UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE ELECTRÓNICA Y AUTOMATIZACIÓN

SISTEMA IOT CON SAAC PARA LA AUTOMATIZACIÓN DE SEGURIDAD DE UN HOGAR

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Electrónica y Automatización

AUTOR: Alexis Patricio Pugarin Pincay
TUTOR: Andrés Sebastián Calero Calero

Quito-Ecuador

2024

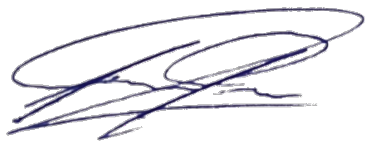
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Alexis Patricio Pugarin Pincay con documento de identificación N°1723949598 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de maneratotal o parcial el presente trabajo de titulación.

Quito, 11 de marzo del año 2024

Atentamente,



Alexis Patricio Pugarin Pincay

1723949598

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Alexis Patricio Pugarin Pincay con documento de identificación No. 1723949598, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del proyecto técnico: "Sistema IoT con saac para la automatización de seguridad de un hogar" el cual ha sido desarrollado para optar por el título de: Ingeniero en Electrónica y Automatización, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad PolitécnicaSalesiana.

Quito, 11 de marzo del año 2024

Atentamente,

Alexis Patricio Pugarin Pincay
1723949598

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Andrés Sebastián Calero Calero con documento de identificación N° 1719252346, docente de la Universidad Politécnica Salesiana, declaro quebajo mi tutoría fue desarrollado el trabajo de titulación: SISTEMA IOT CON SAAC PARA LA AUTOMATIZACIÓN DE SEGURIDAD DE UN HOGAR, realizado por Alexis Patricio Pugarin Pincay, con documento de identificación N° 1723949598, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 11 de marzo del año 2024

Atentamente,

Ing. Andrés Sebastián Calero Calero Ms.C.
1719252346

DEDICATORIAS

En este momento de gran importancia para mi vida académica, quiero agradecer de corazón y dedicar este trabajo de titulación a mis padres Susana Leonor Ortiz Pincay y Patricio Pugarin Diaz. Su amor incondicional en cada momento de mi vida, su apoyo constante y sabios consejos han sido los pilares más importantes para poder convertirme en la persona que soy en la actualidad en este gratificante viaje, que llamamos vida.

A ustedes Priscila Acosta y Dilan Pugarin, que siempre creyeron en mis sueños y me alentaron a alcanzar cada meta, les dedico este logro. Su sacrificio y esfuerzo han sido la fuente de inspiración que me impulsó a superar desafíos y a perseverar en este camino académico.

Este trabajo no solo representa mi dedicación, sino también la influencia positiva de su gran amor y ejemplo en mi vida para culminar una meta de relevancia y avanzar a la próxima. Gracias por ser mis pilares, por compartir las alegrías y los desafíos, y por ser la mejor familia que alguien podría desear.

Con gratitud infinita.

Alexis Patricio Pugarin Pincay

AGRADECIMIENTOS

En este momento en el que culmina una etapa académica de relevancia para mi vida, no puedo dejar de expresar mi profundo agradecimiento por el apoyo constante e inquebrantable que me han brindado a lo largo de mi trayecto de titulación. Su amor, aliento y comprensión han sido las fuentes de motivación y trabajo que me han llevado a alcanzar este logro significativo.

Agradezco sinceramente su orientación y apoyo durante la realización de este trabajo de titulación. Su experiencia y consejos han sido fundamentales para mi desarrollo académico, a ustedes, que siempre estuvieron en cada momento, celebrando mis triunfos y brindando su apoyo en los momentos desafiantes. Su sacrificio y dedicación han sido la luz que iluminó mi camino durante esta etapa de formación profesional.

Gracias principalmente a Dios, a mi familia, a mis padres y a mis docentes, por ser mis guías, por inspirarme con su ejemplo y por ser la base sólida sobre la cual construí mis ambiciones. Este logro no solo es mío, sino también de ustedes, quienes han sido mi mayor fuente de fortaleza e inspiración.

Con amor y agradecimiento infinitos.

Alexis Patricio Pugarin Pincay

ÍNDICE DE CONTENIDO

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN II
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA III
CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN IV
DEDICATORIAS V
AGRADECIMIENTOS VI
ÍNDICE DE CONTENIDO VII
ÍNDICE DE FIGURAS IX
ÍNDICE DE TABLAS X
RESUMEN XI
ABSTRACT XII
INTRODUCCIÓN XIII
CAPÍTULO I 1
ANTECEDENTES 1
1.1 Problema de Estudio 1
1.2 Justificación 2
1.3 Objetivos 3
1.3.1 Objetivo General 3
1.3.2 Objetivo Específicos 3
CAPÍTULO II 4
MARCO TEORICO 4
2.1 Automatización Residencial 4
2.1.1 Definición 4
2.1.2 Tecnologías de la información y comunicación 4
2.2 Sistemas automáticos y sistemas domóticos 6
2.3 Fundamentos de Internet de las Cosas (IoT): 7
2.3.1 Principios y conceptos básicos de IoT 7
2.3.2 Evolución de IoT 7
2.3.3 Aplicaciones de IoT en entornos residenciales para la seguridad. 8
2.4 Sistemas Complementarios para Automatizaciones y Control (SAAC) 9
2.4.1 Características y funcionalidades de los SAAC 10
2.5 Home Assistant como Plataforma de Automatización Residencial 10
2.5.1 Características y Funcionalidades de Home Assistant 11
2.5.2 Integración de Home Assistant en el Contexto de Seguridad Residencial 12
2.6 Arquitectura de un Sistema IoT con SAAC 12
CAPITULO III 17
DISEÑO E IMPLEMENTACIÓN 17

3.1 Análisis del diseño del proyecto. 17
3.1.1 Descripción del Sistema y Desarrollo del prototipo 17
3.2 Funcionamiento del sistema 18
3.3 Diagrama de flujo del sistema 21
3.3.1 Fase de detección 21
3.3.2 Fase de análisis de datos 23
3.3.3 Fase de interpretación y toma de decisiones 24
3.3.4 Fase de alarma 25
3.3.5 Fase de grabación y almacenamiento 25
3.4 Diseño Electrónico 26
3.4.1 Unidad central 26
3.4.2 Sistema sensor, controlador y actuador (SCA) 27
3.4.3 Escenario y transcurso de la prueba 33
CAPITULO IV 39
ANÁLISIS Y RESULTADOS 39
4.1 Recopilación de datos 39
4.1.1 Detección de sensores de la residencia 39
4.1.2 Detección de actuadores 41
4.1.3 Detección de notificaciones 42
4.2 Análisis de datos 43
4.2.1 Análisis de los sensores del hogar 43
4.2.2 Análisis de los actuadores del hogar 48
4.2.3 Análisis de las notificaciones enviadas a los usuarios 51
CONCLUSIONES 53
RECOMENDACIONES 55
BIBLIOGRAFÍA 56
ANEXOS 58
ANEXO 1- Instalación del sistema operativo de Home Assistant en el hardware Raspberry Pi 58
ANEXO 2- Instalación de Home Assistant en dispositivos móviles 60
ANEXO 3 - Instalación del coordinador universal Sonoff-P Zigbee USB 61
ANEXO 4 - Instalación de dispositivos Wifi 63
ANEXO 5- Añadir dispositivos cableados con un nodo esp32 para su integración con Home Assistant 64

ÍNDICE DE FIGURAS

Figura 2. 1. Equipamiento tecnológico del hogar (en miles) de 2014 a 2023 5
Figura 2. 2. Hogares con acceso a internet del 2014 a 2023 5
Figura 2. 3. Aplicación de internet en los hogares (en miles) de 2014 a 2023 6
Figura 2. 4. Aplicaciones de IoT en entornos residenciales para la seguridad. 9
Figura 2. 5. Interacción de los SAAC con la seguridad del hogar. 10
Figura 2. 6. Plataforma Home Asistant 11
Figura 2. 7. Gestión de dispositivos IoT: importancia, desafíos, soluciones 13

Figura 3. 1. Diagrama de flujo del funcionamiento del sistema 21
Figura 3. 2. Fase de detección 22
Figura 3. 3. Fase de análisis de datos 23
Figura 3. 4. Fase de interpretación y toma de decisiones 24
Figura 3. 5. Fase de Alarma 25
Figura 3. 6. Fase de grabación y almacenamiento 26
Figura 3. 7. Unidad Central 27
Figura 3. 8. Sensor de Movimiento cableado- PIR100PT 28
Figura 3. 9. Sensor de movimiento exterior- PIR-126MWA 28
Figura 3. 10. Sensor de movimiento Aqara 29
Figura 3. 11. Sensor de magnético 29
Figura 3. 12. Cámara de seguridad 30
Figura 3. 13. Esp32 31
Figura 3. 14. Zonoff zegbee 31
Figura 3. 15. Home Assistant web 32
Figura 3. 16. Sirena 32
Figura 3. 17. Residencia parte exterior 34
Figura 3. 18. Residencia, puerta ingreso 34
Figura 3. 19. Patio de la residencia 35
Figura 3. 20. Parte posterior de la residencia 36
Figura 3. 21. Planta baja de la residencia – sala de estar 37
Figura 3. 22. Planta baja de la residencia – comedor 37
Figura 3. 23. Casa interior, planta alta 38

Figura 4. 1. Prueba de funcionamiento – sensor magnético puerta exterior 43
Figura 4. 2. Prueba de Funcionamiento - sensor de movimiento exterior 44
Figura 4. 3. Prueba de funcionamiento - cámara exterior 45
Figura 4. 4. Prueba de funcionamiento – sensores magnéticos puertas internas 46
Figura 4. 5. Prueba de funcionamiento - sensores de movimiento internos del hogar 47
Figura 4. 6. Prueba de Funcionamiento - sirena 48
Figura 4. 7. Prueba de Funcionamiento – alarma interna cámara 49
Figura 4. 8. Prueba de funcionamiento – iluminación del hogar 50
Figura 4. 9. Prueba de Funcionamiento - Notificaciones de emergencia Administrador 51
Figura 4. 10. Prueba de Funcionamiento - Notificaciones de emergencia usuarios 52

ÍNDICE DE TABLAS

Tabla 3. 1. Tabla indicativa de estado del sistema de seguridad. 20

Tabla 4. 1. Prueba de sensores residencia 40
Tabla 4. 2. Prueba de actuadores en la residencia 41
Tabla 4. 3. Prueba de notificaciones a los usuarios 42

RESUMEN

La expansión tecnológica constituye un elemento esencial en la estructura de cualquier sociedad, actualmente existe una tendencia del desarrollo tecnológico mediante la aplicación de soluciones automatizadas. Este estudio se focaliza en la implementación de un sistema de seguridad económico y orientado al usuario final donde se proyecta la implementación de una arquitectura centralizada que cumpla con los requisitos para establecer un sistema de comunicación IoT entre dispositivos finales, de acción e información hacia la plataforma Home Assistant.

El sistema será respaldado por hardware y software especializados, supervisará diversos procesos domóticos con el propósito de ser instalado en residencias y ser gestionado de forma local o remota, y proporcionar una interfaz de control amigable para los usuarios, utilizando diferentes herramientas y estrategias que sirven para complementar el lenguaje oral y acciones emergentes.

La integración de este sistema en una residencia convencional será evaluada en un entorno controlado, permitiendo a los usuarios administrar la seguridad de su hogar según una jerarquía asignada para cada usuario. Además de recibir notificaciones e interactuar con los diferentes métodos de gestión del sistema. El objetivo final es mejorar la calidad de vida de los usuarios, presentando este proyecto como una alternativa económica y efectiva para reforzar la seguridad en los hogares.

Palabras clave: IoT, Arquitectura, Hardware, Software, SAAC.

ABSTRACT

Technological expansion constitutes an essential element in the structure of any society; currently there is a trend of technological development through the application of automated solutions. This study focuses on the implementation of an economical security system oriented to the end user where the implementation of a centralized architecture is projected that meets the requirements to establish an IoT communication system between end devices, action and information towards the platform. HomeAssistant.

The system will be supported by specialized hardware and software, will supervise various home automation processes with the purpose of being installed in residences and being managed locally or remotely, and providing a user-friendly control interface, using different tools and strategies that serve to complement oral language and emerging actions.

The integration of this system in a conventional residence will be evaluated in a controlled environment, allowing users to manage the security of their home according to a hierarchy assigned to each user. In addition to receiving notifications and interacting with the different system management methods. The final objective is to improve the quality of life of users, presenting this project as an economical and effective alternative to reinforce security in homes.

Keywords: IoT, architecture, Hardware, Software, SAAC.

INTRODUCCIÓN

El presente trabajo se enmarca en el contexto tecnológico del Ecuador, donde la adopción de sistemas automatizados en diversos sectores ha experimentado un crecimiento sostenido de acuerdo con el informe "Tecnologías de la Información y comunicación", publicados por el Instituto Nacional de Estadística y Censos (INEC, 2023). En este contexto, el hogar es el núcleo fundamental de la vida cotidiana y en general de la población, se convierte en un área crucial para implementar un ecosistema de dispositivos inteligentes mediante el Internet de las cosas (IoT), con el propósito de proteger la integridad, bienes y mejorar la seguridad y calidad de vida de los usuarios (Asghari, Rahmani, & Javadi, 2019).

Desde los inicios de la era contemporánea, el avance tecnológico ha permeado todos los aspectos de la sociedad, marcando un cambio significativo en la forma en que interactuamos con nuestro entorno, cada vez implementando más dispositivos tecnológicos en el hogar y automatizando procesos, mejorando la calidad de vida de las personas, los asistentes inteligentes han ganado una considerable popularidad entre la población, brindando una experiencia de interacción novedosa. Sin embargo, esta adopción masiva no está exenta de desafíos, siendo la preocupación sobre el control de la información personal uno de los obstáculos más significativos (McCue, 2018). Este problema se agudiza al depender de dispositivos y servicios proporcionados por diferentes fabricantes, sin explorar otras vías para salvaguardar la integridad de los datos y funcionamiento.

Los principales asistentes inteligentes convencionales, son basados en la escucha de sonidos para su activación, presentan limitaciones como la ejecución de procesos, solo con palabras específicas, negando la activación de procesos desde dispositivos finales, también se presentan problemas de accesibilidad a algunos usuarios, especialmente para personas con discapacidad que enfrentan dificultades en la vocalización (Chaparro Misó, 2021) y en respuesta a estas problemáticas, Cabrera, Calatayud Sánchez, H. (2021) propusieron un sistemas de vigilancia domóticos que utilizan, sensores PIR, placas de desarrollo como Arduino con el fin de enviar notificaciones, integrando una arquitectura basada en Home Assistant. Asimismo, Chaparro Misó, D. (2021) implementó un Sistema

Aumentativo y Alternativo de Comunicación (SAAC) para dispositivos móviles Android, brindando la posibilidad de activar dispositivos, abordando la comunicación no verbal.

El diseño de un sistema de seguridad IoT y SAAC centralizado para la seguridad del hogar, integrando una arquitectura capaz de gestionar la comunicación entre dispositivos de acción e información a través de la plataforma Home Assistant. Este sistema busca no solo proporcionar seguridad y escalabilidad, sino también facilitar el acceso y control para personas con capacidades especiales, diseñados para tratar de compensar dificultades del habla, audición entre otros, que pueden dificultar el uso de las tecnologías.

Este trabajo de titulación busca diseñar un sistema de ejecución de forma local y remota para la seguridad en una residencia mediante un sistema IoT con SAAC, un sistema centralizado para la seguridad del hogar, integrando una arquitectura centralizada capaz de gestionar la comunicación entre dispositivos de acción e información a través de la plataforma Home Assistant de formal local o remota. Este sistema busca no solo proporcionar seguridad y escalabilidad, sino también facilitar el acceso y control para personas con capacidades especiales, diseñados para tratar de compensar dificultades del habla, audición entre otros, que pueden dificultar el uso de las tecnologías.

En consecuencia, este trabajo pretende ofrecer una solución integral, permitiendo la activación del asistente no solo por voz, sino también mediante sensores, facilitando la toma de decisiones y accionamientos múltiples para el control del hogar, especialmente diseñado para ser accesible y amigable para el usuario en ambientes controlados, destacando su capacidad para proporcionar beneficios en áreas como la gestión eficiente, la seguridad, la comunicación, el ahorro energético y el confort (Asghari, Rahmani, & Javadi, 2019; Calatayud Sánchez, 2021).

CAPÍTULO I

ANTECEDENTES

1.1 Problema de Estudio

El creciente uso de Automatizaciones para el para el hogar ha generado una aceptación generalizada en la sociedad contemporánea, sin embargo, esta enfrenta a un obstáculo crucial en su adopción. Este problema se centra en la inquietud al depender de dispositivos y servicios proporcionados por diferentes fabricantes restringiendo la interconexión entre dispositivos, para salvaguardar la integridad de la información personal recopilada por estos y garantizar su funcionamiento en cualquier escenario, que, hasta ahora, se aborda únicamente mediante sistemas de autenticación tradicionales. La falta de opciones de verificación alternativas limita la capacidad de mantener la integridad de los datos personales en caso de algún siniestro, planteando cuestionamientos éticos y de privacidad (McCue, 2018).

Adicionalmente, los sistemas convencionales de asistencia por voz, al depender principalmente de la escucha activa para detectar sonidos ambientales, ignoran la posibilidad de utilizar dispositivos finales (sensores) para la toma de decisiones y la realización de accionamientos secundarios. Este enfoque excluyente, señalado por Calatayud Sánchez (2021) y Romero Cabrera (2019), presenta un sesgo hacia la vocalización como único medio de interacción, ignorando a personas con discapacidad que enfrentan dificultades para comunicar sus necesidades de forma verbal, ya sea por problemas de vocalización, pérdida de la voz debido a accidentes o enfermedades, generando así problemas significativos de accesibilidad (Chaparro Misó, 2021).

En este contexto, el desarrollo de sistemas de asistencia inteligente como el propuesto por Cabrera, Calatayud Sánchez, H. (2021), que integra un sistema de vigilancia domótico automatizado utilizando cámaras IP, sensores PIR y protocolo MQTT, destaca la necesidad de explorar soluciones que vayan más allá de la escucha activa y consideren la diversidad de formas de comunicación.

En resumen, el problema de estudio se centra en la falta de opciones de autenticación en asistentes inteligentes, la limitación en la toma de decisiones basada únicamente en la escucha de sonidos y la exclusión de personas con discapacidad en la interacción con estos sistemas, planteando la necesidad de investigar y desarrollar enfoques más inclusivos y seguros para el diseño de asistentes inteligentes en el futuro.

1.2 Justificación

La creciente penetración de la tecnología de la información y comunicación (TIC) en los hogares ecuatorianos, como se evidencia en los indicadores recopilados por el Instituto Nacional de Estadística y Censos (INEC, 2023), señala un cambio paradigmático en las dinámicas cotidianas de la sociedad. Este aumento progresivo en el uso de sistemas inteligentes revela una necesidad creciente de soluciones tecnológicas que se integren de manera armoniosa en la vida diaria de los individuos.

El Internet de las cosas (IoT) emerge como un ecosistema vital que conecta objetos inteligentes para ofrecer servicios y beneficios complementarios en diversas áreas de la vida, según lo destacado por Asghari, Rahmani, y Javadi (2019). Entre las aplicaciones más significativas, se encuentra la monitorización y la toma de decisiones inmediatas, proporcionando una gestión eficiente, seguridad, comunicación, ahorro energético, optimización de procesos y confort para familias, hogares y empresas, según las investigaciones de Calatayud Sánchez (2021).

En este contexto, el presente trabajo de titulación se justifica como una respuesta pertinente y necesaria a esta realidad tecnológica en constante evolución. La propuesta de desarrollar un sistema de seguridad en hogares, aprovechando la plataforma Home Assistant y dispositivos finales, responde a la demanda de soluciones inteligentes y accesibles. La inclusión de la activación del asistente por voz y sensores, así como la posibilidad de accionamientos y toma de decisiones a través de un dashboard intuitivo, no solo busca ofrecer una mayor eficiencia y seguridad en el hogar, sino también garantizar la accesibilidad y comodidad para personas con capacidades especiales.

En síntesis, este trabajo se posiciona como una contribución relevante y aplicada que busca integrar tecnologías emergentes en el tejido cotidiano de la sociedad ecuatoriana, alineándose con las tendencias tecnológicas actuales y respondiendo a las necesidades cambiantes de los hogares contemporáneos.

1.3 Objetivos

1.3.1 Objetivo General

- Diseñar un sistema de ejecución de forma local y remota para la seguridad en una residencia mediante un sistema IoT con SAAC

1.3.2 Objetivo Específicos

- Investigar diversos protocolos, arquitecturas, servicios en línea y plataformas de servicios para el diseño de una arquitectura IoT para la seguridad en hogares.

- Diseñar una arquitectura IoT de comunicación entre dispositivos finales, de acción y de información hacia la plataforma Home Assistant para los diferentes procesos domóticos, mediante herramientas de tecnología de información y operación.

- Implementar en una residencia un sistema IoT con SAAC local y remoto para la seguridad y procesos domóticos mediante Hardware y Software especializados.

- Verificar el funcionamiento del sistema de seguridad en hogares para su validación mediante pruebas experimentales en un entorno controlado.

CAPÍTULO II

MARCO TEORICO

2.1 Automatización Residencial

2.1.1 Definición

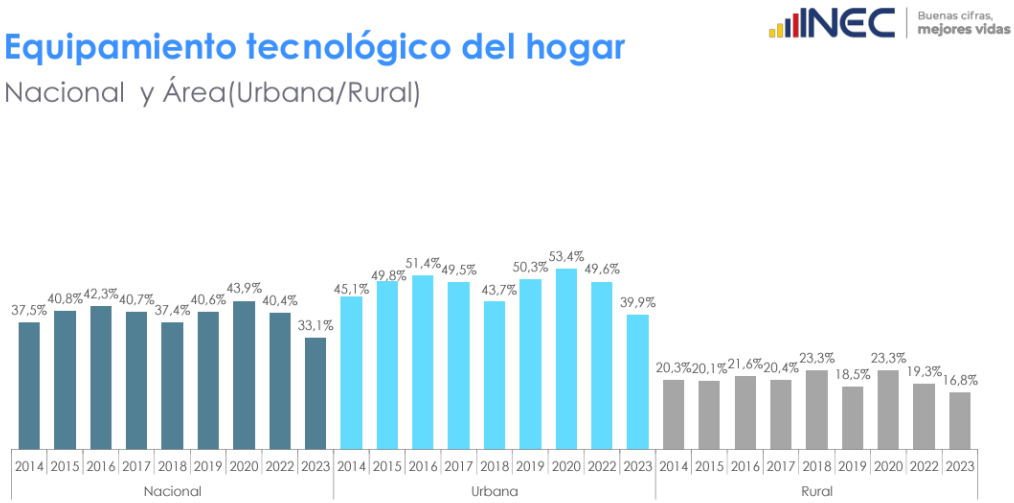
La automatización residencial se presenta como una solución integral para llevar a cabo tareas fundamentales en la vida cotidiana de los hogares, simulando acciones e interactuando con el usuario si este lo desea. Facilita una comunicación eficaz entre los residentes y diversos dispositivos, incluso en situaciones en las que los usuarios no se encuentran físicamente presentes. Esta capacidad permite aprovechar la tecnología disponible para proporcionar a las personas un entorno doméstico que les brinde tranquilidad, seguridad y comodidad. La implementación de automatizaciones se revela como una opción viable para potenciar varios campos entre los más destacados tenemos la seguridad en una residencia, utilizando elementos disuasorios como iluminación y sirenas, y recibiendo alertas ante cualquier intrusión no autorizada (Panchano, 2023).

2.1.2 Tecnologías de la información y comunicación

En el contexto tecnológico del Ecuador, donde la adopción de estos sistemas, ha experimentado un crecimiento sostenido de acuerdo con el informe “Tecnologías de la Información y comunicación”, publicados por el Instituto Nacional de Estadística y Censos (INEC, 2023).

En la Figura 2.1 se ilustra el incremento del uso de tecnología como resultado de la pandemia y el proceso de transformación digital. En el año 2014, se registra un índice del 37,5% en la incorporación de equipamiento tecnológico en los hogares, mientras que, en el año 2022, dicho índice asciende a un 40,4%, indicando un aumento en la posesión de dispositivos tecnológicos por parte de la población (INEC, 2023).

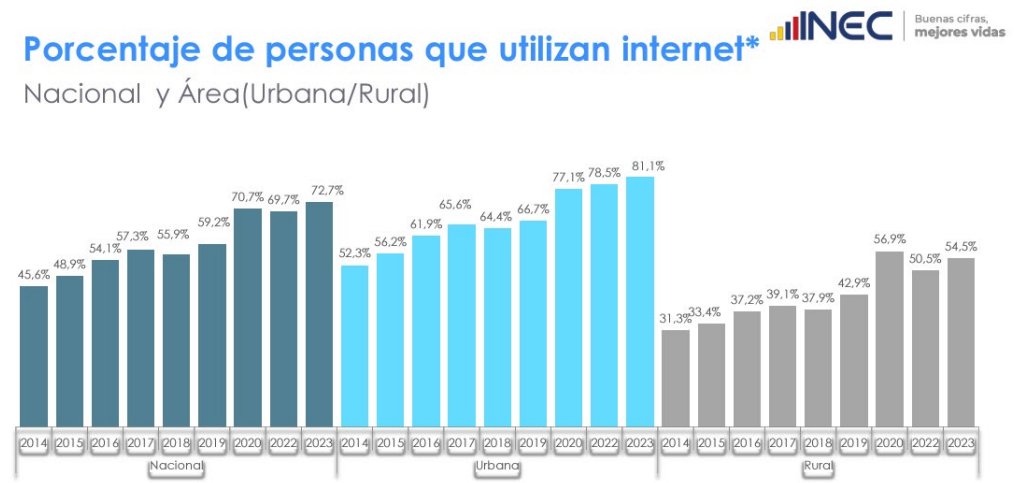
Figura 2. 1. Equipamiento tecnológico del hogar (en miles) de 2014 a 2023



Nota. *Equipamiento Tecnológico del Hogar. [Infografía]*, Tomado de (INEC, 2023)

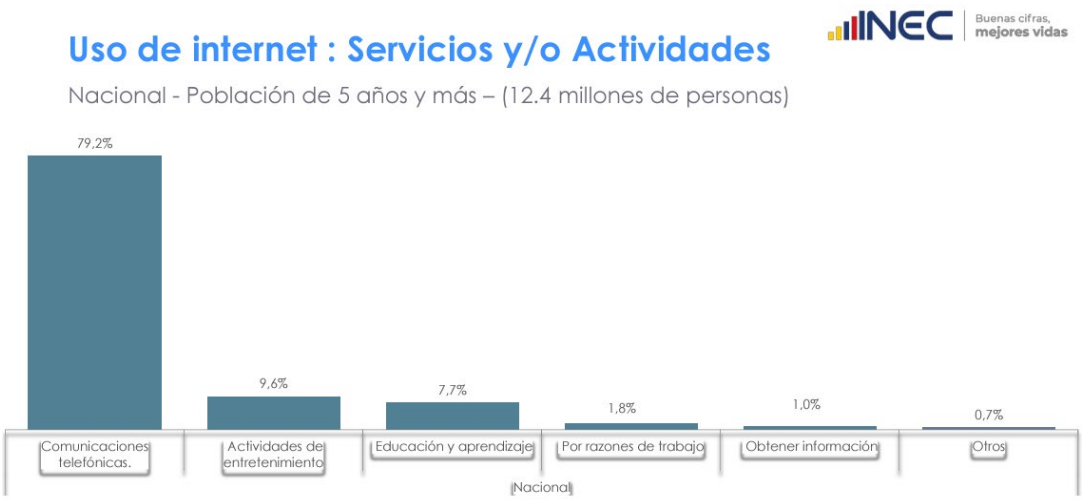
En la Figura 2.2, se destaca el aumento de hogares con acceso a internet, en el 2014 se obtiene un índice con un valor de 32,4% y en el 2023 se ubica en 62,2%, destacando que la población en el Ecuador adquiere mayores herramientas en el ámbito tecnológico, ahora como se observa en la Figura 3, un aspecto de gran relevancia es indicar, que la población en general utiliza el internet para la comunicación telefónica con un índice de 79,2%, mientras que para otros usos como integrar sistemas de seguridad en sus residencias, se obtiene un índice de 0,7%, denotando que la población en su gran mayoría aun no integra sistemas de seguridad inteligentes en sus hogares (INEC, 2023).

Figura 2. 2. Hogares con acceso a internet del 2014 a 2023



Nota. *Personas que Utilizan Internet. [Infografía]*, Tomado de (INEC, 2023)

Figura 2. 3. Aplicación de internet en los hogares (en miles) de 2014 a 2023



Nota. Uso de Internet: Servicios y/o Actividades. [Infografía], Tomado de (INEC, 2023)

2.2 Sistemas automáticos y sistemas domóticos

Tanto un sistema automático como un sistema domótico comparten la capacidad intrínseca de llevar a cabo acciones, no obstante, se diferencian significativamente en la amplitud y complejidad de las tareas que pueden ejecutar, así como en el grado de integración con tecnologías y dispositivos interconectados.

En el caso de un sistema automático, su enfoque está en la automatización de tareas específicas, resolviendo problemas particulares. Estos sistemas engloban una serie de componentes, como sensores, actuadores, lógica de control e interfaz de usuario, reunidos en un único dispositivo. Aunque pueden coexistir varios sistemas independientes en el mismo entorno, cada uno opera sin conocimiento de la información procesada por los demás. Por lo general, estos sistemas están diseñados para llevar a cabo funciones repetitivas y básicas, como encender o apagar actuadores. Su capacidad para adaptarse a preferencias individuales o responder a cambios en tiempo real suele ser limitada en comparación con los sistemas domóticos (González, 2023).

En contraste, un sistema domótico tiene como objetivo principal la integración y coordinación de una amplia variedad de sistemas y dispositivos. Busca crear un entorno inteligente donde la información recopilada por los automatismos independientes sea compartida y accesible para la toma de decisiones en procesos secundarios. Este enfoque

ofrece un mayor nivel de personalización, permitiendo a los usuarios programar escenarios complejos que involucren interacciones entre múltiples dispositivos. Además, un sistema domótico puede ser gestionado y monitoreado centralmente a través de una interfaz única, como una aplicación móvil o una plataforma en línea, lo que proporciona un acceso más fácil y una gestión remota más eficiente, además estos tienden a ser escalables, lo que significa que permiten la integración con diversos protocolos de comunicación y dispositivos provenientes de diferentes fabricantes. Esto contribuye a su versatilidad y capacidad para evolucionar con las necesidades cambiantes del usuario (González, 2023).

2.3 Fundamentos de Internet de las Cosas (IoT):

2.3.1 Principios y conceptos básicos de IoT

El término "Internet de las cosas" (IoT) se refiere a la interconexión entre diversos tipos de objetos físicos y virtuales, así como sistemas de información, a través de internet y ha experimentado una amplia adopción en varios aspectos de la vida diaria, incluyendo entornos urbanos, hogares y entidades educativas.

Las aplicaciones del IoT utilizan la interconexión de dispositivos para crear servicios compuestos mediante la combinación de servicios individuales preexistentes. Estos escenarios se despliegan mediante el uso de dispositivos inteligentes en diferentes áreas de la rutina diaria de los usuarios. Además, las aplicaciones de IoT aportan beneficios notables, facultando a los usuarios para tomar decisiones informadas, gestionar recursos y supervisar su entorno.

2.3.2 Evolución de IoT

La evolución del Internet de las Cosas (IoT) ha sido notable a lo largo del tiempo, marcando un progreso significativo en la interconexión de dispositivos y la generación de datos. Con el tiempo, ha evolucionado hacia la integración de tecnologías más avanzadas, como la inteligencia artificial y el aprendizaje automático, permitiendo un procesamiento de datos más sofisticado y la toma de decisiones automatizada. El concepto surge por primera vez de la mano de Kevin Anston en el año 1999, donde investigaba principalmente el uso de las tecnologías RFID (Radio Frequency

Identification), donde describia una vision donde los ordenadores fueran capaces de recopilar datos sin ayuda humana y conviertan esta información en una utilidad para los usuarios por medio de sensores y RFID, es decir que los ordenadores posean la habilidad de observar, identificar y comprender.

El Internet de las Cosas (IoT) representa una fase avanzada en la evolución de la red mundial, que tuvo sus inicios como el Internet de las Computadoras. Inicialmente, se estableció una red global con servicios como la World Wide Web (WWW), que contribuyó a la popularización del Internet y estimuló el rápido desarrollo de la Web de las Cosas (WoT). En los últimos años, hemos observado la transformación hacia un Internet de las Personas, dando origen a conceptos como la Social Web (Web 2.0), donde el contenido es generado y consumido por personas interconectadas. Este cambio se ha manifestado claramente mediante el crecimiento exponencial de los servicios de redes sociales, en conjunto con la explosiva expansión del acceso a Internet móvil y las aplicaciones móviles, evidenciando una madurez significativa en la evolución de Internet, marcando así la siguiente etapa.

2.3.3 Aplicaciones de IoT en entornos residenciales para la seguridad.

La tecnología IoT (Internet de las cosas) en los últimos años se ha convertido en una herramienta valiosa para mejorar la seguridad en los hogares como se observa en la Figura 4, existen aplicaciones de IoT en entornos residenciales para la seguridad que incluyen:
Sistemas de vigilancia: Los dispositivos de seguridad como las cámaras de seguridad inteligentes pueden detectar movimientos sospechosos y enviar alertas a los propietarios de viviendas e incluso pueden grabar videos y imagénes para luego puede ser revisados y analizados.

- **Sistemas de alarma:** La instrumentación como los sensores de movimiento, sensores electromagnéticos y detectoreses de humo inteligente que pueden detectar incendios, humo y otros peligros en el hogar y enviar alertas a los popiedarios.
- **Sistemas de monitoreo de agua**. Los sensores de agua inteligente pueden detectar fuga agua y enviar alertas a los propietarios.

- **Sistemas de monitoreo de energía eléctrica**. Medidores de consumo eléctrico inteligente capaces de enviar información de consumo energético excesivo. (Associations, 2023)

Figura 2. 4. Aplicaciones de IoT en entornos residenciales para la seguridad.

Nota. Sistema de seguridad Asistida. Home Security, (Associations, 2023)

2.4 Sistemas Complementarios para Automatizaciones y Control (SAAC)

La comunicación aumentativa y alternativa está compuesta por todas las modalidades de comunicación, aparte del habla, que son utilizadas para comunicar y expresar tanto necesidades como pensamientos o ideas y deseos. El sistema (SAAC) todos los seres humanos lo utilizarnos en el día a día, es decir, cuando usamos gestos, expresiones faciales, símbolos, escritura e incluso dibujos. (Chaparro Misó, 2021).

Quienes necesitan este recurso disponen de diferentes métodos de comunicación, ya que se pueden dividir en sistemas asistidos y no asistidos.

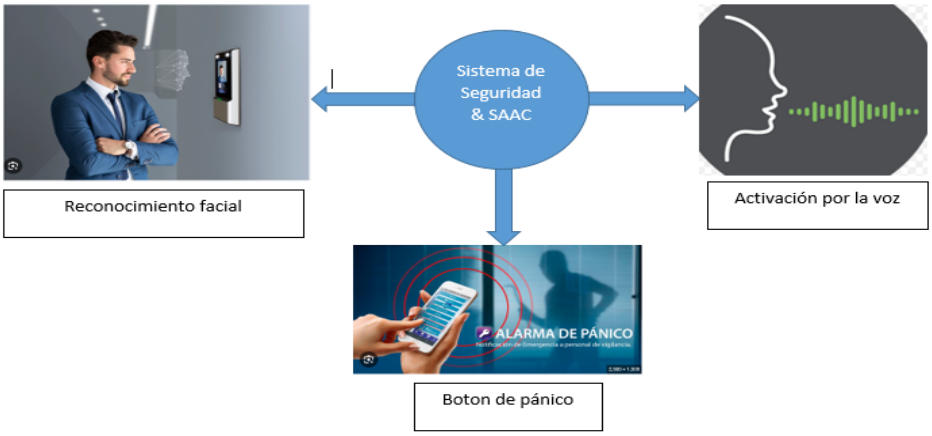
Los sistemas sin ayuda, también conocidos como sistemas de comunicación no asistidos, utilizan códigos que no requieren ningún elemento físico fuera del remitente, como el habla o el lenguaje de señas. Por otro lado, encontramos sistemas auxiliares, los llamados de comunicación asistida, que requieren de un soporte físico independiente del emisor, como los sistemas jeroglíficos, que hacen referencia a un conjunto estructurado de códigos no fonéticos. (verde, 2017)

2.4.1 Características y funcionalidades de los SAAC

Para ello, es necesario considerar los factores que intervienen en el proceso de toma de decisiones en función de los propios factores de la persona como:

- Son los cognitivos (memoria, razonamiento, categorización),
- Motores (motricidad gruesa y fina, autonomía motora),
- Habilidades comunicativas del lenguaje (habilidades sociales), capacidades perceptivas.

Figura 2. 5. Interacción de los SAAC con la seguridad del hogar.

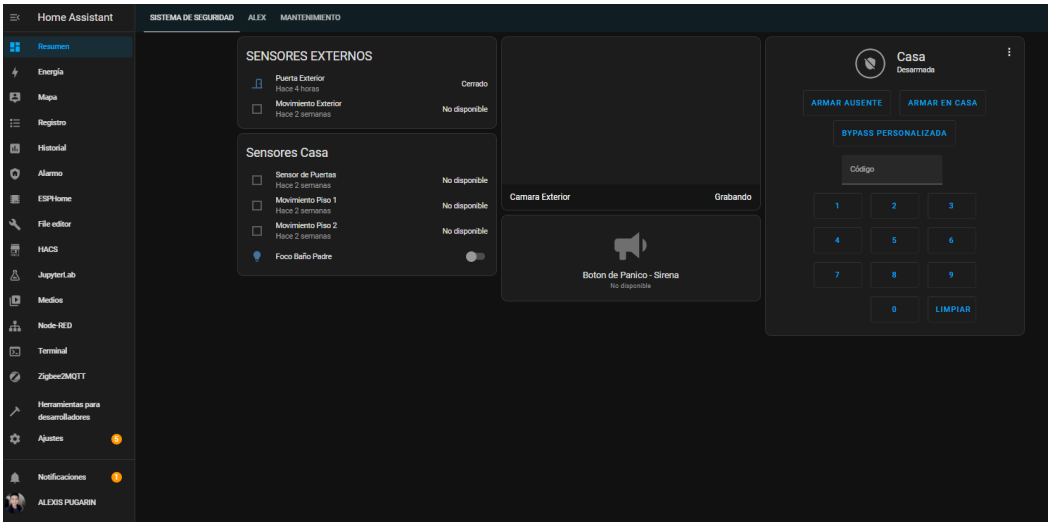


Nota. SAAC y la seguridad del hogar, Autor: Pugarin Alexis

2.5 Home Assistant como Plataforma de Automatización Residencial

Home Assistant es una plataforma de automatización del hogar de código abierto que permite a los usuarios controlar y monitorear dispositivos inteligentes en el hogar. (Home Assitant, 2023) Figura 6. Home Assistant se puede instalar en computadoras, servidores e incluso en Raspberry Pi 4. La plataforma proporciona una experiencia fácil de usar para configurar, actualizar y administrar dispositivos (Home Automation ideas, s.f.). Home Assistant también ofrece varias integraciones integradas que abstraen tipos de dispositivos como luces, interruptores, tapas, unidades climáticas y más. Los usuarios pueden crear sus propias integraciones personalizadas utilizando Authoring Platform 4.

Figura 2. 6. Plataforma Home Assistant



Nota. Interfaz gráfica Home Assistant, Autor: Pugarin Alexis

2.5.1 Características y Funcionalidades de Home Assistant

Home Assistant también ofrece muchas funciones y opciones, que incluyen:

- Automatización avanzada

Automatización avanzada: Home Assistant provee un programa de automatización avanzado que permite a los usuarios crear automatizaciones personalizadas para hasta 25 de sus dispositivos. Los usuarios pueden crear automatización basada en eventos como la hora del día, la ubicación del usuario o el estado del dispositivo (Comapanion Apps, 2024).

- Integración de servicios

Home Assistant se integra con múltiples servicios como Amazon Alexa, Google Assistant, IFTTT, Philips Hue, Nest, SmartThings, etc. Los usuarios pueden controlar sus dispositivos mediante comandos de voz o aplicaciones móviles que hoy en día es de fácil acceso y uso.

- Personalización

Home Assistant facilita a los usuarios personalizar la interfaz de usuario y crear paneles de control acorde a las necesidades y de fácil acceso la supervisón i/o control de sus dispositivos. Los usuarios pueden crear paneles de control para dispositivos específicos o para una habitación completa (HMI).

- Seguridad

La plataforma Home Assistant ofrece una variedad de funciones de seguridad, como autenticación de dos factores, cifrado SSL/TLS y autenticación de dispositivo. Los usuarios también pueden configurar alertas de seguridad para recibir notificaciones cuando se detecte actividad sospechosa.

2.5.2 Integración de Home Assistant en el Contexto de Seguridad Residencial

Las personas invierten en sistemas de seguridad domésticos inteligentes para que sus hogares sean más inteligentes y seguros. Estas soluciones innovadoras brindan acceso sin llave a su casa y lo actualizan en tiempo real sobre su estado de seguridad. Las cerraduras digitales usan un pin o le permiten desbloquear la puerta a través de un teléfono.

2.6 Arquitectura de un Sistema IoT con SAAC

En la actualidad, muchos sistemas no abarcan a todos los usuarios, y en menor medida, encontramos sistemas que incorporan técnicas de compensación para garantizar la accesibilidad universal. Aunque estos sistemas más inclusivos tienden a ser más complejos, hay enfoques como la implementación de iconos que se traduzcan en información vocal o la activación de automatizaciones de manera no verbal para abordar esta necesidad.

La mayoría de los sistemas con SAAC no son perfectos y no han experimentado años de mejoras continuas, lo que limita su integración con otros sistemas. Sin embargo, esta situación crea una oportunidad para que nuevas personas ingresen a este mercado. La mejora constante de estos sistemas tiene el potencial de generar éxito y proporcionar ayuda significativa a aquellas personas que enfrentan dificultades para comunicar sus necesidades o deseos (Chaparro Misó, 2021).

Con esta solución, buscamos fusionar las ventajas de todas las soluciones previas en una única aplicación, con el objetivo de integrar a personas con problemas de accesibilidad en el ámbito de la tecnología IoT y facilitar el acceso a herramientas útiles, como los asistentes virtuales. Conforme aumenta el número de dispositivos conectados en un ecosistema de IoT, es esencial contar con una estrategia de gestión de dispositivos de IoT

para supervisar y controlar los dispositivos (SAAC) de IoT implementados, como se ilustra en la Figura 2.7.

Figura 2. 7. Gestión de dispositivos IoT: importancia, desafíos, soluciones

Nota: Aquitectura Golbal de un Sistema IoT & SACC (INTuz, 2022)

La tecnología tiene la capacidad de integrar diversos dispositivos electrónicos, permitiendo su comunicación y ofreciendo beneficios como la comodidad y la tranquilidad para los usuarios al simplificar la vida cotidiana. Por lo general, el desarrollo tecnológico implica la estructuración de redes para lograr eventos específicos. Sin embargo, cada sistema sigue un proceso detallado, el cual se describe en párrafos subsiguientes, delineando cada etapa que contribuye al funcionamiento del sistema.

En una arquitectura IoT, resulta crucial contar con dispositivos de entrada, como sensores y actuadores, que puedan comunicarse a través de protocolos de comunicación o conexiones cableadas. Estos elementos desempeñan la función de adquirir información y transmitirla a otro dispositivo o controlador maestro. La información recopilada se somete a un proceso de análisis, donde el controlador maestro la recibe directamente o, en algunos casos, a través de un nodo intermedio que facilita la comunicación. Se implementan medidas de seguridad en la red, como diversos métodos de cifrado, para proteger esta información. El controlador maestro asume la responsabilidad de interpretar los datos recibidos y toma decisiones para activar actuadores o ejecutar automatizaciones según sea necesario. Además, en la mayoría de los casos, se incorporan interfaces para la interacción del usuario con el sistema (Geeks Forge, 2019).

CAPITULO III

DISEÑO E IMPLEMENTACIÓN

3.1 Análisis del diseño del proyecto.

En este capítulo, se abordarán diversos temas relacionados con la creación de una arquitectura para el Internet de las Cosas. Se explorarán aspectos como el diseño, los recursos y los procesos esenciales, incluida la programación necesaria para establecer una comunicación efectiva entre dispositivos encargados de la acción e intercambio de información. Se hará hincapié en el uso de una plataforma de gestión centralizada, la cual asumirá la responsabilidad de supervisar y coordinar los distintos procesos relacionados con la domótica y las automatizaciones implementadas.

Se contemplará la posibilidad de escalabilidad a lo largo del tiempo, considerando la incorporación progresiva de Hardware y Software especializado. Además, se examinará cómo esta arquitectura puede ser aplicada en entornos residenciales, sometiéndola a validación en un ambiente controlado. Se busca implementar y desarrollar un sistema funcional, aplicable en cualquier hogar que demuestre su eficacia en la gestión para la seguridad en el hogar.

3.1.1 Descripción del Sistema y Desarrollo del prototipo

Un sistema de seguridad basado en el Internet de las Cosas (IoT) tiene como objetivo la detección de intrusiones no autorizadas y permitir la activación de medidas de emergencia en respuesta a tales intrusiones, notificar a los usuarios en tiempo real para que puedan gestionar el sistema y permita la toma de decisiones tanto de manera local como remota. Para implementar este sistema, es necesario incorporar una variedad de sensores, destacando que estos permiten la detección de presencia e irrupción en un área controlada.

Se implementaron sensores de movimiento para corroborar la presencia de individuos a una distancia determinada del mismo, además se incorporarán sensores magnéticos para identificar cuando una puerta o ventana se apertura o se cierra. La inclusión de cámaras de seguridad es crucial para la monitorización, la cual envía una notificación al usuario

en caso de intrusiones no deseadas durante un horario predefinido, con la capacidad de activar acciones secundarias, como la activación de una sirena, generando una alarma sonora para las personas y las residencias cercanas.

Estos dispositivos de distintos fabricantes se integrarán en un sistema embebido, junto con un sistema operativo de código abierto conocido como Home Assistant. Esta integración permitirá gestionar todos los elementos de seguridad localmente y con posibilidad de ser controlada de manera remota, asegurando la integridad de los usuarios y sus propiedades, al mismo tiempo que previene posibles incidentes futuros.

3.2 Funcionamiento del sistema

El sistema IoT diseñado para la gestión de seguridad del hogar con SAAC (Sistemas Aumentativos y Alternativos de Comunicación), ejecuta una Raspberry Pi 4 como el elemento principal de hardware, el cual albergará el sistema operativo Home Assistant, como software principal y controlador maestro del sistema. Este enfoque proporciona un control total sobre la domótica y las automatizaciones destinadas al hogar. Además, este sistema es escalable según las preferencias del usuario, permitiendo la integración de diversos dispositivos de diferentes marcas y funciones, permitiendo su operación simultánea de manera local.

Para la instalación del software, se presentan diferentes opciones de instalación desde su página web. Uno de ellos es Home Assistant Operating System, una opción sencilla que incorpora un supervisor para facilitar la gestión del sistema, detectar errores y abordar su solución. Este método será utilizado en nuestro sistema de seguridad. Además, existen tres métodos de instalación avanzados destinados a desarrolladores o aquellos que requieren funciones específicas.

En cuanto a las automatizaciones implementadas por el administrador, se componen de un disparador y una acción, con la opción de incluir una condición, por lo que se destaca que el sistema de seguridad incorpora tres modalidades de administración destinadas al usuario del sistema.

El administrador posee un acceso completo a todas las funciones y configuraciones del sistema, otorgándole la capacidad de añadir, modificar o eliminar dispositivos y configuraciones. Además, tiene la facultad de gestionar los permisos concedidos a otros usuarios. El usuario podrá gestionar la interfaz designada por el administrador, la cual le permite controlar funciones específicas de los dispositivos, limitando el acceso a modificaciones en la configuración del sistema. Los invitados, por último, cuentan con permisos altamente restringidos, centrándose únicamente en proporcionar información permitida del sistema.

El usuario podrá acceder al sistema mediante un teléfono inteligente o una página web, donde dispondrá de un panel de control, ya sea para activar la vista previa de la cámara de seguridad o activar el botón de pánico, entre otras funciones, incorporando iconos de fácil reconocimiento para su accionar en caso de emergencia o de armar el sistema de seguridad, cabe mencionar que el sistema implementará un código PIN, mediante el cual se podrá activar o desactivar el armado del sistema.

El sistema ofrece tres métodos distintos de armado: "Armar Ausente", que activa el sistema y todos los dispositivos de control tanto internos como externos del hogar; "Armar en Casa", que activa el sistema pero excluye los dispositivos de control internos del hogar, dejando operativos solo los dispositivos externos; y el "Bypass Personalizada", que permite la activación del sistema incluso cuando hay dispositivos de control inactivos, excluyéndolos y habilitando el resto de los dispositivos para la activación del sistema de seguridad.

Tabla 3. 1. Tabla indicativa de estado del sistema de seguridad.

SISTEMA DE SEGURIDAD			
	Armar Ausente	Armar en Casa	Bypass Personalizada
Sensor magnético puerta exterior	✓	✓	✓✗
Sensor de movimiento puerta exterior	✓	✓	✓✗
Sensores de puertas y ventanas del hogar	✓	✓	✓✗
Sensor de movimiento del comedor	✓	✗	✓✗
Sensor de movimiento gradas piso 1	✓	✗	✓✗
Sensor de movimiento gradas piso 2	✓	✗	✓✗
Cámara de seguridad	✓	✓	✓✗
Botón de pánico	✓	✓	✓✗

Nota. Tabla de sensores en los diferentes modos de armado, Autor: Pugarin Alexis

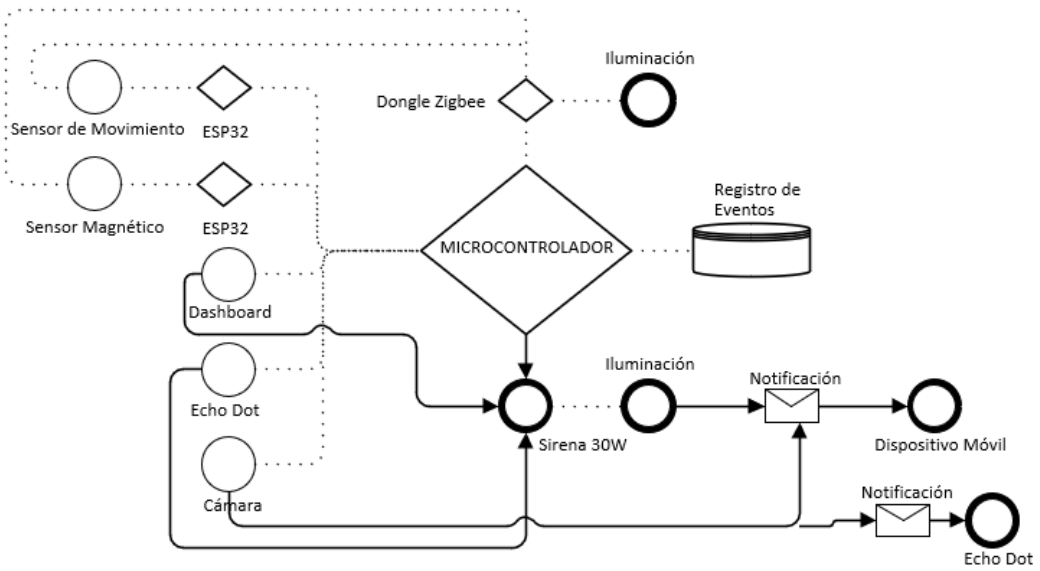
Cuando el sistema se seguridad se encuentra activado, según el modo de armando preferencia representado en la tabla 3.1 y exista una violación al sistema por una intrusión no deseada, se activarán medidas disuasivas, como una iluminación de advertencia y una alarma sonora en el exterior. En el interior del hogar se escuchará un mensaje audible en parlantes inteligentes y notificaciones “push” enviadas a dispositivos móviles vinculados al sistema.

3.3 Diagrama de flujo del sistema

En la figura 3.1 se presenta el diagrama de flujo del del sistema, en cual se detalla el funcionamiento del sistema de seguridad, donde se denotan las diferentes fases del sistema, detallando los procesos de comunicación, control y acción que se llevan a cabo.

La propuesta para el sistema de seguridad se fundamenta en una estructura centralizada que involucra diversos dispositivos y protocolos de comunicación. Para la implementación, se empleó una tarjeta Raspberry Pi 4 como el componente principal de hardware, sobre el cual se instaló el sistema operativo Home Assistant. Este sistema operativo desempeña el papel de software maestro en la configuración, facilitando la integración simultánea de varios dispositivos y posibilitando la creación de automatizaciones que serán ejecutadas por nuestro sistema operativo.

Figura 3. 1. Diagrama de flujo del funcionamiento del sistema



Nota. Diagrama de flujo del sistema, Autor: Pugarin Alexis

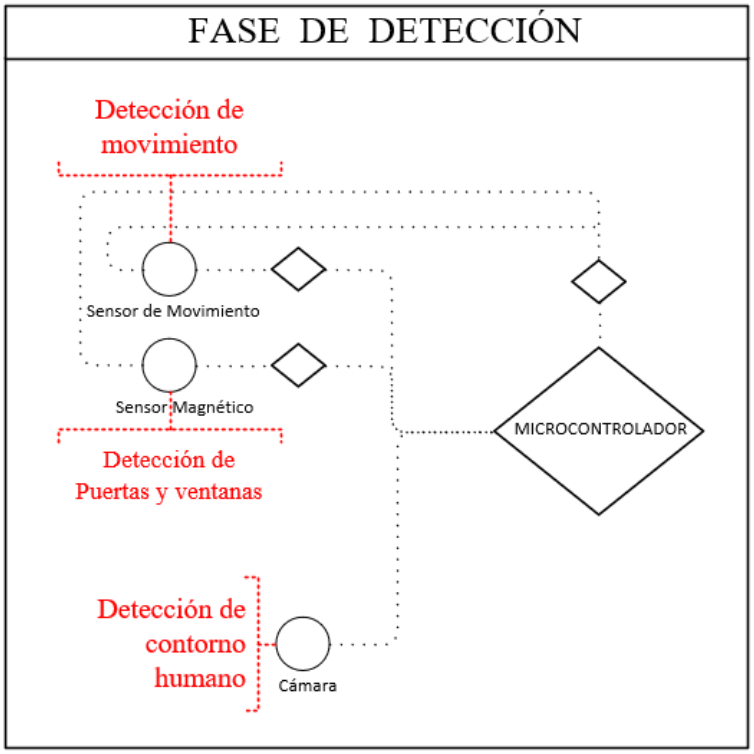
3.3.1 Fase de detección

En la figura 3.2 se presenta la fase de detección, el cual es fundamental en un sistema de seguridad, para adquirir información o detectar eventos que pudieran indicar amenazas o un cambio en un ambiente controlado, estos cambios en el entorno proporcionan los medios para que procesos posteriores se realicen a partir de esta primera etapa.

3.3.1.1 Recopilación de datos

El sistema de seguridad está dotado de dispositivos de entrada que incluyen sensores de movimiento, sensores magnéticos y cámaras. Cada uno de estos dispositivos recopila información específica según su función en el sistema de seguridad. La obtención de esta información se realiza a partir del estado del entorno y de las variaciones que puedan ocurrir en un ambiente controlado, la obtención de esta información se realiza a partir del estado del entorno o de los eventos que pueda suceder en un ambiente controlado.

Figura 3. 2. Fase de detección



Nota. Fase de detección del sistema, Autor: Pugarin Alexis

3.3.1.2 Detección de movimiento

La detección de movimiento está conformada por un sensor de movimiento para exterior, que se especializa en funciones específicas como tecnologías microwave, medición de radiación infrarroja y anti mascotas, que reducen significativamente el riesgo de falsas alarmas en el exterior, además se introducen sensores PIR para el interior del hogar que solo optan por la medición IR, para entornos controlados.

3.3.1.3 Detección de Puertas y ventanas

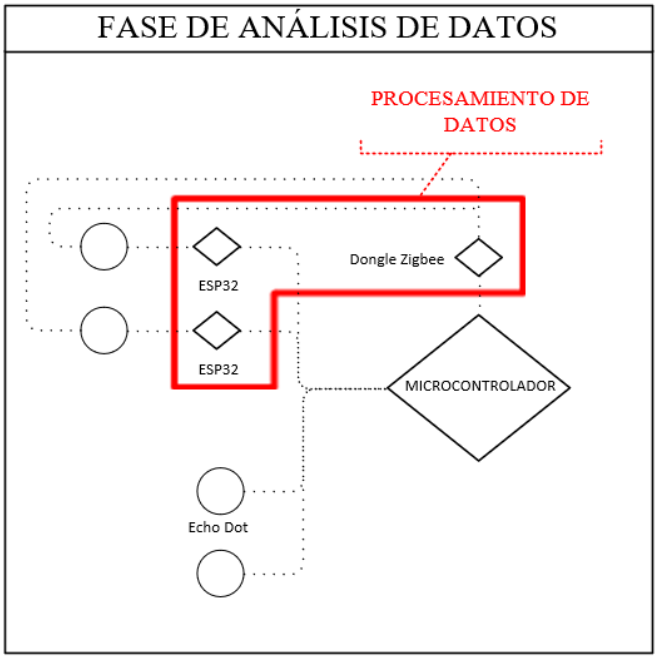
Para un sistema de seguridad, resulta esencial mantener un monitoreo o detección constante de los accesos al interior de la residencia, es decir puertas y ventanas. Es por ello que se incorporan sensores magnéticos, los cuales tienen la función de identificar el estado de apertura o cierre de puertas y ventanas, con el fin de asegurar todos los puntos de acceso a la residencia cuando el sistema se encuentre armado, contribuyendo así a prevenir intrusiones no autorizadas.

3.3.1.4 Detección de contorno humano

En el diseño de un sistema de seguridad para una vivienda, es necesario implementar cámaras de seguridad que lejos de ser un disuasivo por sí mismas contra posibles intrusiones, otorgan funciones esenciales como la capacidad de verificar el estado de la residencia en cualquier momento, ya sea de forma local o remota otorgando tranquilidad a los propietarios cuando no se encuentren en la residencia, además esta implementa una detección de contorno humano para activar el sistema en caso de una intrusión no deseada.

3.3.2 Fase de análisis de datos

Figura 3. 3. Fase de análisis de datos



Nota. Fase de análisis de datos del sistema, Autor: Pugarin Alexis

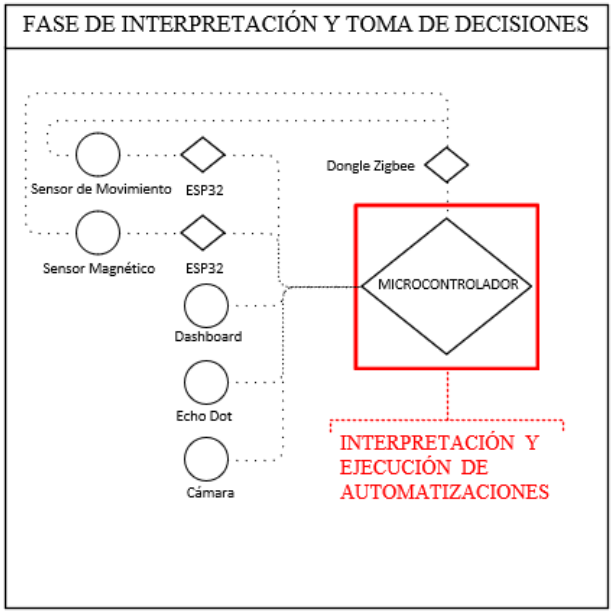
3.3.2.1 Procesamiento de datos

En la figura 3.3, podemos denotar que una vez que la información es capturada mediante los dispositivos de entrada, es necesario procesar y convertir estos datos en formatos comprensibles para el sistema. Luego, se lleva a cabo una interconexión mediante diversos protocolos de comunicación, ya sean cableadas o inalámbricas, como Wi-Fi, Zigbee, Z-Wave, entre otros. Es importante señalar que algunos dispositivos, al ser cableados se vinculan a un microcontrolador (Esp32), que actúa como nodo para procesar la información y transmitirla al controlador principal.

3.3.3 Fase de interpretación y toma de decisiones

En presencia de cualquier variación o alteración en el entorno de un ambiente controlado, los dispositivos de entrada envían información utilizando los métodos previamente mencionados hacia la Raspberry Pi 4 o microcontrolador denotado en la figura 3.4, que conjuntamente con el software Home Assistant, cumplen la función de controlador maestro del sistema de seguridad. Este controlador interpreta y analiza la información recibida, y dependiendo de esta, el sistema de seguridad activará las automatizaciones asociadas a esta información específica o proporcionará información relevante al usuario para facilitar la toma de decisiones inmediatas.

Figura 3. 4. Fase de interpretación y toma de decisiones

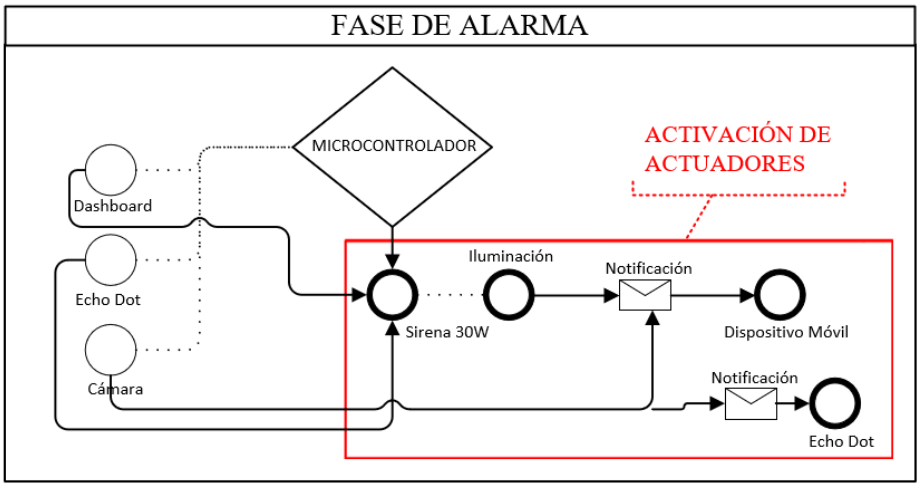


Nota. Fase de interpretación y toma de decisiones del sistema, Autor: Pugarin Alexis

3.3.4 Fase de alarma

Una intrusión desencadenará una serie de acciones automatizadas en el sistema, conocida como la fase de alarma que está constituida por una gran cantidad de elementos denotados en la Figura 3.5. Durante esta fase, se activará una sirena audible simultáneamente con luces intermitentes u otras señales visuales, proporcionando alertas visuales para informar a las personas cercanas a la residencia sobre la posible amenaza. Además, se enviarán alertas instantáneas a los dispositivos móviles conectados al sistema, como teléfonos inteligentes o tabletas, notificando la detección de eventos de seguridad. Como medida adicional, se emitirá un mensaje audible a través de parlantes inteligentes ubicados en el interior del hogar, brindando información y orientación a los residentes de la residencia. Este enfoque integral busca no solo alertar sobre la intrusión, sino también proporcionar una respuesta inmediata y efectiva para disuadir y tomar medidas emergentes para proteger el hogar y a sus ocupantes.

Figura 3. 5. Fase de Alarma



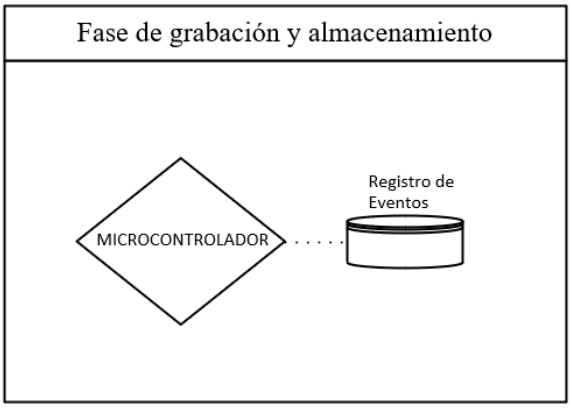
Nota. Fase de alarma, Autor: Pugarin Alexis

3.3.5 Fase de grabación y almacenamiento

En la Figura 3.6 se representa la fase de Grabación y Almacenamiento en un sistema de seguridad, que conlleva la captura y conservación de datos significativos provenientes de eventos del sistema, que puedan representar amenazas o situaciones de riesgo. El sistema se encarga de almacenar de manera segura y accesible esta información en un medio de almacenamiento específico dentro del software del controlador principal. Esta fase permite tener un registro de los eventos de seguridad, proporcionando un registro

histórico que contribuye a la toma de decisiones a largo o corto plazo, para optimizar el sistema de seguridad.

Figura 3. 6. Fase de grabación y almacenamiento



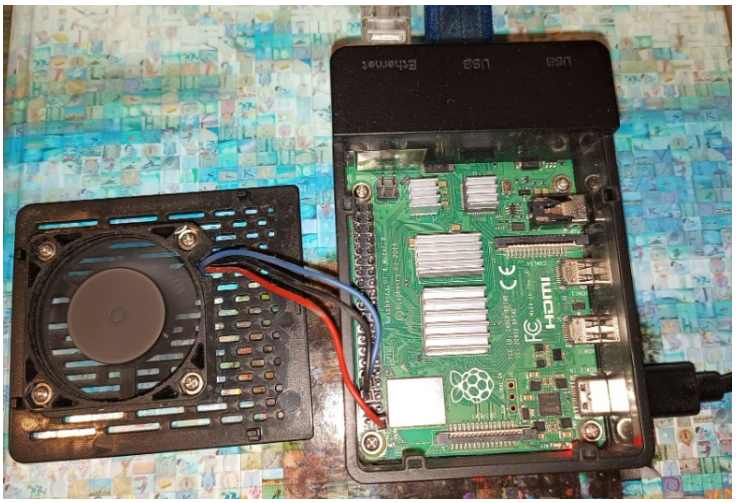
Nota. Fase de almacenamiento, Autor: Pugarin Alexis

3.4 Diseño Electrónico

3.4.1 Unidad central

En el sistema de seguridad se tomó la decisión de introducir una Raspberry Pi 4 que se presenta como un miniordenador con hardware potente, pequeño y de bajo consumo, logrando ser implementada en proyectos relacionados con el Internet de las Cosas (IoT), haciéndolo perfecto para el desarrollo de este proyecto de seguridad como controlador maestro, ya que incluye dispositivos de entrada y salida, así como características físicas que lo convierten en una opción ideal para recibir y transmitir información mediante diversos protocolos de comunicación, facilitando la conexión de sensores, controladores y actuadores, permitiendo gestionar procesos en simultaneo o paralelamente.

Figura 3. 7. Unidad Central



Nota. Raspberry Pi 4, Autor: Pugarin Alexis

Para lograr realizar automatizaciones o procesos de gestión es necesario descargar una imagen del sistema en una tarjeta micro SD, la cual se inserta en el hardware y posteriormente, se procede a la instalación del software Home Assistant, que actuará como sistema operativo y controlador principal del sistema de seguridad. El objetivo es permitir que este software y hardware posibiliten la integración y automatización eficiente de todos los nodos y dispositivos asociados al sistema.

3.4.2 Sistema sensor, controlador y actuador (SCA)

3.4.2.1 Sensores del sistema

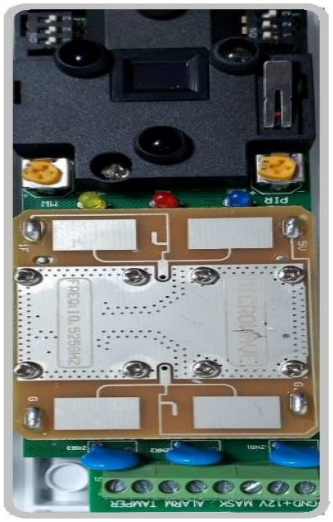
El sistema presenta en su arquitectura tres tipos diferentes de sensores de movimiento, el primero de ellos que se utilizo es un sensor de movimiento cableado, para interior de marca teclam de modelo PIR100PT como se observa en la figura 3.8, siendo este un sensor tradicional con una sensibilidad previamente establecida por el fabricante y sin opción a modificarla ideal para zonas controladas.

Figura 3. 8. Sensor de Movimiento cableado

Nota. PIR100PT, Autor: Pugarin Alexis

Se eligió implementar el sensor de movimiento para exterior PIR-126MWA denotado en la figura 3.9, para supervisar un área al aire libre, dado que este sensor está diseñado con características específicas para entornos exteriores, lo que ayuda a evitar falsos positivos. Este dispositivo se convierte en una herramienta de control efectiva, especialmente en lugares como patios o garajes, donde puede desempeñar un papel beneficioso.

Figura 3. 9. Sensor de movimiento exterior



Nota. PIR-126MWA, Autor: Pugarin Alexis

Se implementó un sensor de movimiento inalámbrico de la maraca Aqara denotado en la figura 3.10, de modelo P1 con tecnología ZigBee 3.0 que permite ajustar los parámetros de sensibilidad, tiempo de detección e incluye un campo de visión más amplio. Este tipo de sensores serán implementados en ambientes controlados para cubrir áreas como los ingresos principales, facilitando la instalación de estos en zonas específicas.

Figura 3. 10. Sensor de movimiento Aqara

Nota. Aqara P1, Autor: Pugarin Alexis

Se implementan sensores magnéticos cableado s de marca Teclam denotados en la figura 3.11, en puertas y ventanas del hogar con el fin de garantizar que no exista una irrupción no deseada por estos espacios vulnerables, algunos de estos sensores están conectados en serie cubriendo las puertas de ingreso al hogar, es decir que supervisan múltiples ubicaciones en una misma zona.

Figura 3. 11. Sensor de magnético

Nota. Sensor de magnético Teclam, Autor: Pugarin Alexis

El ultimo dispositivo que se implementó es una cámara de seguridad de la marca EZVIZ con modelo CS- C3TN denotada en la figura 3.12, esta permite visualizar el entorno del hogar en tiempo real e implementa una detección de contorno humano que establecido en un horario especifico, la cámara puede detectar una intrusión no deseada y gracias a su integración en Home Assistant por medio del protocolo de comunicación RTSP (Protocolo de transmisión en tiempo real), activar los actuadores de alarma del sistema.

Figura 3. 12. Cámara de seguridad

Nota. EZVIZ CS- C3TN, Autor: Pugarin Alexis

3.4.2.2 Controladores del sistema

En el sistema de seguridad, se utilizan algunos dispositivos de entrada que son cableados, como sensores de movimiento, magnéticos y al cambiar de estado, establecen una transmisión y recepción de datos, por lo que se realiza una interconexión física entre los pines de transmisión del sensor hasta los pines designados del microcontrolador ESP32 denotado en la figura 3.13, para posteriormente programar este microcontrolador para que lea la información proveniente desde los sensores y la transmita a través de una conexión wifi a la red doméstica, lo cual da apertura a integrar y gestionar la información con el software de Home Assistant y utilizando este microcontrolador como nodo entre el sensor y la unidad central.

Figura 3. 13. Nodo del sistema

Nota. Esp32, Autor: Pugarin Alexis

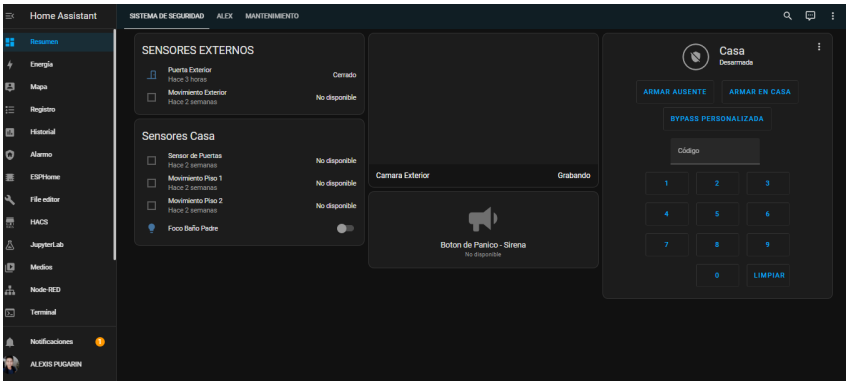
El sistema cuenta con dispositivos de entrada que utilizan el protocolo de comunicación inalámbrica ZigBee como sensores de movimiento, magnéticos e iluminación y es obligatorio utilizar un coordinador denotado en la figura 3.14 que actúa como nodo entre el sensor y la unidad central, por lo cual implementamos el coordinador universal de la marca Sonoff Zigbee 3.0 Dongle Plus. Este dispositivo puede utilizar los protocolos ZHA o Zigbee2MQTT para crear una red mesh de dispositivos para nuestro sistema de seguridad. En consecuencia, solo es necesario conectarlo a una Raspberry Pi 4 a través de uno de sus puertos USB y realizar la integración adecuada con el controlador maestro.

Figura 3. 14. Coordinador zegbee

Nota. Sonoff Zigbee 3.0 Dongle Plus, Autor: Pugarin Alexis

Finalmente se implementa un dashboard denotado en la figura 3.15, para la gestión del sistema de seguridad para los usuarios, contiene iconos accionables de fácil acceso para suplir una posible dificultad en su capacidad de comunicación, además se implementa un parlante inteligente echo dot de la marca de Amazon, estos dispositivos dispondrán de funciones como activación del sistema de seguridad y botón de pánico.

Figura 3. 15. Home Assistant application



Nota. Samsung Tab A, Autor: Pugarin Alexis

3.4.2.3 Actuadores del sistema

El sistema de seguridad implementa 3 tipos de actuadores en caso de una intrusión no deseada, cuando el sistema de seguridad se encuentre armado. Se implemento iluminación para disuadir en un horario nocturno y una sirena audible denotada en la figura 3.16 que cubre una distancia aproximada de 40 metros, además de contar con la cámara de seguridad que implementa una defensa activa de luz y sirena propias del dispositivo, mencionada con anterioridad.

Figura 3. 16. Sirena

Nota. Sirena 30w DSC, Autor: Pugarin Alexis

3.4.3 Escenario y transcurso de la prueba

El sistema IoT con SAAC para la automatización de seguridad en el hogar, se instaló en la residencia de la señora Elsa Beatriz Díaz. Esta casa alberga a personas con edades comprendidas entre los 5 y 70 años. Por consiguiente, se implementó un sistema de seguridad que incorpore métodos aumentativos y alternativos, especialmente diseñados para aquellos usuarios que puedan tener dificultades para expresar sus necesidades o deseos de manera verbal. Este escenario incluye situaciones donde los residentes pueden enfrentar problemas de vocalización o incluso perder la capacidad de hablar debido a diversos motivos, como accidentes o enfermedades.

Se llevó a cabo un análisis detallado del entorno y las áreas en la residencia de la señora Elsa Beatriz Díaz para identificar zonas vulnerables. Estas áreas se categorizaron como ambientes controlados o no controlados, y se introdujeron dispositivos específicos para monitorear cada zona vulnerable. A continuación, se proporciona una descripción detallada de los lugares donde se instaló los dispositivos de entrada para el monitoreo de la seguridad en el hogar.

3.4.3.1 Exterior de la residencia

En la parte externa de la residencia se identificó dos posibles formas de vulnerar la seguridad del hogar. La primera implica la manipulación forzada de la cerradura para acceder a la vivienda, mientras que la segunda involucra escalar el muro como método para ingresar denotadas en la figura 3.17. Por lo tanto, esta área se categoriza como un ambiente no controlado.

Figura 3. 17. Residencia parte exterior

Nota. Exterior de la residencia, Autor: Pugarin Alexis

Para abordar las vulnerabilidades identificadas, se ha instalado un sensor magnético inalámbrico con tecnología Zigbee. Este dispositivo está diseñado para monitorear el estado de apertura o cierre de la puerta principal que conduce al interior de la residencia denotado en la figura 3.18.

Figura 3. 18. Residencia, puerta ingreso

Nota. Puerta de ingreso principal, Autor: Pugarin Alexis

Para prevenir la intrusión mediante la escalada de paredes hacia el interior de la residencia, se implementa un sistema de seguridad que consta de una cámara de vigilancia, un sensor de movimiento diseñado para exteriores y un sensor magnético conectado a la puerta principal denotados en la figura 3.19. Estos dispositivos tienen la función de identificar y reaccionar ante cualquier intento de intrusión, activando los mecanismos correspondientes para disuadir y notificar a los residentes, facilitando así la toma de decisiones inmediatas.

Figura 3. 19. Parte frontal de la residencia

Nota. Patio de la vivienda, Autor: Pugarin Alexis

En la parte posterior de la residencia, se colocan dos sensores magnéticos denotados en la figura 3.20, conectados por cable a las puertas para supervisar su estado de apertura en caso de una intrusión no autorizada, siempre y cuando el sistema de seguridad esté activado, monitoreando una posible vulneración en las puertas de ingreso al hogar.

Figura 3. 20. Parte posterior de la residencia

Nota. Patio de la vivienda, Autor: Pugarin Alexis

3.4.3.2 Interior de la residencia

En el interior de la vivienda, hemos identificado tres áreas críticas que requieren supervisión de presencia cuando no hay ocupantes en la residencia. Con el fin de prevenir intrusiones no autorizadas, se han instalado tres sensores de movimiento en ubicaciones estratégicas. Estos sensores actúan como dispositivos de entrada preventivos en caso de que se logre evadir los sensores mencionados anteriormente, activando los actuadores en respuesta a una posible intrusión. Por lo tanto, esta área interior se caracteriza como un entorno controlado.

3.4.3.3 Planta baja interior de la residencia

Estos sensores de movimiento abarcan el área correspondiente a la planta baja de la vivienda, con el propósito de identificar alguna intrusión que pueda ocurrir desde el exterior hacia el interior del hogar. Su cobertura incluye áreas críticas como la sala y el comedor denotadas en las figuras 3.21 y figura 3.22, que proporcionan el acceso a otras secciones de la residencia.

Figura 3. 21. Sala de estar de la vivienda

Nota. Planta baja de la residencia, Autor: Pugarin Alexis

Figura 3. 22. Comedor de la vivienda

Nota. Planta baja de la residencia, Autor: Pugarin Alexis

3.4.3.4 Planta alta interior de la residencia

El sensor de movimiento denotado en la figura 3.23 es un dispositivo cableado que cubre el área correspondiente a la planta alta de la residencia, con la finalidad de identificar posibles intrusiones provenientes del nivel inferior, cubriendo el acceso a las escaleras que conectan las distintas plantas de la residencia.

Figura 3. 23. Gradas de la planta alta

Nota. Planta Alta, Autor: Pugarin Alexis

CAPITULO IV
ANÁLISIS Y RESULTADOS

Se presentan los resultados adquiridos por medio de la experimentación en cuanto al funcionamiento o activación de sensores magnéticos, detección de presencia, sensores de movimiento aqara modelo P1 y detección de contorno humano mediante la cámara EZVIZ, las señales emitidas son registradas por el controlador Rasberry Pi 4 y almacenadas en el sistema Home Assistant. Toda la información registrada se considera como eventos por fecha de modo que se pueda tener un seguimiento de las zonas de mayor riesgo en cuanto a la violación del sistema de seguridad.

Es importante recalcar que en el proyecto se realizó algunos ajustes de configuración en cuanto a sensibilidad de los sensores y cámaras para tener una mejor respuesta en tiempo real y así lograr disuadir si algún evento no usual ocurre.

4.1 Recopilación de datos

4.1.1 Detección de sensores de la residencia

Como se puede observar en la tabla 4.1 muestra el registro de activación de cada dispositivo sensores inductivos, de movimiento y cámara por fecha como evento y así calibrar su sensibilidad.

Tabla 4. 1. Prueba de sensores residencia

PRUEBA DE INTEGRACIÓN Y ACTIVACIÓN – ACTUADORES						
Fecha	**Número de evento**	**Sensor magnético puerta exterior**	**Sensor de movimiento exterior**	**Cámara de seguridad exterior**	**Sensores magnéticos de puertas del hogar**	**Sensores de movimiento interiores**
20/10/2023	1	No	No	No	No	No
21/10/2023	2	No	No	No	No	No
22/10/2023	3	No	No	No	No	No
23/10/2023	4	No	No	No	No	No
24/10/2023	5	No	No	No	No	No
25/10/2023	6	No	No	No	No	No
26/10/2023	7	No	No	No	No	No
27/10/2023	8	No	Si	No	No	No
28/10/2023	9	No	Si	No	No	No
29/10/2023	10	Si	Si	Si	No	No
30/10/2023	11	Si	Si	Si	No	No
31/10/2023	12	Si	Si	Si	No	No
01/11/2023	13	Si	Si	Si	No	No
02/11/2023	14	Si	Si	No	No	No
03/11/2023	15	Si	No	No	No	No
04/11/2023	16	Si	No	No	No	Si
05/11/2023	17	Si	No	No	No	Si
06/11/2023	18	Si	No	No	No	Si
07/11/2023	19	No	No	No	No	Si
08/11/2023	20	No	No	No	Si	Si
09/11/2023	21	No	No	No	Si	Si
10/11/2023	22	No	No	No	Si	Si
11/11/2023	23	No	No	No	Si	Si
12/11/2023	24	No	No	No	Si	Si
13/11/2023	25	No	No	Si	Si	Si
14/11/2023	26	Si	No	Si	Si	Si
15/11/2023	27	Si	No	Si	Si	Si
16/11/2023	28	Si	No	Si	Si	Si
17/11/2023	29	Si	No	Si	Si	Si
18/11/2023	30	Si	No	Si	Si	Si
19/11/2023	31	Si	No	Si	Si	Si
20/11/2023	32	Si	No	Si	Si	Si
21/11/2023	33	Si	No	Si	Si	Si
22/11/2023	34	Si	No	Si	Si	Si
23/11/2023	35	Si	Si	Si	Si	Si
24/11/2023	36	Si	Si	Si	Si	Si
25/11/2023	37	Si	Si	Si	Si	Si
26/11/2023	38	Si	Si	Si	Si	Si
27/11/2023	39	Si	Si	Si	Si	Si
28/11/2023	40	Si	Si	Si	Si	Si
29/11/2023	41	Si	Si	Si	Si	Si
30/11/2023	42	Si	Si	Si	Si	Si
01/12/2023	43	Si	Si	Si	Si	Si
02/12/2023	44	Si	Si	Si	Si	Si
03/12/2023	45	Si	Si	Si	Si	Si
04/12/2023	46	Si	Si	Si	Si	Si
05/12/2023	47	Si	Si	Si	Si	Si
06/12/2023	48	Si	Si	Si	Si	Si
07/12/2023	49	Si	Si	Si	Si	Si
08/12/2023	50	Si	Si	Si	Si	Si

Nota. Tabla de pruebas de sensores, Autor: Pugarin Alexis

4.1.2 Detección de actuadores

Tabla 4. 2. Prueba de actuadores en la residencia

PRUEBA DE INTEGRACIÓN Y ACTIVACIÓN – ACTUADORES				
Fecha	**Número de evento**	**Sirena**	**Cámara de seguridad**	**Iluminación**
20/10/2023	1	No	No	No
21/10/2023	2	No	No	No
22/10/2023	3	No	No	No
23/10/2023	4	No	No	No
24/10/2023	5	No	No	No
25/10/2023	6	No	No	No
26/10/2023	7	No	No	No
27/10/2023	8	No	No	No
28/10/2023	9	No	No	No
29/10/2023	10	No	No	No
30/10/2023	11	Si	No	No
31/10/2023	12	Si	No	No
01/11/2023	13	Si	No	No
02/11/2023	14	Si	No	No
03/11/2023	15	Si	No	Si
04/11/2023	16	Si	No	Si
05/11/2023	17	Si	No	Si
06/11/2023	18	Si	No	Si
07/11/2023	19	Si	No	Si
08/11/2023	20	Si	No	Si
09/11/2023	21	Si	No	No
10/11/2023	22	Si	Si	No
11/11/2023	23	Si	Si	No
12/11/2023	24	Si	Si	No
13/11/2023	25	Si	Si	Si
14/11/2023	26	Si	Si	Si
15/11/2023	27	Si	No	Si
16/11/2023	28	Si	No	Si
17/11/2023	29	Si	No	Si
18/11/2023	30	Si	No	Si
19/11/2023	31	Si	No	Si
20/11/2023	32	Si	Si	Si
21/11/2023	33	Si	Si	Si
22/11/2023	34	Si	Si	Si
23/11/2023	35	Si	Si	Si
24/11/2023	36	Si	Si	Si
25/11/2023	37	Si	Si	Si
26/11/2023	38	Si	Si	Si
27/11/2023	39	Si	Si	Si
28/11/2023	40	Si	Si	Si
29/11/2023	41	Si	Si	Si
30/11/2023	42	Si	Si	Si
01/12/2023	43	Si	Si	Si
02/12/2023	44	Si	Si	Si
03/12/2023	45	Si	Si	Si
04/12/2023	46	Si	Si	Si
05/12/2023	47	Si	Si	Si
06/12/2023	48	Si	Si	Si
07/12/2023	49	Si	Si	Si
08/12/2023	50	Si	Si	Si

Nota. Tabla de pruebas de actuadores, Autor: Pugarin Alexis

4.1.3 Detección de notificaciones

Tabla 4. 3. Prueba de notificaciones a los usuarios

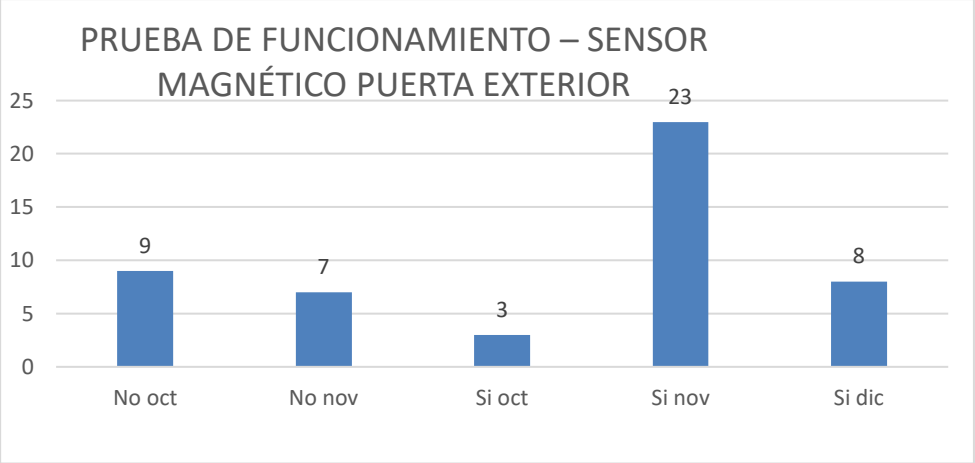
PRUEBA DE INTEGRACIÓN Y ACTIVACIÓN – NOTIFICACIONES					
Fecha	**Número de evento**	**Administrador**	**Usuario 1**	**Usuario 2**	**Invitado**
20/10/2023	1	No	No	No	No
21/10/2023	2	No	No	No	No
22/10/2023	3	No	No	No	No
23/10/2023	4	No	No	No	No
24/10/2023	5	No	No	No	No
25/10/2023	6	No	No	No	No
26/10/2023	7	No	No	No	No
27/10/2023	8	No	No	No	No
28/10/2023	9	Si	No	No	No
29/10/2023	10	Si	No	No	No
30/10/2023	11	Si	No	No	No
31/10/2023	12	Si	No	No	No
01/11/2023	13	Si	No	No	No
02/11/2023	14	Si	No	No	No
03/11/2023	15	Si	No	No	No
04/11/2023	16	Si	No	No	No
05/11/2023	17	Si	No	No	No
06/11/2023	18	Si	No	No	No
07/11/2023	19	Si	No	No	No
08/11/2023	20	Si	No	No	No
09/11/2023	21	Si	No	No	No
10/11/2023	22	Si	Si	Si	Si
11/11/2023	23	Si	Si	Si	Si
12/11/2023	24	Si	Si	Si	Si
13/11/2023	25	Si	Si	Si	Si
14/11/2023	26	Si	Si	Si	Si
15/11/2023	27	Si	Si	Si	Si
16/11/2023	28	Si	Si	Si	Si
17/11/2023	29	Si	Si	Si	Si
18/11/2023	30	Si	Si	Si	Si
19/11/2023	31	Si	Si	Si	Si
20/11/2023	32	Si	Si	Si	Si
21/11/2023	33	Si	Si	Si	Si
22/11/2023	34	Si	Si	Si	Si
23/11/2023	35	Si	Si	Si	Si
24/11/2023	36	Si	Si	Si	Si
25/11/2023	37	Si	Si	Si	Si
26/11/2023	38	Si	Si	Si	Si
27/11/2023	39	Si	Si	Si	Si
28/11/2023	40	Si	Si	Si	Si
29/11/2023	41	Si	Si	Si	Si
30/11/2023	42	Si	Si	Si	Si
01/12/2023	43	Si	Si	Si	Si
02/12/2023	44	Si	Si	Si	Si
03/12/2023	45	Si	Si	Si	Si
04/12/2023	46	Si	Si	Si	Si
05/12/2023	47	Si	Si	Si	Si
06/12/2023	48	Si	Si	Si	Si
07/12/2023	49	Si	Si	Si	Si
08/12/2023	50	Si	Si	Si	Si

Nota. Tabla de pruebas de notificaciones, Autor: Pugarin Alexis

4.2 Análisis de datos

4.2.1 Análisis de los sensores del hogar

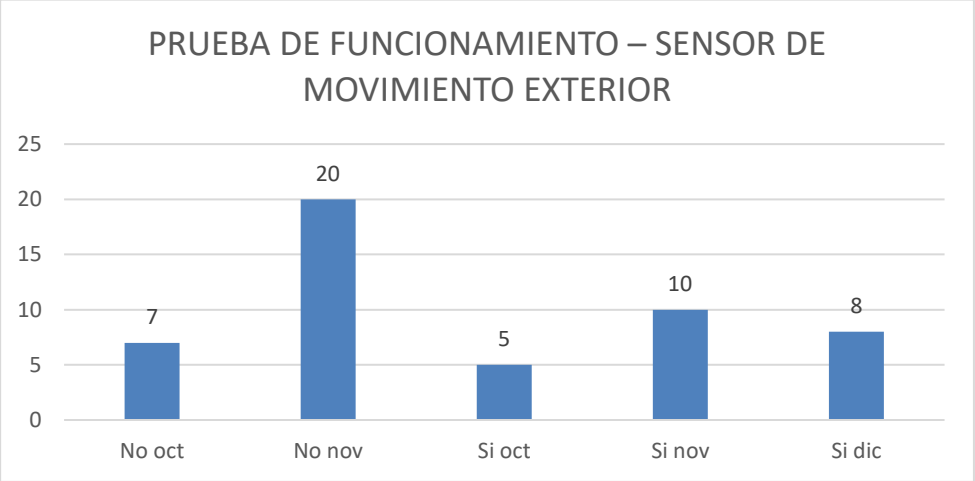
Figura 4. 1. Prueba de funcionamiento – sensor magnético puerta exterior



Nota. Análisis sensor magnético puerta exterior, Autor: Pugarin Alexis

En la figura 4.1 se detalla el funcionamiento del sensor magnético inalámbrico implementado en el exterior de la residencia, se observa un primer período, del 20 al 28 de octubre, durante el cual el dispositivo no operó debido a dificultades en su vinculación con el sistema. Posteriormente, se registra un período a fines de octubre, del 29 de octubre al 6 de noviembre, donde se logró la correcta vinculación del sensor al sistema, funcionando adecuadamente durante 9 días. Sin embargo, se identifica otro período de inactividad, del 7 al 13 de noviembre, en el que el dispositivo perdió la conexión con el sistema. Para abordar esta intermitente pérdida de señal, se tomó la medida de ampliar la red mesh. Finalmente, desde el 14 de noviembre al 8 de diciembre, el dispositivo opera de manera estable sin presentar inconvenientes futuros.

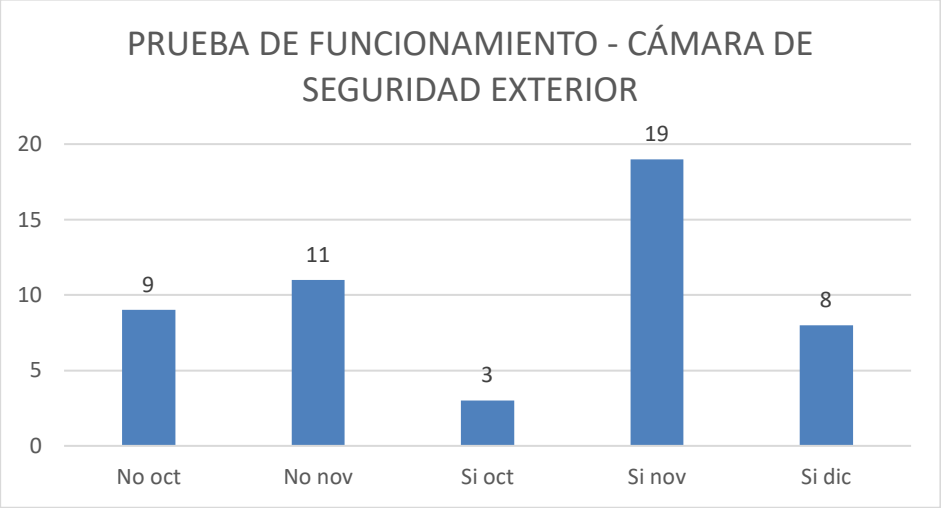
Figura 4. 2. Prueba de Funcionamiento - sensor de movimiento exterior



Nota. Análisis sensor de movimiento exterior, Autor: Pugarin Alexis

En la figura 4.2 se detalla el funcionamiento del sensor instalado para el exterior, donde se evidencia un primer período, del 20 al 26 de octubre, durante el cual el dispositivo no operó debido a dificultades en su vinculación con el sistema. Posteriormente, se registra un período a fines de octubre, del 27 de octubre al 2 de noviembre, donde se logró la correcta vinculación del sensor al sistema, funcionando adecuadamente durante 7 días. Sin embargo, se identifica otro período de inactividad, del 3 al 22 de noviembre, en el que el dispositivo presentó funcionamiento intermitente, generando falsos positivos, a pesar de los intentos de solucionarlos mediante ajustes físicos en la configuración del sensor. Ante esta situación, se optó por sustituir el dispositivo por uno de mejores prestaciones y, finalmente, desde el 23 de noviembre al 8 de diciembre, el sensor opera de manera estable y sin inconvenientes, superando estos errores para el sistema en el futuro.

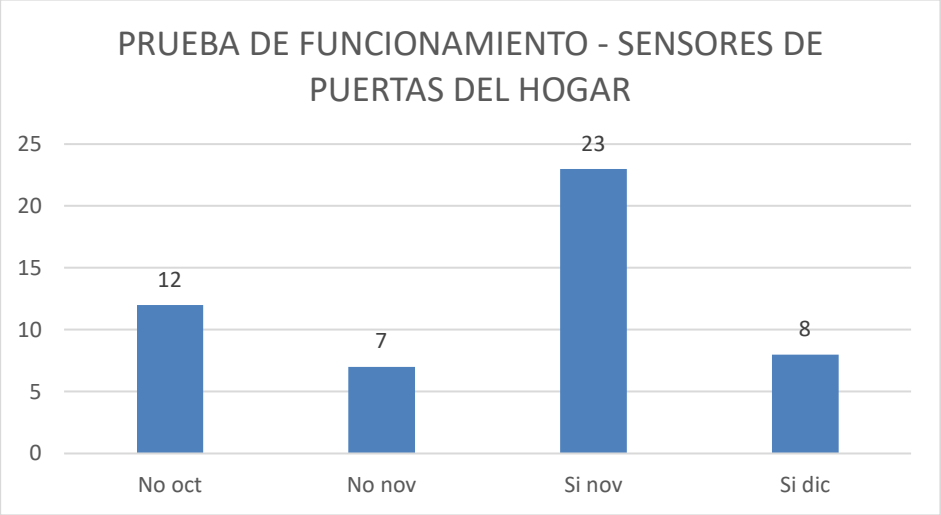
Figura 4. 3. Prueba de funcionamiento - cámara exterior



Nota. Análisis cámara exterior, Autor: Pugarin Alexis

En la figura 4.3 se detalla el funcionamiento de la cámara de seguridad implementada en el exterior de la residencia, donde se observa un período inicial, del 20 al 28 de octubre, durante el cual el dispositivo no operó debido a dificultades en su vinculación con el sistema. Posteriormente, se registra un período a fines de octubre, del 29 de octubre al 1 de noviembre, donde se logró la vinculación de la cámara al sistema, aunque funcionó de manera intermitente durante 4 días. Ante esto, se optó por desvincularla del sistema durante 11 días, período durante el cual se abordaron los inconvenientes accediendo a la configuración avanzada de la cámara y modificando sus parámetros para solventar errores de transmisión de video con el sistema. Finalmente, desde el 13 de noviembre al 8 de diciembre, la cámara de seguridad opera de manera correcta, estable y sin ningún problema, asegurando un funcionamiento sin contratiempos en el futuro.

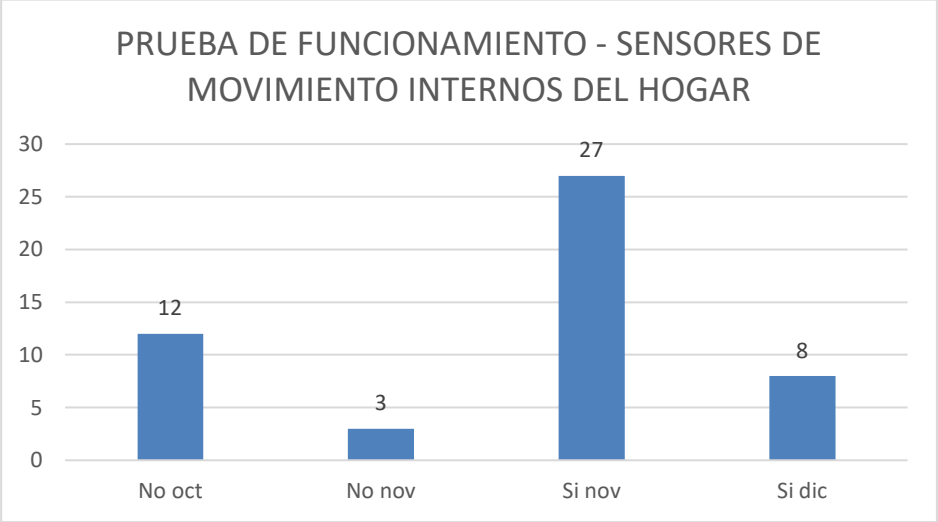
Figura 4. 4. Prueba de funcionamiento – sensores magnéticos puertas internas



Nota. Análisis de sensores magnéticos puertas internas, Autor: Pugarin Alexis

En la figura 4.4 se detalla la implementación de sensores magnéticos en las puertas internas de la residencia, donde se identifica un periodo inicial desde el 20 de octubre al 7 de noviembre, en el cual estos dispositivos, al estar cableados, presentaban un funcionamiento intermitente. Para abordar esta situación, se llevó a cabo una revisión minuciosa del cableado, la distancia y el amperaje, lo cual resultó crucial para corregir los falsos positivos que se estaban generando en el sistema. Finalmente, desde el 8 de noviembre al 8 de diciembre, se verifica el funcionamiento óptimo de estos sensores, solventando de manera efectiva las intermitencias en su operación.

Figura 4. 5. Prueba de funcionamiento - sensores de movimiento internos del hogar

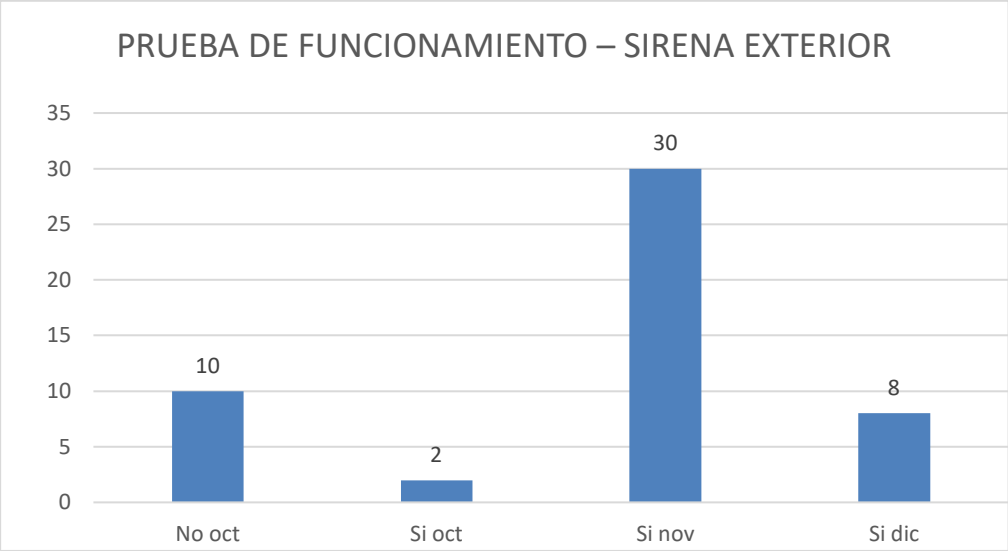


Nota. Análisis de sensores de movimiento internos del hogar, Autor: Pugarin Alexis

En la figura 4.5 se detalla el funcionamiento de sensores de movimiento en el interior de la residencia, donde se denota un periodo inicial que abarca desde el 20 de octubre al 3 de noviembre. Durante este lapso, se llevaron a cabo pruebas específicas de distancia de reconocimiento y ajustes en su funcionamiento para garantizar una cobertura efectiva de la zona y determinar los tiempos de detección adecuados para un desempeño óptimo en el sistema de seguridad. Finalmente, desde el 4 de noviembre al 8 de diciembre, se realizaron pruebas continuas para verificar la estabilidad de estos sensores, obteniendo como resultado un funcionamiento perfecto en la detección de movimiento en los pisos interiores del hogar.

4.2.2 Análisis de los actuadores del hogar

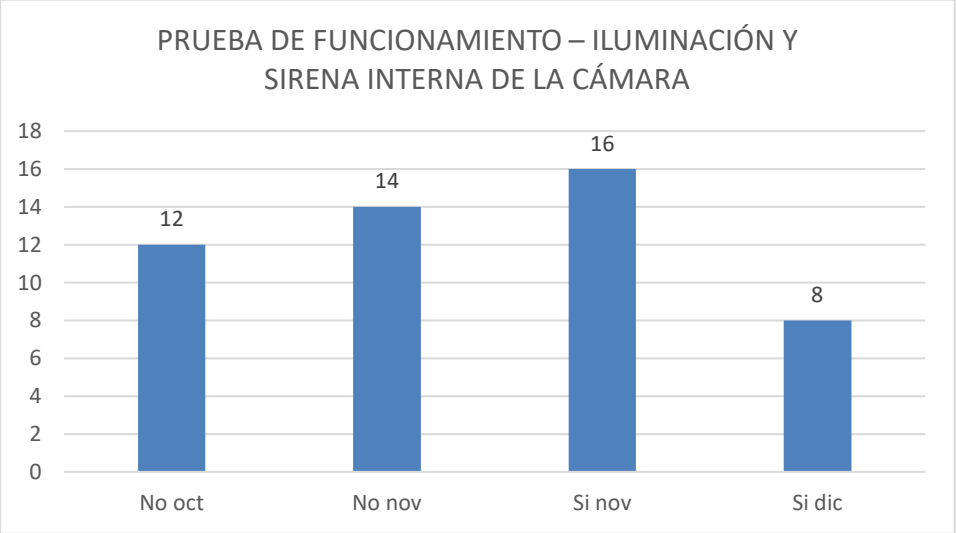
Figura 4. 6. Prueba de Funcionamiento - sirena



Nota. Análisis del actuador sirena exterior, Autor: Pugarin Alexis

En la figura 4.6 se detalla el funcionamiento de la sirena para exterior, se destaca un periodo inicial que abarca desde el 20 al 29 de octubre. Durante estos 10 días, se instaló en el exterior y se intentó incorporar a la automatización del sistema para activarse eficientemente ante cualquier intrusión no autorizada. Durante este periodo inicial, se registraron algunos falsos positivos. Finalmente, desde el 30 de octubre al 8 de diciembre, se logró integrar de manera adecuada al sistema de seguridad, asegurando un funcionamiento correcto en la activación de este actuador. Vale la pena señalar que las intermitencias en el funcionamiento se atribuyeron a la distancia a la cual se colocó este actuador.

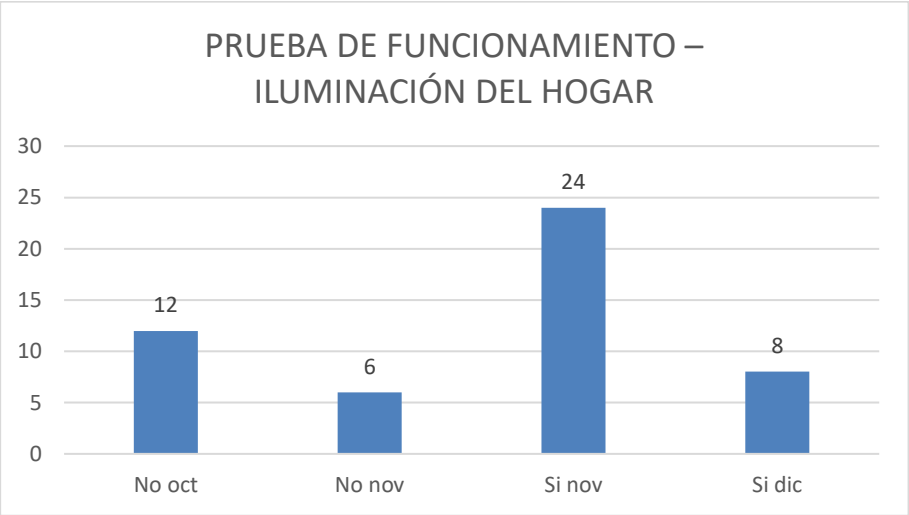
Figura 4. 7. Prueba de Funcionamiento – Alarma interna cámara



Nota. Análisis de iluminación y sirena interna camara, Autor: Pugarin Alexis

En la figura 4.7 se detalla el funcionamiento de la iluminación disuasiva y la sirena interna de la cámara, se observa un periodo inicial que abarca desde el 20 de octubre al 9 de noviembre. Durante este tiempo, se evidenció un funcionamiento intermitente de estas funciones debido a la configuración errónea de un horario de operación, lo que ocasionaba que en ciertas ocasiones sí funcionaran y en otras no. Estas fallas fueron subsanadas entre el 10 y el 14 de noviembre. Sin embargo, se desactivó nuevamente esta función hasta el 19 de noviembre, momento en el cual se detectaron y corrigieron las activaciones no deseadas, como las causadas por la lluvia. Finalmente, el 20 de noviembre, se implementó la detección de contorno humano, logrando un perfecto funcionamiento y manteniéndose en operación a lo largo del tiempo para la activación en el sistema de seguridad.

Figura 4. 8. Prueba de funcionamiento – iluminación del hogar

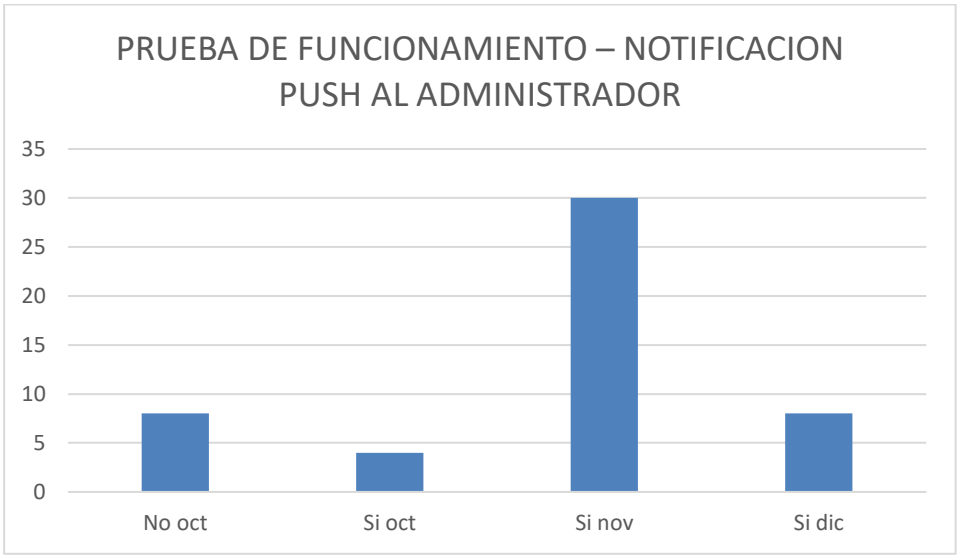


Nota. Análisis iluminación del hogar, Autor: Pugarin Alexis

En la presente figura 4.8, se ilustra el funcionamiento de la iluminación en la vivienda como actuadores en caso de emergencia, se tiene un periodo inicial, desde el 20 de octubre al 2 noviembre, donde no funcionan de manera óptima por las automatizaciones implementadas, desde el 3 al 8 de noviembre se logra implementar un funcionamiento con colores de luz cálida, pero se desactivan por 4 días en los cuales se trata de implementar colores y parpadeos al momento de la activación por intrusión y finalmente desde el 13 de noviembre al 8 de diciembre, se logra obtener el funcionamiento correcto de la iluminación como actuador, en respuesta de una intrusión no deseada cuando el sistema se encuentre armado.

4.2.3 Análisis de las notificaciones enviadas a los usuarios

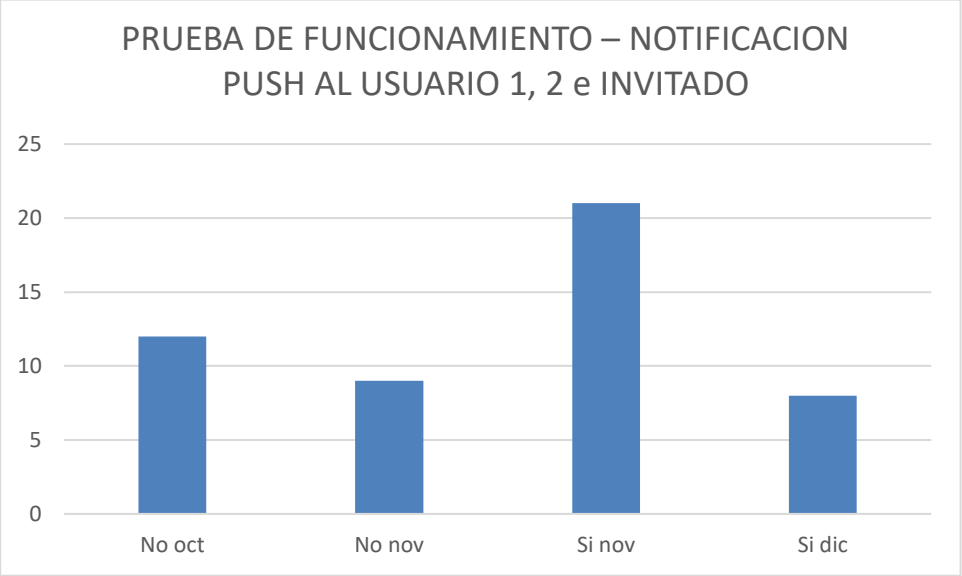
Figura 4. 9. Prueba de Funcionamiento - Notificaciones de emergencia Administrador



Nota. Análisis notificaciones de emergencia Administrador, Autor: Pugarin Alexis

En la figura 4.9 se ilustra el funcionamiento del envío de notificaciones al administrador en caso de suceder algún evento, cabe mencionar que el sistema de seguridad debería estar armado. Se registra un periodo inicial desde el 20 al 27 de octubre, durante el cual se realizaron pruebas con diversos métodos de envío de notificaciones, como Telegram y otros, evidenciando intermitencias en su funcionamiento. En respuesta a esta situación, se implementó la aplicación "Alarmo" para el envío de notificaciones, llevando a cabo pruebas exclusivamente con la inclusión del administrador. Desde el 28 de octubre hasta el 8 de diciembre, se logró establecer en el sistema un mecanismo de notificación estable y eficaz, como se evidencia en todas las pruebas realizadas.

Figura 4. 10. Prueba de Funcionamiento - Notificaciones de emergencia usuarios



Nota. Análisis notificaciones de emergencia usuarios, Autor: Pugarin Alexis

En la figura 4.10 se ilustra el funcionamiento del envío de notificaciones a los usuarios e invitados, en caso de suceder algún evento, cabe mencionar que el sistema de seguridad debería estar armado. Se abarca un periodo inicial desde el 20 de octubre hasta el 9 de noviembre, durante el cual los usuarios se encontraban inactivos para recibir notificaciones. Posteriormente, desde el 10 de noviembre hasta el 8 de diciembre, se otorgaron los permisos necesarios a los usuarios e invitados para recibir notificaciones push a través de la aplicación del software de Home Assistant, informándoles sobre eventos ocurridos en la residencia.

CONCLUSIONES

Se creó un sistema de seguridad centralizado capaz de integrar diversas tecnologías para controlar dispositivos y realizar automatizaciones en respuesta a eventos emergentes, incorporando métodos aumentativos y alternativos de comunicación para aquellos con dificultades de comunicar sus necesidades, por medio de iconos de fácil accionamiento, proporcionando tranquilidad ante posibles amenazas de su integridad y bienes, ya sea con presencia o ausencia de usuarios en la residencia, mejorando la calidad de vida a través de un sistema amigable y confiable, que puede gestionarse local y remotamente, utilizando Home Assistant y hardware especializado para analizar y reducir las posibilidades de intrusiones no deseadas en áreas vulnerables de la vivienda.

Para implementar un sistema de seguridad en una residencia, se evaluaron propuestas orientadas a gestionar eficientemente procesos concurrentes, permitir la toma de decisiones inmediatas en automatizaciones y pueda soportar diversos protocolos de comunicación como zigbee2mqtt, Z-Wave, Bluetooth, UPnP, RTSP, entre otros, por estas razones descritas se seleccionó Home Assistant como el protocolo en donde se centralizada la interfaz del sistema de seguridad, con el objetivo de centralizar y coordinar todas las operaciones desde un único punto de control, facilitando la detección de eventos inesperados en la residencia y la toma de decisiones rápidas frente a intrusiones no deseadas, mediante sensores, actuadores y controladores conectados a una central como la Raspberry Pi4, generando eventos disuasorios y alertas correspondientes para asegurar un entorno seguro para los usuarios del sistema de seguridad.

El proyecto de seguridad residencial diseñado mediante la integración de sensores, actuadores y controladores Rasberry Pi 4 facilita la vigilancia remota, es decir mediante la implementación de las IoT que integra una red de comunicación de los dispositivos se logra un sistema de seguridad que puede ser supervisado y controlado desde cualquier parte del mundo

Para instaurar un sistema de seguridad con SAAC, se realizó un minucioso análisis del entorno y las áreas dentro de la residencia, identificando zonas vulnerables y categorizándolas como ambientes controlados o no controlados. El propósito fue asignar dispositivos específicos para monitorear cada área vulnerable y garantizar la seguridad en

tiempo real, es decir se diseñó alternativas de comunicación rápidas para controlar los eventos suscitados, siendo los botones de pánico digital y activación por la voz para garantizar una comunicación dual usuario máquina.

La pruebas de funcionamiento del sistema se llevó a cabo mediante pruebas por fechas llamadas eventos, en donde se verifica la activación de todos los dispositivos esclavos , sensores , cámaras, iluminación y sirenas cuando se provoca apertura de puertas , movimientos y presencia de personas en dichas zonas, logrando calibrar la sensibilidad y resolución de los esclavos y así poder obtener las señales que informen al controlador Rasberry Pi 4 de los eventos en cada zona y finalmente la plataforma de home asistant genere mensajes de notificación a los usuarios.

RECOMENDACIONES

En un sistema de seguridad, es crucial garantizar el funcionamiento constante de todos los dispositivos. Se sugiere identificar un rango de señal de Internet dentro del cual los dispositivos puedan operar sin inconvenientes. La estabilidad de la conexión a Internet es esencial, ya que la falta de una conexión estable puede resultar en un funcionamiento intermitente, manifestándose a menudo como desconexiones y afectando las automatizaciones. En situaciones donde se supere el alcance establecido, la implementación de dispositivos mesh puede ser considerada para ampliar la cobertura operativa.

Clasificar las distintas áreas de la residencia como ambientes controlados o no controlados y determinar las zonas vulnerables es esencial para la implementación eficaz de un sistema de seguridad. Además, es crucial identificar el tipo de sensor que se empleará en estas áreas vulnerables, considerando sus funciones y las tecnologías asociadas. Se recomienda realizar pruebas periódicas a lo largo de un período específico para asegurar el adecuado funcionamiento de los sensores, actuadores y controladores para evitar falsos positivos en el sistema.

Es fundamental proporcionar capacitación a los residentes del hogar donde se ha instalado el sistema de seguridad. Esto garantizará que los usuarios estén preparados para tomar decisiones inmediatas, ya sea cuando el sistema de seguridad esté activado o desactivado. Pueden realizar acciones como activar la automatización mediante un botón de pánico virtual o físico en caso de una intrusión no deseada, garantizando la integridad de los habitantes de la residencia en cualquier momento.

BIBLIOGRAFÍA

ASHA. (1997-2024). *American Speech-Language-Hearing Association*. Obtenido de American Speech-Language-Hearing Association: https://www.asha.org/public/speech/spanish/los-sistemas-aumentativos-y-alternativos-de-comunicacion/

Associations, A. &. (25 de Abril de 2023). *Intuz*. Obtenido de Intuz: https://www.intuz.com/blog/iot-smart-home-security-benefits-use-cases-and-top-devices

Chaparro Misó, D. (2021). *Desarrollo de una aplicación móvil para la comunicación de personas con discapacidad con asistentes virtuales inteligentes de dispositivos IoT.* España: Universidad de Alicante. Departamento de Lenguajes y Sistemas Informáticos.

Comapanion Apps. (2024). *Home Assistant Companion Docs*. Obtenido de https://companion.home-assistant.io/

Geeks Forge. (Enero de 2019). Obtenido de https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/

González, R. (2023). *Estudio y desarrollo de sistema domótico para vivienda privada con Home Assistant*. Recuperado el 18 de 12 de 2023, de Archivo Digital UPM: https://oa.upm.es/74970/

HIR, H. I. (Diciembre de 2020). *Internet of Things (IoT*. Obtenido de http://eps.ieee.org/hir: http://eps.ieee.org/hir

Home Assitant. (Octubre de 2023). Obtenido de Home Assistant Operating System: https://www.home-assistant.io/

Home Automation ideas. (s.f.). Obtenido de Best Platform for Your Home Assistant System: A Comprehensive Guide: https://www.espforbeginners.com/guides/best-platform-for-home-assistant/

INEC. (7 de 2023). *Tecnologías de la información y comunicación*. Recuperado el 16 de 12 de 2023, de Tecnologías de la Información y Comunicación-TIC: https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

INTuz. (Diciembre de 2022). *Building and ship remarkable digital products with IoT*. Obtenido

de https://www.intuz.com/

Martínez, P. (2020). *Sistema de monitorización inalámbrica de temperatura mediante sensor de infrarrojos y microcontrolador ESP32.* Recuperado el 23 de 12 de 2023, de riunet.upv.es: http://hdl.handle.net/10251/153154

Panchano, R. (30 de 5 de 2023). *Investigación sobre la Aplicación de la Automatización Residencial con el Objetivo de Reducir el Riesgo de Robo en una Vivienda Común*. Recuperado el 16 de 12 de 2023, de Ibero-American Journal of Engineering & Technology Studies: https://tech.iberojournals.com/index.php/IBEROTECS/article/view/623

Suárez, C. (2020). *Sistema seleccionador de botellas mediante visión artificial en Raspberry pi*. Recuperado el 20 de 12 de 2023, de riunet.upv.es: http://hdl.handle.net/10251/158714

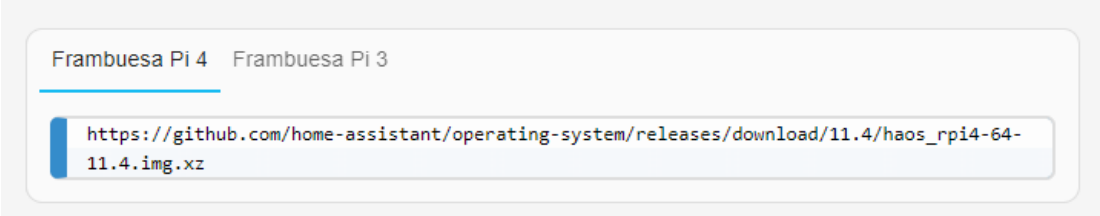
verde, G. C. (2 de Mayo de 2017). *¿Qué son los SAAC?* Obtenido de https://www.grupocasaverde.com/2017/04/25/que-son-los-saac/: https://www.grupocasaverde.com/2017/04/25/que-son-los-saac/

ANEXOS

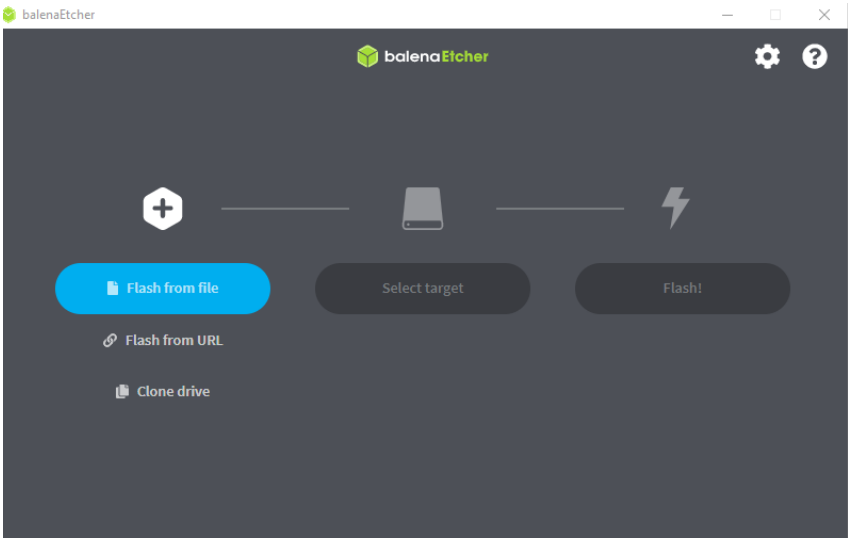
ANEXO 1- Instalación del sistema operativo de Home Assistant en el hardware Raspberry Pi

Para la instalación del software, se presentan diferentes opciones de instalación desde su página web, en el sistema se instalará Home Assistant Operating System, que incorpora un supervisor para facilitar la gestión del sistema, detectar errores y abordar su solución.

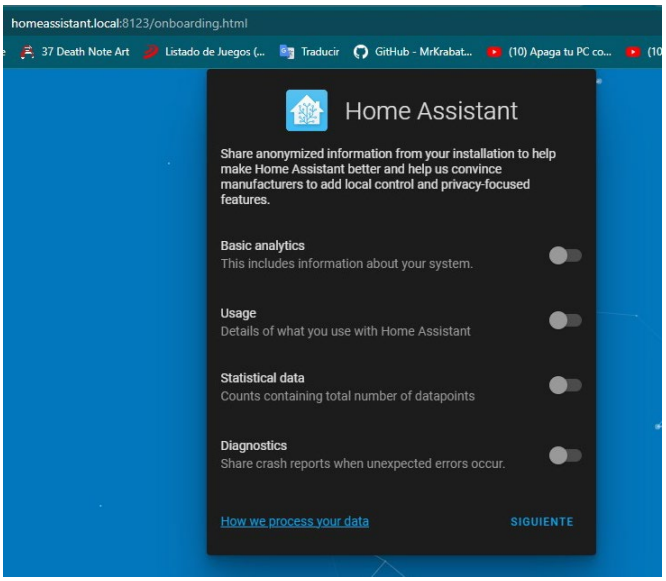
Paso 1. Descarga la imagen del sistema desde la página oficial de Home Assistant, según el tipo de hardware soportado a utilizar



Paso 2. Una vez obtenida la imagen del sistema, descargamos e instalamos el software Balena Etcher en un ordenador y posteriormente cargar la imagen de Hassbian en una tarjeta micro SD, que disponga un mínimo de 32 GB

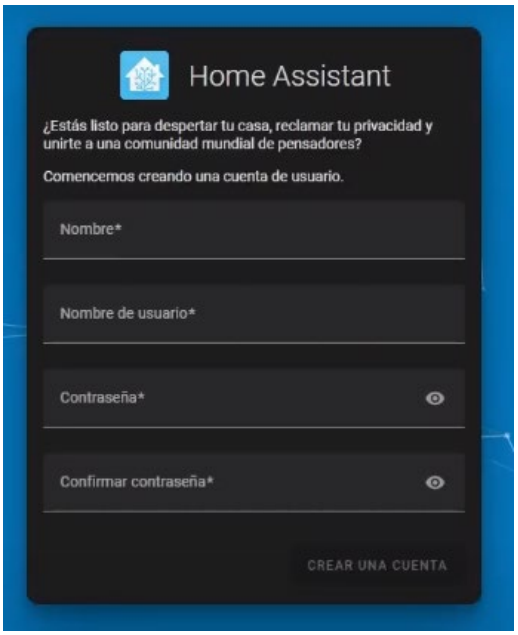


Paso 3. Cuando el sistema termina de arrancar ya se puede acceder a Home Assistant desde un navegador accediendo a la dirección http/192.168.8.100-8123 o a través de la dirección http://homeassistant.local:8123/, con el fin de proseguir con la instalación del mismo.



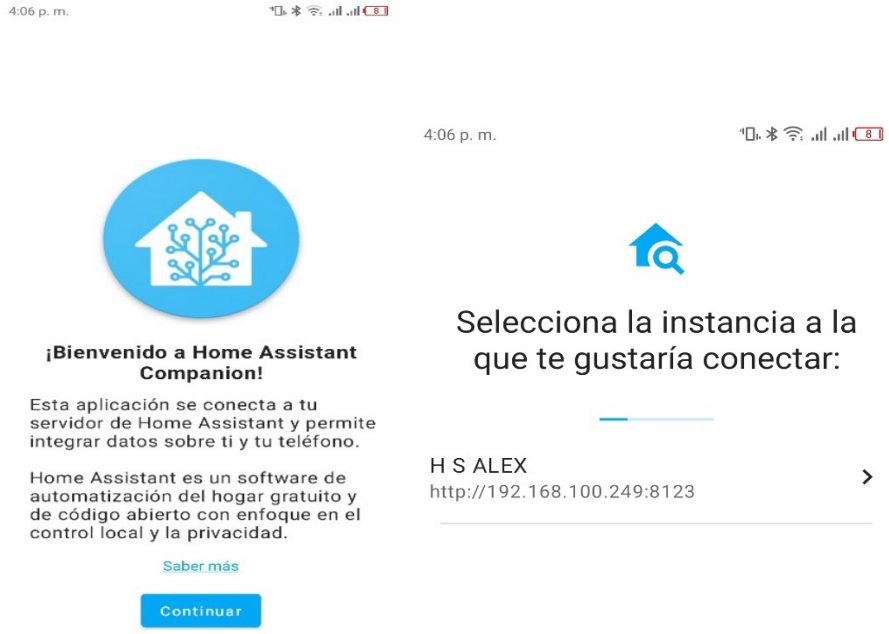
Paso 4. Finalmente se inserta la tarjeta SD con la imagen de Hassbian en el hardware Raspberry Pi y conectamos a la red y automáticamente comenzará el arranque inicial del sistema.

Este proceso puede tardar aproximadamente 15 minutos por ser la primera vez, ya que se descarga e instala la última versión de la herramienta hasshian-confíg y de Home Assistant, pasado el tiempo de espera y por ser la primera vez en la que arranca el dispositivo se deberá crear un usuario y una contraseña única para el sistema, habilitando al primer usuario como administrador del sistema.

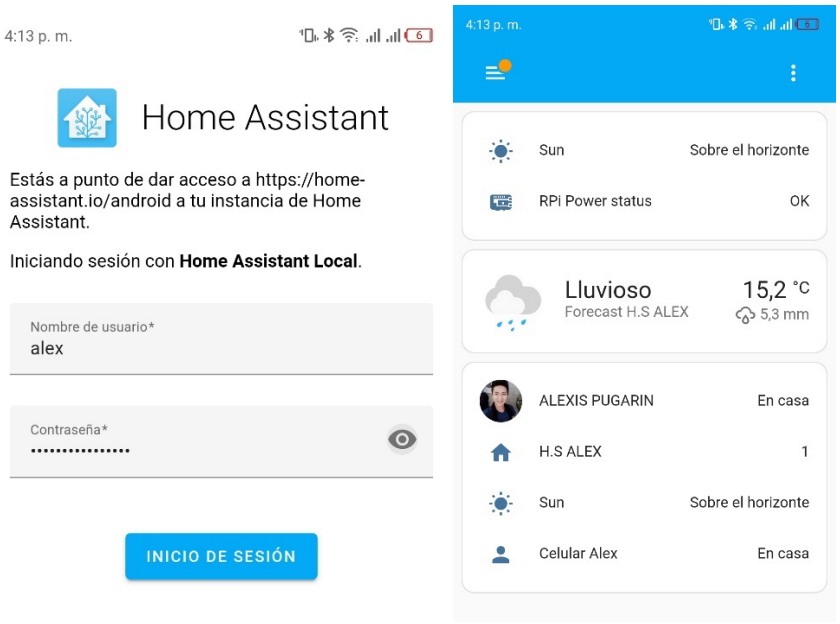


ANEXO 2- Instalación de Home Assistant en dispositivos móviles.

Paso 1. Para descargar Home Assistant en un dispositivo móvil, descargamos la aplicación de Home Assistant desde la Play Store o Apple Store y seleccionamos la instancia o introducimos la dirección manualmente de la instancia a la cual deseamos conectarnos, ya sea para conectarse localmente o remotamente.

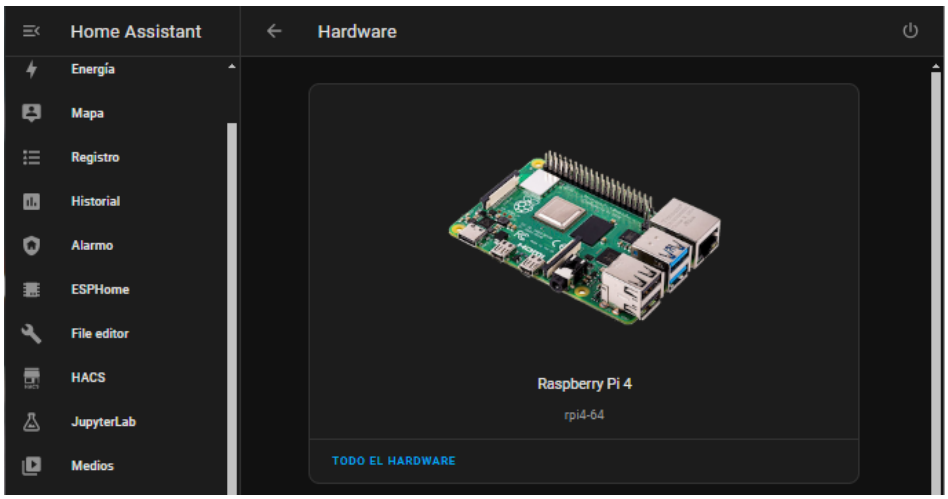


Paso 2. Ingresamos con la cuenta de usuario y contraseña. En este apartado se podrá acceder como Administrador o Usuario y la misma determinará el grado de manipulación al sistema.

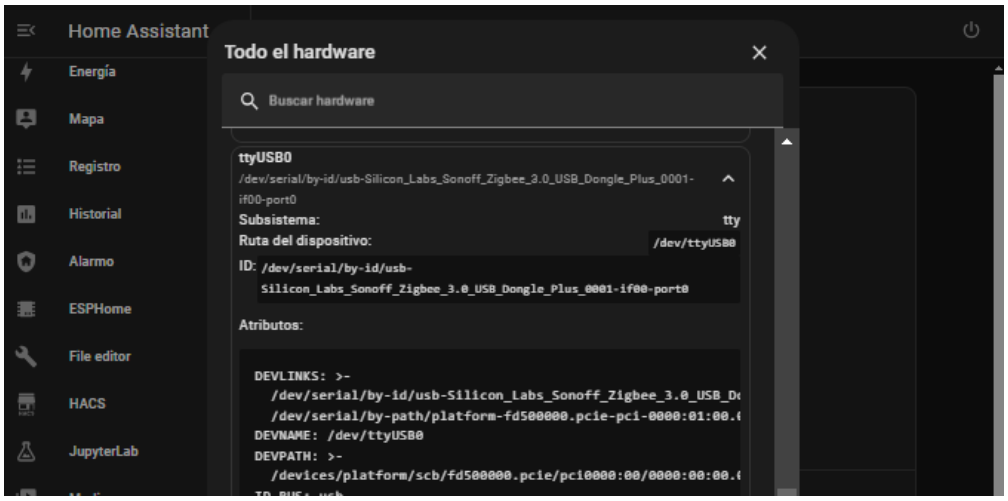


ANEXO 3 - Instalación del coordinador universal Sonoff-P Zigbee USB

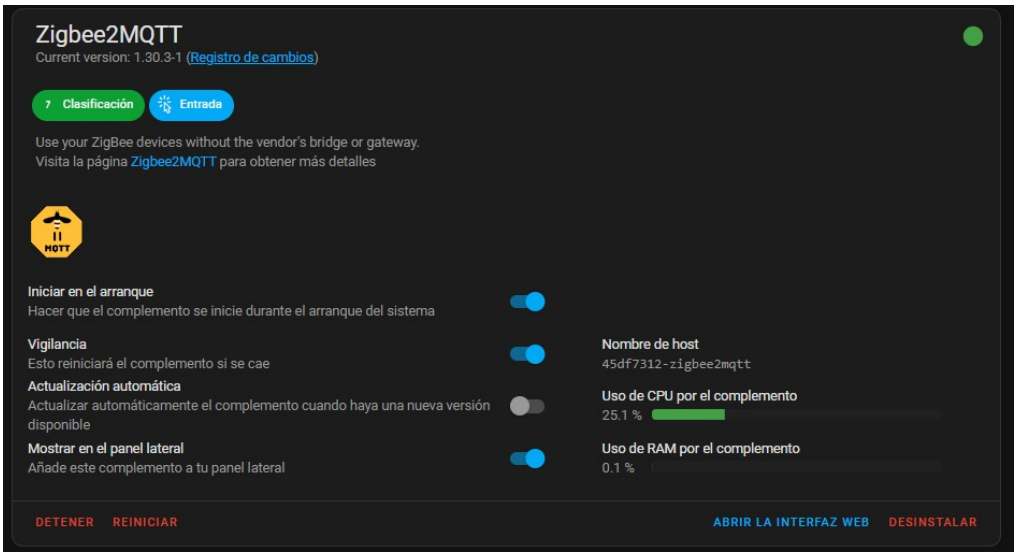
Paso 1. Después de conectar el coordinador Zigbee a la Raspberry Pi 4 por medio de uno de sus periféricos USB, en la interfaz gráfica seleccionamos configuraciones y nos dirigimos al apartado de hardware.



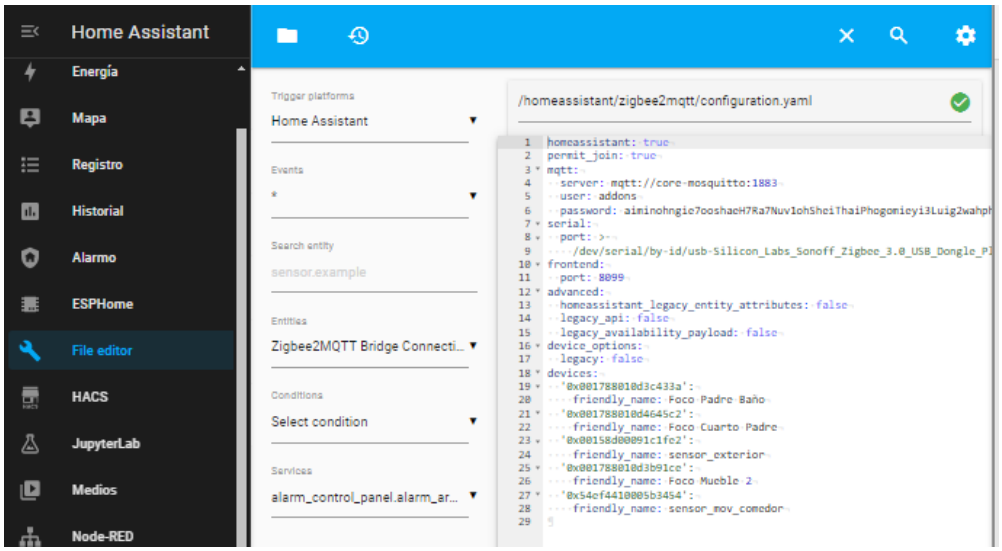
Paso 2. Seleccionamos el periférico en el cual tenemos conectado nuestro coordinador universal, y observamos en la leyenda que haga referencia a Silicon Labs Zigbee USB Dongle, y tendremos presente esta información



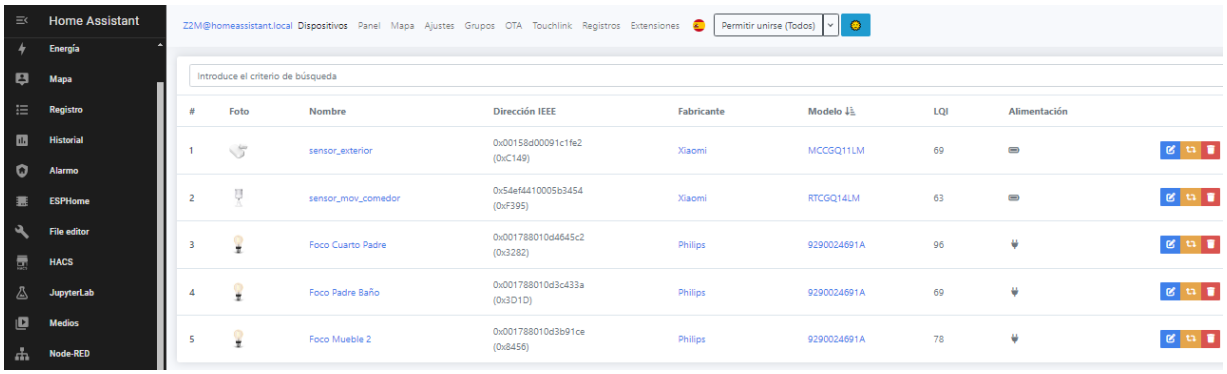
Paso 3. Accederemos a configuraciones y al apartado de Add-ons, donde buscaremos e instalaremos el siguiente addon.



Paso 4. Finalmente nos dirigimos a File editor, donde introducimos el siguiente código de configuración. yaml, tomando en cuenta port corresponde al ID del hardware del coordinador Zigbee.

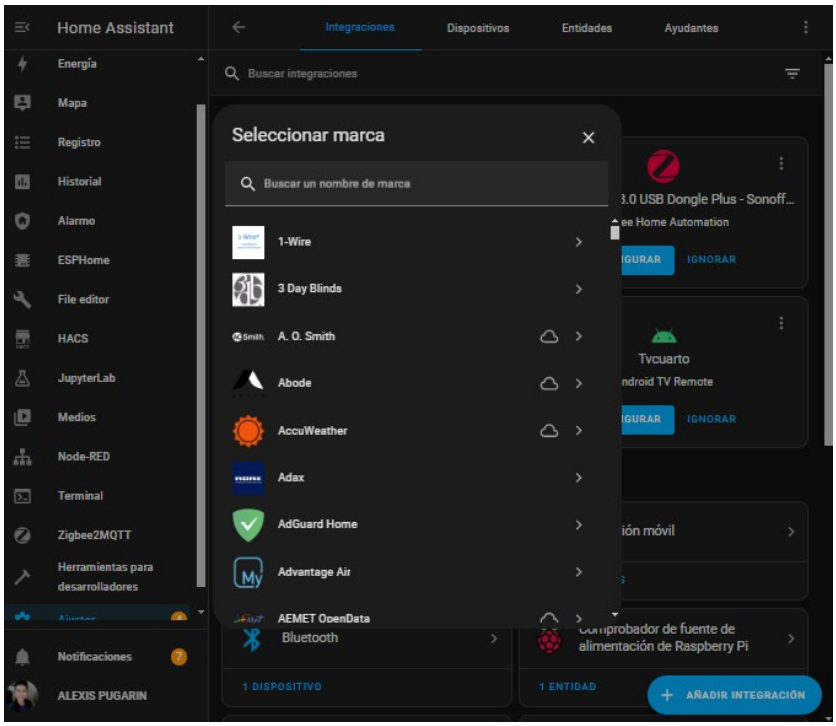


Paso 5. Posteriormente se realiza la integración con los dispositivos de entrada Zigbee, integrándolos al sistema sin problema alguno.

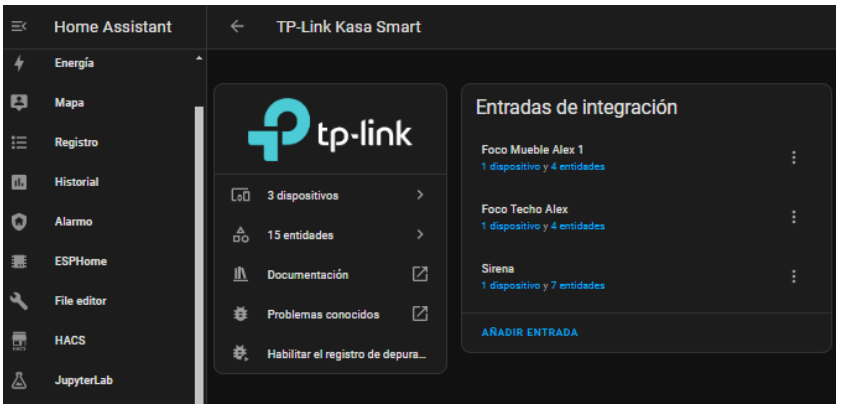


ANEXO 4 - Instalación de dispositivos Wifi

Paso 1. Para la instalación de dispositivos controlados por Wi-Fi, debemos vincular los dispositivos a la red, buscamos dispositivos y servicios, añadimos la integración, y desentendiendo del fabricante este puede trabajar localmente o no.

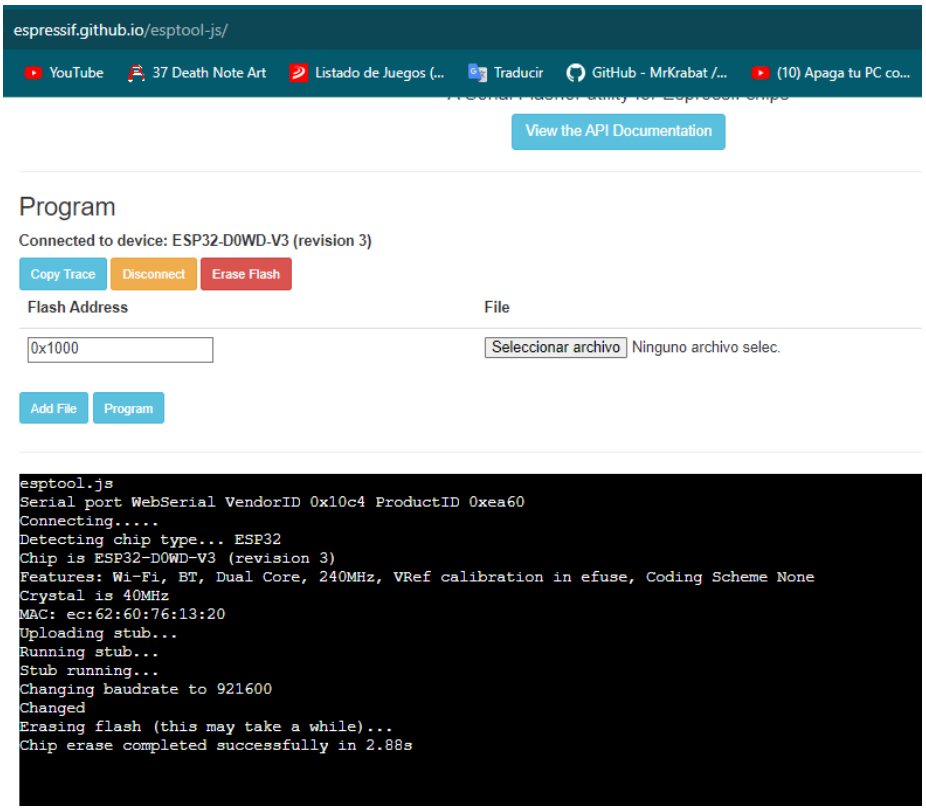


Paso 2. Se integrarán los dispositivos necesarios.



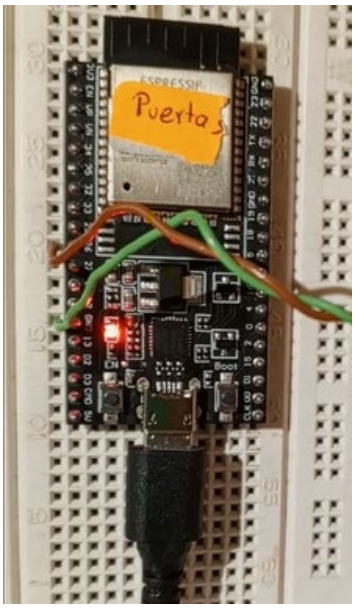
ANEXO 5- Añadir dispositivos cableados con un nodo esp32 para su integración con Home Assistant

Paso 1. Conectaremos el microcontrolador esp32 al ordenador, y a través de la herramienta de realizaremos un formateo de la memoria de este, para asegurar una instalación limpia y que no presente errores.

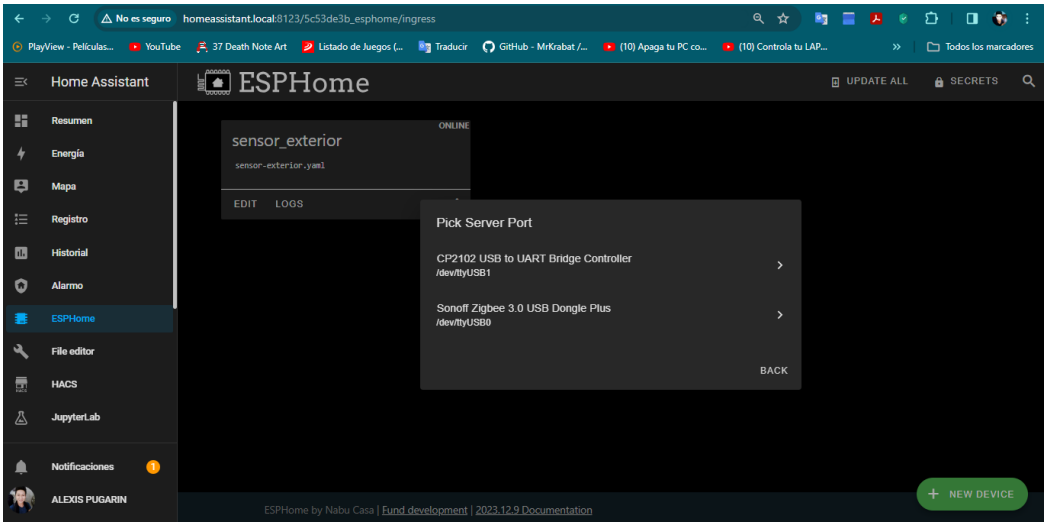


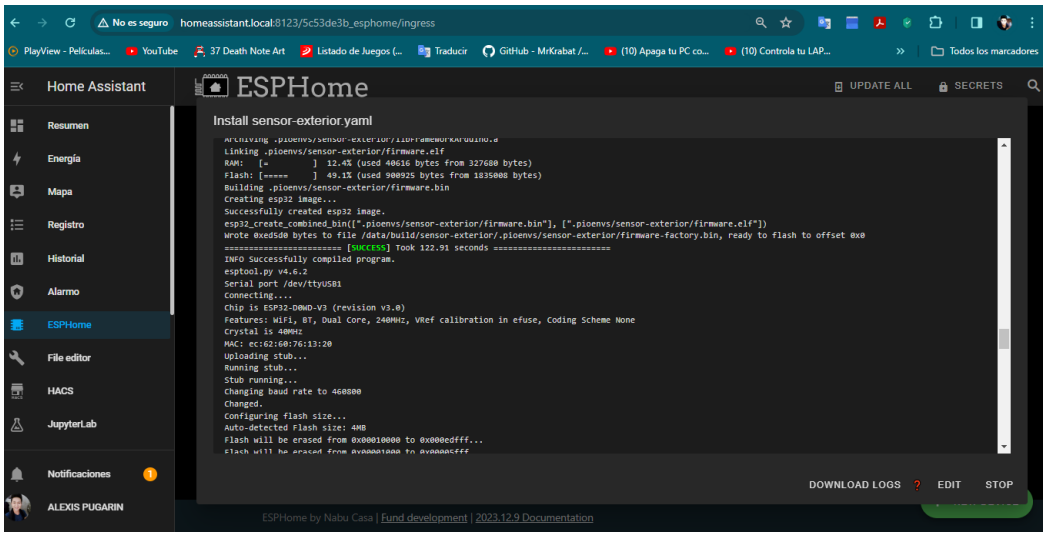
Paso 2. Los dispositivos cableados siempre disponen, de dos bornes para la transmisión de la señal según sea su función de detección, estos independientemente de la alimentación que utilizaran, para esta demostración de usaran los bornes alarm.

Posteriormente estos bornes se conectarán al microcontrolador esp32, se realizará la interconexión entre los pines 26 y GND del microcontrolador y los bornes de transmisión del sensor cableado a utilizar.

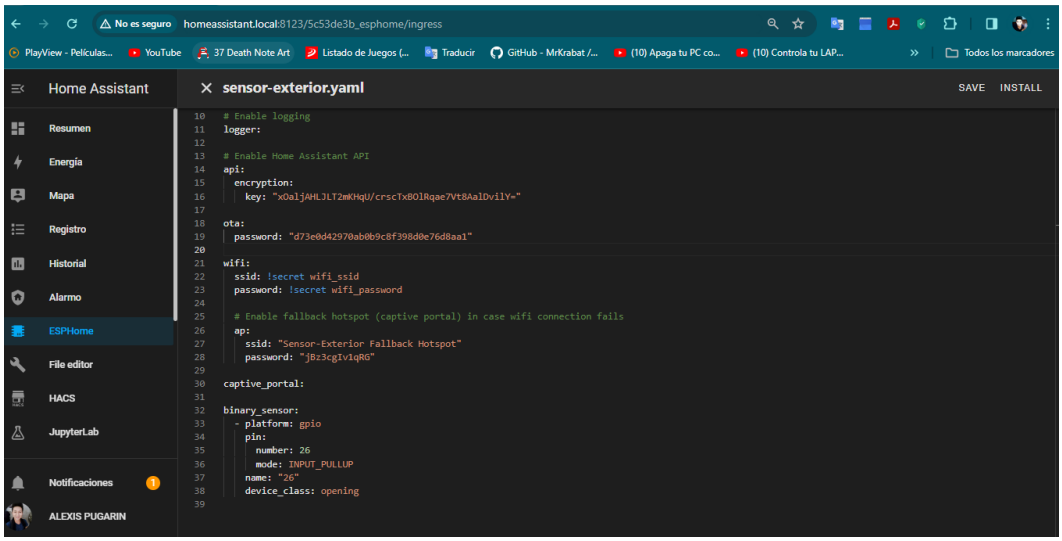


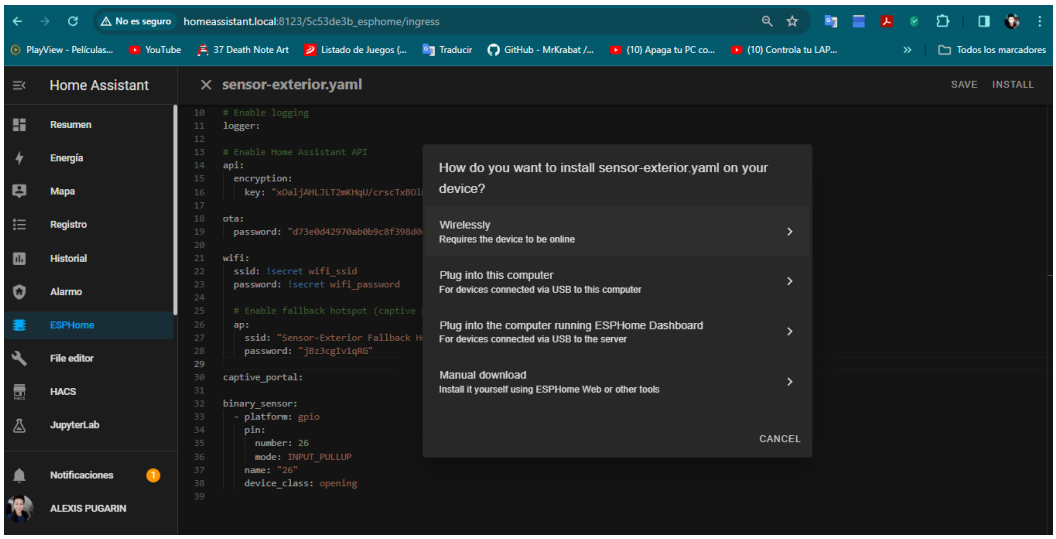
Paso 3. Ya teniendo el hardware correspondiente integraremos a Home Assistant por medio de un add- on de la misma, este dispositivo lo conectaremos a la Raspberry Pi4 a uno de sus periféricos USB, donde utilizaremos la opción “Plug into computer running ESPHome”, para poder instalar el software de configuración inicial de nuestro microcontrolador, y seleccionamos nuestro dispositivo y esperamos su instalación.



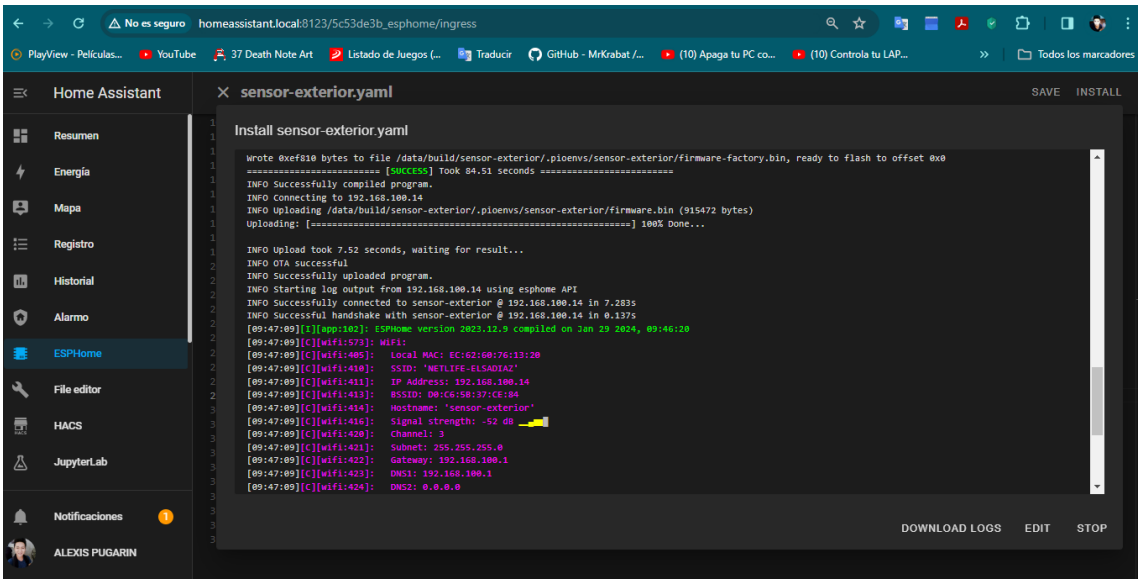


Paso 4. Ahora introducimos la programación requerida para el sensor y lo instalaremos por medio de la opción “wirelessly”, para cargar el programa en el microcontrolador,

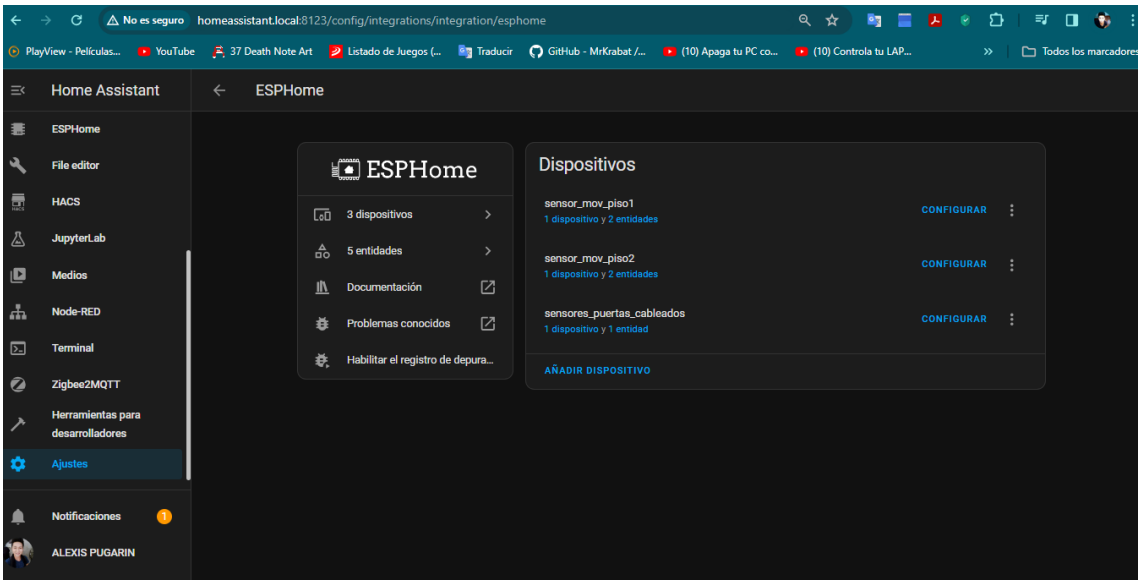




Paso 5. Esperamos a la confirmación de que la programación se cargó con éxito, y verificar tenemos señal en nuestro microcontrolador, teniendo conexión con la red de la residencia y detecte los cambios del dispositivo cableado.



Paso 6. Ahora podemos revisar la integración y vincular el microcontrolador con cualquier otro dispositivo, y se obtener un censado del dispositivo cableado hacia la plataforma de control de Home Assistant.


No es seguro
homeassistant.local:8123/config/integrations/integration/esphome
Home Assistant
ESPHome
File editor
HACS
JupyterLab
Medios
Node-RED
Terminal
Zigbee2MQTT
Herramientas para desarrolladores
Ajustes
Notificaciones
ALEXIS PUGARIN
ESPHome
3 dispositivos
5 entidades
Documentación
Problemas conocidos
Habilitar el registro de depura...
Dispositivos
sensor_mov_piso1
1 dispositivo y 2 entidades
CONFIGURAR
sensor_mov_piso2
1 dispositivo y 2 entidades
CONFIGURAR
sensores_puertas_cableados
1 dispositivo y 1 entidad
CONFIGURAR
AÑADIR DISPOSITIVO