1	10,0	4,8	4,4	5,6	5,7	6,1	4,8
Oct 2019 - Mar 2020	10,4	10,5	10,1	4,9	4,7	5,5	5,9	6,2	5,0
Nov 2019 - Abr 2020	10,9	10,9	11,0	5,0	4,7	5,7	6,3	6,5	5,9
Dic 2019 - May 2020	11,5	11,1	12,3	5,2	5,0	5,8	6,7	6,5	7,2
Ene 2020 - Jun 2020	11,9	11,6	12,7	5,3	5,1	5,9	7,0	6,8	7,6

Figura 1. Análisis de inseguridad enero-junio 2020
Fuente:https://www.inei.gob.pe/media/MenuRecursivo/boletines/boletin-de-seguridad-ciudadana.pdf

JUSTIFICACIÓN

Ante la situación de aumento de indicadores de agravios contra el patrimonio, la población está viendo con mayor énfasis la idea de optar por una opción de protección para sus hogares. Existen diversas alternativas en el mercado peruano tales como Prosegur y Verisure. Estas empresas ofrecen planes en la modalidad de suscripción orientados para diferentes espacios o ambientes entre los cuales se encuentran las viviendas o espacios residenciales. Las empresas con mayor tiempo en el mercado tales como las mencionadas Prosegur y Verisure cuentan con una amplia gama de productos y personal de operación que brindan servicios de promoción e instalación de sus productos. Estas son las razones por las que sus costes sean elevados en el sentido que no pueden ser adquiridos muy fácilmente por personas que no cuenten con un poder adquisitivo elevado o acorde al servicio a contratar. Las viviendas con un estándar de ingresos moderado no logran en la mayoría de los casos cubrir los costos mensuales que empresas del rubro de la seguridad cobran por brindar el soporte a sus equipos. Esto resulta contraproducente y de alto impacto en los indicadores de criminalidad. En consecuencia se refleja la carencia de sistemas de seguridad y en específico sistemas de seguridad electrónica en las viviendas.

La Tabla 1 muestra la información recopilada por el Instituto Nacional de Estadística e Informática (INEI) respecto a la cantidad de ingresos promedios obtenidos del trabajo por la población dentro del área de Lima metropolitana. De ello se logra denotar una cifra de S/.1562.7(INEI, 2020b). Se puede inferir que existe un ingreso promedio por familia que es el suficiente para poder costear el sistema de seguridad propuesto. Dado que está pensado principalmente para hogares de medianos ingresos debido a su bajo costo. Se puede concluir además que el ingreso promedio del año 2020 en comparativa con el trimestre junio-julio-agosto del año 2019 fue un 9 %(INEI, 2020b) menor. Lo que implica que las personas tengan un menor poder adquisitivo.

Tabla 1
Ingresos promedios provenientes del trabajo en Lima Metropolitana

Sexo/Grupos de edad	Jun-Jul-Ago 2019	Jun-Jul-Ago 2020	Variación	
			Absoluta (Soles)	Porcentual (%)
Total	1717.1	1562.7	-154.4	-9.0
Sexo				
Hombre	1963.9	1694.8	-269.1	-13.7
Mujer	1419.4	1391.3	-28.1	-2.0
Grupos de edad				
De 14 a 24 años	1038.4	961.0	-77.4	-7.5
De 25 a 44 años	1082.9	1511.6	-291.3	-16.2
De 45 a más años	1920.9	1893.8	-27.1	-1.4

Fuente:Elaboración propia, extraído de https://www.inei.gob.pe/media/MenuRecursivo/boletines/09-informe-tecnico-mercado-laboral-jun-jul-ago-2020.pdf

Existen alternativas de alarmas en el mercado que pueden ser adquiridas en tiendas por departamento que brindan una alternativa de único pago. Sin embargo el precio de las mismas sigue siendo elevado para el promedio de ingresos. Ante lo anteriormente expuesto surge la necesidad de desarrollar el prototipo de sistema de alarma de intrusión. El cual utiliza el concepto del internet de las cosas (objetos conectados a la internet con capacidad de interacción) como principio para su funcionamiento y despliegue. El prototipo planteado en el presente trabajo provee de interacción al usuario final brindándole la experiencia de estar utilizando un sistema de alarma comercial.

El presente trabajo está centrado en el concepto de seguridad ciudadana (Mujica y Zevallos, 2016), haciendo énfasis en la seguridad en el hogar. Con la finalidad de proteger la integridad de las personas que yacen en el interior de la vivienda como espacio físico. Además de ello asegurar la no vulnerabilidad de los bienes materiales protegiéndolos de robos y agravios por parte de terceros.

OBJETIVOS

Objetivo General

Brindar una alternativa de sistema de alarma de intrusión de hardware y software libre para el hogar; funcionalmente viable que cuente con capas de seguridad, de bajo costo y consumo energético, que sea de fácil uso e instalación para su aplicación en hogares del distrito de Villa el Salvador y distritos cercanos.

Objetivos Específicos

- Diseñar y dimensionar un sistema de seguridad utilizando componentes de fácil adquisición en el mercado, de bajo costo y consumo de batería para lograr prolongar la vida útil del sistema.
- Implementar una red de sensores independiente de una red local de comunicación inalámbrica con funcionalidad de alerta inmediata al sistema de alarma de intrusión, manteniendo un estándar de seguridad en la transferencia de información y haciendo uso de un servicio de mensajería instantánea funcional alrededor del mundo.
- Validar el sistema de seguridad, verificando funcionalidad y análisis de coste.

CAPITULO I: MARCO TEÓRICO

1.1. Introducción

En el presente capítulo se analizarán los conceptos generales de internet de las cosas(IoT), normatividad de frecuencias y seguridad. Se analizarán también los diversos componentes de hardware que existen en el mercado para desarrollos IoT. Se realizará un balance entre sistemas de alarma de seguridad comerciales.

1.2. Normatividad del MTC

Es de necesidad pública tener una distribución adecuada del espacio radioléctrico para los diversos servicios que son ofrecidos por los operadores de telecomunicaciones en el Perú. Ante ello y en base al análisis desarrollado por el MTC(Ministerio de Transportes y Telecomunicaciones) se ha formulado un documento detallando la distribución y el uso de las frecuencias a lo largo del espacio geográfico del territorio peruano. El documento en cuestión es denominado Plan Nacional de Atribución de Frecuencias(Ministerio de transportes y comunicaciones, 2008).

Al tratar con dispositivos IoT inalámbricos se hace indispensable realizar un estudio de las tecnologías de transmisión y las diversas normativas que deben de cumplirse para garantizar un óptimo desempeño y cumplimiento de los estándares establecidos. Una de las virtudes primordiales expuestas en la presente propuesta es la de cumplir con ser de libre uso y ello implica el no utilizar bandas de frecuencias licenciadas por entidades privadas o estatales. Para tal caso se hace énfasis en las frecuencias ISM o en español ICM(Industrial, Científico y Médico) las cuales se encuentran detalladas en la Tabla 1.1.

Tabla 1.1
Bandas de frecuencia ICM

Bandas de frecuencia ICM
13 553 – 13 567 kHz (frecuencia central 13 560 kHz)
26 957 – 27 283 kHz (frecuencia central 27 120 kHz)
40,66 – 40,70 MHz (frecuencia central 40,68 MHz)
902 – 928 MHz (frecuencia central 915 MHz)
2 400 – 2 500 MHz (frecuencia central 2 450 MHz)
5 725 – 5 875 MHz (frecuencia central 5 800 MHz)
24 - 24,25 GHz (frecuencia central 24,125 GHz)

Fuente:Elaboración propia, extraído de https://portal.mtc.gob.pe/comunicaciones/autorizaciones/servicios_privados/documentos/pnaf_act_feb08.pdf

En el Perú aún no se cuenta con una normativa específica para el despliegue de dispositivos IoT; por tal motivo se debe de cumplir con los estándares planteados por las instituciones pertinentes. Existen disposiciones y condiciones para los equipos que hagan uso de las frecuencias ICM propuestas por intermedio del MTC en la resolución ministerial N° 199-2013-MTC/03(Ministerio de transportes y comunicaciones, 2013), las cuales se especifican en la Tabla 1.2.

Tabla 1.2
Normatividad de frecuencias libres según MTC

Banda de frecuencias	Potencia de salida del transmisor			Ganancia máxima de la antena	PIRE máxima
(MHz)	**(W)**	**(mW)**	**(dBm)**	**(Dbi)**	**(dBm)**
916-928	1	1000	30	6	36
2400-2483.5	0.5	500	27	9	36
5725-5850	0.25	250	24	12	36
5250-5350	0.25	250	24	6	30
5470-5725	0.125	125	21	9	30

Fuente:Elaboración propia, extraído de https://portal.mtc.gob.pe/comunicaciones/autorizaciones/servicios_privados/documentos/pnaf_act_feb08.pdf

La norma expone que para los equipos que hagan uso de las bandas de frecuencia 916-928 MHz, 2400 – 2483,5 MHz y 5725 – 5850 MHz están libre de restricciones siempre y cuando su PIRE máxima no exceda los 36dBm.

1.3. Internet de las cosas

El internet de las cosas o IoT(Internet of Things) por sus siglas en inglés es un concepto usado por primera vez en el año 1999 por Kevin Ashton informático del MIT(Massachusetts Institute of Technology). El mismo hace referencia a objetos o cosas como tal, dotados de diversos elementos de hardware y software que le brindan la capacidad de recopilar información del exterior y llevar dichos datos a la Internet. Para que posteriormente puedan ser almacenados o procesados según sea la necesidad del usuario final. Cabe mencionar que los dispositivos IoT pueden ser actuadores y cumplir determinadas funcionalidades dependiendo de las capacidades con las que hayan sido fabricados.

Los usos y aplicaciones del IoT han ido cambiando con el pasar de los años conforme se iban presentando necesidades o problemáticas nuevas. Entre las aplicaciones más resaltantes en la actualidad tenemos las siguientes:

- **Smart Cities**

  Las ciudades inteligentes hacen uso de dispositivos electrónicos desplegados en el territorio geográfico con la finalidad de hacer más interactivos, inteligentes y eficientes los servicios brindados por el estado.(Telefónica, 2011)

- **Smart Retail**

  La tecnología del dispositivos inteligentes no es ajena al sector del consumo en tiendas por departamento. En la actualidad ciertos locales poseen tecnología de ayuda al consumidor a través de pantallas informativas e interactivas que brindan apoyo al momento de hacer la elección de los productos.(Pantano y Timmermans, 2014)

- **Agro Smart**

  La agricultura se ha tecnificado con el pasar de lo años lo cual no es ajeno al IoT. Se logra definir también como la mecanización de procedimientos agrícolas para mejorar la productividad y rendimiento de los procesos. Se han desarrollado prototipos con la capacidad de recopilar y enviar datos como: humedad del suelo, temperatura, etc. Esto hace que la persona encargada de

los cultivos esté al tanto del estado actual del suelo y si presenta condiciones favorables o no para poder trabajar.(PMG Bussines Improvement, 2016)

1.3.1. Arquitectura IoT

Los diferentes fabricantes de tecnología IoT en el mundo dentro de los cuales se pueden nombrar marcas de relevancia mundial como son: Cisco, IBM, Microsoft, etc. Han realizado diversos planteamientos de la arquitectura de sus servicios ajustándolos a las necesidades del consumidor. Se puede simplificar la arquitectura de un servicio IoT de la siguiente manera: nodos, redes de comunicación y la nube de datos.

1.3.2. Nube de datos

Hace referencia al despliegue de tareas y servicios alojados en computadoras o servidores ubicados en centros de datos a los cuales se puede acceder de manera remota y cuyo soporte es brindado por el proveedor de dicho servicio. La nube de datos brinda la posibilidad de almacenar, procesar y hasta analizar los datos obtenidos a manera de analítica. Ofrece la facilidad al usuario de tener el control de sus aplicaciones sin correr el riesgo de caídas de fluido eléctrico o alguna alteración externa. Estos servicios son brindados a cambio de una membresía que puede ser anual o mensual dependiendo del proveedor. La tecnología de la nube de datos permite el acceso a los datos y servicios montados desde cualquier lugar del mundo que cuente con conexión a internet.(Camps Sinisterra y Oriol Allende, 2012)

Algunos ejemplos de la nube de datos son:

- **Amazon**

  Amazon es el pionero de la computación en la nube. Como un modelo de negocio nuevo surgió Amazon Web Services. El cual provee a los usuarios el alquiler de espacios en sus centros de datos para diversas funciones. Entre los servicios que provee resaltan Elastic Compute Cloud(EC2) y Simple Storage Services(S3). Actualmente Amazon Web Services(AWS) también brinda servicios en la nube de datos para el uso y desarrollo de aplicaciones de inteligencia artificial.

- **Microsoft**

  De manera similar a Amazon, Microsoft apostó por brindar servicios de computación en la nube. El servicio se denominó Microsoft Azure el cual brinda espacios de almacenamiento en los centros de datos de Microsoft para diversos servicios. Una de las principales apuestas de Microsoft para la computación en la nube al igual que Azure es la migración de los aplicativos Office.

- **Google**

  Google apuesta por la tecnología de la nube para múltiples servicios y aplicaciones. Algunos ejemplos son: Google Drive y Google Cloud. Por otro lado Google también apuesta por el desarrollo de la inteligencia artificial proporcionando una plataforma que brinda espacios para el desarrollo de algoritmos complejos. La plataforma anteriormente mencionada es denominada Google Colaboratory.

1.3.3. Hardware IoT

En el mercado existen diversas alternativas para el diseño de hardware IoT entre las más comerciales, masivas y de fácil uso podemos nombrar al Arduino como una de las principales tarjetas de desarrollo. Así como también se puede mencionar el ESP8266 con su mejora el ESP32 y el Raspberry Pi en sus diferentes versiones.

Arduino

Es una tarjeta de desarrollo de hardware libre que está formado en su núcleo central con un microcontrolador ATMEGA que irá variando dependiendo del modelo que se tenga.(Herrador, 2009)

Entre las características más relevantes tenemos:

- **Hardware libre**
  Los diagramas para el ensamblado de una tarjeta Arduino son completamente libres.
- **Software libre**
  Se tiene la libertad de modificar y mejorar el código para ajustarlo a las necesidades que se presenten.
- **Mutiplataforma**
  La interfaz de programación Arduino IDE es multiplataforma lo que significa que puede ser instalada en los sistemas operativos más utilizados, los cuales son: Windows, MAC OS y Linux.

- **Amplia comunidad**

  En la red se pueden hallar muchos foros y blogs especializados en Arduino, los cuales comparten sus desarrollos y despejan de dudas a los desarrolladores novatos.

Existen diversos modelos de la tarjeta Arduino, los cuales difieren en la cantidad de pines, tamaños, funcionalidades y modelo de microcontrolador. Entre los modelos más utilizados tenemos los que se aprecian en la Figura 1.1.

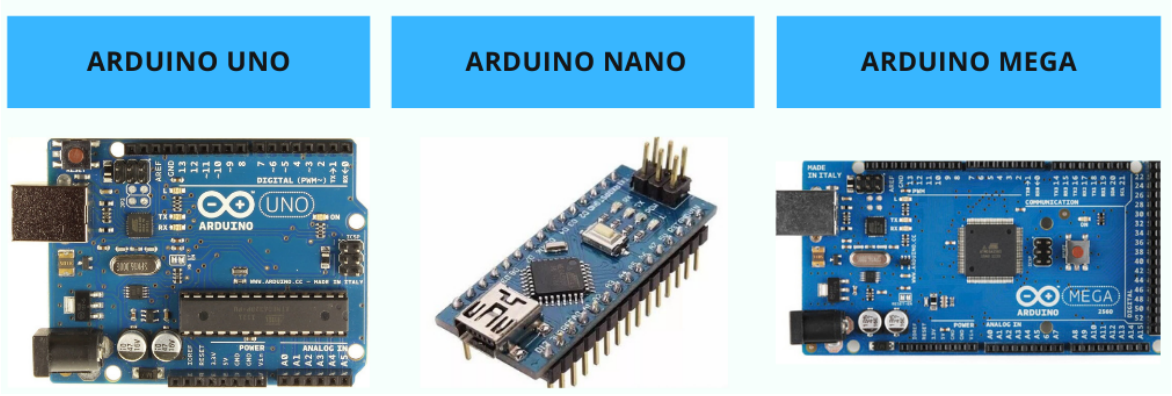


Figura 1.1. Ejemplos de tarjetas de desarrollo Arduino
Fuente: Elaboración propia - Google imágenes

ESP8266

Los módulos ESP8266 son una línea de dispositivos que cuentan con conectividad Wi-Fi lo cual los provee de comunicación inalámbrica. Se pueden adaptar a diversas tarjetas y se encuentran muy fácilmente en el mercado y son de bajo costo. Existen diversas versiones de tarjetas que utilizan el SoC del modelo ESP8266 haciendo más sencilla su adaptación a proyectos. Permiten además validar la funcionalidad de los proyectos para posterior despliegue.

Las tarjetas de desarrollo más utilizadas en el entorno de los desarrolladores IoT es el ESP-01 y el NodeMCU que contiene el SoC del modelo ESP-12. En la Figura 1.2 se puede apreciar un ejemplo de tarjeta NodeMCU. Los ejemplos mencionados tienen la capacidad de ser programados en diversos lenguajes tales como C++, Python y LUA. Dependiendo del firmware utilizado permite incluso interactuar con ellos vía comandos AT.(Valderrama y Brea, 2020)

Figura 1.2. Tarjeta de desarrollo

NodeMCU
Fuente:https://www.amazon.com/nodemcu/s?k=nodemcu

ESP32

El SoC ESP32 es un dispositivo que encapsula la tecnología de conectividad Wi-Fi y Bluetooth BLE. Posee un chip Tensilica Xtensa con un doble núcleo de 32 Bits y una frecuencia de reloj de 240 MHz. Existe diversas familias de módulos que son modificaciones y variantes que parten del SoC del modelo ESP32. La clasificación y uso va a depender de la aplicación para la cual se desee orientar. Esta familia de SoC's son una mejora de las versiones anteriores de chips's de la línea ESP8266. En la Figura 1.3 se muestra un ejemplo de tarjeta que usa el SoC ESP32 denominado módulo ESP-WROOM-32.(FIGUEROA MARÍN, 2020)

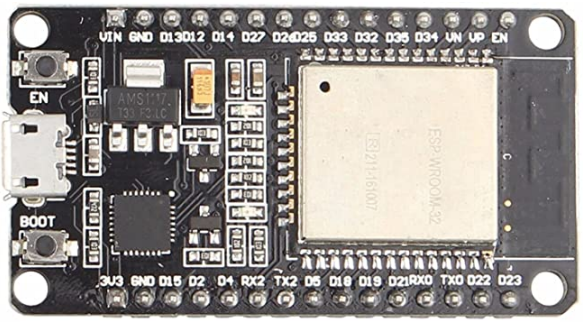


Figura 1.3. Tarjeta basada en

ESP-WROOM-32
Fuente:https://www.amazon.com/ESP32/s?k=ESP32

Raspberry Pi

La tarjeta Raspberry Pi se presenta como una alternativa más completa para el desarrollo de prototipos de IoT. Esto debido a que cuenta con un microprocesador de arquitectura ARM que le da la capacidad de poder soportar un sistema operativo. El sistema operativo por excelencia es Raspbian, una distribución de GNU/Linux basada en Debian. Las tarjetas Raspberry cuentan con pines GPIO para propósitos generales lo cual es provechoso para el despliegue de hardware IoT. Puede ser programado en lenguajes de alto nivel como Python y C++. En la actualidad han salido a la venta diversas versiones de la tarjeta Raspberry como ejemplo de ellas existen: Zero, 3B, 3B+ y la última versión lanzada es la 4B. La Figura 1.4 muestra una Raspberry Pi 3B+ el cual es uno de los modelos de mayor demanda en el mercado.(Salcedo Tovar, 2015)

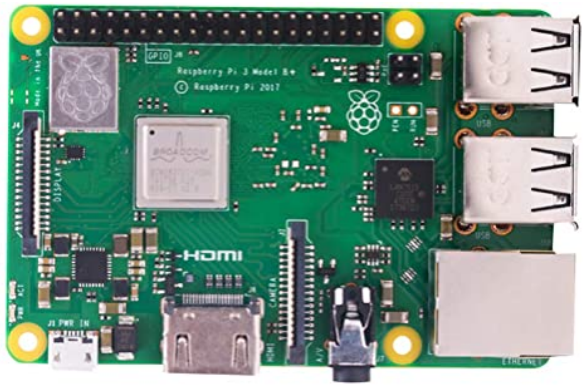


Figura 1.4. Tarjeta Raspberry Pi 3B+
Fuente:https://www.amazon.com/s?k=raspberry+pi

1.4. Protocolos de comunicación usados en IoT

No existe un protocolo único para el internet de las cosas, ello va a depender de la aplicación y los requerimientos de hardware y software del proyecto. A continuación se detallarán algunos de los más utilizados:

- **HTTP**

  Las siglas HTTP significan HyperText Transfer Protocol o en español ”Protocolo de transferencia de hipertexto”. Es el protocolo por excelencia y predominante en la red de datos, es también usado en el despliegue de proyectos de IoT. Es recurrentemente usado en especial cuando se requiere enviar una gran cantidad de datos de tipo imágenes o videos.(Naik, 2017)

- **CoAP**

  El protocolo Constrained Application Protocol o por su siglas en inglés CoAP, hacen referencia al protocolo de aplicación restringido que se maneja bajo un estándar cliente-servidor. Funciona bajo la lógica que el dispositivo cliente logre comunicarse con otro nodo de la misma tecnología vía un servidor CoAP. El cual se encargará de procesar la solicitud de información y permitirla si es el caso.(Naik, 2017)

- **MQTT**

  Las siglas MQTT significan Message Queue Telemetry Transport o en su traducción al español sería ”Transporte de telemetría de cola de mensajes”. Es un protocolo ideado especialmente para nodos sensores y actuadores IoT debido a su bajo consumo de ancho de banda lo que hace que la transferencia de datos sea ligera y rápida a diferencia de otros protocolos. El protocolo MQTT funciona a manera de publicación-suscripción, se pueden tener muchos nodos sensores publicando datos de manera simultánea. Un cliente puede estar suscrito a varios tópicos y recibir información de diversos dispositivos.(Naik, 2017)

En la Tabla 1.3 se apreciarán algunas de las características relevantes de las tecnologías anteriormente mencionadas.

Tabla 1.3
Comparativa de protocolos de comunicación usados en IoT

	HTTP	CoAP	MQTT
Abstracción	Solicitud / respuesta	Publicación / suscripción Solicitud / respuesta	Publicación / suscripción
Protocolo de transmisión	TCP	UDP	TCP
Calidad de servicio	Limitado	-Mensaje confirmado -Mensaje no confirmado	-QoS 1 -QoS 2 -QoS 3
Arquitectura	Cliente - servidor	-Cliente - servidor -Cliente - broker	Cliente - broker
Ventajas	-Es posible transferir gran cantidad de información. -Protocolo estandarizado a nivel mundial.	-Semántica similar a HTTP. -Ideado para dispositivos de baja potencia.	-Protocolo ligero, requiere poco ancho de banda. -Menor consumo de energía.
Desventajas	-Si no se encripta es muy vulnerable. -Lenta transferencia de información.	-Pocas librerías en existencia. -Problemas en NAT.	-Encriptación no definida. -Envío de mensajes cortos.

Fuente:Elaboración propia, extraído de Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP (Naik, 2017)

1.5. Tecnologías inalámbricas utilizadas en IoT

En la actualidad existen múltiples tecnologías inalámbricas para el despliegue de aplicaciones IoT. En el presente apartado se detallarán algunos de los más utilizados.

- **Wi-Fi**

  La tecnología Wi-Fi hace referencia a un estándar de conectividad a internet WLAN que es de uso común en la mayoría de hogares y oficinas de trabajo. La frecuencia en la que trabaja es de 2.4GHz y 5GHz.(INTEL, 2020)

- **LoRa**

  Es una tecnología de transmisión inalámbrica cuyas principales características son su gran alcance y bajo consumo de energía. Es principalmente utilizado para comunicaciones que impliquen largas distancias. LoRa trabaja en frecuencias ICM alrededor del mundo.(Bo True Activities SL, 2020)

- **Sigfox**

  La tecnología Sigfox es denominada red 0G, esto debido a su baja cantidad de transferencia de información. Está diseñada para equipos de bajo consumo energético que permitirá un uso bastante prolongado. Posee una infraestructura de antenas que generan una red independiente de cualquier operador.(Bo True Activities SL, 2020)

- **Bluetooth**

  Es una tecnología de comunicación muy usada en la actualidad para el envío de información de manera inalámbrica. Utiliza la banda libre de 2.4 GHz. Es utilizado en dispositivos de audio inalámbrico tales como parlantes y audífonos. Tiene un rango de distancia promedio de unos 10 m.(Wim Hoogenraad, 2018)

- **Zigbee**

  Es una tecnología usada en trabajos y proyectos de comunicaciones inalámbricas industriales como uno de sus campos aplicativos. Una aplicación de Zigbee también es la domótica debido a su bajo coste y altas prestaciones.

Hace uso de la banda libre ISM 2.4 GHz, 868 MHz en Europa y 915 MHz en los Estados Unidos.(Gordon Colbach, 2013)

En la Tabla 1.4 se puede apreciar una comparación entre las principales características de las tecnologías mencionadas.

Tabla 1.4
Comparativa entre tecnologías inalámbricas para IoT

	Wi-Fi (802.11)	**LoRa**	**Sigfox**	**Bluetooth**	**Zigbee**
Frecuencia	-2.4 GHz - 5 GHz	- 433 MHz - 868 MHz - 780 MHz - 915 MHz	- 868 MHz - 962 MHz	- 2.4 GHz	- 2.4 GHz
Rango de distancia	100 m	3 - 10 Km	2 - 5 Km	10 m	10 - 75 m
Velocidad de transferencia de datos	- b 11 Mbps - g 54 Mbps - n 72.2 Mbps	50 Kbps	100 bps	721 Kbps	20-250 Kbps
Ventajas	- Alta compatibilidad con múltiples dispositivos.	- Alta tolerancia contra interferencias.	- Gran conectividad a nivel mundial.	- Fácil vinculación de equipos.	- Opera en una banda libre.
Desventajas	- Consumo relativamente alto de energía.	- No provee datos en tiempo real.	- Transporta solo 12 bytes de datos.	- Menor nivel de seguridad.	- Baja tasa de transferencia.

Fuente:Elaboración propia, extraído de https://www.intel.la/content/www/xl/es/support/articles/000005725/network-and-i-o/wireless.html. Extraído de https://botrueactivities.com/comparativa-entre-sigfox-y-lorawan/. Extraído de https://es.itpedia.nl/2018/07/12/wifi-en-bluetooth-wat-is-het-verschil. Extraído de https://www.ecured.cu/ZigBee

1.6. Protocolo ESP-NOW

ESP-NOW es un tipo de protocolo derivado de la tecnología de comunicación inalámbrica Wi-Fi. Es propiedad de la marca ESPRESSIF, fabricante y distribuidora de los SoC's ESP32. Este protocolo tiene como característica la de crear una comunicación entre dispositivos sin contar con una conexión a una red Wi-Fi. La transferencia entre dispositivos se realiza previo emparejamiento usando las direcciones MAC. Una de las ventajas es la de persistir con el emparejamiento en caso los dispositivos se queden sin energía. Esto quiere decir que puede retomar su comunicación una vez que se energice nuevamente o supere el inconveniente que presente.

La velocidad de transferencia del protocolo ESP-NOW es 1 Mbps y permite una carga útil de datos de 250 Bytes por transferencia. En la Figura 1.5 se expone la trama utilizada para transferir datos utilizando ESP-NOW.(ESPRESSIF, 2016)

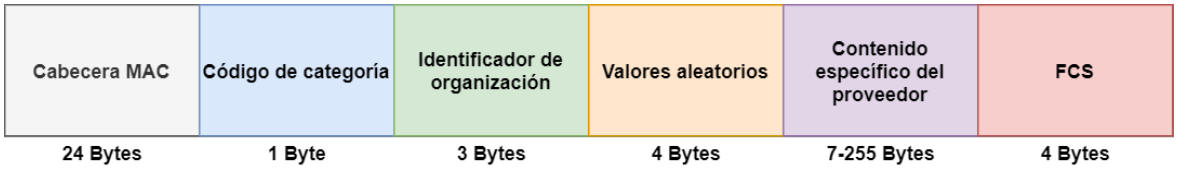


Figura 1.5. Trama utilizada en ESP-NOW
Fuente: Elaboración propia, extraído de: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/network/esp_now.html

- La **cabecera MAC** es diferente a las tramas convencionales debido a que el protocolo ESP-NOW no hace uso de una conexión Wi-Fi.
- El **código de categoría** es seteado en el único valor de 127 por el fabricante ESPRESSIF.
- El **identificador de organización** está determinado por los 3 primeros Bytes de las direcciones MAC otorgadas al fabricante ESPRESSIF para la distribución de sus productos.
- Los **valores aleatorios** son usados como mecanismos de seguridad para evitar ataques de retransmisión.

- El **contenido específico del proveedor** cuenta con un mínimo de 7 Bytes especificados por el fabricante,los cuales son: ID del elemento, longitud, identificador de organización, tipo y versión. Los parámetros anteriormente mencionados se acompañan de 250 Bytes libres para la carga útil que se resume en el contenido a ser transmitido.

- El **FCS** o en su traducción a español secuencia de verificación de trama, es de utilidad para aseverar una correcta transmisión de la trama.

Las características más relevantes del protocolo ESP-NOW son detalladas a continuación:

- Permite el emparejamiento de hasta 20 pares y 10 de ellos cifrados.

- Permite una transferencia de hasta 250 Bytes de información.

- Conexión rápida.

- Compatible con la tecnología de cifrado CCMP.

Existen diversas configuraciones para la transferencia de información entre dispostivos que usen el protocolo ESP-NOW, de manera direccional o bidireccional. La conexión unidireccional se aprecia en la Figura 1.6 y en la Figura 1.7 la comunicación unidireccional múltiple.

Figura 1.6. ESP-NOW unidireccional
Fuente: Elaboración propia, adaptado de https://randomnerdtutorials.com/esp-now-esp32-arduino-ide/

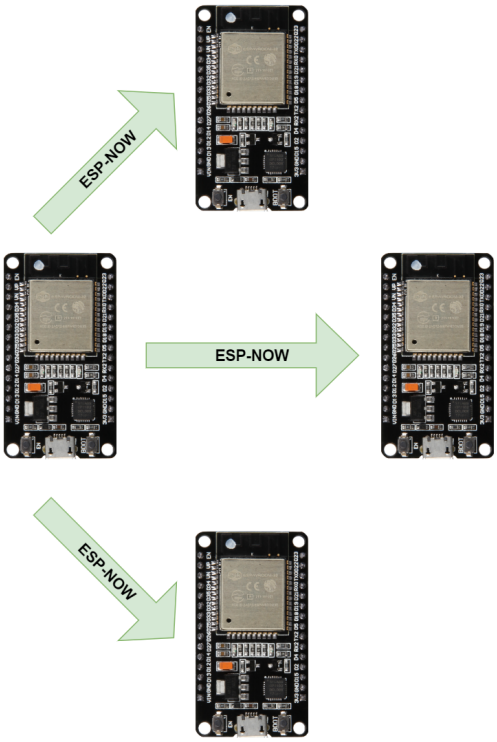


Figura 1.7. ESP-NOW unidireccional múltiple 1
Fuente: Elaboración propia, adaptado de https://randomnerdtutorials.com/esp-now-esp32-arduino-ide/

Otra variante de la comunicación unidireccional es la del envío de información de múltiples dispositivos a uno solo. En la Figura 1.8 se aprecia una boceto de dicha configuración.

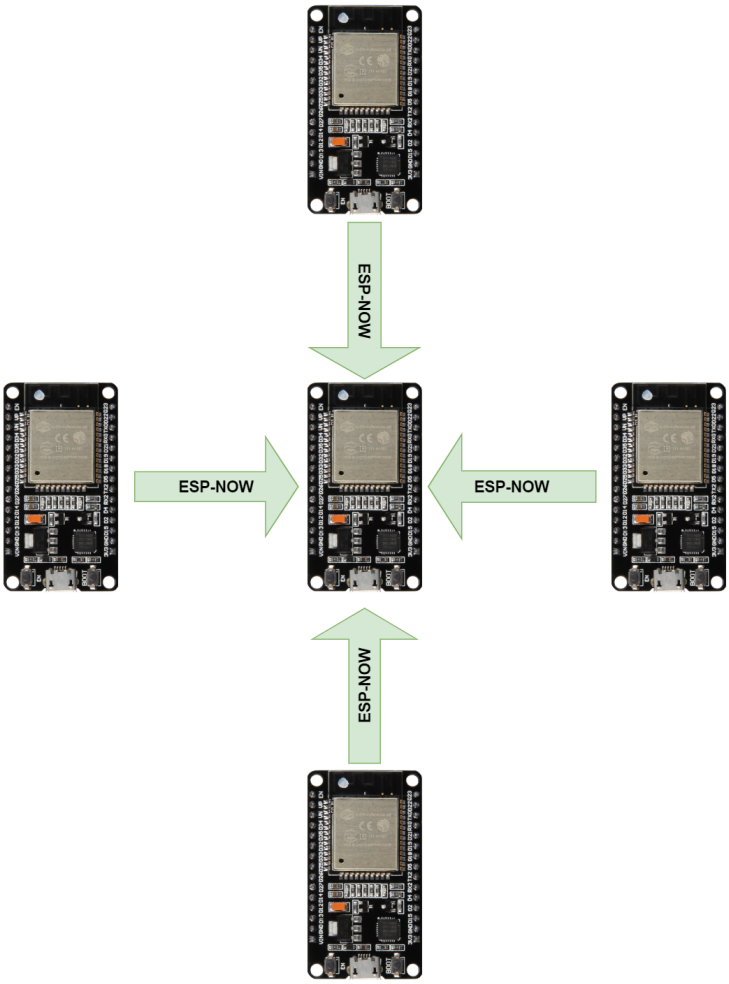


Figura 1.8. ESP-NOW unidireccional múltiple 2
Fuente: Elaboración propia, adaptado de https://randomnerdtutorials.com/esp-now-esp32-arduino-ide/

Es de uso también la configuración bidireccional que implica una comunicación entre 2 o más dispositivos. En la Figura 1.9 se aprecia la comunicación bidireccional simple entre 2 dispositivos; por otro lado en la Figura 1.10 se aprecia la configuración bidireccional múltiple que implica que diversos dispositivos intercambien información con uno solo.

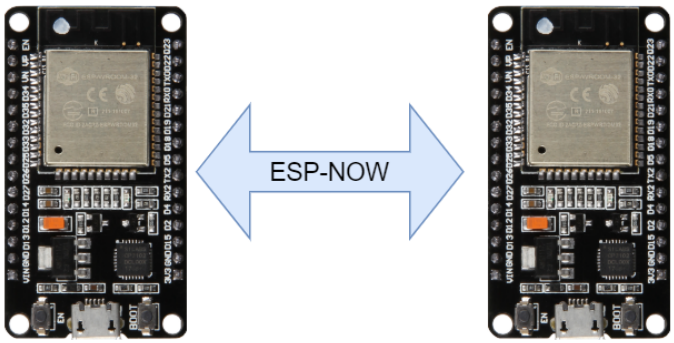


Figura 1.9. ESP-NOW bidireccional

Fuente: Elaboración propia, adaptado de https://randomnerdtutorials.com/esp-now-esp32-arduino-ide/

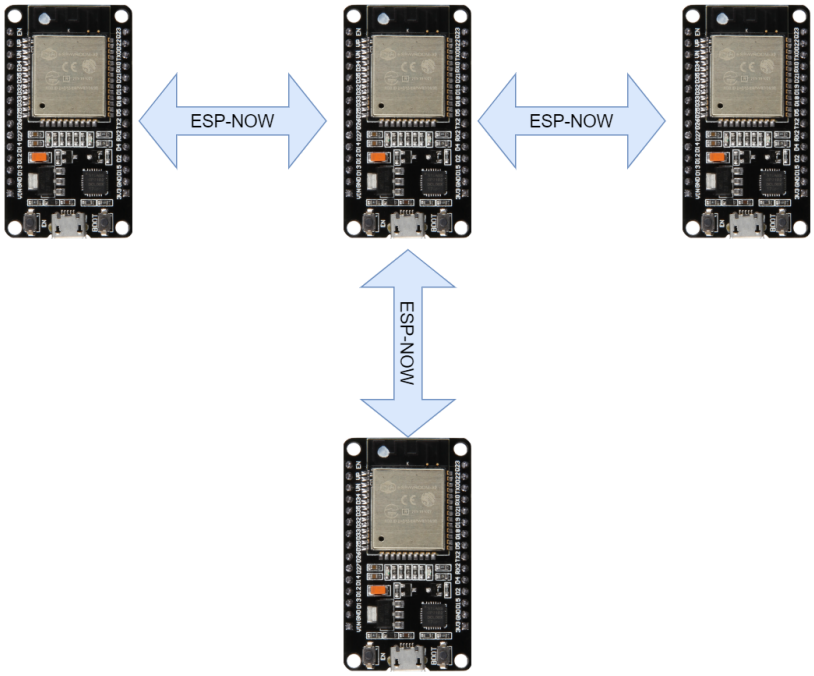


Figura 1.10. ESP-NOW bidireccional múltiple 1

Fuente: Elaboración propia, adaptado de https://randomnerdtutorials.com/esp-now-esp32-arduino-ide/

El protocolo ESP-NOW permite la comunicación entre todos los dispositivos emparejados en su red, siendo esta la configuración de mayor complejidad y de manera más completa para aplicaciones como la domótica. Se denominará descentralizada para efectos descriptivos en el presente trabajo. Un ejemplo de esta configuración es descrita en la Figura 1.11.

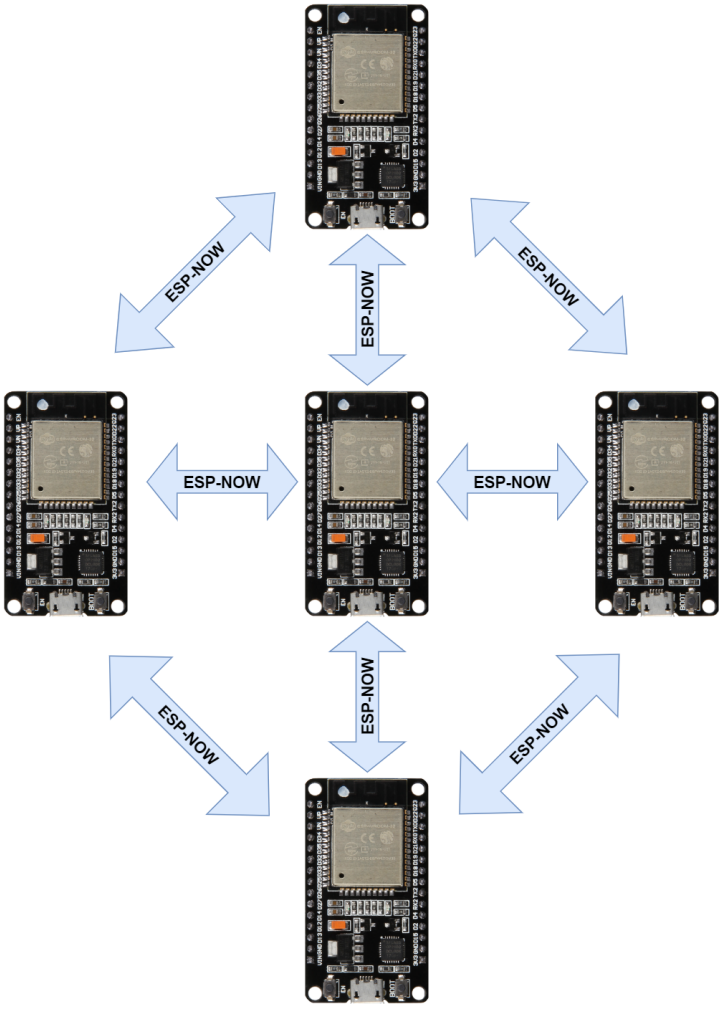


Figura 1.11. ESP-NOW bidireccional múltiple 2
Fuente: Elaboración propia, adaptado de https://randomnerdtutorials.com/esp-now-esp32-arduino-ide/

1.7. Teoría de la seguridad

1.7.1. Conceptos

El concepto general de seguridad hace referencia al sentir del ser humano de poseer y experimentar una sensación de bienestar y protección en contra de las amenazas externas que puedan perturbar su espacio personal o entorno en general.

Seguridad ciudadana

La seguridad ciudadana parte de la premisa inicial de seguridad humana (Mujica y Zevallos, 2016). Es además necesaria para el desarrollo en conjunto de la población y protege que los derechos de la misma no sean vulnerados. Todo ello con la finalidad de establecer un estado de convivencia pacífica y fortalecer lazos de solidaridad y bienestar común.

Robo y hurto

La diferencia entre robo y hurto yace medularmente en el modo de perpetuar el acto. Es importante conocer los términos debido a que para cuestiones legales y contractuales no son asumidos de igual manera.

El **robo** es definido por el código penal peruano en el artículo 188º como la apropiación ilegítima de bienes materiales haciendo uso de la violencia y poniendo en riesgo el bienestar de la víctima (Penal, 2015).

El **hurto** es aquella actividad comprendida en el marco del código penal peruano en su artículo 185º y definida por el mismo como la acción de sustraer un bien mueble de su lugar legítimo (Penal, 2015). Cabe mencionar además que el hurto no comprende el uso de la violencia.

Sistemas de alarma

El sistema de alarma se puede definir como aquel dispositivo o conjunto de dispositivos que notifican al usuario sobre algún evento irregular que pueda presentarse y que atente contra sus bienes personales. Es catalogado como pasivo debido

a que no cuentan con la capacidad de impedir que se concrete un evento negativo; sin embargo pueden proveer de mecanismos actuadores capaces de producir luces intermitentes o activar sirenas con la finalidad de advertir que se está presentando una alerta.

Sistemas de alarma electrónicos

Es aquel sistema de alarma que involucra componentes electrónicos, tales como sensores y actuadores que proveen de tecnología a un sistema clásico. Con la finalidad de dotarlo de autonomía y que funcione independientemente de la intervención del ser humano. Con el avance de la tecnología se han presentado modificaciones y mejoras al momento de enviar las alertas al usuario utilizando protocolos de comunicaciones tales como IP y GSM/GPRS en su mayoría. Los sistemas de alarma electrónicos se catalogan acorde a su finalidad y el lugar en el que serán instalados.

Existen sistemas de alarma electrónicos de diverso uso e implementación así como de instalación. A continuación se detallarán los tipos de sistemas de alarma electrónicos más utilizados:

- **Sistema de alarma contra incendios**

  Son aquellos sistemas que están enfocados en detectar y alertar al usuario de la existencia de un incendio antes de su proliferación y evitar de esta manera que genere daños mayores. Además envía notificaciones a los dispositivos a los que esté vinculado para avisar que se está presentando un evento. Cuentan también con sistemas de extinción que son activados de haberse confirmado la existencia de un incendio. En la Figura 1.12 podemos apreciar un ejemplo de sistema de alarma contra incendio de la marca Opalux. Existen sistemas de alarma contra incendios de dos tipos: convencionales e inteligentes.

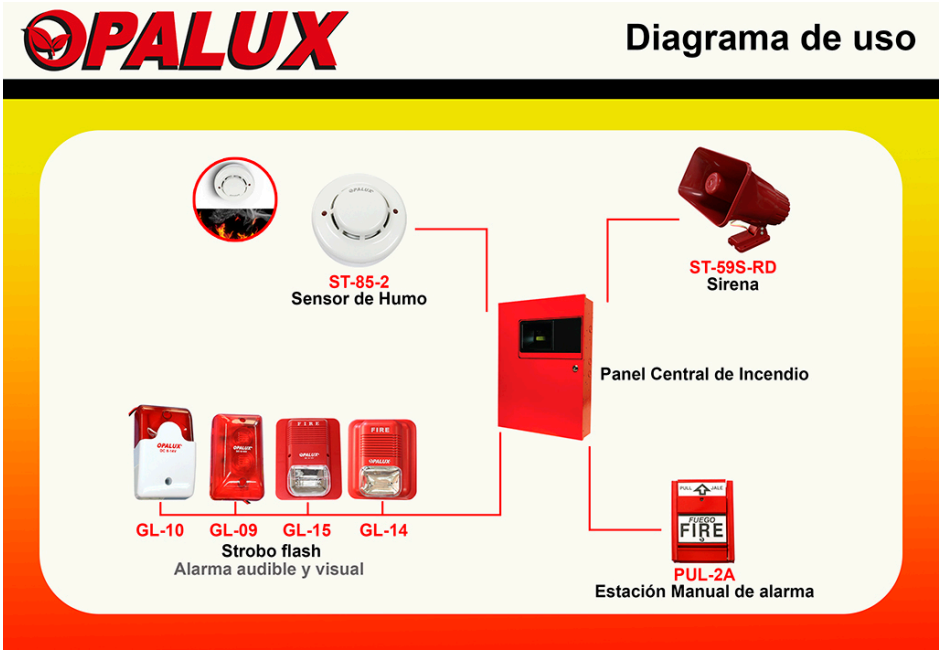


Figura 1.12. Sistema de alarma contra incendio

Fuente:https://opalux.com.pe/wp-content/uploads/2016/08/SistemaACI.jpg

- **Sistema de alarma vehicular**

  La función que cumplen las alarmas vehiculares es la de detectar la presencia de personas que puedan atentar contra un auto ya sea para vulnerarlo o vandalizarlo. El 1,8 %(INEI, 2020a) de la población peruana ha sufrido el robo de su vehículo en el primer semestre del año 2020. En la Figura 1.13 se puede apreciar un ejemplo de sistema de alarma vehicular de la marca POSITRON. Existen en el mercado sistemas de alarmas para vehículos que utilizan sensores volumétricos o sensores perimetrales.

Figura 1.13. Sistema de alarma vehicular
Fuente:https://www.equipamientolibertad.com/wp-content/uploads/2016/02/vehicular2.png

- **Sistema de alarma de intrusión**

  Un sistema de alarma de intrusión se define como aquella amalgama de dispositivos electrónicos que cumplen la función de prevenir la entrada de personas no gratas a un determinado lugar. En caso de presentarse el escenario, servir de disuasivo impidiendo de esa manera posibles hurtos o robos y alteraciones a la tranquilidad de los moradores o habitantes del recinto.

  Los sistemas de alarma de intrusión en la actualidad se hayan en diversas presentaciones y funcionalidades desde las más completas hasta las más básicas y esenciales. Todos los sistemas de alarma de intrusión independientemente del fabricante deben de cumplir la labor primordial de hacer llegar al usuario un mensaje en caso se produzca un evento que atente contra lo que se desee resguardar. Ello puede realizarse de diversas maneras y haciendo uso de distintos protocolos de comunicación. En los últimos años y con los avances tecnológicos se han producido mejoras en la versatilidad y velocidad de respuesta para los sistemas de alarma de intrusión. Haciendo uso de protocolos de internet tal como es el caso de IP que hace prácticamente instantánea

la alerta que se desee transmitir. Además de ello la convierte en universal dado que el usuario puede acceder a dicha información desde cualquier parte del mundo. Todo lo anteriormente mencionado depende de la configuración brindada por el proveedor de la tecnología.

Las partes principales de un sistema de alarma de intrusión son las siguientes:

Sensores

Los sensores cumplen la función de identificar las alertas del exterior, siendo fundamentales al momento de detectar la presencia de personas no gratas en el espacio que se está protegiendo. En gran parte de diseños de sistemas de alarma de intrusión los sensores envían la información captada a una central vía cables conectores y en otros casos la información es transmitida de manera inalámbrica a dicha central. La central se encargará de realizar las acciones debidas acorde a su programación y diseño.

Central comunicadora

La central comunicadora es la encargada de concentrar la información enviada por los sensores. Además de cumplir con una determinada programación realizada por el usuario. Cuenta además con la posibilidad de adherir dispositivos periféricos tales como llaveros para activación a distancia. Es la parte responsable del control de los dispositivos adheridos a el; así como también de la comunicación con el exterior. Haciendo uso de protocolos diversos dependiendo del fabricante del sistema. En la actualidad los protocolos más utilizados son IP y GSM/GPRS que agilizan la comunicación y la vuelven inmune a determinados cortes de servicio a los que pueda estar sujeta la línea telefónica. Existen sistemas de alarma de intrusión que presentan conexión directa con las autoridades municipales para llevar a ellas la alerta presentada. Los fabricantes de estas tecnologías implementan centrales de monitoreo con un determinado personal que está al tanto de las incidencias.

Actuador disuasivo

La función disuasiva se genera a la par de la alerta enviada generando un efecto de desconcierto en el delincuente al momento de perpetuar una intrusión. La manera de actuar de una alarma disuasiva es a través de una sirena y/o bocina. Las mismas que pueden ir acompañadas de luces intermitentes que nublen la visibilidad y provoquen desesperación en el delincuente a fin de que cometa alguna equivocación y dé por perdido su intento de intrusión. En los sistemas de alarma de intrusión las sirenas son las más comunes; sin embargo existe la posibilidad de añadir una bocina que es capaz de transmitir un mensaje de voz por parte del usuario. Cabe resaltar que dicha función depende del fabricante del sistema y no está disponible en todos los modelos existentes en el mercado.

1.7.2. Instalaciones de seguridad

Los sistemas de alarma de intrusión presentan esquemas muy similares en su diseño; dado que la función a cumplir es en finalidad la misma. Las tecnologías de comunicación varían dependiendo del fabricante y el campo de aplicación en un determinado espacio. Se mostrará a continuación un ejemplo de esquema utilizado.

Esquema básico de un sistema de alarma de intrusión

- **Sensor magnético:** Los accesos principales a los hogares en su mayoría son a través de puertas de diversos materiales y muchos de ellos con facilidad de ser vulneradas rápidamente. Es importante que se tenga un sensor que controle el acceso a la vivienda y que sea capaz de detectar cuando esta ha sido abierta en momentos en los que no son usuales. Se caracterizan por su fácil instalación y por ser una de las principales barreras de defensa ante una intrusión. Existen 2 configuraciones para estos sensores: normalmente abierto(N.A) y normalmente cerrado(N.C). Existen diversos tipos de sensores magnéticos, entre los cuales se pueden resaltar son: reed o switch y de efecto Hall como los de mayor uso en el mercado de los sistemas de alarma de intrusión.

- **Sensor PIR:** El sensor PIR (Passive infrared sensor) cumple la funcionalidad de detectar la temperatura del cuerpo humano y enviar la señal de alerta en base a ello. Se utiliza además del sensor un lente de Fresnel, el cual amplifica el rango de cobertura del sensor. Existen muchos tipos de sensores PIR en el mercado para diversos fines, los más demandados son aquellos que únicamente detectan el calor del cuerpo humano y no de animales.

- **Sensor de ruptura de cristal:** Los sensores de ruptura de cristal actúan utilizando una tecnología de reconocimiento de sonido, siendo especifico en la detección de la frecuencia de sonido que produce un vidrio al ser roto.

- **Teclado:** Es utilizado para programar el sistema de alarma de intrusión indicando las zonas habilitadas para detección, además de tener la opción de temporizar el período en que estará habilitado el sistema.

- **Central de control:** La central del sistema de alarma de intrusión es la encargada de recepcionar las señales provenientes de los sensores estratégicamente colocados en el recinto.

- **Sirena:** Es el dispositivo encargado de actuar al momento de producirse una alerta, arrojará un sonido que cumplirá la función de disuasivo. Puede ser programable para ser accionada por un determinado tiempo o hasta que se reciba una señal por parte del usuario que indique desactivación, todo ello por medio de la central de control.

- **Mando a distancia:** Es un dispositivo adicional al sistema, cumple con la función de enviar indicaciones a la central de alarma de manera inalámbrica vía RF, pudiendo también activar una alerta instantánea a manera de botón de pánico. Los controles a distancia están delimitados por un determinado rango de cobertura.

1.7.3. Sistemas de comunicación

Los sistemas de alarma de intrusión han ido cambiando y mejorando con el pasar del tiempo y las tecnologías de comunicaciones a la par. Por tal motivo los fabricantes de sistemas han optado por adecuar los modelos clásicos a ello. Con la explosión de internet y los diversos protocolos y servicios brindados a nivel de la nube los fabricantes ofrecen aplicaciones generalmente gratuitas para que el usuario tenga control general de su sistema de alarma de intrusión desde cualquier parte del mundo a través de internet. Para ello la central comunicadora debe de enviar la información respecto de las alertas reportadas por los sensores. La manera de comunicación de la central de los sistemas modernos de alarmas de intrusión se realizan a través del protocolo IP sin hacer uso de la línea telefónica como se hacía convencionalmente. Otra forma de comunicación de los sistemas es a través del protocolo GSM/GPRS. En la Tabla 1.5 se puede apreciar un cuadro comparativo entre algunas características que presentan las tecnologías anteriormente mencionadas.

Tabla 1.5
Comparativo entre sistemas de comunicación

	IP	GSM / GPRS
Funcionamiento	-Inalámbrico -Cableado	Inalámbrico
Velocidad	Rápida(dependiendo del proveedor).	Relativamente baja.
Comunicación	Dependiente de un punto de acceso.	Independiente de un punto de acceso.
Uso de chip	No	Si
Cobertura de red	Total si se cuenta con un buen punto de acceso.	Dependiendo del proveedor de servicio y ubicación de la central.

Fuente:Elaboración propia, extraído de https://www.argseguridad.com/blog/alarmas-por-gprs-3g-gsm-ip-diferencias-que-usar/

1.8. Sistemas similares

1.8.1. Kit de alarma EZVIZ

El kit inicial de alarma EZVIZ es un sistema de alarma contra intrusión que hace uso de la tecnología WI-FI para el envío de alertas en tiempo real. Esto se lleva a cabo mediante una aplicación del mismo proveedor. Permite además interconectar diversos equipos; sin embargo solo aquellos productos de la misma serie son posibles de acoplar. Está enfocado en cubrir las zonas de un hogar de dimensiones no muy grandes principalmente departamentos o residencias pequeñas y medianas. Su versatilidad reside en la simplicidad de uso y aún mayor facilidad de instalación la cual no requiere la presencia de un técnico especializado. El sistema cuenta con una central de control a la cual los sensores enviarán las respectivas alertas de presentarse el caso; dichos sensores son 2: sensor PIR y sensor magnético. Los sensores se comunican con la central de manera inalámbrica enfatizando mucho el ahorro de baterías haciendo que el sistema sea altamente eficaz a nivel energético. La central posee una sirena incluida; sin embargo es posible también adherir una sirena de mayores prestaciones. Además de ello se cuenta con un control remoto para armar o desarmar el sistema como también enviar una alarma instantánea a manera de botón de pánico. Este sistema está pensado para personas con pocos o nulos conocimientos de configuraciones de sistemas de alarma; dado que su uso e interfaz de configuración es sumamente intuitiva. En la Figura 1.14 se muestra la presentación de un sistema de alarma EZVIZ.

Los componentes del sistema son los siguientes:

- **Central de alarma:** Concentra la información enviada por los sensores y/o por el usuario.
- **Sensor PIR:** Inalámbrico con un período de duración de batería aproximado 2 años.
- **Sensor Magnético:** Inalámbrico con un período de duración de batería aproximado 3 meses, recargable.

- **Control remoto:** Utilizado para enviar señales de alerta instantáneas o activar determinadas configuraciones.

Figura 1.14. Ejemplar de sistema de alarma

EZVIZ
Fuente:https://s3.amazonaws.com/mfs.ezvizlife
.com/f8dd18a08e719f2cfacf9927fac5880f.jpg

1.8.2. Kit de alarma AJAX

El sistema de alarma de intrusión del fabricante AJAX hace uso de tecnologías inalámbricas casi en su totalidad. Está compuesto por una central de control la cual recibe las señales provenientes de los diversos sensores instalados. Su conexión con el exterior puede darse a través de tres diferentes modos como son: Wi-Fi, Ethernet y GSM/GPRS lo que provee redundancia en el caso que una de las tecnologías presente algún inconveniente para el envío de la notificación de alerta. Los sensores básicos con los que cuenta el sistema son el PIR y sensor magnético. La central de control provee la capacidad de gestionar el funcionamiento de los sensores a través de una aplicación móvil la cual puede ser instalada en los dispositivos móviles de los usuarios. Permite además enlazar dispositivos de videovigilancia únicamente de la misma marca. Su principal aplicación es para residencia de tamaño mediano como pueden ser departamentos. Los dispositivos inalámbricos se comunican con la central a través de un protocolo llamado ”Jeweller” el cual

provee encriptación y es decodificado por la central de control. Además de hacer uso exclusivo de baterías con un promedio estimado de vida 4 años, aumentando de esta manera la eficiencia y duración de los módulos. La central es capaz de enlazarse además a dispositivos de detección de incendio lo que hace el kit más completo a nivel de eventos posibles. Es posible también la adición de un control remoto para determinadas funciones específicas como botón de pánico o armada y desarmado de la central de control.

Es posible lograr un alcance perimetral de cobertura en el caso se desee proteger espacios amplios como jardines, utilizando repetidores comercializados por el mismo fabricante de la marca. En la Figura 1.15 se muestra un ejemplar de alarma AJAX. Los componentes básicos del sistema AJAX son los siguientes:

- **Central de alarma:** Posee redundancia de comunicación con el exterior, implementando Wi-Fi, Ethernet y GSM/GPRS.
- **Sensor PIR:** Inalámbrico con un período de vida útil de la batería de 5 años. Posee detección anti-mascota.
- **Sensor Magnético:** Inalámbrico con un período de vida útil de la batería de 7 años. Tiene protección anti-sabotaje.
- **Control remoto:** Aditamento adicional del sistema usado con la finalidad de activar o desactivar el sistema de alarma.
- **Detector de humo:** Posee una sirena interna capaz de alertar de manera independiente en caso de detectarse la presencia de humo.

Figura 1.15. Ejemplar de sistema de alarma AJAX
Fuente:https://www.actualidadgadget.com/ajax-tu-completo-sistema-de-seguridad-sin-cuotas/

1.8.3. Kit de alarma Prosegur

La alarma Prosegur para detección de intrusos es un sistema implementado para hogares medianos y departamentos. Haciendo uso de sensores inalámbricos como son el sensor PIR y el sensor magnético en específico. Todo ello conectado a una central de control que es la encargada de ser el eje sobre el que se construye el ecosistema de sensores. El sistema cuenta con una aplicación móvil brindada por el fabricante con la cual el usuario puede realizar configuraciones a su sistema. El proveedor habilita además de lo anteriormente mencionado un teclado inalámbrico con la capacidad de configurar las diversas zonas de cobertura del sistema. Cuenta adicional a ello un lector de ”Tags” inteligente que le provee la capacidad de detectar a las personas que cuenten con acceso seguro a la vivienda. Una sirena conectada a la central sirve de artefacto disuasivo y da aviso a los intrusos que existe un sistema anti-robos en la vivienda. Se hace uso de un mando a distancia para activar patrones programados en la central de control.

El producto es también un servicio; dado que la empresa fabricante cuenta con una central de monitoreo que al detectar una alarma envía un personal motorizado a verificar si efectivamente se ha producido un incidente. En la Figura 1.16 vemos una imagen de la presentación del kit de alarma PROSEGUR.

Los componentes del sistema son los siguientes:

- **Central de alarma:** Hace uso de la tecnología IP(Wi-Fi) además de GSM/GPRS para el envío de alertas al usuario.

- **Sensor PIR:** Inalámbrico y con detección anti-mascotas además cuenta con una cámara que envía las fotografías del evento al usuario.
- **Sensor Magnético:** Inalámbrico, ubicable en puertas y/o ventanas.
- **Control remoto:** Hace posible la configuración rápida de los modos de uso de la alarma.
- **Sirena:** Elemento actuador que sirve para impedir que el ladrón perpetúe el hurto, haciendo uso de un potente sonido.

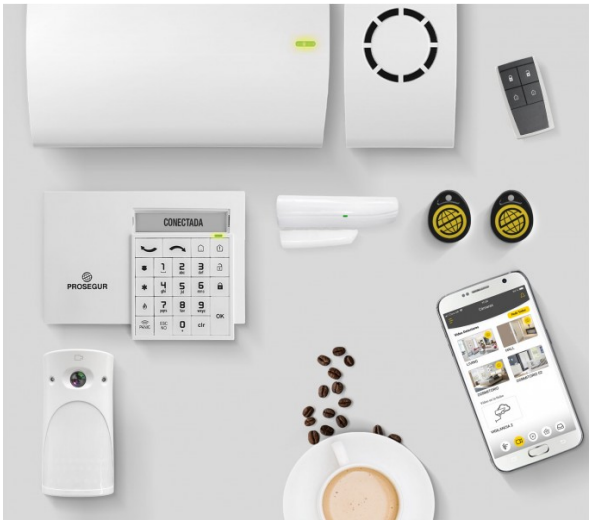


Figura 1.16. Ejemplar de sistema de alarma Prosegur
Fuente:https://www.prosegur.com.pe/hogares-y-personas/prosegur-smart

1.9. Análisis de sistemas similares

Los sistemas de alarma de intrusión presentan un alto grado de similitud, esto debido a que el fin principal sigue siendo el mismo. Existen algunos sistemas que poseen mayores prestaciones que otros en algunas características. Entre las más relevante tenemos el costo, conexión con el exterior al momento de enviar las alertas, la dificultad de instalación y complejidad de uso. En la Tabla 1.6 se aprecia un comparativo entre los sistemas anteriormente descritos.

Tabla 1.6
Comparativo entre fabricantes

	EZVIZ	**AJAX**	**PROSEGUR**
Precio	≈S/.600	≈S/.559.92	S/.700 + S/.144(mensualidad)
Modo de conexión	Inalámbrica	Inalámbrica	Inalámbrica
Protocolo(s) de uso	-Wi-Fi	-Wi-Fi -Ethernet -GSM/GPRS	-Wi-Fi -GSM/GPRS
Agente de instalación	Usuario	Usuario	Técnico
Central de monitoreo	No	No	Si
Aplicación móvil	Si	Si	Si

Fuente: Elaboración propia

Los sistemas de alarma de intrusión presentados poseen un precio similar; sin embargo la marca Prosegur presenta un precio de membresía a diferencia de los sistemas Ezviz y Ajax.

Todos los sistemas presentan una aplicación móvil con la cual los usuarios pueden gestionar el estado de sus sistemas a través de la red.

Otro punto a resaltar es la complejidad en la instalación dado que permite al usuario simplemente adquirir el sistema e instalarlo sin necesidad de contratar un especialista técnico.

1.10. Estado del Arte

En el presente apartado se detallarán estudios similares relacionados al marco principal del desarrollo de sistemas de seguridad electrónicos y su amalgama con el concepto del internet de las cosas(IoT), haciendo énfasis en sus características y uso en contraste con la solución planteada.

En el trabajo de grado elaborado por Parra titulado ”Diseño de un sistema para control de las alarmas de seguridad en el hogar utilizando la tecnología M2M”, expone el uso de la tecnología GSM/GPRS como principal agente de notificación al momento de presentarse una situación de alerta. Además expone la carencia de uso de un sistema de seguridad en los hogares debido a su alto costo.(Parra Marroquin y cols., 2019)

En el trabajo fin de máster elaborado por Martinez llamado ”Diseño e implementación de un sistema de alarma IoT basada en tecnologías Open Source”, propone una solución basada en los principios del internet de las cosas(IoT) así como también el uso del cloud computing adicionalmente a ello se añaden funcionalidades de domótica. Se presenta una proyección a futuro de producto comercial.(Martínez Moreno y cols., 2019)

Para el trabajo de titulación elaborado por Herrera nombrado ”Diseño e implementación de un prototipo de seguridad para control domótico basado en IoT bajo ambientes de dispotivos móviles con Android”, se propone un modelo de solución basado en la tarjeta de desarrollo Raspberry Pi 3 B+ y junto a ello el desarrollo de una aplicación móvil para el sistema operativo Android vinculado a una base de datos en Firebase desde donde se realizará la gestión del sistema de alarma.(Herrera Chávez, 2020)

En el trabajo de titulación desarrollado por Vilañez nombrado ”Implementación de un prototipo de sistema de seguridad doméstico basado en WPAN para una red IoT”, se expone un modelo de solución basado en la tecnología WPAN(Wireless Personal Area Network) cuyos nodos sensores y actuadores se comunican a través de la tecnología inalámbrica Zigbee.(Uvidia y Alexander, 2019)

En el trabajo de titulación desarrollado por Arequipa llamado ”Desarrollo de un prototipo de un sistema de seguridad contra intrusos utilizando protocolos de IoT sobre la plataforma Zolertia remote”, el trabajo realiza una propuesta basada en el protocolo MQTT(Message Queue Telemetry Transport) para la comunicación de los nodos sensores. Los cuales están basados en el hardware de la empresa Zolertia que brindan la facilidad de adaptar diversos sensores de uso comercial como es el caso de los sensores PIR.(Arequipa Cunalata, 2019)

1.11. Definición de términos básicos

- **IoT:** Internet of things o en español internet de las cosas, hace referencia a la conectividad de aparatos u objetos convencionales con la capacidad de hardware y software para enviar datos a internet y con la capacidad de interactuar.

- **Telegram:** Servicio de mensajería instantánea y videollamadas.

- **WPAN:** Wireless Private Area Network o en su traducción al español red de área privada inalámbrica, hace referencia a un estándar de comunicación inalámbrica cuya principal característica es la corta distancia entre los dispositivos involucrados.

- **M2M:** Machine to machine o maquina a maquina en su traducción al español, se refiere a la comunicación o transferencia de información entre dispositivos sin intervención del ser humano.
- **Wi-Fi:** Wireless Fidelity o en su traducción al español fidelidad inalámbrica, es una tecnología diseñada para la comunicación inalámbrica en una red de dispositivos conectados a un gateway.

- **GSM/GPRS:** Global System for Mobile/General Packet Radio Services , son Tecnologías de comunicación inalámbricas facilitadas por un proveedor de servicios de red de telefonía.

- **Ethernet:** Se define como un estándar de conexión de área local de manera cableada entre dispositivos.

- **IP:** Internet Protocol o protocolo de internet, es el estándar que rige las comunicaciones en internet.

- **MQTT:** Message Queue Telemetry Transport o en español transporte de telemetría de cola de mensajes, es un protocolo pensado para el internet de las cosas ligero y de bajo consumo, utiliza el modelo publicación-suscripción.

- **Open Source** Es también conocido código abierto, lo que quiere decir que no posee un dueño en específico y puede ser compartido y mejorado por la comunidad de usuarios.

- **Zigbee:** Se definen como protocolos de comunicación inalámbricos de redes de área personal(WPAN) con la característica principal de soportar una gran cantidad de dispositivos conectados en una misma red.

- **Python:** Lenguaje de programación interpretado, de alto nivel y multiplataforma.

- **C++:** Lenguaje de programación compilado, existe como mejora del lenguaje de programación C.

- **LUA:** Lenguaje de programación multiparadigma, diseñado en base a C.

- **AT:** Se definen como una serie de códigos que cumplen la función de instrucciones para permitir la comunicación entre el usuario y una terminal.

CAPITULO II: METODOLOGÍA DE DESARROLLO DEL TRABAJO PROFESIONAL

2.1. Delimitación temporal y espacial del trabajo

El sistema propuesto fue desarrollado entre los meses de marzo y noviembre del año 2020. El sistema es implementado en un hogar referencial del distrito de Villa el Salvador similar a los de los distritos aledaños como Villa María del Triunfo y San Juan de Miraflores. En dichos distritos el área promedio de una vivienda es de 140 m^2. Por lo tanto puede ser extrapolable para la población de la provincia de Lima.

2.2. Determinación y análisis del problema

Los problemas relacionados con la inseguridad en el hogar se han vuelto recurrentes. Los hogares con ingreso monetario bajo se han visto afectados. La tecnología puede aportar soluciones a estos problemas de inseguridad. Por tal motivo está en constante mejora para desarrollar sistemas más avanzados y efectivos. Los sistemas de seguridad para el hogar en la actualidad están siendo desarrollados por empresas de gran renombre y prestigio. Los sistemas mencionados no están orientados a viviendas de dimensiones estándar de 140m^2 y de un solo nivel. En los distritos de Villa el Salvador, Villa María del Triunfo y San Juan de Miraflores se hallan viviendas de este tipo. Muchos de estos sistemas no están alcance del consumidor promedio debido a su alto costo. Lo que conlleva a que una gran parte de la población no pueda adquirir uno de estos productos. Los sistemas más comerciales hacen uso de aplicaciones móviles dependiendo del fabricante; sin embargo carecen de una interacción más directa con el usuario. Los servicios de mensajería instantánea brindan mayor versatilidad de comunicación con el usuario final. Los dispositivos que conforman los sistemas de seguridad mencionados anteriormente son en su mayoría dispositivos cableados. Lo cual genera un mayor trabajo y costo de instalación.

2.2.1. Problema general

Los sistemas de seguridad electrónica que se utilizan en domicilios actualmente son de alto costo para usuarios o clientes que no cuenten con un poder adquisitivo alto. El precio hace que estos sistemas sean restrictivos al publico en general.

2.2.2. Problemas específicos

1. No existen diseños disponibles de sistemas de seguridad de bajo coste y consumo de batería en el mercado peruano.

2. No existen implementación de sistemas de seguridad con sensores independientes de una red local de comunicación inalámbrica con funcionalidades de alerta inmediata al sistema de alarma de intrusión que utilicen mensajería instantánea.

3. No existen métodos de validación de la funcionalidad de este tipo de sistemas de seguridad.

2.3. Modelo de solución propuesto

2.3.1. Introducción

En el presente apartado se detallará el modelo de solución propuesto basado en los requerimientos básicos que debe de cumplir para su correcto desempeño y óptimo rendimiento usando los componentes apropiados acorde al sistema. Se profundizará en los procedimientos para el diseño e implementación de los dispositivos y el funcionamiento del sistema **(VER ANEXO 01)**. Así como también se presentarán las pruebas realizadas para comprobar la efectividad del modelo propuesto y de esta manera validar su correcto funcionamiento. En la Figura 2.1 se detalla el flujograma de trabajo.

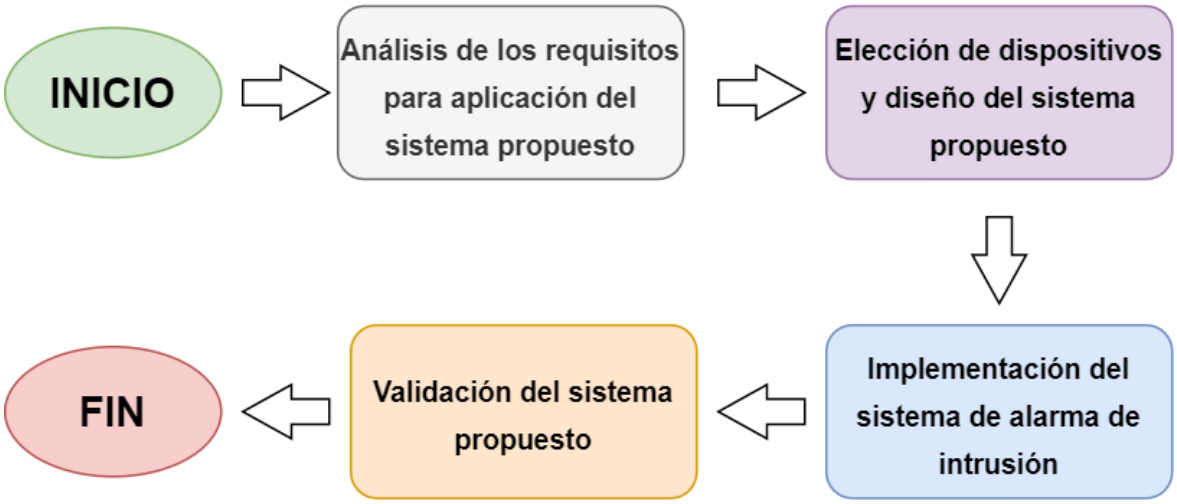


Figura 2.1. Flujograma de desarrollo del trabajo
Fuente: Elaboración propia

2.3.2. Diseño y dimensionamiento del sistema

Dimensionamiento de requisitos

- El modelo de solución propuesto está diseñado para viviendas pequeñas y medianas; tales como departamentos o casas de una dimensión no mayor a 140 m^2 y de una sola planta o nivel. En la Figura 2.2 se visualiza un ejemplo de domicilio modelo que cumple con los requisitos máximos para el despliegue del sistema propuesto. Se denota una cantidad de ambientes igual a 8 detallados de la siguiente manera: entrada principal, sala principal, sala de estudio, baño 1, cocina, baño 2, dormitorio 1 y dormitorio 2. Dichos ambientes son óptimos para una vivienda de aproximadamente 4 habitantes.

- Se debe de considerar que las paredes de preferencia no sean de concreto para evitar el efecto de la atenuación de la señal de los nodos sensores hacia la central comunicadora y viceversa.

Figura 2.2. Ejemplo de domicilio apto para aplicación
Fuente: Elaboración propia

- El sistema de notificaciones está diseñado para funcionar en teléfonos móviles de sistema operativo Android e IOS. Para lo cual se requiere que los usuarios posean dispositivos con alguno de los 2 sistemas operativos anteriormente mencionados.

Selección de áreas vulnerables

Los nodos sensores deberán ser instalados en puntos vulnerables y deben de ser seleccionados teniendo en cuenta los siguientes criterios:

- Accesibilidad para instalación.
- Amplia cobertura de área a ser protegida.
- Ubicarse en una entrada principal que dé acceso hacia áreas comunes.
- No estar al alcance de mascotas
- Buscar línea de vista con la central.
- No estar separados por más de 40m de la central comunicadora.

Las 2 áreas que cumplen con los requisitos anteriormente mencionados son la entrada principal y la sala principal, siguiendo con el modelo de vivienda visto en la Figura 2.2 se elegirán los 2 puntos de instalación de los nodos sensores.

En el caso de la entrada principal se requiere cubrir un área de dimensiones 12 m^2(3m x 4m) en dicho espacio se encuentra la puerta que brinda acceso principal a la vivienda. Por tal motivo se hace la elección de un nodo sensor magnético.

Para el caso de la sala principal se requiere cubrir un área de dimensiones 48 m^2(12m x 4m). La entrada no cuenta con una puerta que brinde acceso al ambiente y es vulnerable a una posible intrusión en caso se produzca un error en el sensado de la entrada principal. Por tal motivo se hace uso de un nodo sensor PIR.

Como se aprecia en la Figura 2.3, se ubicaron los nodos sensores en los ambientes estipulados y se denominaron nodos **A** y **B**

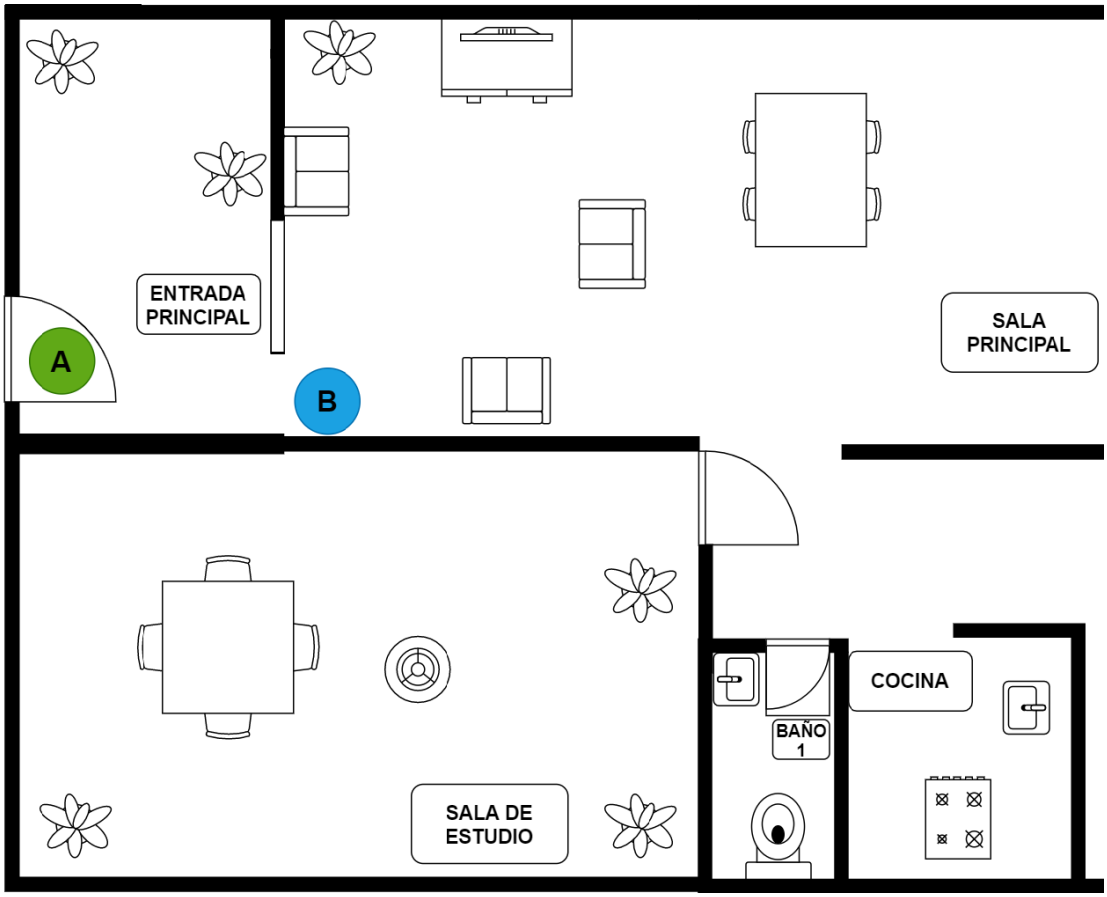


Figura 2.3. Distribución de nodos sensores
Fuente: Elaboración propia

Requisitos de instalación de nodos sensores

En la Figura 2.4 se aprecia la vista lateral del nodo sensor PIR. La altura de instalación adecuada está entre los 2m y 2.5m sobre el nivel del suelo. Para la instalación del nodo sensor PIR se debe de tener en cuenta los siguientes requisitos:

- No debe de estar expuesto a altas temperaturas.
- Debe permanecer alejado de instalaciones eléctricas.
- No ubicarse en paredes metálicas.
- Debe ubicarse en una superficie estable.
- No debe exponerse a la luz del sol.
- No exponerse a la humedad.

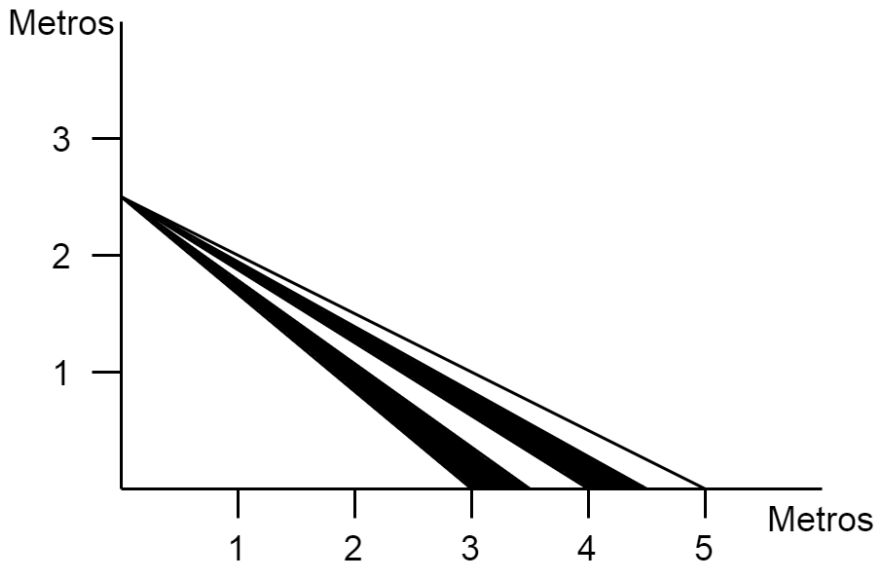


Figura 2.4. Vista lateral del nodo sensor PIR
Fuente: Elaboración propia

Un detalle relevante del nodo sensor PIR es el ángulo de sensado. Para el caso presentado es menor o igual a 100º, el cual es representado gráficamente en la Figura 2.5.

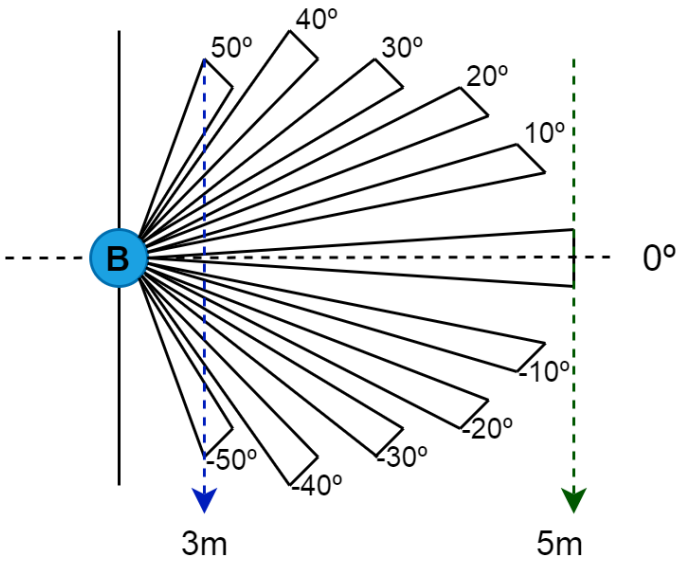


Figura 2.5. Vista superior del nodo sensor PIR
Fuente: Elaboración propia

El nodo sensor magnético es instalado en la puerta principal. Cuenta con 2 partes, las cuales se colocan una en la puerta y la otra en la pared adyacente. La altura de instalación adecuada está entre los 1.8m y 2m sobre el nivel del suelo. Los requisitos para la instalación del nodo sensor magnético son los siguientes:

- No instalarse en puertas ni paredes metálicas.
- Evitar la instalación en lugares con exceso de polvo.
- No estar expuesto a altas temperaturas.
- Evitar espacios donde haya posibilidad de golpes al equipo.
- Evitar puntos de instalación donde haya humedad.

Requisitos de instalación de la central comunicadora

La comunicación con el exterior es fundamental para el correcto funcionamiento del sistema. Para ello es necesario que la central comunicadora cuente con algunos requisitos básicos de instalación, los cuales serán detallados a continuación:

- Se encuentre vinculada a un punto de acceso brindado por el usuario final a una distancia recomendable de **1m** del equipo.
- Es necesario que el punto de acceso de conexión sea de hogar o de personas cercanas de confianza y de preferencia no compartido con terceros para de esta manera evitar la vulnerabilidad de atacantes externos.
- La ubicación de la central comunicadora debe de estar a una altura aproximada de **2m** del suelo a fin de evitar posibles golpes no intencionales y al mismo tiempo ser difícil de ubicar para posibles intrusos. Este requisito también es aplicable para evitar la desconexión por parte de animales domésticos.
- Para la instalación de la central controladora del sistema es necesario un punto de alimentación fijo de **220V AC** y que la distancia entre el equipo y el punto no sea mayor a **1.5m** que es la longitud máxima del cable del equipo.

Método de comunicación

El sistema propuesto es principalmente inalámbrico y para ello es de carácter relevante elegir una tecnología de comunicación para la transferencia de la información y alerta de los nodos sensores hacia la central controladora. De la misma manera de la central controladora hacia el exterior. En el apartado 1.5 se hizo referencia entre las tecnologías inalámbricas de aplicación en el IoT las cuales fueron las siguientes:

- Wi-Fi
- LoRa
- Sigfox
- Bluetooth
- Zigbee

En la Tabla 1.4 se realizó una comparativa entre las tecnologías anteriormente mencionadas y se determinó el uso de la tecnología **Wi-Fi** por motivos de uso de bandas de frecuencia, velocidad de transmisión y accesibilidad en el hogar además de su bajo costo. Para el presente desarrollo se hará uso de **Wi-Fi** para el principio general de todo el proyecto y en específico el protocolo **ESP-NOW** para la comunicación entre los nodos sensores y la central comunicadora. Es elegido bajo los siguientes criterios:

- Rápida transferencia de datos.
- Compatibilidad con el hardware utilizado.
- Alto rendimiento
- Uso práctico en los nodos y provee ahorro de componentes.
- Libre documentación
- Uso de frecuencias liberadas bajo los lineamientos del MTC.

Requisitos del servicio de mensajería instantánea

En el mercado existen diversos servicios de mensajería instantánea; sin embargo no todos cumplen con la versatilidad y adaptación para sistemas de seguridad. Se deben de cumplir determinados criterios para la aplicación en el sistema propuesto, los cuales serán detallados a continuación:

- Encriptación de los mensajes.
- Multiplataforma y de uso gratuito.
- Compatibilidad con plataformas y entornos de código libre.
- Amplia comunidad de usuarios.

El elemento de elección para uso en el presente desarrollo es el servicio de mensajería instantánea **Telegram**, el cual cumple con los requisitos anteriormente mencionados. El logo de **Telegram** se aprecia en la Figura 2.6.

Figura 2.6. Logo de Telegram
Fuente:https://web.telegram.org/

Caracterísiticas generales

Las características de uso enfocadas en el usuario final son las siguientes:

- El modelo de sistema de alarma de intrusión propuesto admite la posibilidad de emparejamiento de hasta un máximo de **10 nodos sensores** con una central comunicadora todos ellos con transferencia de información encriptados. Se debe de tener en cuenta ello antes de determinar la aplicación del modelo propuesto en un determinado espacio.
- Uso de aplicación de mensajería instantánea para una amigable configuración de los estados del sistema.

Descripción de componentes utilizados

- **Sensor magnético MC-38**

  El sensor magnético tiene aplicación en el presente trabajo cumpliendo con la función de detectar alertas en puertas y ventanas; dado que funciona como si fuese un interruptor. Para el modelo propuesto se hará uso del sensor magnético MC-38, su bajo costo y altas prestaciones lo hace ideal para el planteamiento del proyecto. En la Figura 2.7 se aprecia una fotografía del sensor a utilizar, de igual manera en la Tabla 2.1 se detallan las características técnicas del sensor en cuestión.

  A continuación se presentarán las características técnicas:

  Tabla 2.1
  Características técnicas de sensor magnético MC-38

Características técnicas del sensor magnético MC-38	
Material	Plástico ABS
Voltaje máximo	100 VDC
Corriente nominal	100mA
Tipo de contacto	Normalmente cerrado(N.C)
Distancia de activación	15-25 mm
Potencia nominal	3w

  Fuente: Elaboración propia, extraído de https://cdmxelectronica.com/producto/sensor-magnetico-mc-38/

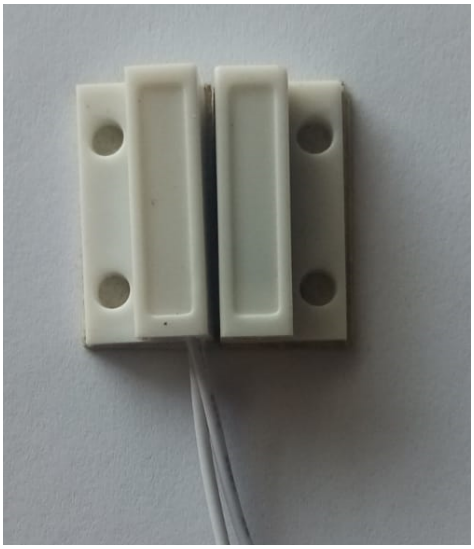


Figura 2.7. Sensor magnético

MC-38
Fuente: Elaboración propia

- **Sensor PIR AM312**

  El sensor PIR o sensor piroeléctrico es un dispositivo con la capacidad de medir la radiación infrarroja que emiten los diversos cuerpos y con ello poder detectar la presencia de los mismos. Se hace uso del sensor PIR AM312. Como se aprecia en Figura 2.8 se denota el componente a utilizar y en la Figura 2.9 se aprecia el esquema interno del sensor AM312.

Figura 2.8. PIR AM312
Fuente: Elaboración propia

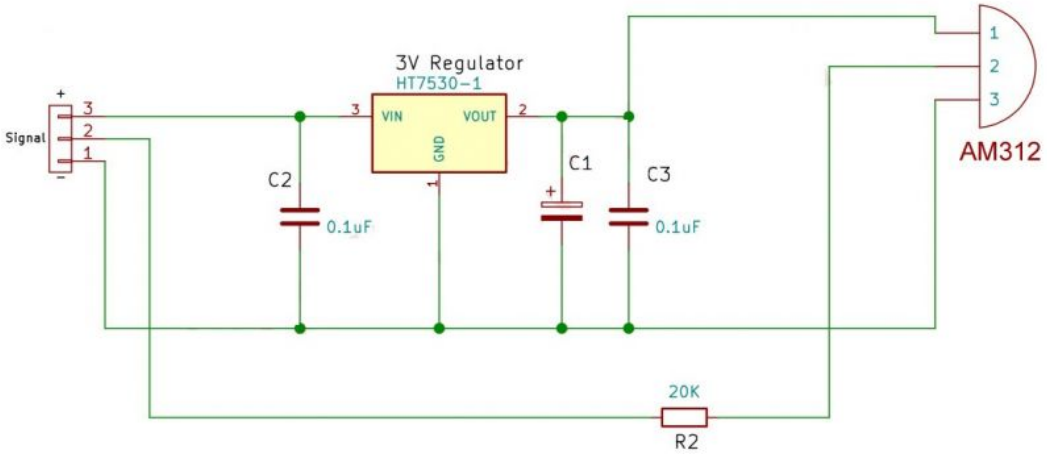


Figura 2.9. Esquema interno PIR AM312
Fuente:https://robojax.com/products.php?pid=807

El sensor PIR AM312 posee 3 pines de sencillo uso los cuales son GND, VCC y OUT. El voltaje de alimentación está en el rango de 2.7V DC - 12V DC, a diferencia de otros sensores que están configurados internamente para trabajar con 5V DC. Los cuales requieren de hacer ajustes en el hardware para compatibilizar el sensor con el desarrollo que se realiza. La alimentación que recibirá el sensor se hará desde una batería de 3.7V DC para lo cual el sensor AM312 es el ideal para la presente solución.

Un punto relevante del desarrollo de los sensores es el bajo consumo de energía. Se requiere que el modelo propuesto cumpla con ello. El sensor AM312 tiene un consumo promedio menor a 0.1mA. Por tal motivo lo hace la opción ideal para el desarrollo.

El funcionamiento básico del sensor es el de detectar la presencia de un intruso en la zona donde esté instalado y enviar una señal de alerta. En la Tabla 2.2 se aprecian las características técnicas del sensor AM312.

Tabla 2.2
Características técnicas del sensor PIR AM312

Características técnicas del sensor PIR AM312	
Voltaje de funcionamiento	2.7V DC - 12V DC
Consumo de corriente	<0.1mA
Temperatura de trabajo	-20ºc - 60ºc
Rango de detección	3m - 5m
Ángulo de detección	≤ 100º
Tiempo de retardo	2s

Fuente:Elaboración propia, extraído de http://www.mantech.co.za/datasheets/products/EIE32-0002-01-R0.pdf

- **Módulo de carga de batería**

  El módulo de carga tiene la función de proveer energía a la batería y mantenerla energizada hasta que haya cumplido con el límite de capacidad. Para fines del presente desarrollo se ha empleado el módulo basado en el chip TP4056 el cual se aprecia en la Figura 2.10. Por motivos de bajo costo, fácil adquisición en el mercado y reducido tamaño lo convierte ideal para el sistema propuesto.

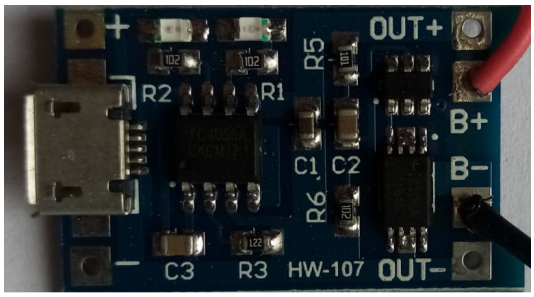


Figura 2.10. Módulo de carga

TP4056
Fuente:Elaboración propia

Las características del módulo se detallarán en la Tabla 2.3.

Tabla 2.3
Características técnicas del módulo de carga TP4056

Características técnicas del módulo de carga TP4056	
Corriente de carga	1A(modificable)
Voltaje de entrada	4.5V DC - 5.5V DC
Temperatura de trabajo	-10ºc - 85ºc
Entrada	Micro USB
Circuito de protección	Si
Led indicador de carga	Si

Fuente:Elaboración propia, extraído de https://www.naylampmechatronics.com/baterias/641-cargador-usb-de-bateria-litio-18650-1a-tp4056-con-proteccion.html

El módulo de carga está diseñado para baterías de tipo Lipo y Li-ion de 3.7V DC hasta los 4.2V DC. Estas últimas son las utilizadas en el presente trabajo. Además de ello el módulo posee un circuito de protección lo que provee de mayores prestaciones y beneficios. Esto genera un mayor tiempo de vida útil de la batería. Cuenta con un led de batería llena, así como un led de carga en proceso. En la Figura 2.11 se detalla el circuito interno del módulo de carga basado en el chip TP4056.

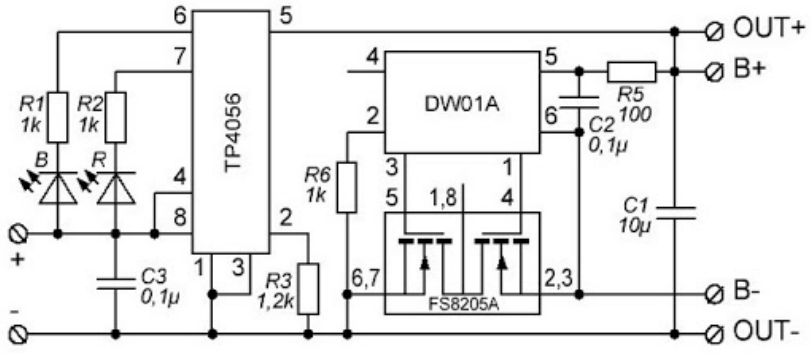


Figura 2.11. Circuito módulo TP4056
Fuente:http://acoptex.com/project/9446/basics-project-082a-lithum-battery-charger-tp4056-at-acoptexcom/#sthash.Qhv29XRv.dpbs

- **Batería Li-ion 18650**

  La fuente de alimentación principal de los nodos sensores es la batería de tipo Li-ion del tipo 18650. Las cuales cuentan con una tensión de 3.7V DC, llegando algunas hasta la tensión de 4.2V DC. Para el presente desarrollo se usarán las últimamente mencionadas. Las cuales cuentan con una capacidad de corriente de 3500mAh. En la Figura 2.12 se visualiza el modelo de batería a utilizar.

Figura 2.12. Batería Li-ion 18650
Fuente: Elaboración propia

- **Convertidor de voltaje**

  El módulo convertidor cumple la función de realizar una disminución del nivel de voltaje de la fuente de alimentación principal. Ello con la finalidad de no perjudicar a los módulo que se alimenten con voltajes inferiores al valor de la fuente de alimentación. Para efectos del presente proyecto se hará uso del módulo basado en el encapsulado LM2596, el cual se puede apreciar en la Figura 2.13.

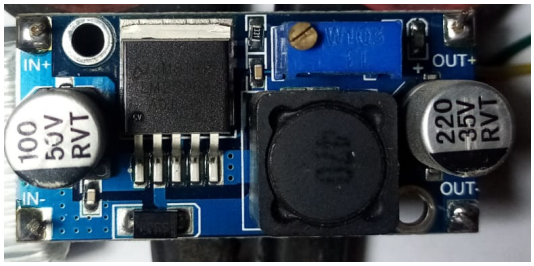


Figura 2.13. Módulo convertidor LM2596
Fuente: Elaboración propia

En la Tabla 2.4 se aprecian las principales características técnicas del módulo regulador de tensión.

Tabla 2.4
Características técnicas del módulo convertidor LM2596

Características técnicas del módulo convertidor LM2596	
Corriente de salida max.	3A
Voltaje de entrada	4.5V DC - 40V DC
Voltaje de salida	1.5V DC - 35V DC
Potencia salida	25w
Frecuencia de trabajo	150KHz

Fuente:Elaboración propia, extraído de https://www .naylampmechatronics.com/conversores-dc-dc/196 -convertidor-voltaje-dc-dc-step-down-3a-lm2596.html

- **ESP32**

  El ESP32 es el elemento principal del desarrollo del trabajo expuesto en el presente documento. El SoC ESP32 se encuentra presente en diversos módulos para aplicaciones distintas. Para efectos del presente trabajo se hará uso del módulo ESP-WROOM-32. El cual es de fácil adquisición en el mercado así como contar con dimensiones reducidas, versatilidad de programación y una amplia comunidad de desarrolladores. Estos últimos aportan constantemente para la mejora continua de diversos proyectos. El módulo a utilizar se visualiza en la Figura 2.14.

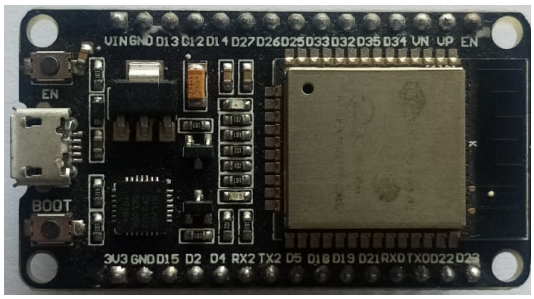


Figura 2.14. Módulo ESP-WROOM-32
Fuente:Elaboración propia

El módulo ESP-WROOM-32 presenta características relevantes para distintas aplicaciones de IoT, se hará una reseña en la Tabla 2.5.

Tabla 2.5
Características técnicas del módulo ESP-WROOM-32

Características técnicas del módulo ESP-WROOM-32	
Voltaje de alimentación	5V DC(USB) y 3.3V DC
Voltaje de GPIO's	3.3V DC
Wi-Fi	802.11 b/g/n/e/i
Bluetooth	v4.2 y BLE
USB-Serial	CP2102

Fuente:Elaboración propia, extraído de https://www.naylampmechatronics.com/espressif-esp/384-nodemcu-32-esp32-wifi.html

La distribución de pines del módulo ESP-WROOM-32 se puede apreciar en la Figura 2.15.

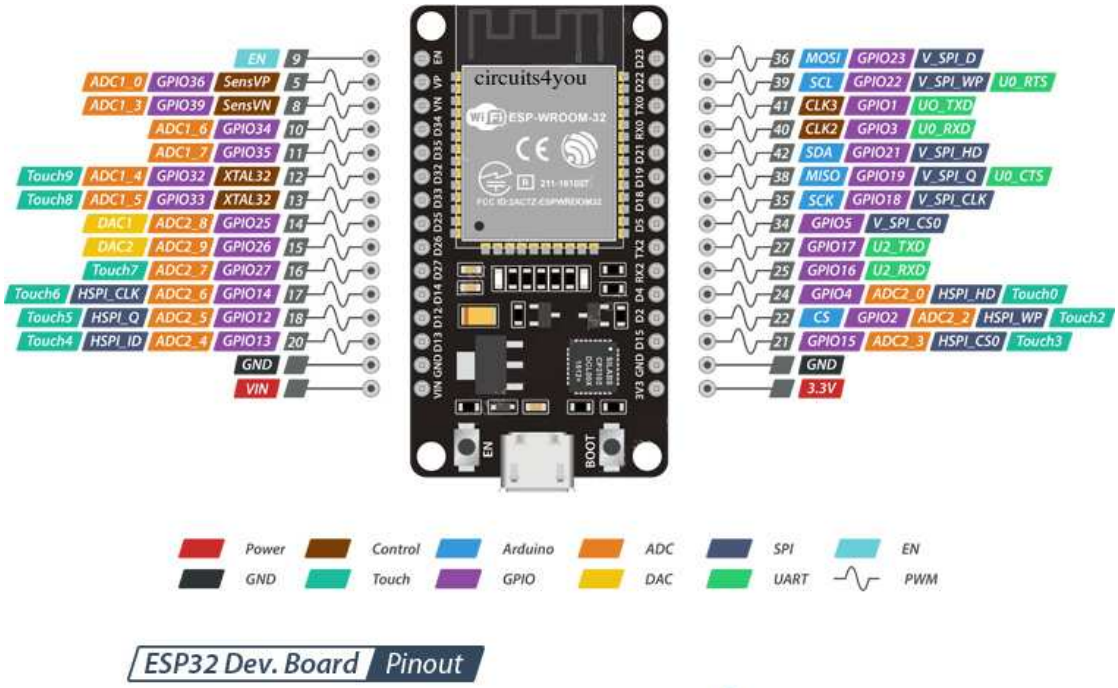


Figura 2.15. Distribución de pines del módulo ESP-WROOM-32
Fuente:https://www.naylampmechatronics.com/espressif-esp/384-nodemcu-32-esp32-wifi.html

Diseño del sistema

La presente propuesta de solución se sintetiza en 2 bloques principales: el **bloque controlador** central y el **bloque detección**. Para ambos casos anteriormente mencionados se hace uso del SoC ESP32. El cual se encarga de la gestión principal de los procesos. En la Figura 2.16 se denota el diagrama de bloques del sistema propuesto.

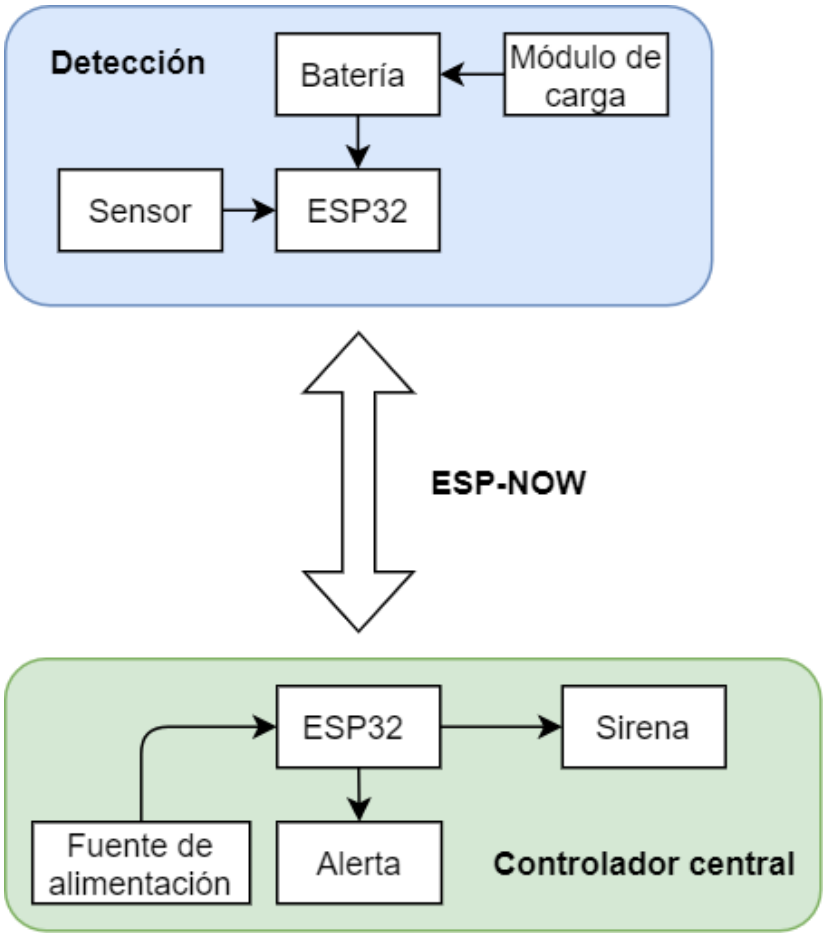


Figura 2.16. Diagrama de bloques del sistema propuesto
Fuente:Elaboración propia

El **módulo de carga** se encarga de proveer la energía necesaria a la **batería** para la alimentación del módulo.

El bloque **sensor** se encarga de la detección de una posible intrusión.

El **ESP32** es el eje principal del sistema propuesto; dado que se encarga de la transferencia de información entre los bloques principales vía el protocolo **ESP-NOW**.

Para el caso del **controlador central** es el encargado de enviar la **alerta** así como también de la activación del módulo relé para luego proveer de energía a la **sirena**. Por otro lado el bloque **detección** se encarga de procesar la señal del **sensor** y posterior envío de la misma hacia la central.

La construcción del sistema se hará en base a los bloques anteriormente mencionados y se detallará de manera técnica los procedimientos de diseño.

Para el caso del **bloque detección** se han diseñado 2 tipos de nodos sensores, los cuales están desarrollados en base al sensor magnético y sensor PIR. En ambos casos cumplen etapas de manera similar para su correcto funcionamiento, las cuales son detalladas a continuación:

- Etapa de carga
  En esta etapa se asegura que el nodo sensor se haya cargado correctamente. Cada nodo sensor posee en su interior un circuito de carga y protección de baterías. El cual será utilizado para hacer independiente al dispositivo de una fuente de alimentación perenne. El módulo de carga utilizado en el presente trabajo es el basado en el chip TP4056 el cual se aprecia en la Figura 2.10.

- Etapa de alerta.
  En cuanto el dispositivo se encuentre cargado se colocará en estado de alerta enviando señales en caso se presente una intrusión en el sistema.

- Etapa de ahorro de energía.
  Una vez el mensaje por parte de los nodos sensores se haya enviado a la central, el nodo sensor entrará en un etapa de sueño profundo haciendo que su consumo de energía sea el mínimo posible, limitado por el microcontrolador.

Las etapas de los nodos sensores son secuenciales como se aprecia en la Figura 2.17.

Figura 2.17. Etapas de nodos sensores
Fuente:Elaboración propia

Circuito de carga de los nodos sensores

El esquema de la Figura 2.18 tiene el componente de entrada el módulo de carga de baterías seleccionado el cual está basado en el chip TP4056. La elección parte de la premisa del bajo costo del módulo, su fácil adquisición en el mercado y pequeño tamaño,lo que lo hace ideal para el proyecto. El módulo TP4056 es alimentado por una entrada micro-USB de tipo C, cuya entrada es la que provee de carga a la batería de 3.7V DC. El voltaje de entrada es de 4.5V DC hasta los 5.5V DC como se aprecia en la Tabla 2.3. Al finalizar la carga se encederá un led azul indicando el fin del proceso.

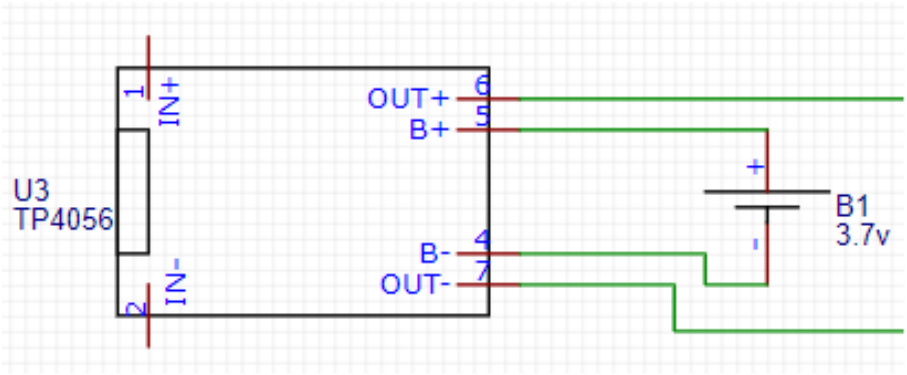


Figura 2.18. Circuito de carga-alimentación nodos sensores
Fuente: Elaboración propia

Circuito de regulación

La alimentación de los nodos sensores debe de ser 3.3V DC; dado que es el voltaje con el que trabaja el módulo ESP-WROOM-32. Ante ello se ha diseñado el circuito esquematizado en la Figura 2.19. Cabe resaltar que el voltaje de 3.3V DC entregado por el circuito de regulación es usado para todos los nodos sensores y es el óptimo para trabajar con el resto de componentes seleccionados.

El circuito de regulación cuenta con el componente AMS1117-3.3V DC el cual es el responsable de regular el voltaje de entrada al circuito y mantener los 3.3V DC estables. Para evitar picos y filtrar correctamente la entrada, se coloca un capacitor electrolítico (C2) de 2.2uF entre la entrada al regulador y GND. De igual manera para la salida y estabilizar aún más el circuito se coloca un capacitor cerámico (C1) entre la salida regulada y GND.

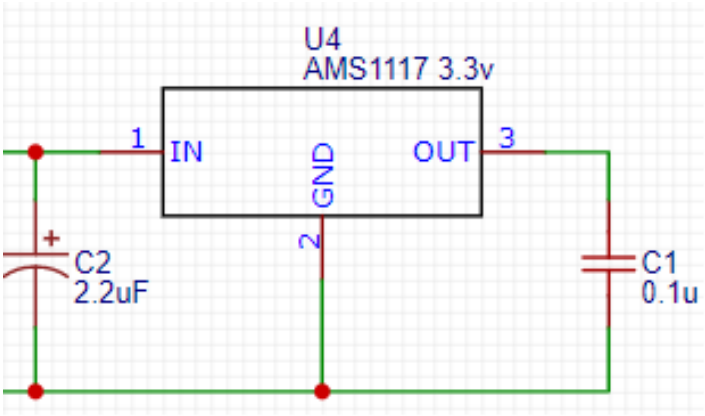


Figura 2.19. Circuito de regulación de tensión
Fuente: Elaboración propia

Nodo sensor magnético

El nodo sensor magnético forma parte del bloque detección. Cumple con las etapas anteriormente mencionadas. Para su diseño se ha estipulado el uso del sensor magnético MC-38 como se determinó en el capítulo anterior. Se puede apreciar una fotografía del componente en la Figura 2.7. El sensor magnético MC-38 ha sido elegido para el desarrollo del prototipo debido a sus altas prestaciones, bajo costo, fácil adquisición en el mercado y gran compatibilidad.

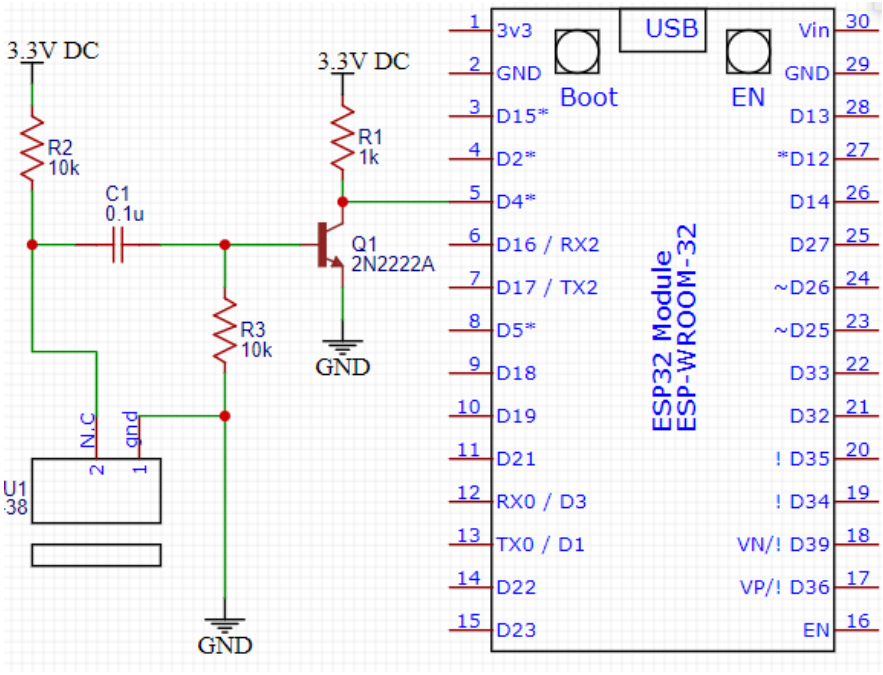


Figura 2.20. Circuito de funcionamiento del nodo sensor magnético
Fuente: Elaboración propia

El circuito presentado en la Figura 2.20 es diseñado para su uso en caso de activación del sensor MC-38 el cual trabaja con un contacto normalmente cerrado (N.C). Mientras el contacto está en reposo y no presenta apertura, mantiene su estado original y el módulo ESP-WROOM-32 recibirá a través de su GPIO 4 un estado lógico 0 y por tal motivo no emitirá ninguna alerta. De darse el caso que se aperture el contacto el transistor 2N2222A (Q1) recibirá una señal en la base haciendo que se emita un voltaje de entrada de 3.3V DC al GPIO 4, que es análogo a un 1 lógico produciendo de esta manera que se envíe una alerta. Para obtener el voltaje de 3.3V DC necesario para las operaciones del circuito se hace uso del esquema regulador presentado en la Figura 2.19.

Nodo sensor PIR

El nodo sensor PIR de manera análoga al nodo sensor magnético también forma parte del bloque detección y está compuesto por el módulo ESP-WROOM-32 como el encargado del envío de la alerta. El sensor PIR AM312 es el gestor de la señal que será procesada por el módulo para su posterior envío. Se realizó la elección

de sensor PIR AM312 como el ideal para el proyecto debido a su voltaje de alimentación, el cual opera entre los 2.7V DC y 12V DC. Ello es favorable dado que los nodos sensores operan al voltaje de 3.3V DC. Además de ser de bajo costo.

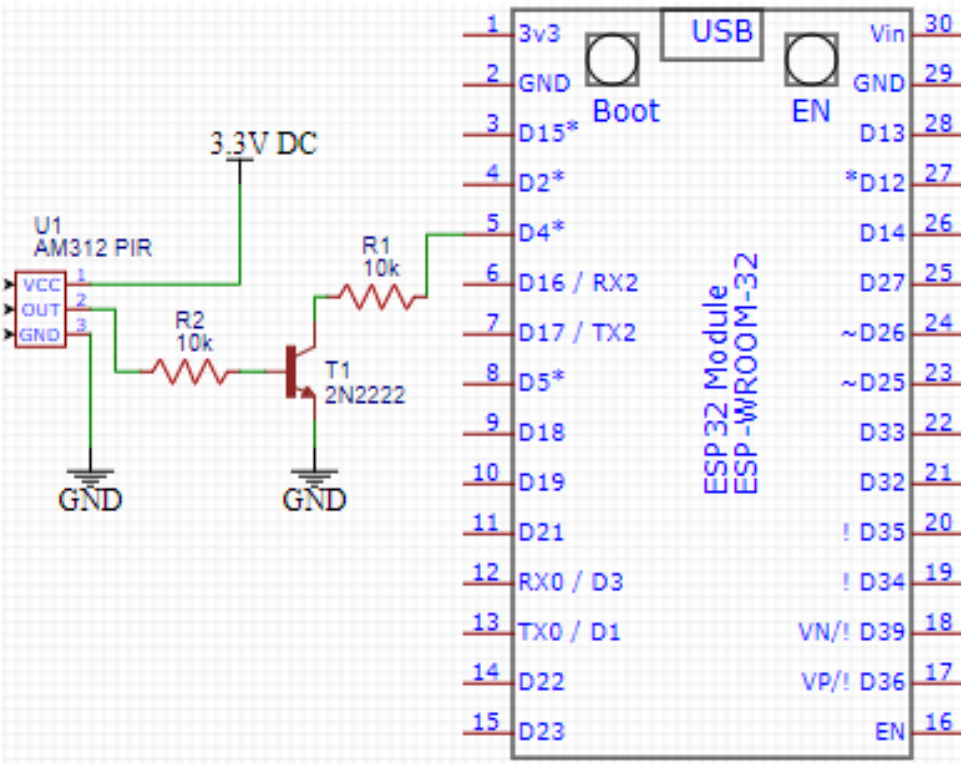


Figura 2.21. Circuito de funcionamiento del nodo sensor PIR
Fuente: Elaboración propia

El esquema presentado en la Figura 2.21 está planteado para la activación de la alerta en caso el sensor PIR AM312 detecte alguna intrusión. Por medio del pin OUT del sensor enviará una señal al transistor 2N2222 (T1) en la base del mismo. Posteriormente la señal será recibida por el módulo ESP-WROOM-32 que procesará la señal y enviará la alerta a la central comunicadora. Para la alimentación del nodo sensor PIR se hace uso del circuito de alimentación presentado en la Figura 2.19.

Para el caso del bloque **controlador central** se hace uso del módulo ESP-WROOM-32 para el procesamiento de las alertas que serán enviadas por los nodos sensores para su posterior envío al servicio de mensajería instantánea.

De manera similar a los nodos sensores el **controlador central** pasa por una serie de etapas para su funcionamiento, las cuales son:

- Etapa de alimentación

  En esta etapa la central comunicadora será energizada a través de la fuente de alimentación.

- Etapa de regulación

  La alimentación se dará a través de una fuente de 12V DC que para efectos del trabajo se hará uso de 5V DC para energizar el módulo ESP-WROOM-32. Para ello se hará uso del módulo LM2596.

- Etapa de alerta

  Se produce mientras se mantiene energizada o en caso del uso de la batería estará en modo de alerta esperando las alertas de los nodos sensores.

Las etapas son presentadas gráficamente en la Figura 2.22.

Figura 2.22. Etapas de central comunicadora
Fuente: Elaboración propia

Central comunicadora

La central comunicadora es la encargada de recibir las señales de alerta de parte de los nodos sensores y posteriormente enviar un mensaje al servicio de mensajería instantánea Telegram. A la par activar el módulo relay para energizar la sirena y emitir la señal audible. El esquema diseñado se presentará de manera gráfica en la Figura 2.23.

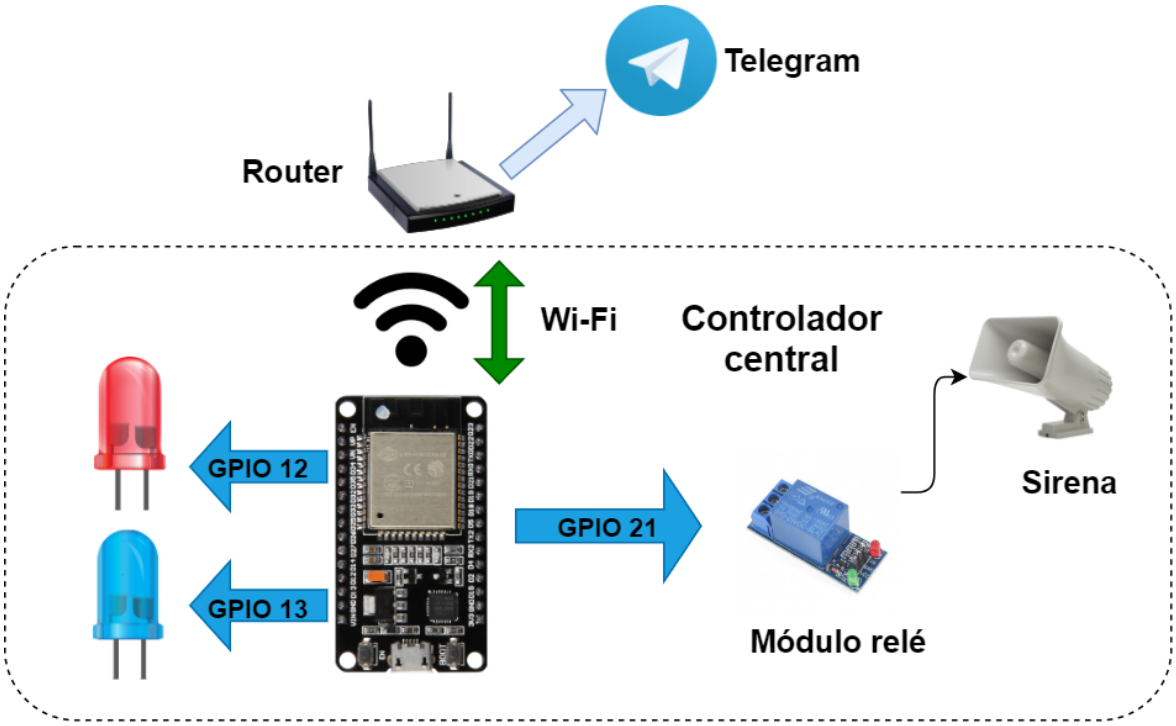


Figura 2.23. Esquema de diseño de central comunicadora
Fuente: Elaboración propia

El funcionamiento de la central comunicadora consiste en cumplir la función de una puerta de enlace con el exterior al estar conectada a una red Wi-Fi, manteniéndose emparejada con los nodos sensores. Al producirse una intrusión y estar activado el sistema la central comunicadora realizará sus funciones alertando al usuario final.

Regulación de voltaje

El voltaje utilizado por el módulo ESP-WROOM-32 es de 5V DC o 3.3V DC como se aprecia en la Tabla 2.5; por tal motivo se usará el módulo de regulación LM2596. El cual posee una perilla reguladora de voltaje la cual se ajustará a 5V DC para su aplicación en la central comunicadora. La distribución de pines del módulo LM2596 así como el esquemático del circuito se presentan en la Figura 2.24.

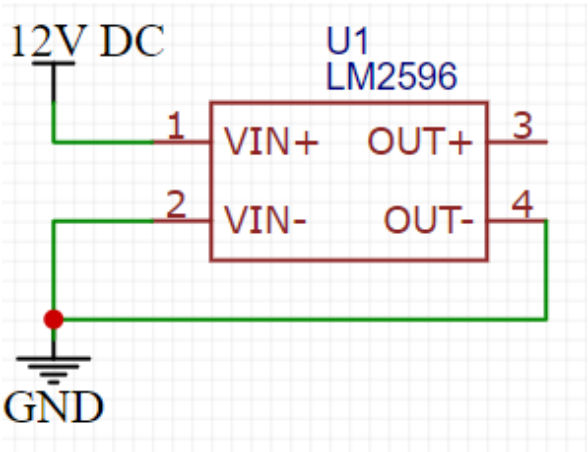


Figura 2.24. Circuito de regulación
Fuente: Elaboración propia

Circuito de activación de sirena

La activación de la alerta sonora o sirena se hará por intermedio de un módulo relay de 1 canal de activación con 5V DC, que cuenta con un circuito de protección para evitar corto circuitos. El circuito de activación de la sirena se aprecia en la Figura 2.25.

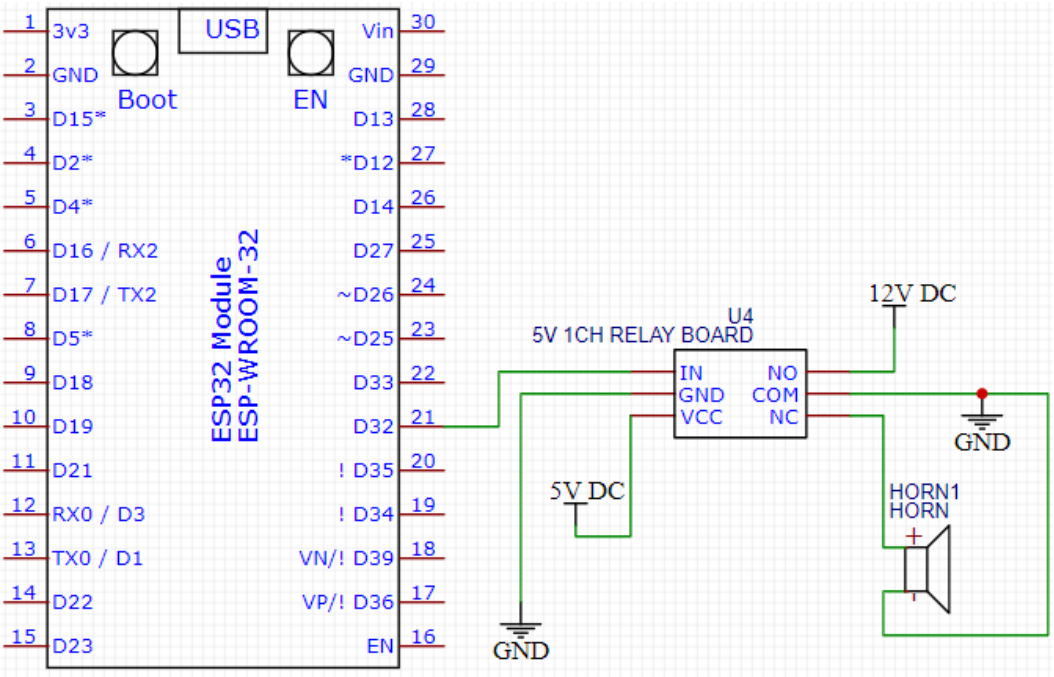


Figura 2.25. Circuito de activación de sirena
Fuente: Elaboración propia

El circuito actuará en caso la central comunicadora haya recibido una alerta por parte de los nodos sensores. En tal caso se emitirá una señal por intermedio del GPIO 21 del módulo ESP-WROOM-32 hacia el módulo relay activando el switch interno del mismo haciendo que conmute y active la alimentación a 12V DC de la sirena produciendo la alerta sonora del sistema que permanecerá activa por 90 segundos.

Indicador visual

Para efecto de indicar en el caso de activación o desactivación de la central, se colocan 2 led's de colores rojo y azul en la central controladora, los mismo que representan lo siguiente:

- Rojo

  Indica que el sistema se encuentra desarmado.

- Azul

  Indica que el sistema se encuentra armado.

En la Figura 2.26 se aprecia las conexiones con el módulo ESP-WROOM-32.

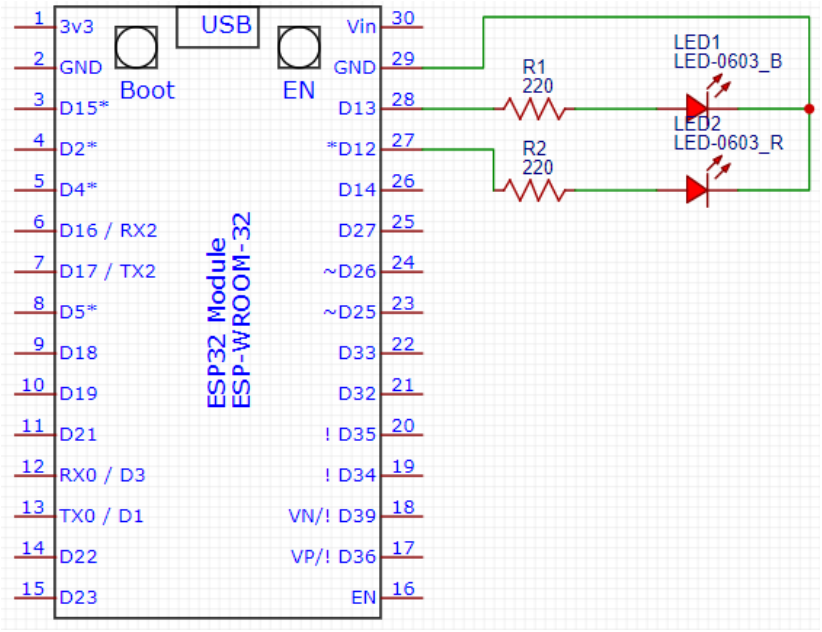


Figura 2.26. Circuito de conexión de led's
Fuente: Elaboración propia

Descripción del software utilizado

El software utilizado en el desarrollo del trabajo conlleva el uso del entorno de programación Arduino IDE y el uso de librerías hechas para dicha plataforma. Así como también el uso del software de control de versiones Git. Se detallarán los elementos a continuación:

- **Arduino IDE**

  Es el entorno de programación por excelencia de las tarjetas de desarrollo Arduino, es multiplataforma y de uso libre. Por tal motivo cuenta con una amplia comunidad de desarrolladores que brindar soporte y comparten conocimientos. Los lenguajes utilizados para la programación en este entorno son C y C++ con algunas variantes propias del IDE. Su aplicación en el presente trabajo está ligada a su versatilidad de uso y compatibilidad con diversas tarjetas de desarrollo en el mercado. Lo cual lo vuelve una excelente alternativa para el trabajo en cuestión. En la Figura 2.27 se puede visualizar una vista al software.

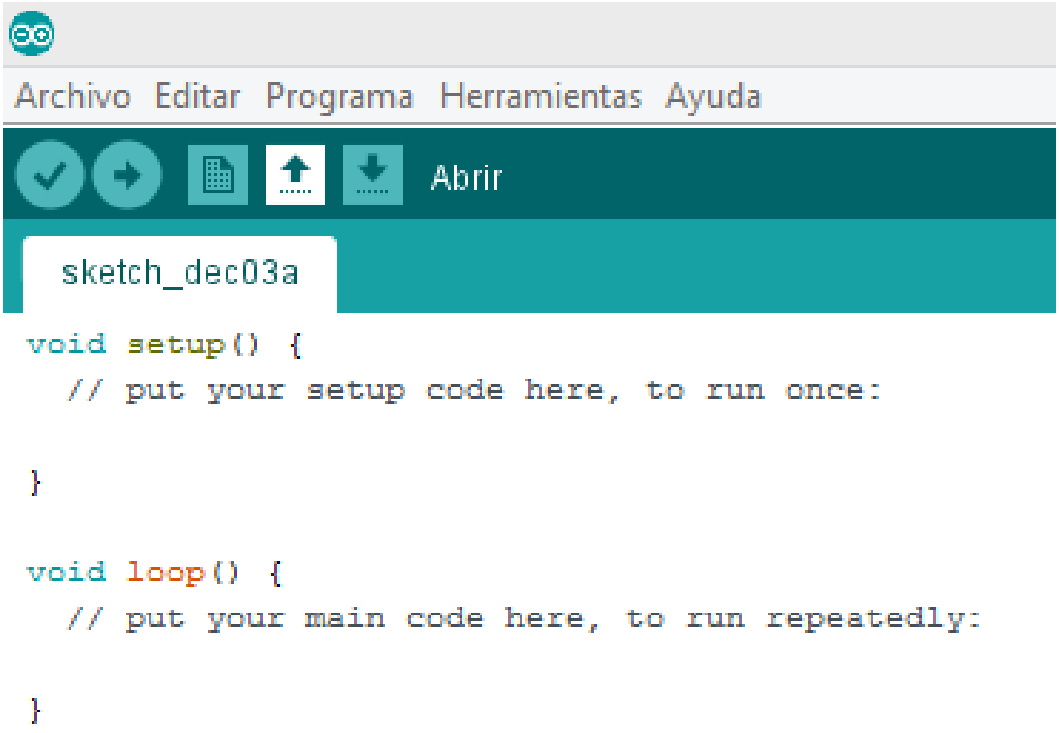


Figura 2.27. Entorno de Arduino IDE
Fuente: Elaboración propia

- **Git**

  Es un sistema de control de versiones creado por Linus Torvarlds y fue concebido con la idea de administrar los cambios que se generan en los proyectos de software y poder con ello evitar que la información se pierda o existan alteraciones que no puedan ser reversibles. Por otro lado la idea de tener un control de versiones se volvió fundamental en los trabajos colaborativos dado que Git permite que diversos desarrolladores trabajen de manera separada en las denominadas ”ramas”. De esta forma no alterar el desarrollo de algún compañero. Es de código libre y existen en la red muchos desarrolladores que crean una gran comunidad para compartir códigos y mejoras de algún software como es el caso de las redes Github y Gitlab.

  Git posee un entorno gráfico denominado Git Gui como se aprecia en la Figura 2.28 y un entorno de consola denominado Git Bash, cuyo ejemplo se visualizar en la Figura 2.29.

Git trabaja con repositorios o entornos virtuales en los que se almacena la información de los cambios realizados por los participantes del desarrollo de software. Su aplicación en el presente proyecto es la de clonación de repositorios para permitir la programación del módulo ESP-WROOM-32 con el Arduino IDE.

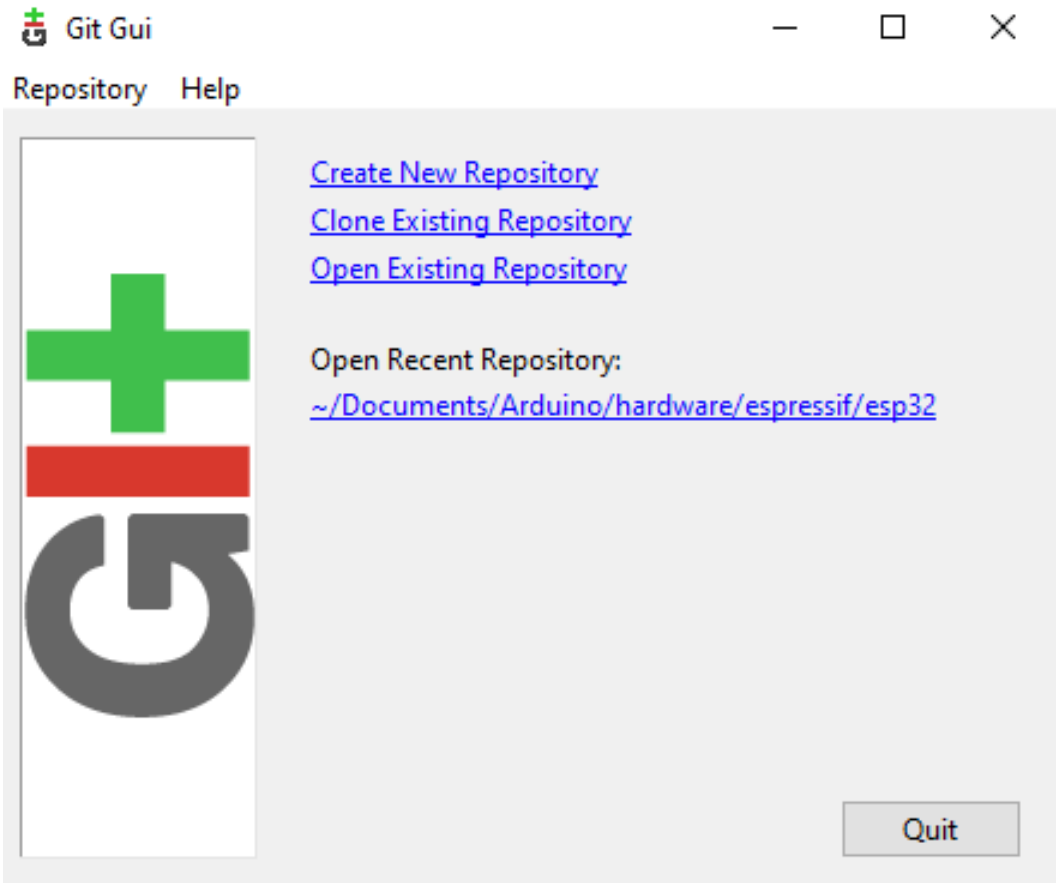


Figura 2.28. Entorno de Git Gui
Fuente: Elaboración propia

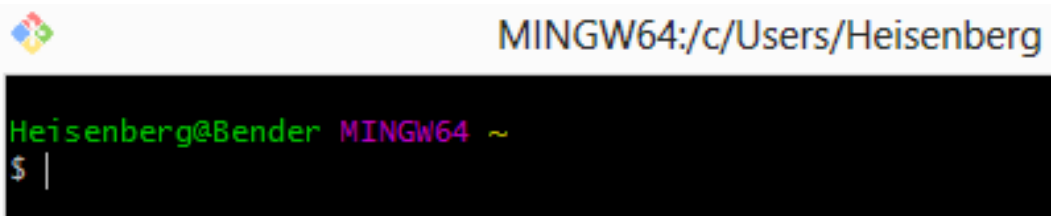


Figura 2.29. Entorno de Git Bash
Fuente: Elaboración propia

2.3.3. Implementación del sistema

El sistema implementado consta de 2 nodos sensores basado uno de ellos en un sensor PIR AM312 y el otro en un sensor magnético MC-38, ambos con la finalidad de detectar intrusiones a un determinado hogar. Todo ello basado en el módulo ESP-WROOM-32. Por otro lado la central comunicadora también está basada en el módulo ESP-WROOM-32.

En el presente apartado se detallará el procedimiento para la configuración del asistente o Bot del servicio de mensajería instantánea e implementación del sistema propuesto.

Creación y configuración del Bot

El servicio de mensajería instantánea provee la opción de creación de asistente virtual o Bot. El cual se configurará para efectos del presente desarrollo a manera de ”vigilante” dentro del hogar. Por tal motivo para ello se instalará la aplicación móvil Telegram y se iniciará una conversación con @BotFather que es el Bot propuesto por Telegram para la creación de nuevos Bots para los usuarios. Se iniciará la conversación utilizando el comando **/start** como se aprecia en la Figura 2.30.

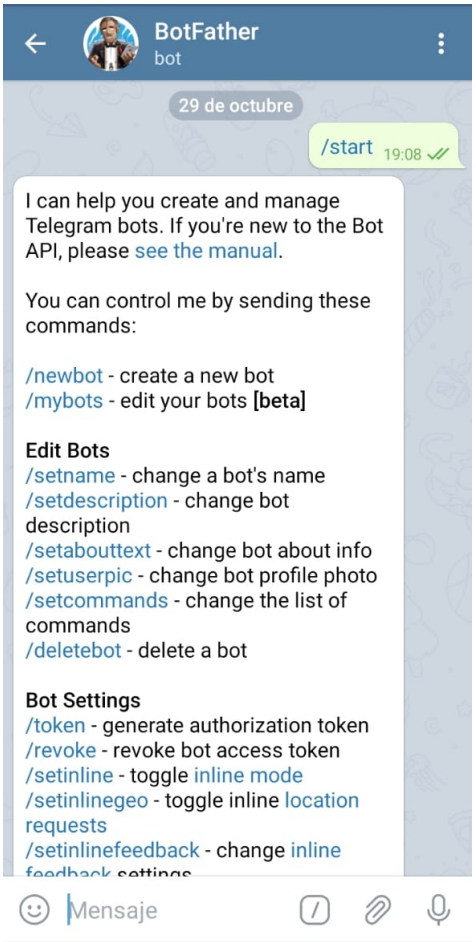


Figura 2.30. Comunicación inicial
Fuente: Elaboración propia

Una vez iniciada la comunicación con BotFather se procederá con la creación del Bot asistente enviándole el comando **/newbot** como se aprecia en la Figura 2.31. La respuesta del BotFather es la de consultar por el nombre que se colocará al Bot.

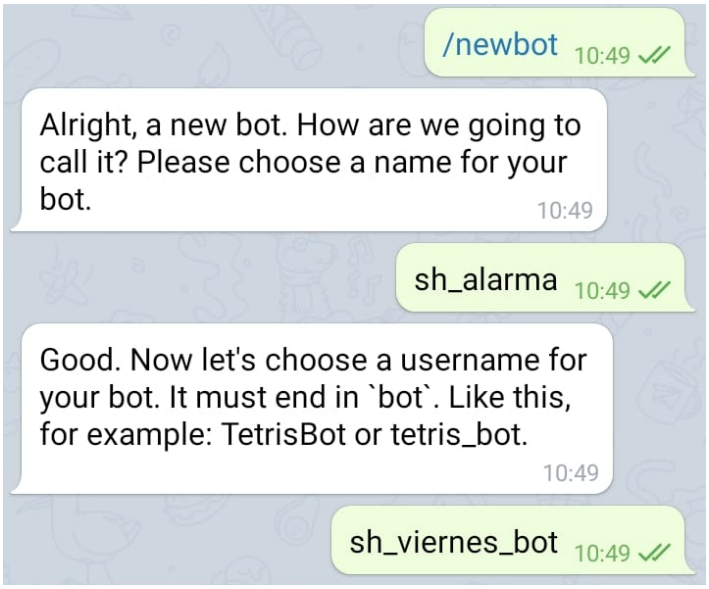


Figura 2.31. Creación de nuevo bot
Fuente: Elaboración propia

Para la implementación del sistema se usó el nombre **sh_ alarma** a manera de nombre corto y para el nombre de configuraciones se usará **sh_viernes_bot**. Una vez creado el nombre se hará uso del token para la futura configuración en el módulo ESP-WROOM-32 para ello se hará una solicitud a BotFather para que brinde el token utilizando el comando **/token**. Responderá preguntando respecto al Bot para el cual se hará la consulta, este procedimiento se aprecia en la Figura 2.32.

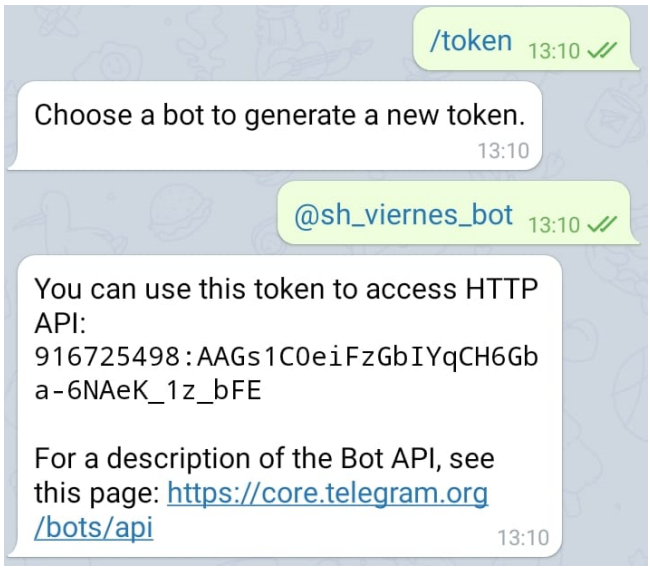


Figura 2.32. Obtención del token del Bot
Fuente: Elaboración propia

Los datos del token obtenido se usarán para la programación de la central comunicadora. Para que esta, haciendo uso del Wi-Fi pueda conectarse con el servicio de mensajería Telegram e identificándose con el Bot pueda generar una alerta al grupo creado por los residentes del hogar.

Es de importancia general la creación de un grupo para hacer que el mensaje de alerta sea general en caso suceda alguna intrusión. Para ello se generará un grupo el cual por motivos demostrativos del presente trabajo se denominará **Alarma**, en dicho grupo se agregará al Bot para que pueda hacer uso de la mensajería. En la Figura 2.33 se muestra el grupo creado con el Bot.

Para la configuración de los estados del sistema de alarma, se hará uso de los siguientes comandos:

- **/start:** Para el inicio de las configuraciones y mostrar el menú de opciones.
- **/alarma_on:** Para la activación o armado del sistema.
- **/alarma_off:** Para la desactivación o desarmado del sistema.

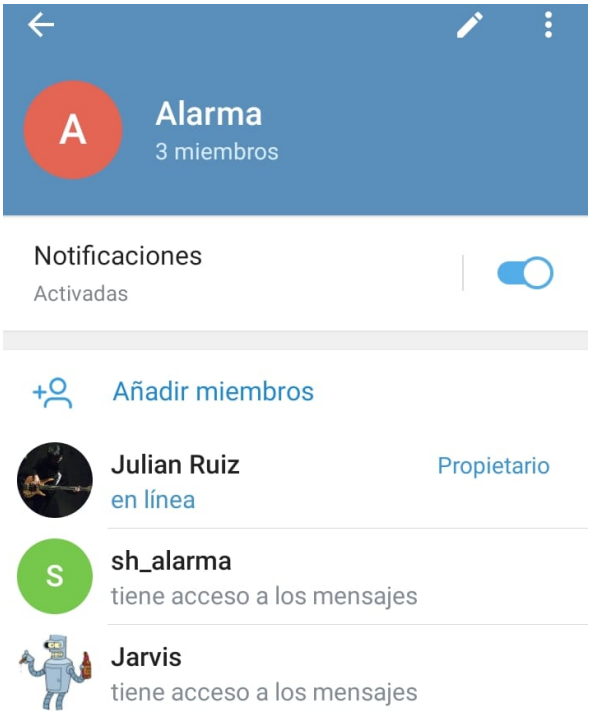


Figura 2.33. Creación de grupo de

Telegram
Fuente:Elaboración propia

Programación de los módulos

Los módulos programables que serán utilizados a lo largo de desarrollo del proyecto son los ESP-WROOM-32, para ello se utilizará la interfaz de programación Arduino IDE. Para lograr programar dichos módulos se requiere copiar el repositorio que contiene la información de la tarjeta en cuestión con la finalidad de hacer compatible el entorno. Para la instalación del módulo ESP-WROOM-32 y los demás módulos derivados del SoC ESP32 se realizará la instalación de Git y la última versión del Arduino IDE. Después de ello se clonará el repositorio de Github: **https://github.com/espressif/arduino-esp32** brindado por el fabricante de los módulos y SoC's, ESPRESSIF.

Se hará uso de Git Gui para la clonación del repositorio anteriormente mencionado como se aprecia en la Figura 2.34.

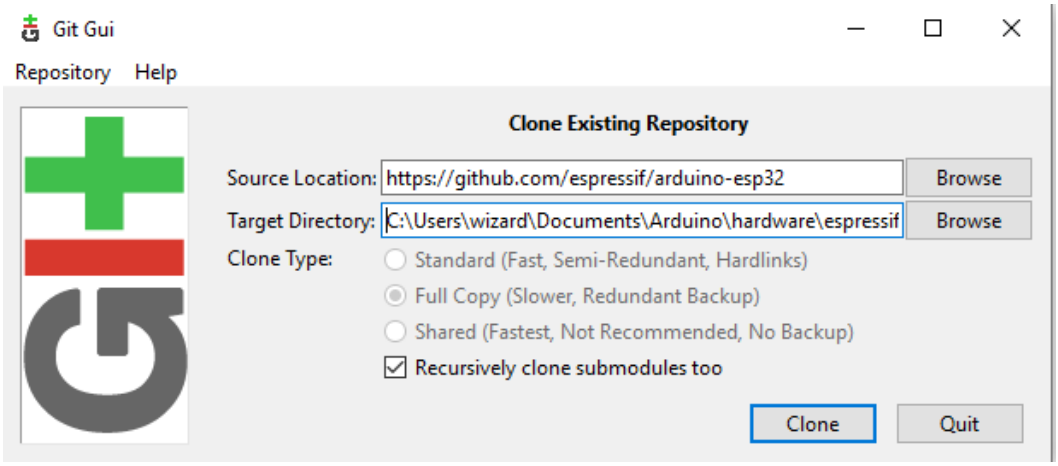


Figura 2.34. Clonación de repositorio ESP32 de ESPRESSIF
Fuente: Elaboración propia

Una vez clonado el repositorio se agregarán nuevos archivos a la carpeta destino. Entre ellos el más relevantes es uno denominado **get.exe** el cual se ejecutará para finalizar la instalación de los requisitos para la compatibilidad de los módulos y SoC's ESP32 con el entorno Arduino IDE. Las carpetas y archivos instalados se muestran en la Figura 2.35.

dist	14/06/2020 14:05	Carpeta de archivos	
esptool	14/06/2020 14:05	Carpeta de archivos	
mkspiffs	14/06/2020 14:05	Carpeta de archivos	
partitions	14/06/2020 14:00	Carpeta de archivos	
sdk	14/06/2020 14:00	Carpeta de archivos	
xtensa-esp32-elf	14/06/2020 14:04	Carpeta de archivos	
espota	14/06/2020 14:00	Aplicación	3,936 KB
espota	14/06/2020 14:00	Python File	10 KB
esptool	14/06/2020 14:00	Python File	144 KB
gen_esp32part	14/06/2020 14:00	Aplicación	3,262 KB
gen_esp32part	14/06/2020 14:00	Python File	21 KB
get	14/06/2020 14:00	Aplicación	5,090 KB
get	14/06/2020 14:00	Python File	6 KB
platformio-build	14/06/2020 14:00	Python File	11 KB

Figura 2.35. Archivos de ESP32 en Arduino
Fuente:Elaboración propia

Para la verificación de la correcta instalación de los componentes necesarios para la programación se comprobará abriendo el entorno Arduino IDE y en la pestaña: Herramientas >Placa se debe de hallar **ESP32 Arduino**. El cual contendrá todos los módulos ahora compatibles con Arduino IDE. Se aprecia muestra de ello en la Figura 2.36

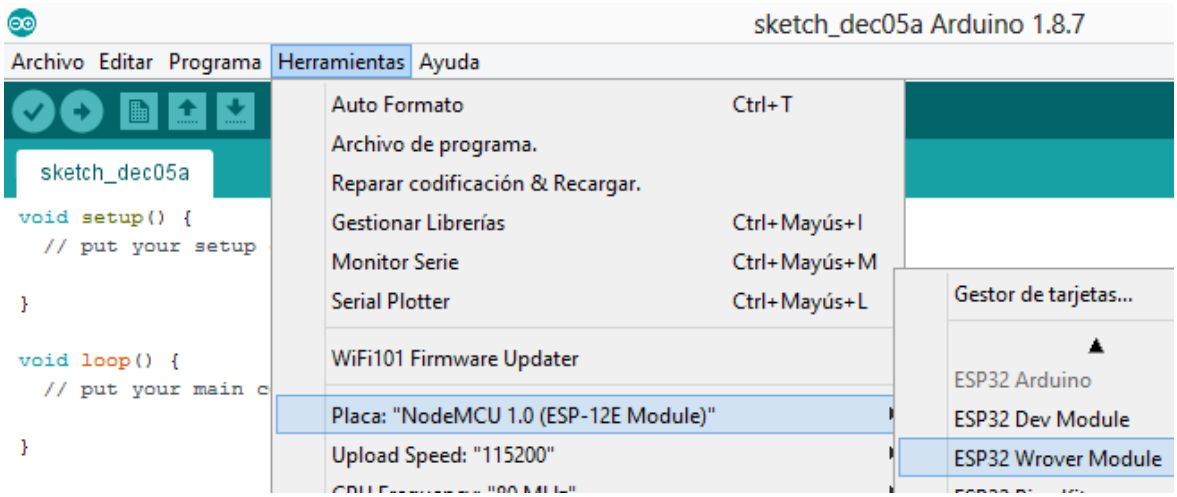


Figura 2.36. Comprobación de instalación de ESP32 en Arduino IDE
Fuente: Elaboración propia

Programación de nodos sensores

La programación de los **nodos sensores** es similar en estructuración para el caso de los basados en el sensor PIR AM312 y el sensor magnético MC-38. Para ello se plantea el siguiente orden del código medular:

- Importación de librerías
- Determinación de datos a transmitir
- Emparejamiento con la central comunicadora
- Inicio del protocolo ESP-NOW
- Envío de datos
- Confirmación de recepción.

Las librerías a importar para la programación de ambos nodos sensores son las siguientes: **esp_now.h**, **esp_wifi.h** y **WiFi.h** las cuales permitirán el uso de las herramientas de conexión a la red Wi-fi del hogar en el que será instalado. Además de permitir el uso del protocolo ESP-NOW en los módulos programados. En la Figura 2.37 se visualizan las librerías mencionadas anteriormente en el entorno de programación Arduino IDE.

```
#include <esp_now.h>
#include <esp_wifi.h>
#include <WiFi.h>
```

Figura 2.37. Librerías importadas
Fuente: Elaboración propia

Los datos a ser transmitidos son 2 básicamente la identificación del nodo sensor que es determinado por la variable **num_sensor**. Según las características del sistema se permite un máximo de 10 nodos sensores encriptados. Para el caso de la variable **a** contendrá el valor a transmitirse que para efectos del trabajo se planteará el número **1** representando activación. Ello se aprecia en la Figura 2.38.

```
//------------Datos a transmitir---------------//
typedef struct mensajes {
  int num_sensor;
  int a;
}mensajes;

mensajes datos;
//---------------------------------------------//
```

Figura 2.38. Datos a ser transmitidos
Fuente: Elaboración propia

El emparejamiento con la central comunicadora se realiza a través de la dirección MAC(requisito del protocolo ESP-NOW) y la clave de encriptación. Se declaran las variables correspondientes con los valores que se usarán en el desarrollo del proyecto. Se visualiza lo mencionado en la Figura 2.39.

```
uint8_t broadcastAddress[] = {0x24,0x6F,0x28,0x10,0x4E,0x80};//MAC de la central comunicadora
uint8_t key[16] = {0,255,1,1,1,1,1,1,1,1,1,1,1,1,1,1};
```

Figura 2.39. Declaración de los valores para emparejamiento con la central comunicadora
Fuente: Elaboración propia

Para completar el emparejamiento son necesarias las líneas de código mostradas en la Figura 2.40, las cuales realizan el emparejamiento con la central comunicadora y en caso que no se logre la primera vez reiniciará el módulo e intentará nuevamente.

```
memcpy(peerInfo.peer_addr, broadcastAddress, 6);
memcpy(peerInfo.lmk, key, 16);
peerInfo.encrypt = true;

if (esp_now_add_peer(&peerInfo) != ESP_OK){
Serial.println("Fallo en emparejamiento");
return;}
```

Figura 2.40. Emparejamiento con la central comunicadora
Fuente: Elaboración propia

Una vez realizado el emparejamiento del nodo sensor con la central comunicadora se procede con el inicio del protocolo ESP-NOW dentro del módulo para alistar una futura transferencia de información. Para ello se hace uso del código mostrado en la Figura 2.41 el cual muestra la manera de inicio del protocolo y en caso no logre el inicio del mismo se procederá a reiniciar para volver a intentarlo.

```
//---------------Inicio de ESP-NOW-----------------//
if(esp_now_init()!=0)
{Serial.println("Conexión no establecida");
 ESP.restart();}
else
{ Serial.println(" ");
  Serial.println("ESP-NOW iniciado");}
//-------------------------------------------------//
```

Figura 2.41. Inicio del protocolo ESP-NOW
Fuente: Elaboración propia

El envío de datos es primordial para el desarrollo del proyecto y dicho proceso se lleva a cabo digitando las siguientes líneas de código expuestas en la Figura 2.42. El código realiza una confirmación de salida de la información; sin embargo no logra confirmar que el mensaje haya sido recepcionado por la central comunicadora.

```
datos.num_sensor = 2; //Número de sensor
datos.a= 2;//datos de alerta

esp_err_t result = esp_now_send(broadcastAddress, (uint8_t *) &datos, sizeof(datos));

if (result == ESP_OK) {
      Serial.println("Enviado");
    }
    else {
      Serial.println("Error enviando los datos");
    }
delay(1000);
```

Figura 2.42. Envío de datos a la central comunicadora
Fuente: Elaboración propia

Para culminar con el proceso de programación es necesario tener una confirmación de recepción de parte de la central comunicadora; para ello es necesario que se aplique una función de confirmación. En caso que el mensaje no sea recepcionado el nodo sensor se reiniciará hasta lograr una confirmación. Caso contrario si se logra la correcta recepción ingresará en el modo **deep sleep** o en su traducción al español **sueño profundo**. El cual mantendrá en su mínimo consumo de energía el módulo ESP-WROOM-32 reduciendo el consumo energético del nodo sensor al mínimo.

Para activar nuevamente el módulo es necesario que reciba nuevamente una señal de activación por el GPIO 4. En la Figura 2.43 se detalla en código el procedimiento descrito.

```
void envio_datos(const uint8_t *mac_addr, esp_now_send_status_t status) {
 Serial.println("Estado de paquete enviado");
 if(status == ESP_NOW_SEND_SUCCESS)
 {digitalWrite(2,HIGH);
  delay(1500);
  digitalWrite(2,LOW);
  esp_sleep_enable_ext0_wakeup(GPIO_NUM_4, 0);
  esp_deep_sleep_start();}

 else
 {Serial.println("No recepcionado");
  ESP.restart();}
}
```

Figura 2.43. Confirmación de recepción de los datos
Fuente: Elaboración propia

Implementación de los nodos sensores

La implementación de los nodos sensores se llevaron a cabo haciendo uso los circuitos que se esquematizaron en la Figura 2.20 y Figura 2.21. Se utilizaron materiales de fácil adquisición en el mercado para su ensamble tales como caja de paso plástica para el casco que encapsula y protege los componentes, taladro para dar forma y hacer que encajen los materiales acorde a la forma del contenedor, placas de baquelita para el montaje de los componentes y silicona líquida para pegar y completar espacios restantes en el contenedor. Respetando el diseño de vivienda planteado y los puntos de instalación vistos en la Figura 2.3 se implementó los nodos sensores en los siguientes puntos:

- Nodo sensor magnético en la entrada principal
- Nodo sensor PIR en la sala principal

En la Figura 2.44 se aprecia la implementación del **nodo sensor magnético**.

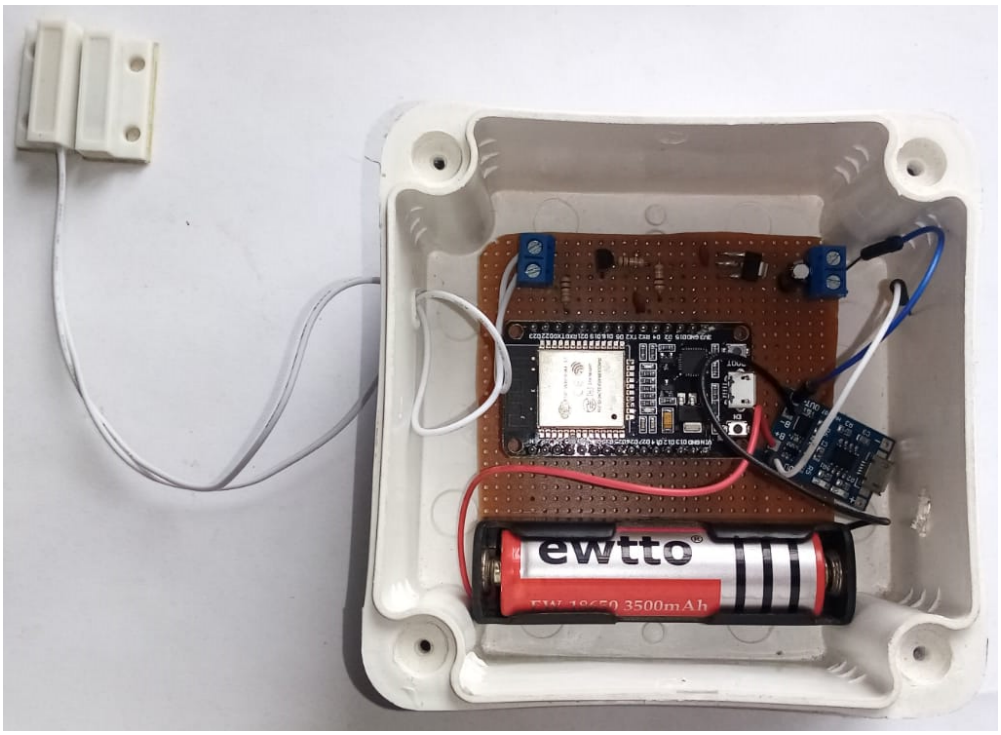


Figura 2.44. Implementación de nodo sensor magnético
Fuente: Elaboración propia

En la Figura 2.45 se muestra la implementación del nodo sensor **PIR**.

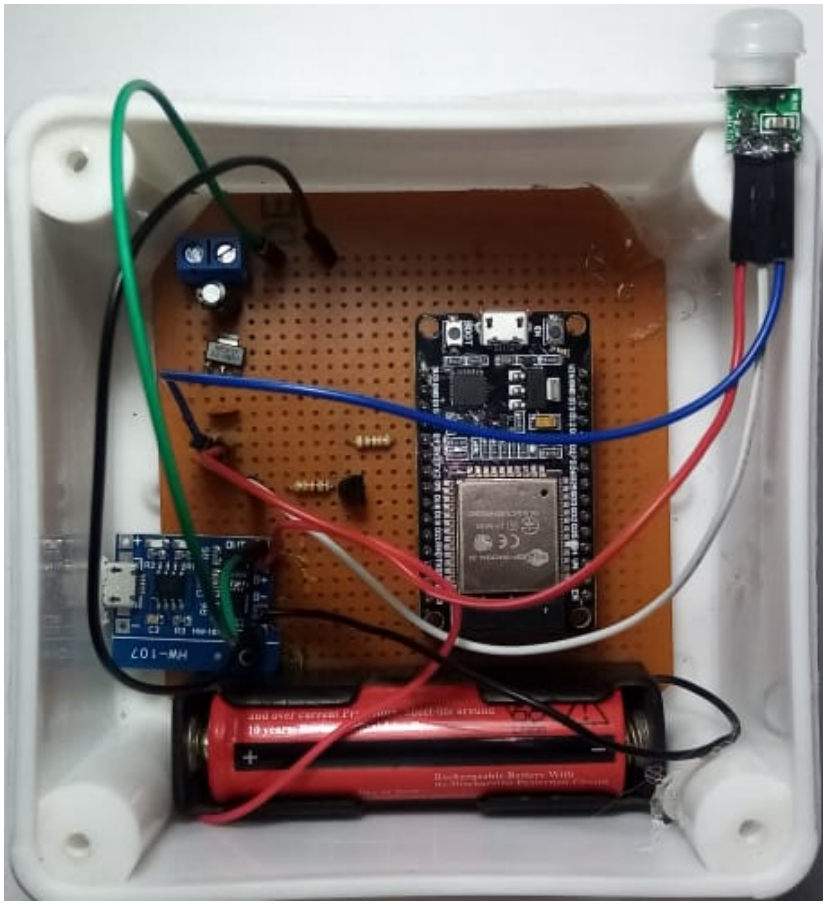


Figura 2.45. Implementación de nodo sensor PIR
Fuente:Elaboración propia

Programación de la central controladora

La central controladora contiene el código que hará posible la recepción de la información enviada por los nodos sensores. Además de transferir la información al servicio de mensajería instantánea Telegram. El proceso que sigue se detalla a continuación:

- Importación de librerías
- Datos a ser recibidos
- Datos de conexión a Bot de Telegram
- Conexión a internet e inicio de protocolo ESP-NOW
- Recepción de datos
- Envío de alerta a Telegram

Las librerías importadas para el funcionamiento de la central controladora son: **UniversalTelegramBot.h**, **WiFi.h**, **WiFiClientSecure.h**, **esp_now.h**, **esp_wifi.h** y **ArduinoJson.h**. Adicionalmente se define el **chatID** del grupo de Telegram creado al que se enviarán las alertas. En la Figura 2.46 se aprecian las líneas de código programadas. Los datos a ser recibidos deben de tener la misma estructura que los enviados por los nodos sensores. De tal forma se mantiene lo mostrado en la Figura 2.38 en las líneas de código.

```
#include <UniversalTelegramBot.h>
#include <Arduino.h>
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <esp_now.h>
#include <esp_wifi.h>
#include <ArduinoJson.h>
#define CHAT_ID "-318676680"
```

Figura 2.46. Librerías importadas
Fuente:Elaboración propia

Los datos para la conexión con el servicio de mensajería Telegram son requeridos por la librería y son detallados en las líneas de código. El token del Bot de Telegram no debe de ser compartido; sin embargo por motivos del presente estudio se presentarán con fines académicos. En la Figura 2.47 se visualiza el código escrito en el entorno de programación.

```
//------------BOT-INFO----------------------//
#define BOTtoken "916725498:AAGs1C0eiFzGbIYqCH6Gba-6NAeK_1z_bFE"
WiFiClientSecure client;      // Instancia para la red WiFi
UniversalTelegramBot bot(BOTtoken, client); // Instancia para el Bot Telegram
```

Figura 2.47. Datos para conexión del Bot
Fuente:Elaboración propia

Para mantener la conexión Wi-Fi y utilizar el protocolo ESP-NOW al mismo tiempo se requiere que la configuración del módulo ESP-WROOM-32 sea AP+STA (Punto de acceso y estación). Posterior a ello se puede iniciar la conexión Wi-Fi e iniciar ESP-NOW sin mayores complicaciones. De igual manera que los nodos sensores si no se establece el inicio del protocolo ESP-NOW el módulo se reiniciará hasta conseguir una correcta iniciación. Las líneas de código de lo anteriormente mencionado se ubican en la Figura 2.48.

```
WiFi.mode(WIFI_AP_STA); // AP+STA en simultáneo

//--------------- Conexión a WIFI------------------//

WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(1000);
    Serial.print(".");
  }
  Serial.print("Station IP Address: ");
  Serial.println(WiFi.localIP());
  Serial.print("Wi-Fi Channel: ");
  Serial.println(WiFi.channel());

//---------------Inicio de ESP-NOW-----------------//
if(esp_now_init()!=0)
{Serial.println("Conexión no establecida");
 ESP.restart();}
else
{ Serial.println(" ");
  Serial.println("ESP-NOW iniciado");}
//-------------------------------------------------//
```

Figura 2.48. Conexión a internet e inicio del protocolo ESP-NOW
Fuente:Elaboración propia

Los datos al recepcionarse envían una confirmación a los nodos indicando que pueden ingresar al modo de reposo o sueño profundo y ahorrar batería. Una vez que se tenga el dato en la central controladora hará que el sistema lo procese y determine si es factible de activación. En caso que el sistema se encuentre armado y reciba una señal de algún nodo sensor, este se activará y producirá la alerta al servicio de mensajería y la alarma sonora. En caso de no estar armado simplemente lo ignorará. El código usado se visualiza en la Figura 2.49.

Si se dan las condiciones para el envío de la alerta, las cuales son la activación del usuario y la detección de intrusión por parte de los nodos sensores se enviará el mensaje vía Telegram indicando que está aconteciendo una intrusión. El código responsable de enviar el mensaje se detalla en la Figura 2.50.

```
esp_now_register_recv_cb([](const uint8_t *mac, const uint8_t *array_datos, int len) {

    memcpy(&datos,array_datos, sizeof(datos));

    if (datos.num_sensor==1){
       alertal = datos.a;
       all= !all;
       Serial.println(alertal);

    }
    else if (datos.num_sensor==2){
        alerta2 = datos.a;
        al2= !al2;
        Serial.println(alerta2);
    }
  });

}
```

Figura 2.49. Recepción de alertas
Fuente:Elaboración propia

```
if (activacion_alarma ==true && (all==true || al2==true))
{bot.sendMessage("-318676680","Intrusión detectada");
```

Figura 2.50. Código para envío de mensaje a Telegram
Fuente:Elaboración propia

Implementación de la central comunicadora

La implementación de la central comunicadora se realizó haciendo uso del circuito mostrado en la Figura 2.25. Al igual que los nodos sensores se usaron materiales de bajo costo como cajas de paso, pistola de silicona y demás materiales que se pueden ubicar en el hogar o en ferreterías cercanas. Respetando el modelo de vivienda propuesta en la Figura 2.3 se instaló la central controladora en el ambiente de la cocina que está ubicado a 12m y 5m del nodo sensor magnético y nodo sensor PIR de manera respectiva.

En la Figura 2.51 se aprecia la implementación de la central comunicadora.

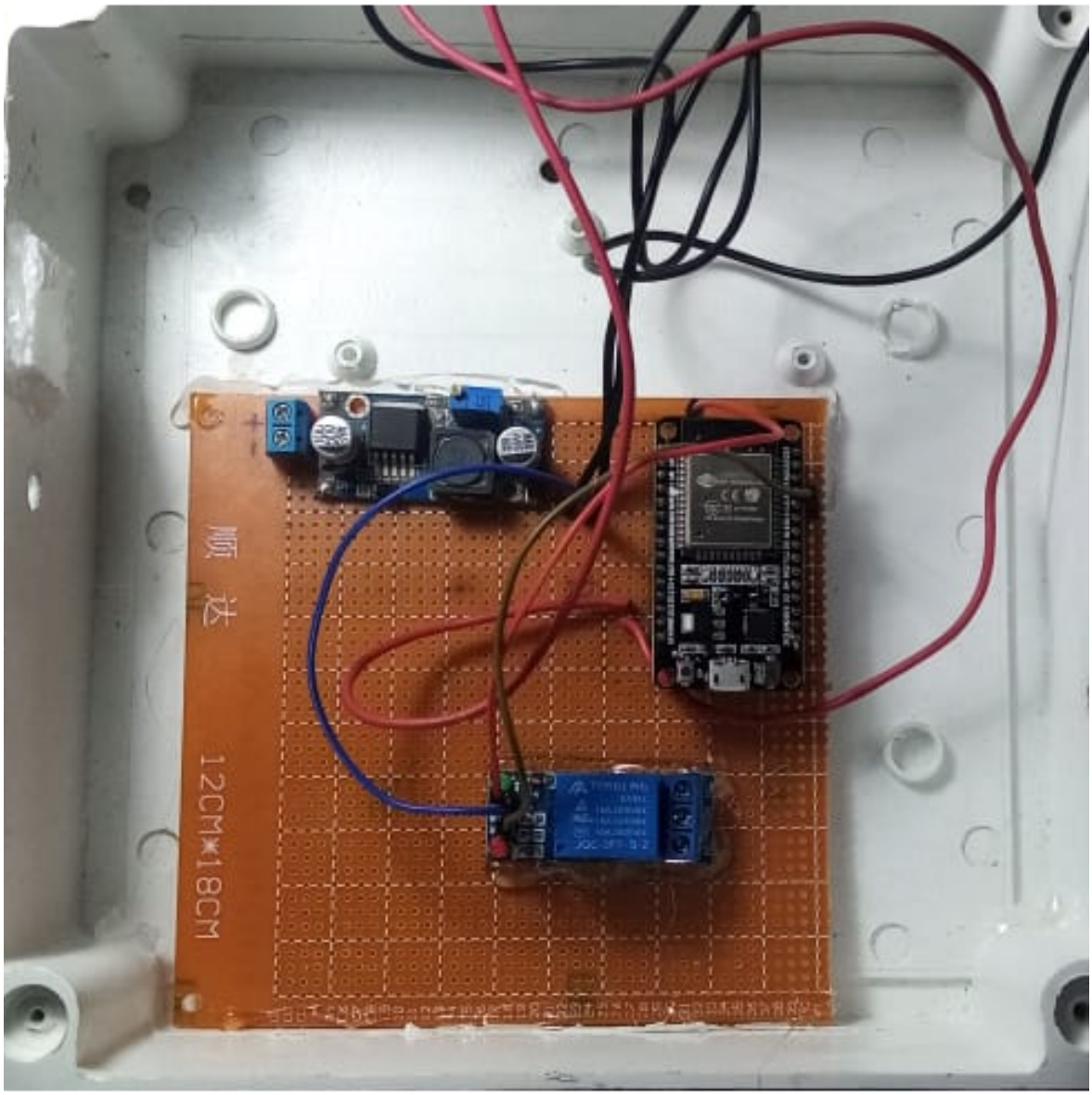


Figura 2.51. Implementación de central comunicadora
Fuente: Elaboración propia

2.4. Pruebas y Resultados

Las pruebas realizadas en el sistema propuesto se realizaron de manera independiente en los nodos sensores y en la central comunicadora. Las mediciones de tiempo se realizaron usando el cronómetro de un teléfono móvil y redondeando al primer decimal.

2.4.1. Pruebas realizadas en el nodo sensor magnético

El sensor magnético una vez activado demora un tiempo estimado y referencial de 3 segundos en llegar a la central comunicadora y activar la sirena. Para realizar las pruebas se tomaron muestras de 100 intrusiones simuladas en la entrada principal. Las pruebas fueron tomadas en 2 días y en diferentes condiciones. En el caso del día 1 se tomaron 50 pruebas bajo el escenario de batería recién cargada. En la Figura 2.52 se aprecian los resultados obtenidos.

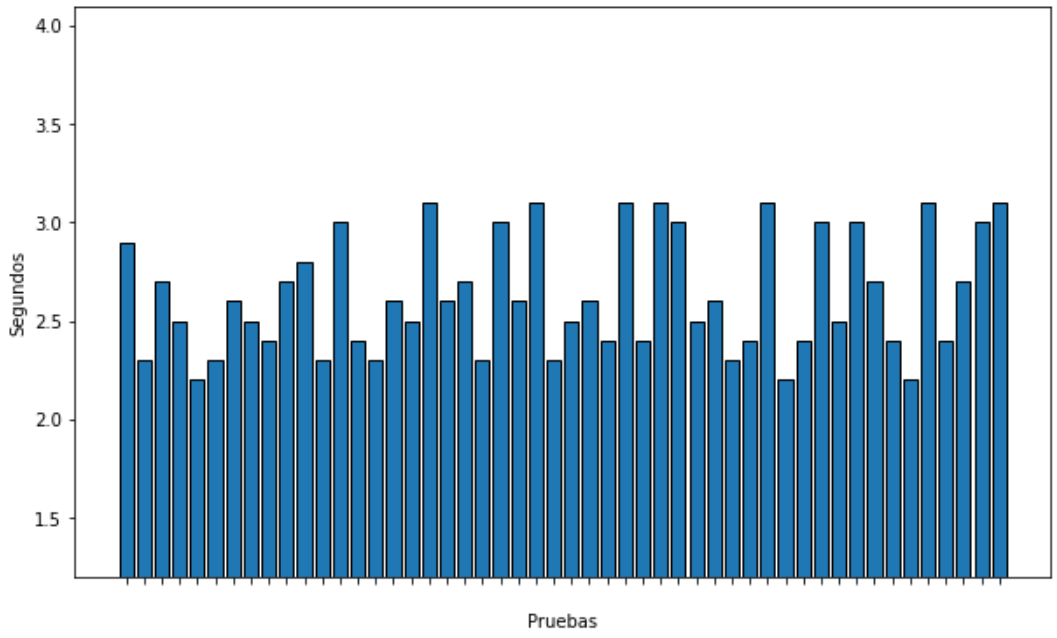


Figura 2.52. Pruebas con batería cargada en el nodo sensor magnético
Fuente: Elaboración propia

En el caso del día 2 se tomaron las 50 pruebas restantes. Las pruebas se realizaron habiendo pasado 3 días de uso del nodo sensor. Los resultados de las muestras se pueden apreciar en la Figura 2.53.

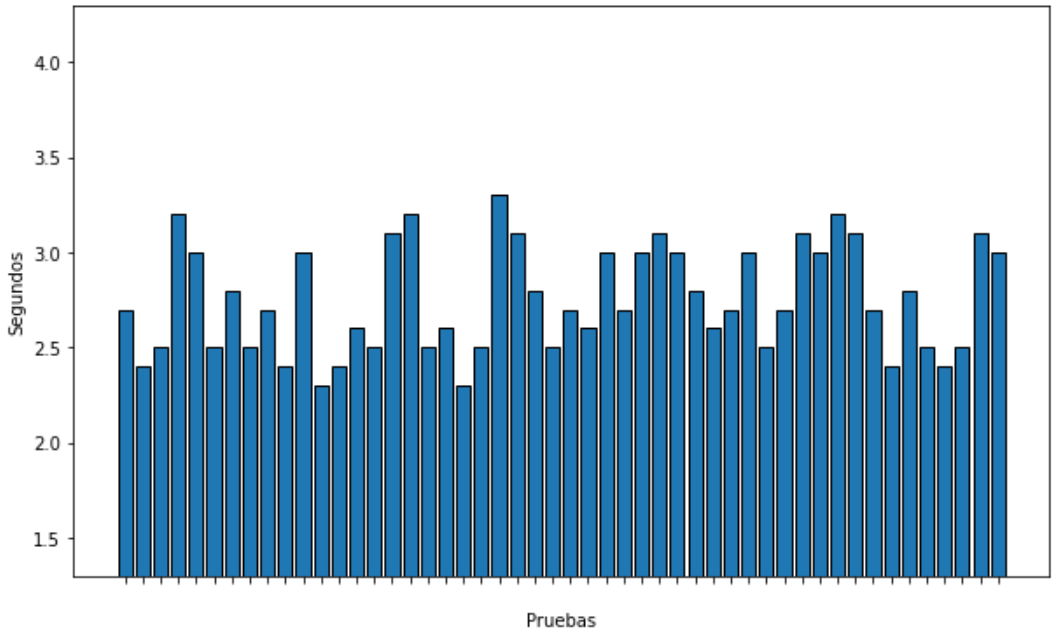


Figura 2.53. Pruebas con batería en 3 días de uso en el nodo sensor magnético
Fuente: Elaboración propia

El balance de las 100 muestras tomadas se visualiza en la Figura 2.54. Se interpreta de la gráfica mostrada que el 83 % del total de pruebas realizadas se rigen a respuestas menores a 3 segundos. Por otro lado el 17 % de las pruebas supera los 3 segundos de tiempo, lo cual reduce el rendimiento. Se denota que la gran parte de las muestra superiores a 3 segundos se dieron en las pruebas realizadas a 3 días de haberse cargado el nodo sensor.

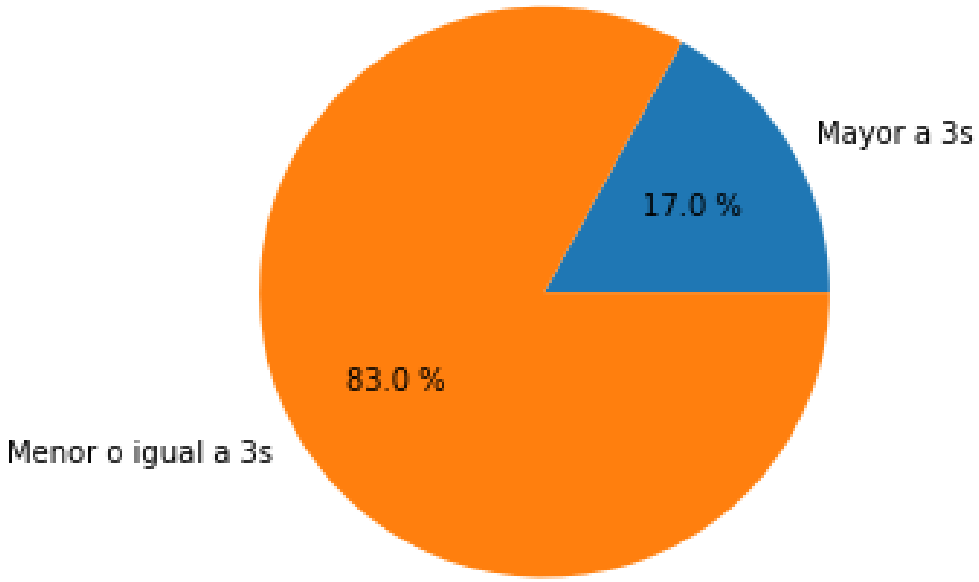


Figura 2.54. Pruebas totales realizadas en el nodo sensor magnético
Fuente: Elaboración propia

2.4.2. Pruebas realizadas en el nodo sensor PIR

De manera similar al nodo sensor magnético se han realizado un total de 100 pruebas de intrusiones realizadas con el nodo sensor PIR. Se separan las muestras en 2 grupos de 50 realizadas en 2 días. Se miden 3 segundos referenciales que toma el proceso de envío de la alerta y posterior activación de la sirena. Los resultados de las muestras obtenidas en el día 1 con batería recién cargada se aprecian en la Figura 2.55.

Respecto al día 2 y habiendo pasado 3 días de la última carga completa del nodo sensor, se aprecian los resultados de las muestras obtenidas en la Figura 2.56.

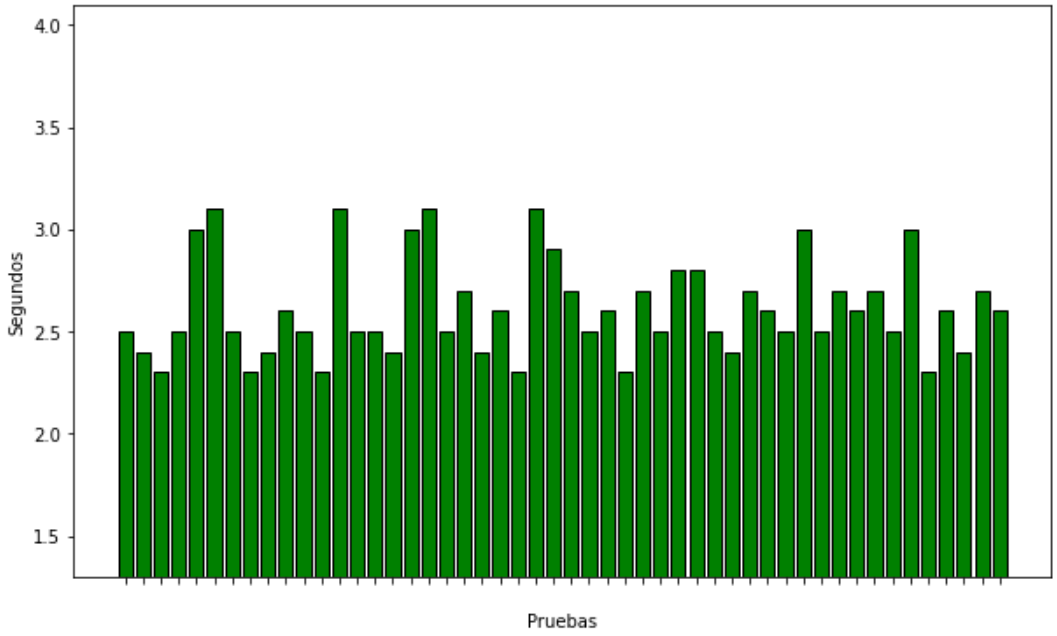


Figura 2.55. Pruebas con batería cargada en el nodo sensor PIR
Fuente: Elaboración propia

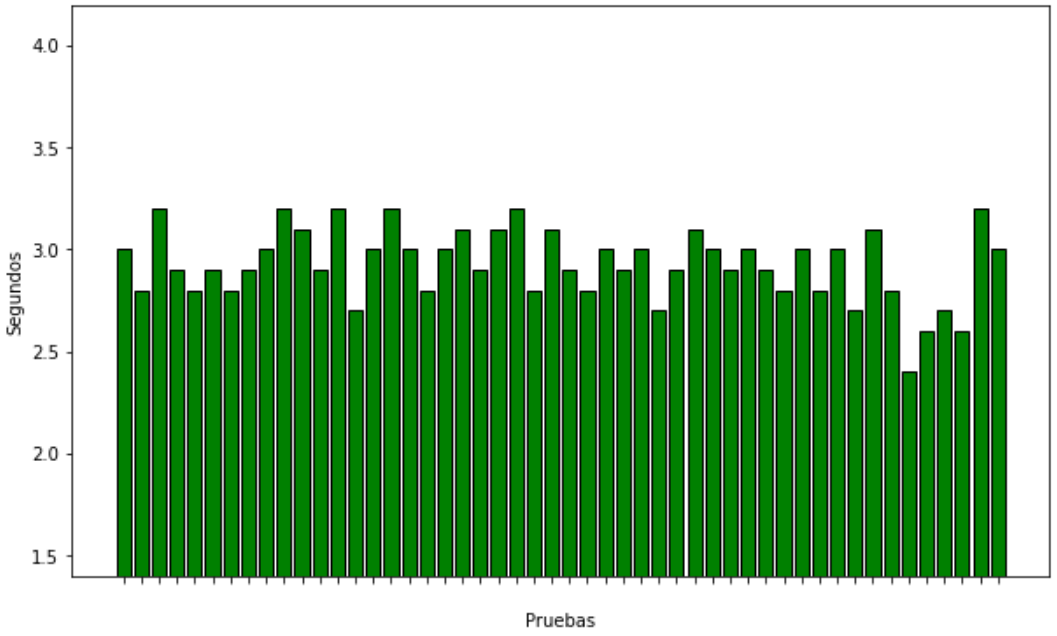


Figura 2.56. Pruebas con batería en 3 días de uso en el nodo sensor PIR
Fuente: Elaboración propia

Los resultados obtenidos de las 100 pruebas realizadas en el nodo sensor PIR en ambos escenarios tanto de batería llena como de batería baja arrojan que el 84 % de las pruebas son menores o iguales a 3 segundos. El 16 % de las pruebas superan los 3 segundos referenciales. Se puede denotar que el porcentaje de muestras mayores a 3 segundos es similar al nodo sensor magnético. Se aprecian los resultados en la Figura 2.57.

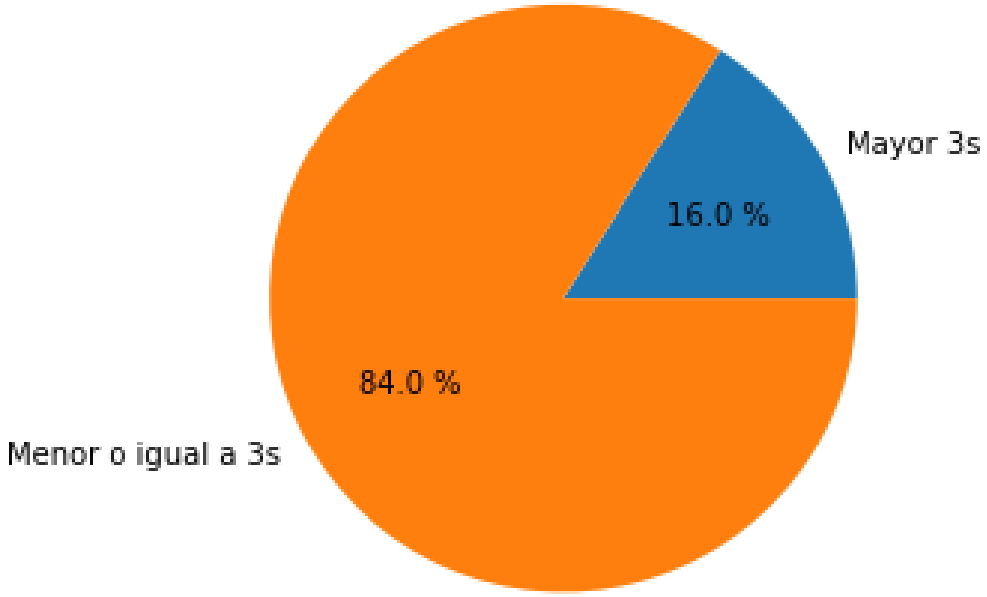


Figura 2.57. Pruebas totales realizadas en el nodo sensor PIR
Fuente: Elaboración propia

2.4.3. Pruebas realizadas en la central comunicadora

En el caso de la central comunicadora se realizaron las pruebas en base al tiempo que demora en remitir el mensaje de alerta al servicio de mensajería, el cual es de 5 segundos en promedio desde que la alerta es recibida por la central. Las pruebas fueron realizadas en 2 grupos de 50 y en 2 días diferentes. Los resultados obtenidos de las 50 pruebas realizadas en el día 1 se aprecian en la Figura 2.58.

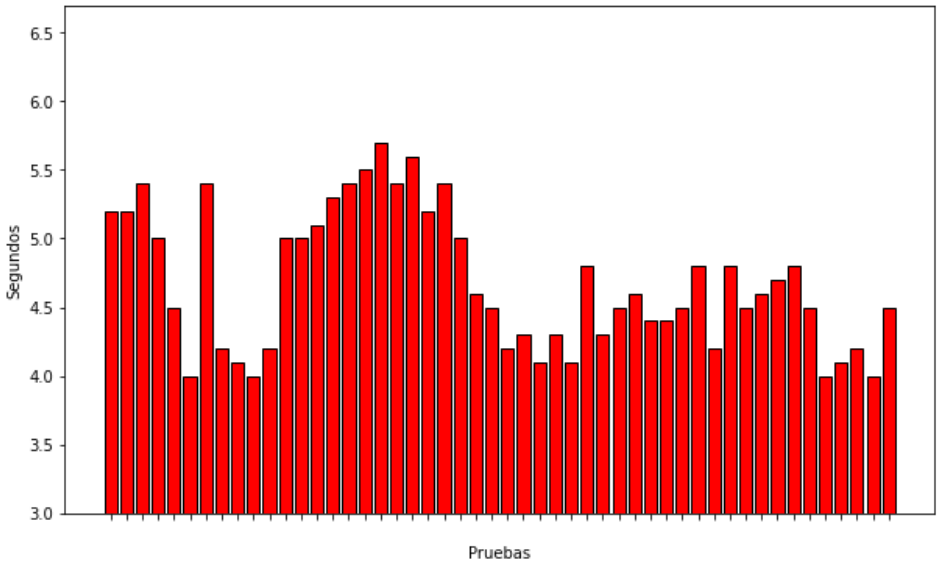


Figura 2.58. Pruebas realizadas en la central comunicadora - día 1
Fuente: Elaboración propia

Los resultados de las muestras obtenidas en el día 2 se aprecian en la figura 2.59.

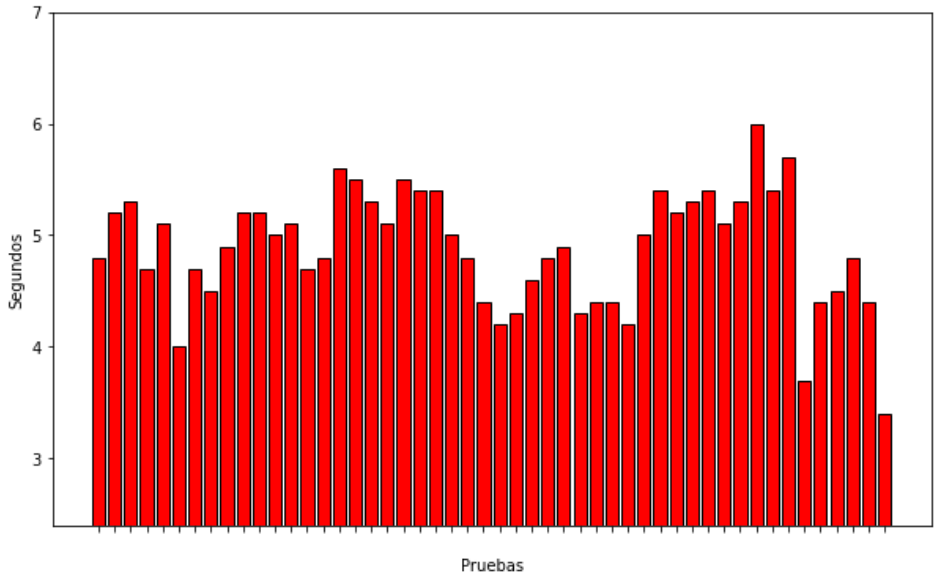


Figura 2.59. Pruebas realizadas en la central comunicadora - día 2
Fuente: Elaboración propia

Los resultados totales de las 100 pruebas realizadas en los 2 días, determinaron que el 34 % del total de pruebas tomó más de 5 segundos en realizar el envío del mensaje de alerta. Por otro lado el 66 % de las pruebas demoraron un tiempo de 5 segundos o inferior a ello. Se denotan gráficamente los resultados en la Figura 2.60.

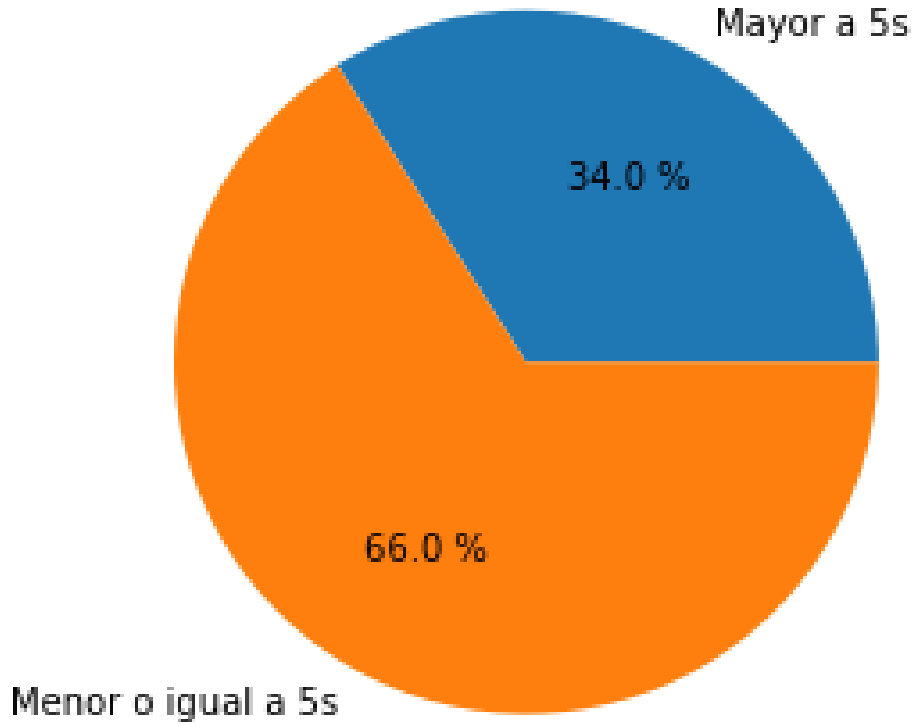


Figura 2.60. Pruebas totales realizadas en la central comunicadora
Fuente: Elaboración propia

2.4.4. Tabla de costos

Los costos planteados en la Tabla 2.6 son acorde a lo gastado en la compra de materiales para la implementación del prototipo propuesto en el presente trabajo.

Tabla 2.6
Tabla de costos de materiales

Material	Cantidad	Precio (S/.)	Total (S/.)
ESP32	3	15	45
Cajas de paso chicas	2	8	16
Baterías Li-ion	2	8	16
Reguladores LM2596	1	10	10
Módulos de carga TP4056	2	3.5	7
Sirena	1	30	30
Caja de paso mediana	1	14	14
Módulo relay 5V	1	1.5	1.5
Fuente de 12v	1	5	5
Sensor magnético MC-38	1	3	3
Sensor PIR AM312	1	2.5	2.5
Electrónica general	1	15	15
Baquelita chica	1	2	2
Baquelita mediana	1	3	3
Total			170

Fuente: Elaboración propia

CONCLUSIONES

- Se concluyó que el prototipo presentado cumple con los estándares establecidos respecto a funcionamiento y costo. Funciona de manera óptima en viviendas del distrito de Villa el Salvador y distritos aledaños. Es además extrapolable a viviendas de características similares.

- Se determinó que los componentes utilizados son los ideales para el desarrollo del sistema debido a su fácil ubicación en el mercado, bajo costo y consumo de energía. El dimensionamiento del sistema se determinó en base a las medidas de una vivienda promedio del distrito de Villa el Salvador.

- Se determinó que la red de nodos sensores independientes implementada funciona de manera rápida conteniendo la información de alerta. Se aseguró la compatibilidad con diversos dispositivos debido al servicio de mensajería instantáneo usado.

- Se concluyó que la instalación de los dispositivos se realizó en los puntos adecuados de la vivienda modelo utilizada, obteniendo alertas rápidas y efectivas manteniendo un bajo margen de error respecto a las pruebas realizadas. En el balance de costos se concluye que el sistema propuesto es favorable en contraste con los sistemas comerciales existentes.

RECOMENDACIONES

- Para reducir al mínimo el margen de error, se recomienda tratar en la medida de lo posible ubicar los nodos sensores en línea de vista con la central comunicadora y evitar que hayan obstáculos de concreto o paredes entre ambos dispositivos.

- Se recomienda ubicar la central comunicadora en un punto de difícil acceso para personas ajenas a la propiedad de manera tal que se puedan evitar posibles vulneraciones debido a ello, de preferencia no mostrar el lugar de ubicación a terceros.

- Para mejorar el diseño se recomienda realizar la implementación utilizando componentes superficiales e implementar las tarjetas a base de materiales más resistentes. De igual manera reducir el consumo energético aún más.

BIBLIOGRAFÍA

Arequipa Cunalata, D. A. (2019). *Desarrollo de un prototipo de sistema de seguridad contra intrusos utilizando protocolos de iot sobre la plataforma zolertia remote* (B.S. thesis). Quito, 2019.

Bo True Activities SL. (2020). *Comparativa entre sigfox y lorawan.* Descargado 24/11/2020, de https://botrueactivities.com/comparativa-entre-sigfox-y-lorawan/

Camps Sinisterra, C., y Oriol Allende, A. (2012). La nube: oportunidades y retos para los integrantes de la cadena de valor. *Management Solutions. Recuperado de https://www. managementsolutions. com*.

ESPRESSIF. (2016). *Esp-now user guide.* Descargado 15/09/2020, de https://www.espressif.com/sites/default/files/documentation/esp-now_user_guide_en.pdf

FIGUEROA MARÍN, I. (2020). Manual de prácticas esp32.

Gordon Colbach. (2013). *Zigbee characteristics.* Descargado 25/11/2020, de http://www.tutorial-reports.com/wireless/zigbee/zigbee-characterstics.php

Herrador, R. E. (2009). Guía de usuario de arduino. *Universidad de Córdoba*, *13*.

Herrera Chávez, D. W. (2020). *Diseño e implementación de un prototipo de seguridad para control domótico basado en iot bajo ambientes de dispositivos móviles con android* (B.S. thesis). Quito, 2020.

INEI. (2020a). *Informe técnico - estadísticas de seguridad ciudadana: Enero - junio 2020.* Descargado 28/08/2020, de https://www.inei.gob.pe/media/MenuRecursivo/boletines/boletin-de-seguridad-ciudadana.pdf

INEI. (2020b). *Informe técnico - situación del mercado laboral en lima metropolitana.* Descargado 15/09/2020, de https://www.inei.gob.pe/media/MenuRecursivo/boletines/09-informe-tecnico-mercado-laboral-jun-jul-ago-2020.pdf

INTEL. (2020). *Diferentes protocolos de wi-fi y velocidades de datos.* Descargado 25/11/2020, de https://www.intel.la/content/www/xl/es/support/articles/000005725/network-and-i-o/wireless.html

Martínez Moreno, F. J., y cols. (2019). Diseño e implementación de un sistema de

alarma iot basada en tecnologías open source.

Ministerio de transportes y comunicaciones. (2008). *Plan nacional de atribución de frecuencias(pnaf).* Descargado 28/08/2020, de https:https://portal.mtc.gob.pe/comunicaciones/autorizaciones/servicios_privados/documentos/pnaf_act_feb08.pdf

Ministerio de transportes y comunicaciones. (2013). *Resolución ministerial n° 199-2013-mtc/03.* Descargado 28/08/2020, de https://cdn.www.gob.pe/uploads/document/file/358686/1_0_4486.pdf

Mujica, J., y Zevallos, N. (2016). Seguridad ciudadana. *Lima: CIES*.

Naik, N. (2017). Choice of effective messaging protocols for iot systems: Mqtt, coap, amqp and http. En *2017 ieee international systems engineering symposium (isse)* (pp. 1–7).

Pantano, E., y Timmermans, H. (2014). What is smart for retailing?

Parra Marroquin, M. A., y cols. (2019). *Diseño de un sistema para control de las alarmas de seguridad en el hogar utilizando la tecnología m2m* (Tesis Doctoral no publicada).

Penal, C. (2015). Código penal del perú. *Lima, Perú: Juristas Editores EIRL*.

PMG Bussines Improvement. (2016). *Agricultura smart: Minimizar el riesgo y aumentar la rentabilidad de los cultivos.* Descargado 15/11/2020, de https://www.pmgchile.com/wp-content/uploads/2016/12/Agricultura-Smart.pdf

Salcedo Tovar, M. L. (2015). Minicomputador educacional de bajo costo raspberry pi: primera parte. *Revista Ethos Venezolana*, *7*(1), 28–45.

Telefónica, F. (2011). *Smart cities: un primer paso hacia la internet de las cosas* (Vol. 16). Fundación Telefónica.

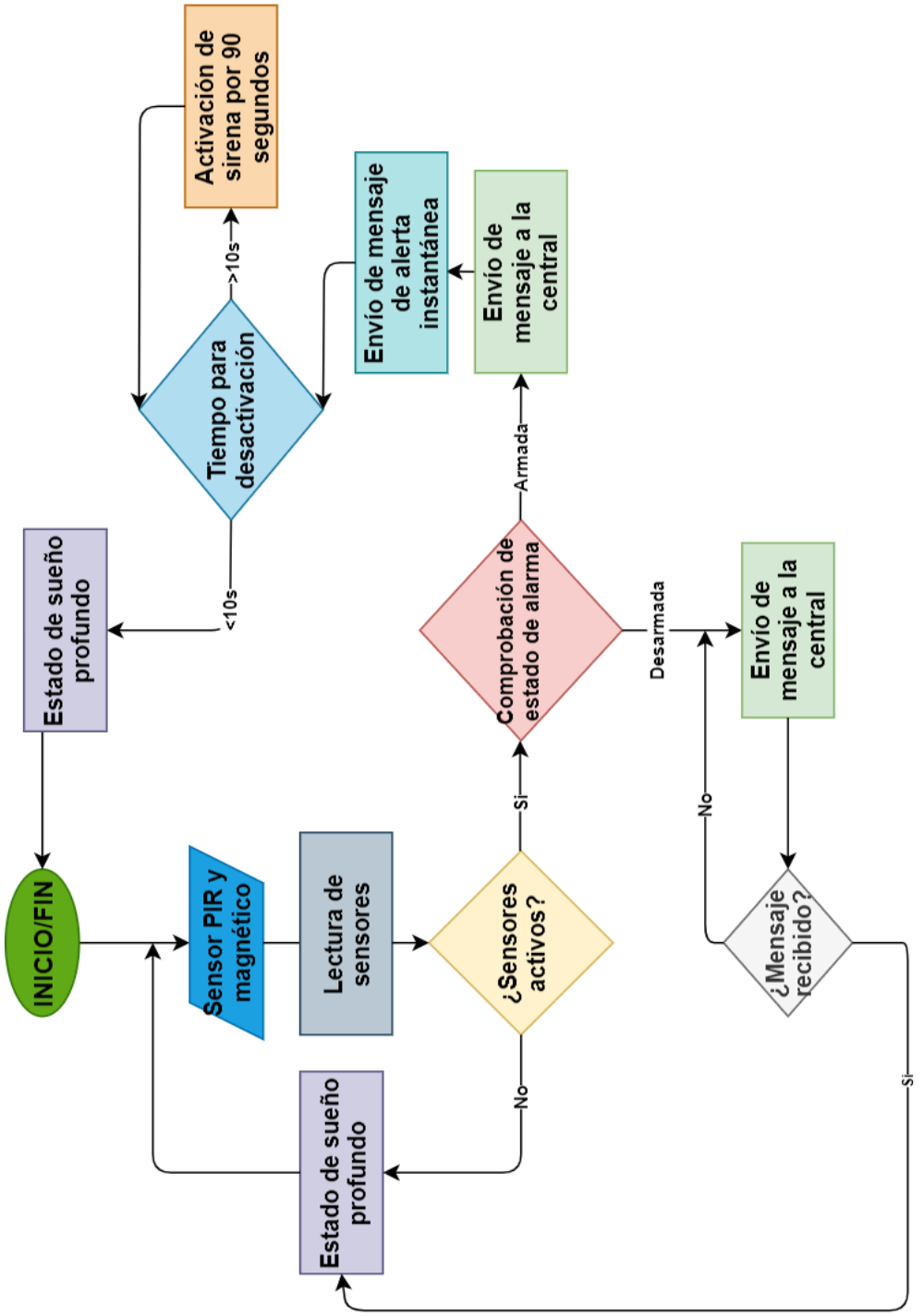
Uvidia, V., y Alexander, D. (2019). *Implementación de un prototipo de sistema de seguridad doméstico basado en wpan para una red iot.* (B.S. thesis). Escuela Superior Politécnica de Chimborazo.

Valderrama, J., y Brea, E. (2020). Esp8266: Un microcontrolador para el internet de las cosas. *Universidad Central de Venezuela, Tech. Rep. Accessed: May*, *8*.

Wim Hoogenraad. (2018). *Wifi y bluetooth, ¿cuál es la diferencia?* Descargado 18/11/2020, de https://botrueactivities.com/comparativa-entre-sigfox-y-lorawan/

ANEXOS

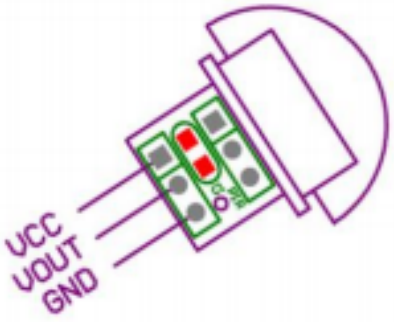
ANEXO 1: FLUJOGRAMA DE FUNCIONAMIENTO DEL SISTEMA



ANEXO 2: DATASHEET SENSOR PIR AM312

AM312

MINIATURE PIR SENSOR



SPECIFICATIONS	
Working voltage	DC 2.7-12V
Static power consumption	0.1mA
Delay time	2 seconds
Trigger mode	repeatable
Sensing range	≤100 degree cone angle, 3-5 meters
Working temperature	-20 - +60 °C
PCB dimensions	10mm*8mm

ANEXO 3: DATASHEET SENSOR MAGNÉTICO MC-38

Door & Window Magnetic Sensor Switch for Arduino / IOT / Alarm System

MC-38 Wired Door Window Sensor | Magnetic Switch | Home Alarm System, Recess able style (which means they can be "set into" for example: a door or window). The MC38 can be wired to your door, or window, any where you want a magnetic sensor to alarm when opened.

Metal shield anti-fire ABS, the alarm sounds when the magnets separated. No external power supply is required-- simply connect to wired or wireless alarm control panel GND and N.C ports directly!

SPECIFICATIONS:

- Connecting Mode: N.C.
- Rated current: 100mA
- Rated voltage: 200VDC
- Operating distance: more than 15mm, less than 25mm
- Rated power: 3W
- Dimension: 28x15x0.9cm
- Cable Length: 30.5cm ± 12mm
- Switch output: normally closed (switch and magnet are together when the switch is closed)

FEATURES:

- Easy installation Reliable performance
- Good characteristic of abrasion-proof
- Best Choice for you to protect family

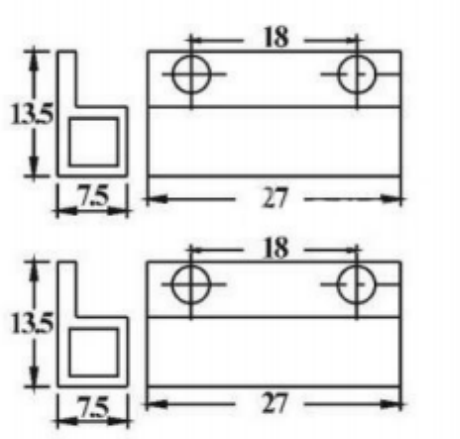
APPLICATION:

- Easy installation Reliable performance
- Good characteristic of abrasion-proof
- Best Choice for you to protect family
- There are two types of reed switches: "normally open" reed switches and "normally closed" reed switches.
- The metal reeds on a normally open switch stay open when there is no magnet near the switch. In the presence of a magnetic field, the contacts of a normally-open reed switch will close. A normally-closed reed switch is closed when it is not near a magnet; as a magnet is brought close to it, a normally-closed switch will open

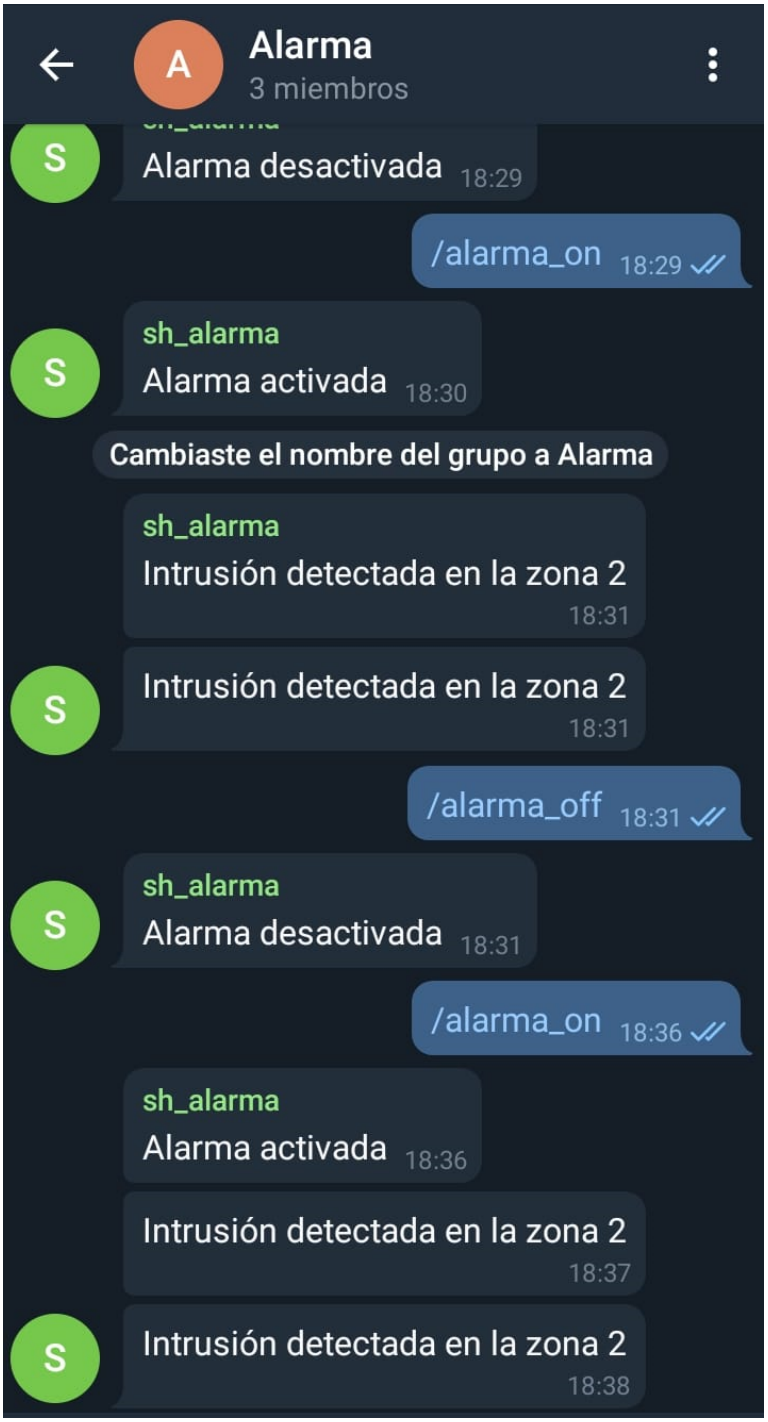
PIN-OUTS:

The switch is non polar, so you can plug in the wires in any way.

DIMENSIONS (MM):



ANEXO 4: PRUEBAS DE ALERTA VÍA TELEGRAM



ANEXO 5: MEDICIÓN DE CORRIENTE EN NODOS SENSORES

ANEXO 6: DURACIÓN TEÓRICA EN HORAS DE LA BATERÍA DE LOS NODOS SENSORES EN MODO DE SUEÑO PROFUNDO

Capacidad Disponible:	3500	mA·h
Consumo:	11.93	mA
Duración:	293,378	Horas

Capacidad Disponible:	3500	mA·h
Consumo:	10.8	mA
Duración:	324,074	Horas

ANEXO 7: PATENTE DE MARCA SHIELD PERÚ

PERÚ | Presidencia del Consejo de Ministros | INDECOPI

Registro de la Propiedad Industrial

Dirección de Signos Distintivos

CERTIFICADO N° 00278948

La Dirección de Signos Distintivos del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, certifica que por mandato de la Resolución N° 010061-2019/DSD - INDECOPI de fecha 14 de mayo de 2019, ha quedado inscrito en el Registro de Marcas de Producto, el siguiente signo:

Signo	:	La denominación SHIELD PERÚ y logotipo (se reivindica colores), conforme al modelo
Distingue	:	Sensores (aparatos de detección); cámara de seguridad; aparatos e instrumentos científicos; aparatos de control (inspección); aparatos de detección, equipo de procesamiento de datos; alarmas acústicas; alarmas anti-robo; aparatos de salvamento; soporte de grabación digital
Clase	:	09 de la Clasificación Internacional.
Solicitud	:	0790471-2019
Titular	:	MATIAS SANCHEZ PIERO YAHIR y RUIZ SANDOVAL JULIAN ANTONIO
País	:	Perú; Perú
Vigencia	:	14 de mayo de 2029
Tomo	:	1396
Folio	:	058

RAY MELONI GARCIA
Director
Dirección de Signos Distintivos
INDECOPI

SHIELD
PERÚ