

UNIVERSIDAD NACIONAL DE HUANCABELICA

(Creado por Ley N° 25265)

FACULTAD DE INGENIERÍA ELECTRÓNICA - SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA



TESIS

**“DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA INTERNET DE
LAS COSAS PARA ALERTAR EL ROBO EN VIVIENDAS”**

LÍNEA DE INVESTIGACIÓN

CONTROL Y AUTOMATIZACIÓN

PRESENTADO POR:

BACH. ING. JESSICA JOVANA VIVAR CARDENAS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

HUANCABELICA, PERÚ

2022



"Año del Fortalecimiento de la Soberanía Nacional"

ACTA DE SUSTENTACIÓN DE TESIS

En la Facultad de Ingeniería Electrónica - Sistemas, Escuela Profesional de Ingeniería Electrónica, local de PARANINYO, a los 27 días del mes de DICIEMBRE de 2022 siendo las 11 horas con 00 minutos, se instaló el Jurado Evaluador de Tesis, teniendo como miembros:

1. PRESIDENTE : DR. MARCO AURELIO ROSARIO VILLARREAL
ORCID 0000-0003-0250-9137
DNI N° 18189058
2. SECRETARIO : MG. RAUL PADILLA SANCHEZ
ORCID 0000-0001-7220-9193
DNI N° 23274132
3. VOCAL : MG. EVERETH MANUEL ROMOS LOPA
ORCID 0000-0001-6157-110X
DNI N° 23270398
4. ASESOR : MG. EVERETH MANUEL ROMOS LOPA
ORCID 0000-0001-6157-110X
DNI N° 23270398

Con la finalidad de evaluar la sustentación de tesis, titulado: "DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA INTERNET DE LAS COSAS PARA ALERTAR EL ROBO EN VIVIENDAS", presentado por la (los) bachiller

(es): JESSICA JOVANA VIVAR CARDENAS, de la Escuela Profesional de Ingeniería Electrónica, quien (es) ha (n) sido declarado (s) expedito (s) para el presente acto, con Resolución de Consejo de Facultad N° 0429-2022-FIES-UNH, de fecha 16 de DICIEMBRE del 2022.

Se da inicio a la sustentación de tesis siendo las 11 horas con 00 minutos. Concluido la sustentación, se pasó a la segunda etapa de preguntas y/u observaciones.

Enseguida el Jurado deliberó en secreto para obtener el resultado, siendo el veredicto del jurado:

APROBADO ☒ POR UNANIMIDAD

DESAPROBADO ☐

A horas 11:45, se da por concluido el acto, y procedieron a firmar en señal de conformidad.

Ciudad Universitaria PAMPAS, 27 de DICIEMBRE del 20 22.

OBSERVACIONES: _____

Presidente

Vocal

Secretario

TÍTULO

**“DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA
INTERNET DE LAS COSAS PARA ALERTAR EL ROBO
EN VIVIENDAS”**

AUTOR:

Bach. Ing. JESSICA JOVANA VIVAR CARDENAS

ASESOR:

Mg. Ing. Everth Manuel Ramos Lapa.

DNI: 23270398

<https://orcid.org/0000-0001-6157-118X>

AGRADECIMIENTO

A mis queridos padres por que formaron con mucho cariño para ser la persona de hoy; a Manuel quien apoya mis decisiones para cristalizar mis objetivos, a la Universidad Nacional de Huancavelica por acobijarme en su seno, a mis docentes de la EPI Electrónica y a mi asesor Mg Everth Manuel Ramos Lapa, mi gratitud sincera, porque permitieron culminar el presente trabajo de investigación.

ÍNDICE

ÍNDICE	vii
ÍNDICE DE TABLAS	xi
ÍNDICE DE FIGURAS.....	xii
RESUMEN.....	xvi
ABSTRACT.....	xvii
INTRODUCCIÓN	xviii
CAPÍTULO I.....	19
PLANTEAMIENTO DEL PROBLEMA	19
1.1. Descripción del problema	19
1.2. Formulación del problema	22
1.2.1. Problema general	22
1.2.2. Problemas específicos.....	22
1.3. Objetivos	22
1.3.1. Objetivo general	22
1.3.2. Objetivos específicos	23
1.4. Justificación	23
1.4.1. Justificación social.....	23
1.4.2. Justificación tecnológica.....	23
1.4.3. Justificación económica.....	24
CAPÍTULO II	25
MARCO TEÓRICO.....	25
2.1. Antecedentes	25
2.2. Bases conceptuales.....	27

2.2.1. Sistemas de comunicación.....	27
2.2.2. Medio de comunicación inalámbrica.....	28
2.2.3. Tipos de redes inalámbricas	29
2.2.4. IoT	30
2.2.5. Funcionamiento de la IoT.....	30
2.2.6. Beneficios de IoT.....	31
2.2.7. Automatización.....	31
2.2.8. Elementos de un proceso a automatizar	32
2.2.9. Sistema de control	35
2.2.10. Sistema de Control Automático	35
2.2.11. Clasificación de sistema de control.....	36
2.2.12. Acciones de control.....	37
2.2.13. Sistemas de seguridad	39
2.2.14. Sensores.....	42
2.2.15. Arduino.....	43
2.2.16. Módulo wifi NodeMcu V3 Esp8266.....	53
2.2.17. Modulo wifi Node ESP32	54
2.2.18. Wemos D1 Mini ESP8266 Wifi.....	55
2.2.19. Raspberry Pi 3	56
2.2.20. Módulo Wifi ESP8266	57
2.2.21. Sensor magnético de puerta MC-38	58
2.2.22. Módulo PIR HC-SR501	59
2.2.23. Sensor Final de Carrera	60
2.2.24. Actuadores.....	61
2.2.25. Plataforma Iot.....	63

2.3. Hipótesis	75
2.3.1. Hipótesis general	75
2.3.2. Hipótesis específica	75
2.4. Definición de términos.....	75
2.5. Definición operativa de variables	77
2.5.1. Variables dependientes	77
2.5.2. Variables independientes	77
CAPÍTULO III.....	79
MATERIALES Y MÉTODOS	79
3.1 Ámbito de estudio	79
3.2 Tipo y nivel de investigación	80
3.3 Método de investigación	80
3.4 Diseño de investigación	81
3.5 Población y muestra	81
3.5.1. Población	81
3.5.2. Muestra	81
3.5.3. Muestreo	82
3.6 Técnicas e instrumentos de recolección de datos.....	83
3.7 Procedimiento de recolección de datos	85
3.8 Técnicas de procesamiento y análisis de datos	85
CAPÍTULO IV.....	86
DISCUSIÓN DE RESULTADOS	86
4.1 Análisis de información	86
4.2 Prueba de hipótesis	86
4.3 Discusión de resultados.....	92

CONCLUSIONES	94
RECOMENDACIONES	95
BIBLIOGRAFÍA	96
ANEXOS	99
MATRIZ DE CONSISTENCIA	100
ANEXO A.....	101
1. Requerimientos de diseño	101
1.1. Sistema electrónico de funcionamiento.....	101
1.2. Requerimiento de diseño según la aplicación.....	102
2. Diagrama de bloques.....	103
3. Sistema de adquisición de datos.....	103
3.1. Sensor final de carrera	104
3.2. Visualización de datos	106
3.3. Transmisión de datos	107
3.4. Visualización de los datos a través del aplicativo.	125
4. Diagrama de flujo	127
5. Circuito electrónico del sistema de alarma.	128
6. Diseño de placa electrónica	129
ANEXO B.....	131
ANEXO C	177

ÍNDICE DE TABLAS

Tabla N° 1 Las variables, indicador y unidad de medida.	77
Tabla N° 2 Instrumento de recolección de datos de activación de alarma.....	83
Tabla N° 3 Instrumento de recolección de datos de monitoreo de la alarma.....	84
Tabla N° 4 Estadística de muestras relacionadas.....	87
Tabla N° 5 Correlación de muestras relacionadas.	87
Tabla N° 6 Prueba de muestras relacionadas.	88
Tabla N° 7 Prueba de muestras relacionadas.	90
Tabla N° 8 Prueba de muestras relacionadas.	90
Tabla N° 9 Prueba de muestras relacionadas.	91
Tabla B. 1 Muestra tomada de activación y desactivación de la alarma.....	131
Tabla B. 2 Muestra tomada del monitoreo de la alarma.	154

ÍNDICE DE FIGURAS

Figura 1. Viviendas del área urbana del 2010 - 2017.	19
Figura 2. Elementos de un sistema de comunicación.	28
Figura 3. Comunicación a través de radio.....	29
Figura 4. Elementos de un proceso a automatizar.....	32
Figura 5. Conversión entre códigos numéricos.....	32
Figura 6. Elemento de entrada de información.	33
Figura 7. Elemento de salida de información.....	34
Figura 8. Preaccionadores y accionadores.	34
Figura 9. Sistema de control automático.....	35
Figura 10. Sistema de control de lazo abierto.	36
Figura 11. Sistema de control de lazo cerrado.	37
Figura 12. Acción del control ON-OFF.	37
Figura 13. Control proporcional, integral, derivativo (PID).	38
Figura 14. Sistema CCTV.....	40
Figura 15. Sistema contra incendio.....	40
Figura 16. Plataforma Arduino.	43
Figura 17. Placa Arduino Mega 2560.	44
Figura 18. Placa Arduino Uno.	45
Figura 19. Placa Arduino Nano.....	46

Figura 20. Placa Arduino MKR WiFi 1010.	47
Figura 21. Placa Arduino Uno Wifi.	48
Figura 22. Placa Arduino Nano 33 IOT.	48
Figura 23. Placa Arduino Leonardo.	49
Figura 24. Placa Arduino Portenta H7.	50
Figura 25. Placa Arduino Nano Ble Sense.	52
Figura 26. Placa Arduino Yún.	53
Figura 27. Imagen de la placa Módulo wifi NodeMcu.	54
Figura 28. Imagen de la placa Módulo wifi NodeMcu ESP32.	55
Figura 29. Imagen de la placa Wemos D1 Mini ESP8266.	56
Figura 30. Imagen de la placa Raspberry PI 3.	57
Figura 31. Imagen de la placa Módulo wifi NodeMcu.	58
Figura 32. Imagen del sensor magnético MC38.	59
Figura 33. Imagen del sensor PIR.	60
Figura 34. Imagen del sensor final de carrera.	61
Figura 35. Sirena.	62
Figura 36. Plataforma Artik Cloud.....	64
Figura 37. Imagen de la plataforma de Blynk.....	65
Figura 38. Imagen de la plataforma Domoticz.	66
Figura 39. Imagen de la plataforma Zetta.	67

Figura 40. Imagen de la plataforma Node-RED.	67
Figura 41. Imagen de la plataforma Flutter.....	69
Figura 42. Imagen de la plataforma M2MLabs Mainspring.....	70
Figura 43. Imagen de la plataforma ThingsBorad.	72
Figura 44. Imagen de la plataforma Kinoma.	72
Figura 45. Imagen de la plataforma Kaa IoT.	73
Figura 46. Plataforma Arduino Cloud.....	74
Figura 47. Ubicación geográfica de la ciudad de Pampas, Tayacaja.	79
Figura 48. Correlación de estado actual con el estado deseado.	87
Figura 49. distribución de t estadístico.	89
Figura 50. Monitoreo de la alarma por la plataforma Blynk.	89
Figura 51. distribución de t estadístico.	92
Figura A.1. Diagrama de bloque del sistema electrónico.	101
Figura A.2. Imagen del sensor final de carrera.	104
Figura A.3. Diagrama de bloques.	105
Figura A.4. Imagen del circuito electrónico del final de carrera.	106
Figura A.5. Imagen del indicador led.....	106
Figura A.6. Imagen del circuito electrónico del indicador led.....	107
Figura A.7. Imagen del módulo MCU Node ESP8266.....	108
Figura A.8. Imagen del icono de la plataforma Blynk.....	126

Figura A.9. Imagen del aplicativo diseñado para el sistema.....	126
Figura A.10. Diagrama de flujo de programa de Arduino.	127
Figura A.11. Diagrama de flujo del aplicativo.....	128
Figura A.12. Imagen del circuito eléctrico del sistema de alarma.	129
Figura A.13. Imagen de la placa por la parte superior.	129
Figura A.14. Imagen del placa por la parte inferior.	130

RESUMEN

La investigación presentada tuvo como objetivo principal implementar y diseñar un sistema de alarma para alertar el robo y/o intento de robo de las viviendas. Hoy en día existe una gran variedad de tecnologías, es esta la razón que utilizamos la tecnología de sensores asociado a internet de las cosas (IoT), la cual es la más adecuada para realizar esta investigación. En esta investigación se utilizaron sensores de contacto, módulo NodeMCU ESP8266, una red wifi de alta velocidad. El método de investigación que se realizó fue el científico y como método particular fue el experimental. Tipo aplicada Se demostró que este sistema tiene una eficiencia de un 97.4 % en la activación y desactivación de la alarma mediante la plataforma Blynk y también se obtuvo una eficiencia del 97.4 % en el monitoreo del estado de la alarma mediante la plataforma Blynk. Lo cual demuestra que esta investigación alertar el robo y/o intento de robo en las viviendas.

Palabras clave: IoT, antirrobo, sistema de alerta, plataforma Blynk, alarma.

ABSTRACT

The main objective of the research presented was to implement and design an alarm system to alert theft and/or attempted theft of homes. Today there is a wide variety of technologies, this is the reason that we use sensor technology associated with the Internet of Things (IoT), which is the most appropriate to carry out this research. In this research, contact sensors, NodeMCU ESP8266 module, a high-speed Wi-Fi network were used. The research method that was carried out was the scientific one and as a particular method it was the experimental one. Applied type This system was shown to have an efficiency of 97.4% in activating and deactivating the alarm using the Blynk platform and an efficiency of 97.4% was also obtained in monitoring the status of the alarm using the Blynk platform. Which shows that this investigation alert the robbery and / or attempted robbery in homes.

Keywords: IoT, anti-theft device, alert system, Blynk platform, alarm.

INTRODUCCIÓN

La inclusión de los sistemas de automatización se está popularizando con el avance de las aplicaciones de Tecnología de la información y la comunicación. Los sistemas ofrecen comodidad tanto en edificios privados como comerciales a través del control remoto de calefacción, ventilación, aire acondicionado, iluminación, etc., y permiten al usuario controlar todo tipo de electrodomésticos remotamente.

Sin embargo, por otro lado, el robo de viviendas a nivel nacional está afectando alrededor del 10% de la población, lo cual perjudica a los ciudadanos de manera económica, emocional y físico. En la actualidad existen empresas dedicadas a la protección y vigilancia privada ya sea para viviendas, almacenes, condominios, etc. Al contratar uno de estos servicios a estas empresas privadas se tiene que realizar pagos mensuales. Son motivos que se dio iniciativa para realizar este proyecto de investigación con el propósito de diseñar un prototipo de bajo costo el cual pueda alertar del robo que puedan ser efectuados en viviendas. Tomando en cuenta la metodología científica, método particular experimental y tipo aplicada, con ello se demostró que este sistema tiene una eficiencia de un 97.4 % en la activación y desactivación de la alarma mediante la plataforma Blynk y también se obtuvo una eficiencia del 97.4 % en el monitoreo del estado de la alarma mediante la plataforma Blynk. Demostrando que el resultado de esta investigación permite alertar el robo y/o intento de robo en las viviendas.

En el Capítulo 1 se enfoca en el problema de la investigación, planteamiento del problema, formulación del problema, objetivos, y las justificaciones de la investigación.

El Capítulo 2 se expone los antecedentes, se desarrolla el marco teórico, definición de términos.

El Capítulo 3 se enfoca en el desarrollo de la metodología de la investigación, población, muestra y muestreo, técnicas e instrumentos de recolección de datos.

El Capítulo 4 está referido al aspecto administrativo, los materiales a usar, el presupuesto, los recursos humanos, el cronograma de actividades.

CAPÍTULO I

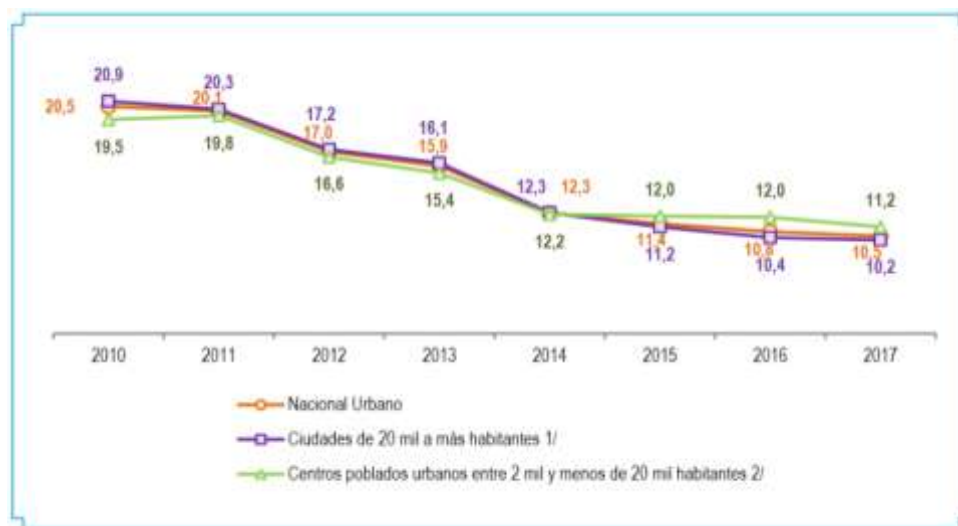
PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del problema

A nivel nacional urbano, las viviendas fueron frecuentemente víctimas de robo o intento de robo en ciudades con mayor población como 20 mil a más pobladores en los años 2010 y 2011, este porcentaje superó el 20%; mientras que, “en los años 2012, 2013, 2014 y 2015 fue de 17,0%, 15,9%, 12,3% y 11,4% respectivamente. Según ámbito de estudio, los centros poblados urbanos entre 2 mil y menos de 20 mil habitantes, presentaron las mayores cifras porcentuales (11,2%) de viviendas afectadas por robo o intento de robo en el año 2017”, según estadísticas del INEI (INEI, 2017, p. 113).

Figura 1.

Viviendas del área urbana del 2010 - 2017.



Nota. Tomado de (INEI, 2017).

Se sabe que solo un 17.9 % de las personas afectadas denuncian el hecho delictivo ante las autoridades. Una de las razones principales de las personas para no denunciar es el hecho que piensan que es pérdida de tiempo, porque no se

conoce que persona fue el delincuente o el robo no fue realizado. Se concluye de estos datos que de cada 100 habitantes 12 sufrieron de robo en su vivienda.

Por ello, se pone en evidencia, la necesidad de alertar a la población el robo o intento de robo en viviendas:

- Según el diario La República de fecha 27 de julio 2021, 11:55 h | Surco – Lima, (Portuguez, 2021), señala:
“Delincuentes ingresan a vivienda y se llevan S/ 400.000 soles mientras la dueña descansaba”.

Los ladrones sustrajeron una caja fuerte, además de joyas y relojes. En solo minutos hampones treparon el cerco de una vivienda en Surco para ingresar y robar una caja fuerte que contenía 15.000 dólares, 10.000 euros y 10.000 soles en efectivo, además de joyas, relojes y objetos de alta gama valorizados en un total de 200.000 soles.

Noemi Olinda Rojas Domínguez (56) se encontraba descansando cuando estos sujetos se llevaron un valor total de 400.000 soles de su vivienda. Dedicada al rubro de muebles durante años, la agraviada había decidido retirar sus ahorros recientemente para guardarlos en la caja fuerte de su domicilio, pero no contó con que estas personas se llevarían el esfuerzo de tanto tiempo en cuestión de minutos y sin que nadie se diera cuenta.

Eran aproximadamente las tres y media de la madrugada del domingo 25, cuando al menos dos sujetos burlaron el cerco de la casa de cuatro pisos ubicada en la calle Las Cantutas en la urbanización Casuarinas de Surco y se fueron directamente a la caja fuerte.

El robo fue captado por las cámaras de video vigilancia de la iglesia San Roque, ubicada al frente de la casa de la víctima. En las imágenes se observa al sujeto acercarse a los exteriores del lugar y subir trepando el cerco hasta entrar hacia el otro lado.

- Según el diario La República de fecha 25 de julio 2021, 23:09 h| Pueblo Libre -Lima, (LR, 2021), señala:

Roban bicicleta a joven por segunda vez en su propia vivienda

Una joven denunció que un delincuente ingresó a su vivienda en Surco para llevarse la bicicleta que recientemente había empezado a usar. Ella se

encuentra indignada, pero a la vez preocupada por la facilidad con la que el malhechor vulneró su inmueble.

El robo fue captado por las cámaras de video vigilancia de la iglesia San Roque, ubicada al frente de la casa de la víctima. En las imágenes se observa al sujeto acercarse a los exteriores del lugar y subir trepando el cerco hasta entrar hacia el otro lado.

El hampón actuó rápidamente al agarrar el vehículo motorizado y lanzarlo con fuerza hacia la calle. Luego volvió a trepar y fugó manejando la bicicleta.

- Según el diario La República de fecha 09 de julio 2021, 17:29 h| Pueblo Libre -Lima, (LR, Pueblo Libre: delincuente roba en vivienda y se lleva hasta el helado, 2021), señala:

Desvalijan vivienda mientras familia paseaba en el Parque de La Leyendas.

Una familia denunció que su casa fue asaltada por delincuentes que ingresaron aprovechando que no había nadie en el interior. El hecho ocurrió el último 8 de julio en la urbanización San Antonio, en Surco.

Los malhechores se dieron el trabajo de ir a cada ambiente para revisar los objetos de valor. En total se llevaron tres televisores grandes, una computadora, una Play Station, varios miles de soles en efectivo, así como el anillo de compromiso, los aros de matrimonio, joyas y alhajas de David, quien recién el año pasado contrajo nupcias.

El joven ingeniero informático comenta que los ladrones también se apropiaron de videos y fotos de su matrimonio, así como un disco duro donde tenía información de propiedad intelectual con bastante valor para él. Aproximadamente todo lo robado asciende a más de S/ 40.000.

- Según el diario La República de fecha 23 de marzo 2021, 11:41 h| Pueblo Libre -Lima, (LR, 2021), señala:

Hampones entran a robar a una vivienda mientras familia dormía.

Las cámaras de seguridad captaron todo el atraco. Tal como se ve en las imágenes, los malhechores forcejean la reja principal de la vivienda, luego ingresan al inmueble y se dirigen hacia el segundo piso.

Según narra el agraviado, los hampones caminaron sigilosamente para evitar ser escuchados, incluso se sacaron los zapatos para entrar por la ventana de la vivienda.

En total, los ladrones se llevaron una computadora, varias laptops, celulares, una Tablet, entre otros elementos. Incluso se llevaron ropa y lentes ópticos. El robo asciende a S/ 9.000.

Esta información motivó a realizar la ejecución de esta investigación con el fin de alertar a los dueños y/o vecinos de viviendas que están siendo víctimas de robo, para así poder disminuir el robo y poder atrapar a los delincuentes de manera infraganti.

1.2. Formulación del problema

1.2.1. Problema general

- ¿Cómo diseñar e implementar un sistema de alarma que permita alertar el robo y/o intento de robo en las viviendas?

1.2.2. Problemas específicos

- ¿Qué plataforma asociado a IoT deberá tener el sistema que active y desactive la alarma para alerte el robo y/o intento de robo?
- ¿Qué plataforma asociado a IoT deberá tener del sistema para el monitoreo del estado de la alarma?

1.3. Objetivos

1.3.1. Objetivo general

- Diseñar e implementar un sistema de alarma que permita alertar el robo y/o intento de robo de las viviendas.

1.3.2. Objetivos específicos

- Determinar la plataforma asociado a IoT que deberá tener el sistema que active y desactive la alarma para alertar el robo y/o intento de robo.
- Determinar la plataforma asociado a IoT que deberá tener el sistema para el monitoreo del estado de la alarma.

1.4. Justificación

1.4.1. Justificación social

Con la realización de este trabajo de investigación, el propietario de una vivienda podrá prevenir el robo y/o intento de robo de sus bienes valiosos como televisores, joyerías, vehículos o dinero, lo cual beneficia al propietario y aumenta la seguridad dentro de la comunidad.

Al tener una alarma que pueda alertar el robo y/o intento de robo de una vivienda fomenta la organización de los vecinos para tener una comunidad segura para todas las personas.

1.4.2. Justificación tecnológica

Existe tecnología sofisticada que se encarga del monitoreo de la vivienda, activación o desactivación de la alarma mediante el teléfono, monitoreo las 24 horas del día, horas de entrada y salida de los propietarios, triple seguridad, anti intrusos y anti inhibición, como lo provee empresa PROSEGUR los cuales cuenta con sistemas cerrados tanto en software y hardware.

En la presente investigación se utiliza tecnología electrónica de sistemas que poseen plataforma de código abierto, como son los sistemas embebidos (módulos para Arduino), que nos permiten libertad de acceso en hardware y software, para esta investigación se dispuso de placas electrónicas, como principales dispositivos; el módulo wifi NodeMcu

Esp8266, sensores de contacto, indicadores, accesorios electromagnéticos, etc.

1.4.3. Justificación económica.

Hoy en día la tecnología provee diversas posibilidades de solución, para cubrir las necesidades de las personas que requieren soluciones innovadoras, rápidas y precisas. Sin embargo, los elevados precios a los que se encuentran disponibles los servicios de estos sistemas de protección contra robo, limitan enormemente el acceso a los mismos. Por tanto, el presente estudio de investigación propone satisfacer parte de la seguridad de la propiedad de las personas.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

A continuación, se presenta estudios e investigaciones que sirven como antecedentes para el desarrollo de la investigación:

(Gaibor Carrillo & Loor Morán, 2018) “Diseñar un sistema de alarma inalámbrico de bajo costo para la protección de viviendas tipo, en sectores de bajo recursos económicos de la ciudad de Guayaquil.”, tesis para optar título de Ingeniero en networking y telecomunicaciones. Universidad de Guayaquil. Guayaquil – Ecuador

El objetivo principal de este proyecto fue de presentar un diseño de un sistema de alarma inalámbrico de reducido precio para la protección de viviendas, en sectores de bajo recursos económicos en la ciudad de Guayaquil, el principio de funcionamiento está basada en un sistema de control de lazo cerrado.

(Gaibor Carrillo & Loor Morán, 2018) menciona que escogió la topología en estrella por ser la más apropiada para el diseño en una vivienda, por las divisiones que podrían existir y por los posibles aumentos de habitaciones o pisos. Todas las divisiones y áreas de las viviendas estarán instalados varios sensores que captura los movimientos de las personas no autorizadas según el presupuesto del usuario. La red debe cubrir dos partes principales: el tipo de arquitectura según el exterior e interior de la vivienda, con sus respectivas subdivisiones y los posibles componentes tecnológicos destinados para la escalabilidad del sistema.

El sistema está conformado por una placa principal OpenSource denominada Arduino conectada con un conjunto de sensores como los sensores PIR y los switches magnéticos, complementado con un módulo denominado SIM900 que se intercomunica con la placa para enviar mensajes de texto a números celulares,

en el caso llegue activarse la alarma, además de poseer cámaras IP que complementa el monitoreo del sistema.

De esta tesis se toma en cuenta la forma y diseño del prototipo de vivienda para poder instalar los sensores y componentes de la manera más adecuada para que pueda cumplir con lo requerido en esta investigación.

(Hernández Estrada et al., 2010) "Domótica de seguridad por medio de SMS". Tesis para optar el Título de ingeniero en comunicaciones y electrónica. Instituto Politécnico Nacional. Mexico D.F.

El objetivo principal fue solucionar el problema de mantener vigilado un recinto mientras la familia o los usuarios del inmueble no se encontraban e incluso cuando estaban presentes mediante el desarrollo de un sistema de control de seguridad la cual se manipule a distancia mediante mensajes.

(Hernandez Estrada et al., 2010) menciona que esta investigación cubre los objetivos propuestos que son: informar al usuario de un posible robo cuando este no se encuentra en casa y el segundo objetivo era simular presencia en el hogar para hacerlo menos propenso a un robo.

Este sistema alertará sobre la presencia o intento de ingreso a dicho inmueble, de sujetos no autorizados, mediante la activación de dispositivos de seguridad instalados en todas las zonas de posibles accesos. Cuando el sistema detecta intrusión envía un SMS alertándolo, este deberá tomar las medidas necesarias puesto que el sistema no puede ejecutar acciones.

De este trabajo de investigación tomamos como referencia el software, teniendo en cuenta las situaciones que se puedan presentar y la manera en cómo puede ser más eficiente el sistema.

(Ramírez Marocho, 2012) "Diseño e implementación de un sistema de seguridad inalámbrico con tecnología bluetooth para vivienda", Tesis para optar el Título de Ingeniero electrónico. Pontificia Universidad Católica del Perú. Lima – Perú.

El objetivo de esta tesis fue de contribuir con la sociedad peruana en el aspecto de seguridad domiciliaria, se ha enfocado esta tesis en diseñar e implementar un sistema de seguridad inalámbrico para proteger las viviendas contra hurtos y robos. Este sistema podrá ser integrado a futuras tecnologías u otros inventos que contribuyan a la eficiencia para la seguridad total.

(Ramírez Marocho, 2012) menciona que uno de los resultados fue cuando determina el tiempo de retardo para la activación, la cual fue de 10 segundos con un margen de error de 8.6%. En relación a la configuración del tiempo, se ha visto que a mayor actividad del sensor (cuando se presenta la detección) existe mayor probabilidad de error en promedio; cuando el sensor está calibrado a 15 segundos nos brinda un 6.26% de error, mientras que en 5 segundos resulta 5.2%. Asimismo, al momento que describe la transmisión y recepción, también existen errores con 12% en la emisión de data y 10% en la recepción. Esto ocurre por la falta de precisión en la calibración de los dispositivos entre sí; sin embargo, con la elaboración de más pruebas se reducirá el error.

De esta tesis se tuvo como referencia el tiempo de retardo de activación y el margen de error del sistema que hemos planteado.

2.2. Bases conceptuales

2.2.1. Sistemas de comunicación

Un sistema de comunicación es un conjunto de dispositivos que son utilizados con la finalidad de transmitir, emitir y recibir señales de todo tipo, como voz, datos, audio, video, etc., además dichas señales pueden ser del tipo digital o analógica.(México, s. f., p. 1)

Un sistema de comunicación puede describirse fácilmente mediante tres elementos básicos:

Transmisor, el cual se encarga de generar la señal que se desea y acoplarla de tal forma que pueda viajar a través del canal, mediante procedimientos como modulación, filtrado, codificación, etc.

Medio de transmisión: el cuál será el canal mediante el cual la señal va a viajar, y puede ser desde fibras ópticas, cables coaxiales, hasta el mismo aire.

Receptor: que realiza el procedimiento inverso del transmisor con la finalidad de reconstruir la señal y que esta sea lo más parecida a la original.

Figura 2.

Elementos de un sistema de comunicación.



Nota: Elaboración propia.

2.2.2. Medio de comunicación inalámbrica

Son medios de comunicación que envían señales electromagnéticas que representan los dígitos binarios de las comunicaciones de datos mediante frecuencias de radio y de microondas.

Como medio de redes, el sistema inalámbrico no se limita a conductores o canaletas, como en el caso de los medios de fibra o de cobre. De todos los medios, los inalámbricos proporcionan las mayores opciones de movilidad. Además, la cantidad de dispositivos con tecnología inalámbrica aumenta continuamente. Por estos motivos, la tecnología inalámbrica se convirtió en el medio de preferencia para las redes

domésticas. A medida que aumentan las opciones de ancho de banda de red, la tecnología inalámbrica adquiere popularidad rápidamente en las redes empresariales (Tomasi, 2010)

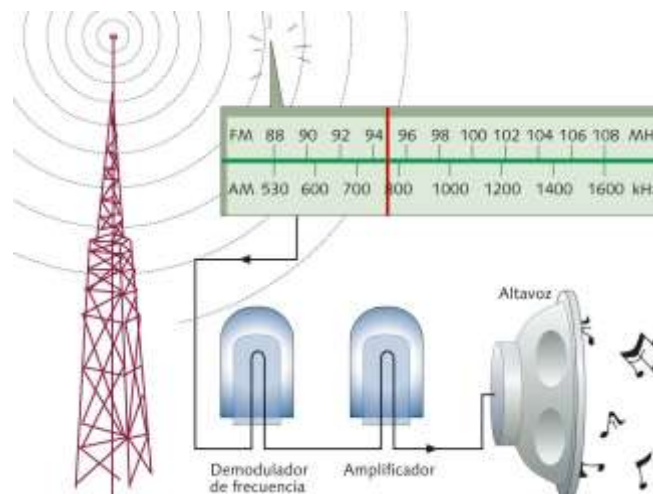
2.2.3. Tipos de redes inalámbricas

Radio: una emisión radiofónica consiste en la transmisión de sonidos, voz y música a distancia por medio de ondas electromagnéticas que son recibidas por un receptor de radio.

Las emisoras de radio no pueden enviar directamente la señal eléctrica producida en el micrófono: al ser frecuencias muy bajas, el alcance de la transmisión sería muy reducido y habría interferencias con otras emisoras que produce el mismo rango de frecuencias. Consiste en que cada emisora utilice una señal portadora de frecuencia más elevada, encargada de transportar el mensaje desde el emisor al receptor. La combinación de la señal que contiene el mensaje de sonido con la portadora recibe el nombre de modulación. Se utilizan dos tipos de modulación: de amplitud (AM) y de frecuencia (FM). (BlinkLearning, s. f.)

Figura 3.

Comunicación a través de radio.



Nota. Tomado de (Wayne, Sistemas de comunicaciones electrónicas, 2003).

2.2.4. IoT

IoT son las siglas de la expresión inglesa INTERNET OF THINGS, que en español traducimos como “INTERNET DE LAS COSAS”. Cuando decimos que algo es un «objeto de internet», lo que queremos decir es que está conectado a dicha red. A veces de forma directa (como nuestro móvil con 5G) y otras a través de redes intermedias (como la pulsera de actividad o Smart band).(Martinez, 2020)

El IoT, es un sistema de dispositivos informáticos interrelacionados, máquinas mecánicas y digitales, objetos, animales o personas que cuentan con identificadores únicos y la capacidad de transferir datos a través de una red sin necesidad de personal interacción humana o humana a computadora.(Valle, 2018)

2.2.5. Funcionamiento de la IoT

Un ecosistema de IoT consiste en dispositivos inteligentes habilitados para la web que utilizan procesadores integrados, sensores y hardware de comunicación para recopilar, enviar y actuar sobre los datos que adquieren de sus entornos. Los dispositivos de IoT comparten la información del sensor que recopilan al conectarse a una puerta de enlace de IoT u otro dispositivo de borde donde los datos se envían a la nube para analizarlos o analizarlos localmente. A veces, estos dispositivos se comunican con otros dispositivos relacionados y actúan sobre la información que obtienen unos de otros. Los dispositivos realizan la mayor parte del trabajo sin intervención humana, aunque las personas pueden interactuar con ellos, por ejemplo, para configurarlos, darles instrucciones o acceder a los datos.

Los protocolos de conectividad, redes y comunicación utilizados con estos dispositivos habilitados para la web dependen en gran medida de las aplicaciones específicas de IoT implementadas. (aula21, 2022)

2.2.6. Beneficios de IoT

El internet de las cosas ofrece una serie de beneficios a las organizaciones, permitiéndoles:

- Monitorear sus procesos comerciales generales;
- Mejorar la experiencia del cliente;
- Ahorre tiempo y dinero;
- Mejorar la productividad de los empleados;
- Integrar y adaptar modelos de negocio;
- Tomar mejores decisiones de negocios; y
- Generar más ingresos.

La IoT alienta a las empresas a repensar las formas en que se acercan a sus negocios, industrias y mercados y les brinda las herramientas para mejorar sus estrategias comerciales.

2.2.7. Automatización

La automatización es el conjunto de elementos o procesos informáticos, mecánicos y electromecánicos que operan con mínima o nula intervención del ser humano. Estos normalmente se utilizan para optimizar y mejorar el funcionamiento de una planta industrial, pero igualmente puede utilizarse la automatización en un estadio, una granja o hasta en la propia infraestructura de las ciudades.

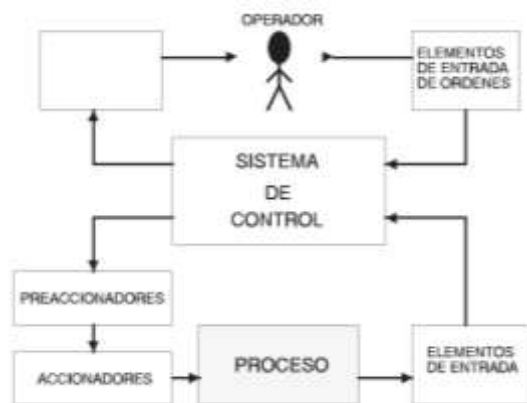
La retroalimentación y la capacidad de hacer ajustes con esa información es la que indica que tan autosuficiente es un sistema automatizado, un brazo robótico que se utiliza en el armado de autos es un ejemplo de alta independencia, ya que con sus sensores y su programación puede ejecutar su tarea sin intervención humana, un tanque de leche que solo tiene un sensor de temperatura, pero el apagado o prendido del mismo se hace de forma manual es un ejemplo de un sistema semi automatizado.(Logicbus, 2019)

2.2.8. Elementos de un proceso a automatizar

Un proceso a automatizar requiere tener en cuenta un conjunto de elementos, cada uno de los cuales realiza su función dentro del proceso. Podríamos representar el proceso mediante la siguiente figura.

Figura 4.

Elementos de un proceso a automatizar.



Nota. Elaboración propia.

Elementos de entrada de ordenes

Son los que permiten al operador la entrada de datos y ordenes al sistema, esto se puede clasificar en dos categorías: los binarios son los que permiten entrar órdenes del tipo si/no entre estos destaca los pulsadores, los numéricos permiten la entrada de números decodificados, entre los más frecuentes son los teclados numéricos.

Figura 5.

Conversión entre códigos numéricos.

CONVERSION ENTRE CODIGOS NUMERICOS:

Decimal (Base 10)	Binario (Base 2)	Octal (Base 8)	Hexadecimal (Base 16)
00	0000	00	0
01	0001	01	1
02	0010	02	2
03	0011	03	3
04	0100	04	4
05	0101	05	5
06	0110	06	6
07	0111	07	7
08	1000	10	8
09	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F

Nota. Tomado de (Slideshare, 2010).

Elementos de entrada de información

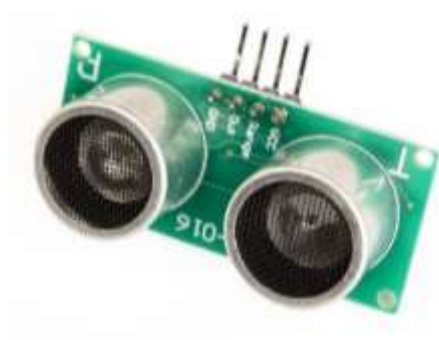
Se clasifican según el tipo de señal que facilitan o según su magnitud. Los binarios comparan la magnitud con una referencia y la salida corresponde al resultado de la comparación.

Los numéricos facilitan un código numérico que corresponde al valor de la magnitud leída.

Los analógicos dan una señal en forma de tensión eléctrica o de corriente eléctrica proporcional al valor de la magnitud.

Figura 6.

Elemento de entrada de información.



Nota. Tomado de (Naylampmechatronics, 2010).

Elemento de salida de información

Se encargan de la comunicación con el operador puede clasificar de igual manera a los de entrada de órdenes, entre ellos se destaca los visualizadores, también podemos citar los timbres, sirenas, etc.

Figura 7.

Elemento de salida de información.



Nota. Tomado de (Tecnimikro, 2012).

Preaccionadores y accionadores

Los accionadores son los encargados de actuar sobre el proceso. A menudo los accionadores no son directamente conectables al sistema de control y requieren preaccionadores. Por ejemplo, un motor eléctrico necesita un contactor o un variador de velocidad para poder funcionar, a un calentador eléctrico necesitara un variador de tensión para poder funcionar, un motor hidráulico necesitara de una válvula distribuidora o válvula proporcional. Si no fijamos entre los citados hay elementos binarios como el contactor y elementos de pedido analógico como el variador de tensión.

Figura 8.

Preaccionadores y accionadores.



Nota. Tomado de (Intercron, 2010).

Sistema de tratamiento de información

Establece la forma en que se tiene que combinar las entradas de información a fin de activar las salidas del proceso. Cuando una combinación de entradas siempre da lugar a la misma combinación de salidas se dice que el proceso es de tipo combinacional.

2.2.9. Sistema de control

Un sistema de control es un conjunto de dispositivos encargados de administrar, ordenar, dirigir o regular el comportamiento de otro sistema, con el fin de reducir las probabilidades de fallo y obtener los resultados teóricamente verdaderos. (Altamiranda, 2019)

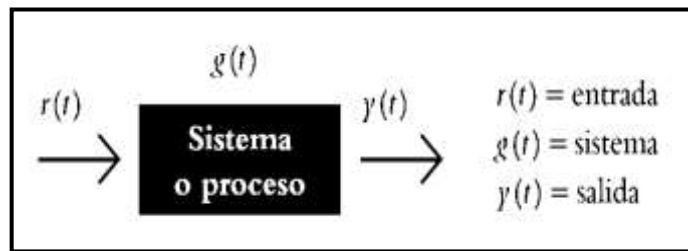
2.2.10. Sistema de Control Automático

Un sistema de control automático es una interconexión de elementos que forman una configuración denominada sistema, de tal manera que el arreglo resultante es capaz de controlarse por sí mismo. (Nise, 2002)

Un sistema o componente del sistema susceptible de ser controlado, al cual se le aplica una señal $r(t)$ a manera de entrada para obtener una respuesta o salida $y(t)$, puede representarse mediante bloques.

Figura 9.

Sistema de control automático.



Nota. Elaboración propia.

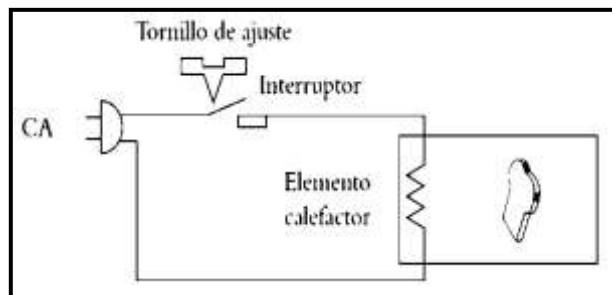
2.2.11. Clasificación de sistema de control

2.2.11.1. Sistema de control de lazo abierto

Es aquel sistema en el cual la acción de control es, en cierto modo, independiente de la salida. Este tipo de sistemas por lo general utiliza un regulador o actuador con la finalidad de obtener la respuesta deseada. (Nise, 2002)

Figura 10.

Sistema de control de lazo abierto.



Nota. Elaboración propia.

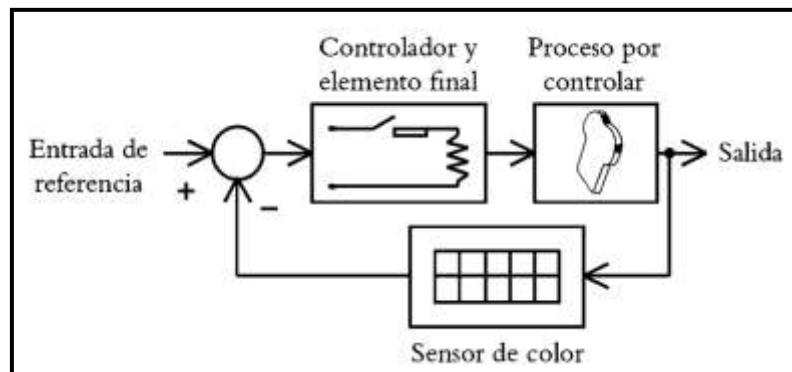
2.2.11.2. Sistema de control de lazo cerrado

Es aquel sistema en el cual la acción de control depende de la salida. Dicho sistema utiliza un sensor que detecta la respuesta real para compararla con una referencia a manera de entrada. Por esta razón, los sistemas de lazo cerrado se denominan sistemas retroalimentados. El término retroalimentar significa comparar;

en este caso, la salida real se compara con respecto al comportamiento deseado, de tal forma que si el sistema lo requiere se aplica una acción correctora sobre el proceso por controlar.(Gaviño, 2010)

Figura 11.

Sistema de control de lazo cerrado.



Nota. Elaboración propia.

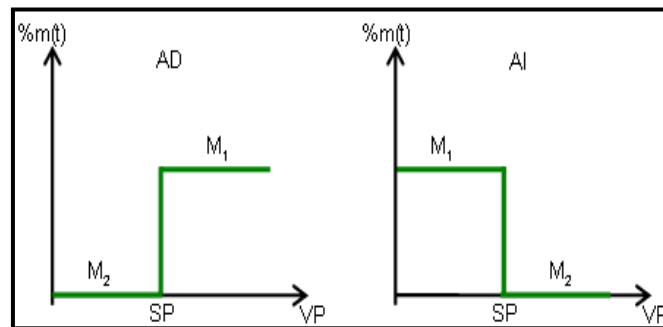
2.2.12. Acciones de control

2.2.12.1. Control ON/OFF

Es la forma más simple de control por realimentación, es un control de dos posiciones en el que elemento final de control ocupa una de las dos posiciones. Las posiciones para el actuador son: encendido (100%) o apagado (0%) del rango de $m(t)$, el control puede ser de acción directa AD o de acción inversa.(Gaviño, 2010)

Figura 12.

Acción del control ON-OFF.



Nota. Elaboración propia.

2.2.12.2. Control proporcional-integral-derivativo (PID)

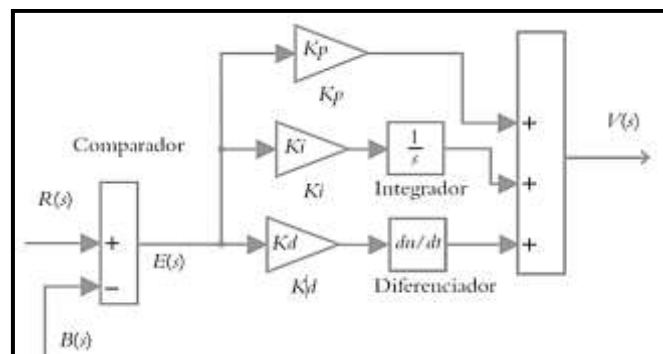
(Nise, 2002) Menciona que un control es de tipo proporcional-integral-derivativo cuando la salida del controlador $v(t)$ es proporcional al error $e(t)$, sumado a una cantidad proporcional a la integral del error $e(t)$ más una cantidad proporcional a la derivada del error $e(t)$:

$$v(t) = K_p e(t) + \frac{K_p}{T_i} \int e(t) dt + K_p T_d \frac{de(t)}{dt}$$

$$G_c(s) = K_p + \frac{K_i}{s} + K_d s$$

Figura 13.

Control proporcional, integral, derivativo (PID).



Nota. Elaboración propia.

2.2.13. Sistemas de seguridad

Acceso: Los sistemas de control de acceso se encargan de administrar y supervisar el ingreso de personas a áreas restringidas y evita que personas no autorizadas o indeseables tengan la libertad de acceder a estas zonas. Este sistema de control es mayormente utilizado en empresas, a través del cual se puede tener conocimiento de la asistencia del personal, horarios de ingreso y egreso, además tener un historial de entradas de personas a todas las áreas. Las características más resaltantes de este sistema son: la facilidad de su uso, los empleados lo pueden usar varias veces por día, la identificación por un número asignado (PIN), es el medio más común para autorizar a los empleados el acceso a una determinada área entre otras.(Encarnación, 2018)

Existe una variedad de sistemas de control de acceso. Entre los más resaltantes podemos mencionar:

- Control de acceso por teclado
- Acceso por sensor biométrico.
- Control de acceso por código de barras.

El circuito cerrado de televisión (CCTV) es una tecnología de video vigilancia visual diseñada para supervisar y controlar una diversidad de ambientes y actividades. El circuito está conformado básicamente por una o más cámaras de vigilancia conectadas a uno o más monitores de video, éstas pueden ser conectadas directamente entre sí o pueden ser enlazadas por red con otros componentes como videos o computadoras. La mayoría de estos sistemas cuentan con visión nocturna, operaciones asistidas por ordenador y detección de movimiento o presencia, garantizando que el sistema trabaje de manera óptima. Este sistema puede trabajar con los sistemas de control de acceso. En la Figura 14 se observa una gráfica del sistema de circuito cerrado de televisión. (Collaboration, 2017)

Figura 14.
Sistema CCTV.



Nota. Tomado de (Segproject, 2020)

Sistemas contra incendios

Los sistemas contra incendios alertan a las personas que se encuentran dentro del lugar donde ocurre el incidente, avisándoles la evacuación del lugar por seguridad. Los sistemas de alarma contra incendio pueden ser activadas de distintas formas: detectores de humo, detectores de calor, o manualmente. Al ser activados, los sensores mandan una señal a la unidad de control a fin de poder activar una alerta que puede ser una sirena o una alarma sonora. En la Figura 15 la imagen de un modelo de sistema contra incendios. (Ramírez Marocho, 2012)

Figura 15.
Sistema contra incendio.



Nota. Tomado de (Ingenieria y proyectos, 2021)

Sistemas contra hurtos, robos y asaltos a los inmuebles

(Morón Uche, 2013) Estos sistemas son los más utilizados para detectar y evitar los actos ilícitos en contra de las viviendas. La protección exterior se realiza mediante detectores volumétricos, los cuales se instalan en las afueras del inmueble para detectar la presencia e invasión en un área concreta. En el interior del inmueble se pueden utilizar sensores magnéticos para puertas, sensores de rotura de ventanas y sensores de presencia (PIR). Todos estos dispositivos son controlados por un centro de control el cual genera las órdenes de activación del funcionamiento de los sensores, y viceversa, es decir, capta el mensaje enviado por estos sensores para la activación de una alarma o bocina. El centro de control posee un teclado para poder asignar una clave al sistema de seguridad, con la cual se activa o desactiva el sistema cuando uno lo requiere.

Las partes de este sistema son tres: conjunto de sensores, centro de control y actuadores.

2.2.14. Sensores

Sensores perimetrales. - Se encargan de vigilar el perímetro de una instalación. Se sitúan mayormente en la periferia de la edificación a proteger las puertas, ventanas, etc., estos pueden ser:

Sensores de vibración. - Estos se colocan sobre una superficie y cuando reciben un golpe o una vibración se produce una separación de dos masas lo que origina una interrupción del envío de la señal eléctrica, todo esto ocurre en el interior del sensor.

Sensores por cinta autoadhesiva conductora. - Es una cinta adhesiva de un material conductor que se adhiere a la superficie del cristal a proteger. La operatividad de este sensor radica en el material que debe actuar como un elemento conductor, éste generará una interrupción al romperse.

Sensores por contactos magnéticos. - Estos sensores son usados en puertas, ventanas y persianas. Su funcionamiento se basa en laminillas finas que por la acción de atracción del campo magnético formado por un imán cierran el circuito, lo que al interrumpir generan la apertura de este y activan la alarma. (Ramírez Marocho, 2012)

Sensores por radar o microondas. - Estos sensores constan de dos partes: emisor y receptor. El emisor emite ondas electromagnéticas que serán reflejadas por los objetos que se encuentren en el área que se protege, luego estas ondas vuelven al receptor. Una de las ventajas de estos sensores es que atraviesan finas superficies como son la madera, cristal, etc., lo que hace más efectivo su detección. (Ramírez Marocho, 2012)

Sensores por infrarrojo pasivo (PIR). - Son sensores que detectan el movimiento de un objeto en una determinada área mediante rayos infrarrojos. Estos rayos son invisibles y se transmiten en línea recta y

pueden ser reflejados por cualquier superficie brillante. El sensor detecta el movimiento de un cuerpo humano cuando éste altera la cantidad de rayos infrarrojos en un área, además se sabe que el cuerpo humano emite calor en forma de radiación infrarroja, por ende, son captados por los detectores. (Ramírez Marocho, 2012)

2.2.15. Arduino

Es una plataforma de creación electrónica, de código abierto, la cual está basada en hardware y software libre, flexible y fácil de utilizar para los creadores y desarrolladores. Esta plataforma permite crear diferentes tipos de microordenadores de una sola, se puede darles diferentes tipos de uso. (Fernández, 2020)

El hardware libre son los dispositivos cuyas especificaciones y diagramas son de acceso público, de manera que cualquiera puede replicarlos. Esto quiere decir que Arduino ofrece las bases para que cualquier otra persona o empresa pueda crear sus propias placas, pudiendo ser diferentes entre ellas, pero igualmente funcionales al partir de la misma base.

El software libre son los programas informáticos cuyo código es accesible para cualquiera que quiera utilizarlo y modificarlo. Arduino ofrece la plataforma Arduino IDE (Entorno de Desarrollo Integrado), que es un entorno de programación con el que cualquiera puede crear aplicaciones para las placas Arduino, de manera que se les puede dar todo tipo de utilidades. (Fernández, 2020)

Figura 16.

Plataforma Arduino.



Nota. Tomado de (U. Arduino, 2019).

Arduino Mega

El Arduino Mega 2560 es una placa de desarrollo basada en el microcontrolador ATmega2560. Tiene 54 entradas/salidas digitales (de las cuales 15 pueden ser usadas como salidas PWM), 16 entradas analógicas, 4 UARTs, un cristal de 16Mhz, conexión USB, jack para alimentación DC, conector ICSP, y un botón de reseteo.

Figura 17.

Placa Arduino Mega 2560.



Nota. Tomado de (U. Arduino, 2019).

Arduino Uno

Arduino Uno R3 SMD utiliza el microcontrolador ATmega328 en formato SMD. En adición a todas las características de las tarjetas anteriores, el Arduino Uno utiliza el ATmega16U2 para el manejo de

USB en lugar del 8U2 (o del FTDI encontrado en generaciones previas). Esto permite ratios de transferencia más rápidos y más memoria. No se necesitan drivers para Linux o Mac (el archivo inf para Windows es necesario y está incluido en el IDE de Arduino).

La tarjeta Arduino Uno R3 SMD incluso añade pins SDA y SCL cercanos al AREF. Es más, hay dos nuevos pines cerca del pin RESET. Uno es el IOREF, que permite a los shields adaptarse al voltaje brindado por la tarjeta. El otro pin no se encuentra conectado y está reservado para propósitos futuros. La tarjeta trabaja con todos los shields existentes y podrá adaptarse con los nuevos shields utilizando esos pines adicionales. (Arduino, 2019)

Figura 18.

Placa Arduino Uno.



Nota. Tomado de (Arduino, 2019).

Arduino Nano

Arduino Nano es una placa de desarrollo de tamaño compacto, completa y compatible con protoboards, basada en el microcontrolador ATmega328P. Tiene 14 pines de entrada/salida digital (de los cuales 6 pueden ser usando con PWM), 6 entradas analógicas, un cristal de

16Mhz, conexión Mini-USB, terminales para conexión ICSP y un botón de reseteo. (Arduino, 2019)

Figura 19.

Placa Arduino Nano.



Nota. Tomado de (Arduino, 2019).

Arduino MKR WiFi1010

El Arduino MKR WiFi 1010 es el punto de entrada más fácil para el diseño de aplicaciones básicas de IoT y pico-red. Ya sea que esté buscando construir una red de sensores conectados a su oficina o router doméstico, o si desea crear un dispositivo BLE que envíe datos a un teléfono celular, el MKR WiFi 1010 es su solución integral para muchos de los escenarios de aplicaciones básicas de IoT.

El procesador principal de la placa es un Arm® Cortex®-M0 SAMD21 de 32 bits de baja potencia, como en las otras placas de la familia MKR de Arduino. La conectividad WiFi y Bluetooth® se realiza con un módulo de u-blox, el NINA-W10, un chipset de baja potencia que opera en el rango de 2.4GHz. Además, la seguridad de la comunicación se garantiza a través del chip criptográfico Microchip® ECC508. Además de eso, se puede encontrar un cargador de batería, y un LED RGB direccionable a bordo.

Figura 20.

Placa Arduino MKR WiFi 1010.



Nota. Tomado de (U. Arduino, 2019)

Arduino Uno Wifi R2

Con esta placa podrás realizar proyectos conectados a internet, utilizando su chip criptográfico ECC608 seguro. El Arduino Uno WiFi es funcionalmente el mismo que el Arduino Uno Rev3, pero con la adición de WiFi / Bluetooth y algunas otras mejoras. (U. Arduino, 2019)

Incorpora un nuevo microprocesador de 8 bits de Microchip y tiene una IMU (Unidad de medición inercial) integrada.

El módulo Wi-Fi es un SoC autónomo con una pila de protocolos TCP / IP integrada que puede proporcionar acceso a una red Wi-Fi o actuar como un punto de acceso.

El Arduino Uno WiFi tiene 14 pines de entrada / salida digital (5 pueden usarse como salidas PWM), 6 entradas analógicas, una conexión USB, un conector de alimentación, un encabezado ICSP y un botón de reinicio. Contiene todo lo necesario para soportar el microcontrolador. Simplemente conéctelo a una computadora con un cable USB o enciéndalo con un adaptador de CA o batería para comenzar.

Figura 21.

Placa Arduino Uno Wifi.



Nota. Tomado de (U. Arduino, 2019).

Arduino Nano 33 IOT

Arduino Nano 33 IoT es una placa pequeña, robusta y potente con conectividad WiFi y Bluetooth, que, combinada con su arquitectura de bajo consumo, la convierte en una solución práctica y rentable para tus proyectos IoT. También es totalmente compatible con Arduino IoT Cloud, el criptochip ATECC608A almacena las claves criptográficas en hardware, ofreciendo un nivel muy alto de seguridad para este tipo de productos. La integración de Arduino Nano 33 IoT con Arduino IoT Cloud también ofrece una forma muy eficiente de configurar paneles en línea con poca codificación y un mínimo esfuerzo.

Figura 22.

Placa Arduino Nano 33 IOT.



Nota. Tomado de (Arduino, 2019)

Arduino Leonardo

Arduino Leonardo es la primera tarjeta de desarrollo que utiliza un microcontrolador con conectividad USB incluida, nos referimos al Atmega32U4. Como este microcontrolador está controlando directamente la conectividad USB, para lo cual existen librerías que permiten que la tarjeta Arduino Leonardo emule un teclado, mouse, joystick o bien el protocolo USB-HID.

Arduino Leonardo posee 20 pines de entrada y salida digitales (de los cuales 7 pueden ser usados como salidas PWM y 12 como entradas análogas), un cristal oscilador de 16MHz, una conexión microB USB, un Jack de alimentación, un header ICSP y un botón de reinicio.

Esta tarjeta incluye todo lo necesario para programar el microcontrolador Atmega32U4; simplemente conéctalo a un computador mediante un cable USB o energízalo con un transformador de 7 a 12VDC o una batería y comienza a programarlo. (L. Arduino, 2019)

Figura 23.

Placa Arduino Leonardo.



Nota. Tomado de (L. Arduino, 2019)

Arduino Portenta H7

La Portenta H7 ejecuta simultáneamente código de alto nivel junto con tareas en tiempo real. El diseño incluye dos procesadores que pueden ejecutar tareas en paralelo. Por ejemplo, es posible ejecutar el código compilado de Arduino junto con el de MicroPython, y tener ambos núcleos para comunicarse entre sí. La funcionalidad de Portenta es doble, puede funcionar como cualquier otra placa de microcontrolador incorporada, o como el procesador principal de una computadora incorporada.

Portenta puede ejecutar fácilmente procesos creados con TensorFlow™ Lite, podría tener uno de los núcleos computarizando un algoritmo de visión artificial, mientras que el otro podría estar haciendo operaciones de bajo nivel como el control de un motor, o actuando como una interfaz de usuario.

Figura 24.

Placa Arduino Portenta H7.



Nota. Tomado de (P. H. Arduino, 2019).

Arduino Nano 33 Ble Sense

Esta placa Arduino Nano está construida con el módulo NINA B306 para comunicación BLE y Bluetooth 5.0; el módulo está basado en el procesador nRF 52840 que contiene un potente Cortex M4F.

Su arquitectura, totalmente compatible con Arduino IDE, tiene una unidad de medición de inercia (IMU) de 9 ejes, sensores de temperatura, presión, humedad, luz, color e incluso gestos y un micrófono que se administra a través de nuestras bibliotecas especializadas. Su consumo de energía reducido, en comparación con otras placas del mismo tamaño, junto con el factor de forma Nano abre una amplia gama de aplicaciones. Esto permite el diseño de dispositivos portátiles y proyectos basados en gestos que necesitan comunicarse con otros dispositivos a corta distancia. Arduino Nano 33 BLE Sense es ideal para proyectos de automatización interactivos gracias a la radio multiprotocolo BT 5.0.

Figura 25.

Placa Arduino Nano Ble Sense.



Nota. Tomado de (Arduino, 2019).

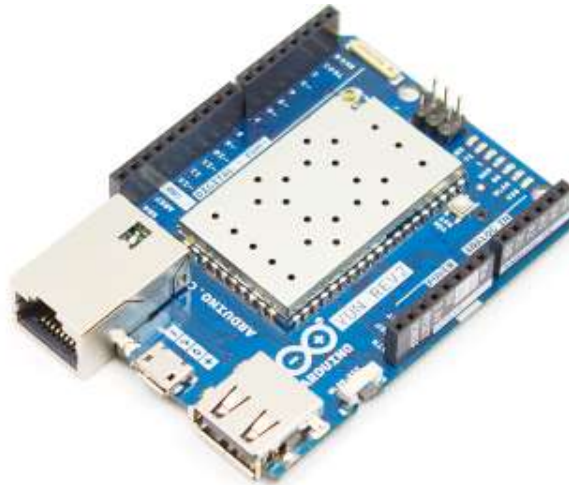
Arduino Yún

El Arduino Yún es una placa de microcontrolador basada en el ATmega32u4 y el Atheros AR9331. El procesador Atheros admite una distribución de Linux basada en OpenWrt llamada Linino OS. La placa tiene soporte incorporado para Ethernet y WiFi, un puerto USB-A, ranura para tarjeta micro-SD, 20 pines de entrada / salida digital (7 de ellos pueden usarse como salidas PWM y 12 como entradas analógicas), un cristal de 16 MHz oscilador, una conexión micro USB, un encabezado ICSP y 3 botones de reinicio. (U. Arduino, 2019)

La conexión a WiFi o red cableada es simple gracias al Panel Web de Yún y al sketch dedicado "YunFirstConfig". El panel web le permite administrar las preferencias del shield y cargar el código. El Yún Rev2 usa la biblioteca Bridge y por lo tanto amplía las capacidades de la placa mediante el uso del procesador Linux. Como siempre, todos los elementos de la plataforma (hardware, software y documentación) están disponibles libremente y son de código abierto.

Figura 26.

Placa Arduino Yún.



Nota. Tomado de (U. Arduino, 2019).

2.2.16. Módulo wifi NodeMcu V3 Esp8266

El módulo WiFi NodeMCU V3 ESP8266 es un kit de desarrollo que utiliza el ya popular chip ESP8266 (ESP-12E) que permite agregar conectividad WiFi a cualquier microcontrolador o hacer uso de su procesador y memoria interna para alojar cualquier aplicación que requiera de este tipo de conectividad.

El NodeMCU facilita el trabajo con el chip ESP8266 ya que en la board incluye un conversor FTDI y regulador de voltaje a 3,3V, de esta manera el módulo se conecta por USB al computador y está listo para programar. Este kit de desarrollo es de código abierto y utiliza el lenguaje de programación Lua.

Esta versión incluye un pin de salida (VU) de 5V proveniente directamente de la conexión USB, utiliza como conversor FTDI el chip CH340G (requiere driver, link de descarga en la documentación) y sus pines permiten que se monte fácilmente en un protoboard.

El ESP8266 es un chip altamente integrado diseñado para las necesidades de un nuevo mundo conectado. Ofrece una solución completa y autónoma de redes Wi-Fi, lo que le permite alojar la aplicación o servir como puente entre Internet y un microcontrolador.

Tiene potentes capacidades a bordo de procesamiento y almacenamiento que le permiten integrarse con sensores y dispositivos específicos de aplicación a través de sus GPIOs con un desarrollo mínimo y carga mínima durante el tiempo de ejecución. Su alto grado de integración en el chip permite una circuitería externa mínima, y la totalidad de la solución, incluyendo el módulo está diseñado para ocupar el área mínima en un PCB (Ssdielect, 2018).

Figura 27.

Imagen de la placa Módulo wifi NodeMcu.



Nota. Tomado de (Ssdielect, 2018).

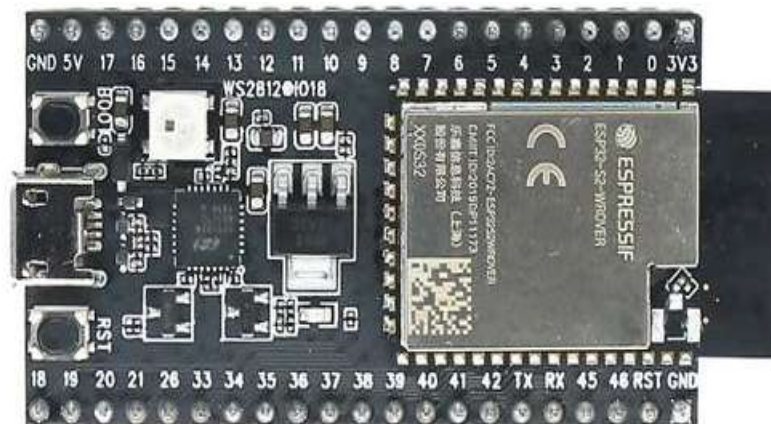
2.2.17. Módulo wifi Node ESP32

La placa de desarrollo o DEVKIT V1 NodeMCU-32 es una herramienta muy potente para el prototipado rápido de proyectos con IoT (Internet de las cosas). Integra en una placa el SoM ESP-WROOM-32 que tiene como base al SoC ESP32, el conversor USB-serial CP2102 necesario para programar por USB el ESP32, reguladores de voltaje y leds indicadores. La plataforma ESP32 es la evolución del ESP8266 mejorando sus capacidades de comunicación y procesamiento computacional. A nivel

de conectividad permite utilizar diversos protocolos de comunicación inalámbrica como: WiFi, Bluetooth y BLE. En cuanto a procesamiento su CPU 32-bit de dos núcleos de hasta 240Mhz que se pueden controlar independientemente. Además, incluye internamente una gran cantidad de periféricos para la conexión con: sensores táctiles capacitivos, sensor de efecto Hall, amplificadores de bajo ruido, interfaz para tarjeta SD, Ethernet, SPI de alta velocidad, UART, I2S e I2C. Aplicado en Mini Servidores Web, Procesamiento digital, Webcams, Cámara IP, Robótica móvil, Domótica y más.

Figura 28.

Imagen de la placa Módulo wifi NodeMcu ESP32.



Nota. Tomado de (Naylampmechatronics, 2021).

2.2.18. Wemos D1 Mini ESP8266 Wifi

tiene como núcleo al SoM ESP-12E que a su vez está basado en el SoC Wi-Fi ESP8266, integra además el conversor USB-Serial TTL CH340G y conector micro-USB necesario para la programación y comunicación a PC. Wemos D1 mini está diseñado especialmente para trabajar montado en protoboard o soldado sobre una placa. Posee un regulador de voltaje de 3.3V en placa, esto permite alimentar la placa directamente del puerto micro-USB o por los pines 5V y GND. Los pines de entradas/salidas (GPIO) trabajan a 3.3V por lo que para conexión a sistemas de 5V es

necesario utilizar conversores de nivel como: Conversor de nivel 3.3-5V 4CH o Conversor de nivel bidireccional 8CH - TXS0108E.

Figura 29.

Imagen de la placa Wemos D1 Mini ESP8266.



Nota. Tomado de (Naylampmechatronics, 2021).

2.2.19. Raspberry Pi 3

El Raspberry Pi 3 Modelo B es una computadora personal completa del tamaño de una pequeña placa de circuito, compuesto por un procesador ARMv8, 4 puertos USB, conexión HDMI, Ethernet, Wifi, Bluetooth y mucho más. Gracias a su procesador ARMv8 de 64-bits soporta el rango completo de distribuciones ARM GNU/Linux (Raspbian, XBMC, Snappy Ubuntu Core) y Microsoft Windows 10. Soporta herramientas de software libre como KOffice, Python, GNU IceCat, etc. Permite un uso flexible en: Juegos, Multimedia, Trabajo, Educación, Proyectos, etc. (Raspberry Pi, 2021)

El Raspberry Pi 3B es la tercera generación de Raspberry Pi, salió al mercado para reemplazar al modelo 2B en febrero del 2016. El factor de forma del Raspberry Pi 3 es idéntico al del 1B+ y 2B y es totalmente compatible con el Modelo 1 por lo que podemos utilizar el mismo case. Se recomienda el uso del modelo 3B en escuelas ya que ofrece un mejor

rendimiento a las versiones anteriores. El modelo A+ se recomienda para aplicaciones embebidas, donde se necesite un consumo menor de energía y un tamaño más compacto.

Figura 30.

Imagen de la placa Raspberry PI 3.



Nota. Tomado de (Raspberry Pi, 2021).

2.2.20. Módulo Wifi ESP8266

Está basado en el SoC (System on Chip) ESP8266, un chip altamente integrado, diseñado para las necesidades de un mundo conectado. Integra un potente procesador con Arquitectura de 32 bits (más potente que el Arduino Due) y conectividad Wifi. Ofrece una completa solución WiFi Networking, permitiéndole trabajar como host de aplicaciones o reducir la carga de WiFi Networking de otro procesador. El módulo puede trabajar en 2 modos: como estación Wifi (Wifi Station) o como Punto de Acceso (Access Point), al trabajar como estación el módulo se conecta a la red Wifi presente en nuestro hogar. El modo Access Point se usa si queremos crear una red propia en el chip y así conectarnos directamente.(E. Arduino, 2022)

El módulo ESP-01 viene cargado de fábrica con el firmware AT, que permite conectar un Arduino a wifi utilizando comandos AT. Es posible cambiar el firmware (flashear) permitiendo trabajar el módulo de forma

independiente (sin un Arduino) y usar toda su capacidad como microcontrolador de 32bits a 80Mhz. Para flasher el chip es necesario utilizar un módulo conversor usb a serial TTL como el Módulo CP2102.

Si optamos por utilizar el chip de forma independiente podemos desarrollar programas en los lenguajes Arduino y Lua. Trabajar dentro del entorno Arduino permite utilizar un lenguaje que ya conocemos y hacer uso de un IDE fácil de utilizar, además de hacer uso de toda la información sobre proyectos y librerías disponibles para Arduino. La comunidad de usuarios de Arduino es muy activa y da soporte a plataformas como el ESP8266. Al trabajar con Lua podemos experimentar con un lenguaje interpretado. (E. Arduino, 2022)

El módulo trabaja a 3.3V por lo que NO se debe alimentar con 5V. Se recomienda colocar un capacitor de 100uF en paralelo con la fuente de alimentación para filtrar los picos de corriente. Posee leds indicadores de alimentación y de comunicación.

Figura 31.

Imagen de la placa Módulo wifi NodeMcu.



Nota. Tomado de Avelectronics.

2.2.21. Sensor magnético de puerta MC-38

Sensor magnético para puertas, ventanas, etc. El sensor y el imán cierran o abren el circuito de acuerdo a si están cerca uno del otro. Estos sensores

se utilizan en proyectos de seguridad del hogar. De fácil integración con Arduino o Raspberry Pi, con lo cual es posible construir un completo sistema de seguridad.

Figura 32.

Imagen del sensor magnético MC38.



Nota. Tomado de (Naylampmechatronics, Sensor magnético de puerta MC-38, 2021).

2.2.22. Módulo PIR HC-SR501

Este módulo contiene un sensor Piroeléctrico, el cual puede detectar cambios de radiación infrarroja. Todo objeto (o cuerpo humano) emite cierto nivel de radiación, y entre mayor temperatura tenga, mayor radiación emitirá. El sensor dentro del detector de movimientos está dividido en 2 mitades o 2 lados. La razón para esto es que estamos buscando la diferencia en el movimiento no el promedio. Las dos mitades están unidas por cables de modo que se cancelan una a otra. Si una mitad recibe más o menos radiación IR, la salida cambiará a Alto o Bajo. (P. H. Arduino, 2019)

Los sensores PIR son perfectos para detectar cuando una persona ingresa o abandona un espacio, a partir de esto podemos programar diferentes acciones como el encendido/apagado automático de luces, sonidos, alarmas, mensajes de texto, llamadas, etc. Si bien son capaces de detectar

personas, no nos pueden decir cuántas, ni en qué dirección se encuentran y en algunos casos puede ser activado por mascotas, la clave está en experimentar y encontrar los valores de sensibilidad que funcionen adecuadamente.

Figura 33.

Imagen del sensor PIR.



Nota. Tomado de (Naylampmechatronics, Sensor magnético de puerta MC-38, 2021).

2.2.23. Sensor Final de Carrera

Dentro de la automatización industrial, existen multitud de dispositivos electrónicos que facilitan los procesos de producción. Los finales de carrera hoy en día, son imprescindibles en muchos de los mecanismos empleados en cualquier tipo de industria.

Un final de carrera o interruptor de posición, es un sensor que detecta la posición de un elemento móvil mediante accionamiento mecánico. Además de ser los sensores más instalados en el mundo, no dejan de ser sensores de contacto que necesitan estar en contacto con el objeto para detectar la llegada de un elemento móvil a una determinada posición. (Alicante, 2018)

La salida de los finales de carrera es binaria y la única información que nos da, es si el objeto está en una posición determinada o no. Hablando en términos tecnológicos, los finales de carrera son sensores

electromecánicos, por lo tanto, disponen de partes mecánicas enlazadas a partes eléctricas.

Figura 34.

Imagen del sensor final de carrera.



Nota. Tomado de (Naylampmechatronics, Sensor magnético de puerta MC-38, 2021).

2.2.24. Actuadores

Unidad central o centro de control

Es un conjunto de dispositivos electrónicos que básicamente se considera como el “cerebro de la instalación”. Su objetivo es interpretar y analizar las señales entregadas por los sensores que indican el intento de agresión y/o penetración en zona protegida. Asimismo, avisara a los encargados de la seguridad para generar una alerta o alarma. (Ramírez Marocho, 2012)

En la parte exterior de la carcasa se dispone una serie de indicadores que brindan información sobre el estado del sistema. En el interior posee una fuente recargable, que se alimenta permanentemente de la tensión de la red, en caso de corte de suministro eléctrico, este continúa generando la energía necesaria.

Actuadores ópticos

Estos actuadores son dispositivos que generan un tipo de señal visible o luminosa; por ello, en el mercado podemos encontrar gran variedad de este tipo de actuadores. Éstos pueden ser: focos, diodos emisores de luz (leds), matriz de leds, pantallas, etc.

Actuadores de llamada

Son aquellos dispositivos capaces de realizar un mecanismo de llamada cuando surge un problema con el equipo o ambiente, estos son ordenados a actuar o son activados por un controlador.

Actuadores acústicos

Los actuadores acústicos son los más comunes para la implementación de un sistema de seguridad y existen varios de este tipo que serán explicados a continuación:

Sirena. - Son las más llamativas y poderosas de todos los actuadores acústicos, por lo que se emplean en ambulancias, camiones de bomberos, sistemas de alarmas, etc. Su radio de alcance sobrepasa el kilómetro, en condiciones favorables, y sus tonos elevados sobrepasan prácticamente cualquier otro sonido exterior

Figura 35.

Sirena.



Nota. Tomado de (NaylampMecatronics, 2021)

Campanillas. - Es la más versátil de todos los actuadores, se emplean por lo general para alarmas contra ladrones o incendios, para compaginación de códigos y señales de horario. El tono varía del moderado y apacible hasta extremadamente insistente.

Zumbadores. - Son transductores electroacústicos que producen un sonido, zumbido continuo o intermitente de un mismo tono. Son populares para las alarmas en los edificios públicos, hospitales y otros lugares donde las demás señales no convienen.

2.2.25. Plataforma Iot

Para (Barrio Andrés, 2022) menciona en su libro Internet de las Cosas lo siguiente:

El «Internet de las Cosas» (Internet of Things, habitualmente referido por sus siglas inglesas IoT), también denominado por algunos «Internet de los Objetos» (IO) es un supraconcepto que caracteriza la próxima gran transformación en la evolución de Internet¹: su expansión más allá de la comunicación entre las personas, o entre las personas y el contenido digital, que ahora se extiende a miles de millones de objetos cotidianos. Los sistemas IoT implican la adquisición de datos de sensores y la entrega de órdenes a dispositivos que interactúan o forman parte del mundo real. También reconocen eventos y cambios, y pueden reaccionar de forma autónoma y apropiada. El internet de las cosas se equipará a menudo con electrodomésticos y bienes de consumo, como las ropas tecnológicas (wearables) o los coches inteligentes. Por lo tanto, muchas de las preocupaciones iniciales se han centrado en los productos de consumo. La atención a este fenómeno es urgente por muchas razones. La mayor parte del tráfico actual de Internet ya es originado por la interconexión de los objetos, no de las personas, y las proyecciones globales del impacto económico del IoT son potencialmente de once billones de euros para 2025. También es apremiante porque la expansión

de Internet en objetos cotidianos utilizados por las personas crea retos de interés público sin precedentes sobre cómo también transformará la intimidad-privacidad y la seguridad humana (incluyendo la ciberseguridad). (Barrio Andrés, 2022)

Samsung Artik

Artik es una plataforma abierta que incluye chips y placas de circuitos, además de memoria, software y otros servicios. Según la compañía “está diseñado para acelerar el desarrollo de una nueva generación de dispositivos IoT mejores y más inteligentes”. (Wootton, 2016)

La presencia de esta compañía en el Internet of Things ha presentad una variedad de placas de desarrollo que espera que sean adoptadas por los desarrolladores. Las placas Artik se ofrecen en varios tamaños y con varios grados de rendimiento, características y componentes, de forma que puedan ajustarse a dispositivos de lo más variado, desde un wereable, a sistemas residenciales, cámaras de video vigilancia, electrodoméstico, etc.

Figura 36.

Plataforma Artik Cloud.



Nota. Tomado de (Sigfox, 2018).

Blynk

Blynk fue diseñado para Internet de las cosas. Puede controlar el hardware de forma remota, puede mostrar datos de sensores, puede

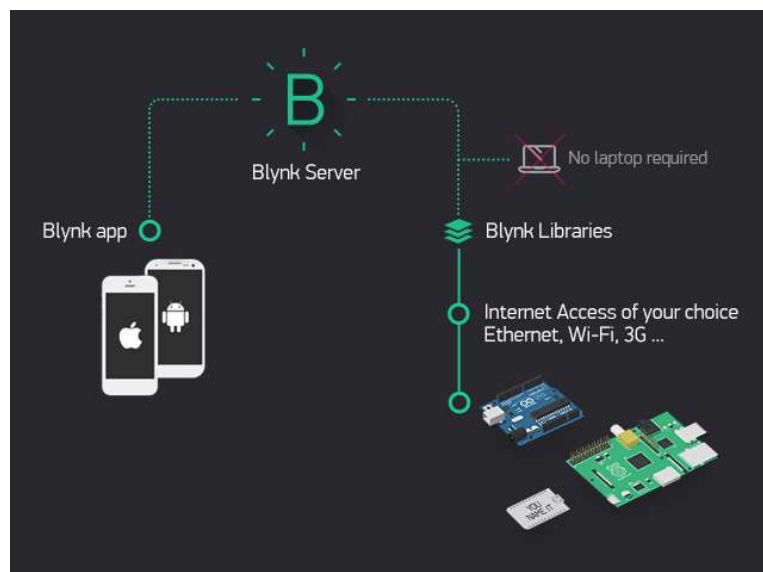
almacenar datos, visualizarlos y hacer muchas otras cosas interesantes. Tiene tres componentes principales en la plataforma: la aplicación Blynk que permite crear interfaces increíbles para sus proyectos utilizando varios widgets que proporcionamos. Blynk Server es el responsable de todas las comunicaciones entre el teléfono inteligente y el hardware y por ultimo las bibliotecas Blynk, para todas las plataformas de hardware populares, permiten la comunicación con el servidor y procesan todos los comandos entrantes y salientes.

Ahora imagine: cada vez que presiona un botón en la aplicación Blynk, el mensaje viaja al espacio de la nube Blynk, donde mágicamente encuentra su camino hacia su hardware pudiéndose observar, esto funciona de igual manera en la dirección opuesta.

La aplicación Blynk es un creador de interfaces bien diseñado. Funciona tanto en iOS como en Android.

Figura 37.

Imagen de la plataforma de Blynk.



Nota. Tomado de (Blynk, 2016).

Domoticz

Es un software libre de control domótico disponible para las plataformas Windows y Linux, y también, está disponible para la tarjeta Raspberry Pi. Eso nos abre muchas posibilidades ya que nos permite montarlo como un centro de control domótico low cost, lo que no significa en absoluto que sea una solución menor ya que ese software ofrece cosas muy interesantes.(Pérez Morales, 2018)

Se caracteriza por consumir pocos recursos del sistema y ofrecer soporte para diversos protocolos domóticos, como Z-Wave, RF, X10, EnOcean. Los dispositivos domóticos que puede controlar Domoticz son pues muy numerosos y variados, además de cámaras IP. Permite crear dispositivos virtuales y admite scripts en Lua. En cuanto a las escenas domóticas, la interfaz es muy sencilla y adopta la misma filosofía que la de servidores domóticos muy conocidos como la Zipabox o el propio Home Center de Fibaro.

Existen aplicaciones móviles tanto para iOS (iDomotic) como para Android (Andromoticz y Dromotica), además de ser compatible con las notificaciones por mail y los sistemas de notificaciones Pushover, Powl y NMA en dispositivos móviles.

Figura 38.

Imagen de la plataforma Domoticz.



Nota. Tomado de (Domoticadomestica, 2020).

ZETTA

Zetta es una plataforma de IoT de código abierto orientada al servidor construida en Node.js. Zetta combina REST API, WebSockets y programación reactiva. Puede ejecutarse en una computadora de placa única, computadora personal o en la nube, y puede conectar diferentes plataformas como Linux, BeagleBones, Raspberry Pis, placa de desarrollo Arduino y PC con plataformas en la nube como Heroku para crear una red distribuida geográficamente. También puede transferir datos a plataformas de análisis de máquinas como Splunk. (Navas-Damas, 2018)

Figura 39.

Imagen de la plataforma Zetta.



Nota. Tomado de (Programmerclick, 2020).

Node-RED

Es una herramienta de programación visual. Muestra visualmente las relaciones y funciones, y permite al usuario programar sin tener que escribir una línea. Node-RED es un editor de flujo basado en el navegador donde se puede añadir o eliminar nodos y conectarlos entre sí con el fin de hacer que se comuniquen entre ellos.

Node-RED es una herramienta muy potente que sirve para comunicar hardware y servicios de una forma muy rápida y sencilla. Simplifica enormemente la tarea de programar del lado del servidor gracias a la programación visual.

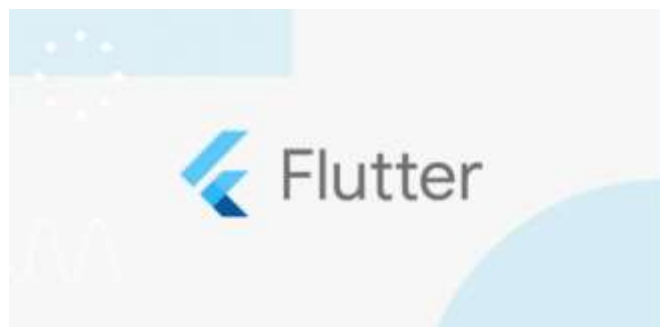
Figura 40.

Imagen de la plataforma Node-RED.

importante es que el código Dart puede ejecutarse no solo en iOS y Android, sino que también se puede usar para escritorio (Windows, Mac y Linux) e incluso aplicaciones web. Hasta la fecha, la oferta de Flutter para escritorio y web es limitada y las aplicaciones no son tan estables como las versiones móviles. Pero la posibilidad de escribir un código unificado para tantas plataformas es increíble, en términos de productividad, de mantenimiento y, lo que es más importante, de negocios.

Figura 41.

Imagen de la plataforma Flutter.



Nota. Tomado de (Geekflare, Geekflare, 2019).

M2MLabs Mainspring

M2M es una tecnología, principalmente porque no requiere ninguna tecnología inalámbrica o dispositivos digitales complejos. Una conexión por cable entre dos máquinas puede aún ser considerada como M2M, y de hecho las primeras versiones de esta tecnología usaban líneas telefónicas para comunicarse. Sin embargo, en el mundo moderno, M2M usualmente se refiere a máquinas que se comunican usando cosas como el Wifi o redes móviles. (Peralta & Martin, s. f.)

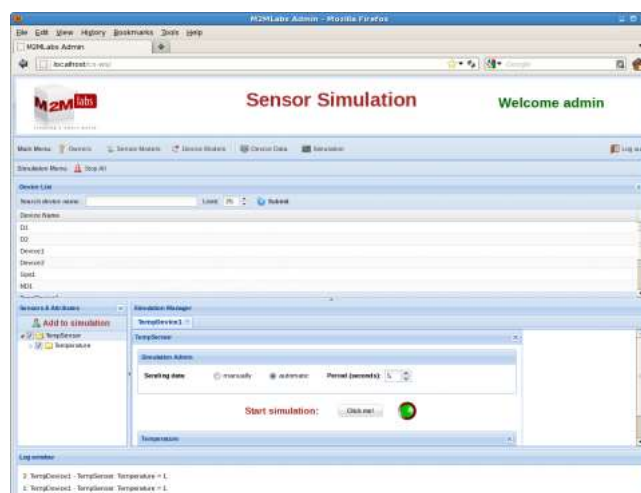
M2MLabs Mainspring es un marco de aplicación para la creación de aplicaciones de máquina a máquina, como el seguimiento de vehículos o la supervisión remota de máquinas. En tales aplicaciones, por lo general,

un dispositivo remoto equipado con sensores (por ejemplo, gps, temperatura, presión) y actores se comunica con una aplicación de servidor que ejecuta el protocolo de comunicación del dispositivo, la configuración del dispositivo, el almacenamiento de datos enviados por los dispositivos y la lógica comercial de la aplicación. y la capa de presentación.

Mainspring se encarga de la comunicación del dispositivo, la configuración, así como el almacenamiento y la recuperación de datos para que los desarrolladores de aplicaciones puedan centrarse exclusivamente en la lógica empresarial. Las aplicaciones M2M pueden crearse un prototipo en horas en lugar de semanas y finalmente transferirse a un entorno de ejecución de alto rendimiento construido sobre un servidor J2EE estándar y la base de datos Apache Cassandra altamente escalable.(Peralta & Martin, s. f.)

Figura 42.

Imagen de la plataforma M2MLabs Mainspring.



Nota. Tomado de (M2mlabs, 2015).

ThingsBoard

Es una plataforma centrada en la gestión de la IoT. Esta tecnología cada vez cobra más peso, y es la base para conseguir una ciudad inteligente que mejore las condiciones de vida de sus habitantes. Para conocerla a fondo, a continuación, explicamos qué es esta plataforma y cuáles son sus principales ventajas. Es de código abierto y está centrada en permitir un rápido desarrollo, gestión y escalado de proyectos relacionados con esta tecnología. Además, en ella tendremos acceso a una solución local o en la nube, que estará lista para usar y que habilitará la infraestructura del lado del servidor para las aplicaciones que vayan a utilizarse.

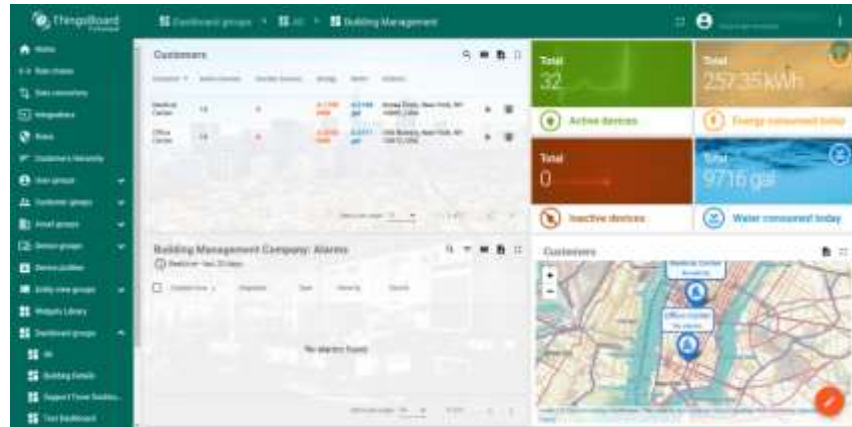
Es compatible con los protocolos de IoT estándar de la industria: MQTT, CoAP y HTTP. Consigue combinar escalabilidad, tolerancia a los fallos y un buen rendimiento a la hora de capturar los datos del dispositivo para su procesamiento y control. Esto es posible gracias a que dispone de un servidor de puerta de enlace que se encarga de la comunicación con los dispositivos conectados a la red. Así se logra una gestión ágil y en permanente actualización.

Está construida alrededor de Netty Framework, que brinda soporte para una amplia variedad de protocolos y aplicaciones. Asimismo, se pueden agregar nuevos protocolos de hardware simplemente añadiendo controladores de canal de entrada y salida.

Es una plataforma de gestión de smart city que pueden aprovechar las provincias; esto se debe a su naturaleza de código abierto. Así, ante un cambio de proveedor como resultado de una licitación, el nuevo no tendrá problemas para adaptarse, lo que contribuye a limitar las ataduras y a buscar siempre las mejores soluciones disponibles en el mercado. Al final los ciudadanos son los que salen ganando, al disfrutar de una ciudad moderna y eficiente.

Figura 43.

Imagen de la plataforma ThingsBoard.



Nota. Tomado de (M2mlabs, 2015).

Kinoma

La plataforma de creación de prototipos de hardware de Marvell Semiconductor, involucra tres proyectos de código abierto diferentes. Kimona Create es un kit de construcción de bricolaje para la creación de prototipos de dispositivos electrónicos. Kimona Studio es el entorno de desarrollo que funciona con Set up y Kinoma Platform Runtime. Kimona Connect es una aplicación gratuita para sistema operativo android que vincula teléfonos inteligentes y soportes con dispositivos IoT. (mattwojo, 2020)

Figura 44.

Imagen de la plataforma Kinoma.



Nota. Tomado de (Geekflare, 2015).

Kaa IoT Platform

Es una plataforma de extremo a extremo para IoT de nivel empresarial, Kaa te pone al día con una amplia gama de tecnologías modernas de internet de las cosas y, al mismo tiempo, te brinda flexibilidad para adaptarlo todo a tu dominio empresarial específico. Para garantizar los mejores resultados, este equipo siempre brinda asistencia a los clientes cuando necesitan ayuda para desarrollar una estrategia de IoT sostenible o un producto exitoso, ya sea un punto de contacto (PoC) o un proyecto de internet de las cosas (IoT) en toda regla. (Espinosa et al., 2020).

Se monta desde pequeñas empresas emergentes hasta una gran empresa y contiene modelos de implementación avanzados para soluciones de IoT de múltiples nubes. Se basa principalmente en micro servicios flexibles y se adapta fácilmente a prácticamente cualquier necesidad y aplicación

Figura 45.

Imagen de la plataforma Kaa IoT.



Nota. Tomado de (Geekflare, 2015).

Arduino Cloud

Arduino IoT Cloud es un servicio poderoso que permite a cualquier persona crear aplicaciones de IoT con solo unos simples pasos. Con una

combinación de tecnología inteligente, interfaces fáciles de usar y funciones poderosas, nuestra nube es para todos: estudiantes, creadores, profesionales por igual. (Salgado Castillo & Coello Moncayo, 2015) (Urbina et al., 2014)

La última versión de Arduino IoT Cloud incluye características como:
Vinculado directamente al entorno de creación.

Bocetos generados automáticamente.

Construcción de redes de sensores.

Monitoreo de datos en tiempo real.

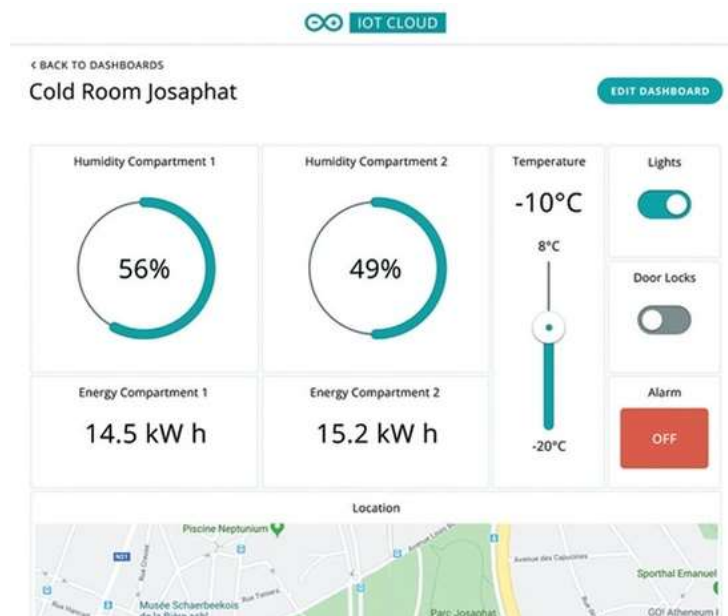
Compatibilidad con Wi-Fi y LoRa.

Cree un panel con más de 15 widgets únicos.

Cree su propia aplicación utilizando Arduino IoT API.

Figura 46.

Plataforma Arduino Cloud.



Nota. Tomado de (Arduino, 2016).

2.3. Hipótesis

2.3.1. Hipótesis general

- El diseño y la implementación del sistema de alarma permite alertar de robo y/o intento de robo en las viviendas.

2.3.2. Hipótesis específica

- El sistema IoT, basado en la plataforma Blynk activa y desactiva la alarma para alertar el robo y/o intento de robo.
- El sistema IoT, basado en la plataforma Blynk monitorea el estado de la alarma.

2.4. Definición de términos

1. **Control:** Es la acción de ejercer algún tipo de poder para obligar el comportamiento de cierto elemento con el fin de lograr un objetivo específico. (Ogata, 2010)

Existen básicamente dos tipos de control industrial:

- a. **Control de lazo abierto:** Es un sistema de control en donde la señal de salida no determina el valor de la señal de entrada, generalmente son sistemas temporizados.
 - b. **Control de lazo cerrado:** Es un sistema en donde la señal de salida se retroalimenta y afecta la señal de entrada con la intención de mantener una relación pre establecida entre la entrada y salida.
2. **Control supervisorio:** Es un sistema en el que la información de diferentes parámetros dispersos se concentra en un lugar para su procesamiento y como criterio para ejecutar alguna acción de control. Se puede definir como el monitoreo y control de procesos. (Acevedo, 2012)

Las acciones de control se pueden clasificar de la siguiente forma:

- a) Manual. - El usuario decide 100% las acciones a ejecutar.
- b) Semiautomático. - Algunas actividades se realizan de manera automática y algunas se dejan a discreción del usuario.

c) Automático. - Todas las acciones se ejecutan de manera automática.

3. **Señal analógica:** Está definida como aquella que es continua en el tiempo y que puede tener un valor cualquiera dentro de un rango definido; es generada por algún tipo de fenómeno electromagnético y que es representable por una función matemática continua en la que es variable su amplitud y periodo en función del tiempo. (Vega & Maza, 2003) (Tomasi, 2010).
4. **Señal digital:** Está definida como aquella que solamente puede tener dos valores (1 ó 0) y es discreta en el tiempo. (Tomasi, 2010)
5. **Sistema:** Es un grupo de elementos que trabajan de manera conjunta para lograr un objetivo. (Urbina et al., 2014)
6. **Sistema de adquisición de datos:** Es un sistema cuyo fin primario es la recolección y procesamiento de datos para su posterior almacenamiento, despliegue, transmisión o manipulación matemática para la obtención de información adicional. (Vizcaíno & Sebastián, 2011)
7. **Sistemas de Autómata:** El propósito de los sistemas de autómata es coleccionar datos de un lugar lejano o de difícil acceso y transmitir los datos a un lugar donde estos podrán ser evaluados. Por lo general, los sistemas de telemetría son usados en las pruebas de movimiento de vehículos como automóviles, aeronaves y misiles. (Balcells et al., 1997)

Los sistemas de telemetría son un conjunto especial de los sistemas de comunicaciones. Cuando la telemetría es usada para control y colección de datos, se aplica el término supervisión y control a datos adquiridos. (Mattos, 2004)
8. **Sistemas de Telecontrol:** Los sistemas de Telecontrol, permiten haciendo uso de un sistema de telecomunicaciones, controlar a distancia un elemento o una variable de otro sistema, esto con múltiples objetivos como por ejemplo dar seguridad a los trabajadores cuando tienen que trabajar en ambientes de alto riesgo para su integridad, o lugares de difícil acceso o distanciados de donde se encuentran quienes desean controlar el sistema. Telecontrol a diferencia de la telemetría, involucra la manipulación o control

de un elemento o un sistema a distancia ya que telemetría solo involucra su medición. (Canales, 2010)

9. **Tiempo real:** Significa que un dispositivo de medida es capaz de mostrar el valor de una variable en el instante preciso en que la misma efectivamente tiene ese valor. (Stremmler, 1989).

Cuando se emplea computadoras, controladores o cualquier dispositivo que funciona en base a un programa de computación para procesar información de campo, aparece un desfase en el tiempo o un retardo, que puede incidir en la exactitud instantánea del valor mostrado. Esta falta de exactitud puede pasar desapercibida, particularmente en la medición de variables “lentas” o puede ser considerable si se trata de variables “rápidas”.

2.5. Definición operativa de variables

El funcionamiento del sistema IOT está en función de la detección por movimiento y apertura de puertas realizado por intrusos dentro del hogar.

$$ADA = f(SA)$$

2.5.1. Variables dependientes

SA: Sistema de alarma.

2.5.2. Variables independientes

ADA: activación y desactivación de la alarma

2.5.3. Definición operacional de variables

Tabla N° 1

Las variables, indicador y unidad de medida.

VARIABLE DEPENDIENTE	INDICADOR	INSTRUMENTO
Sistema de alarma (SA)	Monitoreo de Activación y desactivación de alarma	Observación
	Visualización del estado de alarma	
VARIABLE INDEPENDIENTE	INDICADOR	INSTRUMENTO
Activación y desactivación de la alarma (ADA)	- Apagada - Encendida	Monitoreo por aplicativo

Nota. Elaboración propia.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1 Ámbito de estudio

3.1.1 Ámbito temporal

El estudio tuvo una duración de 15 días, empezó el 01 de noviembre del 2021 y culminó el 15 de noviembre del 2021.

3.1.2 Ámbito espacial

El estudio se realizó en la zona geográfica que conforma la jurisdicción del distrito de Pampas, Tayacaja, región de Huancavelica, cuya plaza principal está ubicada a las coordenadas -12.39790479939864, -74.86837504067644 y a unos 3270 metros sobre el nivel de mar.

Figura 47.

Ubicación geográfica de la ciudad de Pampas, Tayacaja.



Nota. Tomado de (GoogleMaps, 2001).

3.2 Tipo y nivel de investigación

3.2.1 Tipo de investigación

Según el propósito, es aplicada, debido que permitió generar conocimientos que se puedan poner en práctica en el sector de seguridad, con el fin de impulsar un impacto positivo en la vida cotidiana de las personas con el apoyo de la telemetría.

La investigación aplicada busca la generación de conocimiento con aplicación directa a los problemas de la sociedad o el sector de seguridad. Esta se basa fundamentalmente en los hallazgos tecnológicos de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto. (Lozada, 2014)

3.2.2 Nivel de investigación

El nivel de investigación es correlacional. (Sampieri et al., 2014) menciona que “este tipo de estudios tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en una muestra o contexto en particular.

3.3 Método de investigación

En esta investigación se empleó el método científico y como método particular el experimental ya que se utilizó como procesos lógicos la inducción y deducción que permitieron evidenciar la automatización efectiva del proceso de activación y desactivación de la alarma.

“En la investigación de enfoque experimental el investigador manipula una o más variables de estudio, para controlar el aumento o disminución de esas variables y su efecto en las conductas observadas”. (Alonso, et. al, 2021)

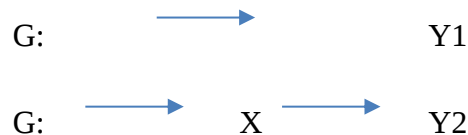
Hernández, et al. (2014) afirma que un enfoque cuantitativo “se vale de la lógica o razonamiento deductivo, que comienza con la teoría, y de ésta se derivan

expresiones lógicas denominadas hipótesis que el investigador somete a prueba”.
(p.6)

“Según el enfoque cuantitativo-deductivo, el estudiante plantearía su problema de investigación definiendo su objetivo y su pregunta (lo que quiere hacer y lo que quiere saber)”. (Hernández, et al., 2014, p.13)

3.4 Diseño de investigación

Para ejecutar el presente proyecto se utilizó el diseño experimental estos diseños llegan a incluir una o más variables independientes y uno o más dependientes. En nuestro diseño, se trata de comparar un grupo de control y un grupo experimental.



Dónde:

G : Muestra de Investigación.

X : Experimento

Y1 : Resultados de la variable sin experimento.

Y2 : Resultados de la variable con experimento.

3.5 Población y muestra

3.5.1. Población

Está constituida por los infinitos valores de mensajes de textos enviados por el transmisor del sistema de telemetría.

3.5.2. Muestra

Las muestras se establecen por cada una de las hipótesis de acuerdo al

tipo de su distribución. El tamaño de la muestra, para una población N infinita, se establece de acuerdo a la siguiente fórmula:

$$n = \frac{Z^2(P)(1 - P)}{E^2}$$

Dónde:

n : Tamaño de la muestra

Z : Nivel de confianza o coeficiente de confianza.

E : Error de la muestra o error permitido.

P : Proporción de unidades que poseen el atributo de interés

Reemplazando los valores en la ecuación anterior, obtenemos como resultado:

$$n = \frac{1.96^2(0.5)(1 - 0.5)}{0.05^2}$$

$$n = \frac{0.9604}{0.0025}$$

$$n \cong 384.26$$

Por lo tanto se tomaran 384 datos para el indicador de activacion y desactivación de la alarma.

3.5.3. Muestreo

El muestreo es aleatorio simple porque cada uno de los datos o elementos de la población posee la misma probabilidad de ser elegido para integrar la muestra.

3.6 Técnicas e instrumentos de recolección de datos

Es un aspecto muy importante en el proceso de una investigación (Fernández Collado , 2014), es el que tiene relación con la obtención de la información, pues de ello depende de la confiabilidad y validez de estudio. Obtener información confiable y válida requiere cuidado y dedicación. Esta etapa de recolección de información de investigación se conoce como toma de datos.

3.6.1. Técnicas de recolección de datos: En la presente investigación, se ha empleado las siguientes técnicas de recolección de datos.

Observación directa: Este método de recolección de datos consiste en el registro sistemático, válido y confiable de comportamientos y situaciones observables, en este proyecto se realizará las siguientes tablas:

Remoto automatizado: este método de recolección de datos consiste en adquirir los datos de variables mediante software y módulos de transmisión. Para este proyecto se utilizó los módulos de Wi-Fi y para procesar los datos se utilizó la plataforma Blynk para almacenar los datos, que después se trasladó a Microsoft Excel.

3.6.2. Instrumentos de recolección de datos: Son los medios o recursos que se elaboran y se aplican para registrar los datos hallados en la muestra de acuerdo a los indicadores que tenemos.

El instrumento de recolección de datos permitió registrar los datos de la activación y desactivación de la alarma por un aplicativo IoT.

Tabla N° 2

Instrumento de recolección de datos de activación de alarma.

Datos	Activación y desactivación de alarma IoT	Estado deseado de alarma	Estado actual de la alarma	¿Estado actual es igual a estado deseado de la alarma?
1				
2				
3				
4				

Nota. Elaboración propia.

Tabla N° 3

Instrumento de recolección de datos de monitoreo de la alarma.

Datos	Monitoreo de alarma IoT	Estado deseado de alarma en el aplicativo	Estado actual de la alarma en el aplicativo	¿Estado actual es igual a estado deseado de la alarma en el aplicativo?
1				
2				
3				
4				

Nota. Elaboración propia.

3.7 Procedimiento de recolección de datos

Los datos se recogieron aleatoriamente, por cada indicador recolectamos 384 muestras, se tomaron cada 10 minutos por 7 días, considerando que se tomaron los datos durante 10 horas diarias y que fueron almacenadas en los instrumentos de recolección de datos.

3.8 Técnicas de procesamiento y análisis de datos

Para procesar los datos del trabajo se aplicará la técnica de procesamiento apareado y se realiza el análisis estadístico de significancia utilizando la prueba *t* de Student por tratarse de 384 datos y con un nivel de confianza de 95 %.

Para la prueba de hipótesis se formuló las hipótesis nulas y alternas. Para averiguar si se rechaza o se acepta la hipótesis nula.

Para la activación y desactivación de la alarma

H₀: La plataforma IoT Blynk no activa y desactiva la alarma.

H_a: La plataforma IoT Blynk activa y desactiva la alarma.

Para el monitoreo del estado de la alarma

H₀: la plataforma IoT Blynk no monitorea el estado de la alarma

H_a: la plataforma IoT Blynk monitorea el estado de la alarma.

CAPÍTULO IV

DISCUSIÓN DE RESULTADOS

4.1 Análisis de información

Para la obtención de resultados se tomaron 420 datos para saber si la plataforma Blynk puede activar o desactivar la alarma y se tomaron 420 datos para saber si la plataforma Blynk monitorea el estado de la alarma.

Activación y desactivación de alarma

Se registraron 384 datos durante 7 días cada 10 minutos por 10 horas diarias, a partir del 01 de noviembre 2021 hasta el 7 de noviembre del 2021, teniendo el sistema con acceso a internet y el aplicativo del móvil con acceso a internet. Estos datos están registrados en la Tabla B.1 del Anexo B.

Monitoreo del estado de la alarma

Se registraron 384 datos durante 7 días cada 10 minutos por 10 horas diarias, a partir del 01 de noviembre 2021 hasta el 7 de noviembre del 2021, teniendo el sistema con acceso a internet y el aplicativo del móvil con acceso a internet. Estos datos están registrados en la Tabla B.2 del Anexo B.

4.2 Prueba de hipótesis

a) Prueba de estadística de la activación y desactivación de alarma por la plataforma Blynk

Para saber si la activación y desactivación de la alarma por la plataforma Blynk se ejecuta, se determinó el porcentaje de datos donde el estado actual de la alarma es igual al estado deseado de la alarma.

En la figura 48 se muestra que el 97.4 % del estado de activación y desactivación de la alarma por plataforma Blynk es igual al estado deseado de la alarma.

La correlación y desviación estándar de las muestras relacionadas fueron analizadas con el programa SPSS, cuyos resultados se muestran en la tabla N°4 y en la tabla N°5.

Figura 48.

Correlación de estado actual con el estado deseado.



Nota. Elaboración propia.

Tabla N° 4

Estadística de muestras relacionadas.

Estadísticos de muestras relacionadas					
		Media	N	Desviación típ.	Error típ. de la media
Par 1	Estado_deseado	1,4740	384	,49997	,02551
	Estado_actual	1,4844	384	,50041	,02554

Nota. Elaboración propia.

Tabla N° 5

Correlación de muestras relacionadas.

Correlaciones de muestras relacionadas

	N	Correlación	Sig.
Par 1 Estado_deseado y Estado_actual	384	,948	,000

Nota. Elaboración propia.

Tabla N° 6

Prueba de muestras relacionadas.

Prueba de muestras relacionadas

		Diferencias relacionadas				t	gl	Sig. (bilateral)	
		Media	Desviación tip.	Error tip. de la media	95% Intervalo de confianza para la diferencia				
					Inferior				Superior
Par 1	Estado_deseado - Estado_actual	-,01042	,16125	,00823	-,02660	,00576	-1,266	383	,206

Nota. Elaboración propia.

Prueba de hipótesis específica

La plataforma IoT Blynk activa y desactiva la alarma

H₀: La plataforma IoT Blynk no activa y desactiva la alarma.

$$\mathbf{H_0:} \mu_1 = \mu_2$$

Donde:

μ_1 : media deseada de activación y desactivación de la alarma por la plataforma Blynk

μ_2 : media de la activación y desactivación de la alarma por la plataforma Blynk

H_a: La plataforma IoT Blynk activa y desactiva la alarma.

$$\mathbf{H_0:} \mu_1 \neq \mu_2$$

Donde:

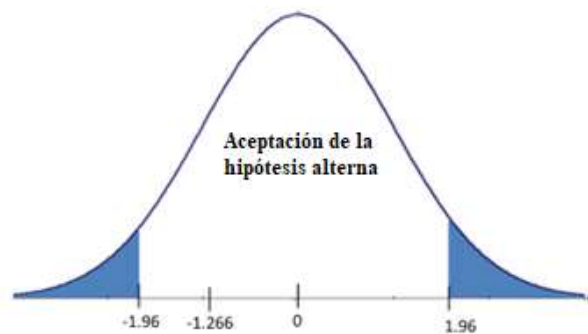
μ_1 : media deseada de activación y desactivación de la alarma por la plataforma Blynk

u_2 : media de la activación y desactivación de la alarma por la plataforma Blynk

Prueba de hipótesis

Figura 49.

distribución de t estadístico.



Nota. Elaboración propia.

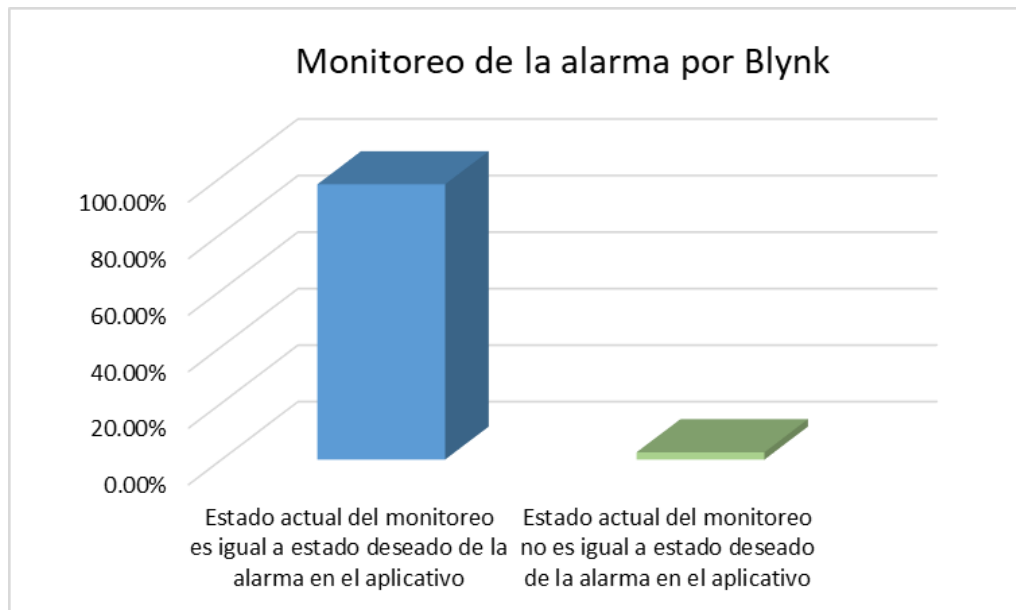
En la tabla N° 6 se puede observar que el valor obtenido de “t” es -1.266, ubicamos este valor en la Campana de Gauss que se puede observar en la figura 49. En esta figura se observa que este valor de “t” está dentro de la región de aceptación de la hipótesis alterna.

b) Prueba de estadística para el monitoreo del estado de la alarma por la plataforma Blynk

En la figura 50 se puede observar que el 97.40 % del estado deseado del monitoreo de la alarma se puede monitorear a través del aplicativo es igual al estado actual del monitoreo del estado de la alarma a través del aplicativo diseñado en la plataforma Blynk. La correlación y desviación estándar de las muestras tomadas fueron analizados por SPSS, cuyos resultados se muestran en las tablas N° 7, 8 y 9.

Figura 50.

Monitoreo de la alarma por la plataforma Blynk.



Nota. Elaboración propia.

Tabla N° 7

Prueba de muestras relacionadas.

Estadísticos de muestras relacionadas					
		Media	N	Desviación típ.	Error típ. de la media
Par 1	Monitoreo_de_la_alarma	1,4740	384	,49997	,02551
	Estado_actual_de_la_alarma	1,4844	384	,50041	,02554

Nota. Elaboración propia.

Tabla N° 8

Prueba de muestras relacionadas.

Correlaciones de muestras relacionadas				
		N	Correlación	Sig.
Par 1	Monitoreo_de_la_alarma y Estado_actual_de_la_alarma	384	,948	,000

Nota. Elaboración propia.

Tabla N° 9

Prueba de muestras relacionadas.

Prueba de muestras relacionadas									
		Diferencias relacionadas				t	gl	Sig. (bilateral)	
		Media	Desviación tip.	Error tip. de la media	95% Intervalo de confianza para la diferencia				
					Inferior				Superior
Par 1	Monitoreo_de_la_alarma - Estado_actual_de_la_alarma	-,01042	,16125	,00823	-,02660	,00576	-1,266	383	,206

Nota. Elaboración propia.

Prueba de hipótesis específica

La plataforma IoT Blynk monitorea el estado de la alarma

H₀: la plataforma IoT Blynk no monitorea el estado de la alarma

H₀: $u_1 = u_2$

Donde:

u_1 : media deseada del monitoreo de la alarma por la plataforma Blynk

u_2 : media del monitoreo de la alarma por la plataforma Blynk

H_a: la plataforma IoT Blynk monitorea el estado de la alarma.

H₀: $u_1 \neq u_2$

Donde:

u_1 : media deseada del monitoreo de la alarma por la plataforma Blynk

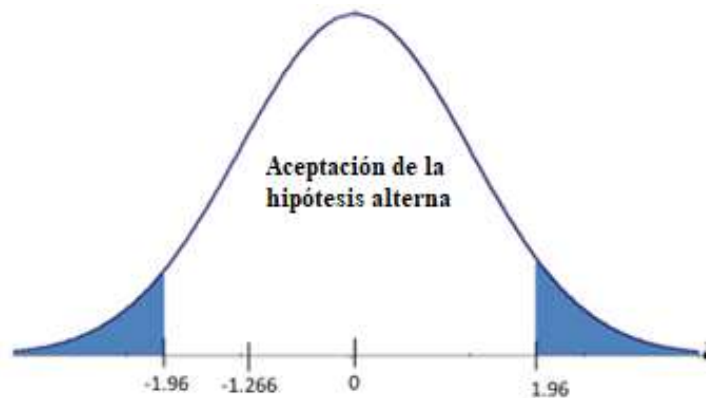
u_2 : media del monitoreo de la alarma por la plataforma Blynk

Prueba de hipótesis

figura 51. En esta figura se observa que este valor de “t” está dentro de la región de aceptación de la hipótesis nula.

Figura 51.

distribución de t estadístico.



Nota. Elaboración propia.

En consecuencia, se acepta todas las hipótesis planteadas en esta investigación.

4.3 Discusión de resultados

Una vez concluida la investigación, análisis de información y prueba de hipótesis, se señala lo siguiente:

1. En la tesis titulada “Diseñar un Sistema de Alarma Inalámbrico de bajo costo para la Protección de Viviendas tipo, en sectores de bajo recursos Económicos de la Ciudad de Guayaquil”. Eligieron una topología tipo estrella por ser la más apropiada para el diseño de las viviendas, colocaron varios sensores de captura de movimiento de las personas no autorizadas, cubre las áreas externas e internas de la vivienda.

Esta investigación se realizó con un prototipo de vivienda donde se colocó sensores de contacto en la puerta principal de la casa, en el segundo piso y en la cochera. Con estos sensores colocados se pueden detectar el robo y/o intento de robo de las casas.

2. De la tesis titulada “Diseño e Implementación de un Sistema de Seguridad Inalámbrico con Tecnología Bluetooth para Vivienda”, se utilizó la

tecnología bluetooth lo cual tiene un rango de conexión, uno de los objetivos era determinar el tiempo de retardo para la activación, la cual fue de 10 segundos.

En nuestra tesis se colocó como retardo para la activación de la alarma de 30 segundos. La tecnología que utilizamos fue la tecnología IoT la cual tiene conexión con internet, en la actualidad todos los celulares tienen el uso de datos el cual proporciona acceso a internet, esto hace que tengamos conexión con el sistema creado las 24 horas del día y de cualquier lugar del mundo, solo se necesita acceso a internet del sistema y del punto de control/monitoreo.

3. En la tesis "Domótica de Seguridad por medio de SMS", el objetivo principal fue solucionar el problema de mantener vigilado un recinto mientras la familia o los usuarios del inmueble no se encontraban e incluso cuando estaban presentes mediante un desarrollo un sistema de control de seguridad la cual se manipule a distancia mediante mensajes.

En nuestra tesis se usó la plataforma IoT Blynk, la cual se encarga de monitorear y controlar el estado de la alarma, también se consideró si los propietarios de la vivienda estaban dentro o fuera de la vivienda para activar y desactivar la alarma.

La contribución que se realizó con esta tesis fue crear un prototipo de sistema de alarma que previene el robo y/o intento de robo que puede sufrir una propiedad o un inmueble, monitorear el sistema de alarma mediante tecnología IoT, el cual es espléndido para poder monitorear el sistema mediante el celular o por página web.

CONCLUSIONES

Al culminar la tesis “Diseño y Construcción de un Sistema IoT para alertar el robo en viviendas”, se tienen las siguientes conclusiones:

Para la activación y desactivación de la alarma

- Se demostró que el 97.4 % del estado de activación y desactivación de la alarma por plataforma Blynk es igual al estado deseado de la alarma.

La plataforma IoT Blynk activa y desactiva la alarma

- Se demostró que el 97.40 % del estado deseado del monitoreo de la alarma se puede monitorear a través del aplicativo es igual al estado actual del monitoreo del estado de la alarma a través del aplicativo diseñado en la plataforma Blynk.

RECOMENDACIONES

1. Para la conexión del sistema se necesita de manera necesaria una red wifi de alta velocidad y estabilidad para que el sistema de monitoreo pueda funcionar de manera eficiente y eficaz dentro de la vivienda.
2. Diseñar una investigación donde se utiliza otros tipos de sensores.
3. Diseñar una investigación con tecnología IoT que esté conectada a cámaras.
4. Implementar esta investigación en una casa ya que esta investigación es solo un prototipo que tiene buenos resultados.
5. Usar tecnología IoT con el uso de plataforma IoT como Zetta, Node- RED entre otros.

BIBLIOGRAFÍA

Arduino. (2003). *Arduino*. Obtenido de <https://www.arduino.cc/>

Arduino. (2016). *Arduino*. Obtenido de <https://store.arduino.cc/usa/due>

Bricogeek. (11 de Octubre de 2021). *Bricogeek*. Obtenido de [https://blog.bricogeek.com: https://blog.bricogeek.com/img_cms/2886-tutorial-node-red.jpg](https://blog.bricogeek.com:https://blog.bricogeek.com/img_cms/2886-tutorial-node-red.jpg)

DISEÑAR UN SISTEMA DE ALARMA INALÁMBRICO DE BAJO COSTO PARA LA PROTECCIÓN DE VIVIENDAS TIPO, E. S. (2018). *Gaibor Carrillo, Karina Dolores; Loo Morán, Fernando Antonio*. GUAYAQUIL: UNIVERSIDAD DE GUAYAQUIL.

Domoticadomestica. (2020). Recuperado el 2021 de octubre de 21, de Domoticadomestica: <http://www.domoticadomestica.com/domoticz-software-libre-control-domotico/>

Fernández Collado , C. (2014). Recuperado el 6 de Junio de 2018, de Metodología de la Investigación: <http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf>

Geekflare. (28 de Julio de 2015). Obtenido de <https://geekflare.com/es/iot-platform-tools>

Geekflare. (25 de Febrero de 2019). *Geekflare*. Obtenido de [https://geekflare.com: https://geekflare.com/wp-content/uploads/2019/10/flutter.png](https://geekflare.com:https://geekflare.com/wp-content/uploads/2019/10/flutter.png)

GoogleMaps. (10 de Enero de 2001). *GoogleMaps*. Obtenido de <https://www.google.com.pe/maps/place/PAMPAS/>

HERNADEZ ESTRADA, J. I., RIVERA VELASQUEZ, J. M., & YAÑEZ MIGUEL, H. A. (2010). DOMÓTICA DE SEGURIDAD POR MEDIO DE SMS. Ciudad de México.

Hernández Gaviño, R. (s.f.). Recuperado el 5 de Junio de 2018, de Introduccion a Los Sistemas de Control: <http://lcr.uns.edu.ar/fcr/images/Introduccion%20a%20Los%20Sistemas%20de%20Control.pdf>

INEI. (2017). INEI. En INEI, ESTADISTICA DEL INIE (pág. 113).

Ingenieriayproyectos. (05 de Junio de 2021). Obtenido de <https://ingenieriayproyectosjgr.com/wp-content/uploads/2019/03/partes-de-un-sistema-contra-incendios-1.jpg>

- Intercron. (21 de Mayo de 2010). *Intercron*. Obtenido de Intercron:
<https://www.intercron.com/simuladores.htm>
- LR, S. (09 de Julio de 2021). Pueblo Libre: delincuente roba en vivienda y se lleva hasta el helado.
- LR, S. (23 de Marzo de 2021). Pueblo Libre: hampones entran a robar a una vivienda mientras familia dormía.
- LR, S. (25 de Julio de 2021). Surco: roban bicicleta a joven por segunda vez en su propia vivienda.
- M2mlabs. (26 de Marzo de 2015). *M2mlabs*. Obtenido de M2mlabs:
<http://www.m2mlabs.com/>
- NaylampMecatronics. (25 de Mayo de 2021). Obtenido de https://m.media-amazon.com/images/I/51A4+9JB0rL._SX342_.jpg
- Naylampmechatronics. (25 de Agosto de 2010). Obtenido de <https://naylampmechatronics.com/sensores-proximidad/283-sensor-ultrasonico-us-100.html>
- Naylampmechatronics. (2 de Octubre de 2021). *Naylampmechatronics*. Obtenido de <https://naylampmechatronics.com/buscar?controller=search&s=ESP32>
- Naylampmechatronics. (10 de Julio de 2021). Sensor magnético de puerta MC-38. Obtenido de <https://naylampmechatronics.com/sensores-proximidad/215-sensor-magnetico-de-puerta-mc-38.html>
- Portuguez, D. (27 de Julio de 2021). Surco: delincuentes ingresan a vivienda y se llevan S/ 400.000 soles mientras la dueña descansaba.
- Programmerclick. (2019). Recuperado el 25 de Octubre de 2021, de <https://programmerclick.com>:
<https://programmerclick.com/article/5967816389/>
- Ramírez Maroch, F. W. (2012). DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE. Lima.
- Segproject. (12 de Julio de 2020). Obtenido de <https://www.segproject.cl/images/slides/cctv.jpg>
- Sigfox. (2018). *Sigfox*. Obtenido de Sigfox:
<https://partners.sigfox.com/companies/samsung-artik-cloud>
- Slideshare. (05 de Enero de 2010). Obtenido de <https://es.slideshare.net/cbtorres/costos-ordenes-especificas>

Tecmikro. (9 de Junio de 2012). Tecmikro. Obtenido de <https://tecmikro.com/led-lcd/180-pantalla-display-lcd-128x64.html>

Wayne, T. (2003). Sistemas de comunicaciones electrónicas. México: Pearson Educación.

Wayne, T. (2003). Sistemas de comunicaciones electrónicas. México: Pearson Educación.

ANEXOS

MATRIZ DE CONSISTENCIA

TÍTULO: DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA INTERNET DE LAS COSAS PARA ALERTAR EL ROBO EN VIVIENDAS				
PROBLEMA	OBJETIVOS	HIPOTESIS	OPERACIONALIZACIÓN VARIABLES	MÉTODO
Problema General: • ¿Cómo diseñar e implementar un sistema de alarma que permita alertar el robo y/o intento de robo en las viviendas?	Objetivo General: • Diseñar e implementar un sistema de alarma que permita alertar el robo y/o intento de robo de las viviendas.	Hipótesis General: • El diseño y la implementación del sistema de alarma permite alertar de robo y/o intento de robo en las viviendas.	Variables Independientes: • DM: Detección por movimiento. • DA: Detección por apertura de puertas	
Problemas Específicos: • ¿Qué plataforma asociado a IoT deberá tener el sistema que active y desactive la alarma para alerte el robo y/o intento de robo? • ¿Qué plataforma asociado a IoT deberá tener el sistema para el monitoreo del estado de la alarma?	Objetivos Específicos: • Determinar la plataforma asociado a IoT que deberá tener el sistema que active y desactive la alarma para alertar el robo y/o intento de robo. • Determinar la plataforma asociado a IoT que deberá tener el sistema para el monitoreo del estado de la alarma.	Hipótesis Específicas: • El sistema IoT, basado en la plataforma Blynk activa y desactiva la alarma para alertar el robo y/o intento de robo. • El sistema IoT, basado en la plataforma Blynk monitorea el estado de la alarma.	Variables Dependientes: • IOT: Sistema IOT.	En esta investigación se empleará el método experimental.

ANEXO A

1. Requerimientos de diseño

Este diseño del sistema debe de realizar lo siguiente:

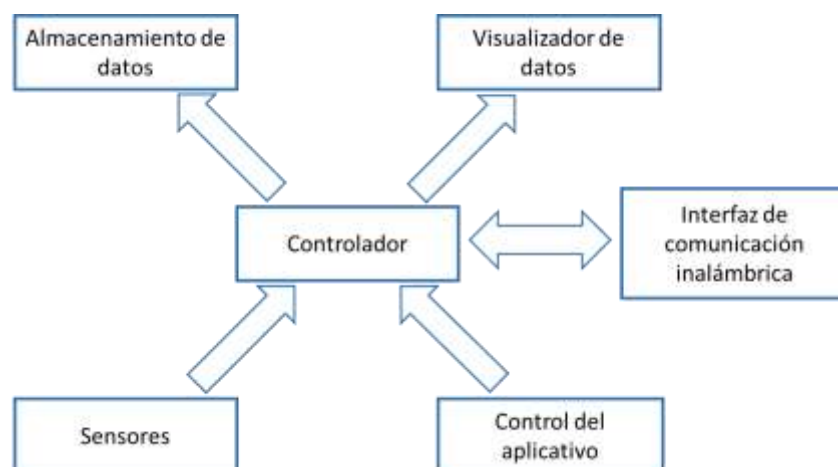
- Detectar el robo y/o intento de robo dentro de la vivienda.
- Alertar al propietario de la vivienda el robo y/o intento de robo de su vivienda mediante un aplicativo.
- Tener una alarma para disuadir a los delincuentes.
- Activar y desactivar el sistema de alarma a través del aplicativo
- Activar y desactivar el sistema de alarma a través del mismo sistema.

1.1. Sistema electrónico de funcionamiento

Un sistema para alertar el robo y/o intento de robo en una vivienda debe de disponer de todos los recursos necesarios para trabajar por sí solo. El dispositivo modular debe de contener las partes mostradas en el diagrama de bloques de la siguiente figura.

Figura A.1.

Diagrama de bloque del sistema electrónico.



Nota. Elaboración propia.

A continuación, se describe brevemente cada uno de ellas

Sensor, captura las variables físicas de las puertas

Control del aplicativo, mediante el aplicativo poder gestionar el sistema analizando los datos que se obtiene.

Controlador, acondiciona los datos capturados de los sensores, procesa la información y da una respuesta según la programación grabada en la memoria del controlador

Interfaz de comunicación inalámbrica, nos es útil para una comunicación entre el controlador y el aplicativo.

Almacenamiento de datos, guarda los datos que necesitamos

Visualizador de datos, muestra los datos obtenidos de los sensores.

1.2. Requerimiento de diseño según la aplicación

Considerando los requerimientos del sistema, los requerimientos específicos se indican a continuación:

a. Capacidad de detectar el robo y/o intento de robo

El sistema debe de ser capaz de detectar un robo y/o intento de robo dentro de una vivienda mediante sensores instalados en lugares estratégicos.

b. Generar una alerta

El sistema debe generar una alerta sonora ante la detección de un intruso dentro de la vivienda.

c. Notificaciones de alerta

El sistema debe de ser capaz de enviar notificaciones al móvil cada vez que el sistema detecta un intruso en la vivienda.

d. Visualización y control a través de un aplicativo móvil

El aplicativo diseñado debe tener la capacidad de visualizar el estado de los sensores, detectar si la alarma está activado o desactivado, poder activar y desactivar el sistema de alarma.

2. Diagrama de bloques

En figura A.2 se muestra el diagrama de bloques. A continuación, se detalla el diagrama de bloque de cada uno de los elementos que lo conforman tal que cumpla con los requerimientos del diseño impuesto anteriormente.

Al detectarse alguna apertura de las puertas principales de la vivienda, el circuito electrónico, que está conformado por los sensores de final de carrera, el controlador Node ESP8266 transmite mediante la conexión a internet una alerta al móvil del propietario, también activará la alarma para poder ahuyentar al delincuente, y por último registrará los datos de robo y/o intento de robo.

El sistema tendrá un tablero de control donde se podrá activar y desactivar la alarma de manera manual y también se podrá visualizar indicadores que indican si la alarma esta activada o desactivada.

En el lado de la aplicación, el propietario de la vivienda puede visualizar en la aplicación si la alarma esta activada o desactiva, además de poder desactivar y activar la alarma, así mismo puede observar que día y que hora se activó o desactivo la alarma.

3. Sistema de adquisición de datos

El sistema de adquisición de datos consta de los siguientes elementos:

- Sensor final de carrera
- Visualización de datos
- Transmisión de datos
- Visualización de los datos a través del aplicativo.

3.1. Sensor final de carrera

Los sensores (final de carrera) que estamos usando se ubicó en puertas estratégicas, ya que al ingresar a la vivienda estos sensores se activaron y dieron una señal que alertó el ingreso de intrusos a la vivienda.

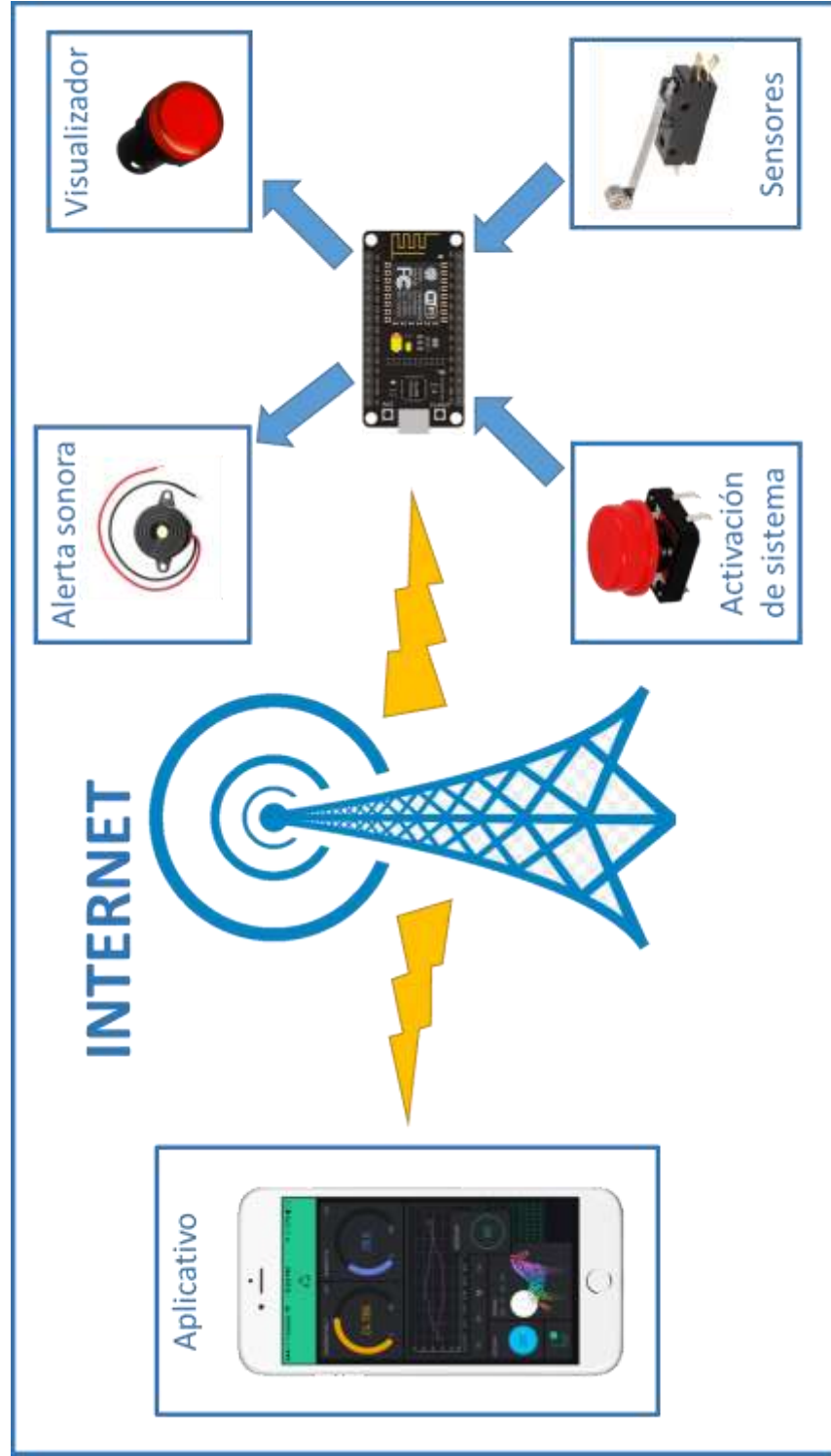
Figura A.2.

Imagen del sensor final de carrera.



Nota. Elaboración propia.

Figura A.3.
Diagrama de bloques.

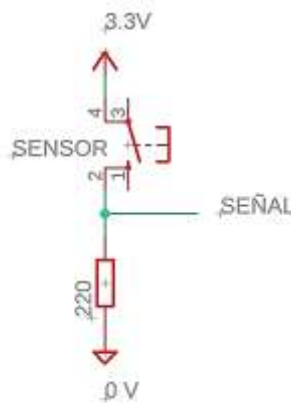


Nota. Elaboración propia.

A los sensores se les alimentó con 3.3 voltios, los cuales envían una señal de 3.3 voltios (1 lógico) o de 0 voltios (0 lógico). Esta señal llega al controlador el cual se encarga de procesar esta información.

Figura A.4.

Imagen del circuito electrónico del final de carrera.



Nota. Elaboración propia.

3.2. Visualización de datos

La visualización de datos consta de un panel con indicador led que indica **si** el sistema de alarma esta activada o desactivada.

Figura A.5.

Imagen del indicador led.



Nota. Elaboración propia.

Este indicador está prendido cuando el sistema de alarma está activado y está apagado cuando el sistema de alarma esta desactivado.

Figura A.6.

Imagen del circuito electrónico del indicador led.



Nota. Elaboración propia.

3.3. Transmisión de datos

En la transmisión de datos se usó el módulo MCU Node ESP 8266 para enviar datos al aplicativo y también para recibir datos del aplicativo mediante la conexión a internet a través del wifi. Este módulo es ideal para este tipo de comunicación por que viene incorporado el transmisor wifi. La forma de programación se realizó con el software de Arduino

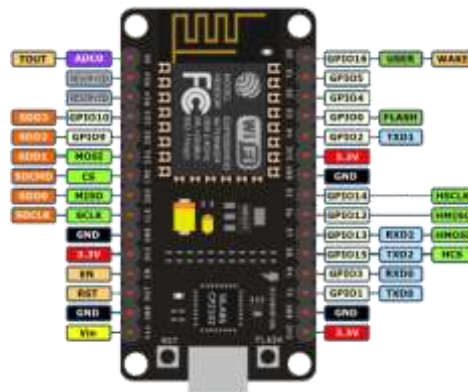
Especificaciones técnicas:

- Voltaje de Alimentación: 5V DC
- Voltaje de Entradas/Salidas: 3.3V DC
- Chip conversor USB-serial: CP2102
- SoM: ESP-12E (Ai-Thinker)
- CPU: Tensilica Xtensa LX3 (32 bit)
- Frecuencia de Reloj: 80MHz/160MHz
- Memoria Flash Externa: 4MB
- Pines Digitales GPIO: 17 (4 pueden configurarse como PWM a 3.3V)
- Pin Analógico ADC: 1 (0-1V)
- Puerto Serial UART: 2

- Antena en PCB
- Potencia de salida de +19.5dBm en modo 802.11b
- Corriente de fuga menor a 10uA
- Pulsador RESET y FLASH

Figura A.7.

Imagen del módulo MCU Node ESP8266.



Nota. Elaboración propia.

Programa en IDE Arduino para la transmisión de datos.

La programación que se utilizó para este diseño se realizó en el software IDE Arduino el cual es un software libre de fácil acceso y de fácil programación.

A continuación, se escribe la programación utilizada en Arduino para el funcionamiento de este sistema de alarma.

Programa para la configuración del módulo con la plataforma Blynk:

```
#define BLYNK_TEMPLATE_ID "TMPLM3AQvQz0"

#define BLYNK_DEVICE_NAME "DOS"

#define BLYNK_FIRMWARE_VERSION "0.1.0"
```

```

#define BLYNK_PRINT Serial

//#define BLYNK_DEBUG

//#define APP_DEBUG

#define USE_NODE_MCU_BOARD

#define LED    5  //

#define BOCINA 13  //

#define INTER  10

#define PUERTA  9  //

#define BALCON 14  //

#define COCHERA 12  //

#define wifiLed 16  //D0

//PINES VIRTUALES QUE SE UTILIZARAN EN EL APLICATIVO

#define PIN_VIRTUAL_1  V1

#define PIN_PUERTA     V2

#define PIN_BALCON     V3

#define PIN_COCHERA    V4

#define PIN_ALARMA     V5

// ESTADOS DE LOS SENSORES DEL SISTEMA

bool INTER_VIRTUAL = LOW;

bool EST_PUERTA    = LOW;

```

```

bool EST_BALCON    = LOW;

bool EST_COCHERA    = LOW;

// ESTADO DE ALARMA

bool EST_INTER = LOW;

#include "BlynkEdgent.h"

BLYNK_CONNECTED() {

    // ESTADO DEL BOTON E INDICADORES DEL APLICATIVO

    Blynk.syncVirtual(PIN_VIRTUAL_1);

    Blynk.syncVirtual(PIN_PUERTA);

    Blynk.syncVirtual(PIN_BALCON);

    Blynk.syncVirtual(PIN_COCHERA);

    Blynk.syncVirtual(PIN_ALARMA);

}

BLYNK_WRITE(PIN_VIRTUAL_1) {

    INTER_VIRTUAL = param.asInt();

    if(INTER_VIRTUAL == 1){

        EST_INTER = HIGH;

        digitalWrite(LED,HIGH);

        Serial.println("Sistema Activado");

        delay(1000);

```

```

    }

else {

    EST_INTER = LOW;

    digitalWrite(LED,LOW);

    digitalWrite(BOCINA,LOW);

    Serial.println("Sistema desactivado");

    delay(1000);

}

}

void setup()

{

    Serial.begin(115200);

    delay(100);

    pinMode(LED, OUTPUT);

    pinMode(BOCINA, OUTPUT);


    pinMode(wifiLed, OUTPUT);

    pinMode(INTER, INPUT);

    pinMode(PUERTA, INPUT);

    digitalWrite(LED, LOW);

```

```

digitalWrite(BOCINA, LOW);

digitalWrite(wifiLed, HIGH);

BlynkEdgent.begin();

Blynk.virtualWrite(PIN_VIRTUAL_1, INTER_VIRTUAL);

Blynk.virtualWrite(PIN_PUERTA, LOW);

Blynk.virtualWrite(PIN_BALCON, LOW);

Blynk.virtualWrite(PIN_COCHERA, LOW);

Blynk.virtualWrite(PIN_ALARMA, LOW);

}

void loop() {

    BlynkEdgent.run();

    manual_control();

}

```

Programa para el funcionamiento de los sensores, actuadores y control

```

extern "C" {

    #include "user_interface.h"

    void app_loop();

}

#include "Settings.h"

#include <BlynkSimpleEsp8266_SSL.h>

```

```

#ifndef BLYNK_NEW_LIBRARY

#error "Old version of Blynk library is in use. Please replace it with the new
one."

#endif

#if !defined(BLYNK_TEMPLATE_ID) ||
!defined(BLYNK_DEVICE_NAME)

#error "Please specify your BLYNK_TEMPLATE_ID and
BLYNK_DEVICE_NAME"

#endif

#include "BlynkState.h"

#include "ConfigStore.h"

#include "ResetButton.h"

#include "ConfigMode.h"

#include "Indicator.h"

#include "OTA.h"

#include "Console.h"

void manual_control();

inline

void BlynkState::set(State m) {

    if (state != m && m < MODE_MAX_VALUE) {

        DEBUG_PRINT(String(StateStr[state]) + " => " + StateStr[m]);

```

```

state = m;

// You can put your state handling here,

// i.e. implement custom indication

}

}

void printDeviceBanner()

{

    Blynk.printBanner();

    DEBUG_PRINT("-----");

    DEBUG_PRINT(String("Product: ") + BLYNK_DEVICE_NAME);

    DEBUG_PRINT(String("Firmware: ") + BLYNK_FIRMWARE_VERSION
" (build " __DATE__ " " __TIME__ ")");

    if (configStore.getFlag(CONFIG_FLAG_VALID)) {

        DEBUG_PRINT(String("Token:  ...") + (configStore.cloudToken+28));

    }

    DEBUG_PRINT(String("Device:  ") + BLYNK_INFO_DEVICE + " @ " +
ESP.getCpuFreqMHz() + "MHz");

    DEBUG_PRINT(String("MAC:  ") + WiFi.macAddress());

    DEBUG_PRINT(String("Flash:  ") + ESP.getFlashChipRealSize() / 1024 +
"K");

    String coreVer = ESP.getCoreVersion();

```

```

coreVer.replace("_", ".");

DEBUG_PRINT(String("ESP core: ") + coreVer);

DEBUG_PRINT(String("ESP SDK: ") + ESP.getSdkVersion());

DEBUG_PRINT(String("Boot Ver: ") + ESP.getBootVersion());

DEBUG_PRINT(String("Boot Mode:") + ESP.getBootMode());

DEBUG_PRINT(String("FW info:  ") + ESP.getSketchSize() + "/" +
ESP.getFreeSketchSpace() + ", MD5:" + ESP.getSketchMD5());

DEBUG_PRINT(String("Free mem: ") + ESP.getFreeHeap());

DEBUG_PRINT("-----");

}

void runBlynkWithChecks() {

  Blynk.run();

  if (BlynkState::get() == MODE_RUNNING) {

    if (!Blynk.connected()) {

      if (WiFi.status() == WL_CONNECTED) {

        BlynkState::set(MODE_CONNECTING_CLOUD);

      } else {

        BlynkState::set(MODE_CONNECTING_NET);

      }

    }

  }

}

```

```

}

class Edgent {

public:

    void begin()

    {

        indicator_init();

        button_init();

        config_init();

        console_init();

        printDeviceBanner();

        if (configStore.getFlag(CONFIG_FLAG_VALID)) {

            BlynkState::set(MODE_CONNECTING_NET);

        } else if (config_load_blnkopt()) {

            DEBUG_PRINT("Firmware is preprovisioned");

            BlynkState::set(MODE_CONNECTING_NET);

        } else {

            BlynkState::set(MODE_WAIT_CONFIG);

        }

    }

    void run() {

```

```

app_loop();

switch (BlynkState::get()) {

case MODE_WAIT_CONFIG:

case MODE_CONFIGURING:    enterConfigMode();  break;

case MODE_CONNECTING_NET:  enterConnectNet();  break;

case MODE_CONNECTING_CLOUD: enterConnectCloud(); break;

case MODE_RUNNING:        runBlynkWithChecks(); break;

case MODE_OTA_UPGRADE:    enterOTA();          break;

case MODE_SWITCH_TO_STA:  enterSwitchToSTA();  break;

case MODE_RESET_CONFIG:   enterResetConfig();  break;

default:                  enterError();        break;

}

}

};

Edgent BlynkEdgent;

BlynkTimer edgentTimer;

void app_loop() {

    edgentTimer.run();

    edgentConsole.run();

    manual_control();

```

```

}

void manual_control()

{

    /////activar o desactivar sistema de seguridad

    if (digitalRead(INTER) == HIGH && EST_INTER == LOW) {

        Blynk.virtualWrite(PIN_VIRTUAL_1, HIGH);

        digitalWrite(LED,HIGH);

        EST_INTER = HIGH;

        Serial.println("Sistema Activado");

        Blynk.logEvent("activado", "SISTEMA ATIVADO");

        delay(1000);

    }

    if (digitalRead(INTER) == HIGH && EST_INTER == HIGH) {

        Blynk.virtualWrite(PIN_VIRTUAL_1, LOW);

        digitalWrite(LED,LOW);

        digitalWrite(BOCINA,LOW);

        EST_INTER = LOW;

        Serial.println("Sistema Desactivado");

        Blynk.logEvent("desctivado", "SISTEMA DESATIVADO");

        delay(1000);
    }
}

```

```

}

/////ESTADO DE PUERTA SIN ALARMA

if(digitalRead(LED) == LOW && digitalRead(PUERTA) == HIGH &&
EST_PUERTA == LOW )

{

    EST_PUERTA = HIGH;

    Blynk.virtualWrite(PIN_PUERTA, HIGH);

    Serial.println("PUERTA ABIERTA 1");

    delay(50);

}

if(digitalRead(LED) == LOW && digitalRead(PUERTA) == LOW &&
EST_PUERTA == HIGH )

{

    EST_PUERTA = LOW;

    Blynk.virtualWrite(PIN_PUERTA, LOW);

    Serial.println("PUERTA CERRADA 1");

    delay(50);

}

/////ESTADO DE BALCON SIN ALARMA

if(digitalRead(LED) == LOW && digitalRead(BALCON) == HIGH &&
EST_BALCON == LOW )

```

```

{

    EST_BALCON = HIGH;

    Blynk.virtualWrite(PIN_BALCON, HIGH);

    Serial.println("BALCON ABIERTO 1");

    delay(50);

}

if(digitalRead(LED) == LOW && digitalRead(BALCON) == LOW &&
EST_BALCON == HIGH )

{

    EST_BALCON = LOW;

    Blynk.virtualWrite(PIN_BALCON, LOW);

    Serial.println("BALCON CERRADO 1");

    delay(50);

}

/////ESTADO DE COCHERA SIN ALARMA

if(digitalRead(LED) == LOW && digitalRead(COCHERA) == HIGH &&
EST_COCHERA == LOW )

{

    EST_COCHERA = HIGH;

    Blynk.virtualWrite(PIN_COCHERA, HIGH);

    Serial.println("COCHERA ABIERTO 1");

```

```

    delay(50);

}

if(digitalRead(LED) == LOW && digitalRead(COCHERA) == LOW &&
EST_COCHERA == HIGH )

{

    EST_COCHERA = LOW;

    Blynk.virtualWrite(PIN_COCHERA, LOW);

    Serial.println("COCHERA CERRADA 1");

    delay(50);

}

//ESTADO DEL SISTEMA CON ALARMA ACTIVADA

if(digitalRead(LED) == HIGH )

{

    ////ACTIVACION POR PUERTA

    if(digitalRead(PUERTA) == HIGH && EST_PUERTA == LOW)

    {

        EST_PUERTA = HIGH;

        Serial.println("PUETA ABIERTA");

        Serial.println("BOCINA ACTIVADA");

        digitalWrite(BOCINA,HIGH);

        Blynk.virtualWrite(PIN_PUERTA, HIGH);

```

```

    Blynk.virtualWrite(PIN_ALARMA, HIGH);

    Blynk.logEvent("puerta",    "ALARMA    ACTIVADA,    PUERTA
ABIERTA");

}

if(digitalRead(PUERTA) == LOW && EST_PUERTA == HIGH)

{

    EST_PUERTA = LOW;

    Serial.println("PUERTA CERRADA");

    Blynk.virtualWrite(PIN_PUERTA, LOW);

    Blynk.virtualWrite(PIN_ALARMA, HIGH);

}

if(digitalRead(PUERTA) == HIGH && digitalRead(BOCINA) == LOW
&& EST_PUERTA == HIGH)

{

    EST_PUERTA = HIGH;

    Blynk.virtualWrite(PIN_PUERTA, HIGH);

    Blynk.virtualWrite(PIN_ALARMA, HIGH);

    Serial.println("PUETA ABIERTA");

    Serial.println("BOCINA ACTIVADA");

    digitalWrite(BOCINA,HIGH);

}

```

```

////ACTIVACION POR BALCON

if(digitalRead(BALCON) == HIGH && EST_BALCON == LOW)

{

    EST_BALCON = HIGH;

    Serial.println("BALCON ABIERTO");

    Serial.println("BOCINA ACTIVADA");

    Blynk.virtualWrite(PIN_BALCON, HIGH);

    Blynk.virtualWrite(PIN_ALARMA, HIGH);

    digitalWrite(BOCINA,HIGH);

    Blynk.logEvent("balcon",    "ALARMA    ACTIVADA,    BALCON
ABIERTO");

}

if(digitalRead(BALCON) == LOW && EST_BALCON == HIGH)

{

    EST_BALCON = LOW;

    Blynk.virtualWrite(PIN_PUERTA, LOW);

    Blynk.virtualWrite(PIN_ALARMA, HIGH);

    Serial.println("BALCON CERRADO");

}

if(digitalRead(BALCON) == HIGH && digitalRead(BOCINA) == LOW
&& EST_BALCON == HIGH)

```

```

{

    EST_BALCON = HIGH;

    Serial.println("BALCON ABIERTO");

    Serial.println("BOCINA ACTIVADA");

    Blynk.virtualWrite(PIN_PUERTA, HIGH);

    Blynk.virtualWrite(PIN_ALARMA, HIGH);

    digitalWrite(BOCINA,HIGH);

}

////ACTIVACION POR COCHERA

if(digitalRead(COCHERA) == HIGH && EST_COCHERA == LOW)

{

    EST_COCHERA= HIGH;

    Blynk.virtualWrite(PIN_COCHERA, HIGH);

    Blynk.virtualWrite(PIN_ALARMA, HIGH);

    Serial.println("COCHERA ABIERTO");

    Serial.println("BOCINA ACTIVADA");

    digitalWrite(BOCINA,HIGH);

    Blynk.logEvent("cochera",  "ALARMA  ACTIVADA,  COCHERA
ABIERTA");

}

if(digitalRead(COCHERA) == LOW && EST_COCHERA == HIGH)

```

```

{

    EST_COCHERA = LOW;

    Blynk.virtualWrite(PIN_COCHERA, LOW);

    Blynk.virtualWrite(PIN_ALARMA, HIGH);

    Serial.println("BALCON CERRADO");

}

if(digitalRead(COCHERA) == HIGH && digitalRead(BOCINA) == LOW
&& EST_COCHERA == HIGH)

{

    EST_COCHERA= HIGH;

    Blynk.virtualWrite(PIN_COCHERA, HIGH);

    Blynk.virtualWrite(PIN_ALARMA, HIGH);

    Serial.println("COCHERA ABIERTO");

    Serial.println("BOCINA ACTIVADA");

    digitalWrite(BOCINA,HIGH);

}

}

}

```

3.4. Visualización de los datos a través del aplicativo.

El aplicativo sé que utilizo para la elaboración de este proyecto fue el aplicativo de la plataforma Blynk 2.0 que es un aplicativo diseñado para vincular

dispositivos con tecnología IoT. Esta plataforma tiene dos modos de uso el modo gratuito y el modo de pago. Nosotros estamos usando el modo gratuito el cual en este proyecto proporciona buenos resultados, cuenta con las librerías necesarias.

Esta plataforma es de fácil acceso, fácil diseño.

Figura A.8.

Imagen del icono de la plataforma Blynk.



Nota. Elaboración propia.

En el aplicativo creado se puede visualizar indicadores y la línea de tiempo donde la alarma fue activada o desactivada.

También en el aplicativo se puede activar o desactivar la alarma con un botón

Figura A.9.

Imagen del aplicativo diseñado para el sistema.



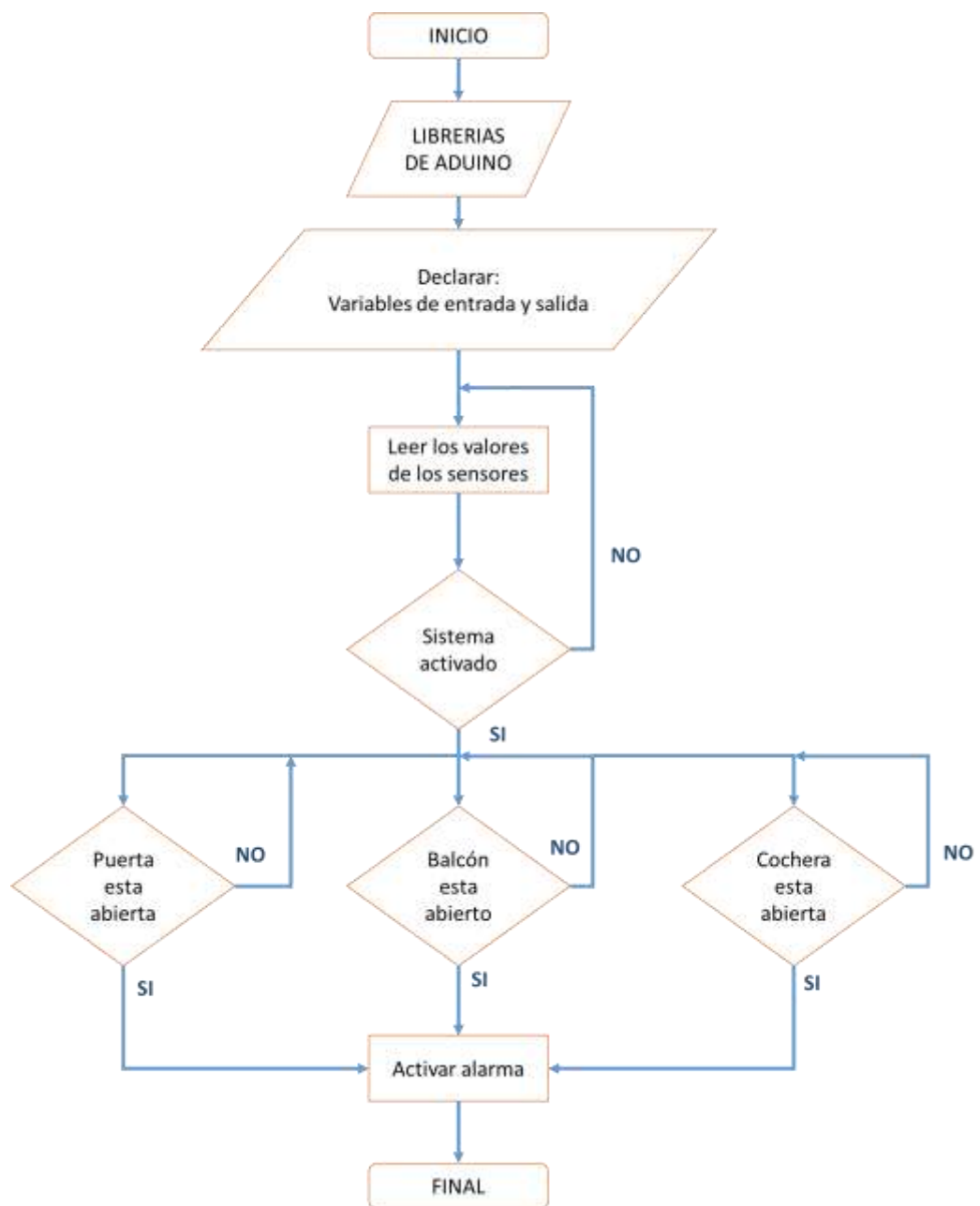
Nota. Elaboración propia.

4. Diagrama de flujo

Se presenta el diagrama de flujo del programa creado en Arduino del sistema de alarma.

Figura A.10.

Diagrama de flujo de programa de Arduino.

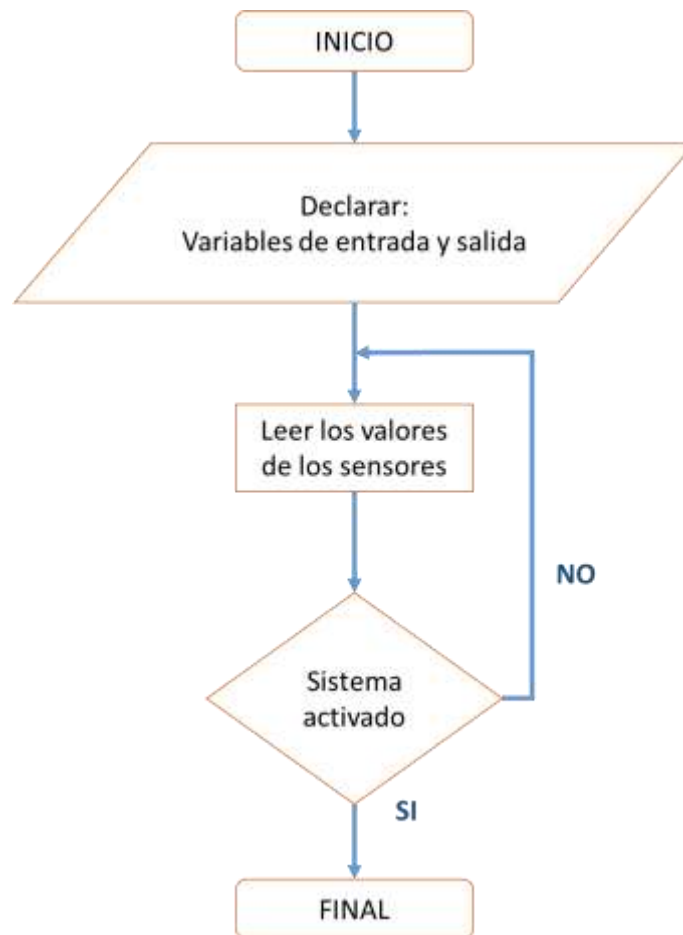


Nota. Elaboración propia.

Se presenta el diagrama de flujo del aplicativo diseñado en la plataforma Blynk 2.0.

Figura A.11.

Diagrama de flujo del aplicativo.



Nota. Elaboración propia.

5. Circuito electrónico del sistema de alarma.

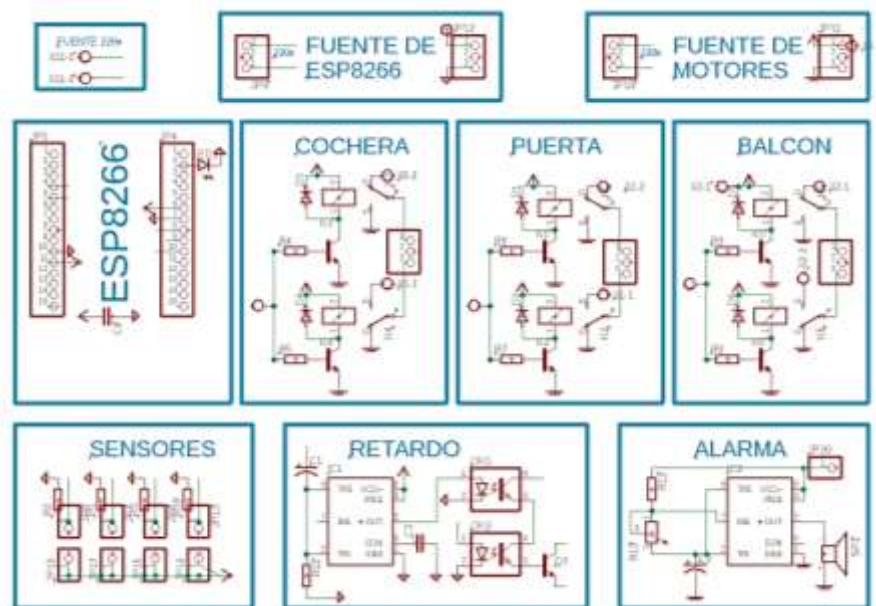
El circuito electrónico del sistema de alarma cuenta con las siguientes partes:

- Transformador de 220 voltios AC a 5.5 voltios DC
- El módulo MCU Node ESP8266
- Relés (para la apertura de puertas)
- Sensores
- Retardo de alarma

- Alarma

Figura A.12.

Imagen del circuito eléctrico del sistema de alarma.



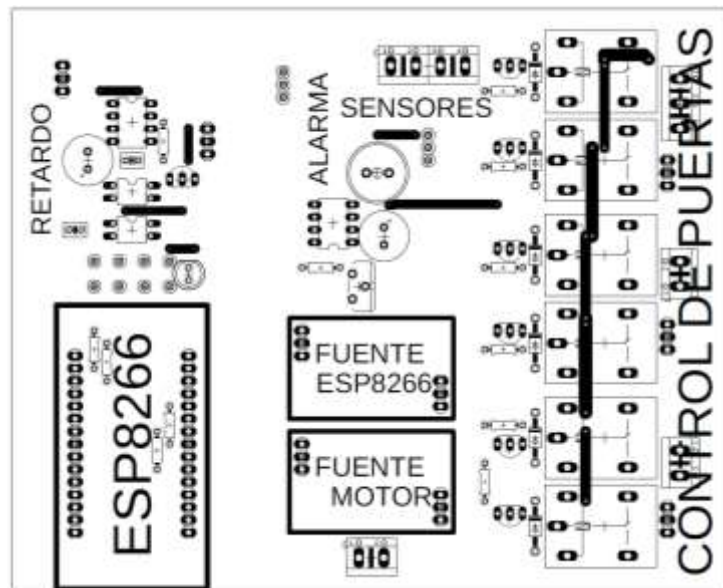
Nota. Elaboración propia.

6. Diseño de placa electrónica

Después de calcular los valores del circuito de acoplamiento, de los sensores, de las resistencias, conexiones con el módulo wifi, conexión con el panel de control y otros se realizó el diseño de placa electrónica con el software Eagle 7.9.

Figura A.13.

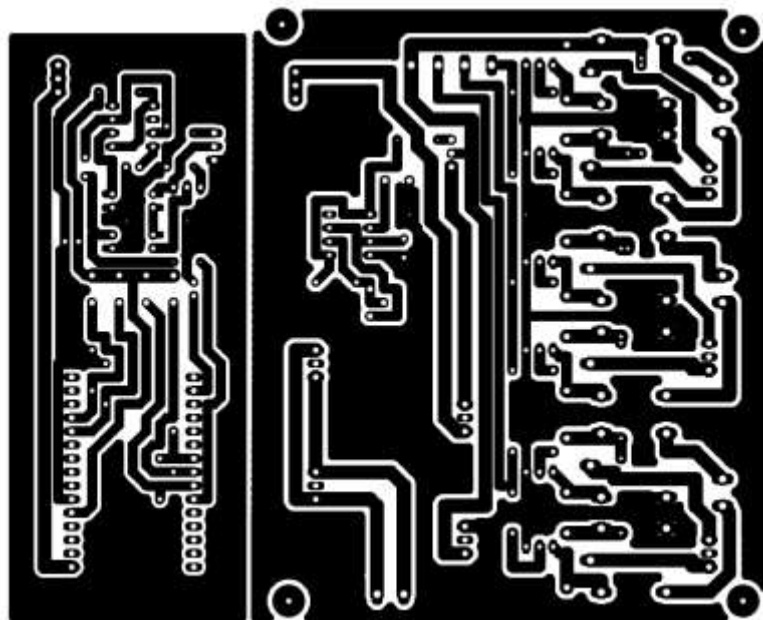
Imagen de la placa por la parte superior.



Nota. Elaboración propia.

Figura A.14.

Imagen de la placa por la parte inferior.



Nota. Elaboración propia.

ANEXO B

Tabla B. 1

Muestra tomada de activación y desactivación de la alarma.

Datos	Activación y desactivación de alama IoT	Estado deseado de alarma	Estado actual de la alarma	¿Estado actual es igual a estado deseado de la alarma?
1	Activación	Activado	Activado	SI
2	Activación	Activado	Activado	SI
3	Activación	Activado	Activado	SI
4	Activación	Activado	Activado	SI
5	Activación	Activado	Activado	SI
6	Desactivación	Desactivado	Desactivado	SI
7	Activación	Activado	Activado	SI
8	Activación	Activado	Activado	SI
9	Activación	Activado	Desactivado	NO
10	Desactivación	Desactivado	Desactivado	SI
11	Activación	Activado	Activado	SI
12	Desactivación	Desactivado	Desactivado	SI

13	Activación	Activado	Activado	SI
14	Desactivación	Desactivado	Desactivado	SI
15	Activación	Activado	Activado	SI
16	Desactivación	Desactivado	Desactivado	SI
17	Activación	Activado	Activado	SI
18	Desactivación	Desactivado	Desactivado	SI
19	Activación	Activado	Desactivado	NO
20	Activación	Activado	Activado	SI
21	Activación	Activado	Activado	SI
22	Desactivación	Desactivado	Desactivado	SI
23	Activación	Activado	Activado	SI
24	Desactivación	Desactivado	Desactivado	SI
25	Activación	Activado	Activado	SI
26	Desactivación	Desactivado	Desactivado	SI
27	Desactivación	Desactivado	Desactivado	SI
28	Desactivación	Desactivado	Desactivado	SI
29	Activación	Activado	Activado	SI

30	Desactivación	Desactivado	Desactivado	SI
31	Activación	Activado	Activado	SI
32	Desactivación	Desactivado	Desactivado	SI
33	Desactivación	Desactivado	Desactivado	SI
34	Desactivación	Desactivado	Desactivado	SI
35	Activación	Activado	Activado	SI
36	Desactivación	Desactivado	Desactivado	SI
37	Activación	Activado	Activado	SI
38	Activación	Activado	Activado	SI
39	Activación	Activado	Activado	SI
40	Desactivación	Desactivado	Desactivado	SI
41	Activación	Activado	Activado	SI
42	Activación	Activado	Activado	SI
43	Activación	Activado	Activado	SI
44	Desactivación	Desactivado	Desactivado	SI
45	Activación	Activado	Activado	SI
46	Desactivación	Desactivado	Desactivado	SI

47	Activación	Activado	Activado	SI
48	Desactivación	Desactivado	Desactivado	SI
49	Activación	Activado	Activado	SI
50	Activación	Activado	Activado	SI
51	Activación	Activado	Activado	SI
52	Desactivación	Desactivado	Desactivado	SI
53	Activación	Activado	Activado	SI
54	Activación	Activado	Activado	SI
55	Activación	Activado	Activado	SI
56	Activación	Activado	Activado	SI
57	Activación	Activado	Activado	SI
58	Desactivación	Desactivado	Desactivado	SI
59	Activación	Activado	Activado	SI
60	Desactivación	Desactivado	Desactivado	SI
61	Desactivación	Desactivado	Desactivado	SI
62	Desactivación	Desactivado	Desactivado	SI
63	Activación	Activado	Activado	SI

64	Desactivación	Desactivado	Desactivado	SI
65	Activación	Activado	Activado	SI
66	Desactivación	Desactivado	Desactivado	SI
67	Desactivación	Desactivado	Desactivado	SI
68	Desactivación	Desactivado	Desactivado	SI
69	Activación	Activado	Activado	SI
70	Desactivación	Desactivado	Desactivado	SI
71	Activación	Activado	Activado	SI
72	Activación	Activado	Activado	SI
73	Activación	Activado	Activado	SI
74	Desactivación	Desactivado	Desactivado	SI
75	Desactivación	Desactivado	Desactivado	SI
76	Desactivación	Desactivado	Desactivado	SI
77	Activación	Activado	Activado	SI
78	Desactivación	Desactivado	Desactivado	SI
79	Activación	Activado	Activado	SI
80	Activación	Activado	Activado	SI

81	Activación	Activado	Activado	SI
82	Desactivación	Desactivado	Desactivado	SI
83	Activación	Activado	Desactivado	NO
84	Desactivación	Desactivado	Desactivado	SI
85	Desactivación	Desactivado	Desactivado	SI
86	Desactivación	Desactivado	Desactivado	SI
87	Activación	Activado	Activado	SI
88	Desactivación	Desactivado	Desactivado	SI
89	Activación	Activado	Activado	SI
90	Activación	Activado	Activado	SI
91	Activación	Activado	Activado	SI
92	Desactivación	Desactivado	Desactivado	SI
93	Activación	Activado	Activado	SI
94	Desactivación	Desactivado	Desactivado	SI
95	Desactivación	Desactivado	Desactivado	SI
96	Desactivación	Desactivado	Desactivado	SI
97	Activación	Activado	Activado	SI

98	Desactivación	Desactivado	Desactivado	SI
99	Desactivación	Desactivado	Desactivado	SI
100	Desactivación	Desactivado	Desactivado	SI
101	Activación	Activado	Activado	SI
102	Desactivación	Desactivado	Desactivado	SI
103	Activación	Activado	Activado	SI
104	Desactivación	Desactivado	Desactivado	SI
105	Desactivación	Desactivado	Desactivado	SI
106	Desactivación	Desactivado	Desactivado	SI
107	Activación	Activado	Activado	SI
108	Desactivación	Desactivado	Desactivado	SI
109	Activación	Activado	Activado	SI
110	Desactivación	Desactivado	Desactivado	SI
111	Desactivación	Desactivado	Desactivado	SI
112	Desactivación	Desactivado	Desactivado	SI
113	Desactivación	Desactivado	Desactivado	SI
114	Desactivación	Desactivado	Desactivado	SI

115	Activación	Activado	Activado	SI
116	Desactivación	Desactivado	Desactivado	SI
117	Activación	Activado	Activado	SI
118	Desactivación	Desactivado	Desactivado	SI
119	Desactivación	Desactivado	Desactivado	SI
120	Activación	Activado	Activado	SI
121	Desactivación	Desactivado	Desactivado	SI
122	Activación	Activado	Activado	SI
123	Desactivación	Desactivado	Desactivado	SI
124	Desactivación	Desactivado	Desactivado	SI
125	Desactivación	Desactivado	Desactivado	SI
126	Desactivación	Desactivado	Desactivado	SI
127	Desactivación	Desactivado	Desactivado	SI
128	Activación	Activado	Activado	SI
129	Activación	Activado	Activado	SI
130	Desactivación	Desactivado	Desactivado	SI
131	Activación	Activado	Activado	SI

132	Activación	Activado	Activado	SI
133	Activación	Activado	Activado	SI
134	Activación	Activado	Activado	SI
135	Desactivación	Desactivado	Desactivado	SI
136	Desactivación	Desactivado	Desactivado	SI
137	Activación	Activado	Activado	SI
138	Desactivación	Desactivado	Desactivado	SI
139	Activación	Activado	Activado	SI
140	Desactivación	Desactivado	Desactivado	SI
141	Desactivación	Desactivado	Desactivado	SI
142	Desactivación	Desactivado	Desactivado	SI
143	Activación	Activado	Activado	SI
144	Desactivación	Desactivado	Desactivado	SI
145	Desactivación	Desactivado	Desactivado	SI
146	Desactivación	Desactivado	Desactivado	SI
147	Desactivación	Desactivado	Desactivado	SI
148	Activación	Activado	Activado	SI

149	Activación	Activado	Activado	SI
150	Desactivación	Desactivado	Activado	NO
151	Activación	Activado	Activado	SI
152	Activación	Activado	Activado	SI
153	Activación	Activado	Activado	SI
154	Activación	Activado	Activado	SI
155	Desactivación	Desactivado	Desactivado	SI
156	Activación	Activado	Activado	SI
157	Activación	Activado	Activado	SI
158	Desactivación	Desactivado	Desactivado	SI
159	Activación	Activado	Activado	SI
160	Desactivación	Desactivado	Desactivado	SI
161	Desactivación	Desactivado	Desactivado	SI
162	Desactivación	Desactivado	Desactivado	SI
163	Activación	Activado	Activado	SI
164	Desactivación	Desactivado	Desactivado	SI
165	Activación	Activado	Activado	SI

166	Activación	Activado	Activado	SI
167	Activación	Activado	Activado	SI
168	Activación	Activado	Activado	SI
169	Activación	Activado	Activado	SI
170	Desactivación	Desactivado	Desactivado	SI
171	Activación	Activado	Activado	SI
172	Desactivación	Desactivado	Desactivado	SI
173	Activación	Activado	Activado	SI
174	Desactivación	Desactivado	Desactivado	SI
175	Desactivación	Desactivado	Desactivado	SI
176	Desactivación	Desactivado	Desactivado	SI
177	Activación	Activado	Activado	SI
178	Activación	Activado	Activado	SI
179	Activación	Activado	Activado	SI
180	Desactivación	Desactivado	Desactivado	SI
181	Desactivación	Desactivado	Desactivado	SI
182	Activación	Activado	Activado	SI

183	Activación	Activado	Activado	SI
184	Activación	Activado	Activado	SI
185	Desactivación	Desactivado	Desactivado	SI
186	Desactivación	Desactivado	Desactivado	SI
187	Activación	Activado	Activado	SI
188	Desactivación	Desactivado	Desactivado	SI
189	Activación	Activado	Activado	SI
190	Activación	Activado	Activado	SI
191	Desactivación	Desactivado	Desactivado	SI
192	Desactivación	Desactivado	Desactivado	SI
193	Activación	Activado	Activado	SI
194	Desactivación	Desactivado	Desactivado	SI
195	Desactivación	Desactivado	Desactivado	SI
196	Activación	Activado	Activado	SI
197	Desactivación	Desactivado	Desactivado	SI
198	Desactivación	Desactivado	Desactivado	SI
199	Desactivación	Desactivado	Desactivado	SI

200	Activación	Activado	Activado	SI
201	Desactivación	Desactivado	Desactivado	SI
202	Activación	Activado	Activado	SI
203	Activación	Activado	Activado	SI
204	Activación	Activado	Activado	SI
205	Desactivación	Desactivado	Desactivado	SI
206	Desactivación	Desactivado	Desactivado	SI
207	Activación	Activado	Activado	SI
208	Desactivación	Desactivado	Desactivado	SI
209	Activación	Activado	Activado	SI
210	Desactivación	Desactivado	Desactivado	SI
211	Activación	Activado	Activado	SI
212	Desactivación	Desactivado	Desactivado	SI
213	Activación	Activado	Activado	SI
214	Activación	Activado	Activado	SI
215	Activación	Activado	Activado	SI
216	Activación	Activado	Activado	SI

217	Activación	Activado	Activado	SI
218	Desactivación	Desactivado	Desactivado	SI
219	Activación	Activado	Activado	SI
220	Desactivación	Desactivado	Activado	NO
221	Activación	Activado	Activado	SI
222	Desactivación	Desactivado	Desactivado	SI
223	Activación	Activado	Activado	SI
224	Desactivación	Desactivado	Desactivado	SI
225	Activación	Activado	Activado	SI
226	Desactivación	Desactivado	Desactivado	SI
227	Activación	Activado	Activado	SI
228	Desactivación	Desactivado	Desactivado	SI
229	Activación	Activado	Activado	SI
230	Desactivación	Desactivado	Desactivado	SI
231	Activación	Activado	Activado	SI
232	Activación	Activado	Activado	SI
233	Activación	Activado	Activado	SI

234	Desactivación	Desactivado	Desactivado	SI
235	Desactivación	Desactivado	Activado	NO
236	Desactivación	Desactivado	Desactivado	SI
237	Activación	Activado	Activado	SI
238	Desactivación	Desactivado	Desactivado	SI
239	Activación	Activado	Activado	SI
240	Desactivación	Desactivado	Desactivado	SI
241	Activación	Activado	Activado	SI
242	Desactivación	Desactivado	Desactivado	SI
243	Activación	Activado	Activado	SI
244	Desactivación	Desactivado	Desactivado	SI
245	Desactivación	Desactivado	Desactivado	SI
246	Desactivación	Desactivado	Desactivado	SI
247	Activación	Activado	Activado	SI
248	Desactivación	Desactivado	Desactivado	SI
249	Activación	Activado	Activado	SI
250	Activación	Activado	Activado	SI

251	Activación	Activado	Activado	SI
252	Activación	Activado	Activado	SI
253	Activación	Activado	Activado	SI
254	Desactivación	Desactivado	Desactivado	SI
255	Activación	Activado	Activado	SI
256	Desactivación	Desactivado	Desactivado	SI
257	Activación	Activado	Activado	SI
258	Desactivación	Desactivado	Desactivado	SI
259	Activación	Activado	Activado	SI
260	Desactivación	Desactivado	Desactivado	SI
261	Activación	Activado	Desactivado	NO
262	Desactivación	Desactivado	Desactivado	SI
263	Activación	Activado	Activado	SI
264	Activación	Activado	Activado	SI
265	Activación	Activado	Activado	SI
266	Activación	Activado	Activado	SI
267	Activación	Activado	Activado	SI

268	Desactivación	Desactivado	Desactivado	SI
269	Desactivación	Desactivado	Desactivado	SI
270	Desactivación	Desactivado	Desactivado	SI
271	Desactivación	Desactivado	Desactivado	SI
272	Desactivación	Desactivado	Desactivado	SI
273	Activación	Activado	Activado	SI
274	Desactivación	Desactivado	Desactivado	SI
275	Activación	Activado	Activado	SI
276	Desactivación	Desactivado	Desactivado	SI
277	Activación	Activado	Activado	SI
278	Activación	Activado	Activado	SI
279	Activación	Activado	Activado	SI
280	Desactivación	Desactivado	Desactivado	SI
281	Activación	Activado	Activado	SI
282	Activación	Activado	Activado	SI
283	Activación	Activado	Activado	SI
284	Activación	Activado	Activado	SI

285	Activación	Activado	Activado	SI
286	Desactivación	Desactivado	Desactivado	SI
287	Activación	Activado	Activado	SI
288	Desactivación	Desactivado	Desactivado	SI
289	Desactivación	Desactivado	Desactivado	SI
290	Desactivación	Desactivado	Desactivado	SI
291	Desactivación	Desactivado	Desactivado	SI
292	Desactivación	Desactivado	Desactivado	SI
293	Activación	Activado	Activado	SI
294	Desactivación	Desactivado	Desactivado	SI
295	Activación	Activado	Activado	SI
296	Desactivación	Desactivado	Desactivado	SI
297	Activación	Activado	Activado	SI
298	Desactivación	Desactivado	Desactivado	SI
299	Desactivación	Desactivado	Desactivado	SI
300	Desactivación	Desactivado	Desactivado	SI
301	Desactivación	Desactivado	Desactivado	SI

302	Desactivación	Desactivado	Desactivado	SI
303	Desactivación	Desactivado	Desactivado	SI
304	Desactivación	Desactivado	Desactivado	SI
305	Activación	Activado	Desactivado	NO
306	Desactivación	Desactivado	Desactivado	SI
307	Activación	Activado	Activado	SI
308	Desactivación	Desactivado	Desactivado	SI
309	Activación	Activado	Activado	SI
310	Desactivación	Desactivado	Desactivado	SI
311	Activación	Activado	Activado	SI
312	Desactivación	Desactivado	Desactivado	SI
313	Activación	Activado	Activado	SI
314	Activación	Activado	Activado	SI
315	Activación	Activado	Activado	SI
316	Activación	Activado	Activado	SI
317	Activación	Activado	Activado	SI
318	Desactivación	Desactivado	Desactivado	SI

319	Activación	Activado	Activado	SI
320	Activación	Activado	Activado	SI
321	Activación	Activado	Activado	SI
322	Desactivación	Desactivado	Desactivado	SI
323	Activación	Activado	Activado	SI
324	Activación	Activado	Activado	SI
325	Activación	Activado	Activado	SI
326	Desactivación	Desactivado	Desactivado	SI
327	Activación	Activado	Activado	SI
328	Desactivación	Desactivado	Desactivado	SI
329	Activación	Activado	Activado	SI
330	Desactivación	Desactivado	Desactivado	SI
331	Activación	Activado	Activado	SI
332	Activación	Activado	Activado	SI
333	Activación	Activado	Activado	SI
334	Activación	Activado	Activado	SI
335	Activación	Activado	Activado	SI

336	Desactivación	Desactivado	Desactivado	SI
337	Activación	Activado	Activado	SI
338	Activación	Activado	Activado	SI
339	Activación	Activado	Activado	SI
340	Desactivación	Desactivado	Desactivado	SI
341	Activación	Activado	Activado	SI
342	Desactivación	Desactivado	Desactivado	SI
343	Activación	Activado	Activado	SI
344	Desactivación	Desactivado	Desactivado	SI
345	Activación	Activado	Desactivado	NO
346	Desactivación	Desactivado	Desactivado	SI
347	Activación	Activado	Activado	SI
348	Activación	Activado	Activado	SI
349	Activación	Activado	Activado	SI
350	Activación	Activado	Activado	SI
351	Activación	Activado	Activado	SI
352	Desactivación	Desactivado	Desactivado	SI

353	Activación	Activado	Activado	SI
354	Activación	Activado	Activado	SI
355	Desactivación	Desactivado	Desactivado	SI
356	Desactivación	Desactivado	Desactivado	SI
357	Activación	Activado	Desactivado	NO
358	Desactivación	Desactivado	Desactivado	SI
359	Activación	Activado	Activado	SI
360	Desactivación	Desactivado	Desactivado	SI
361	Activación	Activado	Activado	SI
362	Desactivación	Desactivado	Desactivado	SI
363	Desactivación	Desactivado	Desactivado	SI
364	Desactivación	Desactivado	Desactivado	SI
365	Activación	Activado	Activado	SI
366	Desactivación	Desactivado	Desactivado	SI
367	Activación	Activado	Activado	SI
368	Activación	Activado	Activado	SI
369	Activación	Activado	Activado	SI

370	Desactivación	Desactivado	Desactivado	SI
371	Activación	Activado	Activado	SI
372	Desactivación	Desactivado	Desactivado	SI
373	Desactivación	Desactivado	Desactivado	SI
374	Desactivación	Desactivado	Desactivado	SI
375	Desactivación	Desactivado	Desactivado	SI
376	Desactivación	Desactivado	Desactivado	SI
377	Activación	Activado	Activado	SI
378	Desactivación	Desactivado	Desactivado	SI
379	Activación	Activado	Activado	SI
380	Activación	Activado	Activado	SI
381	Activación	Activado	Activado	SI
382	Activación	Activado	Activado	SI
383	Activación	Activado	Activado	SI
384	Desactivación	Desactivado	Desactivado	SI

Tabla B. 2

Muestra tomada del monitoreo de la alarma.

Datos	Monitoreo de alarma IoT	Estado deseado de alarma en el aplicativo	Estado actual de la alarma en el aplicativo	¿Estado actual es igual a estado deseado de la alarma en el aplicativo?
1	Activación	Activado	Activado	SI
2	Activación	Activado	Activado	SI
3	Activación	Activado	Activado	SI
4	Activación	Activado	Activado	SI
5	Activación	Activado	Activado	SI
6	Desactivación	Desactivado	Desactivado	SI
7	Activación	Activado	Activado	SI
8	Activación	Activado	Activado	SI
9	Activación	Activado	Desactivado	NO
10	Desactivación	Desactivado	Desactivado	SI
11	Activación	Activado	Activado	SI
12	Desactivación	Desactivado	Desactivado	SI
13	Activación	Activado	Activado	SI

14	Desactivación	Desactivado	Desactivado	SI
15	Activación	Activado	Activado	SI
16	Desactivación	Desactivado	Desactivado	SI
17	Activación	Activado	Activado	SI
18	Desactivación	Desactivado	Desactivado	SI
19	Activación	Activado	Desactivado	NO
20	Activación	Activado	Activado	SI
21	Activación	Activado	Activado	SI
22	Desactivación	Desactivado	Desactivado	SI
23	Activación	Activado	Activado	SI
24	Desactivación	Desactivado	Desactivado	SI
25	Activación	Activado	Activado	SI
26	Desactivación	Desactivado	Desactivado	SI
27	Desactivación	Desactivado	Desactivado	SI
28	Desactivación	Desactivado	Desactivado	SI
29	Activación	Activado	Activado	SI
30	Desactivación	Desactivado	Desactivado	SI

31	Activación	Activado	Activado	SI
32	Desactivación	Desactivado	Desactivado	SI
33	Desactivación	Desactivado	Desactivado	SI
34	Desactivación	Desactivado	Desactivado	SI
35	Activación	Activado	Activado	SI
36	Desactivación	Desactivado	Desactivado	SI
37	Activación	Activado	Activado	SI
38	Activación	Activado	Activado	SI
39	Activación	Activado	Activado	SI
40	Desactivación	Desactivado	Desactivado	SI
41	Activación	Activado	Activado	SI
42	Activación	Activado	Activado	SI
43	Activación	Activado	Activado	SI
44	Desactivación	Desactivado	Desactivado	SI
45	Activación	Activado	Activado	SI
46	Desactivación	Desactivado	Desactivado	SI
47	Activación	Activado	Activado	SI

48	Desactivación	Desactivado	Desactivado	SI
49	Activación	Activado	Activado	SI
50	Activación	Activado	Activado	SI
51	Activación	Activado	Activado	SI
52	Desactivación	Desactivado	Desactivado	SI
53	Activación	Activado	Activado	SI
54	Activación	Activado	Activado	SI
55	Activación	Activado	Activado	SI
56	Activación	Activado	Activado	SI
57	Activación	Activado	Activado	SI
58	Desactivación	Desactivado	Desactivado	SI
59	Activación	Activado	Activado	SI
60	Desactivación	Desactivado	Desactivado	SI
61	Desactivación	Desactivado	Desactivado	SI
62	Desactivación	Desactivado	Desactivado	SI
63	Activación	Activado	Activado	SI
64	Desactivación	Desactivado	Desactivado	SI

65	Activación	Activado	Activado	SI
66	Desactivación	Desactivado	Desactivado	SI
67	Desactivación	Desactivado	Desactivado	SI
68	Desactivación	Desactivado	Desactivado	SI
69	Activación	Activado	Activado	SI
70	Desactivación	Desactivado	Desactivado	SI
71	Activación	Activado	Activado	SI
72	Activación	Activado	Activado	SI
73	Activación	Activado	Activado	SI
74	Desactivación	Desactivado	Desactivado	SI
75	Desactivación	Desactivado	Desactivado	SI
76	Desactivación	Desactivado	Desactivado	SI
77	Activación	Activado	Activado	SI
78	Desactivación	Desactivado	Desactivado	SI
79	Activación	Activado	Activado	SI
80	Activación	Activado	Activado	SI
81	Activación	Activado	Activado	SI

82	Desactivación	Desactivado	Desactivado	SI
83	Activación	Activado	Desactivado	NO
84	Desactivación	Desactivado	Desactivado	SI
85	Desactivación	Desactivado	Desactivado	SI
86	Desactivación	Desactivado	Desactivado	SI
87	Activación	Activado	Activado	SI
88	Desactivación	Desactivado	Desactivado	SI
89	Activación	Activado	Activado	SI
90	Activación	Activado	Activado	SI
91	Activación	Activado	Activado	SI
92	Desactivación	Desactivado	Desactivado	SI
93	Activación	Activado	Activado	SI
94	Desactivación	Desactivado	Desactivado	SI
95	Desactivación	Desactivado	Desactivado	SI
96	Desactivación	Desactivado	Desactivado	SI
97	Activación	Activado	Activado	SI
98	Desactivación	Desactivado	Desactivado	SI

99	Desactivación	Desactivado	Desactivado	SI
100	Desactivación	Desactivado	Desactivado	SI
101	Activación	Activado	Activado	SI
102	Desactivación	Desactivado	Desactivado	SI
103	Activación	Activado	Activado	SI
104	Desactivación	Desactivado	Desactivado	SI
105	Desactivación	Desactivado	Desactivado	SI
106	Desactivación	Desactivado	Desactivado	SI
107	Activación	Activado	Activado	SI
108	Desactivación	Desactivado	Desactivado	SI
109	Activación	Activado	Activado	SI
110	Desactivación	Desactivado	Desactivado	SI
111	Desactivación	Desactivado	Desactivado	SI
112	Desactivación	Desactivado	Desactivado	SI
113	Desactivación	Desactivado	Desactivado	SI
114	Desactivación	Desactivado	Desactivado	SI
115	Activación	Activado	Activado	SI

116	Desactivación	Desactivado	Desactivado	SI
117	Activación	Activado	Activado	SI
118	Desactivación	Desactivado	Desactivado	SI
119	Desactivación	Desactivado	Desactivado	SI
120	Activación	Activado	Activado	SI
121	Desactivación	Desactivado	Desactivado	SI
122	Activación	Activado	Activado	SI
123	Desactivación	Desactivado	Desactivado	SI
124	Desactivación	Desactivado	Desactivado	SI
125	Desactivación	Desactivado	Desactivado	SI
126	Desactivación	Desactivado	Desactivado	SI
127	Desactivación	Desactivado	Desactivado	SI
128	Activación	Activado	Activado	SI
129	Activación	Activado	Activado	SI
130	Desactivación	Desactivado	Desactivado	SI
131	Activación	Activado	Activado	SI
132	Activación	Activado	Activado	SI

133	Activación	Activado	Activado	SI
134	Activación	Activado	Activado	SI
135	Desactivación	Desactivado	Desactivado	SI
136	Desactivación	Desactivado	Desactivado	SI
137	Activación	Activado	Activado	SI
138	Desactivación	Desactivado	Desactivado	SI
139	Activación	Activado	Activado	SI
140	Desactivación	Desactivado	Desactivado	SI
141	Desactivación	Desactivado	Desactivado	SI
142	Desactivación	Desactivado	Desactivado	SI
143	Activación	Activado	Activado	SI
144	Desactivación	Desactivado	Desactivado	SI
145	Desactivación	Desactivado	Desactivado	SI
146	Desactivación	Desactivado	Desactivado	SI
147	Desactivación	Desactivado	Desactivado	SI
148	Activación	Activado	Activado	SI
149	Activación	Activado	Activado	SI

150	Desactivación	Desactivado	Activado	NO
151	Activación	Activado	Activado	SI
152	Activación	Activado	Activado	SI
153	Activación	Activado	Activado	SI
154	Activación	Activado	Activado	SI
155	Desactivación	Desactivado	Desactivado	SI
156	Activación	Activado	Activado	SI
157	Activación	Activado	Activado	SI
158	Desactivación	Desactivado	Desactivado	SI
159	Activación	Activado	Activado	SI
160	Desactivación	Desactivado	Desactivado	SI
161	Desactivación	Desactivado	Desactivado	SI
162	Desactivación	Desactivado	Desactivado	SI
163	Activación	Activado	Activado	SI
164	Desactivación	Desactivado	Desactivado	SI
165	Activación	Activado	Activado	SI
166	Activación	Activado	Activado	SI

167	Activación	Activado	Activado	SI
168	Activación	Activado	Activado	SI
169	Activación	Activado	Activado	SI
170	Desactivación	Desactivado	Desactivado	SI
171	Activación	Activado	Activado	SI
172	Desactivación	Desactivado	Desactivado	SI
173	Activación	Activado	Activado	SI
174	Desactivación	Desactivado	Desactivado	SI
175	Desactivación	Desactivado	Desactivado	SI
176	Desactivación	Desactivado	Desactivado	SI
177	Activación	Activado	Activado	SI
178	Activación	Activado	Activado	SI
179	Activación	Activado	Activado	SI
180	Desactivación	Desactivado	Desactivado	SI
181	Desactivación	Desactivado	Desactivado	SI
182	Activación	Activado	Activado	SI
183	Activación	Activado	Activado	SI

184	Activación	Activado	Activado	SI
185	Desactivación	Desactivado	Desactivado	SI
186	Desactivación	Desactivado	Desactivado	SI
187	Activación	Activado	Activado	SI
188	Desactivación	Desactivado	Desactivado	SI
189	Activación	Activado	Activado	SI
190	Activación	Activado	Activado	SI
191	Desactivación	Desactivado	Desactivado	SI
192	Desactivación	Desactivado	Desactivado	SI
193	Activación	Activado	Activado	SI
194	Desactivación	Desactivado	Desactivado	SI
195	Desactivación	Desactivado	Desactivado	SI
196	Activación	Activado	Activado	SI
197	Desactivación	Desactivado	Desactivado	SI
198	Desactivación	Desactivado	Desactivado	SI
199	Desactivación	Desactivado	Desactivado	SI
200	Activación	Activado	Activado	SI

201	Desactivación	Desactivado	Desactivado	SI
202	Activación	Activado	Activado	SI
203	Activación	Activado	Activado	SI
204	Activación	Activado	Activado	SI
205	Desactivación	Desactivado	Desactivado	SI
206	Desactivación	Desactivado	Desactivado	SI
207	Activación	Activado	Activado	SI
208	Desactivación	Desactivado	Desactivado	SI
209	Activación	Activado	Activado	SI
210	Desactivación	Desactivado	Desactivado	SI
211	Activación	Activado	Activado	SI
212	Desactivación	Desactivado	Desactivado	SI
213	Activación	Activado	Activado	SI
214	Activación	Activado	Activado	SI
215	Activación	Activado	Activado	SI
216	Activación	Activado	Activado	SI
217	Activación	Activado	Activado	SI

218	Desactivación	Desactivado	Desactivado	SI
219	Activación	Activado	Activado	SI
220	Desactivación	Desactivado	Activado	NO
221	Activación	Activado	Activado	SI
222	Desactivación	Desactivado	Desactivado	SI
223	Activación	Activado	Activado	SI
224	Desactivación	Desactivado	Desactivado	SI
225	Activación	Activado	Activado	SI
226	Desactivación	Desactivado	Desactivado	SI
227	Activación	Activado	Activado	SI
228	Desactivación	Desactivado	Desactivado	SI
229	Activación	Activado	Activado	SI
230	Desactivación	Desactivado	Desactivado	SI
231	Activación	Activado	Activado	SI
232	Activación	Activado	Activado	SI
233	Activación	Activado	Activado	SI
234	Desactivación	Desactivado	Desactivado	SI

235	Desactivación	Desactivado	Activado	NO
236	Desactivación	Desactivado	Desactivado	SI
237	Activación	Activado	Activado	SI
238	Desactivación	Desactivado	Desactivado	SI
239	Activación	Activado	Activado	SI
240	Desactivación	Desactivado	Desactivado	SI
241	Activación	Activado	Activado	SI
242	Desactivación	Desactivado	Desactivado	SI
243	Activación	Activado	Activado	SI
244	Desactivación	Desactivado	Desactivado	SI
245	Desactivación	Desactivado	Desactivado	SI
246	Desactivación	Desactivado	Desactivado	SI
247	Activación	Activado	Activado	SI
248	Desactivación	Desactivado	Desactivado	SI
249	Activación	Activado	Activado	SI
250	Activación	Activado	Activado	SI
251	Activación	Activado	Activado	SI

252	Activación	Activado	Activado	SI
253	Activación	Activado	Activado	SI
254	Desactivación	Desactivado	Desactivado	SI
255	Activación	Activado	Activado	SI
256	Desactivación	Desactivado	Desactivado	SI
257	Activación	Activado	Activado	SI
258	Desactivación	Desactivado	Desactivado	SI
259	Activación	Activado	Activado	SI
260	Desactivación	Desactivado	Desactivado	SI
261	Activación	Activado	Desactivado	NO
262	Desactivación	Desactivado	Desactivado	SI
263	Activación	Activado	Activado	SI
264	Activación	Activado	Activado	SI
265	Activación	Activado	Activado	SI
266	Activación	Activado	Activado	SI
267	Activación	Activado	Activado	SI
268	Desactivación	Desactivado	Desactivado	SI

269	Desactivación	Desactivado	Desactivado	SI
270	Desactivación	Desactivado	Desactivado	SI
271	Desactivación	Desactivado	Desactivado	SI
272	Desactivación	Desactivado	Desactivado	SI
273	Activación	Activado	Activado	SI
274	Desactivación	Desactivado	Desactivado	SI
275	Activación	Activado	Activado	SI
276	Desactivación	Desactivado	Desactivado	SI
277	Activación	Activado	Activado	SI
278	Activación	Activado	Activado	SI
279	Activación	Activado	Activado	SI
280	Desactivación	Desactivado	Desactivado	SI
281	Activación	Activado	Activado	SI
282	Activación	Activado	Activado	SI
283	Activación	Activado	Activado	SI
284	Activación	Activado	Activado	SI
285	Activación	Activado	Activado	SI

286	Desactivación	Desactivado	Desactivado	SI
287	Activación	Activado	Activado	SI
288	Desactivación	Desactivado	Desactivado	SI
289	Desactivación	Desactivado	Desactivado	SI
290	Desactivación	Desactivado	Desactivado	SI
291	Desactivación	Desactivado	Desactivado	SI
292	Desactivación	Desactivado	Desactivado	SI
293	Activación	Activado	Activado	SI
294	Desactivación	Desactivado	Desactivado	SI
295	Activación	Activado	Activado	SI
296	Desactivación	Desactivado	Desactivado	SI
297	Activación	Activado	Activado	SI
298	Desactivación	Desactivado	Desactivado	SI
299	Desactivación	Desactivado	Desactivado	SI
300	Desactivación	Desactivado	Desactivado	SI
301	Desactivación	Desactivado	Desactivado	SI
302	Desactivación	Desactivado	Desactivado	SI

303	Desactivación	Desactivado	Desactivado	SI
304	Desactivación	Desactivado	Desactivado	SI
305	Activación	Activado	Desactivado	NO
306	Desactivación	Desactivado	Desactivado	SI
307	Activación	Activado	Activado	SI
308	Desactivación	Desactivado	Desactivado	SI
309	Activación	Activado	Activado	SI
310	Desactivación	Desactivado	Desactivado	SI
311	Activación	Activado	Activado	SI
312	Desactivación	Desactivado	Desactivado	SI
313	Activación	Activado	Activado	SI
314	Activación	Activado	Activado	SI
315	Activación	Activado	Activado	SI
316	Activación	Activado	Activado	SI
317	Activación	Activado	Activado	SI
318	Desactivación	Desactivado	Desactivado	SI
319	Activación	Activado	Activado	SI

320	Activación	Activado	Activado	SI
321	Activación	Activado	Activado	SI
322	Desactivación	Desactivado	Desactivado	SI
323	Activación	Activado	Activado	SI
324	Activación	Activado	Activado	SI
325	Activación	Activado	Activado	SI
326	Desactivación	Desactivado	Desactivado	SI
327	Activación	Activado	Activado	SI
328	Desactivación	Desactivado	Desactivado	SI
329	Activación	Activado	Activado	SI
330	Desactivación	Desactivado	Desactivado	SI
331	Activación	Activado	Activado	SI
332	Activación	Activado	Activado	SI
333	Activación	Activado	Activado	SI
334	Activación	Activado	Activado	SI
335	Activación	Activado	Activado	SI
336	Desactivación	Desactivado	Desactivado	SI

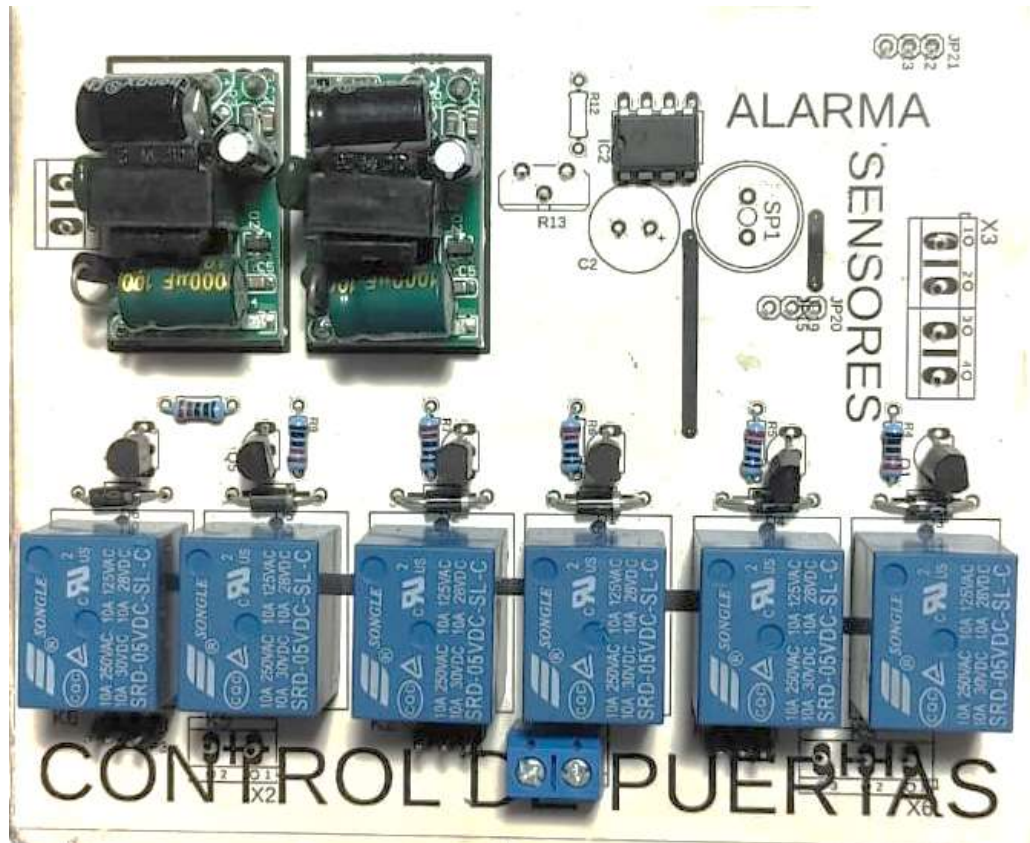
337	Activación	Activado	Activado	SI
338	Activación	Activado	Activado	SI
339	Activación	Activado	Activado	SI
340	Desactivación	Desactivado	Desactivado	SI
341	Activación	Activado	Activado	SI
342	Desactivación	Desactivado	Desactivado	SI
343	Activación	Activado	Activado	SI
344	Desactivación	Desactivado	Desactivado	SI
345	Activación	Activado	Desactivado	NO
346	Desactivación	Desactivado	Desactivado	SI
347	Activación	Activado	Activado	SI
348	Activación	Activado	Activado	SI
349	Activación	Activado	Activado	SI
350	Activación	Activado	Activado	SI
351	Activación	Activado	Activado	SI
352	Desactivación	Desactivado	Desactivado	SI
353	Activación	Activado	Activado	SI

354	Activación	Activado	Activado	SI
355	Desactivación	Desactivado	Desactivado	SI
356	Desactivación	Desactivado	Desactivado	SI
357	Activación	Activado	Desactivado	NO
358	Desactivación	Desactivado	Desactivado	SI
359	Activación	Activado	Activado	SI
360	Desactivación	Desactivado	Desactivado	SI
361	Activación	Activado	Activado	SI
362	Desactivación	Desactivado	Desactivado	SI
363	Desactivación	Desactivado	Desactivado	SI
364	Desactivación	Desactivado	Desactivado	SI
365	Activación	Activado	Activado	SI
366	Desactivación	Desactivado	Desactivado	SI
367	Activación	Activado	Activado	SI
368	Activación	Activado	Activado	SI
369	Activación	Activado	Activado	SI
370	Desactivación	Desactivado	Desactivado	SI

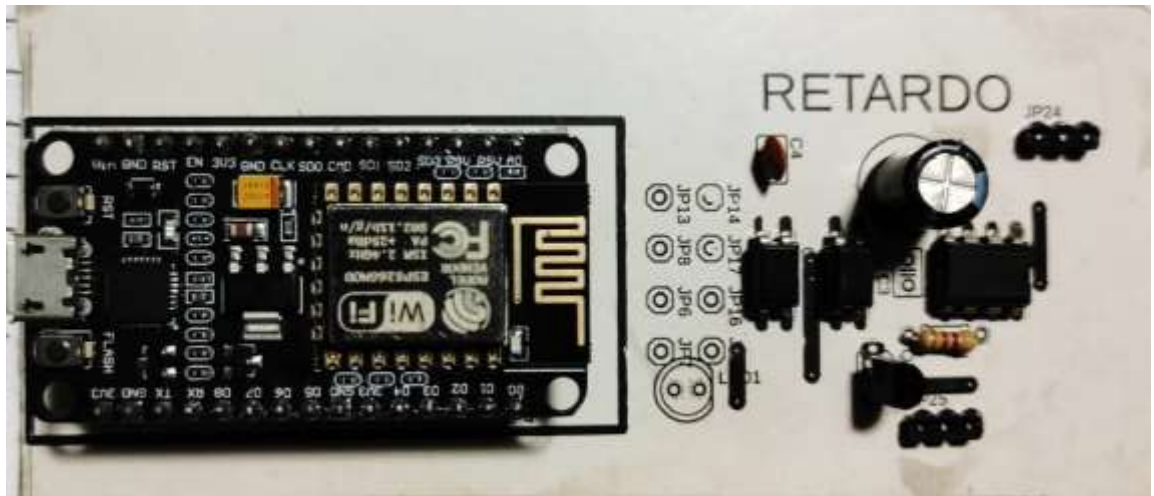
371	Activación	Activado	Activado	SI
372	Desactivación	Desactivado	Desactivado	SI
373	Desactivación	Desactivado	Desactivado	SI
374	Desactivación	Desactivado	Desactivado	SI
375	Desactivación	Desactivado	Desactivado	SI
376	Desactivación	Desactivado	Desactivado	SI
377	Activación	Activado	Activado	SI
378	Desactivación	Desactivado	Desactivado	SI
379	Activación	Activado	Activado	SI
380	Activación	Activado	Activado	SI
381	Activación	Activado	Activado	SI
382	Activación	Activado	Activado	SI
383	Activación	Activado	Activado	SI
384	Desactivación	Desactivado	Desactivado	SI

ANEXO C

PANEL FOTOGRAFICO



FOTOGRAFIA DE TARJETA DE CONTROL DE CARGAS



FOTOGRAFIA DE TARJETA DE COMUNICACIÓN INALAMBRICA



FOTOGRAFIA DE MAQUETA VISTA FRONTAL, DONDE MUESTRA
PUERTA DE COCHERA, PUERTA DE ENTRADA Y PUERTA DE SEGUNDO
PISO



FOTOGRAFIA DE MAQUETA VISTA LATERAL IZQUIERDO



FOTOGRAFIA DE MAQUETA VISTA LATERAL DERECHO, MUESTRA
PUERTA DE PRIMER PISO