UNIVERSIDAD PRIVADA DE TACNA
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

TESIS

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DOMÓTICO ÚNICO HÍBRIDO ZIGBEE-WIFI CON ACCESO REMOTO E INDEPENDIENTE DE SISTEMAS PROPIETARIOS EN UNA VIVIENDA URBANA DE TACNA DURANTE EL AÑO 2025-2026"

PARA OPTAR:

TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:

Bach. REYNALDO JHOSEP CORNEJO TAPIA

TACNA – PERÚ

2026

UNIVERSIDAD PRIVADA DE TACNA
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

TESIS

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DOMÓTICO ÚNICO HÍBRIDO ZIGBEE-WIFI CON ACCESO REMOTO E INDEPENDIENTE DE SISTEMAS PROPIETARIOS EN UNA VIVIENDA URBANA DE TACNA DURANTE EL AÑO 2025-2026"

Tesis sustentada y aprobada el 19 de junio del 2026; estando el jurado calificador integrado por:

PRESIDENTE	**:**	**Dr. ANIBAL JUAN ESPINOZA ARANCIAGA**
SECRETARIO	**:**	**Mag. MARCO ANTONIO SEBASTIAN COLOMA YUNGANINA**
VOCAL	**:**	**Mag. TITO LEONCIO CÓRDOVA MIRANDA**
ASESOR	**:**	**Mag. HUGO JAVIER RIVERA HERRERA**

DECLARACIÓN JURADA DE ORIGINALIDAD

Yo Reynaldo Jhosep Cornejo Tapia, egresado, de la Escuela Profesional de Ingeniería Electrónica de la Facultad de Ingeniería de la Universidad Privada de Tacna, identificado con DNI 72960555 respectivamente, así como Hugo Javier Rivera Herrera con DNI 00494293; declaramos en calidad de autor y asesor que:

1. Somos los autores de la tesis titulado: *Diseño e implementación de un sistema domótico único híbrido Zigbee-Wifi con acceso remoto e independiente de sistemas propietarios en una vivienda urbana de Tacna durante el año 2025-2026*, la cual presentamos para optar el Título Profesional de Ingeniero de *Electrónica*
2. La tesis es completamente original y no ha sido objeto de plagio, total ni parcialmente, habiéndose respetado rigurosamente las normas de citación y referencias para todas las fuentes consultadas.
3. Los datos presentados en los resultados son auténticos y no han sido objeto de manipulación, duplicación ni copia.

En virtud de lo expuesto, asumimos frente a *La Universidad* toda responsabilidad que pudiera derivarse de la autoría, originalidad y veracidad del contenido de la *tesis*, así como por los derechos asociados a la obra.

En consecuencia, nos comprometemos ante a *La Universidad* y terceros a asumir cualquier perjuicio que pueda surgir como resultado del incumplimiento de lo aquí declarado, o que pudiera ser atribuido al contenido de la tesis, incluyendo cualquier obligación económica que debiera ser satisfecha a favor de terceros debido a acciones legales, reclamos o disputas resultantes del incumplimiento de esta declaración.

En caso de descubrirse fraude, piratería, plagio, falsificación o la existencia de una publicación previa de la obra, aceptamos todas las consecuencias y sanciones que puedan derivarse de nuestras acciones, acatando plenamente la normatividad vigente.

Tacna, 9 de junio de 2026

Reynaldo Jhosep Cornejo Tapia
DNI: 72960555

Hugo Javier Rivera Herrera
DNI: 00494293

DEDICATORIA

A mis padres, quienes con su esfuerzo incansable y amor infinito me enseñaron que la educación es el camino más seguro hacia la libertad y la realización personal. gracias por cada consejo, cada sacrificio silencioso y cada palabra de aliento que me sostuvo en los momentos de duda. a mis tías y madre mayor, que siempre estuvieron presente con apoyo y comprensión, incluso cuando mis responsabilidades académicas me alejaban de reuniones y celebraciones, su paciencia y cariño fueron el motor que me impulsó a seguir adelante. a mis maestros, por su dedicación y por sembrar en mí la pasión por el conocimiento. cada enseñanza recibida se convirtió en una herramienta invaluable para construir este trabajo. a mi padre mayor, que ya no está físicamente conmigo, pero cuya memoria y enseñanzas siguen iluminando mi vida. su ejemplo de esfuerzo, humildad y sabiduría me inspira cada día, y este logro también es un homenaje a su legado.

Reynaldo Jhosep Cornejo Tapia

AGRADECIMIENTO

Quiero expresar mi más sincera gratitud a la universidad y a la facultad que me acogieron durante estos años de formación, cada espacio académico, cada curso y cada proyecto fueron oportunidades para crecer no solo como profesional, sino también como persona. agradezco profundamente a mis docentes y tutores de investigación, quienes con paciencia y rigor académico me guiaron en el proceso de construcción de esta tesis; sus observaciones y consejos fueron fundamentales para dar forma y solidez a este trabajo. A los compañeros de clase, por las conversaciones enriquecedoras, el intercambio de ideas y el apoyo mutuo en los momentos de mayor exigencia. La colaboración y el espíritu de equipo hicieron que este camino fuera más llevadero y estimulante.

Reynaldo Jhosep Cornejo Tapia

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

Se diseñó e implementó un sistema domótico híbrido Zigbee-WiFi con acceso remoto e independiente de sistemas propietarios en una vivienda urbana de Tacna durante 2025-2026. Los objetivos específicos fueron determinar el efecto de la interoperabilidad entre dispositivos de diferentes marcas en la coherencia de estados y el retraso acumulado del sistema híbrido; identificar diferencias de estabilidad y confiabilidad según la combinación de marcas en la red Zigbee-WiFi; y desarrollar un sistema de seguridad técnica para una exposición segura a Internet. Se empleó una metodología cuantitativa, basada en mediciones instrumentadas, análisis estadístico, modelado computacional y expresiones matemáticas para cuantificar coherencia, latencias, estabilidad y métricas de seguridad. Los resultados fueron satisfactorios: se observó ahorro energético general significativo y respuesta adecuada para cubrir necesidades primarias en situaciones determinadas; además, se evidenció que la interoperabilidad influyó en la coherencia y en el retraso acumulado, y que la estabilidad variaba según las combinaciones de marcas utilizadas. Se concluyó que el diseño híbrido permitió independencia de plataformas propietarias, mejoró la eficiencia energética y que la implementación de medidas de seguridad redujo la exposición a riesgos en el acceso remoto.

Palabras clave: eficiencia energética; interoperabilidad; seguridad remota; domótica híbrida; Zigbee-WiFi

ABSTRACT

A hybrid Zigbee–WiFi home automation system with remote access and independence from proprietary systems was designed and implemented in an urban residence in Tacna during 2025–2026. The specific objectives were to determine the effect of interoperability among devices from different brands on state coherence and the accumulated delay of the hybrid system; to identify differences in stability and reliability according to the combination of brands in the Zigbee–WiFi network; and to develop a technical security system for safe exposure to the Internet. A quantitative methodology was employed, based on instrumented measurements, statistical analysis, computational modeling, and mathematical expressions to quantify coherence, latencies, stability, and security metrics. The results were satisfactory: a significant overall energy saving was observed and an adequate response to meet primary needs in certain situations; furthermore, it was shown that interoperability influenced coherence and accumulated delay, and that stability varied according to the combinations of brands used. It was concluded that the hybrid design enabled independence from proprietary platforms, improved energy efficiency, and that the implementation of security measures reduced exposure to risks in remote access.

Keywords: energy efficiency; hybrid home automation; interoperability; remote security; Zigbee-WiFi

INTRODUCCIÓN

En el capítulo I se plantea la necesidad de diseñar e implementar un sistema domótico híbrido Zigbee-WiFi en una vivienda urbana de Tacna para evaluar empíricamente interoperabilidad, rendimiento, estabilidad y seguridad entre marcas bajo condiciones locales. El estudio busca medir latencia, consumo y confiabilidad, proponer lineamientos técnicos y validar soluciones económicas y sostenibles adaptadas al contexto tacneño.

En el capítulo II se revisan antecedentes y bases teóricas sobre IoT y domótica, comparando protocolos (Zigbee, MQTT, WiFi), plataformas como Home Assistant, medidas de seguridad (VPN, cifrado, bloqueo DNS) y Zigbee2MQTT se detalla como una solución de código abierto que actúa como una interfaz fundamental entre un sistema anfitrión y la comunicación de radio Zigbee. Se destacan estudios que avalan arquitecturas híbridas, optimización de Zigbee en entornos con interferencia y soluciones de acceso remoto seguro para hogares inteligentes.

En el capítulo III se presenta el diseño metodológico experimental para implementar y evaluar un sistema domótico híbrido Zigbee-WiFi con Home Assistant en Raspberry Pi. Define requisitos (integración multimarca, control remoto seguro, broker MQTT, medición energética), la principal decisión de diseño en cuanto al uso Zigbee2MQTT + Mosquitto, es para lograr la independencia de hubs propietarios y visibilidad completa de tópicos/estados, arquitectura de red segmentada, fases (diagnóstico, instalación, ejecución) y pruebas (unitarias, integración, carga, auditoría) para medir latencia, consumo, interoperabilidad y seguridad.

En el capítulo IV se presentan los resultados: arquitectura final con tres subredes segmentadas y una red Zigbee en malla; mapeo y visualización de la topología Zigbee; inventario de dispositivos y mediciones de consumo; análisis que muestra ahorros energéticos con relés y bombillas inteligentes; y registros de activación para evaluar latencia y coherencia. Como primer resultado a destacar tenemos el diseño esquemático final de la vivienda adaptada con la nueva red domótica. En conjunto, el diagrama comunica una arquitectura doméstica segmentada físicamente y por función.

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1. Descripción del problema

La automatización de viviendas mediante tecnologías inteligentes es una tendencia creciente a nivel global, impulsada por la necesidad de eficiencia energética, seguridad y confort. La domótica (o automatización del hogar) integra sensores, actuadores y protocolos de comunicación para ejecutar tareas previamente manuales, tales como el encendido de luces, control de temperatura o monitoreo remoto. Su adopción ha sido incentivada por el desarrollo del internet de las cosas (IoT), que permite la interconexión eficiente de múltiples dispositivos dentro del hogar.

Uno de los principales retos técnicos es garantizar un rendimiento óptimo cuando se integran múltiples dispositivos de diferentes marcas, usando protocolos de comunicación como Zigbee y WiFi. Estudios como los de (Esposito et al., 2023) o (Silva et al., 2021) muestran cómo estas variables pueden afectar críticamente el tiempo de respuesta, consumo energético y estabilidad operativa. Sin embargo, existe escasa información experimental y contextualizada al entorno urbano peruano, donde las condiciones de red, suministro eléctrico y diversidad de dispositivos presentan un escenario distinto. Por ejemplo, Zigbee ha mostrado un rendimiento superior en escenarios con múltiples dispositivos debido a su bajo consumo y escalabilidad, mientras que WiFi, aunque más veloz, tiende a generar mayor consumo energético y saturación en redes domésticas densas (Dokuz et al., 2024 y Orfanos et al., 2023).

Como afirman Miori et al. (2019) la expansión de las tecnologías facilitadoras del internet de las cosas permite la creación de nuevos escenarios donde la domótica desempeña un papel fundamental. Las plataformas para ciudades y comunidades inteligentes, que deben incluir aplicaciones para la eficiencia energética, la salud, la movilidad, la seguridad, etc. No pueden ignorar el uso de datos recopilados directamente desde los hogares; para implementar estos escenarios, toda la infraestructura tecnológica y los sistemas domésticos relacionados deben ser capaces de comprenderse e intercambiar información. En el caso específico de América Latina, la implementación de sistemas domóticos sigue enfrentando barreras como la limitada estandarización, la interoperabilidad entre marcas y la escasa información técnica local. En ciudades como Tacna, Perú. (Perumal et al., 2010) entienden que los consumidores acceden a dispositivos disponibles comercialmente sin criterios técnicos sólidos para su integración, lo que puede provocar ineficiencias, conflictos de compatibilidad y subutilización tecnológica.

La mayoría de estudios previos han sido realizados en contextos industriales o académicos fuera de la realidad peruana, con escasa información experimental sobre el rendimiento técnico de sistemas domóticos en viviendas urbanas del sur del país. Esta carencia de evidencia local limita el desarrollo de soluciones domóticas adaptadas a la infraestructura eléctrica, las condiciones de red y los hábitos de consumo de la población tacneña. En consecuencia, esta falta de evidencia limita la adopción de soluciones domóticas eficientes, seguras y sostenibles, dificultando la transición hacia viviendas inteligentes en el entorno urbano local. De ahí surge la necesidad de realizar un estudio experimental que evalúe de manera empírica el impacto de la marca de dispositivos en el rendimiento técnico, la interoperabilidad y la seguridad de un sistema híbrido Zigbee-WiFi implementado en una vivienda urbana de Tacna.

1.2. Formulación del problema

1.2.1. Problema general

¿Cómo el diseño e implementación de un sistema híbrido de comunicación Zigbee–WiFi contribuye a la automatización eficiente, segura y accesible de una vivienda urbana en la ciudad de Tacna durante el año 2025-2026?

1.2.2. Problemas específicos

a. ¿Cómo diseñar una arquitectura híbrida Zigbee-WiFi que permita un control remoto confiable de los dispositivos domóticos, sin depender de plataformas o hubs propietarios?
b. ¿Cómo implementar un sistema de control remoto que garantice la seguridad de las comunicaciones y una exposición controlada a Internet en un entorno doméstico basado en IoT?
c. ¿En qué medida la automatización de la iluminación y de los actuadores mediante la arquitectura híbrida propuesta reduce el consumo energético en comparación con el uso convencional de dichos dispositivos?

1.3. Justificación e importancia

La presente investigación se justifica porque responde a un vacío técnico y científico en la evaluación de sistemas domóticos híbridos bajo condiciones reales en viviendas urbanas peruanas. La mayoría de estudios previos se han desarrollado en contextos

internacionales, con entornos altamente controlados (laboratorios o prototipos), lo que no refleja la complejidad de la infraestructura eléctrica y de red en ciudades como Tacna.

a. Justificación técnica

Este estudio permitirá medir de manera empírica el impacto de la marca de dispositivos sobre métricas objetivas de rendimiento técnico, como la latencia de respuesta, el consumo energético, la interoperabilidad y la seguridad, aspectos críticos en entornos residenciales. Según (Silva et al., 2021), la elección del protocolo influye directamente en la latencia y el consumo energético, mientras que (Esposito et al., 2023) recomiendan sistemas híbridos para mejorar la eficiencia energética y la escalabilidad en contextos urbanos, donde la congestión de redes es frecuente. Por otro lado, (Agarwal K., 2021) demostró que el rendimiento de Zigbee puede optimizarse mediante un manejo centralizado de interferencias WiFi, un hallazgo relevante para redes inalámbricas vulnerables. En este marco, la investigación en Tacna proporcionará lineamientos técnicos aplicables a contextos latinoamericanos, donde las redes suelen enfrentar mayores desafíos de congestión y vulnerabilidad, ofreciendo soluciones adaptadas a realidades locales con infraestructuras heterogéneas.

b. Justificación científica

La investigación contribuye a la generación de conocimiento aplicado en el campo de la domótica y el Internet de las Cosas (IoT), abordando una brecha identificada en la literatura. Aunque (Dokuz et al., 2024) y (Liang y Luo, 2024) destacan que los resultados en domótica dependen del contexto de implementación y la heterogeneidad de marcas, existe una escasez de estudios experimentales en entornos residenciales peruanos. Este trabajo se diferencia porque realizara una evaluación experimental en viviendas urbanas reales, incorporara múltiples marcas y protocolos bajo un diseño factorial que garantiza rigor científico, e integra métricas de seguridad (poco exploradas en investigaciones locales) basadas en estudios recientes como los de (Holter y Hjelmtvedt, 2024). Así, no solo valida hallazgos previos, sino que enriquece el corpus teórico con datos empíricos contextualizados.

c. Justificación social

Los sistemas domóticos trascienden el mero confort, al mejorar significativamente la calidad de vida de poblaciones vulnerables, como adultos mayores, personas con movilidad reducida o familias que requieren monitoreo remoto de seguridad. Estudios

como el de (Stepanov et al., 2021) evidencian que herramientas como Zigbee2MQTT son eficaces para integrar sistemas de asistencia a adultos mayores, facilitando su autonomía. Asimismo, (Mero, 2022) reportó altos niveles de satisfacción en usuarios que percibieron mejoras en confort y accesibilidad gracias a la domótica. En Tacna, donde el envejecimiento poblacional y la necesidad de viviendas seguras son prioridades, este estudio puede impulsar la adopción de tecnologías que promuevan la inclusión tecnológica y la seguridad residencial, adaptadas a las necesidades de grupos con menor acceso a soluciones convencionales.

d. Justificación ambiental

La eficiencia energética es uno de los beneficios más relevantes de los sistemas domóticos cuando se seleccionan adecuadamente protocolos y dispositivos. (Gil et al., 2022) destacan que la convergencia de protocolos IoT permite reducir el consumo energético sin sacrificar rendimiento, mientras que (Esposito et al., 2023) reportaron una disminución del 30 % en el consumo al implementar arquitecturas híbridas. La investigación identifica combinaciones óptimas de marcas y protocolos para minimizar el consumo energético en viviendas urbanas de Tacna, apoyando políticas de sostenibilidad ambiental. Los resultados orientarán a hogares y autoridades para adoptar tecnologías que reduzcan la huella de carbono, contribuyan a los ODS y cumplan metas locales de eficiencia energética.

e. Justificación económica

La adopción de plataformas de código abierto y hardware accesible, como Home Assistant y Raspberry Pi, reduce significativamente las barreras de entrada a la domótica en Latinoamérica, donde el poder adquisitivo es limitado. (Cabrera, 2019) demostró que es posible integrar múltiples marcas en Home Assistant con un costo total de hardware de apenas €142,57; mientras que (Lliso, 2021) y (Escobedo y Quispe, 2025) resaltan la importancia de soluciones seguras y de bajo costo basadas en protocolos abiertos como MQT y VPNs. El estudio valida soluciones económicas para democratizar la domótica en Tacna, permitiendo a familias de ingresos bajos y medios acceder a seguridad y confort.

1.4. Objetivos

1.4.1. Objetivo General

Diseñar e implementar un sistema híbrido de comunicación Zigbee-WiFi que contribuya a la automatización eficiente, segura y accesible de una vivienda urbana en la ciudad de Tacna durante el año 2025.

1.4.2. Objetivos Específicos

a. Diseñar una arquitectura híbrida Zigbee-WiFi que permita un control remoto confiable de los dispositivos domóticos, sin depender de plataformas o hubs propietarios
b. Implementar un sistema de control remoto que garantice la seguridad de las comunicaciones y una exposición controlada a Internet en un entorno doméstico basado en IoT
c. Determinar que la automatización de la iluminación y de los actuadores mediante la arquitectura híbrida propuesta reduce el consumo energético en comparación con el uso convencional de dichos dispositivos

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de la investigación

Los avances en internet y las tecnologías web han impulsado la investigación sobre la conectividad de objetos físicos, dando origen al Internet de las Cosas (IdC) (Ashton et al., 2009) e Internet de Todo (IdT) (Evans, 2011). Estas tecnologías hacen que los objetos sean más inteligentes y estén más conectados para realizar tareas complejas en entornos domésticos e industriales, expandiendo el concepto de hogar inteligente a escala de ciudad. (Silva et al., 2021) evaluaron el rendimiento de tres protocolos IoT - MQTT, CoAP y OPC UA- en términos de latencia, consumo energético y ancho de banda, obteniendo que MQTT presenta el menor retardo promedio (~50 ms) y menor consumo energético, mientras CoAP obtiene mejor eficiencia en redes IPv6. Concluyen que MQTT es adecuado para control en tiempo real y CoAP/OPC UA para aplicaciones industriales basadas en recursos.

Esposito et al. (2023) implementaron un sistema domótico usando NB-IoT, MQTT y funciones serverless en maquetas reales, obteniendo latencias promedio de 120 ms y una reducción del consumo energético del 30 % respecto a implementaciones WiFi. Recomiendan sistemas híbridos (celular + MQTT + serverless) para entornos urbanos con cobertura celular, logrando eficiencia energética y escalabilidad. (Agarwal, 2021) demostró que Zigbee2MQTT junto con un manejo centralizado del tráfico WiFi reduce la pérdida de paquetes Zigbee del 67 % al 7 % en ambientes con alta interferencia, mejorando significativamente la estabilidad y confiabilidad de los dispositivos en entornos saturados. (Stepanov et al., 2021) diseñaron en Rusia un sistema domótico con Zigbee2MQTT y Home Assistant orientado a adultos mayores, integrando sensores de movimiento, control de luces, botones SOS y recordatorios. Demostraron que Zigbee2MQTT permite una integración eficiente y económica de múltiples dispositivos sin depender de fabricantes específicos. (Liang y Luo, 2024) integraron Zigbee con MQTT en China para diseñar un sistema de iluminación, seguridad y gestión de electrodomésticos, concluyendo que esta combinación es efectiva para el control remoto y la gestión inteligente de dispositivos, destacando que Home Assistant potencia la interoperabilidad de estos sistemas.

Mero (2022) desarrolló y evaluó un sistema domótico centralizado con Raspberry Pi 4 y Home Assistant, integrando visualización de cámaras, control de luces y dispositivos mediante módulos infrarrojos. La evaluación con 40 usuarios arrojó 100 % de funcionalidad, 98 % de satisfacción y 75 % de mejora del confort, consolidando

los sistemas de bajo costo y código abierto como tendencia creciente para la automatización del hogar. (Holter y Hjelmtvedt, 2024) analizaron la seguridad en Home Assistant mediante una integración maliciosa (PoE) que demostró la adquisición de información sensible de usuarios. La encuesta reveló baja confianza en integraciones personalizadas, recomendando sandboxing, virtualización y arquitectura multiproceso como mitigaciones eficaces.

Escobedo y Quispe (2025) diseñaron una VPN basada en WireGuard para una empresa agroindustrial peruana, demostrando que WireGuard supera a TLS/SSL en rendimiento, reduciendo el uso de CPU, eliminando la fragmentación y optimizando el ancho de banda en redes móviles. (Kazemi, 2024) comparó estrategias de balanceo de carga en NGINX y HAProxy para despliegues de StoRM WebDAV. Mientras el acceso directo fallaba al 40,64 % de éxito con 500 req/s, ambos balanceadores mantuvieron el 100 % de éxito, siendo HAProxy capaz de gestionar 700 req/s con alta disponibilidad y rendimiento sostenido.

Seo et al. (2012) en Corea del Sur desarrollaron una investigación teórica y de diseño titulada "Zigbee security for Home automation using attribute-based cryptography". El estudio propone mejoras en autenticación y distribución de claves para redes Zigbee sin comprometer la compatibilidad con Zigbee2MQTT, concluyendo que es factible robustecer la seguridad en redes Zigbee interoperables con plataformas abiertas como Home Assistant y mantener su rendimiento operativo. En la implementación del hogar inteligente con Home Assistant se emplea Cloudflare para conectividad remota mediante túneles salientes, evitando exponer puertos o depender de IP pública fija; esto simplifica NAT, certificados y reglas de firewall y reduce la superficie de ataque al iniciar el acceso desde el interior de la red (Mohammedi et al., 2025). La arquitectura facilita interoperabilidad entre servicios locales y externos, aplica Zero Trust y autenticación centralizada, aporta redundancia y mejora latencia, aunque genera dependencia del proveedor.

2.2. Bases teóricas

2.2.1. Los sistemas domóticos

En el contexto de las viviendas urbanas modernas, los sistemas domóticos se han consolidado como soluciones clave para mejorar la eficiencia energética, la comodidad y la seguridad. Están compuestos por una red de dispositivos interconectados que permiten la automatización de funciones del hogar mediante tecnologías de comunicación, sensores y actuadores. Dos factores críticos que afectan el rendimiento

técnico de estos sistemas son el protocolo de comunicación utilizado y la variación en el tipo y número de dispositivos instalados. (Mathe et al., 2024) consideran que, para la automatización, Raspberry Pi ofrece diversas aplicaciones en dominios como la automatización del hogar, agricultura, atención médica, control industrial e investigación avanzada, destacando sus beneficios para la creación de prototipos y sus limitaciones y desafíos asociados.

2.2.2. Plataforma interoperable de Internet de las cosas para sistemas de hogares inteligentes

En un entorno de hogar inteligente, es muy importante definir una plataforma centralizada porque permite gestionar y optimizar ecosistemas masivos de forma segura y rentable. Home Assistant permite controlar y automatizar miles de dispositivos de diferentes marcas, además de contar con la arquitectura RESTful, que permite la interoperabilidad en la Arquitectura de Web de Objetos de Hogar Inteligente (SWOA). RESTful es flexible para equipar dispositivos, recursos y protocolos de comunicación heterogéneos para mejorar la satisfacción del usuario (Romero et al., 2010).

Home Assistant destaca frente a opciones como OpenHAB, HomeSeer y otras por ser completamente gratuito, 100 % local y tener una comunidad gigantesca. Ofrece la mayor compatibilidad de dispositivos multimarca del mercado, permitiendo automatizaciones complejas y un control total de privacidad sin depender de la nube, con menor costo y mayor accesibilidad.

2.2.3. Los protocolos de comunicación

Los protocolos de comunicación constituyen el conjunto de reglas que rigen el intercambio de datos entre dispositivos dentro de un sistema domótico. Existen múltiples opciones, como Zigbee, Z-Wave, WiFi y MQTT, cada una con ventajas y limitaciones respecto al consumo energético, la latencia, la escalabilidad y la confiabilidad. La correcta selección del protocolo incide directamente en el tiempo de retardo, el consumo energético y la saturación del sistema (Dokuz et al., 2024; Rákay y Galajdová, 2019).

Se justifica optar por Zigbee en lugar de Z-Wave porque, como muestra la tabla 1, al ser una norma abierta fomenta la innovación y la competencia entre fabricantes; su diseño permite escalar a redes de hasta 65 000 dispositivos teóricos, siendo apropiado para instalaciones industriales, comerciales y residenciales; y la topología de malla admite comunicación multisalto —hasta 30 nodos intermedios—, extendiendo el

alcance sin infraestructura adicional y mejorando la tolerancia a fallos al redirigir tramas para sortear obstáculos o nodos caídos (Haidarzhy, 2023).

Tabla 1

Comparación entre protocolo Zigbee y Z-Wave

Característica	Zigbee	Z-Wave
Banda de frecuencia	915 MHz (EE. UU.) 2,4 GHz (en todo el mundo	908,42 MHz (EE. UU.) 868,42 MHz (Europa)
Tasa de datos	20-250 kbps	9,6-100 kbps
Rango de conexión	10-100 metros (33-328 pies)	30-100 metros (100-330 pies)
Longitud de ruta	30 saltos	4 saltos
Consumo de energía	Ligeramente más bajo	Ligeramente más alto
Precio	Generalmente más bajo	Generalmente más alto
Complejidad	Un poco más complejo	Un poco menos complejo
Estándar de protocolo	IEEE 802.15.4 (Zigbee)	ITU-T G.9959 (Z-Wave)
Número máximo de dispositivos por red	65.000	232
Características de seguridad	Cifrado AES-128	Cifrado AES-128
Principales ventajas	Mayor velocidad de datos, menor coste, mayor compatibilidad con dispositivos	Mayor alcance de conexión directa, configuración más sencilla, menos Interferencias

Nota. Adaptado de Haidarzhy (2023) del sitio web: https://sirinsoftware.com/blog/zigbee-vs-z-wave-comparison-pros-cons-how-do-they-work

2.2.4. Software puente Zigbee2MQTT

Zigbee2MQTT es una solución de código abierto que actúa como interfaz fundamental entre un sistema anfitrión y la comunicación de radio Zigbee. Su propósito principal es permitir la conexión inalámbrica de dispositivos Zigbee directamente a un sistema de automatización del hogar utilizando un bróker MQTT, facilitando el control y el monitoreo a través de mensajes MQTT e integrándolos en plataformas que soportan MQTT incluso si no tienen soporte nativo para Zigbee (Zigbee2MQTT, 2025).

Para operar, Zigbee2MQTT requiere, en primer lugar, un adaptador Zigbee basado en Z-Stack o EmberZNet, que sirve como puente entre el sistema anfitrión y la red de radio Zigbee; un sistema anfitrión compatible (por ejemplo, Raspberry Pi con Linux, Windows o macOS); el bróker MQTT Mosquitto instalado en el sistema anfitrión;

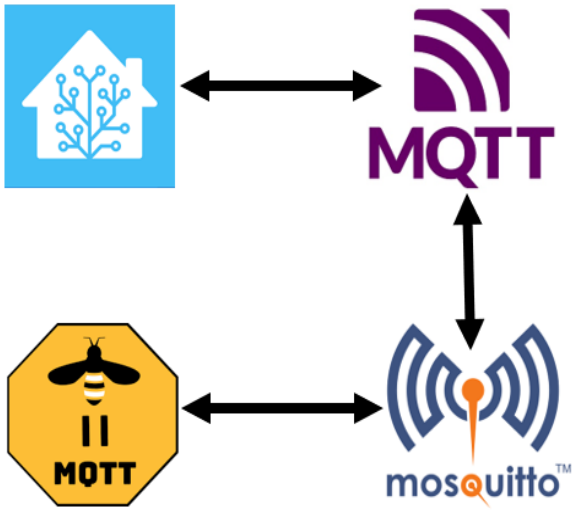
y, por último, uno o más dispositivos Zigbee emparejados con Zigbee2MQTT (Home Assistant, 2025).

2.2.4.1. Arquitectura MQTT y Flujo de Mensajería

MQTT es un modelo de mensajería ligero basado en publicar/suscribir, donde los clientes envían mensajes a topics y un broker central los recibe y distribuye. Su flujo típico consiste en: clientes que publican mensajes en topics; el broker que recibe y encola esos mensajes; y el mismo broker que los entrega a los clientes suscritos, como se expone en la figura 1.

Figura 1

Arquitectura MQTT para Domótica: Home Assistant, Mosquitto y Zigbee2MQTT



Como se observó en la figura 1 sobre Arquitectura MQTT para Domótica: Home Assistant, Mosquitto y Zigbee2MQTT (la comunicación entre softwares se realiza a través de MQTT es por ello que el bloque con el mismo nombre no se encuentra presente), en cuanto a la función de cada bloque se detalla de la siguiente forma:

- Home Assistant: Plataforma que gestiona, centraliza y sobre todo automatiza dispositivos inteligentes.
- Mosquitto: Servidor, bróker MQTT que recibe y reenvía mensajes, funciona como intermediario central para la publicación y suscripción entre clientes.

- Zigbee2MQTT: Cliente/Puente MQTT que traduce mensajes Zigbee a topics MQTT y viceversa.
- MQTT: Protocolo de mensajería, el cual establece el canal de comunicación eficiente entre clientes.

La lógica de control y orquestación se mantiene en la plataforma de automatización, mientras que el broker centraliza la entrega fiable de mensajes entre dispositivos. La separación cliente-broker facilita la interoperabilidad entre distintos fabricantes y reduce la complejidad de las conexiones punto a punto.

Zigbee2MQTT ofrece amplias funcionalidades: mejora alcance y estabilidad de la malla Zigbee, asegura comunicaciones y permite analizar tráfico. Admite añadir dispositivos, usar convertidores externos y extensiones, conectar adaptadores remotos y realizar OTA. Su configuración detallada incluye ajustes del adaptador, parámetros MQTT, red Zigbee y gestión de dispositivos/grupos; optimizar la red (extensiones USB, ubicación estratégica) es crucial (Zigbee2MQTT, 2025).

2.2.5. Los dispositivos de un sistema domótico

Por otro lado, la variación en la cantidad y el tipo de dispositivos interconectados representa un reto en la arquitectura de redes domóticas. A medida que se incrementa el número de dispositivos, el sistema experimenta mayores exigencias en cuanto a procesamiento, tráfico de datos y sincronización, lo cual puede derivar en retraso acumulado y saturación de red (Steane y Radcliffe, 2019).

El protocolo Home Automation Device Protocol, basado en una arquitectura tipo IFTTT, ejemplifica cómo un diseño eficiente puede reducir tanto la latencia como el consumo energético mediante el uso de paquetes mínimos y soporte para múltiples medios de comunicación (Gonnot et al., 2015). Además, estudios centrados en el análisis comparativo de protocolos han señalado que aquellos que permiten flexibilidad y compatibilidad entre plataformas ofrecen mejor desempeño general en sistemas con alta heterogeneidad de dispositivos (Orfanos et al, 2019).

El retardo aumenta con protocolos ineficientes o saturación por muchos dispositivos; mitigarlo requiere arquitectura jerárquica o nodos intermedios para procesamiento local, como Arduino o Raspberry Pi usando protocolos ligeros (HTTP, SNMP) (Kalagara et al., 2018; Robert y Istvan, 2011).

2.2.6. Protocolos de seguridad cibernética

a. Autenticación de usuarios: La autenticación prueba y valida la identidad de los participantes, asegurando que solo entidades autorizadas accedan a los recursos de una red. Como imagen referencial, véase la figura 2. Esto se logra mediante mecanismos como certificados digitales X.509, nombres de usuario y contraseñas, o claves precompartidas (PSK), previniendo accesos no autorizados y suplantación de identidad (De la Cruz y Vera, 2020).

Figura 2

Acceso autorizado, contraseña validada entre servidor y cliente

Nota. Imagen extraída de la siguiente página: https://www.segurilatam.com/actualidad/dia-del-internet-seguro-autenticacion-de-doble-o-multiple-factor-una-capa-adicional-de-seguridad_20210120.html (Segurilatam, 2021).

b. Cifrado de datos: Cifrado de datos: El cifrado de datos es esencial para la confidencialidad de la información, volviéndola ilegible para usuarios no autorizados durante su transmisión en redes públicas. Se logra mediante algoritmos criptográficos y claves secretas que encapsulan y cifran paquetes. Protocolos como IPSec y WireGuard utilizan estas técnicas para

proteger datos sensibles y garantizar su integridad, como se muestra en la figura 3 (De la Cruz y Vera, 2020; Escobedo y Quispe, 2025).

Figura 3

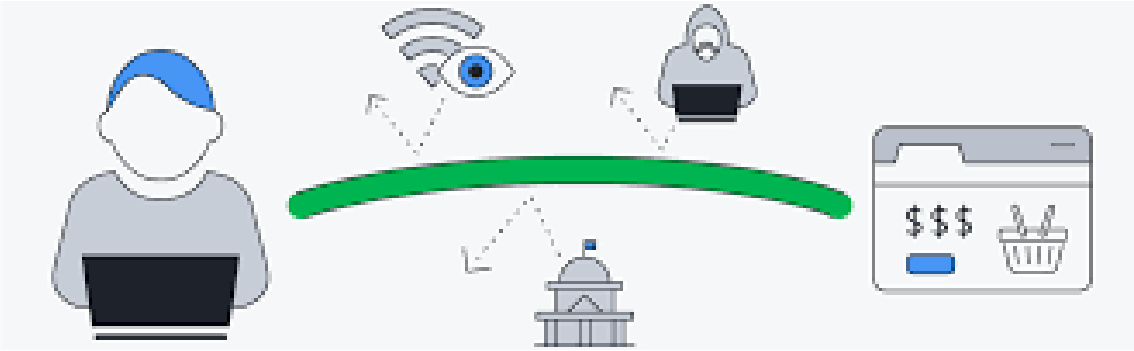
Seguridad digital con múltiples capas de protección

Nota. Imagen extraída de la siguiente página: https://www.infordisa.com/soc/cifrado-para-seguridad-de-datos/ (Infordisa, 2024).

c. Control de acceso: Como se representa en la figura 4, se garantiza que solo usuarios autorizados accedan a recursos específicos, implementado mediante políticas de seguridad y mecanismos de filtrado que definen permisos y restricciones, controlando el tráfico. Incluye autenticación robusta para proteger la red contra intrusiones (De la Cruz y Vera, 2020; Escobedo y Quispe, 2025; Hernández, 2009).

Figura 4

Conexión protegida entre usuario y comercio electrónico frente a amenazas

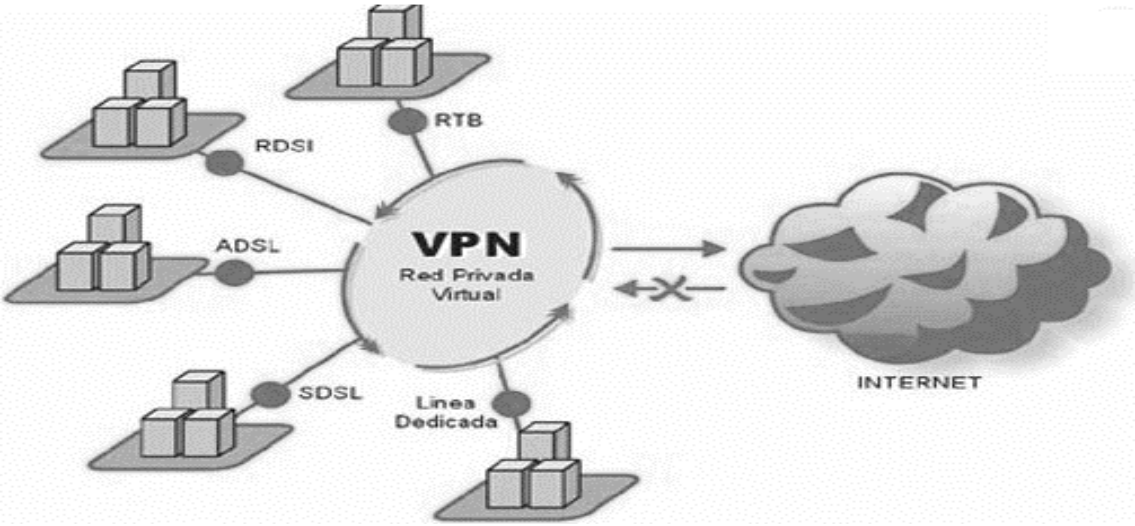


Nota. Imagen extraída de la siguiente página: https://www.avg.com/es/signal/what-is-an-ip-address (Burdova, 2022).

d. Integración de redes: La integración de redes mediante VPN conecta componentes de una red a través de una red pública, extendiendo la red local para el acceso remoto seguro de usuarios y sucursales. Esto se logra mediante túneles cifrados y encapsulación, que permiten una comunicación segura entre subredes, como se aprecia en la figura 5 (De la Cruz y Vera, 2020; Escobedo y Quispe, 2025; De Luz, 2024).

Figura 5

Diagrama de VPN conectando múltiples redes privadas al Internet



Nota. Imagen extraída de la siguiente página: https://inversorlatam.com/la-vpn-crea-una-conexion-privada-y-segura-entre-muchas-personas-y-dispositivos-a-traves-de-internet/ (Inversorlatam, 2019).

e. Encriptación: El cifrado convierte datos legibles en formato cifrado para proteger la confidencialidad; usa algoritmos y claves secretas para encapsular paquetes en VPN, garantizando integridad y evitando accesos no autorizados, como se ilustra en la figura 6 (Escobedo y Quispe, 2025; De la Cruz y Vera, 2020).

Figura 6

Protección de datos y comunicaciones seguras en la nube

Nota. Imagen extraída de la siguiente página: https://tuatara.co/blog/software/encriptacion-de-datos-seguridad-de-informacion/ (González, 2025).

2.2.7. Seguridad con bloqueos DNS

AdGuard Home es un resolutor DNS con filtrado a nivel de red que aplica listas de bloqueo y reglas personalizadas para impedir la resolución de dominios publicitarios, de seguimiento y maliciosos desde cualquier dispositivo conectado a la red (AdGuard Software Ltd, 2026). Sus principales beneficios son:

- Protección para toda la red sin clientes instalados: El filtrado DNS a nivel de red bloquea anuncios para todos los dispositivos sin instalar software individual, ofreciendo cobertura uniforme en IoT y reduciendo la carga de gestión y los recursos necesarios (AdGuard Software Ltd, 2026).

- Políticas por dispositivo y control parental: Permite aplicar listas, excepciones y horarios por dispositivo, ofreciendo segmentación granular; restringe contenido para menores sin afectar a otros usuarios y facilita la gestión de acceso basada en roles (AdGuard Software Ltd, 2026).
- Visibilidad y control centralizados: a integración muestra el total de consultas y las consultas bloqueadas, los clientes activos, y ofrece paneles y automatizaciones útiles (Nijhof, 2026).
- Privacidad y seguridad mejoradas: Al resolver y filtrar localmente se minimizan las consultas a servidores externos y se interceptan dominios maliciosos antes de que lleguen al dispositivo, lo que reduce la exposición a rastreadores y ataques DNS y mejora la confidencialidad y la protección. (AdGuard Software Ltd, 2026).

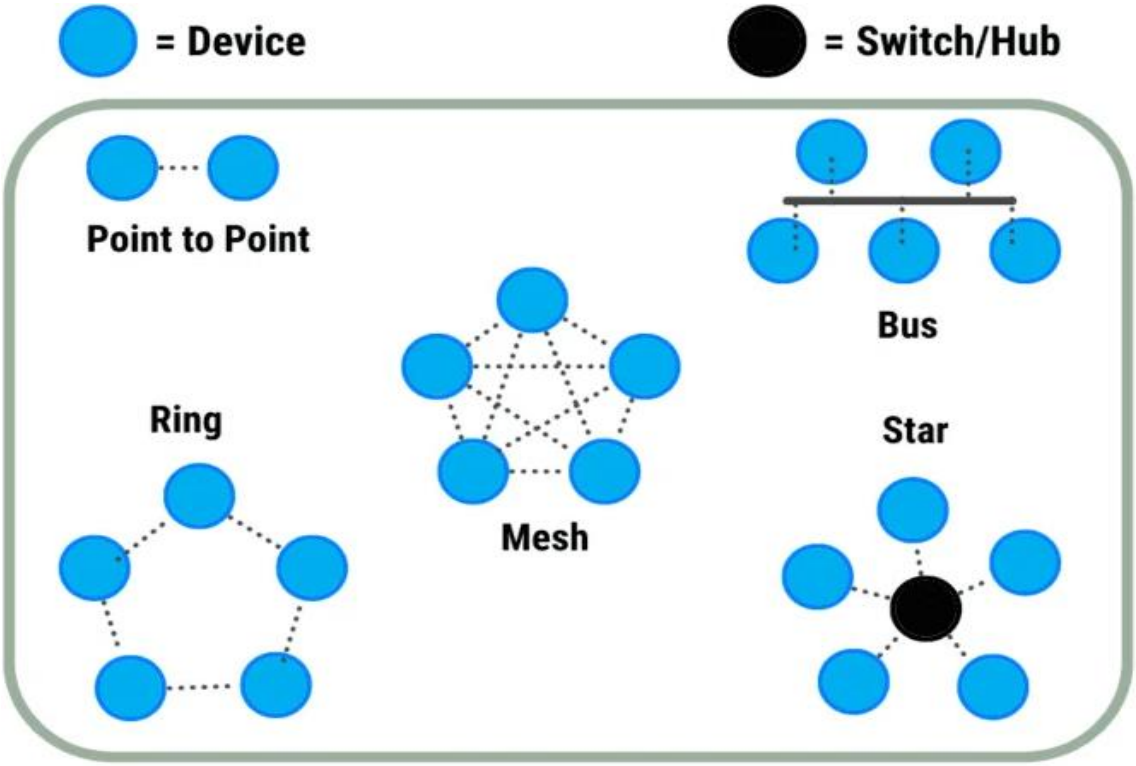
2.2.8. Topología de un sistema IoT

La topología de un sistema IoT describe la disposición de nodos y enlaces que permiten la comunicación entre sensores, actuadores, pasarelas y servicios en la nube. Considera cómo se conectan los dispositivos (punto a punto, estrella, árbol, malla), las rutas de datos y los puntos de traducción entre protocolos. Esta estructura condiciona la latencia, el consumo energético y la tolerancia a fallos, influyendo en la experiencia del usuario y en la gestión remota (WizzDev, 2026).

Una topología bien diseñada optimiza las rutas de comunicación, reduce la latencia y minimiza el consumo energético de dispositivos con recursos limitados, lo que es crítico en nodos alimentados por batería. También permite priorizar el tráfico crítico frente al tráfico de menor importancia, garantizando que las acciones de control se ejecuten con la rapidez necesaria (SigmaOS, 2024). La malla facilita la interoperabilidad entre dispositivos de distintos protocolos mediante pasarelas estratégicamente ubicadas que agregan datos de redes de baja potencia y los encaminan hacia la infraestructura IP, tal como se muestra en la figura 7 (Gaotek, s. f.).

Figura 7

Representación de cada topología



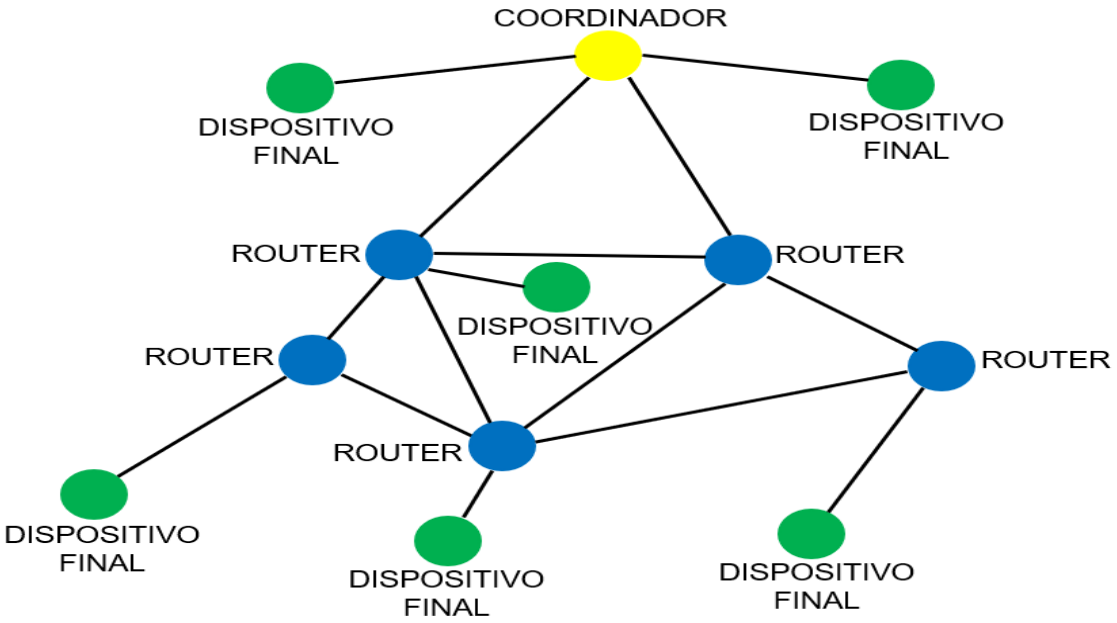
Nota. Imagen extraída de la siguiente página: https://wizzdev.com/blog/overview-of-iot-network-topologies/ (WizzDev, 2026).

En síntesis, la topología es clave para la seguridad y la privacidad porque permite aplicar controles diferenciados según la criticidad del dispositivo: cámaras y asistentes en VLAN inspeccionadas, sensores en mallas aisladas con autenticación local y puertos de enlace con gestión de claves centralizada. En este sistema se empleó la topología en malla, donde los nodos cooperan para enrutar el tráfico, incrementando el alcance efectivo y la robustez frente a fallos mediante rutas alternativas dinámicas (Zigbee Alliance, 2015).

La figura 8 muestra una representación referencial de una conexión en malla. Si bien la malla impone mayor sobrecarga en control y señalización —elevando el consumo y la latencia en escenarios densos—, sus ventajas en cobertura, resiliencia y escalabilidad la convierten en la opción adecuada para sistemas domóticos (Kumar y Mallick, 2018).

Figura 8

Ilustración de una topología en malla

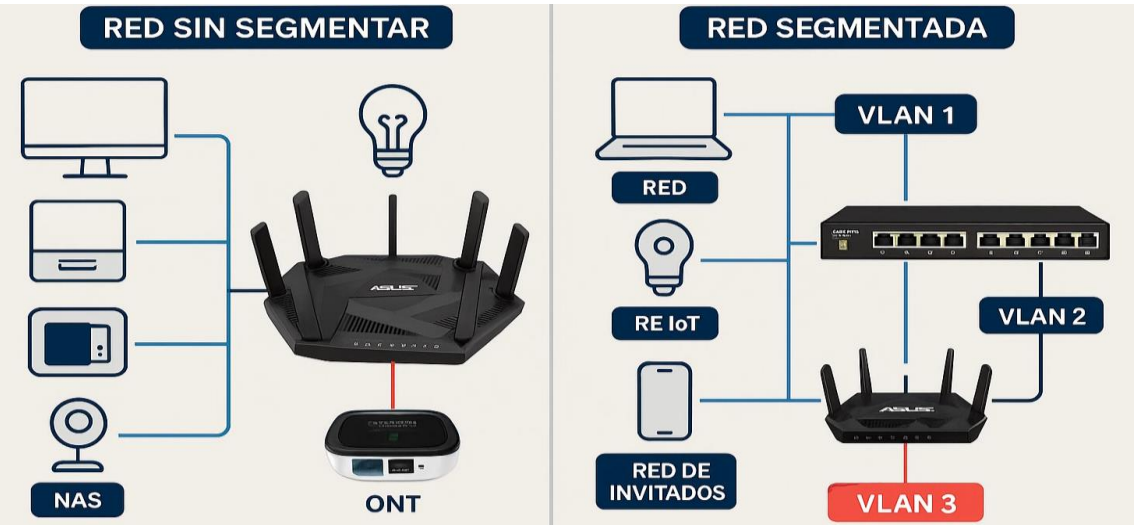


2.2.9. Segmentación de una red doméstica

La segmentación de una red doméstica es una estrategia arquitectónica que divide la infraestructura local en dominios lógicos independientes, por ejemplo: red principal, red IoT y red de invitados, para limitar el alcance de fallos y ataques, mejorar el rendimiento y facilitar la gestión (Basan, 2024). Segregar dispositivos IoT en una VLAN dedicada evita que vulnerabilidades en bombillas o cámaras comprometan equipos de trabajo o de almacenamiento, y facilita la aplicación de reglas de firewall y el control de acceso por roles, mejorando las auditorías y el cumplimiento de buenas prácticas de seguridad (DiCola, 2025). Operativamente, la segmentación mejora la eficiencia del tráfico al reducir los dominios de broadcast y permite priorizar flujos críticos sin afectar otros servicios; por ello se planificó implementar VLAN y reglas de permiso y denegación de acceso. Vidal (2023) señala: "La segmentación por routers consiste en desplegar múltiples routers o puertas de enlace que crean subredes independientes (p. ej., 192.168.1.0/24 y 192.168.18.0/24), cada una con su propio rango de direcciones y reglas de enrutamiento." Una red no segmentada o plana es aquella en la que todos los dispositivos comparten el mismo dominio de red sin restricciones lógicas, lo que implica que una vulnerabilidad en un dispositivo IoT puede permitir el acceso lateral a equipos más sensibles (Stateofsurveillance, 2025). Como muestra la figura 9, se realiza una comparación entre una red sin segmentar y una red segmentada.

Figura 9

Comparación entre una red sin segmentar y segmentada



Nota. Imagen extraída de la siguiente página: https://www.youtube.com/watch?v=vSVWuuSv09w/ (Tecnoyfoto, 2025).

La propuesta organiza dispositivos en VLANs (red principal, IoT, invitados), aplica políticas de firewall intersegmento y centraliza la gestión en un switch gestionado, limitando el movimiento lateral, priorizando flujos críticos y facilitando auditorías. Estas acciones reducen la superficie de ataque, contienen incidentes y optimizan el ancho de banda.

2.2.10. Estándar y protocolo de comunicación para cámaras

Para lograr la comunicación exitosa entre todas las marcas y el controlador central (Home Assistant), resulta imprescindible articular con precisión qué son los puertos de red, cómo operan los protocolos RTSP y ONVIF, y qué puertos deben considerarse en el diseño de red. Un puerto es la entidad lógica que, junto con una dirección IP y un protocolo de transporte (TCP/UDP), define un extremo de comunicación para un servicio concreto. En la práctica operativa de cámaras y servidores de streaming, el puerto 554 es la asignación habitual para RTSP (Touch et al., 2025).

2.2.10.1. Definición de ONVIF (Open Network Video Interface Forum)

El descubrimiento y la gestión de dispositivos ONVIF se basan en servicios web y en el descubrimiento multicast. El descubrimiento utiliza UDP 3702 para que los clientes

detecten dispositivos en la misma subred sin configuración adicional. Con VLANs, el descubrimiento no atraviesa routers por defecto, salvo que exista un reflector o un proxy de descubrimiento. Además, muchos dispositivos ONVIF exponen interfaces de gestión por HTTP/HTTPS y proporcionan URLs RTSP para el stream; por tanto, permitir el acceso a esos puertos de forma controlada es necesario para la administración remota y la orquestación (ONVIF, 2025).

2.2.10.2. Definición de RTSP (Real Time Streaming Protocol)

RTSP: Es un protocolo de control de sesiones de streaming para establecer, controlar y finalizar transmisiones en tiempo real; sus comandos PLAY, PAUSE y TEARDOWN gestionan la reproducción y negocian parámetros de transporte. El envío real de audio y vídeo se realiza típicamente mediante RTP/RTCP, que utiliza puertos UDP dinámicos negociados durante la sesión. El puerto por defecto para RTSP es el 554 (TCP y UDP), y durante la negociación RTSP se acuerdan rangos UDP dinámicos para RTP/RTCP que deben considerarse en las políticas de firewall y NAT para garantizar la entrega del flujo multimedia (Schulzrinne, 2003). En implementaciones domésticas y profesionales, la coexistencia de RTSP con RTP exige que las políticas de firewall y NAT contemplen tanto el puerto de control como los rangos UDP para el transporte de medios; véase la figura 10.

Figura 10

Sistema ONVIF y RTSP integrados

2.2.10.3. Implicaciones operativas: NAT, multicast y seguridad de puertos

Desde la perspectiva de integración con Home Assistant, los problemas en la negociación RTSP/RTP o en la resolución de descubrimiento suelen manifestarse como fallos de stream en la interfaz de usuario; por ello se recomienda validar las URLs RTSP con herramientas como VLC antes del despliegue en producción (Home Assistant, 2026). Sin embargo, desde la perspectiva operativa, según Schulzrinne et al. (1998), el uso de RTSP/ONVIF exige considerar tres aspectos principales:

- NAT y puertos dinámicos: Los puertos UDP negociados para RTP/RTCP complican la traducción en escenarios con NAT y requieren mapeos estáticos, ALG, o el uso de servidores/relays dentro de la misma red local para evitar problemas de conectividad.
- Multicast: El descubrimiento por WS-Discovery y otros mecanismos multicast no atraviesa routers entre VLANs por defecto; la segmentación por VLAN exige soluciones como reflectores/proxies de descubrimiento, túneles L2 o configuración manual de dispositivos para mantener la detección.
- Superficie de ataque: Exponer puertos de gestión (por ejemplo, 80/443) sin cifrado ni controles aumenta el riesgo. Se recomienda restringir accesos por IP, usar HTTPS, aplicar autenticación fuerte y rotación de credenciales, y documentar explícitamente los puertos permitidos en las políticas de firewall y NAT.

2.2.11. Definición de puertos en redes IP

Un puerto de red es un identificador numérico que, junto con una dirección IP y un protocolo de transporte (TCP/UDP), define un extremo lógico de comunicación para un servicio concreto. Los puertos permiten multiplexar múltiples servicios sobre una misma interfaz física y constituyen la unidad básica sobre la que se definen reglas de firewall, NAT y control de acceso (ONVIF, 2021). En sistemas de videovigilancia IP, la asignación dinámica de direcciones mediante DHCP puede provocar interrupciones en la transmisión de vídeo y en la comunicación con sistemas de gestión. La práctica recomendada es configurar direcciones IP estáticas para cámaras y servidores, garantizando que las reglas de firewall, las automatizaciones y las integraciones con software de terceros permanezcan operativas sin necesidad de ajustes manuales tras cada reinicio de red (Cisco Networking Academy, 2023).

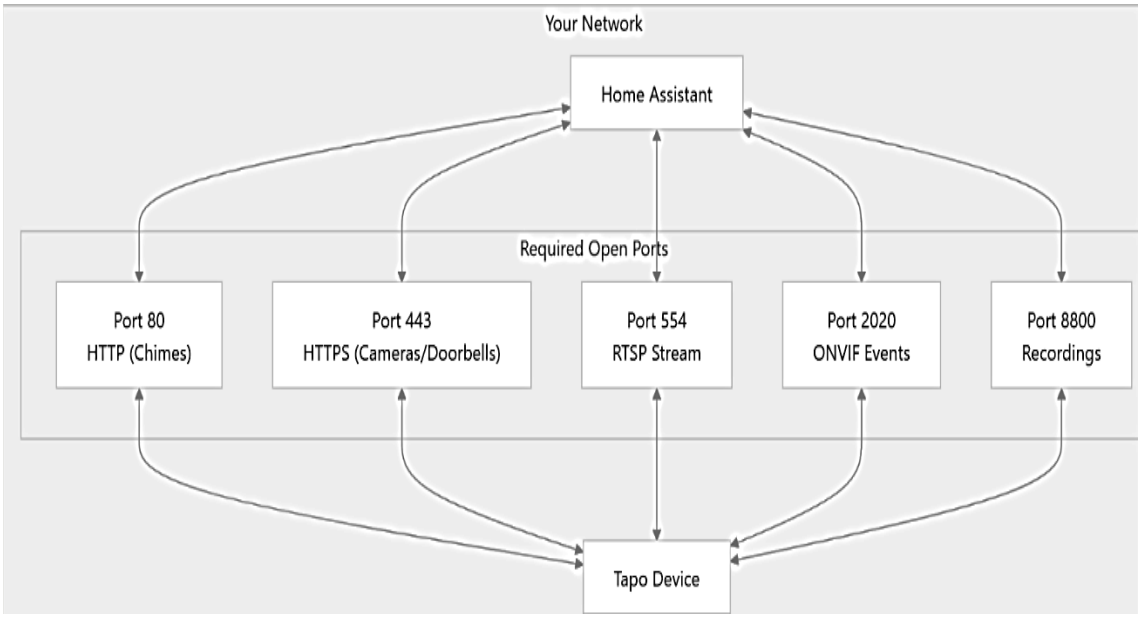
La reproducibilidad en entornos de investigación de sistemas inteligentes exige estabilidad de parámetros de red: asignar direcciones IP fijas a dispositivos IoT evita la variabilidad de las asignaciones dinámicas y permite repetir experimentos bajo las mismas condiciones. Esto es especialmente crítico en arquitecturas híbridas donde servidores locales, como Raspberry Pi, interactúan con múltiples sensores y cámaras IP, garantizando consistencia en mediciones y comunicaciones (IEEE, 2022). Teniendo en cuenta lo anterior, implementar este enfoque exige las siguientes medidas:

- Segmentación de red: Segregar dispositivos IoT de baja confianza en VLANs con enrutamiento controlado, mapeo de SSID/puertos y políticas de firewall y ACLs por puerto/servicio reduce la superficie de ataque y evita que una cámara comprometida acceda a servidores críticos (Marron et al., 2025).
- Gestión de credenciales: La gestión de credenciales debe seguir principios de privilegio mínimo y ciclo de vida seguro: provisión segura, rotación periódica, revocación y registro de uso. Complementar con autenticación basada en certificados o claves y limitar accesos (Juniper Networks, 2022).
- Pruebas y control de versiones: En entornos de laboratorio que reproduzcan la topología (VLANs, trunking, DHCP), realizar pruebas de conectividad (ping, traceroute), pruebas de servicios (RTSP/554, endpoints ONVIF), escaneo de puertos y análisis de vulnerabilidades (Cloud Optics, 2026).

Chris (2024) señala que, si se implementan estas salvaguardas, los beneficios operativos y de automatización en Home Assistant justifican su uso; en caso contrario, conviene mantener la integración estándar para no comprometer la seguridad y la estabilidad. Comprender la comunicación y el papel de los puertos es clave para integrar correctamente dispositivos Tapo de videovigilancia; la figura 11 complementa esta información.

Figura 11

Arquitectura de comunicación y puertos requeridos para la integración de dispositivos Tapo con Home Assistant

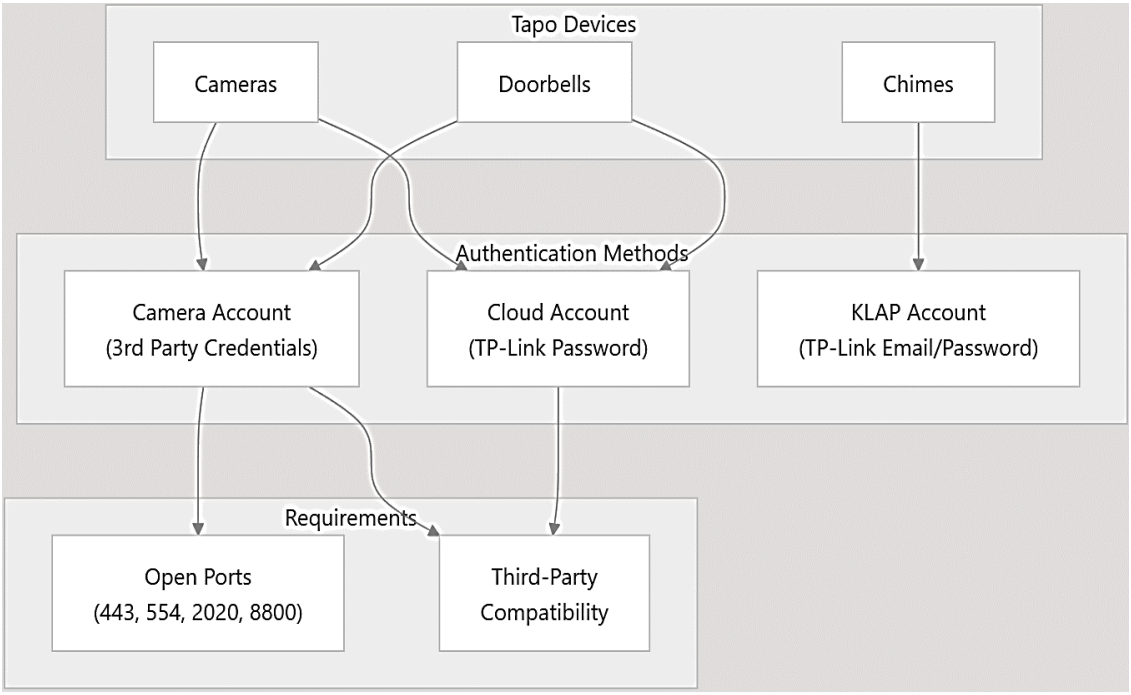


Nota. Imagen extraída de la siguiente página: https://deepwiki.com/JurajNyiri/HomeAssistant-Tapo-Control/2-installation-and-setup (JurajNyiri, 2025).

Un puerto es un identificador numérico que, junto con una dirección IP y un protocolo de transporte (TCP/UDP), define un extremo lógico de comunicación para un servicio. En videovigilancia, los puertos distinguen control de dispositivo, streaming y descubrimiento; su gestión evita colisiones y facilita la definición de políticas de firewall y NAT. Por ejemplo, en la red local Tapo, el control y streaming pueden emplear los siguientes puertos: TCP/UDP 554 (RTSP), TCP 443, TCP 2020 y TCP 8800. Estos puertos son internos y no deben exponerse a Internet mediante redirección de puertos. Abrirlos únicamente en la VLAN o segmento de las cámaras permite que Home Assistant acceda al streaming, a los eventos y a la sincronización de forma local, reduciendo la dependencia de la nube y minimizando la superficie de ataque. La Figura 12 muestra un diagrama extraído del sitio web del fabricante que resume los métodos de autenticación y los requisitos de red asociados a la familia de dispositivos Tapo (cámaras, timbres y chimes).

Figura 12

Relación entre dispositivos Tapo, métodos de autenticación y requisitos de conectividad



Nota. Imagen extraída de la siguiente página: https://deepwiki.com/JurajNyiri/HomeAssistant-Tapo-Control/2-installation-and-setup (JurajNyiri, 2025).

Dejar claro qué credenciales emplea cada tipo de dispositivo, qué servicios y puertos deben estar disponibles en la red local y qué implicaciones tiene esto para integraciones de terceros. Además, enfatiza la compatibilidad con terceros (Third-Party Compatibility), que depende tanto de la exposición de puertos locales como de la existencia de APIs públicas o mecanismos de autenticación que permitan a integradores externos operar sin pasar exclusivamente por la nube (JurajNyiri, 2025). El gráfico organiza la información en tres capas: dispositivos, métodos de autenticación y requisitos.

- 443: Puerto que permite comunicaciones seguras con la nube y con las APIs; es habitual para autenticación y gestión cifrada. Mantenerlo saliente es necesario para integraciones HTTPS del fabricante.
- 554: Puerto por defecto para control y consumo de streaming (RTSP); necesario para que clientes locales o NVR obtengan el flujo. Su disponibilidad en la red local permite que Home Assistant y otros sistemas accedan al stream sin pasar por la nube.

- 2020: Puerto usado por algunos fabricantes para control, APIs alternativas, ONVIF o eventos; si la integración o un componente comunitario lo requiere, debe estar accesible únicamente en la VLAN o segmento de las cámaras.
- 8800: Puerto asociado a streaming propietario y a sincronización/telemetría; su apertura local facilita funciones avanzadas sin exponerlo a Internet.

2.2.12. Control y acceso remoto

2.2.12.1. VPN Tailscale

Tailscale implementa una VPN en malla basada en WireGuard que interconecta nodos con direcciones internas y cifrado, evitando exponer Home Assistant al Internet público. Añade un plano de control que automatiza la distribución de claves, la resolución de identidad y el NAT traversal, reduciendo la carga operativa en despliegues con múltiples dispositivos (Tailscale, 2026). Desde la teoría de sistemas distribuidos, la conectividad segura y la tolerancia a fallos siguen principios de redundancia y minimización de puntos de fallo; topologías en malla y túneles cifrados aumentan la resiliencia de la domótica, mejorando la disponibilidad y el rendimiento en Raspberry Pi y servidores. La estrategia de acceso remoto debe evitar exponer servicios críticos, emplear autenticación fuerte (por ejemplo, la que ofrece Tailscale) y aplicar políticas de respaldo y control de versiones (Morgado, 2025). Operar WireGuard directamente ofrece mayor control y soberanía sobre la conectividad. Su funcionamiento es el siguiente:

- Cada dispositivo con Tailscale recibe una IP única en la red privada (100.88.x.x) y un nombre DNS interno (MagicDNS), lo que permite al celular identificar y localizar el servidor sin depender de la IP pública del ISP.
- Tailscale utiliza WireGuard para crear túneles seguros punto a punto; si ambos extremos están detrás de NAT, Tailscale intenta establecer una conexión directa mediante técnicas de NAT traversal.
- Una vez conectado, el dispositivo móvil puede acceder a los servicios que se ejecutan en el servidor; Tailscale proporciona la conectividad, no los servicios en sí.

Esta solución es especialmente valiosa en entornos domésticos con CGNAT (Carrier Grade NAT), donde varios clientes comparten una dirección IP pública y el reenvío de puertos desde Internet hacia servicios locales suele ser inviable (Zapatero, 2025). Las ventajas principales incluyen:

- No requiere abrir puertos ni configurar DDNS.
- Funcionamiento incluso bajo CGNAT, problema común varios países.
- Proporciona seguridad multicapa: cifrado extremo a extremo, control de acceso y autenticación centralizada.
- Instalación y uso sencillos en Android/iOS y Linux/Windows, sin configuraciones manuales complejas de túneles.

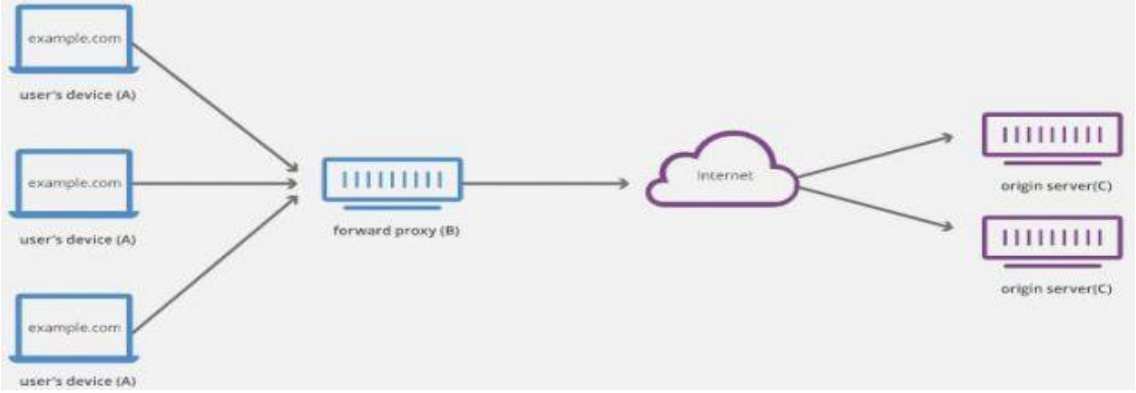
2.2.12.2. Proxy inverso Cloudflare

Cloudflare y proxy inverso: Cloudflare actúa como proxy inverso y capa de seguridad en el borde de Internet, acelerando y protegiendo sitios y aplicaciones. Su uso es especialmente útil para quienes necesitan HTTPS, mitigación DDoS y acceso remoto seguro sin exponer servidores locales. Un proxy inverso centraliza la terminación TLS —gestiona certificados y cifra el tráfico público—, lo que permite que Home Assistant opere en HTTP interno sin gestionar certificados por separado (Pastor, 2019).

Al centralizar la terminación TLS, el proxy obtiene y renueva certificados y cifra el tráfico público, reduciendo errores y facilitando la administración de seguridad. Además, al ser un único punto de entrada puede alojar múltiples servicios bajo el mismo dominio y puertos estándar (80/443), ocultar las IP reales, aplicar filtros y bloquear tráfico malicioso antes de que llegue a Home Assistant. Esto disminuye el riesgo de explotación directa y facilita la auditoría y el registro centralizado de accesos.

Figura 13

Esquema sobre el funcionamiento de un proxy inverso



Nota. Imagen extraída de la siguiente página: https://www.redeszone.net/tutoriales/servidores/diferencias-proxy-vs-proxy-inverso/ (Fernández, 2026).

Ilustrado en la figura 13, un proxy inverso reenvía solicitudes del cliente al servidor de origen, actuando como capa intermedia que mejora la seguridad, el rendimiento y la fiabilidad en la entrega de contenido. Se sitúa delante de uno o varios servidores web e intercepta las solicitudes de los clientes (Cloudflare, 2024). Los beneficios principales incluyen:

- Protección ante ataques: no se revela la dirección IP real del servidor web, dificultando ataques como DDoS (Fernández, 2026).
- Equilibrio de carga global del servidor (GSLB): distribuye las solicitudes entre servidores a nivel global para reducir los tiempos de carga para usuarios en diferentes zonas horarias (MiniOrange, 2026).
- Balanceo de carga: distribuye la carga de las solicitudes web en varios servidores para evitar la sobrecarga (Fernández, 2026).
- Cifrado SSL: el proxy inverso cifra y descifra las comunicaciones, aliviando la carga computacional del servidor de origen y reduciendo la latencia (MiniOrange, 2026).

En conclusión, Cloudflare, como proxy inverso, centraliza y simplifica la gestión de TLS y certificados, ofreciendo HTTPS automático y protección en el borde. Actúa como puerta de entrada segura que oculta el origen y facilita el enrutamiento de múltiples servicios bajo un mismo dominio.

2.3. Definición de términos

2.3.1. Sensores

Un sensor es todo elemento o dispositivo que presenta una propiedad sensible a una determinada magnitud física. Cuando esa magnitud se modifica, la propiedad cambia sus características. (GISI, 2018).

2.3.2. Domótica

Se denomina domótica al conjunto de técnicas y sistemas que permiten la automatización de las distintas instalaciones de una vivienda. La domótica no solo ayuda a mejorar el bienestar, sino que también brinda mayor seguridad y contribuye a ahorrar energía (Pérez y Merino, 2025).

2.3.3. Seguridad domótica

También denominada seguridad del hogar inteligente, es el conjunto de tecnologías y sistemas empleados para proteger una vivienda mediante la integración de dispositivos y sistemas electrónicos conectados a la red (Viserco, 2023).

2.3.4. Interfaces de usuario

Es el medio de interacción entre humanos y sistemas digitales que determina la apariencia, la usabilidad y la interactividad de aplicaciones o sitios web. (Coursera, 2023).

2.3.5. Redes de comunicación en domótica

Las redes de comunicación en sistemas de domótica están compuestas por protocolos y tecnologías que permiten la interconexión de distintos dispositivos de automatización del hogar (Jaihar, 2020).

2.3.6. NAT

Técnica que permite traducir direcciones IP, de modo que redes privadas queden enmascaradas tras una dirección IP pública; es fundamental para la gestión del acceso remoto y la seguridad de redes domésticas (Prieto et al., 2025).

2.3.7. Nikto

Es una herramienta de escaneo de vulnerabilidades para servidores web que examina archivos y servicios en busca de amenazas y configuraciones inseguras. Ofrece soporte para SSL/TLS y genera informes detallados en varios formatos (Campoverde, 2020).

2.3.8. Zigbee

Protocolo inalámbrico de bajo consumo basado en IEEE 802.15.4, diseñado para redes de sensores y para la automatización doméstica. Opera principalmente en la banda de 2,4 GHz, aunque también puede funcionar en otras frecuencias (Camargo et al., 2013).

2.3.9. WiFi

Tecnología de red inalámbrica que permite la transmisión de datos a alta velocidad, basada en el estándar IEEE 802.11. Su uso en domótica es frecuente, aunque con un mayor consumo energético (Chakkor et al., 2014).

2.3.10. Interoperabilidad

Capacidad de diferentes dispositivos, marcas o sistemas para funcionar de manera conjunta y eficiente. Su ausencia genera problemas de sincronización, latencia y pérdida de paquetes (Madadi et al., 2024).

2.3.11. Saturación

Estado de una red en el que ya no puede manejar más dispositivos o datos sin que se generen errores, retardos o pérdida de rendimiento (Ahmad et al., 2023).

2.3.12. Retardo

Tiempo que transcurre desde que se envía una señal hasta que se ejecuta una acción. En redes domóticas, depende del protocolo, de la topología y de la carga de dispositivos (Torres, 2008).

2.3.13. Servicio en la nube Cloudflare

Red perimetral global que enruta y optimiza el tráfico web mediante servidores y túneles seguros; ofrece caché, balanceo de carga, mitigación DDoS y terminación TLS. Facilita el acceso remoto sin exponer puertos, gestionando el cifrado y los certificados (Jaisudthi, 2025).

2.3.14. Cloudflare Zero Trust

Elimina la confianza implícita, verificando la identidad y el contexto en cada solicitud; aplica políticas, autenticación multifactor y control continuo de acceso. Centraliza la verificación y las políticas, reduce la superficie de ataque y mejora la auditoría (Jaisudthi, 2025).

2.3.15. Configuración de VPN (Tailscale basado en WireGuard)

WireGuard es un protocolo VPN moderno, ligero y seguro. Tailscale, al integrar este protocolo, proporciona una red en malla segura y gestionada, ideal para equipos distribuidos, y reduce la complejidad técnica (Escobedo y Quispe, 2025).

2.3.16. Bloqueo de anuncios

Solución de DNS local que bloquea anuncios, rastreadores y contenido inapropiado a nivel de red. Permite filtrado familiar, gestión de listas, mejora la privacidad y la seguridad al interceptar solicitudes DNS antes de que alcancen servidores externos. (Hermawan et al., 2021).

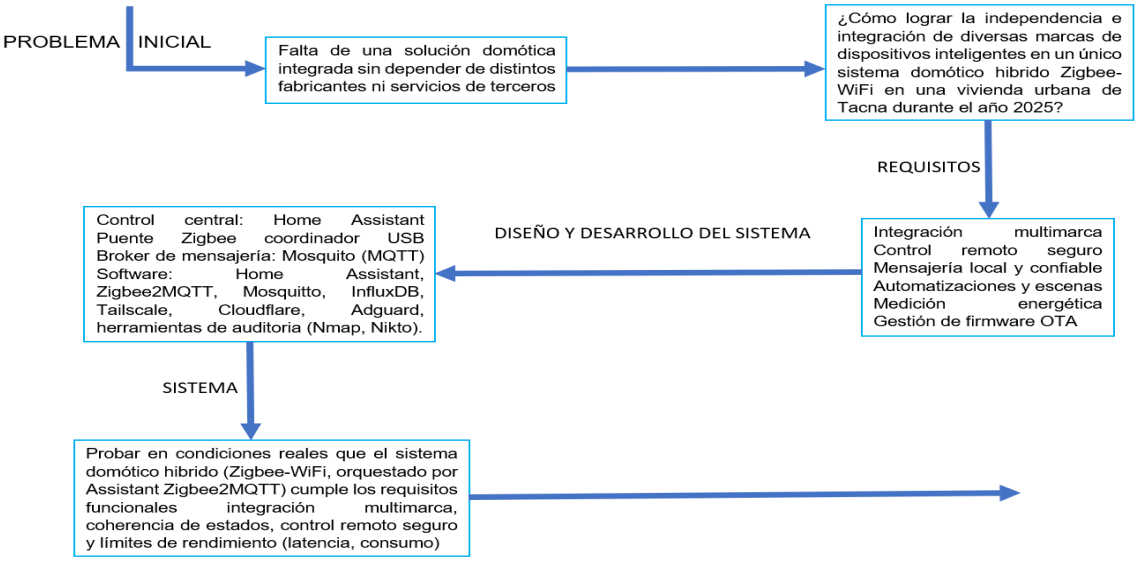
CAPÍTULO III: MARCO METODOLÓGICO

3.1. Diseño de la investigación

La investigación es experimental, su propósito es construir, implementar y evaluar un sistema domótico híbrido Zigbee–WiFi y explicar las relaciones causales entre la marca de dispositivos y las variables como: latencia, consumo energético, interoperabilidad, estabilidad y seguridad. Se adopta un enfoque orientado a diseñar un sistema útil y evaluarlo en condiciones reales, manteniendo trazabilidad entre requisitos, decisiones de diseño y evidencia empírica. Este enfoque permite replicabilidad y rigor, cumpliendo criterios de validez interna mediante la comparación sistemática entre protocolos, marcas y cargas, con un control operacional sobre las condiciones experimentales y la recolección de datos empíricos precisos. Partiendo desde la falta de una solución domótica integrada independiente de distintos fabricantes ni servicios de terceros, tal como se muestra en la figura 14.

Figura 14

Descripción general del marco metodológico



El problema es la ausencia de una solución domótica integrada, interoperable y segura que permita controlar remotamente en Tacna sin depender de hubs propietarios ni de la heterogeneidad de marcas. En la práctica, dispositivos de distintos fabricantes no mantienen coherencia de estados, sufren retrasos o fallos de ejecución, consumen

energía ineficientemente y aumentan la exposición a riesgos. Esto provoca latencias elevadas y variabilidad en automatizaciones; obliga al uso de adaptadores o puentes propietarios que incrementan coste y complejidad; eleva el consumo energético; y genera riesgos de seguridad al exponer hubs o servicios a Internet sin una arquitectura centralizada. La tesis propone diseñar, implementar y evaluar un sistema híbrido Zigbee-WiFi con Home Assistant, Zigbee2MQTT, broker MQTT y capa de seguridad para integración independiente de marcas, rendimiento y acceso remoto seguro. En cuanto a los principales requisitos funcionales que se buscan lograr dentro del sistema se encuentran los siguientes:

- Integración multi marca: Permitir emparejar y controlar dispositivos Zigbee y WiFi de diversas marcas desde una sola plataforma Home Assistant + Zigbee2MQTT.
- Control remoto seguro: Acceso remoto cifrado para control y monitoreo (red privada virtual Tailscale o canal HTTPS mediante Cloudflare).
- Mensajería local: Broker MQTT (Mosquitto) para publicar/suscribirse a estados.
- Sincronización de estados: Coherencia entre interfaces (UI móvil, UI web, dispositivo físico) garantizada en un porcentaje mayor al 95 % de las acciones.
- Automatizaciones y escenas: Creación, ejecución y registro de automatizaciones secuenciales y condicionales (temporizadores, reglas basadas en sensores).
- Medición energética: Registrar consumo por dispositivo/escenario, cálculo comparativo entre escenarios anteriores y actuales, inclusión de system monitor.
- Auditoría y logging: Captura y almacenamiento de logs de eventos, comandos, errores y telemetría con retención configurable.
- Gestión de firmware: Procedimiento controlado de manera personal para actualizar firmwares sin degradar la red Zigbee.
- Interfaces de prueba automatizada: scripts para ejecutar escenarios experimentales y generar evidencia reproducible.

- Control de acceso: Autenticación robusta (usuarios con credenciales fuertes y roles mínimos), IPBan (ip_ban_enabled) para mitigar intentos de fuerza bruta.
- Aislamiento de red: Segmentación lógica entre dispositivos IoT y red de gestión; Adguard Home para filtrar dominios maliciosos.
- Monitoreo y respuesta: Escaneos (Nmap/Nikto) y procedimientos de mitigación documentados; backups automáticos y plan de rollback.
- Gestión de claves: Almacenamiento seguro de claves privadas y rotación planificada.

Además de los requisitos, se adopta el diseño explicativo experimental. Según Hernández (2009) el diseño explicativo experimental es apropiado cuando se busca establecer relaciones de causa-efecto bajo condiciones controladas. Se implementó un sistema híbrido Zigbee-WiFi sobre una Raspberry Pi 4 con Home Assistant para controlar y registrar eventos en tiempo real. El hardware incluirá Raspberry Pi 4, coordinador Zigbee USB, bombillas, enchufes, válvulas de diversas marcas. En software, la plataforma principal será Home Assistant; Zigbee2MQTT gestionará la comunicación entre dispositivos; además se usarán Mosquitto, system monitor, Tailscale y AdGuard Home, junto a herramientas de auditoría (Nmap, Nikto) y scripts MQTT para despliegue y pruebas automatizadas.

La decisión de diseño de usar Zigbee2MQTT + Mosquitto busca independencia de hubs propietarios y visibilidad completa de tópicos y estados, centralizando en Home Assistant la orquestación, trazabilidad e integración con automatizaciones y la interfaz. Se prioriza el control local y se expone acceso remoto solo mediante túnel VPN y un proxy inverso con TLS para reducir la superficie de ataque; además se añaden AdGuard e IPBan como capas de defensa pasiva y detección temprana de anomalías. El control central será una instancia local de Home Assistant sobre Raspberry Pi 4, con un coordinador USB que traduce la malla Zigbee a tópicos MQTT; Mosquitto actuará como broker local para comunicación confiable entre dispositivos y controlador. En ciberseguridad se integran telemetría y visualización con system monitor, acceso remoto seguro con Tailscale, interfaz web protegida por Cloudflare + Zero Trust, y mitigaciones de privacidad y fuerza bruta con AdGuard e IPBan. Para pruebas y verificación se plantea realizar lo siguiente:

- Pruebas unitarias: emparejado y comandos simples por dispositivo; verificación de MQTT y latencia básica.

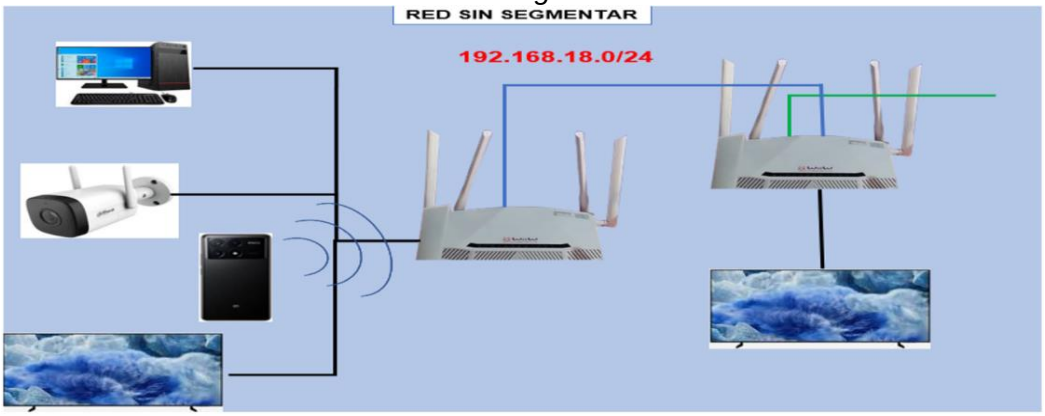
- Pruebas de integración: secuencias de automatización complejas y medición de coherencia de estados.
- Pruebas de carga/saturación: scripts que generan tráfico concurrente sobre WiFi y Zigbee para medir retardo y pérdida.
- Auditoría de seguridad: escaneo Nmap/Nikto; controles de mitigación aplicados y re-evaluados.

3.1.1. Diseño de arquitectura de la red doméstica

Como se mencionó previamente, es muy importante designar la segmentación de una red, por lo que a continuación, en la figura 15 se verá un ejemplo práctico de una red sin segmentar con rango 192.168.18.0/24 y las consecuencias de mantener todos los equipos en la misma red: equipos de escritorio, cámaras, televisores inteligentes y routers comparten el mismo dominio de difusión y las mismas políticas, lo que facilita que una vulnerabilidad en un dispositivo IoT comprometa recursos sensibles, aumente la probabilidad de exfiltración de datos y provoque congestión por tráfico no diferenciado; además, la ausencia de aislamiento complica la aplicación de controles granulares y la detección temprana de anomalías. La configuración contrasta mantener todos los dispositivos en una sola red o dividirlos en segmentos lógicos: una red principal para equipos de trabajo y críticos y una VLAN dedicada a IoT. En ella conviven escritorio, televisores, celulares y dispositivos inteligentes, gestionados por un router y un switch gestionado que aplica reglas entre segmentos, controla movimiento lateral y prioriza tráfico. Esto reduce la superficie de ataque, facilita contención de incidentes, mejora visibilidad y auditoría del tráfico y permite políticas diferenciadas de calidad de servicio y acceso.

Figura 15

Ilustración de la red de la vivienda sin segmentar

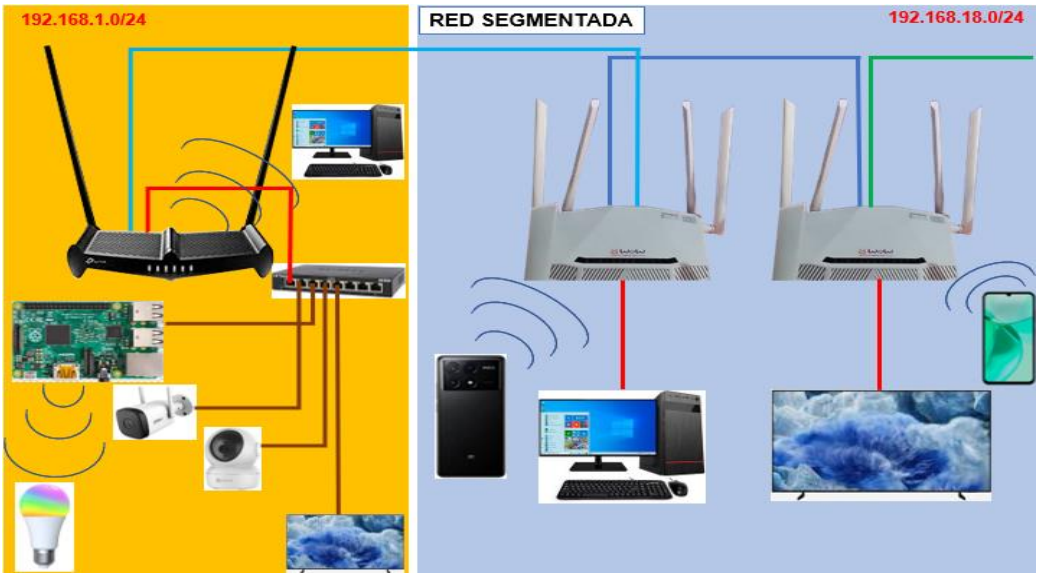


La figura 16 continúa y concreta esa estrategia al presentar dos subredes claramente separadas —una 192.168.1.0/24 con dispositivos generales y otra 192.168.18.0/24 con equipos aislados—, apoyada por routers y un esquema de enrutamiento que mantiene la comunicación controlada entre dominios. Aquí se observa una separación física y lógica más marcada: dispositivos de uso cotidiano y servicios internos quedan en un segmento, mientras que equipos móviles y entretenimiento se ubican en otro, reduciendo interferencias y limitando la exposición de recursos sensibles.

La transición de la propuesta inicial a la implementación actual muestra coherencia operativa: las VLANs y el switch gestionado se materializan en subredes que permiten firewalls intersegmento. La arquitectura final corrige debilidades de la topología monolítica —movimiento lateral, dificultad de auditoría y congestión— y aplica las medidas recomendadas: segmentación, control de acceso, endurecimiento de credenciales y mantenimiento de firmware, equilibrando usabilidad doméstica con controles de seguridad profesional.

Figura 16

Ilustración de la red de la vivienda segmentada

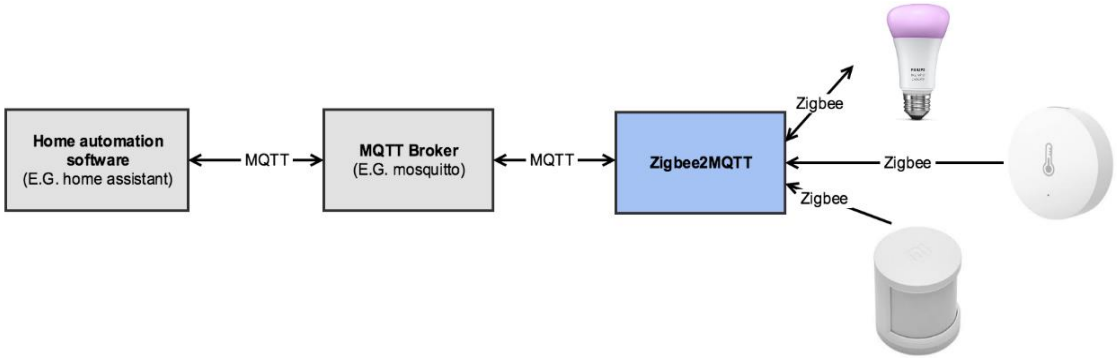


La comunicación se organiza en capas donde los mensajes viajan desde los dispositivos Zigbee hasta la plataforma de automatización a través de un puente y un broker MQTT. A continuación, se describen las etapas principales, las cuales además se encuentra en la figura 17:

- Dispositivos Zigbee a Zigbee2MQTT: los dispositivos Zigbee envían tramas al coordinador; Zigbee2MQTT traduce esos eventos a mensajes MQTT publicados en topics específicos.
- Protocolo Zigbee2MQTT a Mosquitto: Zigbee2MQTT actúa como cliente MQTT y publica estados y suscribe a topics de control en el broker.
- Mosquitto a Home Assistant: Home Assistant se suscribe a los topics relevantes en el broker para recibir estados y publica comandos que Zigbee2MQTT retransmite a los dispositivos Zigbee.
- Las flechas bidireccionales representan este intercambio continuo de mensajes (comandos y estados) usando el modelo publish/subscribe.

Figura 17

Diagrama de comunicación entre Home Assistant y Zigbee2MQTT



Nota. Imagen extraída de la siguiente página: https://www.desdeelreloj.com/e0197/ (DER, 2021).

Algunos detalles operativos a considerar son que los eventos de sensores se publican en topics con un base_topic y subtopics por dispositivo y tipo de dato, además, los comandos generados por la plataforma se publican en topics de control; el puente los traduce a comandos Zigbee y los envía al dispositivo objetivo. Y por último el broker aplica políticas de QoS, retención y autenticación para garantizar entrega fiable y seguridad.

3.1.2. Diseño de una red domótica usando Zigbee2MQTT

Para utilizar un conmutador que gestione toda la red Zigbee, mediante la comunicación MQTT, en Home Assistant para poder gestionar la red Zigbee, para administrar, actualizar, integrar, eliminar, actualizar dispositivos Zigbee para verlos desde Home

Assistant, en síntesis, un “software de control”, siendo ZHA (Zigbee Home Automation) y Z2M (Zigbee2MQTT) las principales opciones, “La integración de ZHA es una implementación de puerta de enlace Zigbee independiente del hardware que puede reemplazar la mayoría de las puertas de enlace Zigbee propietarias, (...) ZHA crea una única red Zigbee a la que se pueden agregar la mayoría de los dispositivos basados en Zigbee.” (Home Assistant, 2025).

Según Tongou (2024), Zigbee2MQTT es un proyecto de código abierto que actúa como puente entre dispositivos Zigbee y el protocolo MQTT, permitiendo que esos dispositivos se comuniquen con un broker MQTT e integrarse con plataformas de domótica como Home Assistant. Se eligió Zigbee2MQTT por su mayor compatibilidad con dispositivos Zigbee frente a ZHA, que incorpora menos entidades y soporta menos modelos. Aunque Z2M exige pasos adicionales respecto a ZHA, ofrece mayor potencia y flexibilidad, facilitando la incorporación progresiva de nuevos dispositivos al ecosistema y mejora la escalabilidad del sistema.

Tabla 2

Comparación entre Zigbee Home Automation y Zigbee2MQTT

Característica	ZHA (Zigbee Home Automation)	Zigbee2MQTT (Z2M)
Facilidad de configuración	Fácil (conectar y usar)	Requiere configuración manual
Compatibilidad de dispositivos	Limitada	Amplia (más de 3000 dispositivos)
Personalización	Configuración básica	Controles de red avanzados
Tipo de integración	Directo en Home Assistant	Utiliza el bróker MQTT
Registro y depuración de red	Limitado	Registros detallados y herramientas de depuración
Actualizaciones de firmware para dispositivos	No integrado	Posible para muchos dispositivos
Rendimiento	Baja latencia	Eficiente, pero con sobrecarga de MQTT

Nota. Adaptado de Wendy (2025) del sitio web https://www.sonoff.in/blog/smart-home-tips-2/zha-vs-zigbee2mqtt-the-best-zigbee-integration-for-home-assistant-17?srsltid=AfmBOor2ouvuhc90fxcaoOLSOQgGDglTdXHmd7A-zA3O02zN3ArxqOvK

Es importante decidir cuál de las dos opciones se empleará, porque de ello depende el tipo de hardware usado como coordinador que gestionará la red. El

coordinador o hub enlaza todos los dispositivos Zigbee y establece la comunicación con el servidor de Home Assistant; por él llegan los datos Zigbee que luego gestionamos y por él salen las órdenes hacia los dispositivos. En el mercado existen hubs de varios fabricantes; por ejemplo, AQARA E1 Zigbee o SONOFF Bridge Pro, y también coordinadores neutrales no ligados a un fabricante. Estos coordinadores neutros permiten integrarlos directamente en Home Assistant sin recurrir a integraciones propietarias, simplificando la gestión y reduciendo dependencias de marca. Así se mejora interoperabilidad, mantenimiento y seguridad del sistema. Ahora, existen varios fabricantes de radios Zigbee, entre los cuales se encuentran los siguientes: Texas Instruments, Silicon Labs y deCONZ (combi).

En líneas generales los tres fabricantes pueden funcionar tanto con Zigbee2MQTT y con ZHA, sin embargo la propia página oficial de Home Assistant, recomienda para el uso de ZHA radios Zigbee que cuenten el chip EFR32MG21 elaborado por el fabricante Silicon Labs (Home Assistant, 2024) y para el uso de Zigbee2MQTT, la propia página oficial de este software recomienda radios Zigbee con chip CC2652P elaborado por el fabricante Texas Instruments (Zigbee2MQTT, 2025), para el caso de deCONZ, la misma página de Home Assistant recomienda en específico el modelo ConBee III elaborado por el fabricante Dresden Elektronik (Home Assistant, 2024).

Para cada recomendación existen muchos modelos y variantes, sin embargo, la elección de utilizar el software Zigbee2MQTT redujo considerablemente las opciones de concentradores, enfocando únicamente en hubs con el chip CC2652P, existiendo coordinadores como: Dongle-P, SLZB-06, entre otros. Los puntos que me llevaron a preferir un hardware como el coordinador USB Dongle-P, fueron las siguientes:

- Simplicidad: Solo requiere conectar por USB y funciona de inmediato con Home Assistant y Zigbee2MQTT.
- Economicidad: Es más barato y fácil de conseguir, una diferencia económica aproximadamente de 35 dólares (AliExpress, 2026).
- Compatibilidad inmediata: Es un coordinador muy recomendado y usado en la comunidad, con soporte oficial y amplia documentación (VueVille, 2025).
- Estabilidad en grandes redes Zigbee: Usuarios reportan que Dongle-P gestiona más de 70 dispositivos sin problemas y admite nuevos Zigbee (Reddit, 2024).

En conclusión, Zigbee2MQTT permite integrar dispositivos Zigbee de múltiples marcas en un único broker MQTT, ofreciendo interoperabilidad y evitando depender de hubs propietarios. Al ser open source y ejecutarse localmente, da control total sobre los datos y la red, mejorando privacidad y reduciendo la dependencia de la nube. Su compatibilidad con Home Assistant y otros sistemas domóticos facilita automatizaciones robustas y flexibles sin protocolos cerrados.

3.1.3. Planos de la vivienda

Incluir el plano del hogar como base del diseño domótico es fundamental: convierte decisiones intuitivas en decisiones basadas en evidencia espacial. Con la planta se modela la topología, se identifican muros, materiales y obstáculos que afectan la propagación Zigbee y se planifica la ubicación de repetidores para garantizar cobertura homogénea. Esto evita pruebas y errores costosos, reduce dispositivos necesarios y permite estimar rutas entre coordinador, routers y nodos finales. Además, facilita crear zonas lógicas para segmentar la red y priorizar tráfico crítico. La literatura y guías comunitarias recomiendan mapear el entorno antes de añadir routers para optimizar la malla y minimizar saltos, latencia y fallos (Hedda, 2024).

El plano facilita la planificación eléctrica y la alimentación de repetidores Zigbee que requieren suministro permanente, como enchufes inteligentes que actúan como routers. Con la planta se ubican puntos de alimentación, se prevén canalizaciones y se decide dónde instalar regletas o tomas dedicadas para evitar sobrecargas y minimizar cables visibles. Planificar así evita soluciones improvisadas que degradan la fiabilidad, facilita la coordinación con electricistas y la documentación para mantenimiento. Integrarlo en obra o remodelación reduce retrabajos y asegura posiciones óptimas para la malla Zigbee (Hedda, 2022).

Una interfaz basada en la planta permite identificar rápidamente qué repetidor o sensor falla y actuar desde el mapa, simplificando la gestión para usuarios; sin embargo, los planos contienen información sensible sobre distribución y hábitos, por lo que es imprescindible aplicar controles de acceso, cifrado y políticas de compartición (SmartHomeScene, 2025). En las figuras 18, 19 y 20, se muestran los planos del primer y segundo piso de la vivienda trabajada, presentando primero el plano base.

Figura 18

Plano del segundo piso

Figura 19

Plano del segundo piso (dormitorio Rocio, lavandería y tendedero)

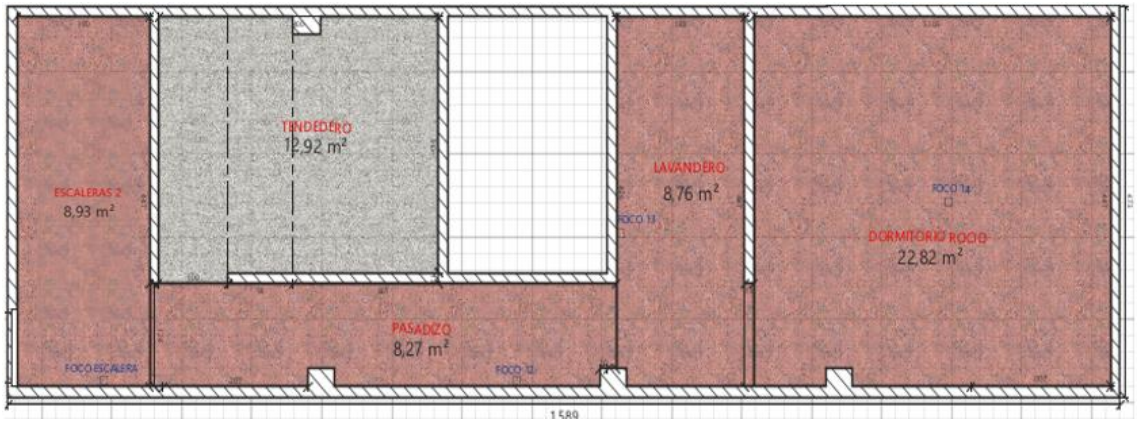


Figura 20

Plano del primer piso (sala y garaje)

3.1.4. Multicopias de seguridad

Las copias de seguridad múltiples en Home Assistant garantizan resiliencia, continuidad y trazabilidad en sistemas domóticos críticos. Un único respaldo puede corromperse o perderse, exponiendo la infraestructura. Se recomienda la regla 3-2-1: mantener tres copias, en dos medios distintos y una fuera de sitio. Este enfoque reduce la probabilidad de pérdida total y asegura la recuperación ante contingencias (Pearson, 2025).

El mantenimiento de copias distribuidas mitiga errores humanos por cambios en configuraciones YAML o integraciones, facilitando restaurar estados. Este principio se alinea con prácticas de versionado y auditoría en sistemas distribuidos, donde la trazabilidad de cambios es crítica para la confiabilidad. “Los sistemas distribuidos requieren mecanismos de redundancia y versionado que permitan recuperar estados consistentes ante fallos o modificaciones erróneas” (Van Steen y Tanenbaum, 2023). Además, las multicopias aportan documentación, permiten comparar configuraciones, justificar decisiones técnicas y auditar la evolución de la infraestructura domótica.

La resiliencia ante ataques, corrupción de datos o fallos de actualización se refuerza diversificando copias en medios locales, externos y remotos. Este enfoque aplica el principio de redundancia, fundamento de la confiabilidad en sistemas complejos (Patterson y Hennessy, 2021). En Home Assistant su implementación es indispensable para garantizar continuidad y recuperación operativa del sistema.

3.2. Acciones y actividades

3.2.1. Metodología

Se empleó una metodología cuantitativa por su aplicabilidad en ciencias naturales y sociales para analizar fenómenos observables mediante estadísticas, computación y matemáticas; las mediciones se realizan con expresiones matemáticas complejas. Se estructura en tres fases secuenciales que permiten planificar, ejecutar, registrar y analizar rigurosamente la influencia de la variable independiente (marca) sobre rendimiento técnico, interoperabilidad y seguridad de un sistema domótico híbrido Zigbee-WiFi. Esta estructura asegura control experimental, reproducibilidad de resultados, validez interna del estudio y facilita la comparación entre configuraciones.

- Fase I: Diagnóstico inicial, levantamiento de condiciones de la vivienda seleccionada (infraestructura eléctrica, cobertura de red, interferencias WiFi).

- Fase II: Instalación e integración del sistema, implementación de Home Assistant sobre Raspberry Pi 4, con integración de dispositivos Zigbee y WiFi.
- Fase III: Ejecución experimental y recolección de datos, medición de indicadores como tiempo de retardo, consumo energético, saturación del sistema, interoperabilidad y vulnerabilidad. Las pruebas se realizarán en distintos horarios para reflejar variabilidad real de red.

3.3. Materiales y/o instrumentos

El enfoque principal se desempeñó en realizar una cobertura en todo el domicilio, es por ello que se utilizó en su mayoría dispositivos repetidores de señal como se muestran en la tabla 3:

Tabla 3
Características de los equipos a utilizar para la implementación del diseño domótico

	Nombre del equipo	Marca	Modelo	Funcionalidad
1	Nodo principal	Raspberry Pi	Raspberry Pi 4 Modelo B (4 GB de RAM)	Dispositivo central del sistema domótico; incluye caja con ventilador, fuente, tarjeta SD precargada, cable HDMI, guía rápida, bolsa y adaptador SD-USB oficial (Raspberry Pi, 2026).
2	Router	TP-LINK	TL-WR841HP	Router inalámbrico de alta potencia, ideal para llevar señal a zonas difíciles atravesando paredes y obstáculos (Tp-Link, 2026).
3	Switch	NETGEAR	GS308Ev4	Es un switch diseñado para hogares y oficinas pequeñas ofrece funciones de red básicas (NETGEAR, 2026).
4	Coordinador	SONOFF	SONOFF ZBDongle Plus-P Zigbee 3.0 USB	Actúa como puerta de enlace para conectar dispositivos Zigbee a Home Assistant, permitiendo control local de dispositivos de diversas marcas (SonOff, 2026).
5	Extensor de cable	Faracent	Cable de extensión de 1,5 m. Usb macho a hembra	Sirve para prevenir posibles interferencias entre la comunicación Wifi y Zigbee, ambos protocolos trabajan en la frecuencia de 2.4 GHz (Amazon, 2025).
6	Cable	INDECO	AWG 16	Conductor eléctrico flexible de cobre con aislamiento de PVC (SODIMAC, 2026).

(continúa)

Tabla 3 (continuación)

	Nombre del equipo	Marca	Modelo	Funcionalidad
7	Cámara para Exteriores	TP-LINK	Tapo C310 V2.2	Cámara 2K exterior, IP66, detección de movimiento y personas, sirena, visión nocturna, nube/SD, con audio bidireccional (TP-LINK, 2026).
8	Cámara para interiores	TP-LINK	Tapo C200 V3.20	Cámara panorámica/inclinable con detección de movimiento, 1080P, audio de 2 vías y visión nocturna (TP-LINK, 2026).
9	Cámara para Exteriores	EZVIZ	Ezviz C6N	Cámara inteligente interior 360°, 1080p, seguimiento de movimiento, visión nocturna 10 m, audio bidireccional y almacenamiento microSD o nube (Promart, 2026).
10	Tarjeta micro SD (256 GB de RAM)	Hiksemi	Neolux V30	Unidad de almacenamiento ideal para grabar contenido fluido en alta resolución (MercadoLibre, 2026).
11	Sensor de movimiento	AQARA	Sensor de movimiento P1	Aqara P1 es un sensor de movimiento y luminosidad inteligente de alto rendimiento, diseñado para automatización del hogar y seguridad (Tiendamia, 2026).
12	Sensor de movimiento	SONOFF	SNZB-03P	Sensor de movimiento Zigbee 3.0 inteligente, compacto y de bajo consumo, diseñado para la seguridad y automatización del hogar (Banggood, 2026).
13	Sensor de presencia	SONOFF	SNZB-06P	Sensor de presencia humana inteligente y de alta precisión, con radar de microondas; diseñado para hogar inteligente, detecta movimientos diminutos, incluso personas sentadas (Alibaba, 2026).
14	Bombilla	INNR	Smart Light Bulbs, A19 Zigbee	Bombilla LED inteligentes de alto brillo que permiten ajustar el color desde blanco cálido hasta frío y regular la intensidad. Usan tecnología Zigbee para integrarse con Philips Hue (Amazon, 2025).
15	Bombilla	MOES	Smart Light Bulb RGB E27	Bombilla inteligente A19 - E26 de iluminación inteligente RGB+CW (2700K-6500K) (Moes, 2026).
16	Bombilla	THIRDREALITY	Smart Color Bulb ZL1	Bombilla inteligente (RGBCW) que ofrece iluminación personalizable con millones de colores y blancos ajustables funciona como repetidor de señal para mejorar la red domótica (Amazon, 2026).

(continúa)

Tabla 3 (continuación)

	Nombre del equipo	Marca	Modelo	Funcionalidad
17	Relé	SONOFF	SONOFF ZBMINI Extreme Zigbee	Interruptor inteligente Zigbee que requiere cable neutro (SonOff, 2026).
18	Relé	AQARA	Relé T2 de contacto seco y mojado	Módulo inteligente doble canal Zigbee 3.0 que automatiza luces, persianas, calderas y motores; convierte interruptores tradicionales en inteligentes, solución versátil para domótica (Blustore, 2026).
19	Enchufe	AQARA	AQARA Smart Plug, EU type (SP-EUC01)	Permite encender o apagar dispositivos manualmente o mediante control temporizado, usado junto con otros componentes de Aqara. También puede registrar el consumo eléctrico (AQARA, 2026).
20	Multímetro Digital	Lion Tools	5958	Herramienta portátil y versátil, Permite medir voltaje de corriente continua (VCD) y alterna (VCA), corriente continua, resistencia, diodos, transistores y continuidad (Mercadolibre, 2026).
21	Controlador de válvula	AQARA	Aqara Controlador de válvula inteligente T1	Controlador de flujo de agua se combina con detectores de fugas de agua para el hogar y soporta el apagado por control remoto (AQARA, 2026).

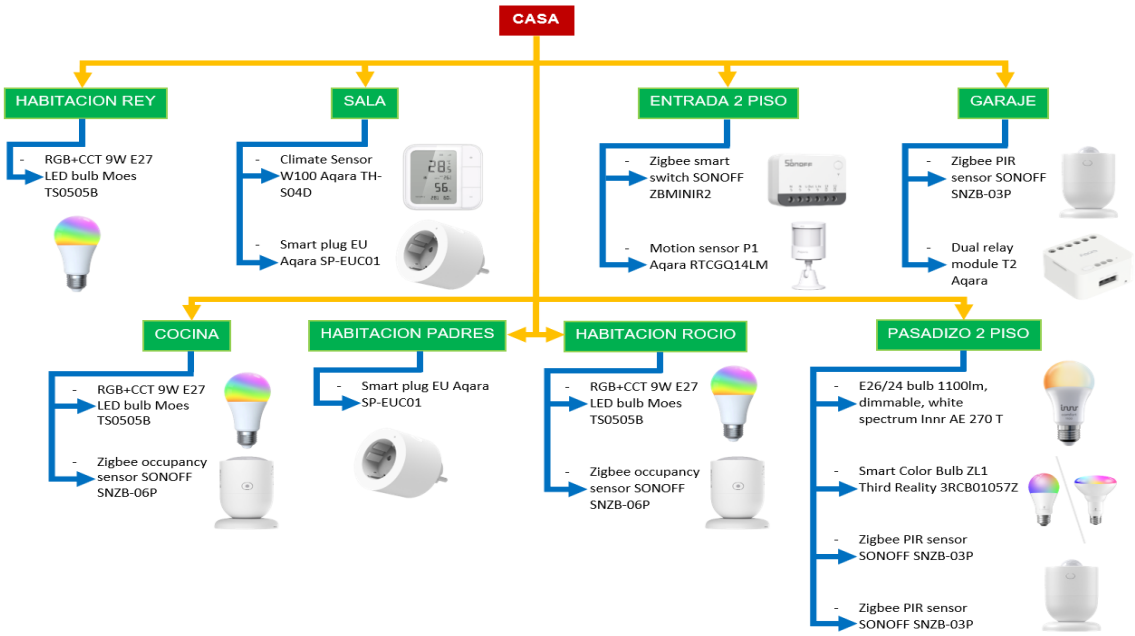
Nota. Los datos corresponden a los dispositivos considerados en la integración del sistema domótico.

3.3.1. Distribución de los dispositivos

La correcta distribución de dispositivos Zigbee que actúan como repetidores es clave: garantiza rutas estables y eficientes en la red en malla, mejora la cobertura en toda la vivienda, reduce interferencias y evita que un nodo se convierta en cuello de botella, logrando comunicación más confiable y robusta entre los equipos domóticos. En la figura 21 se presenta un diagrama que muestra la ubicación de cada dispositivo mencionado en la tabla 3, distribuidos en áreas específicas de la casa.

Figura 21

Diagrama de despliegue domótico de la vivienda



3.3.2. Criterios para la disposición de bombillas

Se expone la justificación y el criterio para la disposición de luminarias en la vivienda estudiada, según la tabla de lúmenes por áreas y zonas. La tabla 4 relaciona habitaciones y zonas de la casa con sus valores de iluminancia mínima, máxima y óptima por unidad de medida. Según (Faro, 2025) la luminancia es el flujo luminoso que incide, emerge o atraviesa una superficie desde un ángulo sólido. La iluminancia mide los lúmenes que caen sobre 1 m².

Tabla 4

Tabla de lúmenes por áreas y zonas

Áreas y clases de local	Mínimo (LUX)	Máximo (LUX)	Óptimo (LUX)
Dormitorios	100	150	200
Cuartos de aseo	100	150	200
Cuartos de estar	200	300	500
Cocinas	100	150	200
Cuartos de trabajo o estudio	300	500	750
Zonas de circulación y pasillos	50	100	150
Escaleras, roperos, lavabos, almacenes y archivos	100	150	200

Nota. Adaptado de Fabricatulampara (2022) del sitio web https://www.fabricatulampara.com/blog/noticias/cuantos-lumen-necesito-para-iluminar-una-habitacion-diferencia-entre-lumen-y-lux

Cabe recalcar que, al ser ambientes libres con el socket en posición perpendicular, no se considerarán los ángulos de las bombillas, pues al ser omnidireccionales emiten luz en todas las direcciones. Para determinar la iluminancia es necesaria la fórmula detallada en la Ecuación 1, ya que la energía luminosa emitida permite calcular la cantidad total de luz visible. (Erco, 2026) expone la siguiente fórmula:

$$E = \frac{\Phi}{A} \tag{1}$$

$Donde$:

$$E = Iluminancia\ en\ lux\ (lx)$$

$$\Phi = Flujo\ luminoso\ en\ lúmenes\ (lm)$$

$$A = Área\ de\ la\ superficie\ en\ metros\ cuadrados\ (m^2)$$

Ahora que se conocen y tenemos los datos podemos llevarlo a todos los casos para saber cuáles son los lúmenes requeridos para una habitación y para cada situación.

3.3.2.1. Proceso de justificación lumínica para bombilla MOES (cocina)

El mismo fabricante MOES (2026), detalla que el flujo luminoso de la bombilla es de 806 lm con un margen de 10 %. La Ecuación 2 revela la justificación de la luminosidad, con los siguientes datos:

Área total de la cocina: $5.49\ m^2$

Lúmenes de bombilla: $806\ lm$

$$E = \frac{806\ lm}{5{,}49\ m^2} = 146{,}8124\ lx \tag{2}$$

En comparativa con la tabla de lúmenes observamos que los lúmenes de la bombilla son suficientes para iluminar la zona de la cocina superando con una gran diferencia los 100 lx mínimamente necesarios.

3.3.2.2. Proceso de justificación lumínica para bombilla MOES (habitación Rocio)

El mismo modelo de bombilla se aplicó a un ambiente mucho mayor, lo que provoca cambios radicales en medidas lumínicas y consumo. Para verificar los lúmenes disponibles, cabe aclarar que en el ambiente anterior había dos focos, cada uno de 16 W y 1140 lm, que se encendían casi simultáneamente; por tanto, el consumo era el doble. Con estos datos se procede a generar la Ecuación 3.

Área total de la habitación: $22{,}82\ m^2$

Lúmenes de bombilla MOES: $806\ lm$

Lúmenes de segunda bombilla: $1140\ lm$

$$E = \frac{1140\ lm + 806\ lm}{22{,}82\ m^2} = 85{,}2761\ lx \quad (3)$$

Teniendo presente la tabla de lúmenes por áreas y zonas percibimos que los lúmenes de bombillas son relativamente bajos para iluminar la zona aun así la capacidad para llenar de luz el ambiente es suficiente siendo una habitación cerrada y sin muchos objetos.

3.3.2.3. Proceso de justificación lumínica para bombilla MOES (habitación Rey)

Del mismo modo tenemos que averiguar la luminancia para la habitación de Reynaldo, siendo así comenzamos con los cálculos de los lx para obtener la Ecuación 4.

Área total de la habitación: $8{,}14\ m^2$

Lúmenes de bombilla: $806\ lm$

$$E = \frac{806\ lm}{8{,}14\ m^2} = 99{,}0172\ lx \quad (4)$$

El cálculo de la Ecuación 4 muestra que la cantidad de lx es cercana a lo que se recomienda, no es ideal, pero cumple el objetivo de iluminar gran parte del entorno.

3.3.2.4. Proceso de justificación lumínica para bombilla INNR (pasadizo)

Los datos técnicos de la bombilla indican potencia de 11 W (equivalente incandescente 75 W) y brillo de 1100 lúmenes; con un margen de aumento del 3.63 % su entrega máxima alcanza 1140 lúmenes. Es ideal para zonas transitadas como una escalera e incluso para iluminar un ambiente cercano, un secadero. A continuación, se presentan los datos y el desglose de la Ecuación 5 para calcular la iluminancia necesaria.

Área total de la escalera: $8{,}93\ m^2$

Lúmenes de bombilla: $1140\ lm$

$$E = \frac{1140\ lm}{8{,}93\ m^2} = 127{,}6596\ lx \tag{5}$$

Siguiendo con la comparativa, los lux calculados para la zona de la escalera, son adecuados para la correcta iluminación, logrando estar en un nivel promedio con respecto al mínimo y máximo de lux; sin embargo, también se planteó que este dispositivo iluminara una zona próxima, siendo la zona de tendedero, generando la Ecuación 6, teniendo el siguiente procedimiento:

Área total de la escalera: $12{,}92\ m^2$

Lúmenes de bombilla: $1140\ lm$

$$E = \frac{1140\ lm}{12{,}92\ m^2} = 88{,}2353\ lx \tag{6}$$

Como se puede apreciar, la cantidad de lux en esta situación no es la indicada, inclusive incumpliendo el mínimo requerido según la tabla 4, es por ello que para este ambiente se necesitaría un foco adicional para lograr iluminar el lugar.

3.3.2.5. Proceso de justificación lumínica para bombilla ThirdReality (escalera)

Acorde con la información que brinda el fabricante ThirdReality (2026), provee un brillo de 800 lúmenes, siendo un buen producto para áreas como pasadizos, además su función adicional de RGB aumenta las posibilidades de avisar al usuario tareas

recordatorios o alertas según las rutinas, automatizaciones o escenarios. Siguiendo con el cálculo de iluminancia obtenemos el procedimiento de la Ecuación 7:

Área total de la escalera: $8{,}27\ m^2$

Lúmenes de bombilla: $800\ lm$

$$E = \frac{800\ lm}{8{,}27\ m^2} = 96{,}7352\ lx \tag{7}$$

Por último, se muestra este caso, donde la zona de circulación cumple con el mínimo requerido según la tabla 4 para una buena iluminación y parte de la zona de tendedero.

3.4. Operacionalización de variables

En la tabla 5 se operacionalizan las variables para la tesis sobre el diseño e implementación de un sistema domótico híbrido Zigbee-WiFi con acceso remoto e independiente de sistemas propietarios en una vivienda urbana de Tacna (2025–2026). Se define el sistema como el conjunto de tecnologías que automatizan y controlan funciones del hogar y se delimitan su alcance práctico, experimental en el estudio. Las dimensiones son: diversidad de marcas integradas, eficiencia del sistema y seguridad y confidencialidad. Indicadores cuantificables: Índice de Heterogeneidad Funcional (IHF), Índice de Estabilidad de Integración (ISI), Ratio de Adaptadores Necesarios (RAN), latencia promedio, consumo energético y capacidad máxima operativa sin fallos, además de métricas de exposición y bloqueo de accesos. Las técnicas y métodos combinan inventario y conteo mediante la plataforma de gestión (logs y catálogos); mediciones de red y scripts de monitorización para latencia y estabilidad; monitoreo energético con medidores para consumo; y auditorías de seguridad con escaneos y registros (puertos abiertos, intentos bloqueados, DNS filtrados y uso de HTTPS). Las unidades de medida incluyen ms, kWh, W, conteos de eventos y estados binarios. Estas métricas permiten diseñar el experimento en una vivienda en Tacna, integrar dispositivos representativos de distintas marcas, ejecutar pruebas de control remoto y medir rendimiento, consumo y seguridad en condiciones reales. Se recomienda automatizar registros para garantizar confiabilidad, definir umbrales operativos y establecer un plan de muestreo temporal que permita comparar resultados y validar la

independencia frente a sistemas propietarios durante 2025–2026. El protocolo detallado se documentará para replicabilidad.

Tabla 5

Operacionalización de variables de investigación

Variable de estudio	Definición conceptual	Dimensiones	Indicadores	Técnicas o métodos	Unidad de medida
Sistema domótico	Conjunto de tecnologías que automatizan y controlan diversas funciones de una vivienda	Diversidad de marcas integradas	Índice de heterogeneidad funcional (IHF) Índice de estabilidad de integración (ISI) Ratio de adaptadores necesarios (RAN)	Conteo y registro técnico (Home Assistant, catálogos de dispositivos)	Unidades conectadas / N° de operaciones / Adaptadores por dispositivo
		Eficiencia del sistema	Tiempo medio de retardo Consumo total Consumo promedio por dispositivo Máximo número de dispositivos funcionando sin fallos	Medición de red (ping, scripts HA), monitoreo energético (dispositivos, calculo eléctrico), logs HA	ms / kWh / W / unidades enteras
		Seguridad y confidencialidad	Número de puertos abiertos Intentos de acceso bloqueados DNS filtrados o bloqueados Uso de HTTPS y certificación de autentificación habilitada	Escaneo de red (Nmap, Nikto), IPBan, Adguard, Cloudflare	Cantidad de eventos bloqueados Registro de direcciones baneadas bloqueados Estado binario

En el Anexo 1 se presenta la matriz de consistencia que articula el problema general y los problemas específicos con los objetivos, las variables, los indicadores y la metodología propuesta para la tesis sobre el sistema domótico híbrido Zigbee-WiFi en Tacna (2025–2026). Esta matriz clarifica cómo cada objetivo se traduce en variables observables e indicadores medibles, garantizando coherencia entre la pregunta de investigación y el diseño experimental aplicado. La matriz vincula directamente indicadores como IHF, ISI, RAN, tiempo medio de retardo y consumo energético con los objetivos específicos de diseño, eficiencia y seguridad. Asimismo, especifica las técnicas a emplear: inventario en la plataforma de gestión, mediciones de red y

consumo, y auditorías de seguridad; y define las unidades de medida necesarias para obtener datos replicables y comparables. En conjunto, la tabla 5 y el anexo 1 permiten planificar el despliegue experimental en una vivienda en Tacna, establecer umbrales de desempeño, programar muestreos temporales y ejecutar pruebas de control remoto y auditorías de seguridad. De este modo se asegura que los resultados evaluarán la interoperabilidad entre marcas, la independencia frente a sistemas propietarios y el impacto energético y de seguridad en condiciones reales.

3.5. Procesamiento y análisis de datos

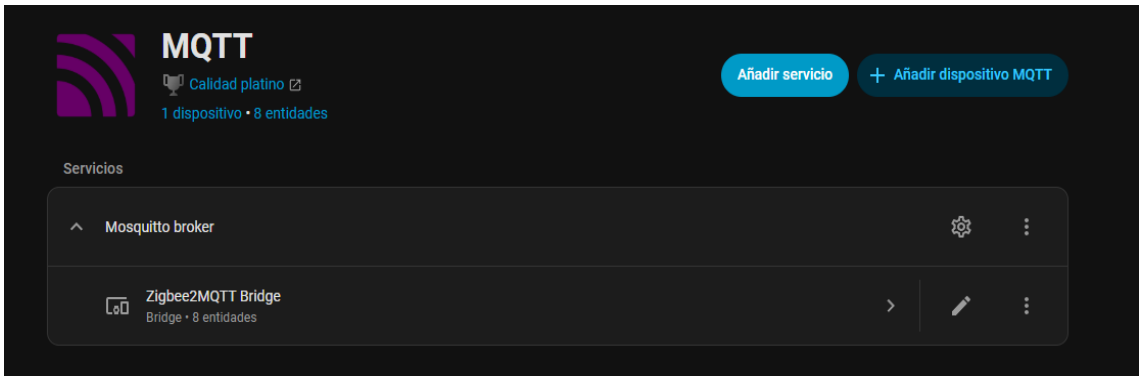
3.5.1. Integraciones de complementos en Home Assistant

3.5.1.1. Mosquitto bróker

Se instaló el complemento oficial Mosquitto broker en Home Assistant. Tras la instalación se asignó usuario y contraseña en configuración, se revisaron los registros y se verificó en Dispositivos y Servicios la correcta incorporación del broker, como muestra la figura 22.

Figura 22

Comprobación del complemento MQTT



3.5.1.2. File editor

File Editor (antes llamado Configurator) es un complemento que proporciona un explorador de archivos y un editor basado en navegador para el sistema donde se ejecuta Home Assistant. Permite editar archivos YAML, revisar errores de sintaxis y guardar cambios sin salir del panel de Home Assistant (IamHDT, 2026).

El propósito principal de este complemento es facilitar la edición rápida desde la propia interfaz, ahorrando pasos como el uso de SFTP o SSH y acelerando correcciones y pruebas. En las figuras 23 y 24 se muestra la instalación y una demostración del complemento en acción.

Figura 23

Instalación del complemento

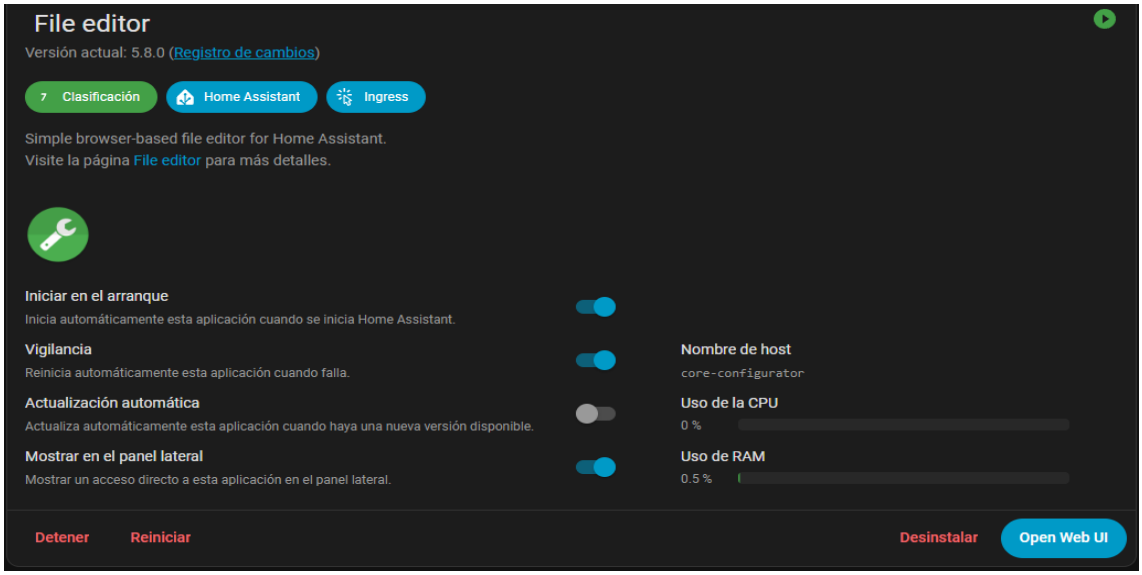
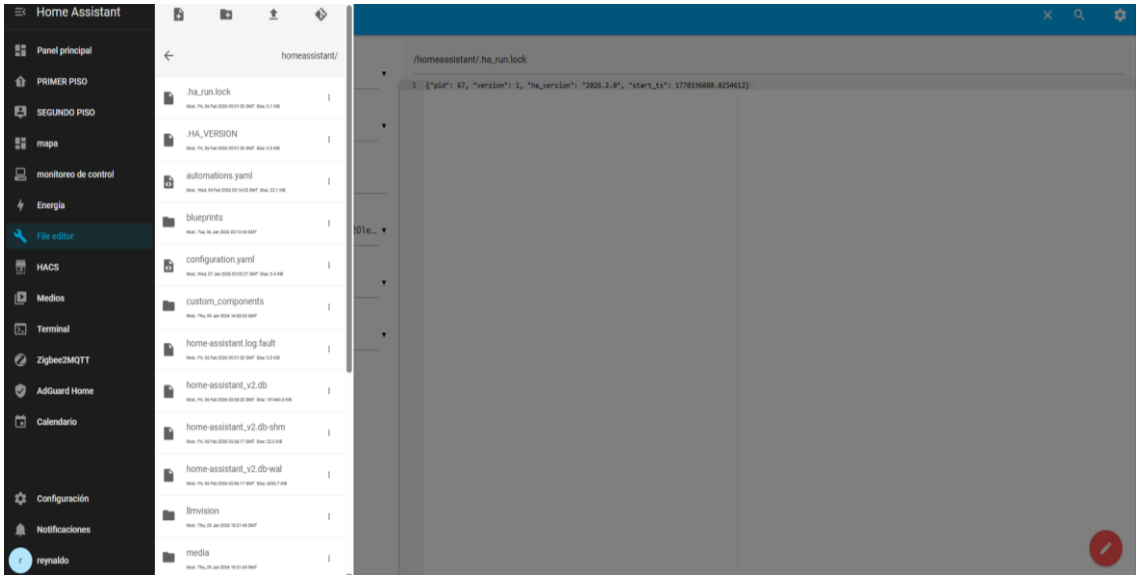


Figura 24

Demostración de los archivos para trabajar

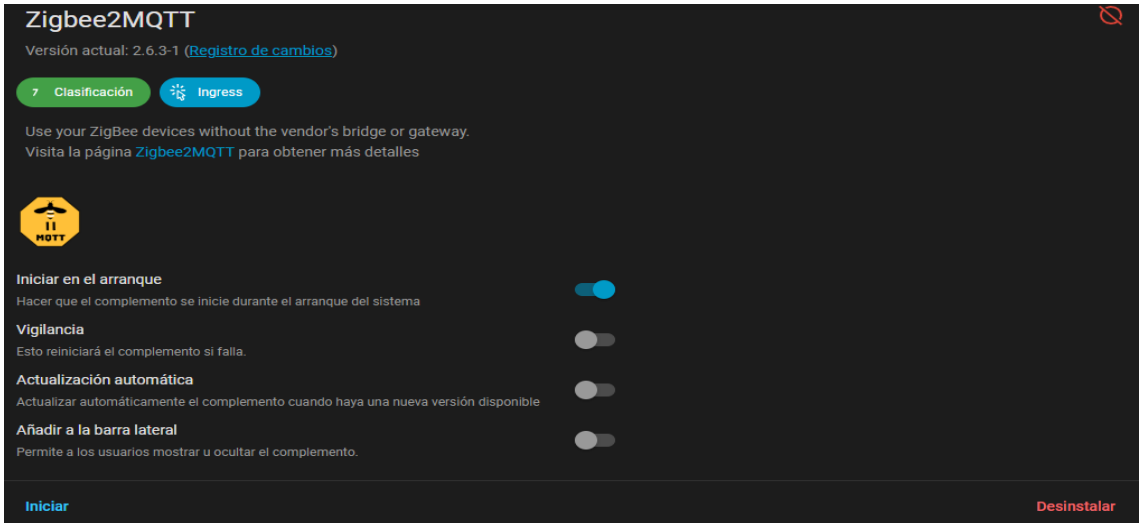


3.5.1.3. Zigbee2MQTT

Primero, vaya a Configuración → Complementos y, en ese apartado, añada el repositorio https://github.com/zigbee2mqtt/hassio-zigbee2mqtt (GitHub, 2025). A continuación, seleccione la versión estándar, que muestra la información general (figura 25). Existen otras versiones para desarrolladores o proxy.

Figura 25

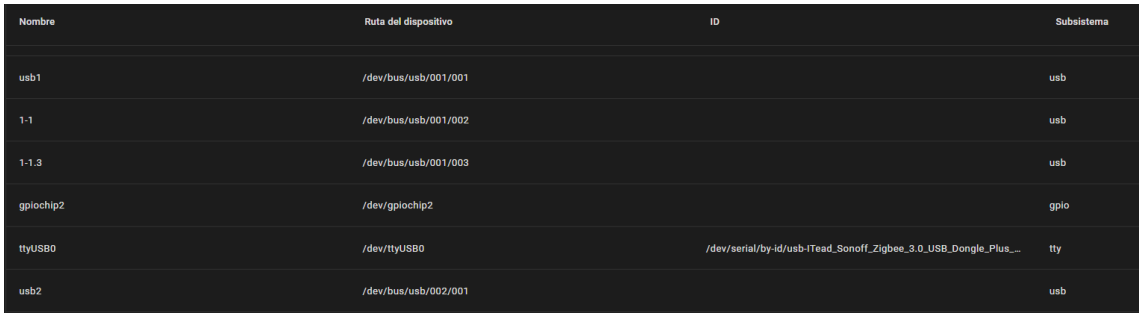
Instalación de Zigbee2MQTT



Antes de iniciar el complemento, es necesario averiguar el nombre del puerto al que está conectado el USB dongle-p. Para ello, vaya a Configuración → Sistema → Hardware; acto seguido se mostrará una imagen similar a la figura 26.

Figura 26

Tarjeta que muestra todo el hardware

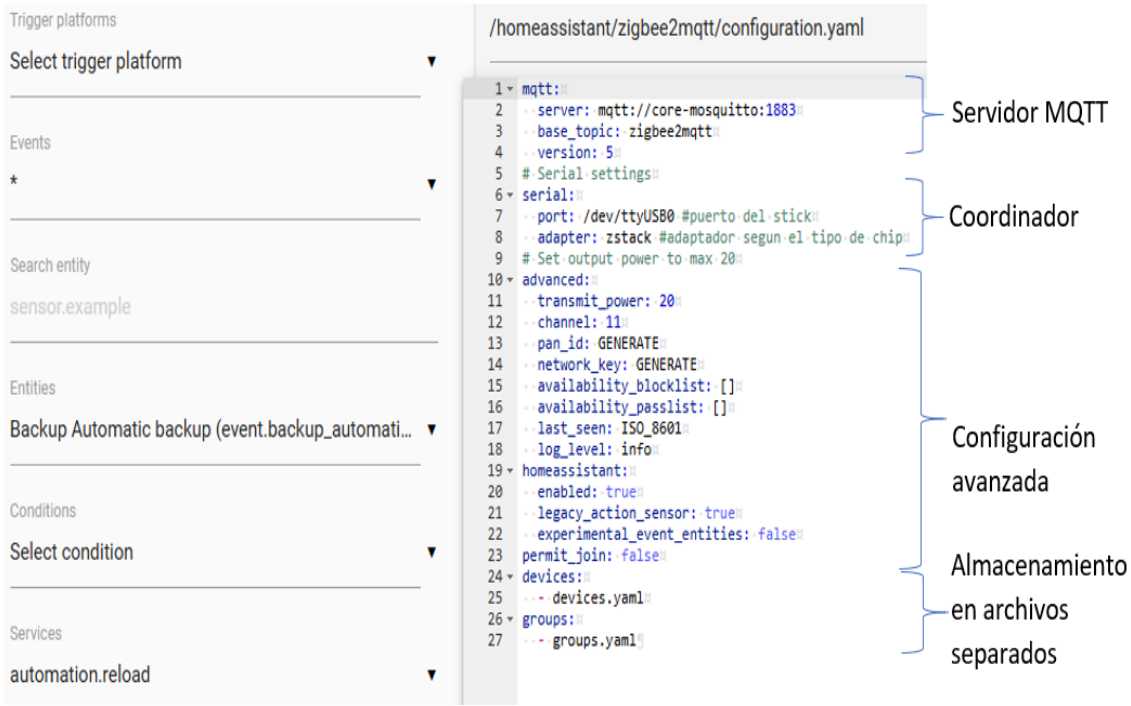


Nota. Se puede utilizar el nombre corto del puerto “/dev/ttyUSB0” para hacer más fácil el reconocimiento.

Para asegurarse del correcto funcionamiento de Zigbee2MQTT en su primera ejecución y con las configuraciones básicas, es recomendable crear manualmente una carpeta junto al directorio principal de Zigbee2MQTT. En esa carpeta debe definirse el servidor MQTT, el puerto serie del coordinador Zigbee, los parámetros de red avanzados y la integración con Home Assistant. Esta configuración se muestra en la figura 27.

Figura 27

Configuración para Zigbee2MQTT



Una vez realizados estos procedimientos, podremos iniciar el complemento. Opcionalmente, se pueden habilitar las opciones de vigilancia y de actualización automática. Posteriormente, es necesario verificar los registros, como se aprecia en la figura 28, para comprobar el correcto funcionamiento del complemento; el primer inicio de la interfaz se muestra en la figura 29.

Figura 28

Registros del complemento

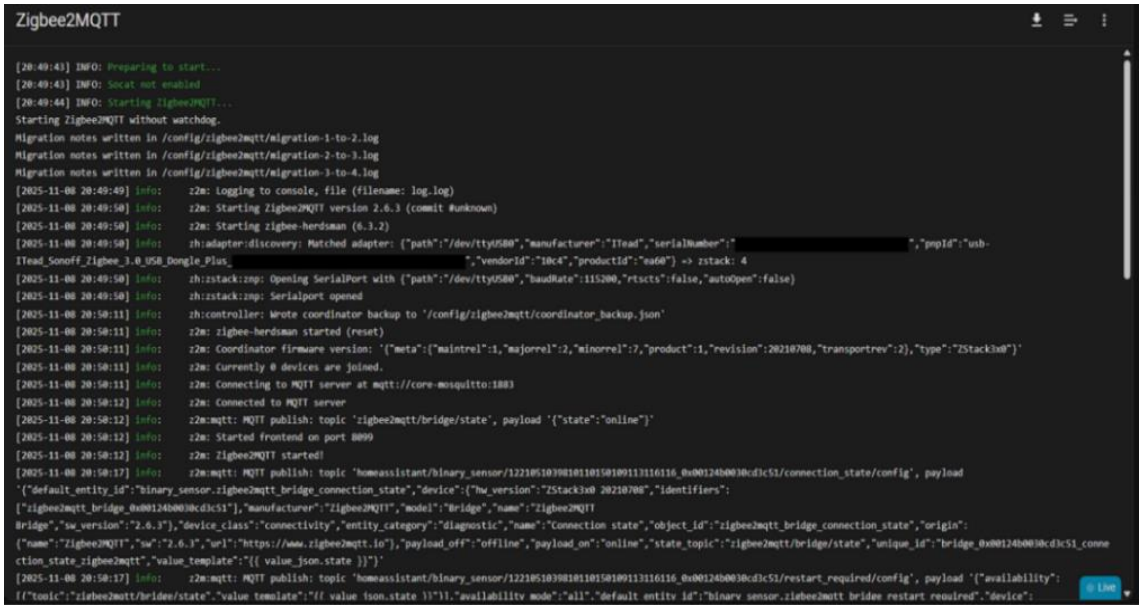
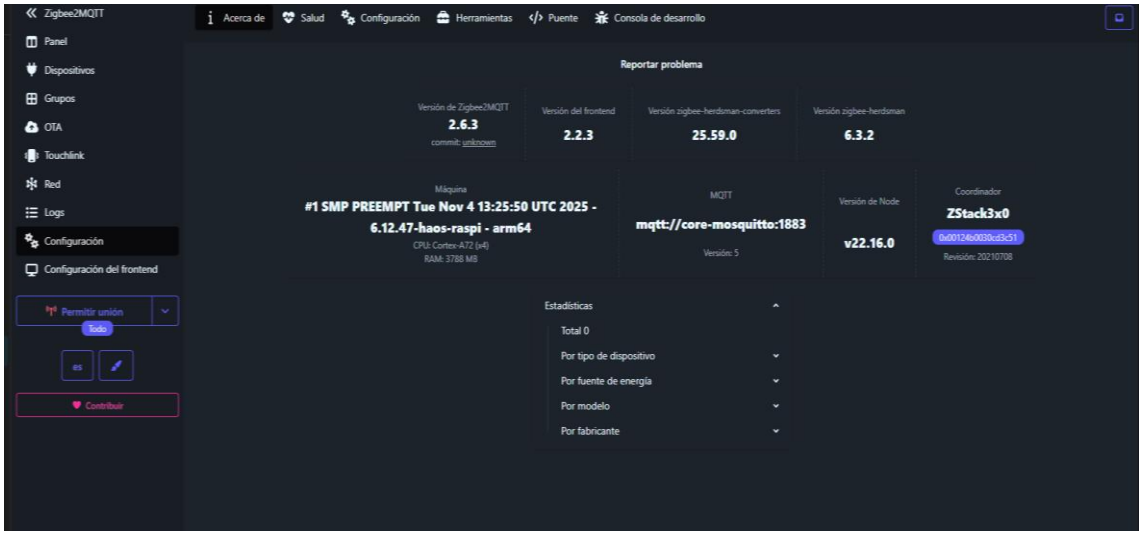


Figura 29

Primer inicio de la interfaz



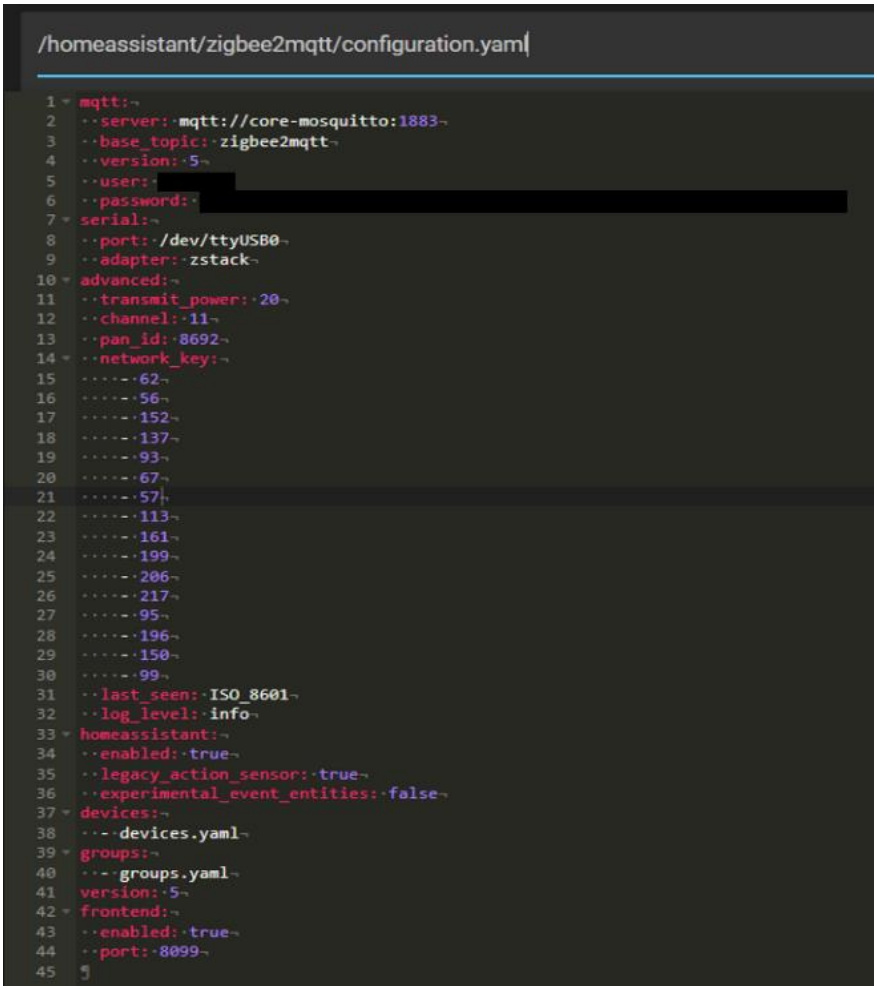
Nota. El primer inicio puede demorar mucho tiempo en iniciar (alrededor de 10 minutos).

Al realizar la comunicación entre los complementos Zigbee2MQTT y MQTT, se efectuarán algunos cambios en el archivo configuration.yaml. En dicho archivo se crean el usuario y la contraseña para el servidor MQTT, además se agregan el pan_id (ID de

red personal) y la clave de la red Zigbee. Aprovechando el editor de código, se puede visualizar esta configuración en la figura 30.

Figura 30

Zigbee2MQTT en configuration.yaml



3.5.1.4. Actualización del firmware del coordinador

Tras instalar Home Assistant en una Raspberry Pi, se actualizó el concentrador Zigbee añadiendo el repositorio https://github.com/mercenaruss/zigstar_addons (GitHub, 2025) para actualizar firmware por categorías. Se detallan modelos de chips y fabricantes para elegir el más adecuado; se seleccionó ZigStar TICC2652P/P7 FW Flasher. La figura 31 ilustra la configuración del complemento antes de actualizar el firmware. Finalmente, la figura 32 muestra el registro utilizado para detectar y corregir posibles problemas.

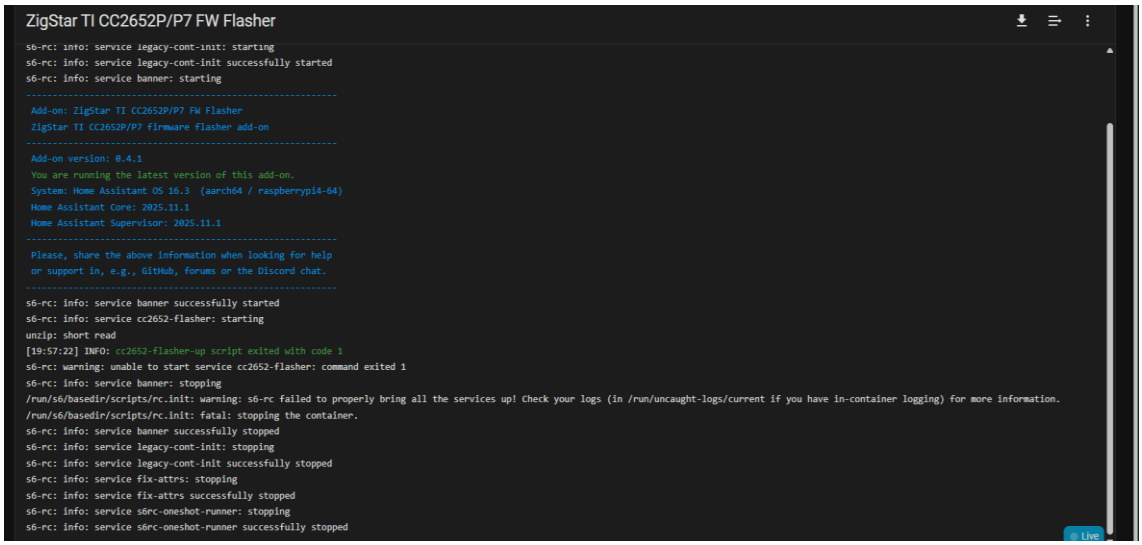
Figura 31

Configuración del complemento

Nota. Device indica puerto del coordinador; Network device/USBdevice habilita modo necesario para actualizar firmware; SonoffUSB actualiza Sonoff Dongle-p; el tercer campo selecciona la versión más reciente; luego iniciamos el complemento.

Figura 32

Registro del complemento

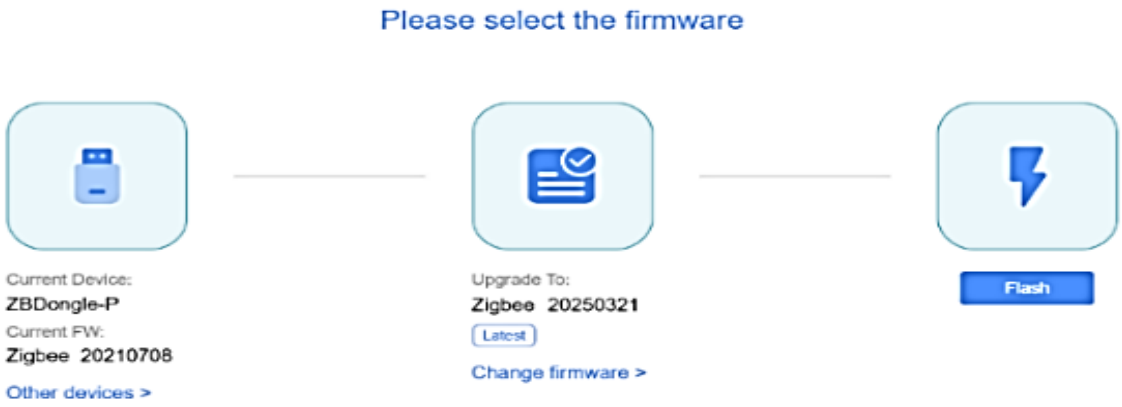


En primera instancia no funcionó la actualización del firmware por una falla de red; por ello se procedió a realizar una actualización manual con la herramienta

SONOFF Dongle Flasher, siguiendo las instrucciones de la página oficial de Sonoff, como se ilustra en la figura 33.

Figura 33

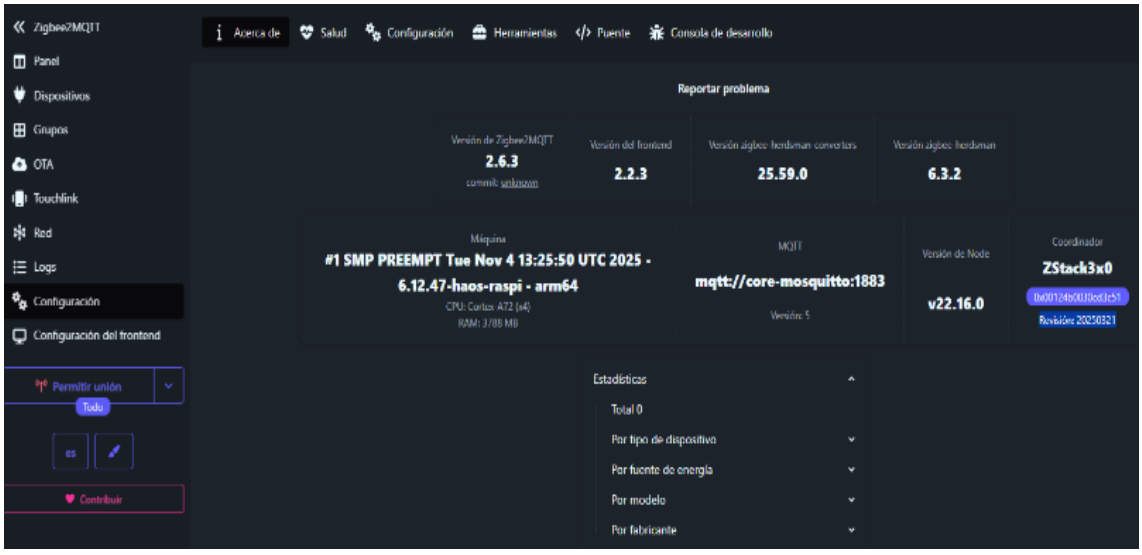
Reconocimiento de hardware



Una vez completado el flasheo, insertamos el coordinador dongle-p en la Raspberry y verificamos que la versión esté actualizada; como referencia, la versión actual es 20250321. Accediendo al apartado de Zigbee2MQTT (Z2M), en la figura 34 se aprecia que la versión mostrada es la correcta.

Figura 34

Comprobación de la actualización



El primer dispositivo que enlacé a mi red Zigbee fue el sensor climático Aqara W100. Para la integración inicial, encienda el dispositivo y conéctelo a Zigbee2MQTT.

Para que exista comunicación entre el dispositivo y el software, el usuario o administrador debe permitir la unión desde el panel principal del complemento. Como se aprecia en las figuras 35 y 36, se muestran los datos del dispositivo, la fuente de alimentación, el tipo de dispositivo, el modelo y otras características.

Figura 35

Emparejamiento con sensor de temperatura Aqara W100

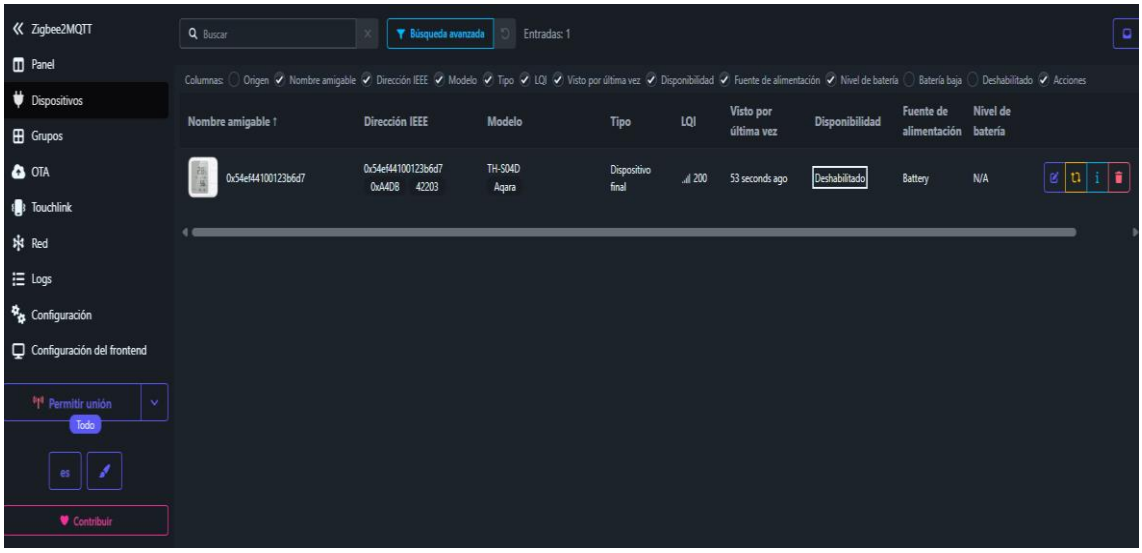
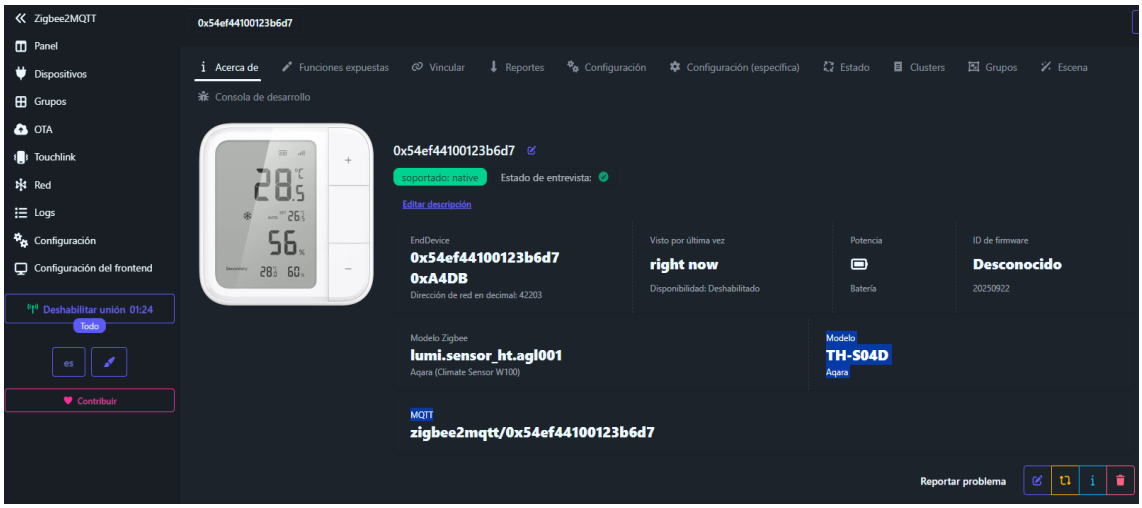


Figura 36

Información sobre el sensor Aqara w100 mediante Zigbee2MQTT

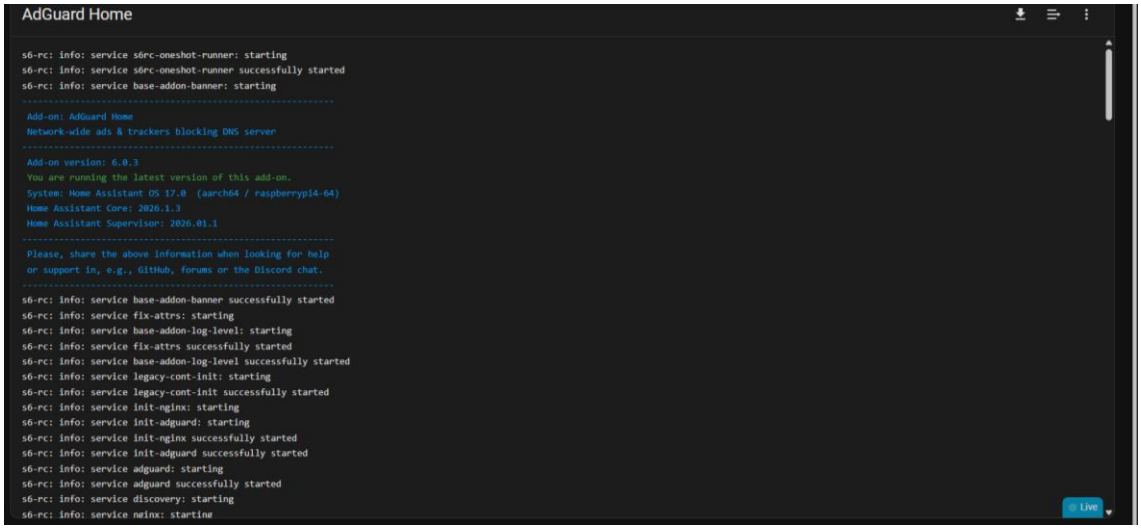


3.5.1.5. Adguard Home

Ejecutamos el complemento desde la tienda de complementos de Home Assistant y dejamos las asignaciones de configuración por defecto. Se deben verificar los registros para evaluar la instalación y detectar posibles problemas; la figura 37 muestra que la instalación fue exitosa y no se registraron errores.

Figura 37

Registros del complemento



La primera vez que se inicia el complemento tarda entre 3 y 5 minutos en arrancar. Véase la figura 38 para los datos obtenidos en ese primer inicio: en ese momento solo había dos dispositivos usando el DNS de AdGuard, que realizaron un total de 72 consultas, y se registraron ocho bloqueos por los filtros nativos de AdGuard durante los primeros aproximadamente dos minutos de uso.

Además, el usuario puede asignar diversos tipos de filtros de bloqueo, servicios y permisos según sus necesidades. En las figuras 39 y 40 se observan las consultas DNS realizadas por varios equipos durante 24 horas y la configuración del DNS de AdGuard en el router principal que gestiona el servicio domótico; en la figura 41 se muestra la lista de bloqueos DNS.

Figura 38

Primer inicio de la interfaz

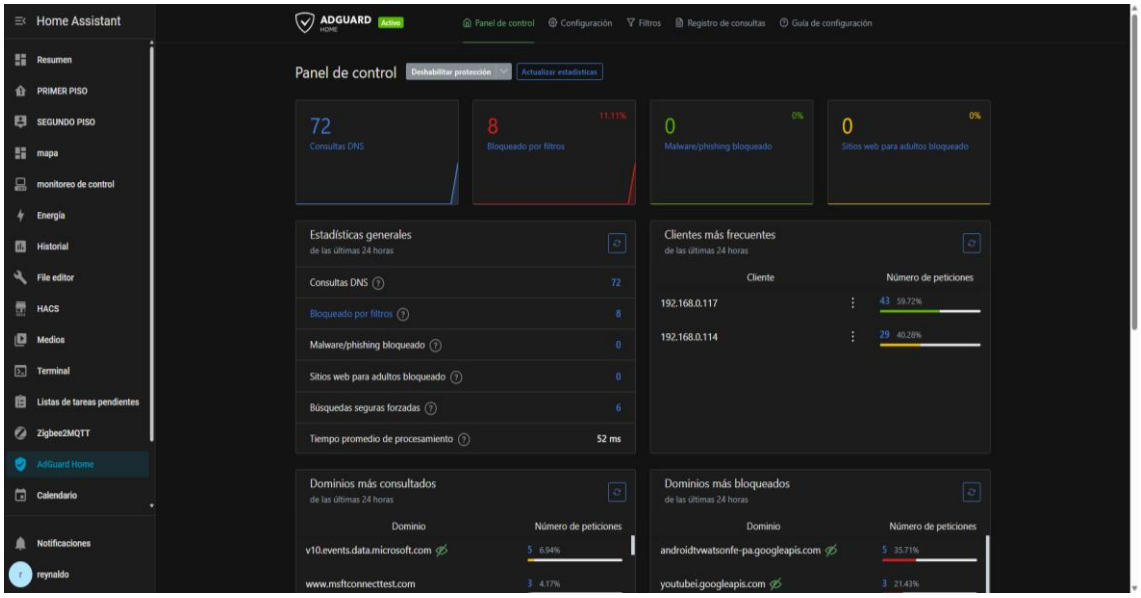


Figura 39

Bloqueos después de 24 horas de activación

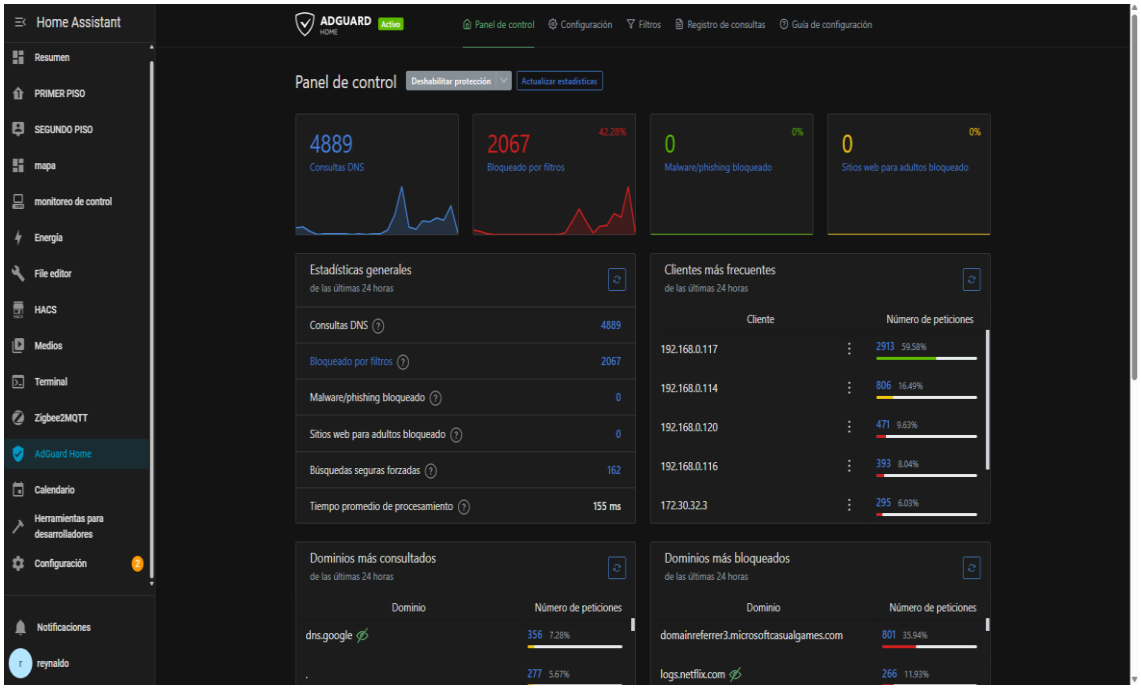


Figura 40

Configuración para el servidor DNS de Adguard en router

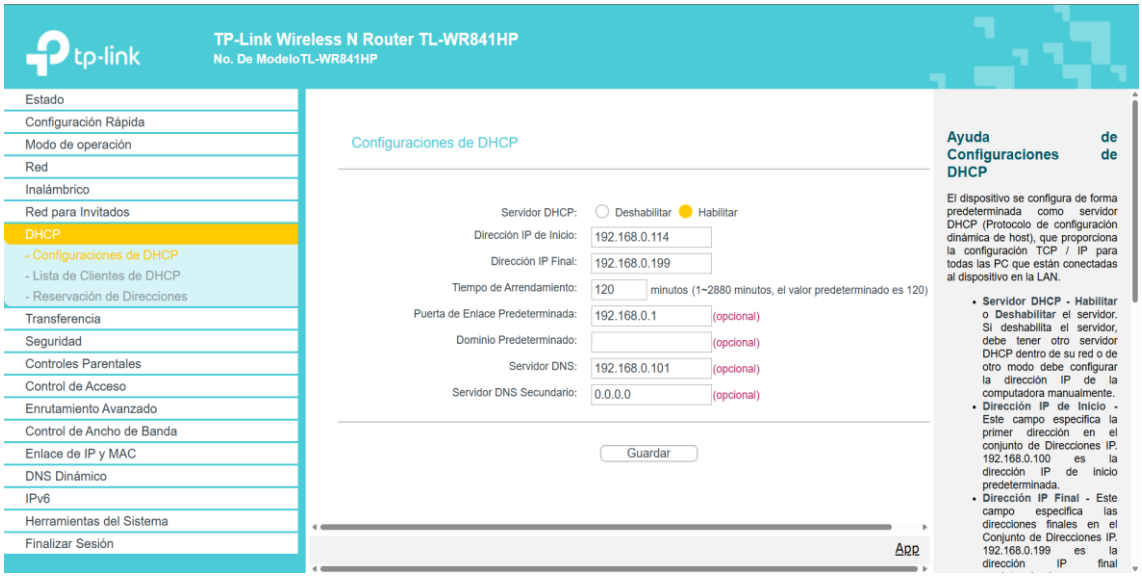
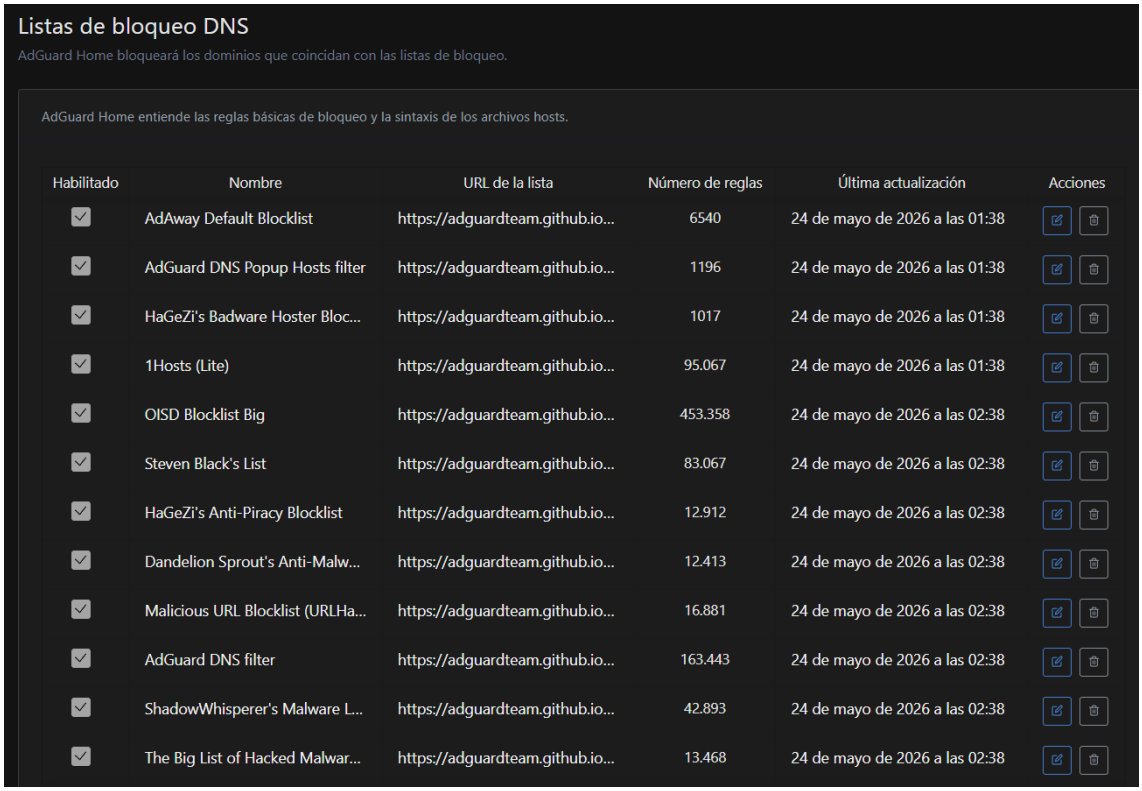


Figura 41

Listas de bloqueo DNS Adguard



Nota. Las listas elegidas son con el fin de bloquear malware, publicidad, popups, servicios de telemetría, rastreadores, ventanas emergentes, hosting y trackers.

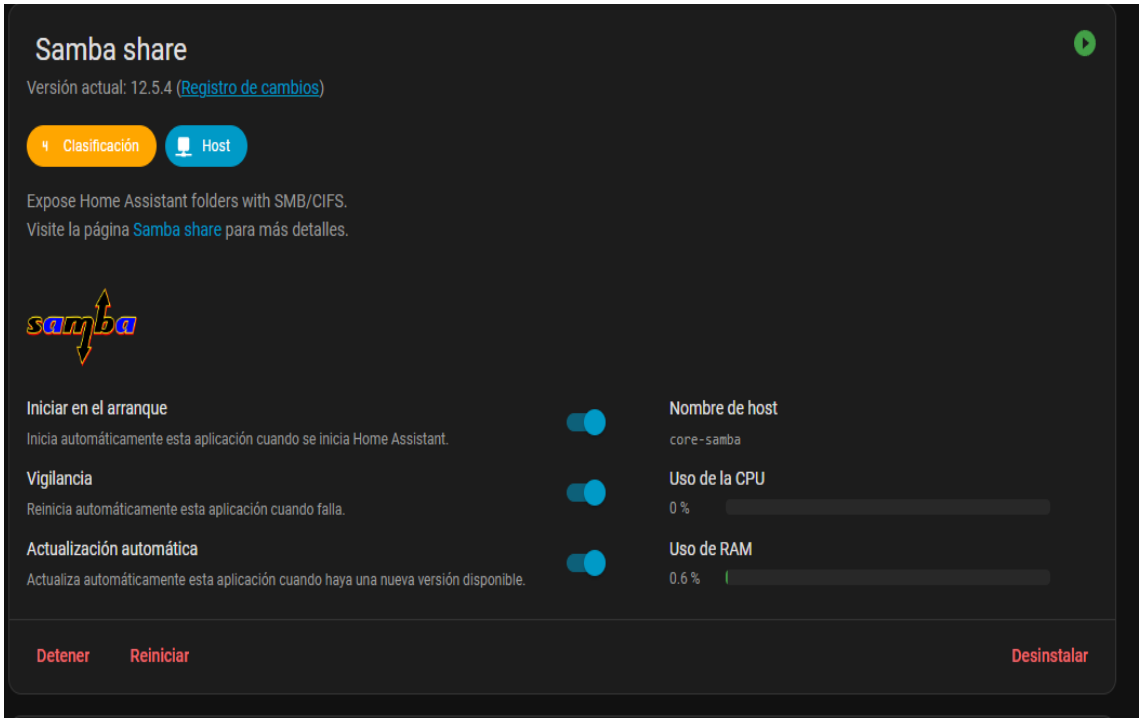
3.5.1.6. Samba share

La guía técnica sobre instalación y características de Samba establece que es una implementación de código abierto del protocolo SMB/CIFS que facilita compartir archivos, impresoras y recursos de red entre sistemas Windows, Linux y macOS como en la figura 42 donde se instaló su complemento en Home Assistant. Un Samba Share es una carpeta o recurso publicado por un servidor Samba al que pueden conectarse clientes de la red usando credenciales y permisos (Demon Warrior Tech Docs, 2026).

En el contexto de su uso en Home Assistant, la página oficial menciona: “La app Samba te permite compartir los directorios de Home Assistant con otros sistemas de tu red. Tras instalarla, también puedes editar archivos con el editor que prefieras desde tu ordenador cliente.” (Home Assistant, 2026).

Figura 42

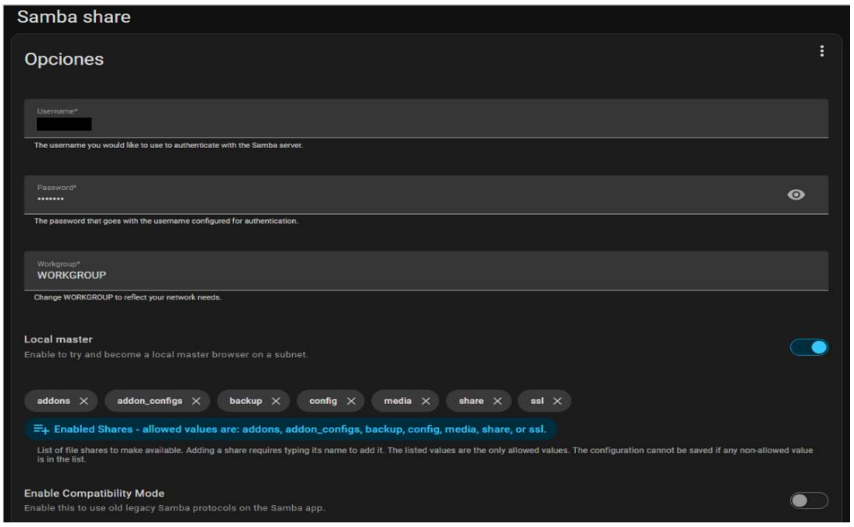
Instalación del complemento



En la figura 43 se muestran los campos personales donde el usuario debe designar su nombre de usuario y contraseña para autenticarse posteriormente y así poder acceder a los distintos documentos y recursos de Home Assistant.

Figura 43

Creación de credenciales personales

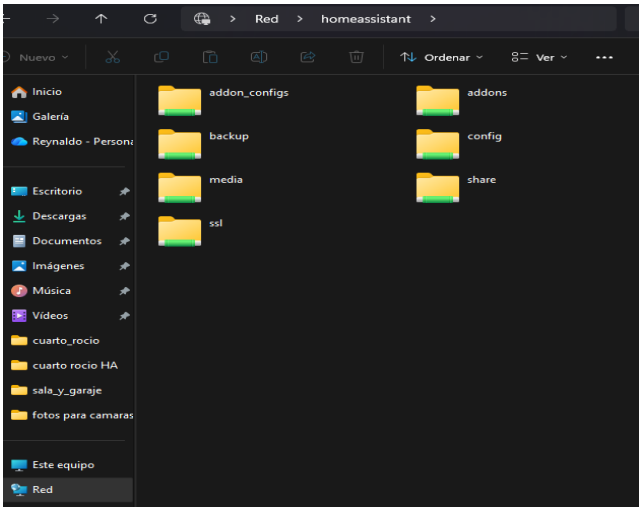


Nota. Estos datos deben ser colocados antes de iniciar el complemento, de otro modo, el nombre del usuario será “homeassistant” y no habrá una contraseña.

Con las credenciales creadas en Samba Share, desde una computadora en la misma red abrimos \\homeassistant. Aparecerá una ventana para introducir las credenciales y, tras autenticarnos, accederemos a los datos internos del servidor, como muestra la figura 44. Podremos navegar, copiar y editar archivos según los permisos asignados, y gestionar configuraciones, registros y respaldos remotos.

Figura 44

Acceso a archivos internos de Home Assistant



3.5.1.7. Terminal & SSH

Terminal & SSH es un complemento para Home Assistant que instala un servidor SSH y un terminal web dentro del frontend, permitiendo iniciar sesión con un cliente SSH o usar la consola integrada para acceder al sistema operativo, editar archivos y ejecutar comandos (Frenck, 2024). Al ser un complemento sencillo, las figuras 45 y 46 muestran su instalación e inicio, respectivamente.

Figura 45

Instalación del complemento

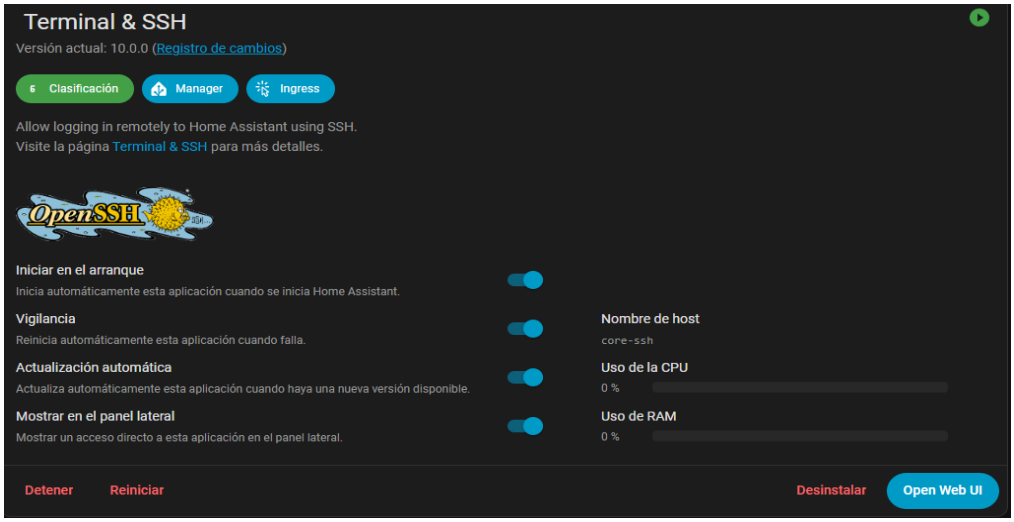
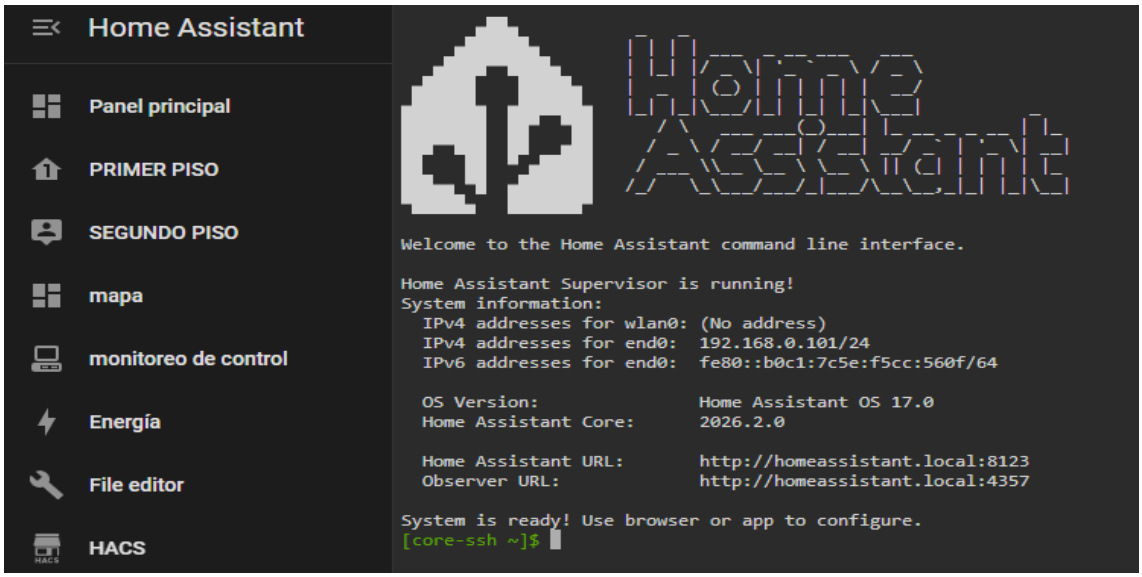


Figura 46

Primer inicio de la interfaz



3.5.1.8. Instalación de HACKS

Desde la web de HACKS se descarga la versión adecuada para la instalación de Home Assistant en host como sistema operativo. Tras descargarla se asigna la dirección IP local que identifica el destino donde se instalará el complemento y se procede a instalar HACKS. Después del reinicio, en Configuración vamos a Dispositivos y servicios se añade la integración de HACKS. Finalmente, se enlaza una cuenta propietaria de GitHub para obtener el código de verificación que autoriza a HACKS a acceder a la red, como muestran las figuras 47 y 48.

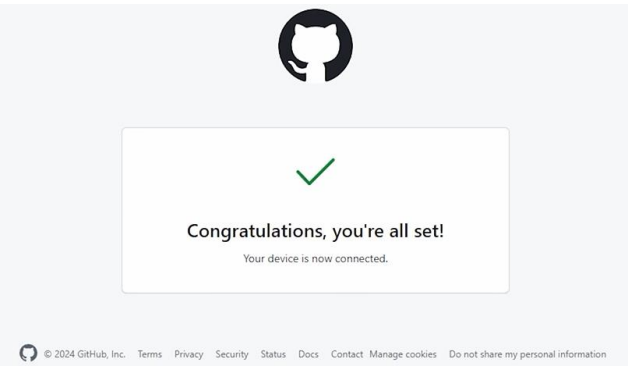
Figura 47

Registro *del complemento*

Nota. Una vez el complemento termine de ejecutarse nos pedirá que reiniciemos Home Assistant.

Figura 48

Activació*n de HACKS*



3.5.2. Mapeo de intensidad de señal estimada

Prosiguiendo con el mapeado de la intensidad de señal estimada para cada dispositivo, cabe señalar que las cámaras no se reflejan en estos planos porque su conectividad es mediante cable UTP. Se debe respetar el tipo de cable adecuado para la conexión entre dispositivos; el cable directo es funcional para conectar dispositivos finales a dispositivos de red. Es indiferente el estándar de cableado elegido, siempre que se use el mismo estándar en ambos extremos del cable; es decir, se puede emplear T-568A en ambos extremos o, de igual modo, T-568B podemos ver los mapas de intensidad de cada dispositivo desde la figura 49 hasta la figura 58.

Figura 49

Mapa de intensidad de señal WIFI del segundo piso

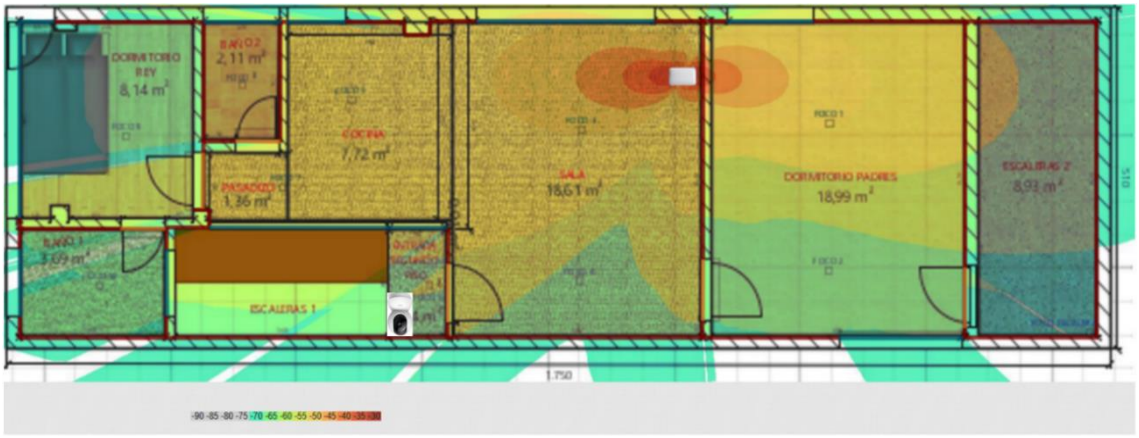


Figura 50

Mapa de intensidad de señal del coordinador Zigbee

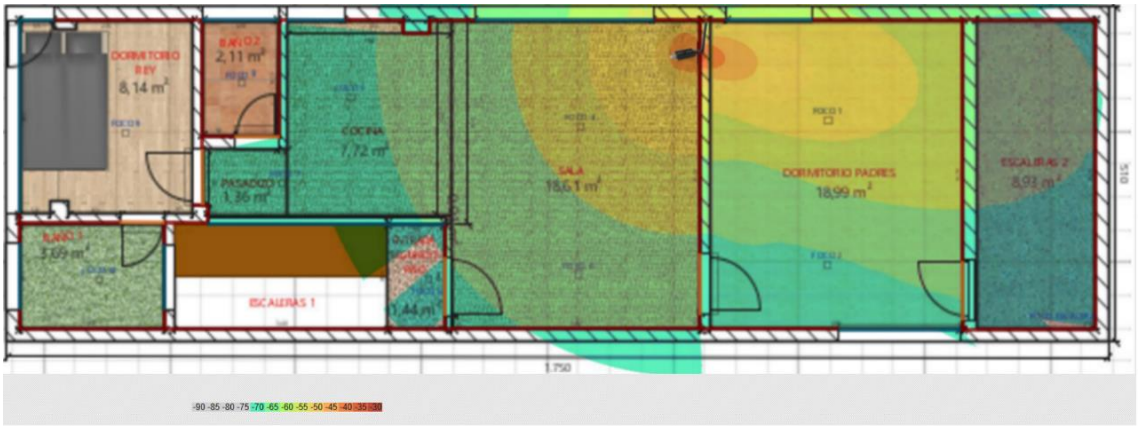


Figura 51

Mapa de intensidad de señal de foco MOES

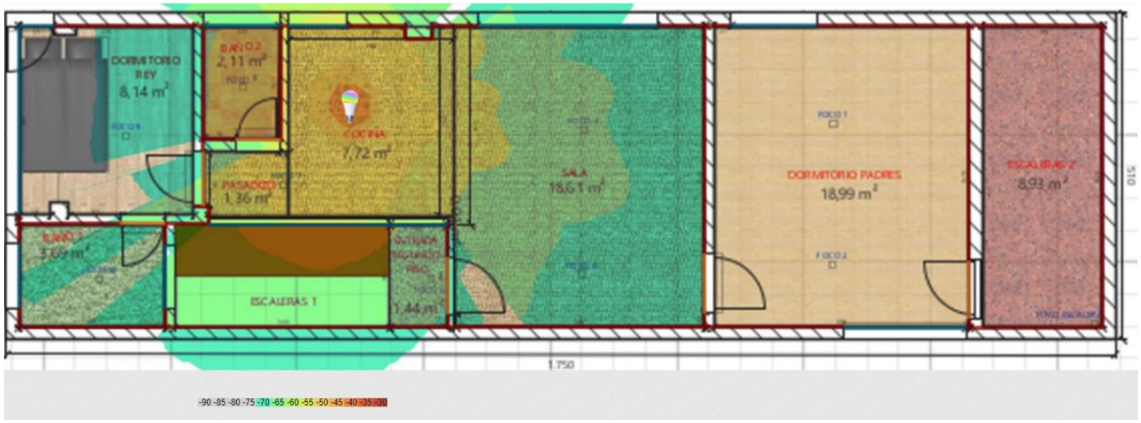


Figura 52

Mapa de intensidad de señal de relay2piso

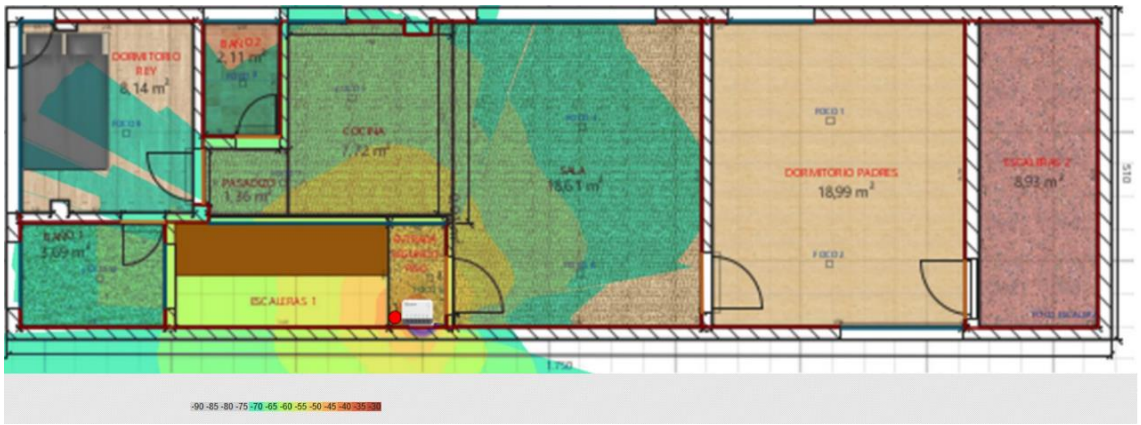


Figura 53

Mapa de intensidad de señal de focorey

Figura 54

Mapa de intensidad de señal de enchufe hab padres

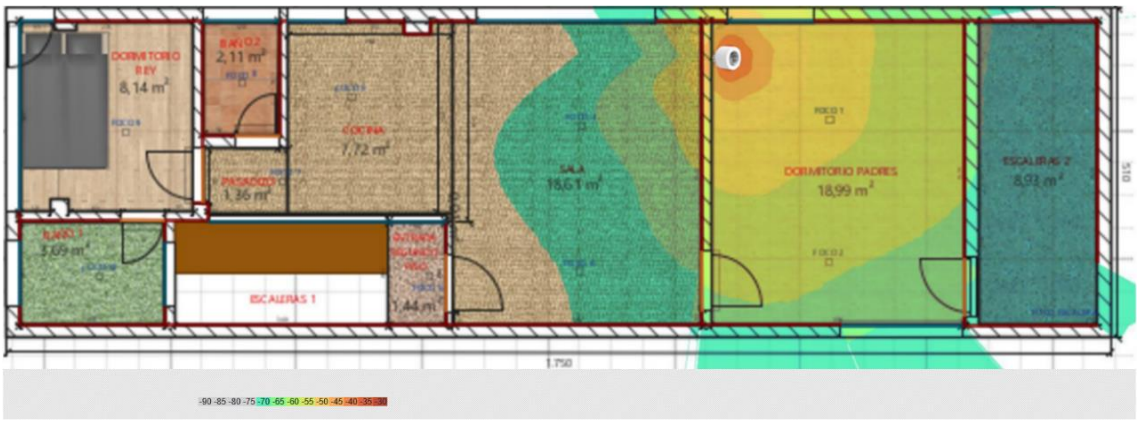


Figura 55

Mapa de intensidad de señal de foco escalera

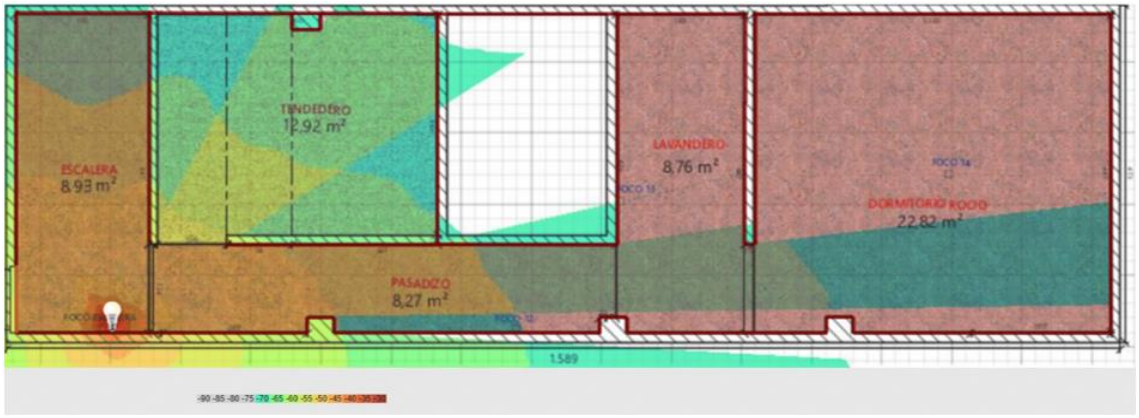


Figura 56

Mapa de intensidad de señal de foco pasadizo

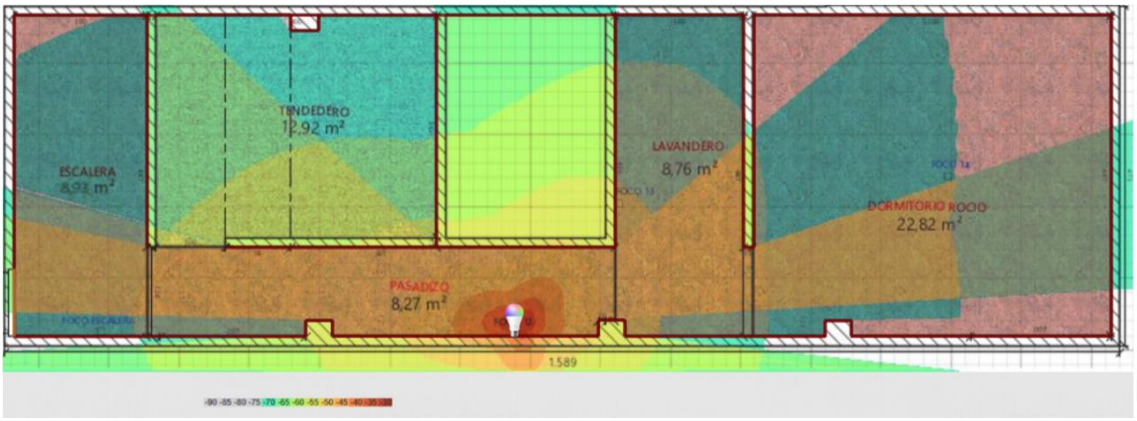


Figura 57

Mapa de intensidad de señal de focorocio

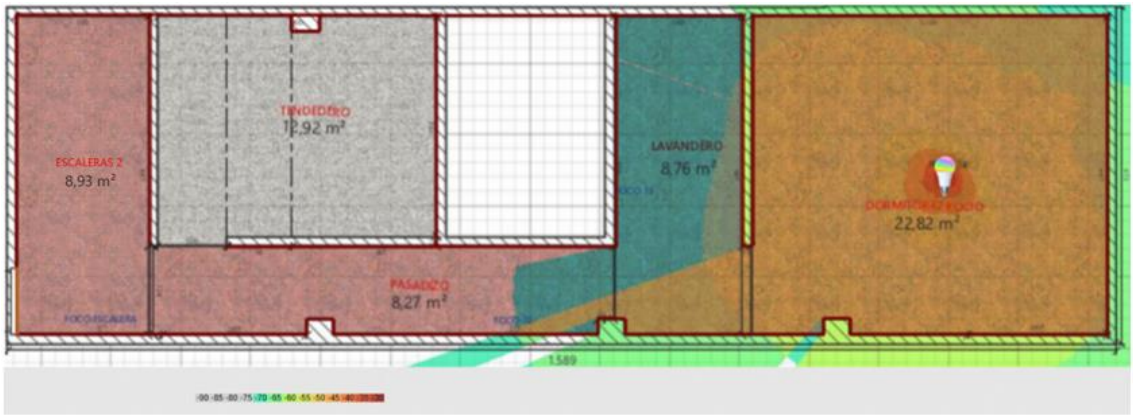
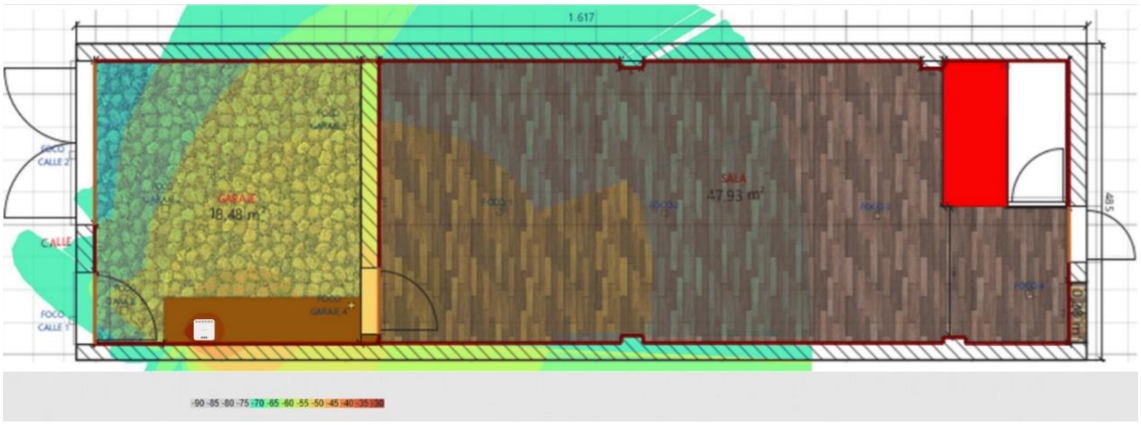


Figura 58

Mapa de intensidad de señal de relay2canales

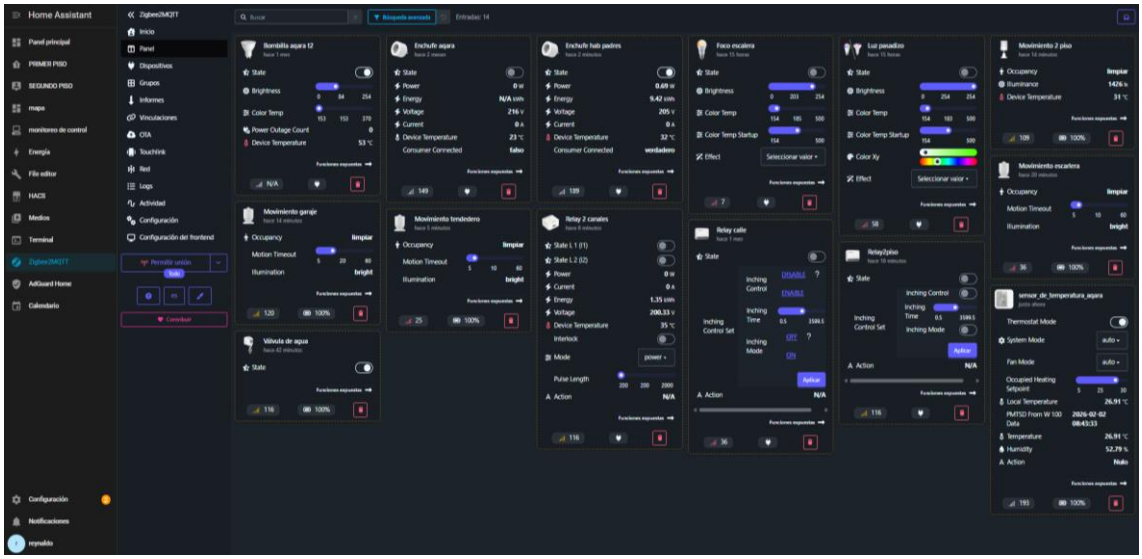


3.5.3. Integración de dispositivos

Como se observó en las figuras 35 y 36, se procedió a enlazar todos los dispositivos mencionados en la tabla 3, estableciendo comunicaciones entre varios nodos. No se concentró toda la conectividad únicamente en el coordinador; la comunicación también fluye a través de dispositivos que repiten la señal Zigbee, funcionando como routers. En la figura 59 se muestra el panel principal con todos los dispositivos.

Figura 59

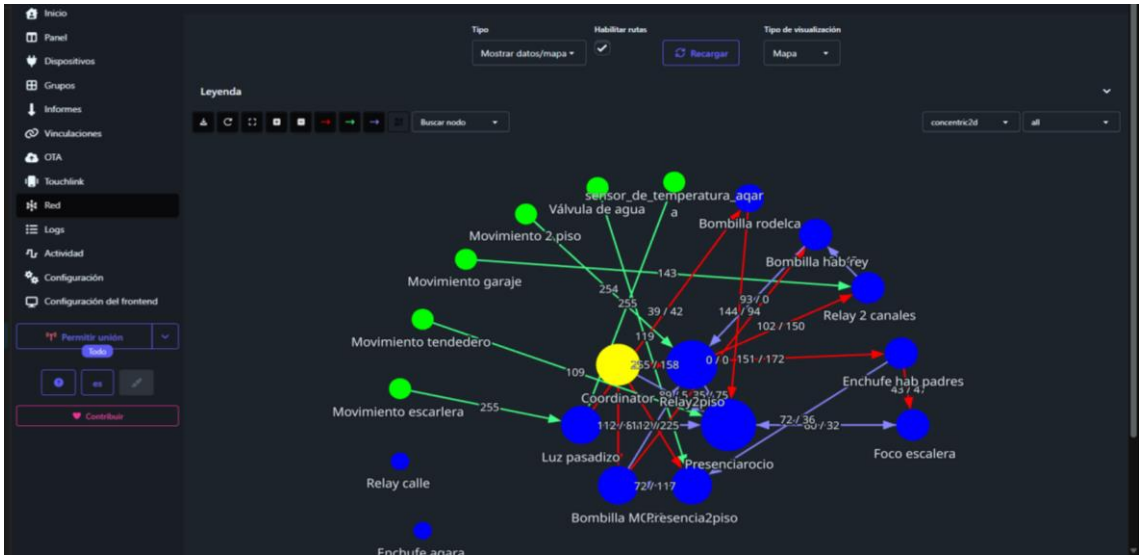
Panel de Zigbee2MQTT



Con los dispositivos anteriormente enlazados, podemos generar desde el propio software de zigbee2mqtt un mapeo sobre la red Zigbee y la comunicación que existe entre todos los dispositivos visto en la figura 60.

Figura 60

Mapa de la red Zigbee (concentric2d)



Nota. Las líneas rojas indican padre, las líneas verdes hijo y las líneas moradas/azules hermano.

En los anexos 2 y 3 se muestra la incorporación de algunos dispositivos de entretenimiento dentro de la central domótica; su proceso de integración es sencillo mediante complementos como Google Cast y Samsung Smart TV. Para aclarar, los padres son los dispositivos enrutadores (routers) a los que un dispositivo final se conecta directamente para enviar y recibir datos; resultan cruciales en la topología de malla, ya que actúan como puentes de red. Los hijos son dispositivos finales conectados directamente a un nodo padre —ya sea el coordinador o un router Zigbee—, formando una relación jerárquica. Los hermanos son dispositivos que comparten el mismo padre o nodo raíz en la estructura de la red mesh; por tanto, los dispositivos que comparten un router padre son hermanos entre sí.

Un dispositivo final (por ejemplo, sensores, botones o módulos a batería) suele caracterizarse por su bajo consumo y por depender de su padre para comunicarse; además, no extiende la malla, lo cual es un dato importante para el diseño de la red. Finalmente, los “hermanos” pueden ser tanto dispositivos finales como routers que comparten la misma conexión directa o el mismo padre en la topología Zigbee.

3.5.4. Asignación de direcciones IP estáticas

Al desplegar Home Assistant OS en una Raspberry Pi e integrar cámaras IP (Tapo C200 por Wi-Fi, Ezviz C6N y Tapo C310 por Ethernet), es esencial asignar direcciones IP fijas al servidor y a cada cámara. Esta práctica garantiza estabilidad, reproducibilidad y seguridad en la arquitectura domótica. Home Assistant identifica y comunica con los dispositivos mediante sus direcciones IP; si una cámara cambia de IP por DHCP del router, la integración configurada en Home Assistant dejará de funcionar hasta que se actualice manualmente la dirección, interrumpiendo servicios y automatizaciones.

Por ejemplo: la Tapo C200 expone su stream RTSP en una URL como rtsp://user:password@192.168.2.x:554/stream1. Si el router asigna una nueva IP (p. ej., 192.168.2.y), Home Assistant perderá acceso al stream. Por ello, una IP fija garantiza que las automatizaciones y los flujos de vídeo no se rompan tras reinicios o cambios en la red. (TP-LINK, 2025). Por lo anterior, en el router designado únicamente para los dispositivos domóticos se procedió a asignar direcciones IP estáticas para evitar posibles conflictos con otros dispositivos electrónicos, como se indica en la figura 61. En la figura 62 se visualiza la distribución de VLANs internas que se planteó.

Figura 61

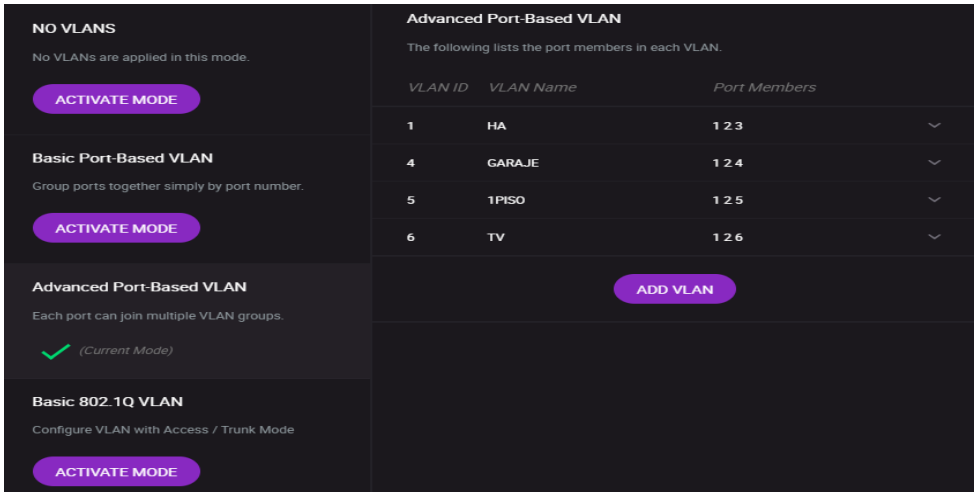
Asignaciones de direcciones IP estáticas para cada dispositivo

Dirección MAC	Dirección IP	Estado	Editar
[redacted]	192.168.0.101	Habilitado	Editar
[redacted]	192.168.0.102	Habilitado	Editar
[redacted]	192.168.0.109	Habilitado	Editar
[redacted]	192.168.0.106	Habilitado	Editar
[redacted]	192.168.0.105	Habilitado	Editar
[redacted]	192.168.0.104	Habilitado	Editar

Nota. La asignación de direcciones IP es: 192.168.0.101 para el servidor de Home Assistant, 192.168.0.102 para la cámara Tapo C310, 192.168.0.109 para la cámara C6N, 192.168.0.106 para el Switch NETGEAR, 192.168.0.105 para la cámara Tapo C200 y 192.168.0.104 para una TV conectada inalámbricamente.

Figura 62

Panel de gestión de VLANS del switch



Nota. Se separaron dispositivos mediante VLAN: el acceso a Internet está en todas las VLAN; en la VLAN 1 está la Raspberry Pi con H. A.; la VLAN 4 para la cámara Tapo C310; la VLAN 5 para la cámara C6N; y la VLAN 6 para la TV de sala.

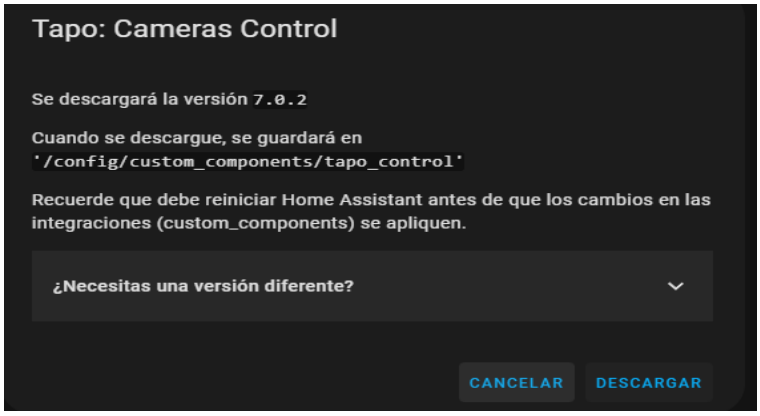
3.5.5. Implementación de cámaras de seguridad

3.5.5.1. Tapo C310

Para la integración de la cámara TP-Link Tapo C310 se probaron dos métodos de comunicación entre la cámara y Home Assistant. La primera conexión se realizó mediante el uso de HACS previamente instalado. Desde la barra de búsqueda de integraciones, buscamos el complemento Tapo Cameras Control y procedimos a descargar su versión más reciente, como se puede ver en la figura 63.

Figura 63

Descarga de la versión 7.0.2 para Tapo Cameras Control



Nota. Después de haber completado la instalación, la integración pedirá que se realice un reinicio del sistema.

Ahora nos dirigimos a configuración, dispositivos y servicios y agregamos una nueva integración con el mismo nombre. Dentro de la marca, introduciremos la dirección IP de nuestra cámara, para saber cuál es la IP de la cámara existen varios métodos, en este caso se revisó desde el router las direcciones IP designadas y de acuerdo a su registro se derivó la dirección IP de mi cámara. En la figura 64 se presenta la asignación IP de la cámara y en la figura 65 se presentan aspectos seleccionables antes de completar el complemento, donde las principales opciones (habilitar sensor de movimiento, habilitar mecanismos automáticos para enviar datos en tiempo real y sincronizar automáticamente la hora).

Figura 64

Asignación de dirección IP de la cámara Tapo C310

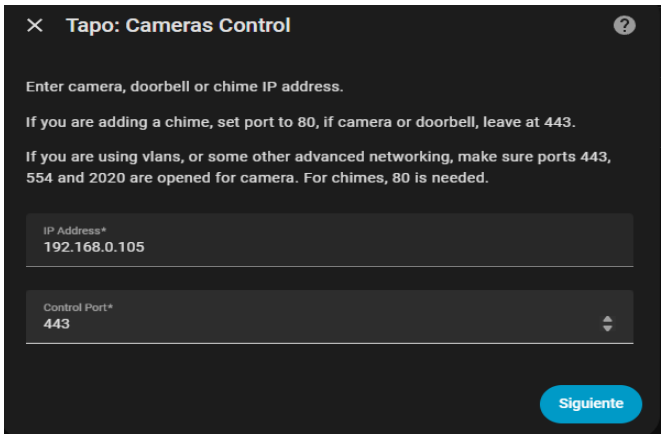
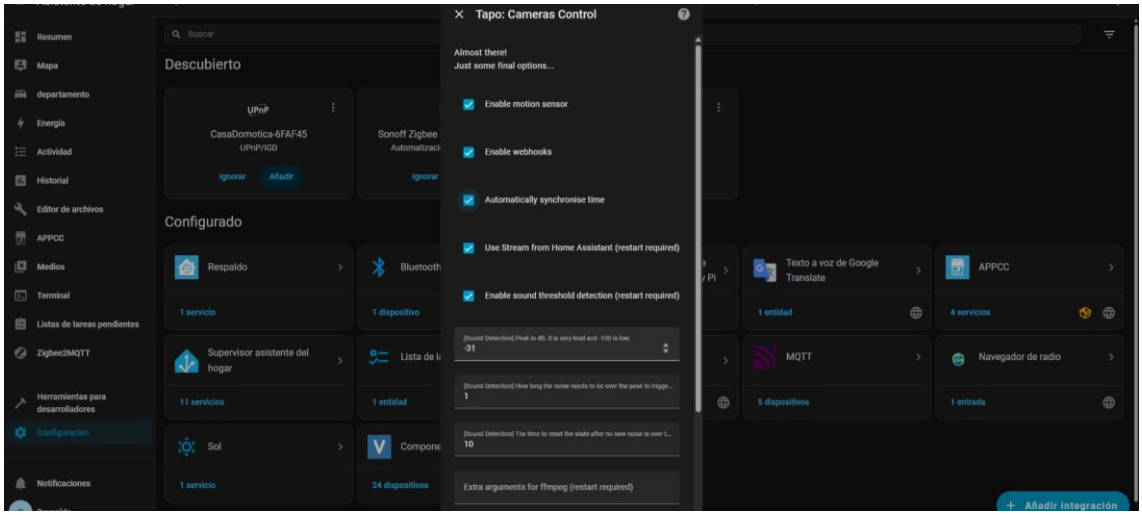


Figura 65

Adición de entidades



Nota. En este caso se habilitó todos los espacios para tener un sistema más completo, pero pueden existir casos donde ciertas funciones no sean prioridad como el usar la transmisión desde Home Assistant o habilitar la detección de umbral de sonido.

Por último, en la figura 66 se exhibe la correcta integración y la adición de entidades que expone el complemento de Tapo, por su parte la figura 67 muestra la transmisión en tiempo real de la cámara.

Figura 66

Exposición de todas las entidades permitidas usando la integración de Tapo

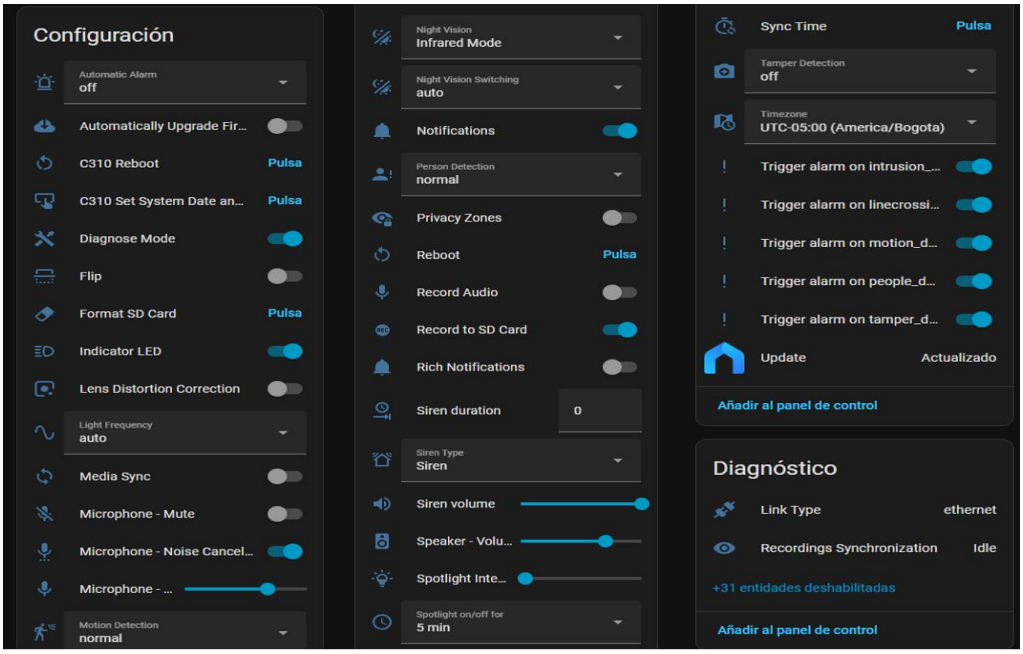
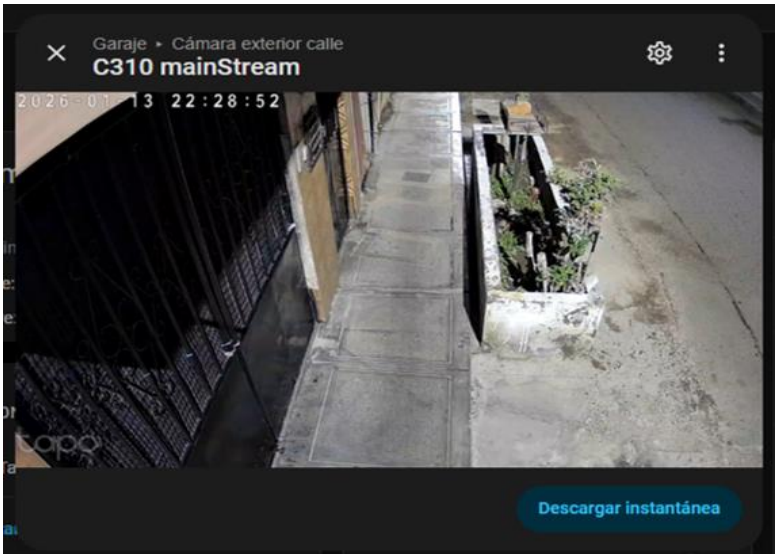


Figura 67

Visualización en tiempo real para Tapo C310



Ahora se procede a implementar la comunicación de la misma cámara mediante ONVIF en Home Assistant, comenzando por la búsqueda del servicio ONVIF en la tienda oficial de Home Assistant y, seguidamente, con ayuda de la figura 68 se aprecia la búsqueda manual al ser la primera vez. Una vez encontrado el dispositivo, se despliega una ventana con toda la información que el complemento encontró, tal como indica la figura 69, teniendo como puerto por defecto el 554, ya que es el puerto estándar usado para RTSP, que soporta protocolos TCP y UDP. La figura 70 concluye la integración con la visualización exitosa del streaming en tiempo real de la cámara C310 en Home Assistant.

Figura 68

Búsqueda manual al ser primera vez

Figura 69

Configuración del dispositivo utilizando el puerto 554

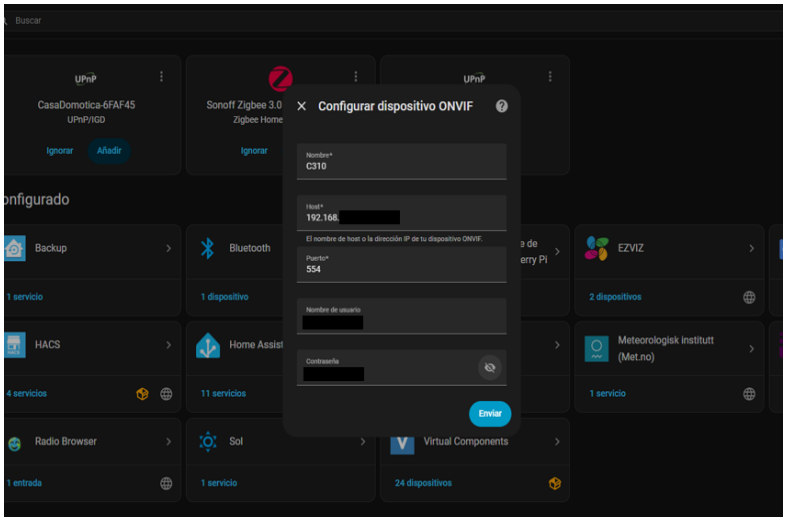
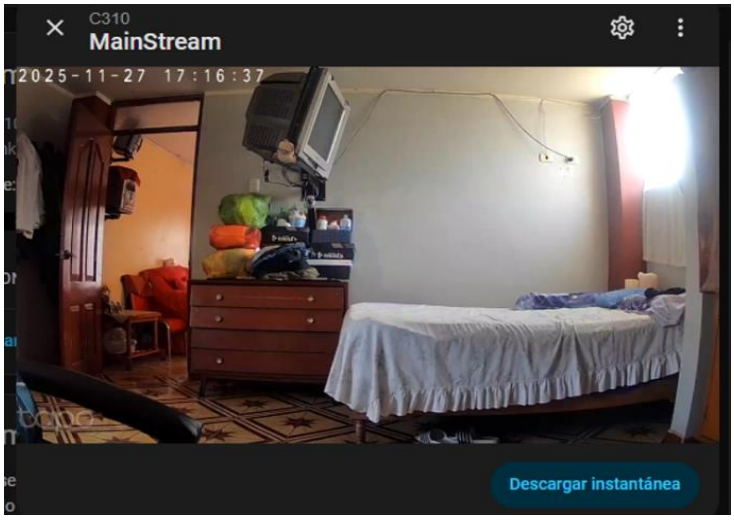


Figura 70

Visualización de transmisión en vivo

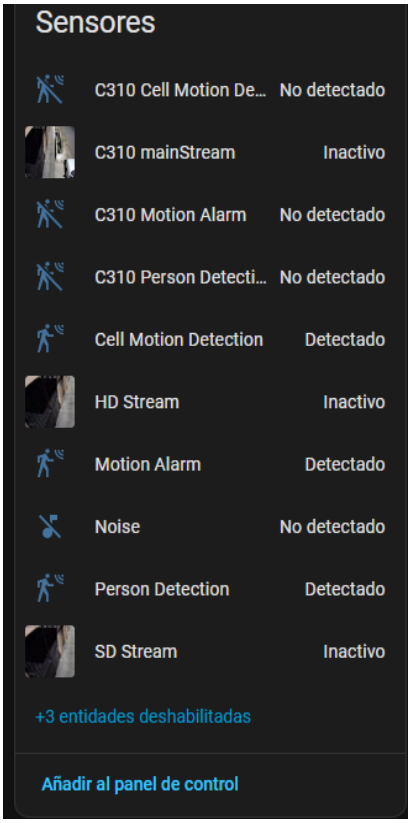


La integración Tapo Cameras Control, mantenida por la comunidad, se instala como componente personalizado (custom_component) o mediante la integración TP-Link/Tapo en Home Assistant. Esta herramienta ofrece entidades específicas para cámaras Tapo y expone controles y eventos que no siempre están disponibles por RTSP/ONVIF (JurajNyiri, 2026). Sin embargo, durante la visualización en tiempo real se detectó un retraso preocupante de aproximadamente diez segundos entre fotogramas, lo cual puede resultar útil para una previsualización inicial, pero es inadecuado para

escenarios de seguridad frente a intrusos. Tal como se observa en la figura 71, esta integración mostró únicamente las siguientes visualizaciones:

Figura 71

Exposición de funciones



3.5.5.2. Tapo C200

Del mismo modo que en las figuras 64 y 66, se aplicó el procedimiento a la cámara Tapo C200, ya que, como se pudo apreciar antes, las diferencias principales radican en la cantidad de entidades expuestas, las cuales son muy importantes en algunos casos específicos en los que se quisieran desarrollar automatizaciones en diversos contextos y escenarios. Por lo tanto, el método es el mismo, con ligeras variaciones, como la dirección IP y la cuenta en la nube de Tapo de la cámara y la del usuario, respectivamente visto en las figuras 72, 73 y 74.

Figura 72

Asignación de dirección IP de la cámara Tapo C200

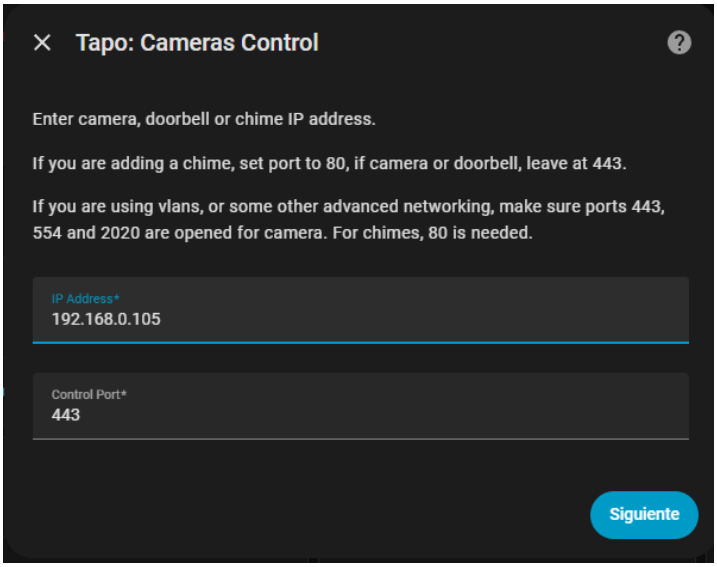


Figura 73

Exposición de entidades para Tapo C200

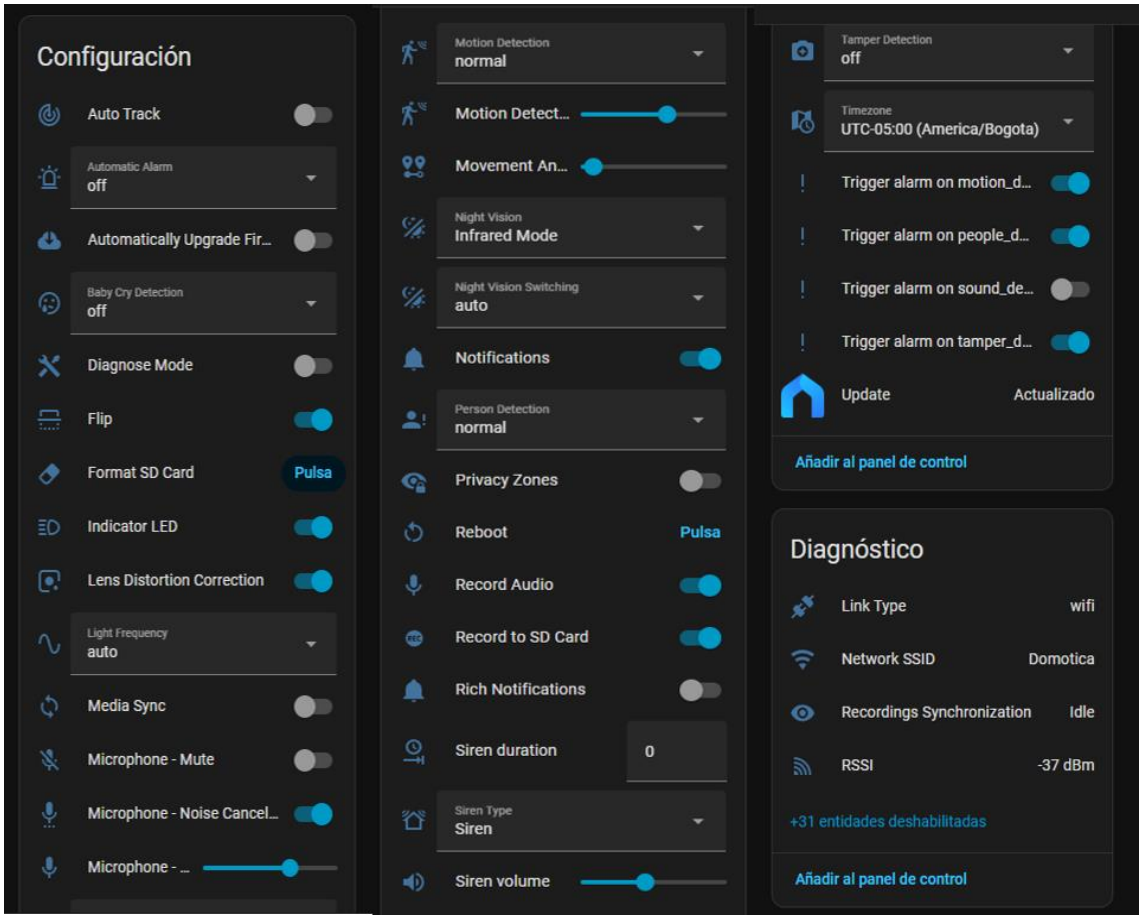
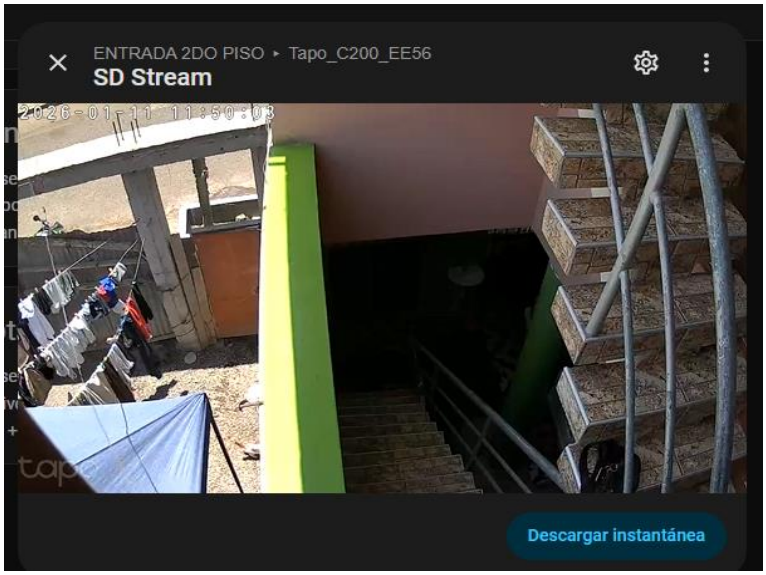


Figura 74

Visualización en tiempo real para Tapo C200



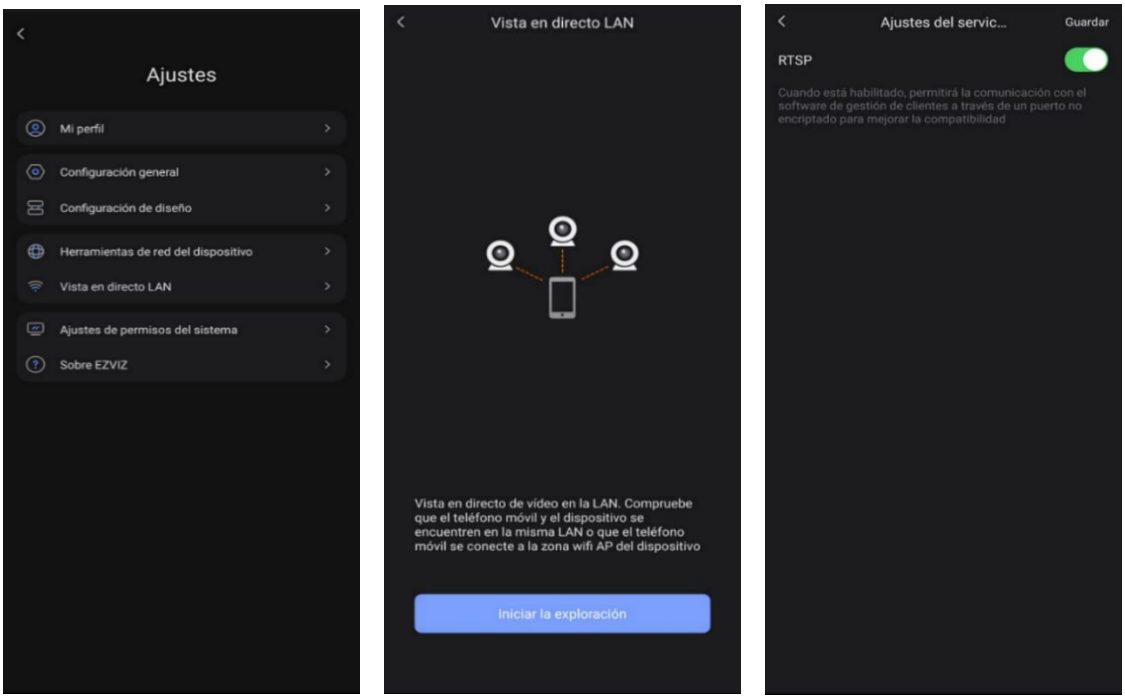
3.5.5.3. Ezviz C6N

La integración oficial de Ezviz para Home Assistant se apoya en la API de Ezviz (ezvizlife.com) para recuperar información de dispositivos y estados, y complementa ese acceso en la nube con la exposición del stream RTSP local usando la IP de la cámara. Esto exige que el host de Home Assistant tenga acceso a la red local de las cámaras. Esta doble vía (API cloud + RTSP local) permite tanto la sincronización de metadatos y eventos como la ingestión eficiente del vídeo para visualización y grabación local. (RenierM26, 2026)

El procedimiento inicial fue instalar la aplicación Ezviz en el teléfono móvil, crear una cuenta y, posteriormente, configurar la cámara en la aplicación principal. El emparejamiento puede realizarse mediante Wi-Fi o cable Ethernet. La personalización de sus características depende de la posición, la ubicación y el contexto en que se encuentre el dispositivo. Una vez emparejado, para que el dispositivo logre comunicarse con Home Assistant se debe configurar un nombre de usuario y una contraseña que permitan el enlace; antes de ello, es primordial habilitar la opción RTSP, como se ve en la figura 75.

Figura 75

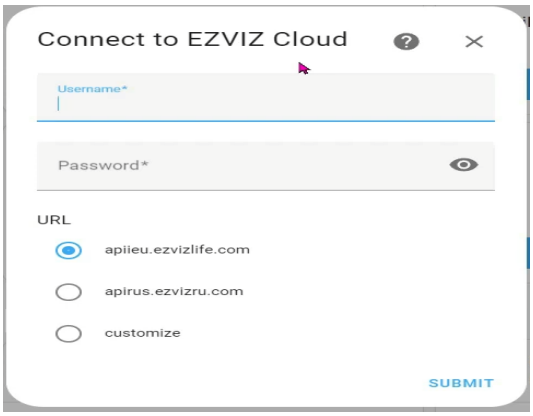
Habilitación de protocolo RTSP



Una vez habilitada la opción, se busca la integración de Ezviz en la tienda de complementos. Como se muestra en la figura 76, hay que autenticar con las credenciales de la cuenta Ezviz (que permiten el acceso a la API cloud) y verificar que Home Assistant puede alcanzar la IP local de la cámara para acceder al stream RTSP.

Figura 76

Conexión por Ezviz Cloud

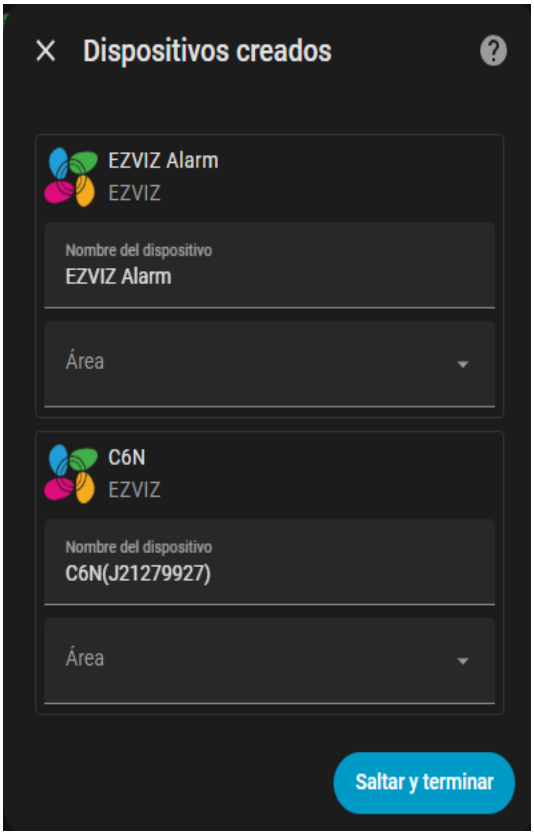


Nota. En este apartado se debe colocar el correo electrónico de la cuenta vinculada a Ezviz y su respectiva contraseña.

Si la integración de la cámara Ezviz es exitosa, deberían aparecer dos dispositivos creados, véase la figura 77, uno que agrupa las entidades de control y los sensores de la cámara, y otro que corresponde a la alarma de la cámara. Por defecto, ambas integraciones se añaden por separado, designación realizada por la propia empresa Ezviz. No obstante, con esto la adición de la cámara aún no está completa: se necesita el nombre de usuario y la contraseña de la propia cámara, tal como se muestran en las figuras 78 y 79.

Figura 77

Integración exitosa de cámara Ezviz



Nota. Se añaden entidades de control y sensores con alarma separada; la transmisión de imágenes en tiempo real aún no está implementada, requiere un siguiente paso.

Figura 78

Adición de la transmisión SD y HD stream

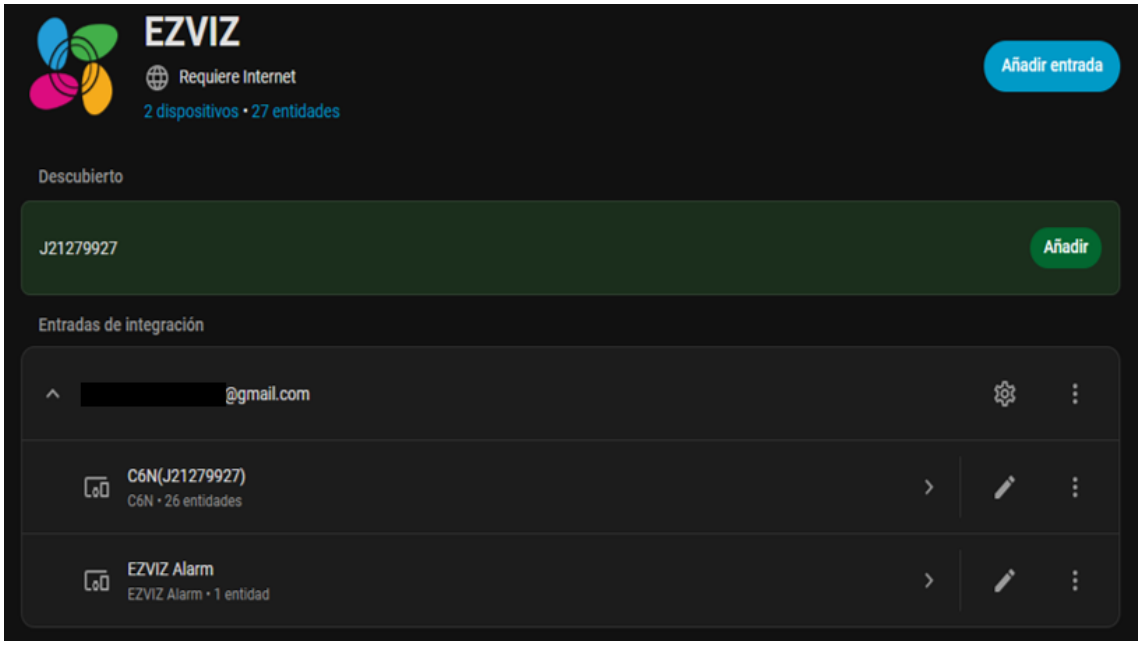
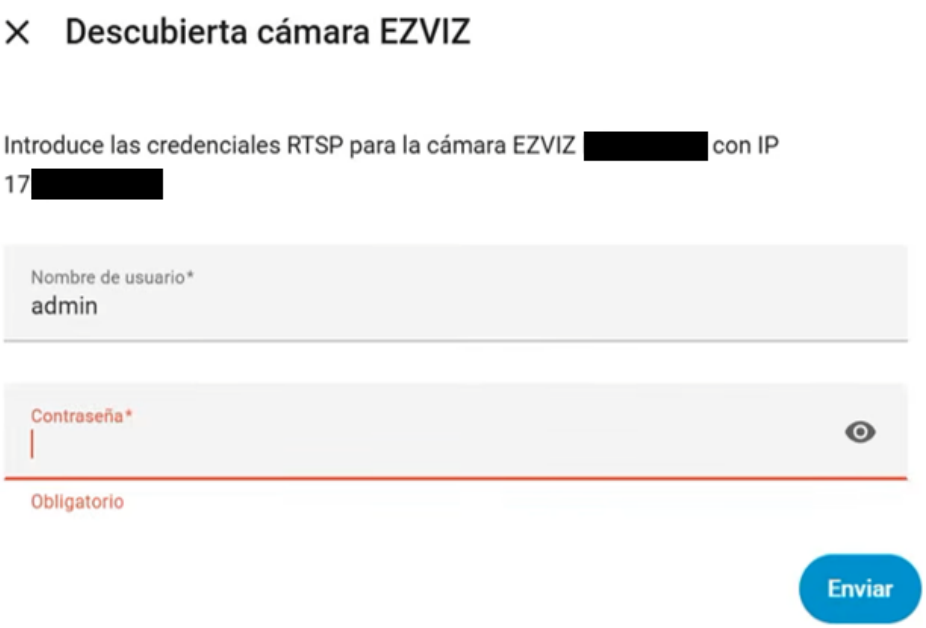


Figura 79

Identificación para agregar la cámara Ezviz



Nota. En el apartado de Username siempre va a estar designado como admin, esto por designación del fabricante; sin embargo, en el apartado de Password, se introduce el código de verificación que se encuentra en la etiqueta ubicada en la parte posterior de la cámara.

Una vez ingresados correctamente los valores, la integración se completará satisfactoriamente, como se puede ver en las figuras 80 y 81, que muestran todas las entidades de la cámara y la transmisión en vivo.

Figura 80

Entidades agregadas por Ezviz

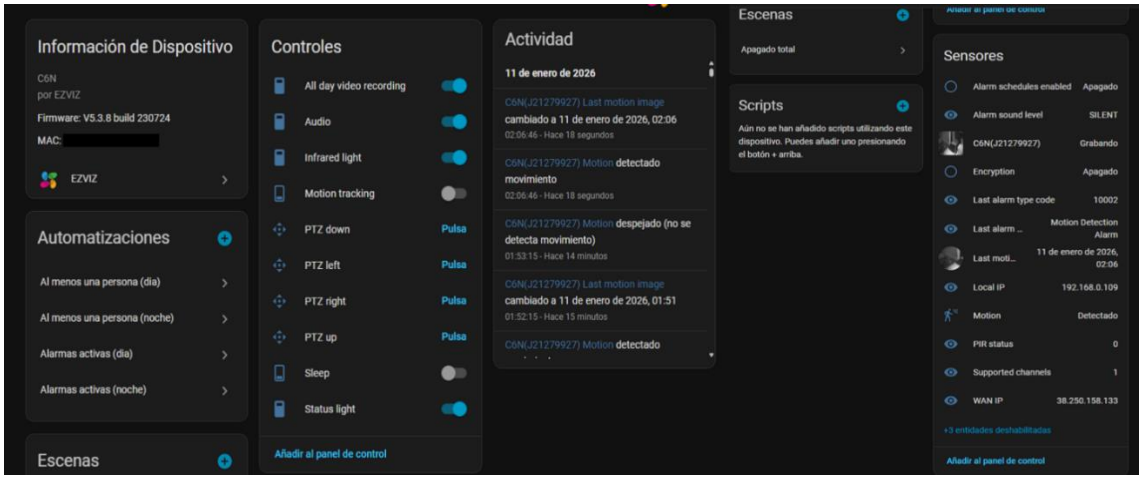


Figura 81

Visualización en tiempo real para Ezviz C6N

Para realizar grabaciones locales en las cámaras, se necesitan tarjetas de memoria compatibles con las especificaciones de cada modelo. Antes de cualquier instalación, se insertó en cada dispositivo su tarjeta correspondiente para que, desde la aplicación de cada cámara, se realice el proceso de formateo. Una vez completado el

formateo, podemos ver el estado del almacenamiento, tal como se muestra en el anexo 4 para la cámara Ezviz, mientras que en el anexo 5 se observa lo mismo para las cámaras Tapo.

Por último, se realizó la geolocalización (geoposicionamiento) usando la función nativa de Home Assistant en la sección Aplicación complementaria (solo en la versión móvil). Esta opción calcula la ubicación con datos GPS mediante la API de ubicación de Google; el proceso está ilustrado en los anexos. Además, se asignaron zonas desde la sección Áreas, etiquetas y zonas de Home Assistant; cada usuario puede crear las que necesite. Las zonas creadas con sus nombres aparecen en los anexos 6 y 7.

3.5.6. Respaldos del sistema domótico

En las figuras posteriores se expone el procedimiento continuo de las copias de seguridad automáticas de forma local, el cual es un proceso simple e intuitivo. Nos dirigimos a Configuración, luego a Sistema y Copias de seguridad; veremos algo similar a la figura 82 y generaremos una clave de encriptación, como se muestra en la figura 83; por último, en la figura 84 vemos la primera copia de seguridad manual.

Figura 82

Configuración para las futuras copias de seguridad

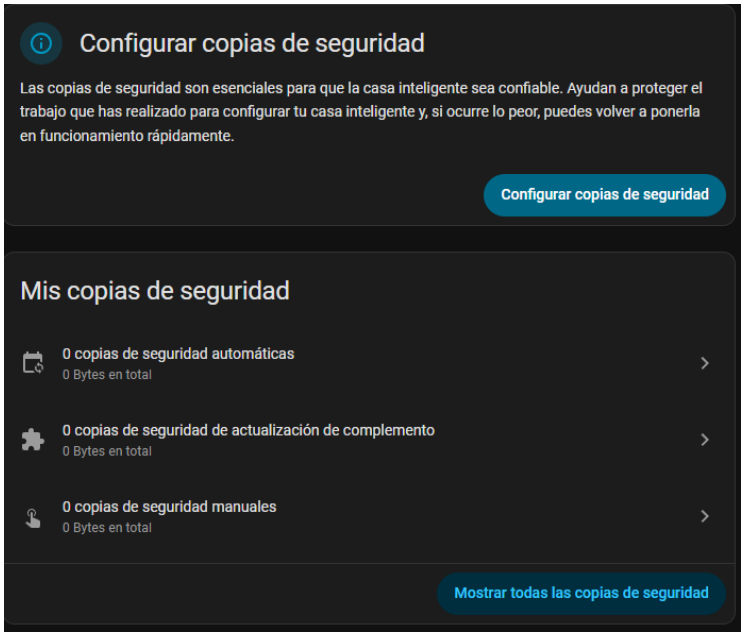
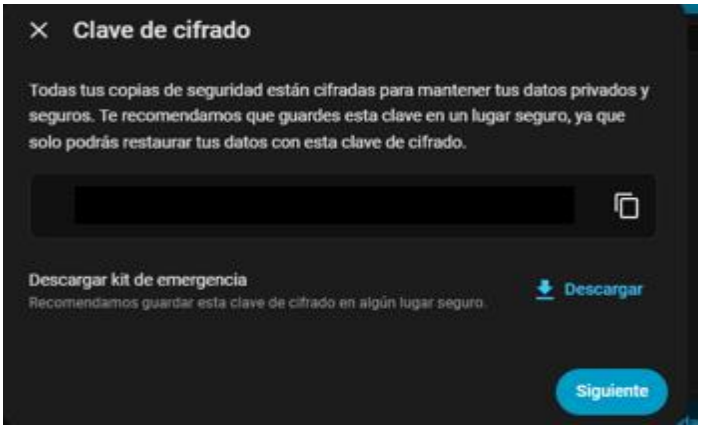


Figura 83

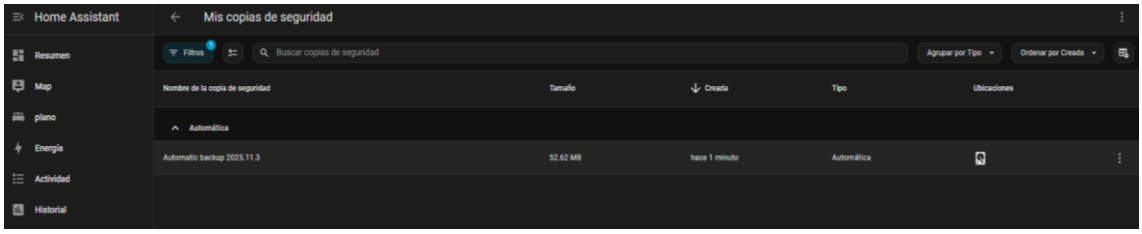
Clave de encriptación



Nota. Esta clave es importante porque se usa para encriptar los backups y restaurar los mismos.

Figura 84

Primera copia de seguridad manual



Nota. La primera copia de seguridad siempre se realizará de manera local en el mismo disco donde se está ejecutando Home Assistant.

3.5.6.1. Copias de seguridad en OneDrive

Al realizar copias de seguridad de Home Assistant en OneDrive se protege la integridad y disponibilidad de la configuración y los datos domóticos frente a ransomware, borrados accidentales y fallos de hardware, y se facilita la recuperación rápida y verificable de estados e historiales. A continuación, se desarrollan los puntos mencionados:

- Protección contra ransomware y recuperación: Incluye la detección e identificación de infecciones para limpiar dispositivos y restaurar archivos desde versiones seguras, además de recuperar la instancia tras un ataque (Microsoft, 2026).
- Versionado, retención y recuperación ante borrados accidentales: Mantiene historiales de versiones para restaurar archivos eliminados o revertir cambios

dentro de ventanas temporales, protegiendo contra errores humanos y fallos de sincronización; facilita pruebas, migraciones y recuperación (Tran, 2025).

Para la copia de seguridad básica, en Complementos añadimos la integración OneDrive, como se muestra en la figura 85. Al elegirla se abre una pestaña del navegador para iniciar sesión en la cuenta donde se guardarán las copias; se recomienda usar un correo exclusivo para la domótica. En la figura 86, Microsoft solicita permisos para acceder y almacenar las copias. OneDrive aparecerá como servicio, acorde con lo mostrado en la figura 87, para posteriormente integrarlo en el servidor.

Figura 85

Búsqueda de integración OneDrive

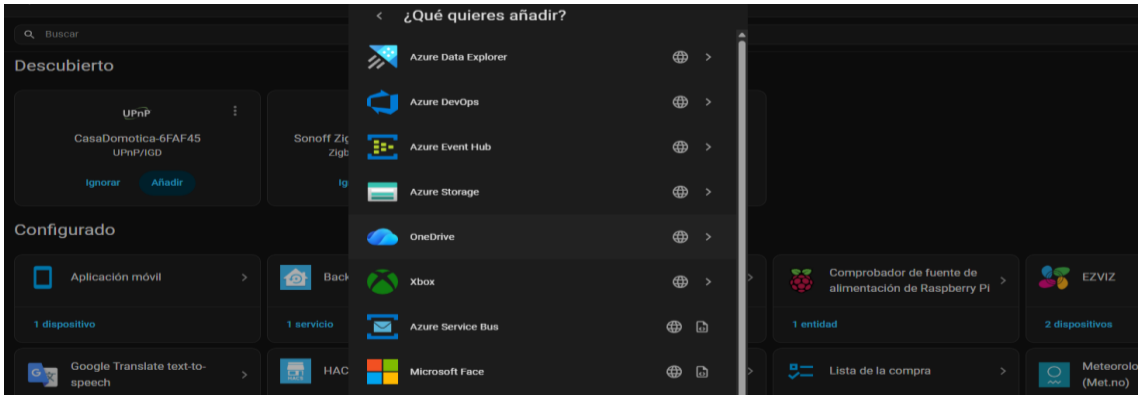
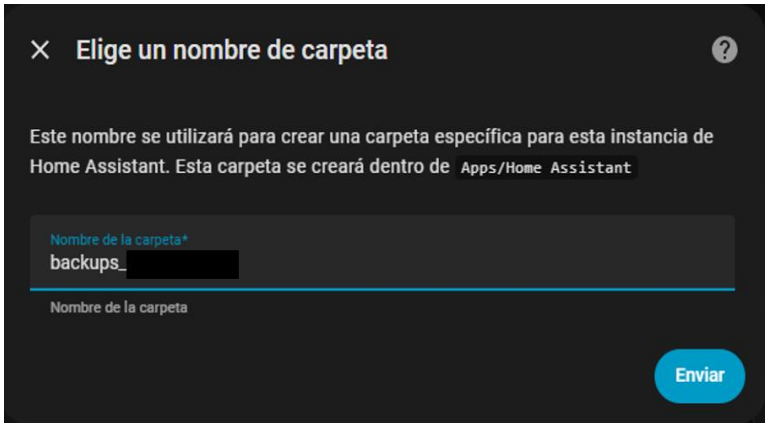


Figura 86

Permisos de Home Assistant

Figura 87

Creación de una nueva carpeta para guardar los backups



3.5.6.2. Copias de seguridad en Google Drive

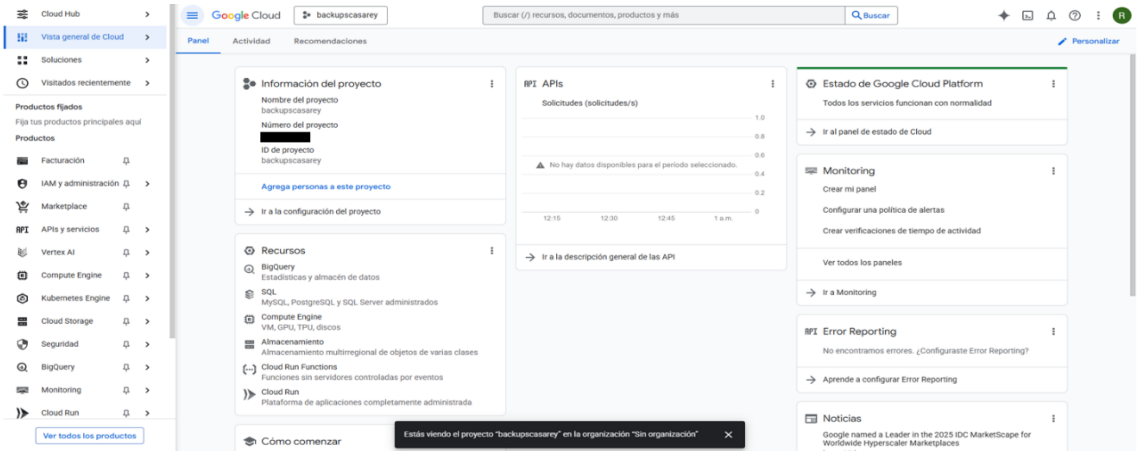
Existen varias opciones maduras para almacenar copias de seguridad de Home Assistant en Google Drive; las más comunes son Home Assistant Google Drive Backup, soluciones basadas en rclone (add-on o scripts) y flujos híbridos que combinan Auto Backup con sincronización a la nube. Este enfoque reproducible permite crear snapshots automáticos, sincronizarlos con Google Drive y gestionar retenciones desde la interfaz de Home Assistant (Beechen, 2026). En esencia, Google Cloud agrupa servicios de computación, almacenamiento, redes, análisis de datos y aprendizaje automático para ejecutar aplicaciones y almacenar datos en centros de datos; su objetivo es ofrecer escalabilidad, resiliencia y herramientas gestionadas que reduzcan la carga operativa (Google Cloud, 2026).

Para que la integración sea exitosa es necesaria la interfaz web de Google Cloud Console; desde allí se crean proyectos, se habilitan APIs y se generan las credenciales OAuth o Service Accounts que requiere el add-on para que Home Assistant pueda leer y escribir backups en Google Drive. En entornos con conexiones limitadas, como Tacna, conviene planificar cuotas y ventanas de sincronización antes de habilitar integraciones en producción (Home Assistant, 2026).

El primer paso es registrar una cuenta en la consola de Google Cloud, lo que permite gestionar, monitorizar y configurar los recursos y servicios de la plataforma. Una vez creada la cuenta, se crea un nuevo proyecto y se obtienen las credenciales OAuth que el add-on necesita para autenticarse con Google Drive; esto se muestra con mayor detalle en las figuras siguientes. Al tener creado el proyecto, se mostrará una vista general de Cloud similar a la figura 88.

Figura 88

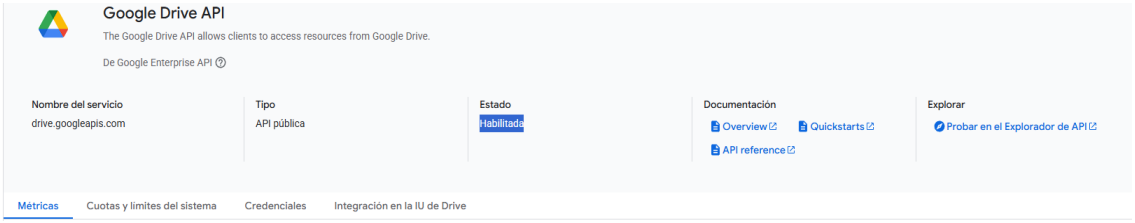
Registro del nuevo proyecto



Debemos buscar y activar la API de Google Drive para que Home Assistant pueda crear, leer y gestionar archivos en Google Drive; sin ella no es posible subir snapshots de forma segura. Esto equivale a crear una aplicación en la cuenta para obtener las claves que permitan la conexión. Por seguridad, volvemos al proyecto creado y verificamos que la API esté habilitada (fig. 89).

Figura 89

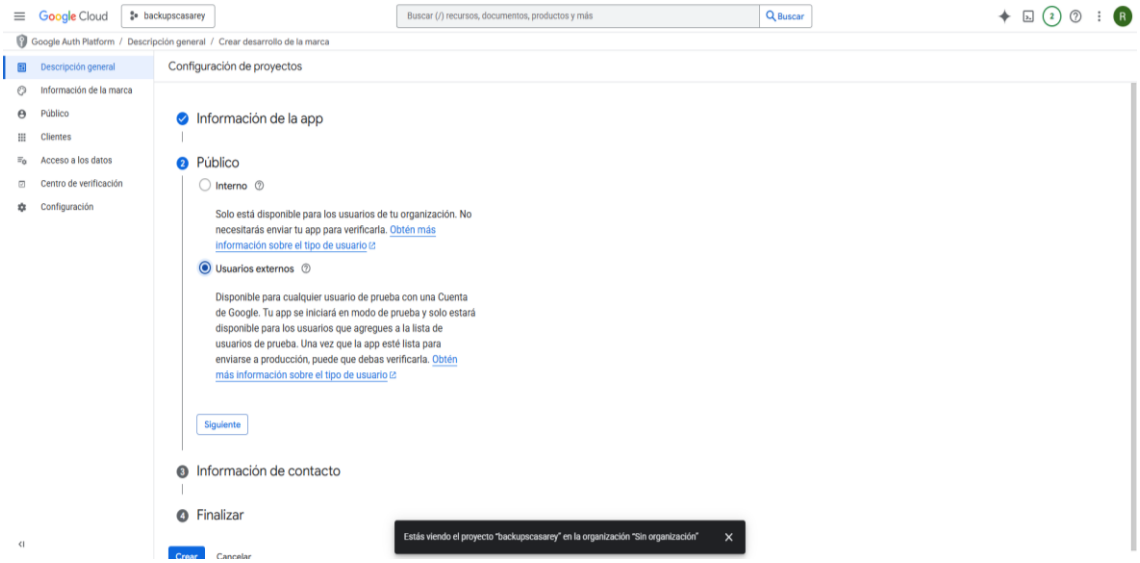
Activación de Google Drive API



Teniendo la API activa, accedemos a la pantalla de consentimiento OAuth, que informa al usuario sobre los permisos que solicita la aplicación, permite a Google gestionar y limitar esos permisos y es requisito para generar credenciales seguras que el add-on de backups de Home Assistant usará para acceder a Google Drive. En esa pestaña ingresamos los datos de la cuenta. Por defecto está seleccionado Interno (solo dentro de una organización); al elegir Externo, la aplicación autoriza cuentas personales o cuentas fuera de la organización. Aceptamos los términos y creamos la pantalla de consentimiento OAuth (fig. 90).

Figura 90

Selección para Usuarios Externos



Nota. Cambiar a usuarios externos permite que la app solicite consentimiento a cuentas fuera del dominio de tu organización (cuentas personales de Google).

Seguidamente vamos a Publicar y cambiamos el estado de la publicación; por defecto está en "prueba", lo que impide que cualquier cuenta Google autorice la app sin restricciones. Para que el add-on funcione establemente es necesario pasar a "en producción". Después buscamos Credenciales y en API y servicios y creamos una nueva credencial: ID de cliente OAuth, como se muestra en las figuras 91 y 92.

Figura 91

Modificación del estado de la publicación a “En producción”

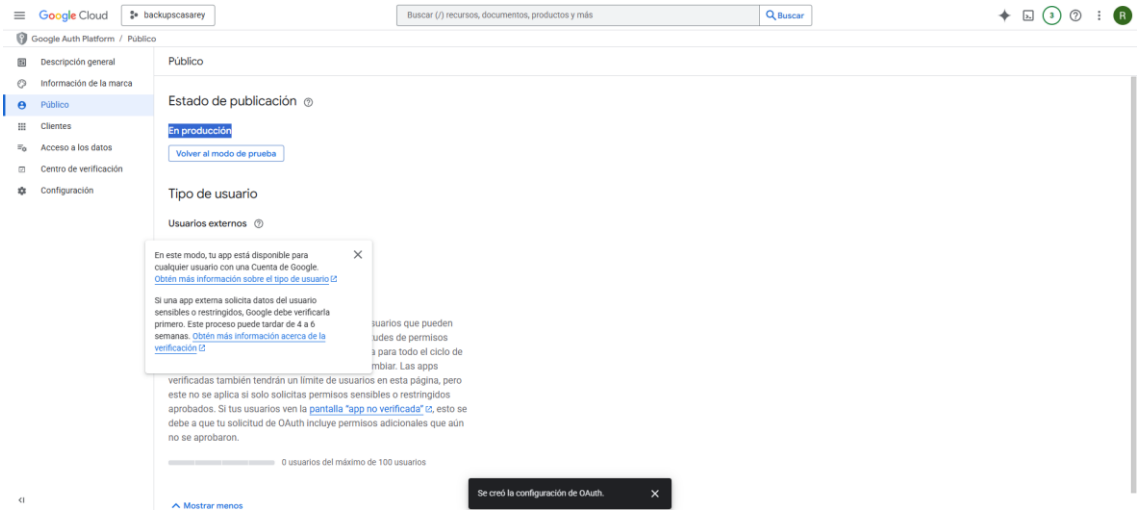
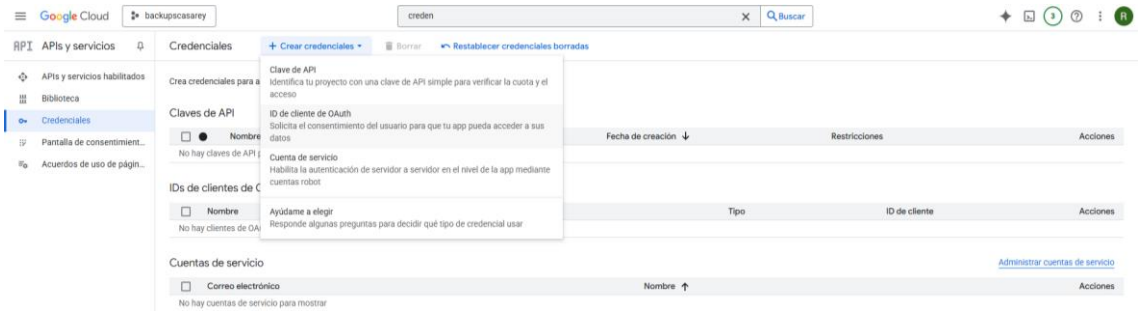


Figura 92

Generar una nueva credencial para un cliente OAuth

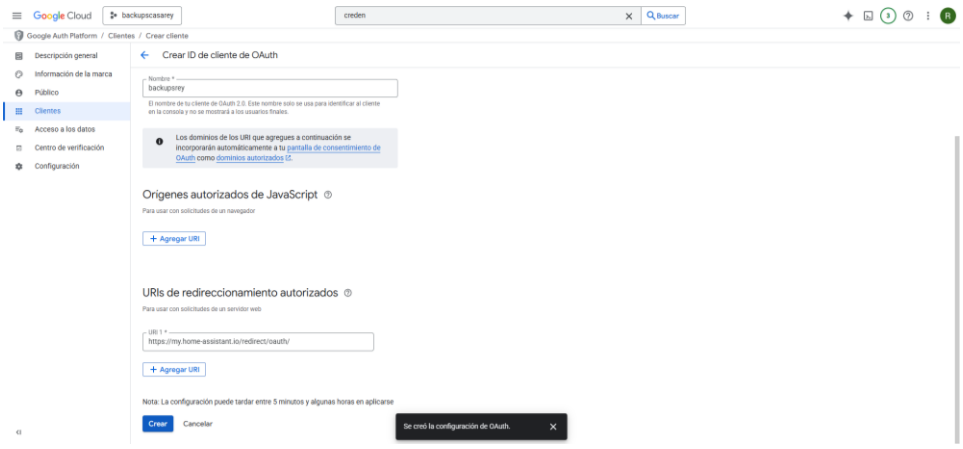


Al realizar estos pasos, permitimos que el ID de cliente OAuth identifique y autentifique la aplicación ante Google para obtener tokens seguros que el add-on usará para acceder y gestionar archivos en Google Drive sin compartir la contraseña. Es muy importante seleccionar el tipo de aplicación Aplicación web, ya que Home Assistant emplea un flujo OAuth que redirige a una URL en nuestra instancia; Aplicación web permite registrar ese URI y manejar la autorización basada en navegadores y redirecciones.

Solo falta introducir la URI de redirección (la cadena que identifica de forma única el recurso en la web) con la dirección mostrada en la figura 93; esa es la URL exacta a la que Google envía el código de autorización (y luego el token). Tras aceptar los permisos, si la URI no coincide, la autorización fallará.

Figura 93

En URL de redireccionamiento

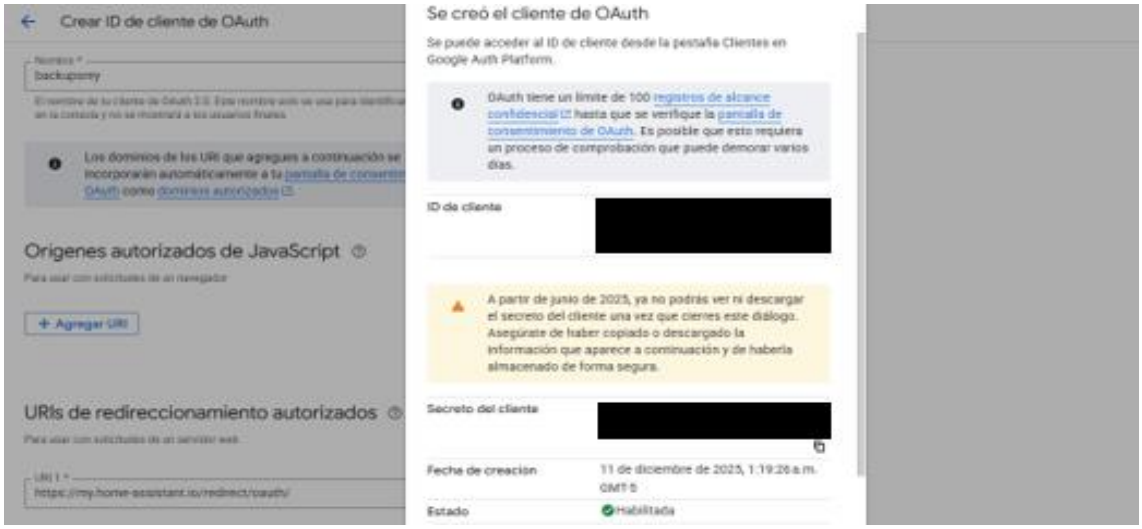


Nota. En esta sección es muy importante añadir la siguiente URL sin ninguna modificación: https://my.home-assistant.io/redirect/oauth

Al completar todos los pasos previos, se generarán un ID de cliente y un secreto del cliente, como se muestra en la figura 94. Son datos sumamente importantes y privados que nos pedirá el servicio de Google Drive en Home Assistant. Luego nos dirigimos a nuestro servidor de Home Assistant y buscamos el servicio de Google Drive, como aparece en la figura 95. Una vez dentro, nos pedirá un nombre para la carpeta de guardado y el ID y el secreto del cliente, tal como se visualiza en la figura 96.

Figura 94

Creación del ID del cliente y el secreto del cliente



Nota. El ID del cliente y el secreto del cliente no se podrá ver despues de que se entregue, es fundamental guardarlos y evitar perderlos.

Figura 95

Búsqueda de Google Drive como integración

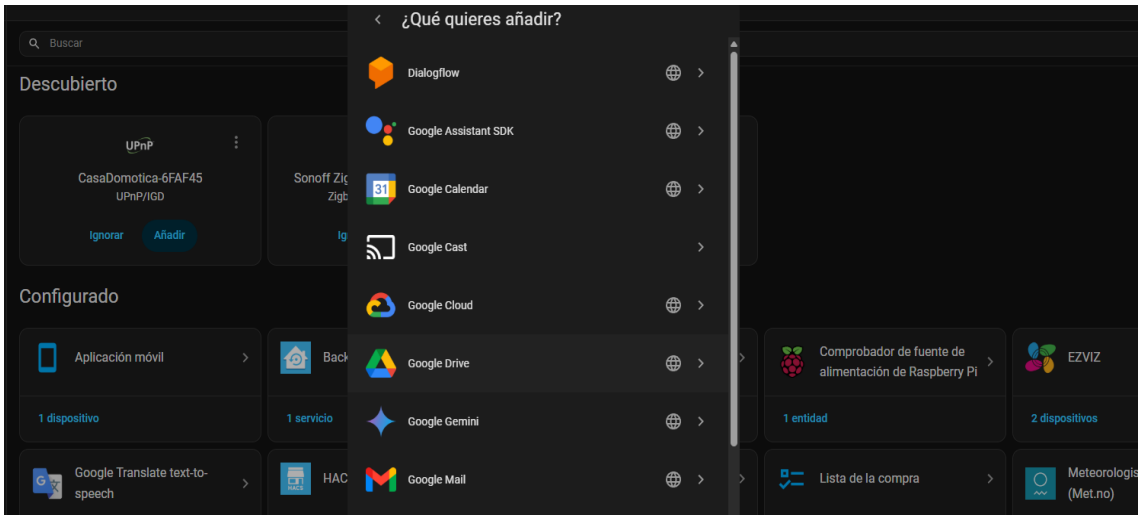


Figura 96

Asignación de un nombre y los datos del cliente

Una vez concretado esto, se procederá a autorizar los permisos para el servicio de copias de seguridad y, a continuación, veremos la vinculación entre Google Drive y Home Assistant, concluyendo el proceso con éxito, como se refleja en la figura 97. Completadas las copias de seguridad en OneDrive y Google Drive, las figuras 98 y 99 muestran el proceso de copias de seguridad automáticas en Home Assistant.

Figura 97

Integración exitosa de Google Drive

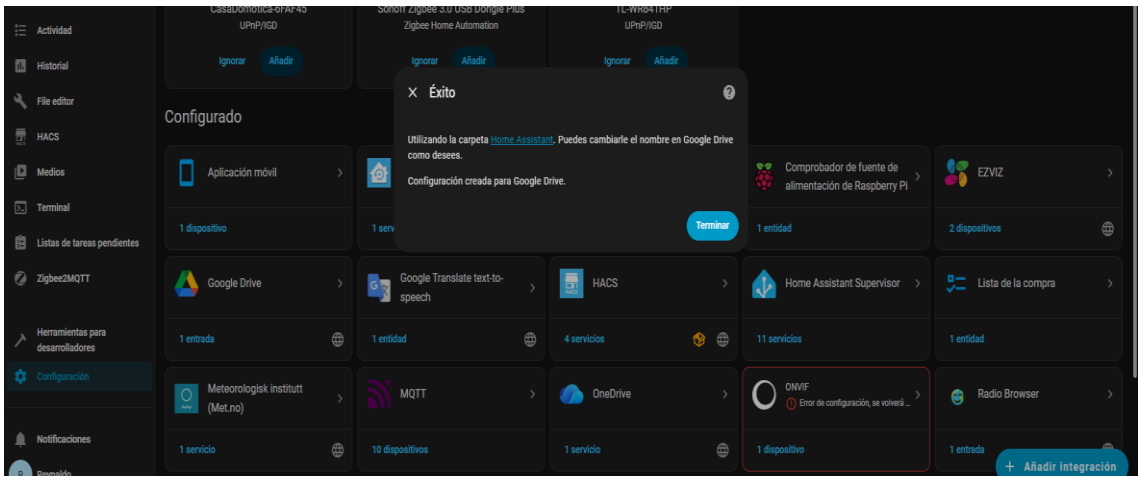


Figura 98

Nuevas ubicaciones paras las futuras copias de seguridad

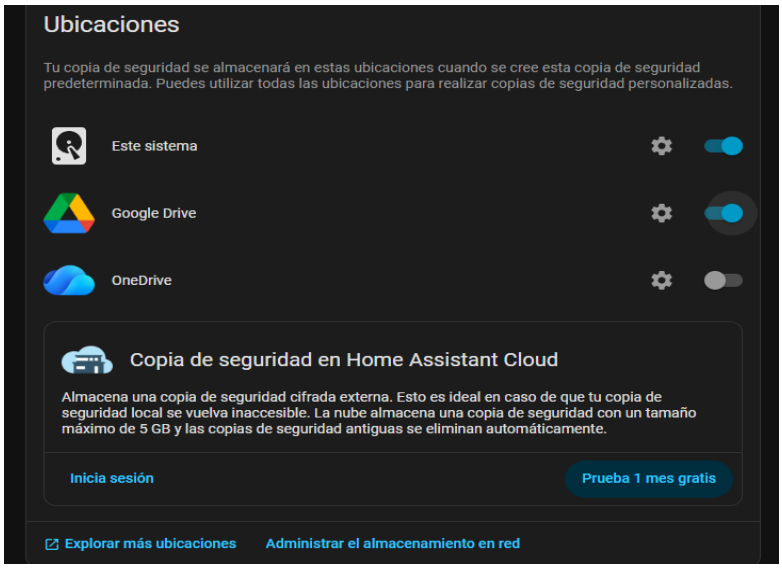
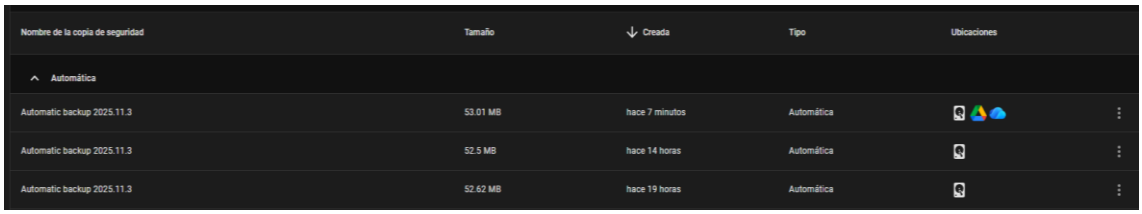


Figura 99

Visualización de las 3 últimas copias de seguridad realizadas



Para contrastar la información anterior, las figuras 100 y 101 confirman que se ha realizado una copia de seguridad de Home Assistant tanto en OneDrive como en Google Drive, en el orden indicado y en los mismos intervalos de tiempo.

Figura 100

Comprobación de copias de seguridad realizadas posteriormente en OneDrive

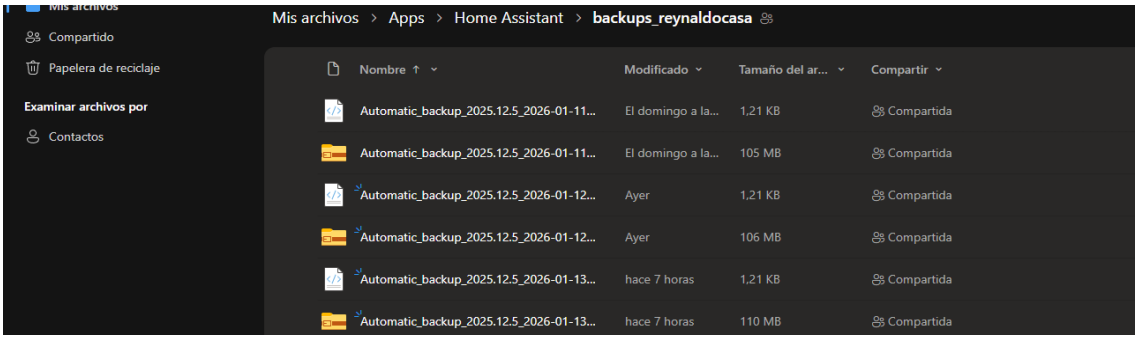


Figura 101

Comprobación de copias de seguridad realizadas posteriormente en Google Drive

3.5.7. Integración de VPN en el servidor

Primero, se debe buscar el complemento de Tailscale en Home Assistant y, a continuación, instalarlo en el servidor. El registro del proceso de instalación en los registros del complemento se muestra en la figura 102. Una vez iniciado el complemento, abrimos la interfaz gráfica de usuario, ubicada en la parte inferior del panel principal; allí nos pedirá que iniciemos sesión. Tras ingresar nuestros datos, conectaremos el servidor de Home Assistant con el servidor de Tailscale, tal como se muestra en la figura 103. Previamente, debemos haber creado una cuenta en la página oficial de Tailscale. Existen versiones gratuitas para trabajar; esa fue la opción elegida en este caso.

Figura 102

Registros del complemento Tailscale al momento de iniciar

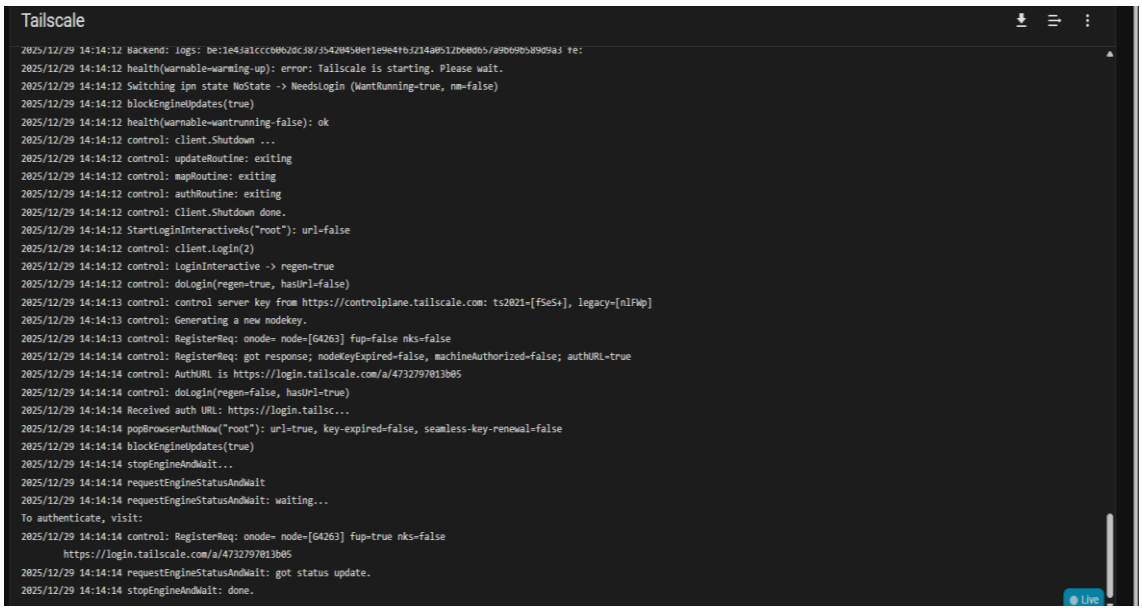
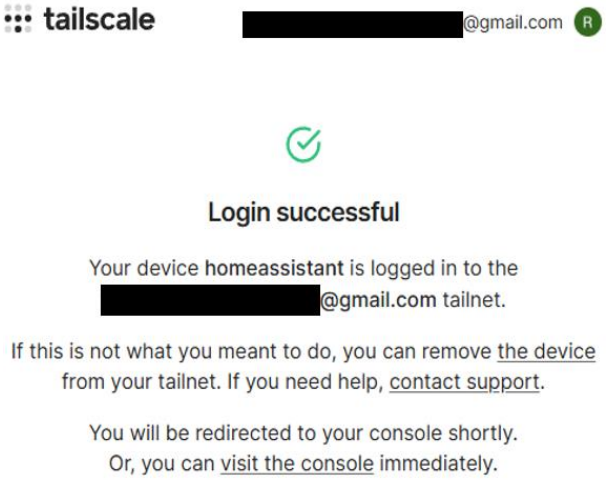


Figura 103

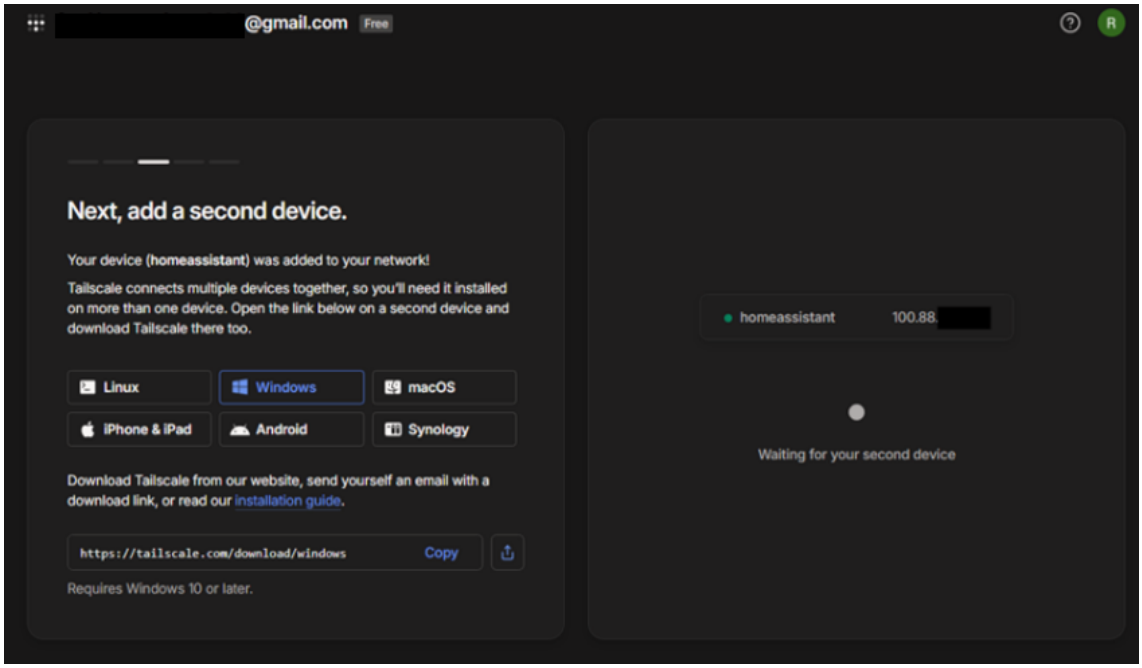
Conexión establecida entre ambos servidores



En esta instancia podemos ver la conexión entre ambos servidores. La figura 104 muestra el panel de Tailscale con los datos ingresados y la opción de añadir más dispositivos para que se comuniquen entre ellos de forma segura. La IP que tiene, en este caso homeassistant, es una IP privada y es la única disponible; para poder acceder a ella necesitamos al menos un segundo dispositivo.

Figura 104

Instancia de Home Assistant conectada

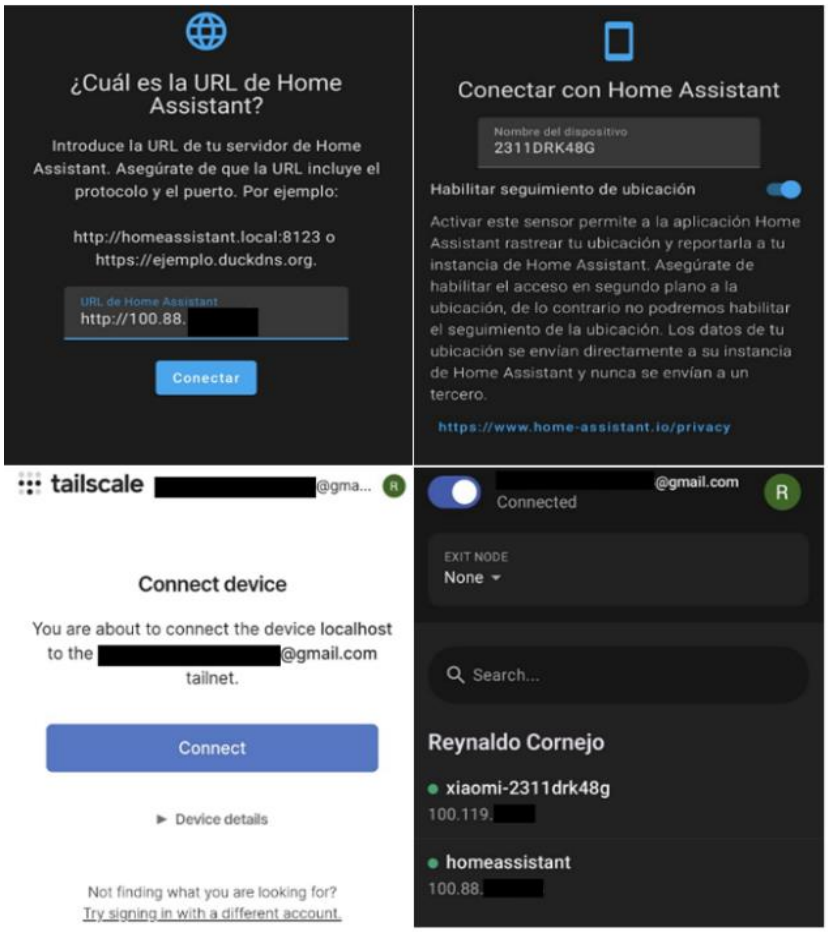


3.5.7.1. Tailscale en móvil

Para acceder al servidor de Home Assistant desde cualquier lugar mediante la VPN privada de Tailscale, el servidor y el dispositivo deben comunicarse como si compartieran la misma LAN. De este modo quedan en una red privada común, independiente de CGNAT o de las limitaciones del ISP, aspecto clave en una infraestructura híbrida. Primero instalamos la aplicación oficial desde Play Store en el móvil y nos registramos con la cuenta de Tailscale. Tras la conexión, copiamos la dirección que Tailscale proporciona e ingresamos esa IP en la aplicación de Home Assistant. Ambos dispositivos mostrarán las direcciones internas de Tailscale y podremos acceder al servidor siempre que tengamos conexión a Internet y estemos conectados al túnel VPN. La figura 105 sintetiza el proceso de adición de un móvil personal a Tailscale, condensado en cuatro imágenes correlativas; en ellas se indica la dirección IP privada de Home Assistant que proporcionó el servidor VPN en la figura 104 y se muestra la conexión del móvil con la misma cuenta de Tailscale.

Figura 105

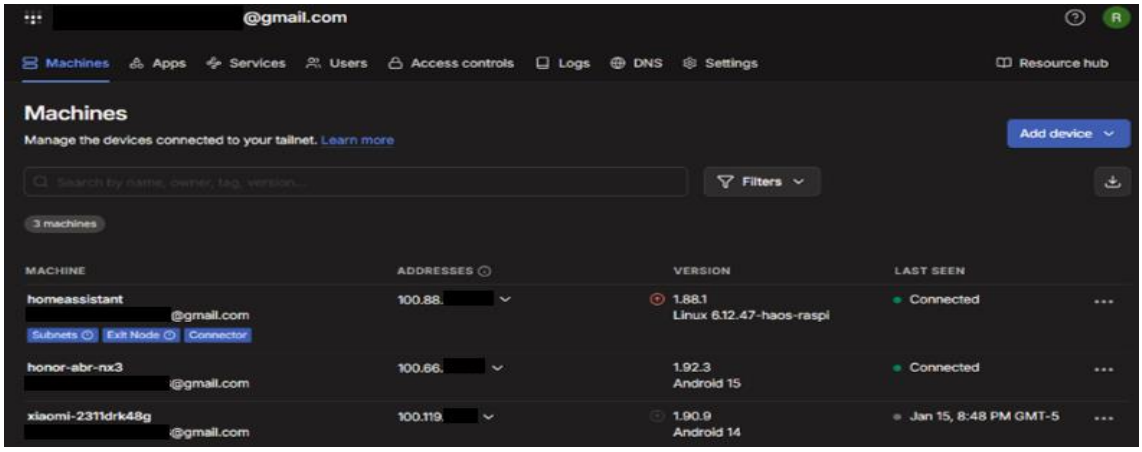
Configuración en la aplicación móvil



Con la ayuda de la figura 106 podemos comprobar la adición del móvil al servidor VPN. Además, se integró un segundo teléfono para complementar la comunicación entre el sistema domótico y los usuarios autorizados.

Figura 106

Consola de administración de dispositivos

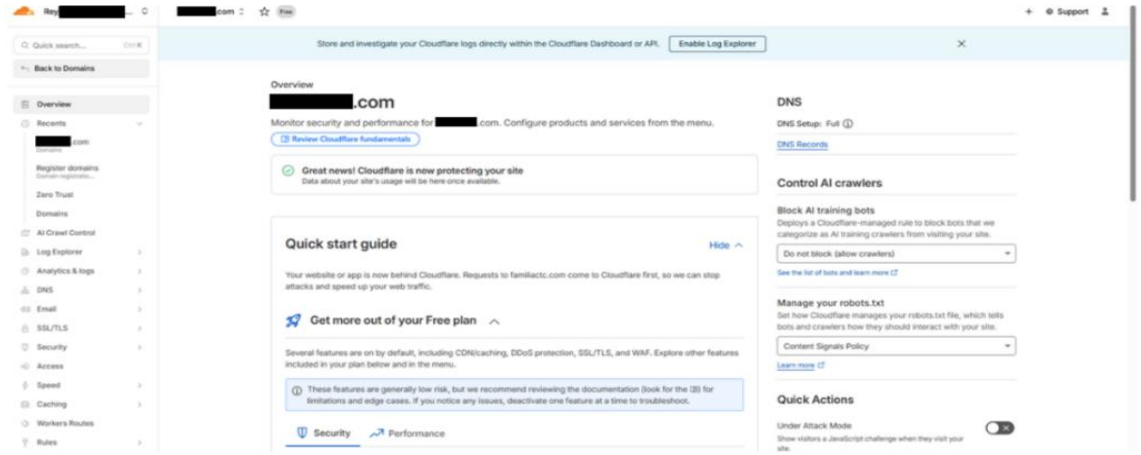


3.5.8. Exposición de servidor domótico a internet mediante Cloudflare

Lo primero es adquirir un dominio propio; esto se puede obtener de muchas formas. Si no se cuenta con una IP pública fija o se está bajo CGNAT, no es posible utilizar subdominios de servicios como DuckDNS. Por ello se optó por comprar un dominio en la página oficial de Cloudflare, como se muestra en la figura 107.

Figura 107

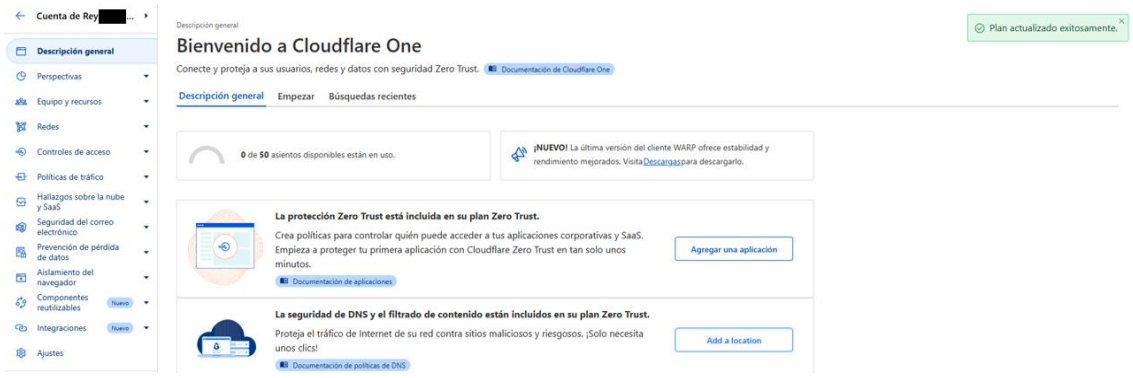
Registro del dominio con Cloudflare



Con el dominio registrado, nos dirigimos a la sección de Cloudflare Zero Trust, que protege y controla el acceso a las aplicaciones y al DNS del usuario. Asignamos un nombre cualquiera y escogemos la versión gratuita. A continuación, se nos redirige a la página principal, como se muestra en la figura 108.

Figura 108

Panel principal de Cloudflare Zero Trust



A partir de aquí comenzamos a configurar el control y el acceso remoto en Internet. Debemos crear un nuevo túnel como en la figura 109 para exponer el servicio local de Home Assistant sin abrir puertos ni disponer de una IP pública, lo cual era el principal problema en este caso. Hay que asignar un nombre de referencia al túnel. Posteriormente, como indica la figura 110, se ingresa un subdominio y el nombre de nuestro dominio previamente registrado, apuntando a la dirección de nuestro servidor local con su respectivo puerto.

Figura 109

Abrir el panel principal para túneles

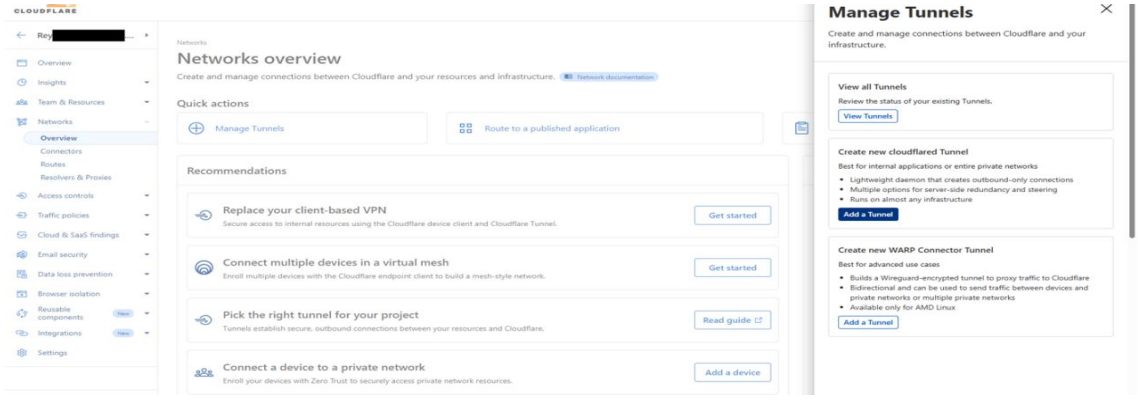
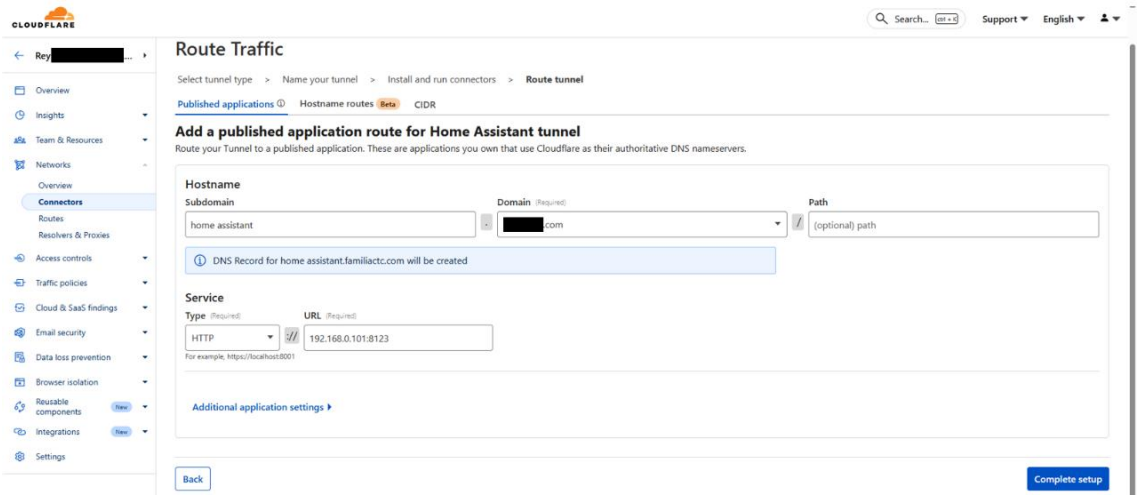


Figura 110

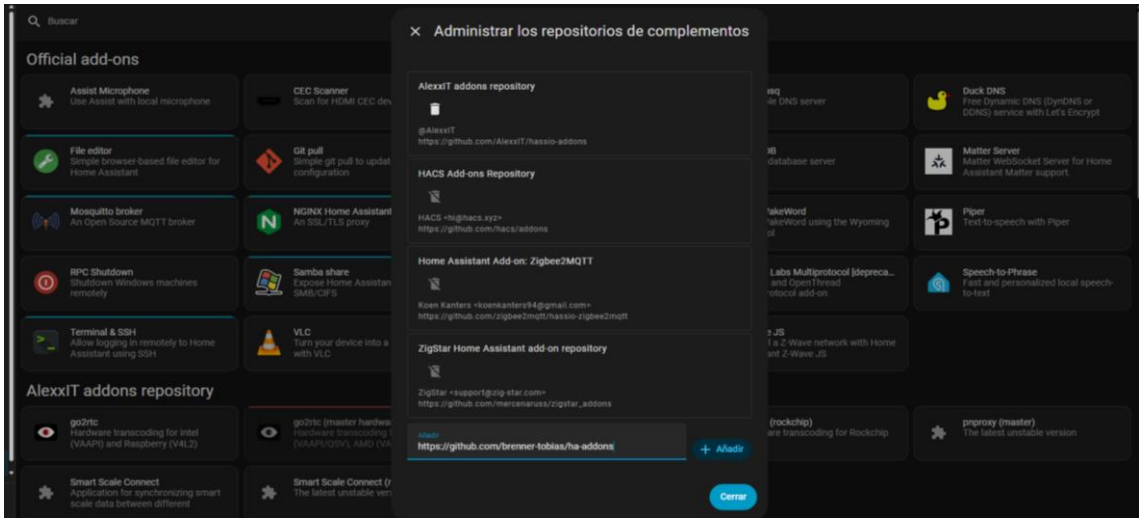
Asignación de un subdominio y el dominio principal para conectar con el servidor local



Nos dirigimos a nuestra central domótica y buscamos el complemento de Cloudflare, como se ve en la figura 111. Después lo agregamos, como muestra la figura 112. Una vez realizado esto, la figura 113 muestra que se genera un token, el cual debemos copiar y pegar en el complemento de Cloudflare en Home Assistant, tal como indica la figura 114.

Figura 111

Adición del repositorio oficial de Cloudflare



Nota. Para tener acceso al complemento oficial de Cloudflare en Home Assistant es necesario colocar el siguiente repositorio: https://github.com/brenner-tobias/ha-addons

Figura 112

Repositorio de Cloudflare agregado

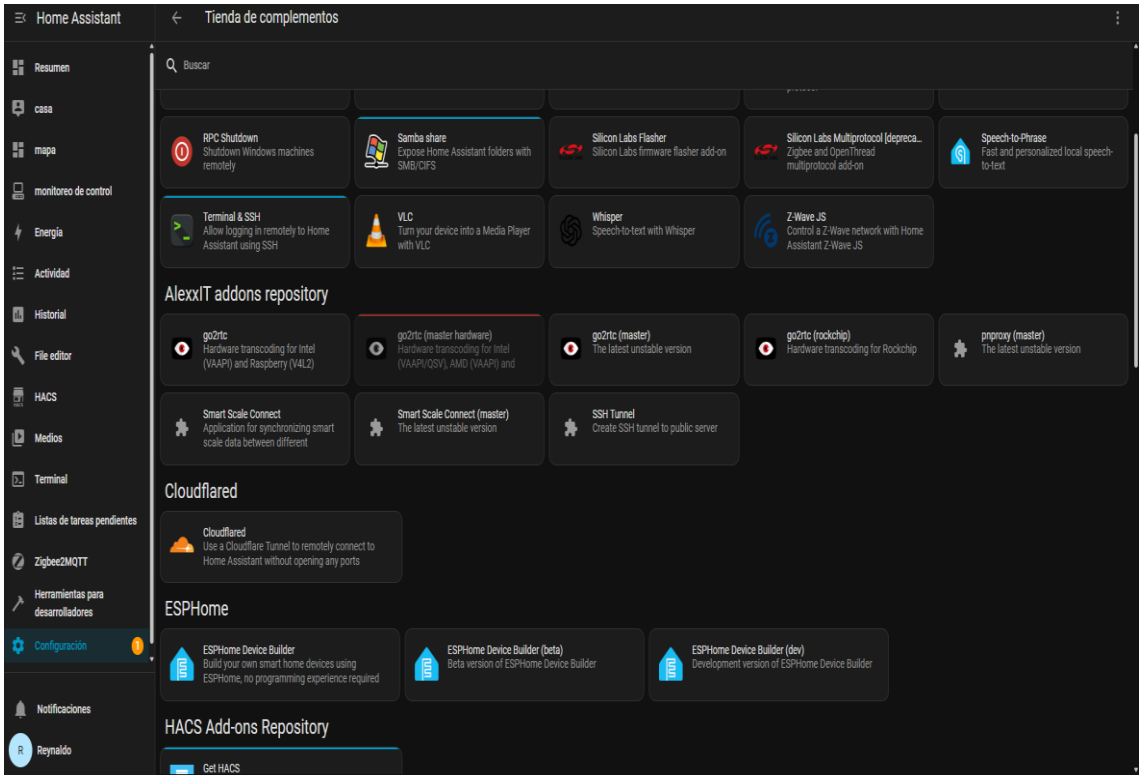
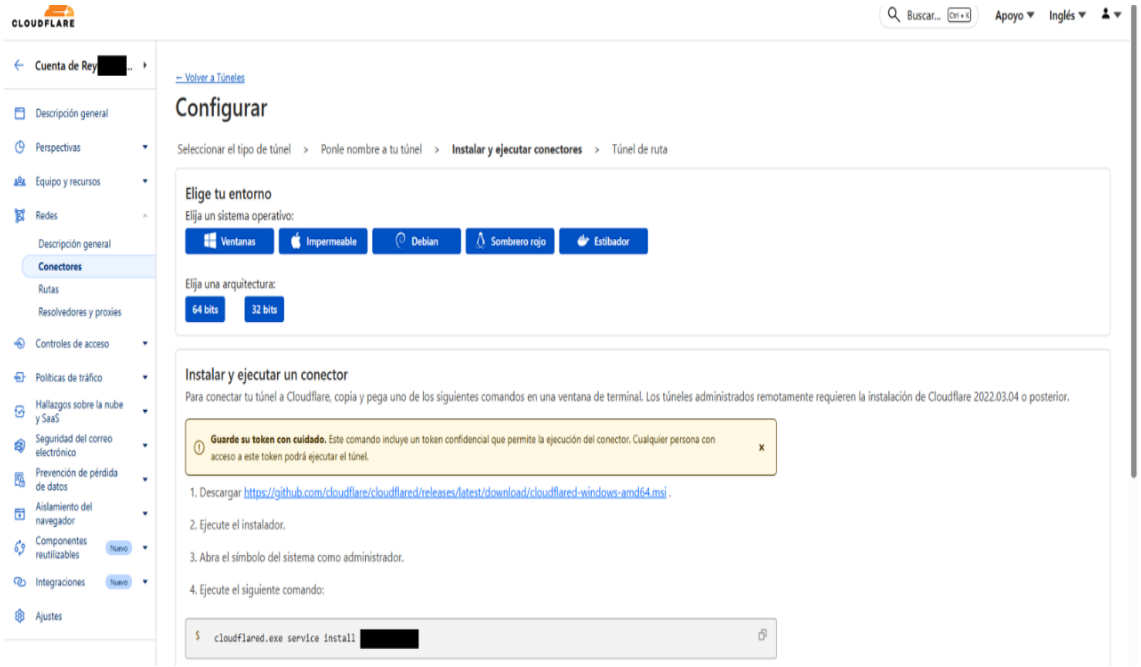


Figura 113

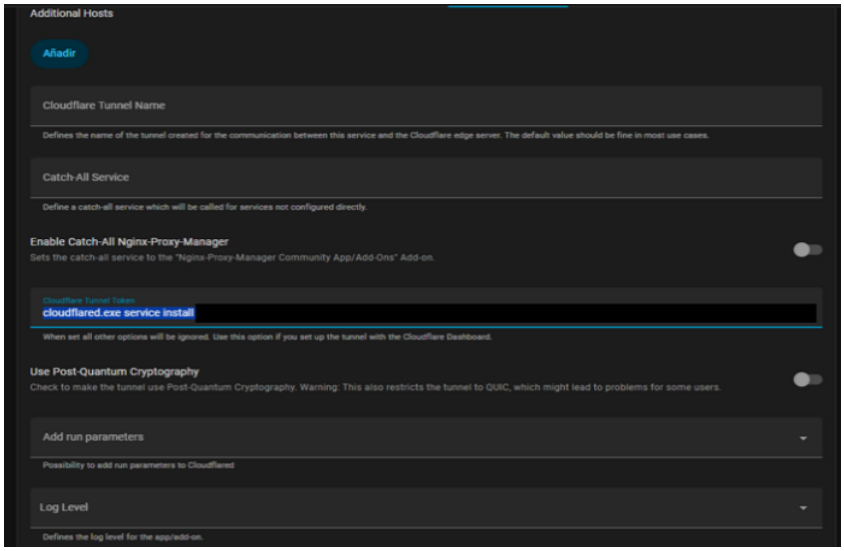
Token generado para la vinculación



Nota. Este token nos servirá como una “contraseña” para poder conectar con nuestro túnel.

Figura 114

Código de Cloudflare para establecer el Token del túnel



Nota. Al copiar el código que proporciona CloudFlare para el token, este puede ejecutar la instalación del servicio si no existe para la comunicación; sin embargo, en nuestro caso solo es necesario añadir el token, pues la comunicación se gestiona mediante el complemento.

Nos aseguramos de no tener errores en los registros del complemento de Cloudflare (figura 115). La figura 116 brinda información sobre el panel de túneles y conectores que hemos creado, con su estado de activación; en la figura siguiente se aprecia información obtenida de Cloudflare acerca del túnel de conexión con el servidor Home Assistant.

Figura 115

Registro del complemento

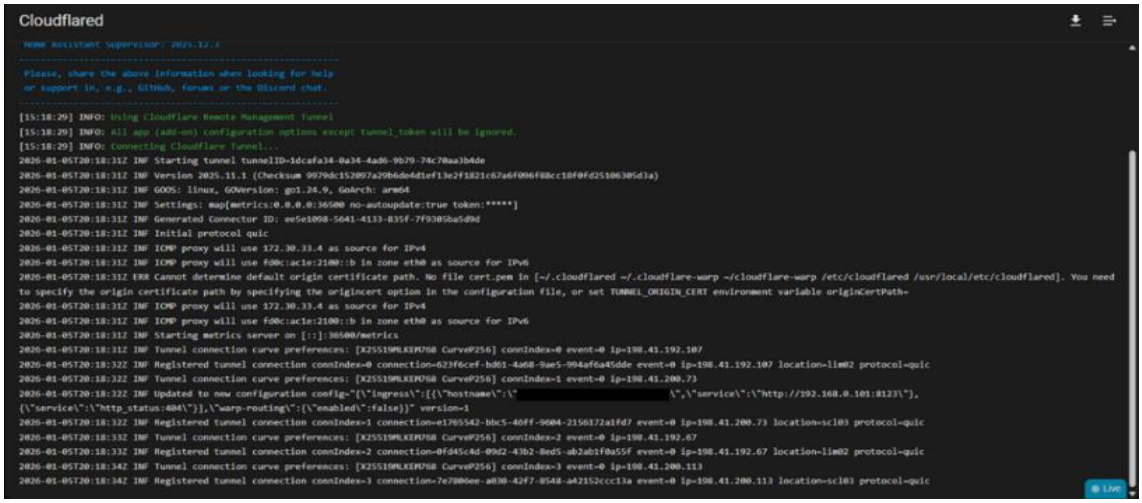
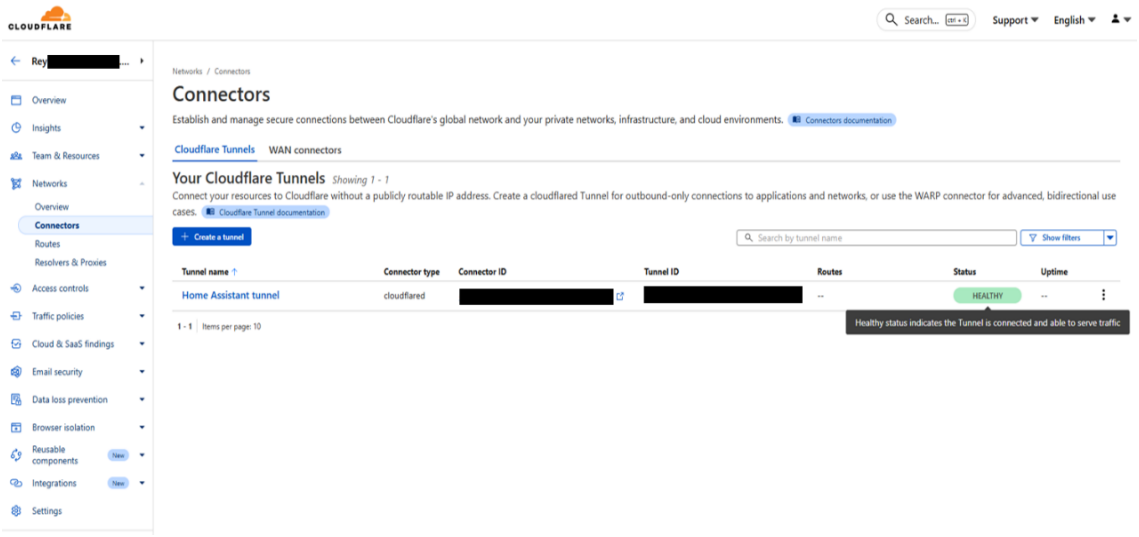


Figura 116

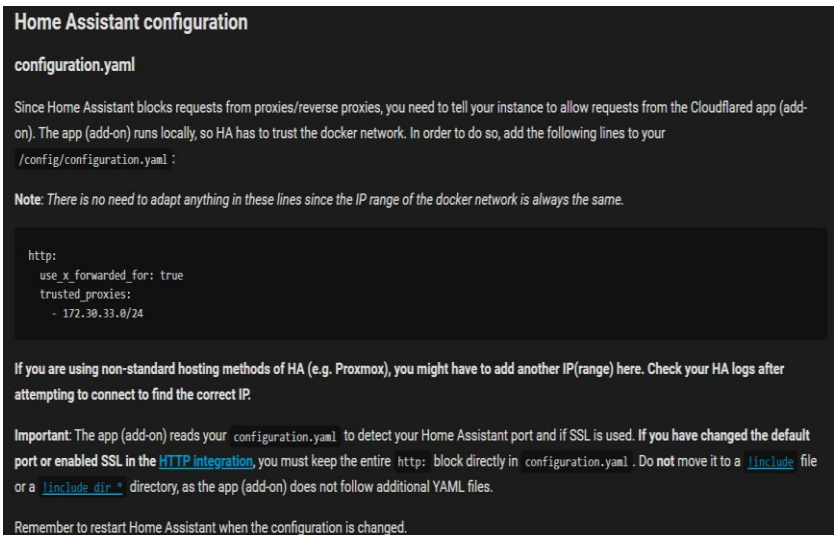
Panel de conectores



Para finalizar, debemos añadir el código que se encuentra en la documentación de Cloudflare al archivo configuration.yaml y reiniciar el servidor local. Con esto se permitirá la conexión de proxies, como se muestra en las figuras 117 y 118.

Figura 117

Configuración para Home Assistant



Nota. Este código permitirá las conexiones a través del túnel, el código sugerido se encuentra en la documentación oficial.

Figura 118

Adición del anterior código en configuration.yaml

/homeassistant/configuration.yaml

```yaml
# Loads default set of integrations. Do not remove.
default_config:

http:
  use_x_forwarded_for: true
  trusted_proxies:
    - 172.30.33.0/24
  ip_ban_enabled: true
  login_attempts_threshold: 5

# Load frontend themes from the themes folder
frontend:
  themes: !include_dir_merge_named themes

automation: !include automations.yaml
script: !include scripts.yaml
scene: !include scenes.yaml
```

Ahora corresponde comprobar si tenemos acceso a nuestro servidor local, independientemente de la conectividad en la red local. Tal como se muestra en las figuras 119 y 120, contamos con acceso directo fuera de la red local y con certificado de seguridad, siempre que el acceso a Internet sea seguro.

Figura 119

Acceso remoto a Home Assistant

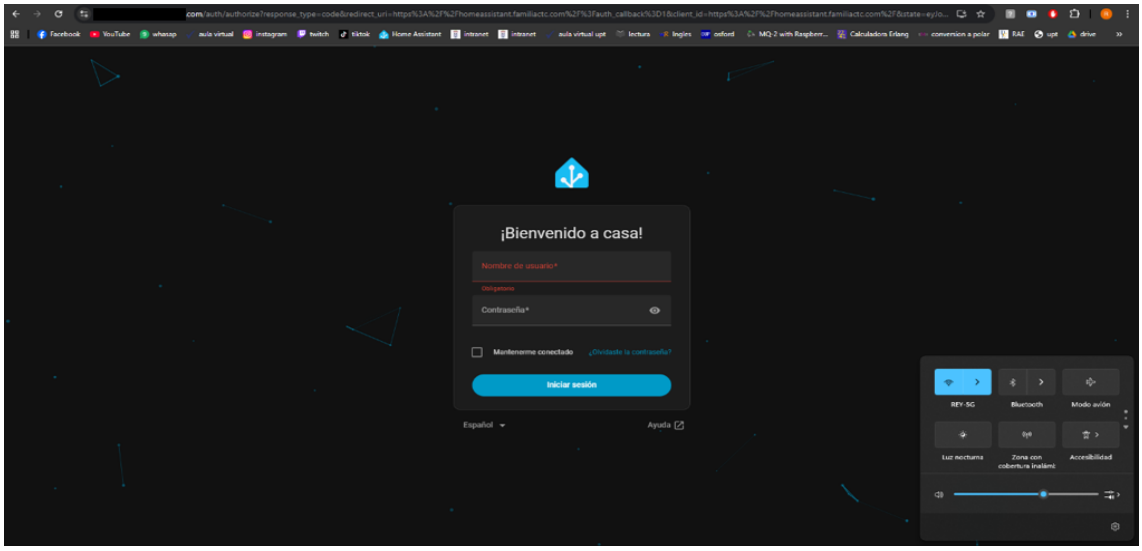
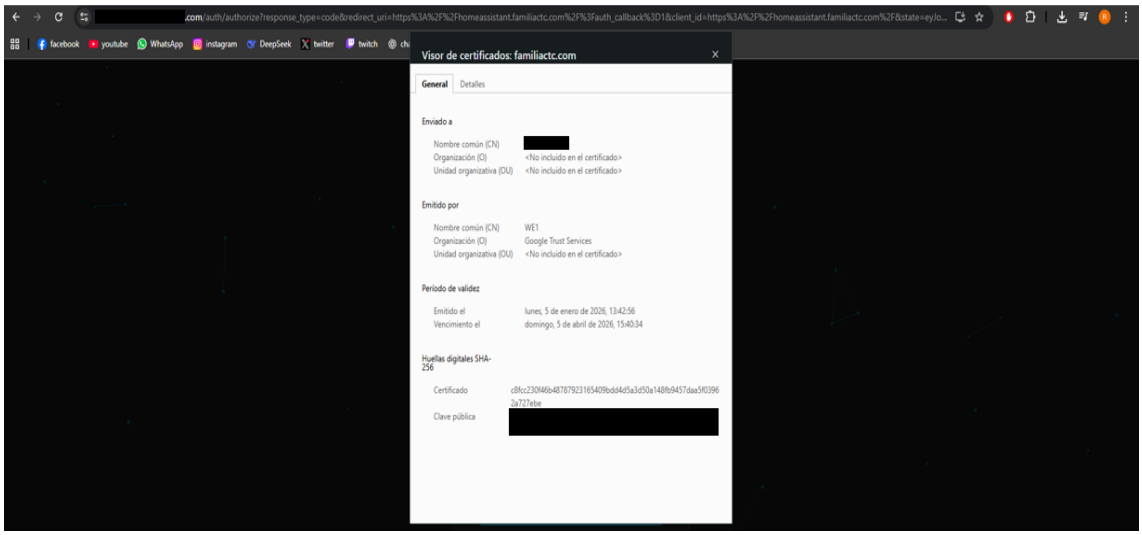


Figura 120

Certificado de encriptación



3.5.9. Control de intentos de ingreso por IP

3.5.9.1. Ip Ban

Según Home Assistant (2026), se debe configurar en el archivo configuration.yaml y definir cuántos intentos fallidos permitidos ocurren antes de banear una dirección IP usando login_attempts_threshold. Su principal función es bloquear direcciones IP que muestran comportamientos de inicio de sesión sospechosos o incorrectos, protegiendo la privacidad de la casa inteligente. Como dato adicional, si se bloquea un usuario, se puede eliminar el baneo borrando el archivo ip_bans.yaml o reiniciando el sistema mediante SSH. Retomando lo visto en la figura 118, ya se había configurado el bloqueo de direcciones IP que intentaran ingresar más de cinco veces sin lograrlo, como se ilustra con mayor énfasis en la figura 121.

Figura 121

Incorporación de ip ban e intentos limitados

```
5  http:
6    use_x_forwarded_for: true
7    trusted_proxies:
8      - 172.30.33.0/24
9    ip_ban_enabled: true
10   login_attempts_threshold: 5
```

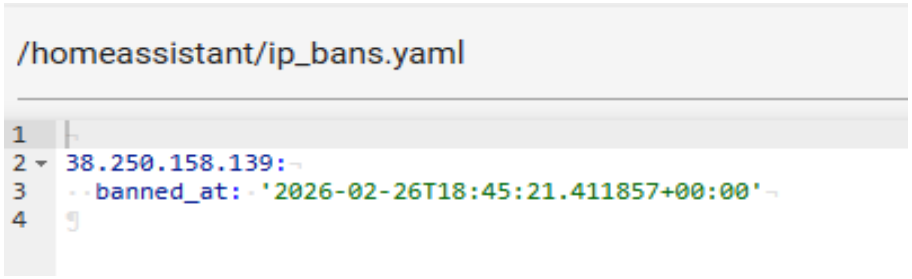
Realizando una prueba con un teléfono ajeno, que no conoce a los usuarios integrados en el sistema domótico y mucho menos sus contraseñas, y simulando un intento de acceso sin permiso, se obtuvieron los resultados expuestos en las figuras 122 y 123. La tentativa de acceso no autorizado provocó el bloqueo de la IP insistente, registrando qué dirección se bloqueó y cuándo.

Figura 122

Intento fallido de acceso

Figura 123

Registro de dirección IP baneada



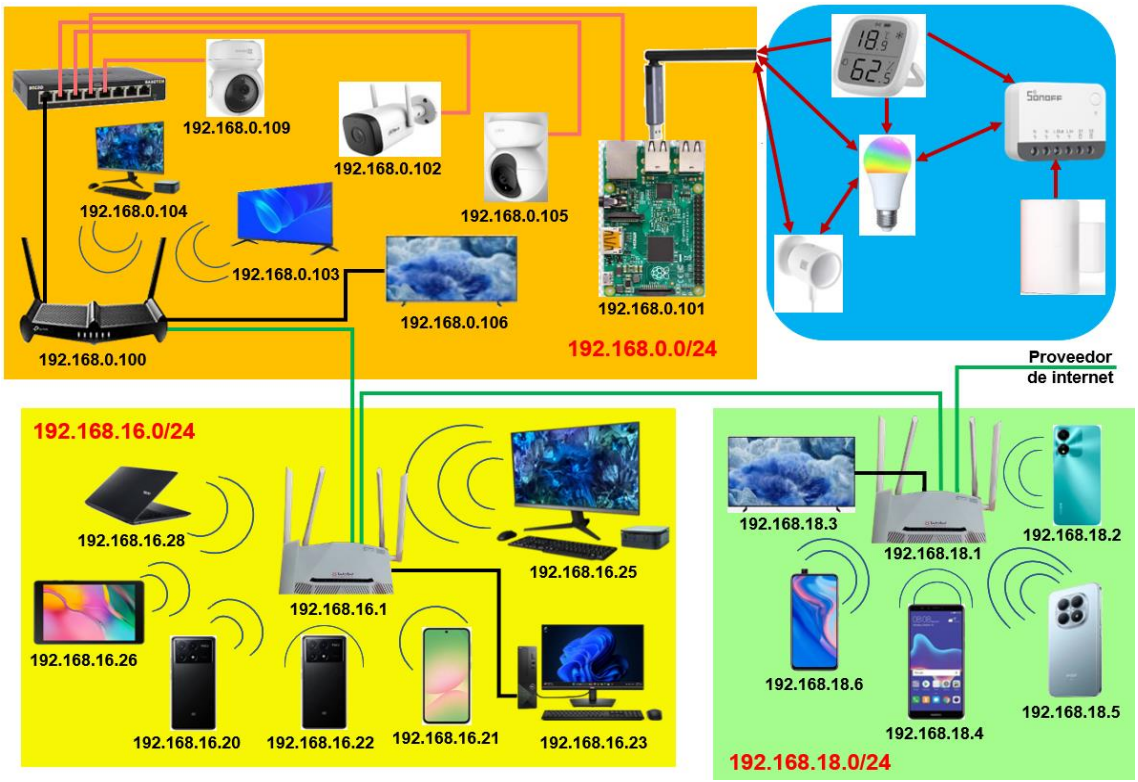
CAPÍTULO IV: RESULTADOS

4.1. Arquitectura final del diseño de la red domestica

Como primer resultado a destacar, se presenta el diseño esquemático final de la vivienda adaptada con la nueva red domótica, ilustrado en la figura 124. En el esquema se aprecian tres subredes diferenciadas por color y sus dispositivos asociados. La primera subred tiene el rango de direcciones 192.168.18.0/24 y representa las conexiones de la primera planta. La segunda subred, con rango 192.168.16.0/24, agrupa los dispositivos utilizados por los usuarios del segundo piso. Por último, la subred con rango 192.168.0.0/24 está dedicada exclusivamente a la red domótica y a su seguridad. El área sombreada en azul claro representa la red Zigbee y sus dispositivos interconectados mediante una topología en malla.

Figura 124

Esquema del diseño final

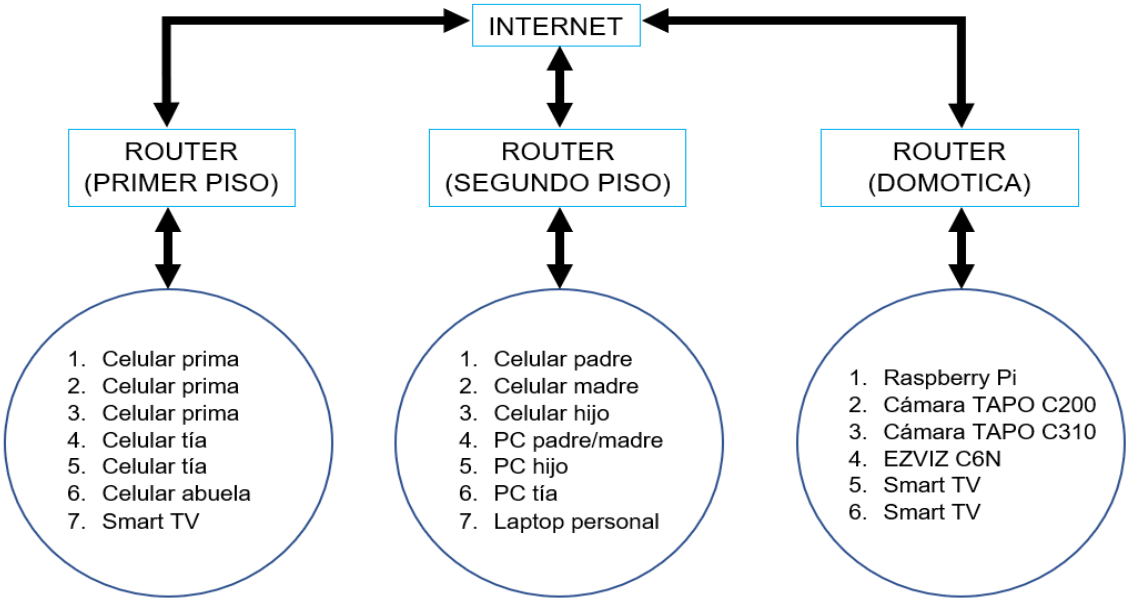


En la figura 125 se aprecia el diagrama de bloques que muestra la conexión a Internet en la parte superior y cómo esta se distribuye hacia tres routers independientes:

uno para el primer piso, otro para el segundo piso y un tercero dedicado a la domótica. El diagrama indica el flujo de conectividad hacia cada segmento de la casa. El router del primer piso distribuye Internet principalmente a dispositivos móviles de los familiares y a una Smart TV. El router del segundo piso conecta dispositivos personales y de trabajo, concentrando equipos informáticos y aislando la comunicación entre pisos. El router de domótica agrupa únicamente dispositivos IoT y de vigilancia —una Raspberry Pi, varias cámaras y dos Smart TV— creando un segmento separado para automatización y monitoreo. Esta separación mejora la privacidad frente a publicidad y telemetría. En conjunto, el diagrama comunica una arquitectura doméstica segmentada física y funcionalmente: separación de tráfico entre áreas habitacionales y un segmento exclusivo para domótica, lo que facilita el control, la organización y el posible aislamiento de los dispositivos IoT respecto a los equipos personales.

Figura 125

Diagrama de red doméstica con routers por piso y segmento domótico



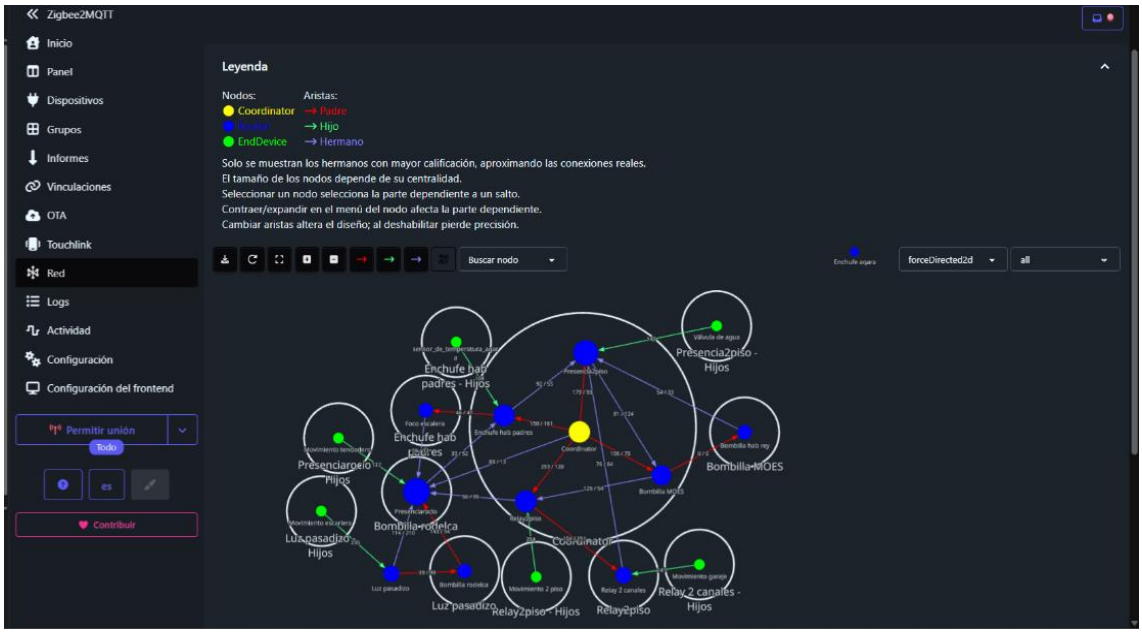
4.2. Mapeo de la red Zigbee

En la figura 126 se muestra el mapeo de dispositivos obtenido mediante un escaneo de red y un algoritmo de visualización, lo que facilita la comprensión de las conexiones y la distribución de actuadores y sensores. Esta vista complementa lo observado en la figura 80. En las figuras solo se representan los nodos mejor valorados (los de mayor centralidad), de modo que la visualización aproxima las conexiones reales. El tamaño

de cada nodo depende de su centralidad; al contraer o expandir un nodo desde el menú se modifica la vista de sus dependencias. Cambiar las aristas altera el diseño del grafo y, si se deshabilitan elementos, la precisión del mapeo disminuye.

Figura 126

Mapa de red Zigbee (forceDirected2d)



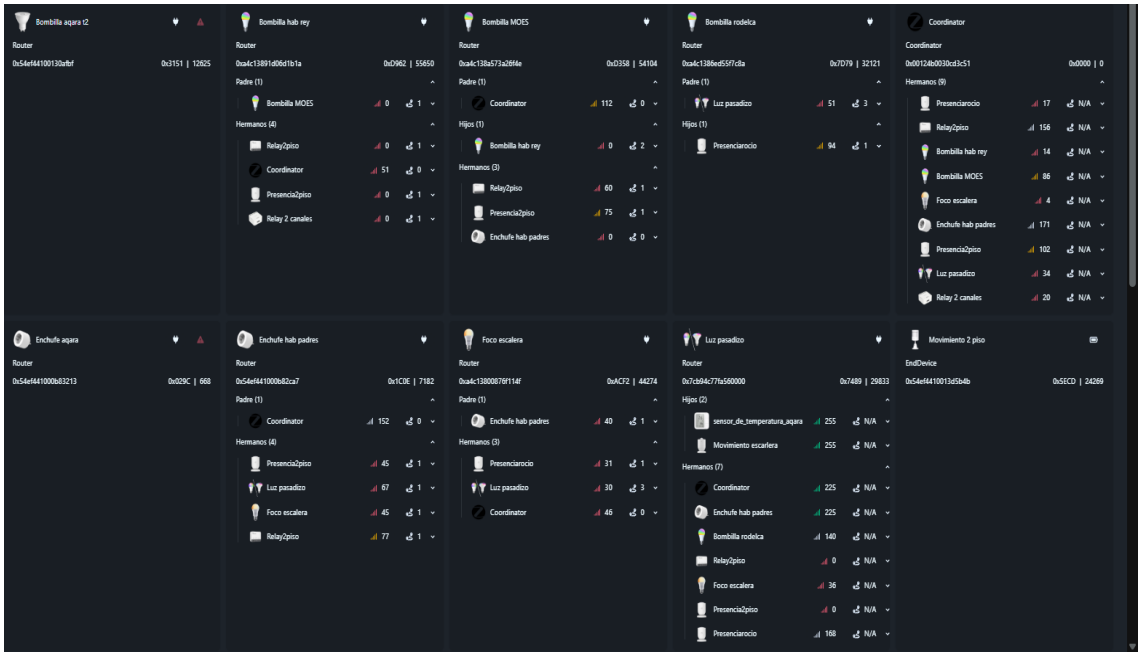
Nota. Este algoritmo de visualización distribuye los nodos (coordinador, routers y dispositivos finales) según fuerzas simuladas de atracción y repulsión, permite ver de manera clara cómo están conectados los dispositivos y cuáles son los enlaces más fuertes o débiles dentro de la malla Zigbee.

4.3. Dispositivos conectados a la red Zigbee

Un router Zigbee es un dispositivo alimentado por la red eléctrica que puede repetir la señal; en teoría puede conectar directamente entre 20 y 32 dispositivos finales (basicjuntti666, 2025). Cada router aumenta la capacidad y la estabilidad de la red, permitiendo que los coordinadores gestionen docenas o incluso cientos de dispositivos en conjunto. Para el desarrollo de este sistema se emplearon repetidores alimentados por la red en puntos estratégicos con el fin de reducir saltos y mejorar la latencia. En las figuras 127 y 128 se aprecian las conexiones entre los dispositivos. Se implementaron routers y dispositivos finales en escenarios reales, teniendo siempre presente la retransmisión de tramas y la mejora de la cobertura de la red.

Figura 127

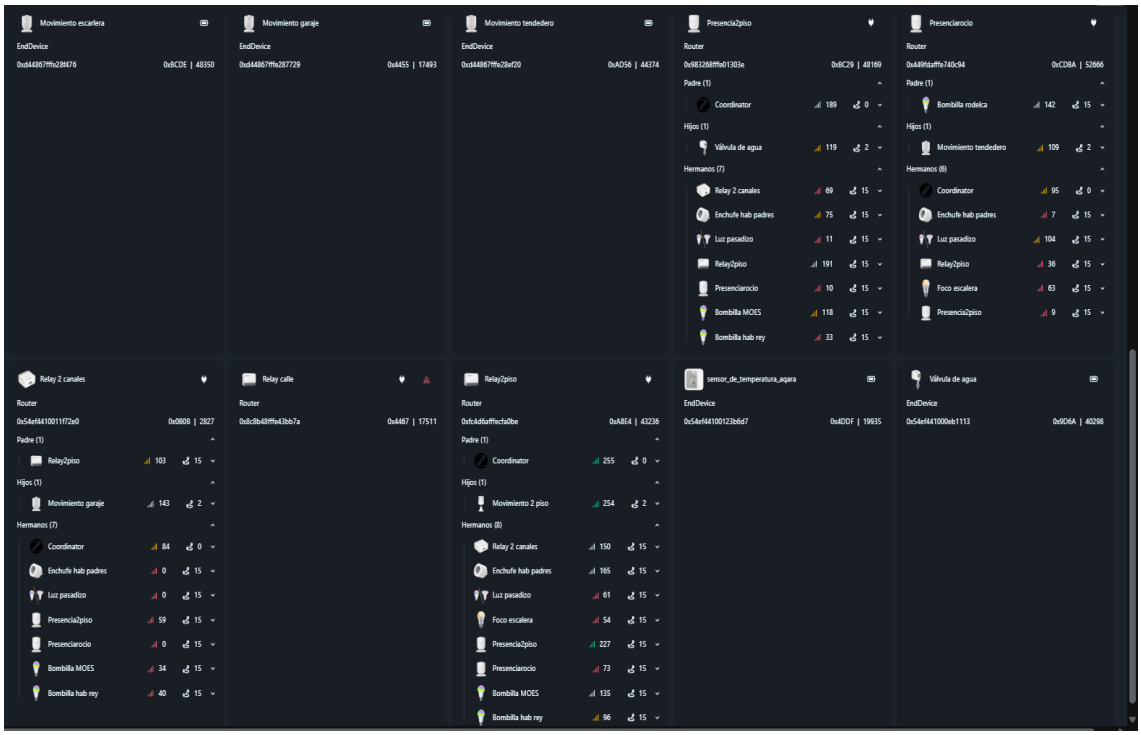
Visualización de datos y enlaces de cada dispositivo en Zigbee2MQTT primera parte



Nota. Algunos de los dispositivos enlazados a la red Zigbee presentan errores de comunicación (Bombilla aqara t2, Enchufe Aqara y posteriormente en la figura 184 relay calle) esto debido a su desconexión.

Figura 128

Visualización de datos y enlaces de cada dispositivo en Zigbee2MQTT segunda parte



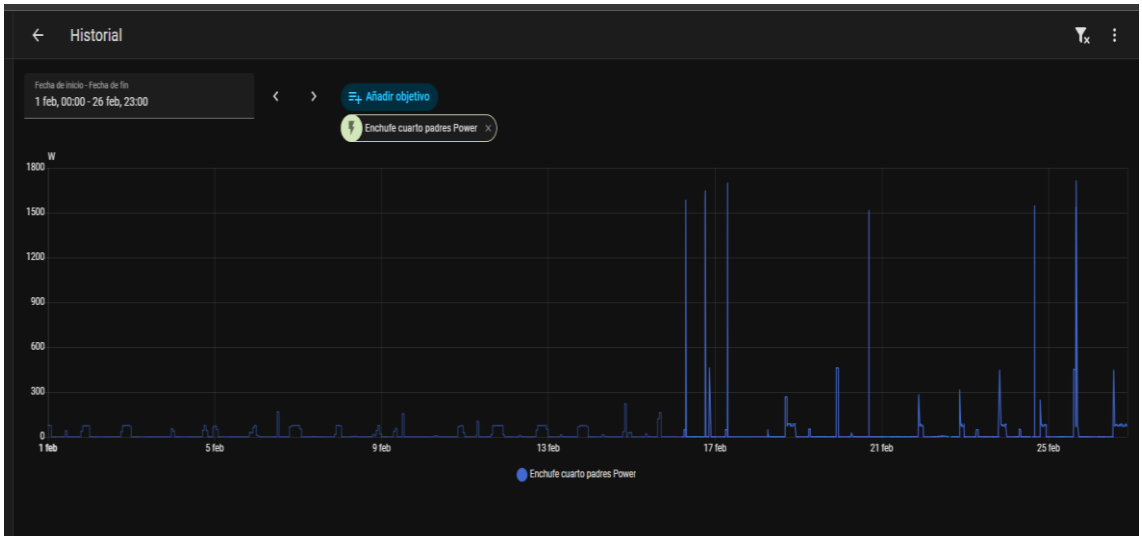
4.4. Consumo de cada dispositivo

4.4.1. Smart Plug Aqara (Modelo SP-EUC01)

Según la ficha técnica, el dispositivo soporta hasta 10 A con alimentación de 250 V AC a 50/60 Hz, equivalente a 2500 W. El fabricante, Aqara, recomienda aplicar un margen del 8 %, estableciendo 2300 W como nuevo máximo operativo para el enchufe inteligente. Su consumo en reposo es mínimo, inferior a 0,5 W (Aqara, 2026). Ubicado en la habitación de los padres, una regleta está conectada de forma permanente y alimenta un televisor Sony Trinitron KV-21FV300 que consume entre 70 y 100 W en funcionamiento. Como muestra la figura 129, se registran detalladamente todos los consumos, cargas y potencias durante los periodos de activación.

Figura 129

Registro de potencia utilizada en el mes de febrero

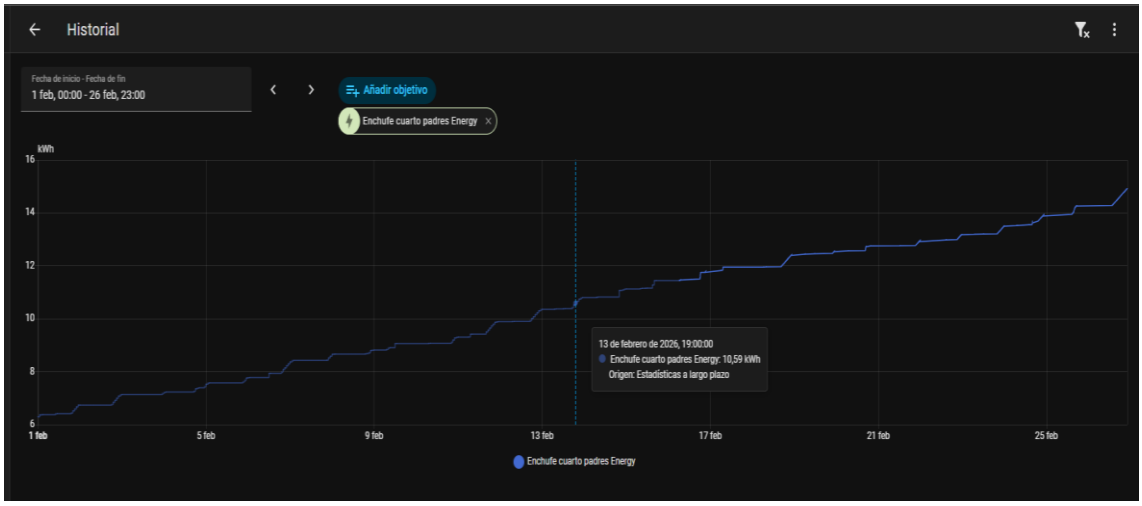


Nota. El uso promedio es de 76 a 89 W en cuanto al uso del televisor, mientras que los picos sobresalientes son por diversos aparatos adicionales temporales como cargadores de celulares, planchas eléctricas, entre otros.

Además, es común conectar a la regleta un cargador de 75 W entre las 6:00 y las 7:00 a.m. y una plancha eléctrica que consume entre 1600 W y 1650 W, con un uso promedio de dos horas por día en rotación. Por ejemplo, la plancha se usa los lunes, martes, jueves y viernes, mientras que los miércoles, sábados y domingos no está en uso. Se registró un pico máximo de 1713 W en febrero, como se refleja en la figura 130.

Figura 130

Registro de consumo en el mes de febrero



Nota. Consumo máximo registrado a día 28 de febrero es de 14.92 kWh, mientras que el consumo inicial del mismo mes es de 6.30 kWh, siendo el promedio de energía consumida de 10.61 kWh.

Para dispositivos sin medidor de consumo, se realizó un registro manual: se anotaron sistemáticamente los momentos de encendido y apagado, las situaciones y los periodos para contrastar tiempos y consumos por ambiente. Se monitorizó personalmente durante una semana mediante observaciones directas y herramientas auxiliares, como temporizadores y aplicaciones de registro, estableciendo periodos de observación diurnos y nocturnos para comparar variaciones según la franja horaria.

Cada cambio de estado del dispositivo se anotó inmediatamente para minimizar errores de memoria. Durante la semana de pruebas se alternaron días normales e intensos para simular picos de demanda e identificar patrones entre días laborables y fines de semana. Las anotaciones por ambiente permitieron comparar comportamientos con las nuevas integraciones y evaluar mejoras o pérdidas; la tabla 6 resume periodos de encendido y tiempos promedios de activación. La tabla 7 ofrece registros por hora y de duración más precisos, pero el sistema almacena datos solo 10 días, por lo que es necesario exportar o consolidar la información periódicamente para permitir análisis a largo plazo. Esta limitación se adoptó para optimizar la memoria interna y reducir la carga de procesamiento en los dispositivos de registro. Como consecuencia, el análisis a largo plazo requiere exportaciones periódicas o la implementación de un sistema de almacenamiento externo si se considera necesario.

Tabla 6

Hora y tiempo activación de cada área iluminada (sin inclusión de domótica)

Garaje)		Entrada 2 piso		Cocina		Habitación Rocio		Habitación Reynaldo		Escalera	
Hora de detección	Tiempo de encendido	Hora de detección	Tiempo de encendido	Hora de detección	Tiempo de encendido	Hora de detección	Tiempo de encendido	Hora de detección	Tiempo de encendido	Hora de detección	Tiempo de encendido
18:30:00	1800	18:30:00	1800	17:04:00	600	17:05:00	1800	17:00:00	3600	17:04:00	3900
19:00:00	3600	19:00:00	3600	17:16:00	900	18:12:00	540	18:00:00	3600	18:10:00	4200
20:00:00	1800	20:00:00	1800	17:33:00	600	19:03:00	300	19:00:00	3600	19:20:00	2700
				17:57:00	1200	19:22:00	900	20:00:00	3600		
				19:06:00	2400	20:16:00	960	21:00:00	3600		
				20:01:00	1620	21:00:00	3600	22:00:00	3600		
				21:13:00	420	22:00:00	3600	23:00:00	3600		
				21:35:00	960	23:00:00	3600				
				22:00:00	300	00:00:00	2700				
Promedio (seg)	7200	Promedio (seg)	7200	Promedio (seg)	9000	Promedio (seg)	18000	Promedio (seg)	25200	Promedio (seg)	10800
Promedio (hrs)	2	Promedio (hrs)	2	Promedio (hrs)	2,5	Promedio (hrs)	5	Promedio (hrs)	7	Promedio (hrs)	3

Nota. Los tiempos de encendido y los periodos de activación fueron obtenidos manualmente, de acuerdo con días laborales y fines de semana, teniendo en cuenta el uso promedio semanal destinado a cada área, según la tabla.

Tabla 7

Registro de hora y tiempo de encendido de cada dispositivo (inclusión de domótica)

Relay de 2 canales (Garaje)		Relay sonoff (Entrada 2 piso)		Bombilla MOES (Cocina)		Bombilla MOES (habitación Rocio)		Bombilla MOES (habitación Rey)		Bombilla INNR y ThirdReality (Escalera)	
Hora de detección	**Tiempo de encendido**	**Hora de detección**	**Tiempo de encendido**	**Hora de detección**	**Tiempo de encendido**	**Hora de detección**	**Tiempo de encendido**	**Hora de detección**	**Tiempo de encendido**	**Hora de detección**	**Tiempo de encendido**
18:00:15	34,47	19:31:36	10,00	18:08:27	267,60	18:14:46	25,04	16:00:00	3600	18:35:23	37,16
18:00:55	45,12	19:32:04	10,00	18:15:37	13,29	18:26:31	28,01	17:00:00	3600	18:50:54	36,10
18:02:20	25,05	19:52:55	10,00	18:16:19	426,00	18:51:47	244,80	18:00:00	3600	18:51:46	62,00
18:03:09	35,61	19:53:40	10,00	18:24:35	181,80	19:14:47	123,60	19:00:00	3600	19:01:44	31,35
18:12:16	18,48	20:24:47	9,99	18:33:20	64,80	19:19:11	193,80	20:00:00	3600	19:03:36	34,19
18:53:22	19,99	20:29:11	9,99	18:36:06	69,60	21:02:41	137,40	21:00:00	3600	19:28:36	34,78
19:29:33	38,70	22:18:12	9,99	18:38:18	60,60	21:09:24	26,87	22:00:00	3600	19:30:36	32,67
19:32:35	56,12	22:19:06	9,99	18:40:52	16,74	21:11:15	34,83	23:00:00	3600	19:31:10	23,58
19:33:35	25,35			18:42:36	46,86	21:57:34	84,6			19.39:24	37,81
19:36:25	18,57			18:44:14	46,14	22.29.07	3435,00			19:41:58	35,77
19:38:22	27,18			18:46:54	14,62					20:00:12	36,48
19:40:49	18,54			18:47:12	25,19					20:02:20	30,68
19:41:28	20,32			18:54:24	22,39					20:08:10	36,02
19:43:58	71,11			18:57:57	30,64					20:29:32	45,18
19:45:29	18,62			19:01:57	28,64					20:34:50	32,24
19:47:24	18,50			19:04:57	52,81					20:35:28	24,84
19:57:50	18,50			19:23:39	36,34					20:55:58	39,18
19:58:15	35,67			19:24:16	257,40					21:01:17	47,20
20:17:42	40,41			19:30:01	623,40					21:35:31	33,64
20:18:30	36,30			21:08:10	14,77					21:58:43	36,85
20:19:51	31,71			21:10:16	34,63					21:59:57	40,67

(continúa)

Tabla 7 (continuación)

Hora de detección	Tiempo de detección			Hora de detección	Tiempo de detección					Hora de detección	Tiempo de detección
20:23:07	20,32			21:53:41	23,14					22:15:57	50,80
20:24:19	36,83			22:58:51	30,16					22:21:04	32,02
20:25:21	40,71			22:59:29	48,88					23:17:17	34,69
21:09:45	28,85			23:26:09	37,01					23:25:53	58,79
21:11:25	18,56			23:28:34	20,84					23:44:18	39,51
21:12:48	20,32			23:40:22	15,93					00:58:26	33,06
21:13:18	18,51			23:42:39	22,67					01:07:14	39,29
21:42:03	42,74										
21:43:09	27,19										
21:44:10	82,10										
21:46:09	20,53										
21:49:01	18,47										
23:26:41	20,59										
23:50:26	21,45										
23:52:30	28,15										
00:18:57	22,64										
00:22:26	24,06										
00:55:37	71,40										
00:56:56	52,27										
00:57:54	39,00										
Promedio (seg)	1309,01	Promedio (seg)	79,96	Promedio (seg)	1909,49	Promedio (seg)	4333,95	Promedio (seg)	25200	Promedio (seg)	1056,55
Promedio (hrs)	0,3636	Promedio (hrs)	0,0222	Promedio (hrs)	0,5304	Promedio (hrs)	1,2038	Promedio (hrs)	7	Promedio (hrs)	0,2935

Nota. Los tiempos de encendido y los periodos de activación fueron obtenidos del registro de cada dispositivo, correspondientes a cada área que figura en la tabla.

4.4.2. Relé 2 canales Aqara (Modelo LLKZMK12LM)

El interruptor inteligente permite controlar de forma independiente dos cargas en modo de contacto seco o húmedo y consume entre 0,5 W y 1 W en espera. Según el manual (Aqara, 2023), controla los focos mediante un sensor de movimiento alimentado por batería, por lo que no incrementa el consumo de la vivienda. Las bombillas instaladas consumen 40 W cada una; dos están en el exterior y otras dos en el interior del garaje, lo que mejora la automatización. Con base en la tabla 7, se añadió el consumo activo de los focos según su tiempo de encendido, generando la Ecuación 8. Para obtener el consumo total, se suma la energía activa de los focos y la energía en reposo del dispositivo. La energía en reposo se calcula como la diferencia entre 24 horas y el tiempo de uso del relé, multiplicada por su consumo en stand-by, como muestra la Ecuación 9. De este modo se obtiene el consumo total aproximado diario reflejado en la Ecuación 10.

$$(40\ W + 40\ W) * 0{,}3636\ h \rightarrow 80\ W * 0{,}3636\ h\ = 29{,}0764\ \frac{W}{h} \tag{8}$$

$$(24\ h - 0{,}3636\ h) * 1\ W = 23{,}6364\ \frac{W}{h} \tag{9}$$

$$29{,}0764\ \frac{W}{h} + 23{,}6364\ \frac{W}{h} = 52{,}7128\ \frac{W}{h}\ (por\ día) \tag{10}$$

En comparación con el uso sin el dispositivo inteligente, la tabla 6 muestra el tiempo promedio de uso. La Ecuación 11 calcula el consumo diario. Considerando un uso alternado con un promedio de tres días por semana, la Ecuación 12 determina el consumo semanal. Finalmente, la Ecuación 13 aplica el periodo de tiempo para el caso del dispositivo inteligente durante siete días:

$$(40\ W + 40\ W) * 2 \rightarrow 80\ W * 2\ h = 160\ \frac{W}{h}\ (por\ día) \tag{11}$$

$$160\ \frac{W}{h} * 3 = 480\ \frac{W}{h}\ (en\ una\ semana) \tag{12}$$

$$52{,}7128\ \frac{W}{h} * 7 = 368{,}9896\ \frac{W}{h}\ (en\ una\ semana) \tag{13}$$

Mostrando una relación beneficiosa en cuanto al consumo eléctrico usando dispositivos inteligentes de manera cotidiana y el uso de un dispositivo no inteligente con un uso alternado. Obteniendo una mejoría del 23,13 % en la reducción eléctrica.

4.4.3. Relay SONOFF (Modelo ZBMINIR2)

En comparación con el relé anterior, este es más compacto y mantiene la misma capacidad de corriente; su voltaje máximo se reduce a 240 V, disminuyendo la carga máxima en un 4 % y consumiendo 0,5–1 W en espera (Sonoff, 2024). Antes se utilizaba un foco de 40 W, por lo que el consumo se mantiene. Es necesario conocer el promedio de activación; la tabla 7 muestra un uso bajo. La Ecuación 14 calcula el consumo promedio con el relé inteligente; la Ecuación 15 utiliza la diferencia de tiempo para calcular el consumo total; y la Ecuación 16 determina el consumo diario.

$$40\ W * 0{,}0222\ h = 0{,}888\ \frac{W}{h} \tag{14}$$

$$(24\ h - 0{,}0222\ h) * 1\ W = 23{,}9778\ \frac{W}{h} \tag{15}$$

$$0{,}888\ \frac{W}{h} + 23{,}9778\ \frac{W}{h} = 24{,}8658\ \frac{W}{h}\ (por\ día) \tag{16}$$

Tomando en cuenta que su uso era continuo, con una duración de dos horas según la tabla 6, las Ecuaciones 17 y 18 muestran el consumo anterior, que en una semana sería equivalente a un promedio de tres días; estas se complementan con la Ecuación 19, que muestra el uso del relé inteligente en una semana:

$$40\ W * 2\ h = 80\ \frac{W}{h} \tag{17}$$

$$80\ \frac{W}{h} * 3 = 240\ \frac{W}{h}\ (en\ una\ semana) \tag{18}$$

$$24{,}8658\ \frac{W}{h} * 7 = 174{,}0606\ \frac{W}{h}\ (en\ una\ semana) \tag{19}$$

Con respecto al consumo con un dispositivo inteligente usado diariamente y un dispositivo no inteligente con un uso alternado se muestra una reducción similar al

anterior caso, pero esta vez la reducción es del 27,47 % en comparación a la situación anterior y la actual.

4.4.4. Bombilla MOES (Modelo ZB-TDA9-RCW-E27-MS) (cocina)

Según la página web oficial de MOES (2026), existen dos versiones de esta bombilla; la versión analizada es de 9 W y consume una cantidad ínfima en modo de reposo, típicamente inferior a 0,5 W. Como dato adicional, el foco utilizado anteriormente tenía un consumo de 18 W. En ambientes como este, las bombillas suelen combinarse con sensores de presencia. En este caso, el sensor SNZB-06P funciona con una tecnología radar de microondas para detectar la presencia humana, incluidas personas estáticas y movimientos sutiles incluso cuando la persona está quieta. Su alimentación es mediante USB y su consumo de corriente estimado en funcionamiento activo se sitúa en torno a 100–200 mA, aunque no se detalla un valor específico de reposo en las especificaciones generales (SONOFF, 2023).

El consumo de la bombilla se expresa en la Ecuación 20. En contraste, la Ecuación 21 representa el consumo en reposo, con un valor de 0,55 W. La Ecuación 22 calcula el consumo del sensor de presencia considerando su operación continua las 24 horas; aunque su consumo varía, se toma el valor máximo de 0,5 W según la ficha técnica. Finalmente, la Ecuación 23 agrupa todos los valores de consumo para obtener el consumo total diario, lo que permite comparar aportes individuales y estimar la demanda energética del sistema en un día.

$$9\ W * 0{,}5304\ h = 4{,}7736\ \frac{W}{h} \tag{20}$$

$$(24\ h - 0{,}5304\ h) * 0{,}5\ W = 11{,}7348\ \frac{W}{h} \tag{21}$$

$$0.5\ W * 24\ h = 12\ \frac{W}{h} \tag{22}$$

$$4{,}7736\ \frac{W}{h} + 11{,}7348\ \frac{W}{h} + 12\ \frac{W}{h} = 28{,}5084\ \frac{W}{h}\ (por\ día) \tag{23}$$

Para el desarrollo de la Ecuación 24 se tendrá en cuenta el uso promedio detallado en la tabla 6. Con esos datos se calcula el consumo diario. A partir de esos valores se genera la siguiente ecuación, que permite determinar la diferencia porcentual entre consumos:

$$18\,W * 2\,h = 36\,\frac{W}{h}\;(por\;día) \tag{24}$$

$$\frac{36 - 28{,}5084}{36} * 100 \rightarrow \frac{7{,}4916}{36} * 100 = 20{,}81\,\% \tag{25}$$

Esto significa que el consumo actual es un 20,81 % menor que el consumo anterior; lo que se traduce en menor gasto energético y menor costo proporcional para este caso.

4.4.5. Bombilla MOES (Modelo ZB-TDA9-RCW-E27-MS) (habitación Rocio)

El mismo modelo de bombilla se aplicó a un ambiente mayor; se calculará el consumo de la bombilla y del sensor. El encendido se estima entre cuatro y cinco horas los días laborables y cinco horas los sábados y domingos. Con esos datos y la tabla 7, que expone horas y tiempos de detección, se inician los cálculos. Las Ecuaciones 26, 27 y 28 desarrollan, respectivamente, el consumo por uso de la bombilla; la suma del consumo en reposo de 0,55 W; y el cálculo del consumo del sensor, de forma análoga a la Bombilla MOES (cocina). La Ecuación 29 suma estos valores para obtener el consumo diario.

$$9\,W * 1{,}20\,h = 10{,}8\,\frac{W}{h} \tag{26}$$

$$(24\,h - 1{,}2038\,h) * 0{,}5\,W = 11{,}4\,\frac{W}{h} \tag{27}$$

$$0{,}5\,W * 24\,h = 12\,\frac{W}{h} \tag{28}$$

$$10{,}8\,\frac{W}{h} + 11{,}4\,\frac{W}{h} + 12\,\frac{W}{h} = 34{,}2\,\frac{W}{h} \tag{29}$$

Equiparando el consumo de los focos, se considerará solo uno para equilibrar la comparativa. Las Ecuaciones 30 y 31 muestran el consumo semanal tanto en días laborables como en fines de semana. La Ecuación 32 expresa el consumo diario en semanas laborales, incluyendo todos los días de lunes a viernes; el consumo diario de fines de semana incluye sábado y domingo. Sumando ambos se obtiene el consumo semanal total:

$$16\ \mathrm{W} * 4\ \mathrm{h} = 64\ \frac{W}{h}\ (por\ dia\ en\ las\ días\ laborales) \quad (30)$$

$$16\ W * 5\ h = 80\ \frac{W}{h}\ (por\ dia\ en\ los\ fines\ de\ semana) \quad (31)$$

$$\left(64\ \frac{W}{h} * 5\right) + \left(80\ \frac{W}{h} * 2\right) = 480\ \frac{W}{h}\ (en\ una\ semana) \quad (32)$$

Del mismo modo, se aplica una operación equivalente para el consumo del dispositivo inteligente encontrando en la Ecuación 33 que su consumo en una semana aproximado, con estos valores se puede averiguar la diferencia porcentual entre consumos generando la Ecuación 34:

$$34{,}2\ \frac{W}{h} * 7 = 239{,}4\ \frac{W}{h}\ (en\ una\ semana) \quad (33)$$

$$\frac{480 - 239{,}4}{480} * 100 \rightarrow \frac{240{,}6}{480} * 100 = 50{,}125\ \% \quad (34)$$

El nuevo consumo refleja un 50,125 % menor que el consumo anterior; significando una mejoría considerablemente beneficiosa, ya que el coste energético se reduce a la mitad con respecto al contexto anterior sin uso de dispositivos inteligentes.

4.4.6. Bombilla MOES (Modelo ZB-TDA9-RCW-E27-MS) (habitación Reynaldo)

Como muestran las tablas 6 y 7, el tiempo de encendido permanece igual debido al uso frecuente en ambos casos, salvo cuando el ocupante está ausente. La presencia se determinará mediante la geolocalización nativa de Home Assistant a través de la App Companion. Además, la potencia del foco anterior era de 16 W. Con estos datos se desarrollan las Ecuaciones 35 y 36. La primera calcula el consumo con el nuevo relé inteligente; la segunda, el consumo previo sin su uso, lo que permite comparar ambos escenarios diarios.

$$9\ W * 7\ h = 63\ \frac{W}{h} \quad (35)$$

$$16\ W * 7\ h = 112\ \frac{W}{h} \quad (36)$$

Mostrando un beneficio económico del 56,25 %, reduciendo el coste por parte del área de la habitación Reynaldo.

4.4.7. Bombilla Innr (Modelo AE 270 T)

La bombilla LED inteligente Innr AE 270T está diseñada principalmente para 110 V, por lo que en este contexto es necesario un reductor de voltaje. Sus datos técnicos indican una potencia de 11 W, un equivalente incandescente de 75 W y un consumo en apagado de 0,55 W (Amazon, 2025). Estos valores son relevantes para dimensionar la instalación y estimar el consumo energético del sistema en entornos domésticos. Se trabajó con bombillas de base E26, estándar de tornillo para 110–120 V; si se conectan a 220 V se quemarían, por lo que es imprescindible emplear un reductor de voltaje adecuado y conocer su potencia de trabajo. La conexión ideal del cableado de iluminación es en paralelo. En la Ecuación 37 se deben sumar las potencias de la siguiente forma para obtener el consumo total del circuito:

$$11\ W + (8{,}5\ W + 0{,}85\ W) \rightarrow 11\ W + (9{,}35\ W) = 20{,}35\ W \quad (37)$$

“Para cargas continuas se aplica habitualmente un factor de seguridad del 125 % —es decir, no cargar el transformador por encima del 80 % de su capacidad— al calcular la capacidad necesaria del transformador o de la protección asociada. Esto implica que el transformador seleccionado suele ser al menos 1,25 veces la carga prevista, o que la carga debe ser ≤ 80 % de la capacidad nominal (Calculatorsconversion, 2025). Por tanto, se considerará que la potencia de trabajo esté en torno al 80 % de la capacidad del reductor; de este modo se obtiene la Ecuación 38 como valor mínimo a considerar para el reductor. En la Ecuación 39, para el cableado, se calcula la corriente dividiendo la potencia total entre la tensión de trabajo.

$$\frac{20{,}35\ W}{0{,}8} = 25{,}4375\ W \quad (38)$$

$$I = \frac{20{,}35\ W}{110\ V} \rightarrow I = 0{,}185\ A \quad (39)$$

Según NEC (2026) y su tabla de ampacidad para corrientes, si se usan cordones flexibles se puede emplear cable 18 AWG solo si el cordón está listado y su ampacidad nominal y clasificación de temperatura/aislamiento son adecuados para 110 V y el uso previsto. La NEC trata los cordones flexibles en el Artículo 400 y sus tablas (ampacidades dependen del tipo de cordón).

4.4.8. Bombilla ThirdReality (Modelo 3RCB01057Z)

La mayoría de los modelos comerciales de bombillas están diseñados para tensiones bajas; por ello, también es necesario el uso de un reductor de voltaje. Su potencia de trabajo es de 8,5 W, con un margen de incremento de ±10 %, lo que significa que en periodos de uso prolongado la potencia puede subir hasta 9,35 W. Generalmente consumen entre 0,1 W y 0,5 W en modo reposo (Amazon; THIRDREALITY, 2026). Para comparar la situación anterior con la nueva implementación de focos inteligentes, antes se empleaba un foco de 10 W en el pasadizo con uso intermitente, ya que las estancias eran temporales y a veces no era necesaria la iluminación por fuentes cercanas.

En la escalera se usaba un foco de 20 W con uso constante, porque no podía apagarse desde la planta baja; por ello, a menudo quedaba encendido por descuido o falta de accesibilidad. Considerando estos patrones de uso y las diferencias de potencia y control, se calculan las aportaciones energéticas individuales. Con esas consideraciones se expresa la potencia total de ambos focos en la Ecuación 40, que resume el consumo combinado del sistema.

$$10\ W + 20\ W = 30\ W \tag{40}$$

En la tabla 7 se observa que los tiempos de uso varían según lo detectado por dos sensores de movimiento ubicados en puntos específicos; el encendido presenta un promedio de 0,2935 h (≈ 17,61 minutos). Este valor determina el consumo asociado al uso de las bombillas inteligentes en la escalera y el pasadizo, que se expresa en la Ecuación 41. El consumo en reposo se recoge en la Ecuación 42, tomando como referencia el valor máximo en reposo para ambos epicentros de luz. Finalmente, la Ecuación 43 agrupa los términos anteriores para obtener el consumo total diario. A partir de estas ecuaciones se generan los datos siguientes:

$$20{,}35\ W * 0{,}2935\ h = 5{,}9727\ \frac{W}{h} \quad (41)$$

$$(24\ h - 0{,}2935\ h) * 0{,}55\ W = 13{,}0386\ \frac{W}{h} \quad (42)$$

$$13{,}0386\ \frac{W}{h} + 5{,}9727\ \frac{W}{h} = 19{,}0113\ \frac{W}{h} \quad (43)$$

Retornando al uso de fuentes no inteligentes, para la Ecuación 44 se toma un promedio de uso de tres horas diarias; su encendido era diario durante la semana laboral, con la excepción de los fines de semana, cuyo consumo queda reflejado en la Ecuación 45, ya que esos días no se encendían o su encendido era muy corto. La Ecuación 46 muestra el caso de los dispositivos inteligentes, cuyo uso es simplemente diario. Finalmente, la Ecuación 47 calcula la reducción porcentual de energía entre ambos escenarios.

$$30\ W * 3\ h = 90\ \frac{W}{h} \quad (44)$$

$$90\ \frac{W}{h} * 5 = 450\ \frac{W}{h}\ (en\ una\ semana) \quad (45)$$

$$19{,}0113\ \frac{W}{h} * 7 = 133{,}0791\ \frac{W}{h}\ (en\ una\ semana) \quad (46)$$

$$\frac{450 - 133{,}0791}{450} * 100 \rightarrow \frac{316{,}9209}{450} * 100 = 70{,}4269\ \% \quad (47)$$

4.5. Demostración del sistema domótico

Para demostrar la implementación del sistema domótico se realizó un video que muestra, paso a paso, el comportamiento real de un sistema híbrido Zigbee + WiFi en una vivienda de Tacna. El material comienza en la planta alta con el acceso a la central domótica, mostrando dos opciones de ingreso: mediante una URL en cualquier navegador o a través de un túnel virtual. A lo largo del video se presentan las activaciones manuales de cada dispositivo inteligente, partiendo por el equipo ubicado en la parte superior de la vivienda —la válvula de paso de agua— y continuando con relés inteligentes, sensores de movimiento o presencia, diversas bombillas y enchufes inteligentes, y dispositivos con protocolo WiFi. Se ofrece una vista general del hogar y la ubicación física de la central domótica (coordinador, router, switch). Además, se

exhibe el control de escenas tanto local como en la nube, y se muestran automatizaciones ejecutadas en cada ambiente bajo distintos contextos y situaciones.

4.6. Calidad de señal de cada dispositivo

Para medir la calidad de la señal de cada dispositivo según su ubicación se utiliza el LQI (Link Quality Indicator), un indicador que refleja la calidad del enlace radio en una red Zigbee, con valores entre 0 y 255. Según la documentación oficial de Zigbee2MQTT (2026), los valores LQI pueden ser difíciles de interpretar porque las especificaciones de Zigbee y la IEEE 802.15.4 no estandarizan cómo realizar las mediciones. Además, el valor que proporcionan los dispositivos Zigbee no sigue estándares unificados entre fabricantes y pilas Zigbee, por lo que no siempre es fiable.

En teoría, un valor LQI de 255 significa una tasa de error cero, lo que indica una calidad de enlace absolutamente perfecta. En general, un valor LQI alto y positivo es mejor, mientras que un valor LQI bajo es peor. Sin embargo, dependiendo de tus dispositivos, esto podría no ser así. Por lo general, si un dispositivo mantiene un valor LQI de 40 o superior, ese enlace suele considerarse aceptable para condiciones operativas normales.

Los datos de LQI suelen estar deshabilitados al enlazar al coordinador; la calidad de señal solo se muestra al acceder al panel de Zigbee2MQTT. Para registrar el Link Quality Indicator es necesario habilitar la opción LQI en cada dispositivo, lo que permite conservar un historial de calidad de enlace. A continuación se proporciona un enlace que contiene un documento con información detallada sobre las medidas de calidad de enlace de cada dispositivo integrado: https://docs.google.com/spreadsheets/d/1457lYM2xvSgiEE67MN1UXbd4gnfieL6L/edit?usp=sharing&ouid=113818302442887739485&rtpof=true&sd=true. Dentro del documento encontramos los siguientes valores promedios en cuanto a la calidad de señal zigbee para cada dispositivo:

Tabla 8

Valores promedios de LQI para cada dispositivo

Dispositivo	LQI
Bombilla hab rey	31,03

(continúa)

Tabla 8 (continuación)

Sensor de temperatura	118,4331
Luz escalera	26,1812
Luz pasadizo	60,7948
Válvula de agua	102,1123
Bombilla rodelca	41,1284
Movimiento escalera	57,3952
Movimiento tendedero	53,1431
Presenciarocio	43,8968
Relay2piso	144,4647
Bombilla MOES	79,9259
Relay 2 canales	88,2762
Movimiento 2 piso	153,5434
Presencia2piso	101,7772
Movimiento garaje	78,3639
Enchufe cuarto padres	151,6164

En la tabla 8 se exponen los valores promedio de la calidad de señal de cada dispositivo. Como se aprecia, la mayoría de los artefactos Zigbee inteligentes presentan una media operativa aceptable según la documentación oficial; solo tres dispositivos muestran una baja calidad de enlace: Bombilla hab rey, Luz escalera y Bombilla rodelca. Estos problemas pueden mitigarse mediante la reubicación de los dispositivos o la adición de repetidores cercanos. No obstante, las pérdidas de conexión fueron poco frecuentes o nulas, por lo que las interacciones y automatizaciones no se vieron afectadas durante el periodo de uso.

4.7. Resultados de latencia

La medición de latencia en redes Zigbee en entornos domóticos es clave para evaluar el desempeño, sobre todo en arquitecturas híbridas que integran WiFi. En mi tesis analicé la interacción entre nodos finales, routers y el coordinador Zigbee para cuantificar tiempos de respuesta en condiciones domésticas reales. Para recolectar datos, se empleó la herramienta Last Seen, que estima el tiempo desde la última comunicación efectiva de un dispositivo en la red. Aunque es una métrica indirecta, resulta útil en Zigbee, donde el tráfico es esporádico y depende de eventos como activación de sensores o cambios de estado en actuadores.

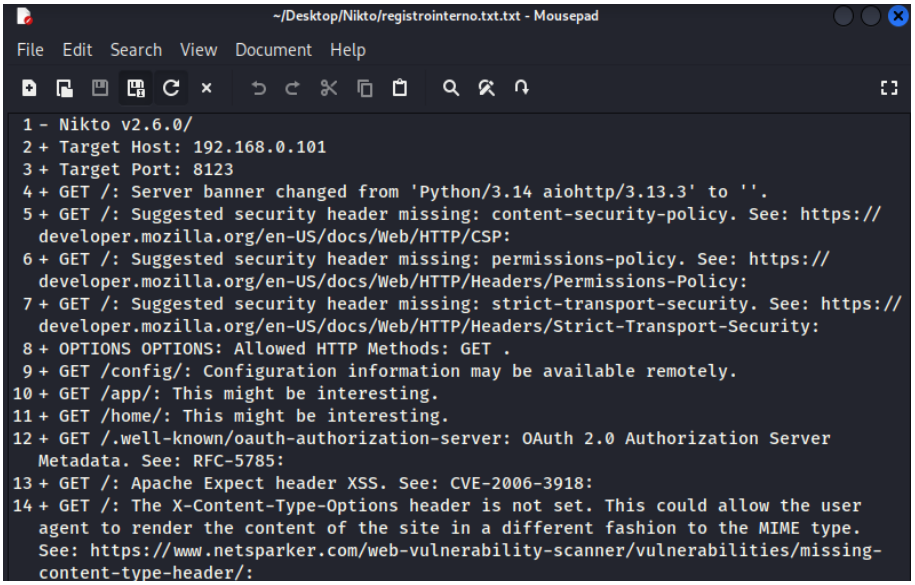
Del mismo modo que para el caso anterior, la información recopilada se encuentra en el siguiente enlace: https://docs.google.com/spreadsheets/d/1QMHh3wMHy0eIQGMtY0qnVqFkVdBFy_9B/edit?usp=sharing&ouid=113818302442887739485&rtpof=true&sd=true, durante las pruebas realizadas, se observó un comportamiento notable en los valores de latencia: muchos dispositivos reportaron 0 ms, lo que puede interpretarse como una comunicación prácticamente instantánea o, más exactamente, como una actualización muy reciente dentro del intervalo de muestreo de la herramienta. Esto evidencia la eficiencia de Zigbee en redes de baja carga y topologías optimizadas. El valor máximo registrado fue 0,347723 ms, cifra que sigue siendo extremadamente baja frente a otros protocolos inalámbricos. Tales resultados confirman que, aun en condiciones menos favorables, la red mantiene un desempeño adecuado para aplicaciones domóticas que requieren tiempos de respuesta rápidos, pero no estrictamente en tiempo real. La medición mediante "Last Seen" permitió validar que la implementación híbrida Zigbee-WiFi cumple los requisitos esperados, mostrando baja latencia y estabilidad de comunicación cuando la integración se realiza correctamente.

4.8. Escaneo de vulnerabilidades

Para detectar riesgos y realizar auditorías de ciberseguridad se empleó Nikto 2.6.0 desde una máquina virtual con Kali Linux. Se actualizaron paquetes con sudo apt update y sudo apt upgrade; los comandos de escaneo vienen configurados por defecto, agilizando el proceso. El comando ejecutado fue: nikto -h 192.168.0.101 -p 8123 -o registrointerno.txt. Nikto apunta al objetivo con -h, especifica el puerto con -p y exporta resultados a un archivo con -o; la ejecución generó el informe cuyos hallazgos se muestran en la figura 131. Los resultados obtenidos permitieron identificar vectores de ataque y recomendaciones.

Figura 131

Escaneo Nikto (dirección IP privada)



La ejecución del escáner de vulnerabilidades correspondió contra el host 192.168.0.101:8123, que identifica la central domótica, con una duración de 89 segundos. No se recuperó un banner completo del servidor, pues la respuesta HTTP no mostró la información habitual sobre software y versión; se observó un cambio de banner desde Python/3.14 aiohttp/3.13.3 a vacío. Se realizaron 8.280 peticiones sin errores reportados por Nikto y se informaron 11 ítems en el host remoto; entre las rutas detectadas figuran las siguientes: /config.js, /app/, /home/, /auth/login/oauth/authorization-server.

La respuesta a OPTIONS indica que el único método HTTP permitido es GET, y Nikto detectó la ausencia de encabezados de seguridad clave: Permissions-Policy, Strict-Transport-Security y Content-Security-Policy. Además, se referencia la vulnerabilidad histórica Apache Expect header XSS (CVE-2006-3981) y se recomienda usar -C all para forzar la búsqueda de CGI. El banner inicial apuntaba a una aplicación Python aiohttp y luego cambió a vacío, lo que puede indicar ocultamiento de información o respuestas variables del servidor. La presencia de /config.js es preocupante por exponer endpoints, claves públicas o configuraciones sensibles; /app/ y /home/ pueden revelar interfaces o recursos estáticos; /auth/login/oauth/authorization-server sugiere endpoints OAuth 2.0 que requieren auditoría. La falta de HSTS, CSP y Permissions-Policy reduce la protección frente a ataques de downgrade, XSS y control de

capacidades del navegador. El escaneo fue agresivo (8.280 peticiones en 89 segundos), lo que pudo provocar respuestas atípicas.

4.9. Automatizaciones

Las automatizaciones constituyen el núcleo de una vivienda inteligente; permiten que dispositivos y servicios actúen de forma coordinada ante condiciones específicas sin intervención manual. Integran disparadores, condiciones y acciones. Se implementaron automatizaciones personalizadas en varias áreas y contextos, mejorando la calidad de vida de los residentes. Las figuras 132, 133 y 134 muestran algunas de las automatizaciones realizadas en Home Assistant y ejemplos de estas.

Figura 132

Automatizaciones realizadas

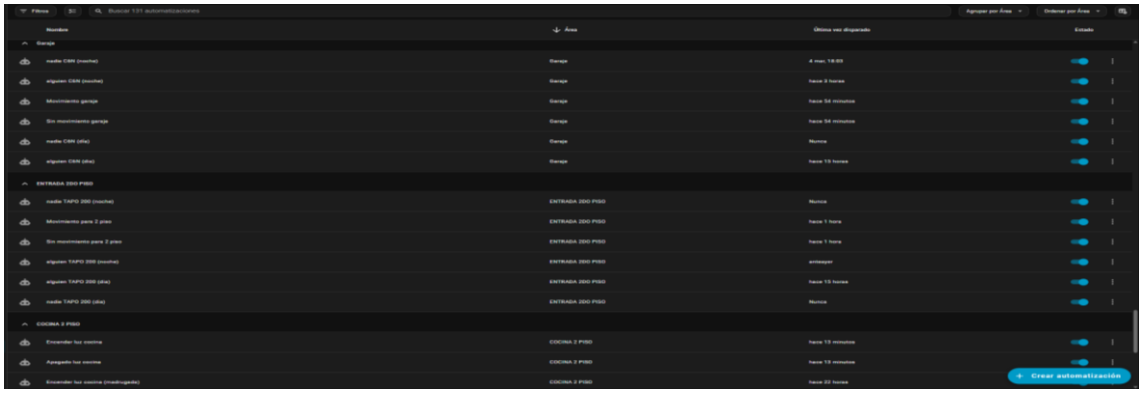


Figura 133

Automatizaciones personalizadas primera parte

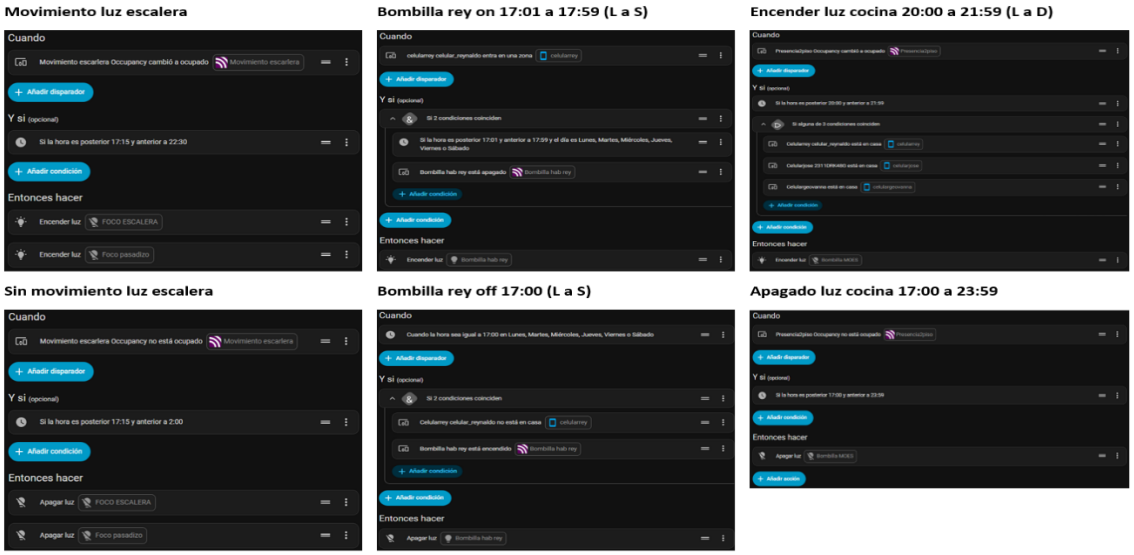
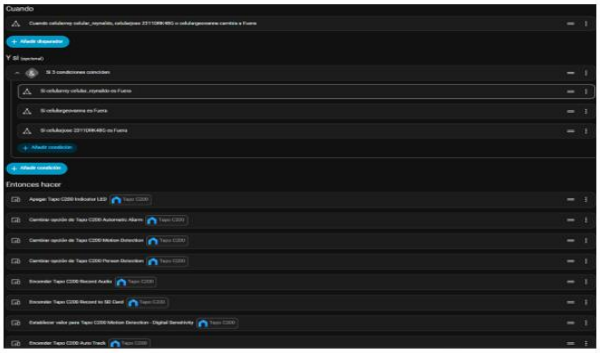


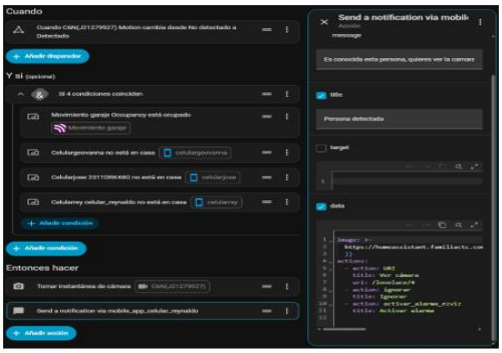
Figura 134

Automatizaciones personalizadas segunda parte

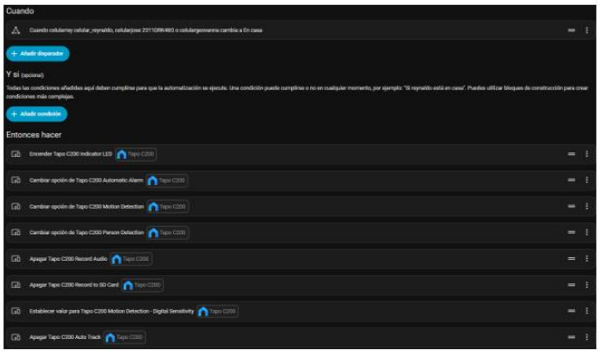
nadie TAPO C200



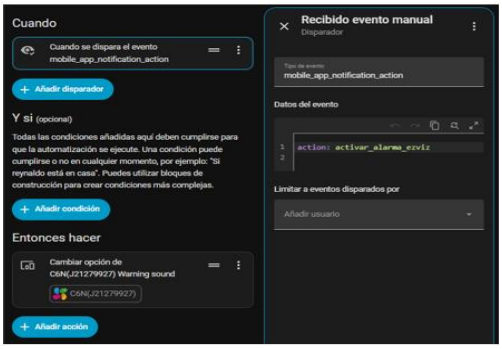
notificación movimiento C6N



alguien TAPO C200



Acción activar alarma EZVIZ C6N



CAPÍTULO V: DISCUSIONES

Al analizar el desarrollo completo del proyecto y los resultados obtenidos, se puede afirmar que en gran parte el sistema cumplió con lo que se esperaba desde su planteamiento inicial. La idea principal consistía en lograr una comunicación fluida entre dispositivos Zigbee y WiFi usando Zigbee2MQTT, dejando una base de red que trabajara con un protocolo específicamente diseñado para domótica sin depender de un centralizador o concentrador de un fabricante en concreto. En la práctica, se consiguió que todos los dispositivos se integraran correctamente y respondieran a los comandos sin fallos críticos. Desde el punto de vista funcional, el sistema opera, automatiza tareas y responde a las acciones del usuario, lo cual representa un resultado positivo, ya que no se trata solo de teoría, sino de una implementación real en un entorno doméstico.

Sin embargo, al tener todo montado en casa y haberlo probado en condiciones reales, se evidenció que la expectativa inicial de que la comunicación sea completamente instantánea y sin ningún tipo de retraso no se cumple al cien por ciento. Si bien los tiempos de respuesta son bastante bajos y, en muchos casos, imperceptibles para el usuario, sí existen pequeños retardos en ciertas situaciones, especialmente cuando intervienen varios componentes, como el broker MQTT, el procesamiento en la Raspberry Pi o cuando la red Zigbee tiene más tráfico. Estos retrasos no afectan el funcionamiento general, pero muestran que el sistema no es totalmente "perfecto" como uno podría imaginar al inicio.

En contraste, uno de los trabajos relacionados con el sistema domótico es el titulado Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control, desarrollado por (Hussein y Nhlabatsi, 2022). Este estudio demuestra de manera integral tanto las fortalezas como las limitaciones inherentes a las arquitecturas modernas basadas en la integración de Zigbee y MQTT dentro del contexto del Internet de las Cosas. En comparación, se puede notar que ambos trabajos comparten una arquitectura básica: dispositivos Zigbee que se comunican a través de una pasarela (gateway) hacia un broker MQTT, lo que refleja un paradigma distribuido y orientado a eventos. La tesis se centra en el diseño, implementación y evaluación aplicada de un sistema domótico híbrido Zigbee–WiFi usando herramientas modernas como Zigbee2MQTT, Home Assistant y un broker MQTT, desplegado en un entorno real.

En ese contexto se analizan métricas prácticas como latencia, consumo energético, estabilidad de red e interoperabilidad entre dispositivos heterogéneos, y se

demuestra que la solución es funcional, escalable y eficiente, con automatización efectiva y reducción de consumo.

El artículo de MDPI adopta un enfoque complementario y crítico al investigar vulnerabilidades de seguridad en arquitecturas Zigbee–MQTT para control de iluminación inteligente. Mediante experimentos, muestra cómo configuraciones comunes sin protecciones adecuadas permiten interceptar o inyectar mensajes en el broker MQTT y tomar control de dispositivos. El estudio enfatiza que las debilidades emergen de la integración y la configuración del sistema más que de los protocolos aislados. Señala fallas típicas como ausencia de autenticación, falta de cifrado y exposición de servicios en red, y demuestra explotaciones prácticas que la tesis no simula.

La diferencia principal radica en el tratamiento de la seguridad: la presente incorpora medidas defensivas como VPN, túneles seguros y control de acceso, pero no realiza pruebas ofensivas ni análisis de explotación; en cambio, el artículo documenta cómo esas vulnerabilidades pueden ser aprovechadas. Cabe mencionar que ambos enfoques son complementarios y, juntos, sugieren una hoja de ruta para sistemas domóticos más robustos: mantener la viabilidad y la eficiencia funcional demostrada por la tesis e integrar, desde el diseño, evaluaciones de amenazas, pruebas de penetración y mecanismos de seguridad avanzados para mitigar los riesgos identificados en la literatura y avanzar hacia soluciones del Internet de las Cosas (IoT) más seguras y sostenibles.

CONCLUSIONES

El diseño híbrido Zigbee–WiFi propuesto demuestra ser una solución equilibrada para domótica, al combinar la eficiencia energética, la topología mallada y la robustez de Zigbee para sensores y actuadores con el ancho de banda y el acceso directo a servicios en la nube que aporta WiFi para cámaras y asistentes. Un gateway centralizado orquesta dispositivos heterogéneos, reduce la congestión del WiFi, optimiza recursos de red y prolonga la vida útil de baterías; sin embargo, su éxito depende de gestionar correctamente la interoperabilidad, el enrutamiento y el mantenimiento de firmware. Se recomienda validar el diseño en otro entorno real para ajustar políticas y mecanismos antes del despliegue.

Las mediciones controladas de consumo realizadas antes y después en periodos equivalentes aportan evidencia cuantitativa sobre las variaciones energéticas y permiten identificar patrones según escenarios y hábitos de uso; el análisis estadístico con medias, intervalos de confianza y pruebas de hipótesis distingue cambios reales de la variabilidad natural y cuantifica ahorros potenciales. Los resultados facilitan priorizar intervenciones de eficiencia y tomar decisiones basadas en datos en lugar de supuestos, aunque la interpretación debe considerar la calidad del firmware y la heterogeneidad de dispositivos. Se aconseja estandarizar protocolos de muestreo, ampliar la muestra temporal y de equipos, y documentar condiciones experimentales para mejorar la representatividad.

El sistema de control remoto diseñado garantiza acceso funcional y minimiza la superficie de ataque mediante una combinación de segmentación de red, control de acceso basado en roles, túneles seguros (VPN/TLS) para telemetría y políticas de actualización automática firmada; el gateway debe incorporar firewall de aplicaciones, inspección TLS, autenticación mutua con certificados, registro y monitorización centralizada con alertas y capacidad de aislamiento de dispositivos comprometidos. Estas medidas equilibran usabilidad y seguridad, permitiendo un despliegue doméstico IoT viable y escalable sin sacrificar privacidad ni integridad. Se recomienda además implementar pruebas de interoperabilidad, procedimientos de recuperación automatizados, mantenimiento continuo y programas de formación para usuarios.

RECOMENDACIONES

En el trabajo de investigación por limitaciones económicas se utilizaron repetidores instalados en áreas principales como habitaciones y pasadizos donde extiendan la señal Zigbee, sería recomendable continuar con el trabajo realizando pruebas con más routers colocando en sitios más cercanos como habitaciones secundarias, baños o pasadizos cortos.

Además, se recomienda para futuras investigaciones, incluir diversos sistemas conformados por dispositivos inteligentes (Zigbee o Wifi) para complementar y solucionar problemas/necesidades que se presenten como: sistemas anti incendios (sensores de humo, alarmas, regaderos); sistemas de climatización inteligente (termostatos y ventiladores); control de accesos (cerraduras, videoporteros inteligentes) para comparar el comportamiento de la red al incrementar el número de dispositivos, evaluando el desempeño antes y después de las nuevas integraciones, con la finalidad de ver cómo afectaría la interoperabilidad en el sistema propuesto.

Para finalizar es necesario tener siempre presente que las adiciones o cambios que se realicen, no deben tener influencias negativas en cuanto a los consumos eléctricos, cualquier intervención debe planificarse y probarse partiendo de un consumo promedio por parte de la distribuidora eléctrica principal, además de verificar su compatibilidad con el software de zigbee2mqtt, especialmente asegurándose de que el dispositivo nuevo se encuentre dentro de los dispositivos soportados en su página oficial.

REFERENCIAS BIBLIOGRÁFICAS

AdGuard Software Ltd (2026). *AdGuard Home Network-wide software for any OS.* https://adguard.com/en/adguard-home/overview.html

AdGuard Software Ltd (2026) *Overview AdGuard DNS Knowledge Base* https://adguard-dns.io/kb/es/adguard-home/overview/

Agarwal, K. (2021). *Improving Zigbee Performance of a Wireless Lighting System in a Smart Home Environment [Master's Thesis, Delft University of Technology].* https://tinyurl.com/cexwt3f9

Ahmad k, Khujamatov H., Lazarev A., Usmanova N., Alduailij M., Alduailij M. (2023) *Sistemas de transporte inteligentes asistidos por Internet de las cosas en ciudades inteligentes: desafíos, oportunidades y futuro* https://onlinelibrary.wiley.com/doi/10.1155/2023/7989079

Alibaba (2026) *SONOFF SNZB-06P sensor de presencia humana Zigbee, detector radar de movimiento, domótica para Alexa, Alice, ZHA y Zigbee2MQTT* https://tinyurl.com/5d5vx57u

AliExpress (2025) *SONOFF ZB Dongle-P Zigbee 3.0 USB Dongle Plus Soporte de puerta de enlace Zigbee universal a través de la serie ZHA o Zigbee2MQTT Sonoff Zigbee* https://tinyurl.com/yyvb77nd

Amazon (2025) *Innr Smart Light Bulbs, A19 Zigbee, Works with Philips Hue* and Alexa (Bridge Required), Warm to Cool White, Dimmable, E26 LED Bulb 75 Watt, Soft White Light, 1140lm, 2-Pack* https://tinyurl.com/3f3fxa2c

Amazon (2026) *THIRDREALITY Smart Color Bulb ZL1,Zigbee hub Required,Compatible with Home Assistant(ZHA&Z2M),SmartThings,Aeotec,Homey,Hubitat or Echo Devices with Built-in Zigbee hub,A19 RGBCW Bulb,800 Lumens* https://tinyurl.com/ynaytx4t

Aqara (2023) *Dual Relay Module T2 User Manual* https://tinyurl.com/3cvanjm8

AQARA. (2025b). *Valve Controller T1 Specs.* https://www.aqara.com/en/product/valve-controller-t1-specs/

AQARA. (2026). *Smart Plug EU Specifications.* https://www.aqara.com/en/product/smart-plug-eu/

Aqara (2026) *AQ-SP-EUC01* https://tinyurl.com/5t2krf29

Ashton, K. & others. (2009). *That 'internet of things' thing. RFID journal, 22(7), 97-114.* https://www.rfidjournal.com/expert-views/that-internet-of-things-thing/73881/

Banggood (2026) *SONOFF SNZB-03P Zigbee3.0 Motion Sensor 5-Seconds Faster Detection Smart Home Security Human Body Detection Smart Scene via eWeLink Work with Alexa Google Home* https://tinyurl.com/358rc8uc

Basan, M. (2024) *What is a VLAN? Ultimate Guide to How VLANs Work* https://www.esecurityplanet.com/networks/what-is-a-vlan/

Basicjuntti666 (2025) *¿Cuántos dispositivos Zigbee puedo usar con Home Assistant Yellow?* https://tinyurl.com/bddra8x5

Beechen, S. (2026) *Home Assistant Google Drive Backup* https://github.com/sabeechen/hassio-google-drive-backup

Blustore (2026) *Módulo Rele Doble T2 Aqara* https://tinyurl.com/2t97brbs

Burdova Carly (2022) *¿Qué es una dirección IP y cómo funciona?* https://www.avg.com/es/signal/what-is-an-ip-address

Calculatorsconversion (2025) *Transformer Sizing Based on Load Calculator – NEC, IEEE* https://tinyurl.com/3kv9wht3

Camargo Ariza L. L., Linero Ramos R. D., Medina Delgado B. (2013) *Análisis de cobertura de redes basadas ISSN 0122-820X* https://dialnet.unirioja.es/descarga/articulo/5364496.pdf

Campoverde Ordóñez, V. D. (2020). *Análisis sobre Nikto como herramienta de escaneo de vulnerabilidades en servidores web [Monografía, Universidad Agraria del Ecuador, Facultad de Ciencias Agrarias].* https://tinyurl.com/2jxdz9rz

Chakkor S., Cheikh E. A., Baghouri M., Hajraoui A. (2014) *Comparative Sensors and Their Applications* https://arxiv.org/abs/1409.6884

Chris (2024) *Cómo agregar una cámara TP-link Tapo a HomeAssistant* https://tinyurl.com/ycyeyfc5

Cisco Networking Academy (2023) *Cisco Networking Academy* https://www.netacad.com/courses/networking

Cloud Optics (2026) *How to Implement Network Segmentation to Secure IoT Devices* https://tinyurl.com/3kpdmvms

Cloudflare (2024) *¿Qué es un proxy inverso? | Servidores proxy explicados* https://www.cloudflare.com/es-es/learning/cdn/glossary/reverse-proxy/

Coursera. (2023). *¿Qué es un diseñador de interfaz de usuario (UI)?* https://www.coursera.org/mx/articles/what-is-a-user-interface-ui-designer-guide

De la Cruz Bernilla, S. M., & Vera Cruz, J. R. S. (2020). *Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo [Universidad Nacional Pedro Ruiz Gallo].* https://hdl.handle.net/20.500.12893/8266

De Luz, S. (2024). *Qué es WireGuard VPN: Instalación y configuración de servidor y clientes VPN. RedesZone.* https://www.redeszone.net/tutoriales/vpn/wireguard-vpn-configuracion/

Demon Warrior Tech Docs (2026) *Complete Samba/SMB File Sharing Guide. Demon Warrior Tech Docs.* https://docs.demonwarriortech.com/Documented%20Tutorials/Storage/Samba/

DER (2021) *E0197: Zigbee2MQTT* http://desdeelreloj.com/e0197/

DiCola, N. (2025) *Network Segmentation vs. VLAN: Which Strategy Delivers True Security?* https://zeronetworks.com/blog/network-segmentation-vs-vlan-strategy-security

Dokuz, A. Ş., Mendebayeva, A., Zhylkybayev, T., & Qaiyrolla, E. (2024). *Basic aspects of selecting and using communication protocols for a smart home system. Bulletin of Shakarim University. Technical Sciences*. https://doi.org/10.53360/2788-7995-2024-3(15)-3

Erco (2026) *Iluminancia: definición, medición y cálculo* https://tinyurl.com/mr2ervy4

Escobedo Rios W. D., Quispe V. E. (2025) *Diseño de una red de acceso remoto utilizando WireGuard como protocolo VPN para la encriptación de los procesos de gestión remota de una empresa agroindustrial del Perú* https://repositorioacademico.upc.edu.pe/handle/10757/685771

Esposito, M., Belli, A., Palma, L., & Pierleoni, P. (2023). *Design and Implementation of a Framework for Smart Home Automation Based on Cellular IoT, MQTT, and Serverless Functions. Sensors, 23(9), Article 9.* https://doi.org/10.3390/s23094459

Eufy team (2026) *Qué es una cámara ONVIF y conocimientos relacionados* https://www.eufy.com/eu-es/blogs/security-camera/what-is-an-onvif-camera

Evans, D. (2011). *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything [White paper]. Cisco Internet Business Solutions Group.* https://tinyurl.com/25837ezu

Exertis (2024) *CGNAT: Carrier-Grade NAT Explained & Why It Matters for Modern Networks*
https://tinyurl.com/yc8yb6vp

Fabricatulampara (2022) *Cuántos lumen necesito para iluminar una habitación: Diferencia entre lumen y lux* https://tinyurl.com/42wj3p2f

Faro (2025) *Luminancia e iluminancia: qué son y en qué se diferencian* https://faro.es/es/blog/luminancia-iluminancia-diferencia/

Fernández, Lorena (2026) *Diferencias entre servidor proxy y servidor proxy inverso* https://tinyurl.com/5n85jkyx

Frenck (2024) *Home Assistant Community Add-on: SSH & Web Terminal* https://tinyurl.com/ys247fpt

Gaotek s.f. *Comprehensive Guide for Zigbee Enabled Home Automation* https://gaotek.com/comprehensive-guide-for-zigbee-enabled-home-automation/

Gil, S., Zapata Madrigal, G. D., García Sierra, R., & Cruz Salazar, L. A. (2022). *Converging IoT protocols for the data integration of automation systems in the electrical industry. Journal of Electrical Systems and Information Technology,*

9(1), 1. https://doi.org/10.1186/s43067-022-00043-4

GISI. (2018). *Ingeniería Mecánica Eléctrica Sensores.* https://virtual.cuautitlan.unam.mx/intar/ime/sensores/

Github, hassio-zigbee2mqtt (2025) *Official Zigbee2MQTT Home Assistant add-on* https://github.com/zigbee2mqtt/hassio-zigbee2mqtt

Github, mercenaruss (2025) *ZigStar Home Assistant add-on repository* https://github.com/mercenaruss/zigstar_addons

Gonnot, T., Yi, W.-J., Monsef, E., & Saniie, J. (2015). *Home Automation Device Protocol (HADP): A Protocol Standard for Unified Device Interactions.* https://doi.org/10.4236/ait.2015.54005

González Fabrizio (2025) *Encriptación de datos: Pilares y métodos para la seguridad de la información* https://tinyurl.com/4avbwh3k

Google Cloud (2026) *Descripción general de Google Cloud* https://docs.cloud.google.com/docs/overview?hl=es-419

H. Seo, C. Kim and H. Kim, (2012) *"ZigBee security for Home automation using attribute-based cryptography," 2011 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2011, pp. 367-368, doi: 10.1109/ICCE.2011.5722631.* https://ieeexplore.ieee.org/abstract/document/5722631

Haidarzhy Valerii (2023) *Zigbee vs. Z-Wave: Zigbee vs. Z-Wave: Comparison, Pros & Cons, How Do They Work?* https://tinyurl.com/2y85xdxk

Hedda (2022) *HowTo - Build a good ZigBee mesh network* https://tinyurl.com/yb7y6v22

Hedda (2024) *Zigbee network optimization: a how-to guide for avoiding radio frequency interference + adding Zigbee Router devices (repeaters/extenders) to get a stable Zigbee network mesh with best possible range and coverage by fully utilizing Zigbee mesh networking* https://tinyurl.com/yc35bv9t

Hermawan R., Maesaroh S., Adhy D. (2021) *Implementasi Plex Media Server dan Adguard Home pada Raspberry pi sebagai Home Server* https://jurnal.unsil.ac.id/index.php/innovatics/article/view/4155/2012

Hernández Guaygua, H. V. (2009). *Diseño de una Red Privada Virtual para el Acceso Remoto a la Información de la Empresa American Jeans de Ambato desde la Empresa Super Exitos de Guayaquil [Universidad Técnica de Ambato].* http://repositorio.uta.edu.ec/handle/123456789/311

Holter, L., & Hjelmtvedt, V. G. (2024). *Security in Open-Source Smart Home Platforms: A Case Study of Home Assistant [Master thesis, NTNU].* https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3172682

Home Assistant. (2025). *Zigbee Home Automation. Home Assistant.* https://www.home-assistant.io/integrations/zha/

Home Assistant (2026) *Generic Camera* https://www.home- assistant.io/integrations/generic/

Home Assistant (2026) *Google Drive* https://www.home- assistant.io/integrations/google_drive/

Home Assistant (2026) *HTTP* https://tinyurl.com/47eb34du

Home Assistant (2024) *Recommended Zigbee radio adapters and modules* https://www.home-assistant.io/integrations/zha/

Home Assistant (2026) *Tareas comunes - Sistema operativo* https://www.home-assistant.io/common-tasks/os/

Hussein Noon & Nhlabatsi Armstrong (2022) *Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control* https://www.mdpi.com/2624-831X/3/4/24

IamHDT (2026) *Home Assistant Add-on: File editor* https://github.com/IamHDT/homeassistant-fileeditor-addon

IEEE (2022) *Internet of Things Journal* https://ieee-iotj.org/

Infordisa (2024) *El cifrado es la base principal de la seguridad de datos* https://www.infordisa.com/soc/cifrado-para-seguridad-de-datos/

Inversorlatam (2019) *La VPN crea una conexión privada y segura entre muchas personas y dispositivos a través de Internet* https://tinyurl.com/435cvsbv

Jaihar, J., Lingayat, N., Vijaybhai, P. S., Venkatesh, G., & Upla, K. P. (2020). *Smart Home Automation Using Machine Learning Algorithms. 2020 International Conference for Emerging Technology (INCET), 1-4.* https://doi.org/10.1109/INCET49848.2020.9154007

JuniperNetworks (2022) *IOT NETWORK SEGMENTATION* https://tinyurl.com/3p29xkzp

JurajNyiri (2025) *HomeAssistant-Tapo-Control* https://tinyurl.com/323eanwu

JurajNyiri (2026) *HomeAssistant - Tapo: Cameras Control* https://github.com/JurajNyiri/HomeAssistant-Tapo-Control

Kalagara, S., Borra, C., Dasari, S. H., & Kondabattula, D. C. (2018). *Smart Home Automation System By analysis of Communication Protocols. International Journal of Research, 5(7), Article 7.* https://journals.pen2print.org/index.php/ijr/article/view/12994

Kartawiguna et al. (2025) *An Open-Sourced Home Monitoring Framework IOP Conf. Ser.: Earth Environ. Sci. 1564 012137* https://iopscience.iop.org/article/10.1088/1755-1315/1564/1/012137/pdf

Kazemi, M. (2024). *Optimizing Web Service Performance: A Comparative Analysis of Load Balancing Strategies Using NGINX and HAProxy with StoRM WebDAV Deployment [Tesi di Laurea Magistrale, Università di Bologna].* https://amslaurea.unibo.it/id/eprint/33906/1/Final-Mahsakazemi.pdf

Kim, T., Ramos, C., & Mohammed, S. (2017). *Smart City and IoT. Future Generation Computer Systems, 76, 159-162*. https://doi.org/10.1016/j.future.2017.03.034

Kumar N. & Mallick P. K. (2018) *The Internet of Things: Insights into the building blocks, component* https://tinyurl.com/yhuhpekd

Lennon (2025) *Overview of ONVIF and RTSP Protocols* https://sponcomm.com/info-detail/onvif-and-rtsp

Liang, Y., & Luo, X. (2024). *Design of Smart Home System Based on ZigBee Technology. 2024 IEEE First International Conference on Data Intelligence and Innovative Application (DIIA), 1-5.* https://doi.org/10.1109/DIIA62678.2024.10871311

Lliso, A. (2021). *Uso de MQTT para el control de dispositivos de IoT [Trabajo Fin de Grado, Universitat Politècnica de València].* http://polipapers.upv.es/index.php/IA/article/view/3293

Madadi Barough S., Ruiz Blanco P., Lin J., Vidal R., Gomez C. (2024) *Matter: IoT Interoperability for Smart Homes* https://arxiv.org/abs/2405.01618

Marron J., Fagan M., Souppaya M., Watrobski P., Mulugeta B., Symington S., Klosterman J., Rearick C., Deane C., Harkins D., Jump D., Richardson M., Dolan A., Haefner K., Pratt C., Thakore D., Romness P., Baker T., Griego D., Wyseur B., Allott N., Mereacre A., Setter A., Delplancke J., Clark S., Dow M., Egerter S., Kent K. (2025) *Trusted Internet of Things (IoT) Device Network- Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol Based IoT Device and Network Security* https://tinyurl.com/ujezuye3

Mathe, S. E., Kondaveeti, H. K., Vappangi, S., Vanambathina, S. D., & Kumaravelu, N. K. (2024). *A comprehensive review on applications of Raspberry Pi. Computer Science Review, 52, 100636.* https://doi.org/10.1016/j.cosrev.2024.100636

MercadoLibre (2026) *Memoria Hiksemi Micro Sd 256gb Neolux Class10/v30 4k 100mb/s* https://www.mercadolibre.com.pe/memoria-hiksemi-micro-sd-256gb-neolux-class10v30-4k-100mbs/p/MPE45256056

MercadoLibre (2026) *Multimetro Digital 7 Funciones Con Puntas Lion Tools 5958* https://www.mercadolibre.com.pe/multimetro-digital-7-funciones-con-puntas-lion-tools-5958/p/MPE27924640

Mero Martínez, J. E. (2022). *Modelo de sistema domótico para la automatización de viviendas utilizando Raspberry Pi 4 con Home Assistant [Trabajo de titulación para la obtención del título de Ingeniero de Sistemas, Universidad Politécnica Salesiana, Sede Guayaquil, Carrera de Ingeniería de Sistemas].* https://dspace.ups.edu.ec/bitstream/123456789/24402/1/UPS-GT004240.pdf

Microsoft (2026) *Detección de ransomware y recuperación de sus archivos* https://tinyurl.com/44k92hc4

MiniOrange (2026) *Proxy inverso Seguridad de las aplicaciones* https://www.miniorange.com/es/reverse-proxy/

Miori, V., Russo, D., & Ferrucci, L. (2019). *Interoperability of home automation systems as a critical challenge for IoT. 2019 4th International Conference on Computing, Communications and Security (ICCCS), 1-7.* https://doi.org/10.1109/CCCS.2019.8888125

Moes (2026) *MOES Zigbee Smart LED Light Bulb Energy Efficient E27 Dimmable RGB White Color Lamp* https://moeshouse.com/products/zigbee-smart-bulb-zb-tda9-rcw-e27-ms

Mohammedi, I. E. ; Drid, S.; Kouzou, A. ; Djeddaoui, N. (2025) *Design and Evaluation of a Smart Home System with Home Assistant* https://ieeexplore.ieee.org/abstract/document/11358018/figures#figures

Morgado, Julia Furst (2025) *What is the 3-2-1 Backup Rule?* https://www.veeam.com/blog/321-backup-rule.html

Nasralla (2025) *Smart Home Automation in the IoT Era: A Comparative Study of Network Topologies and Communication Protocols* https://link.springer.com/chapter/10.1007/978-981-97-8348-9_8#citeas

NEC (2026) *Tablas de Ampacidad NEC - Referencia* https://elecalculator.com/es/guides/code-compliance/nec-ampacity-tables/

NETGEAR (2026) *GS308Ev4 - Switch Ethernet Gigabit Easy Smart Managed Essentials de 8 puertos*

https://www.netgear.com/support/es/product/gs308ev4

Nijhof Franck (2026) *AdGuard Home* https://www.home-assistant.io/integrations/adguard/

ONVIF (2021) *Device Feature Discovery Specification* https://tinyurl.com/3vc55rn7

ONVIF (2025) *Driving the Future of Interoperability* https://www.onvif.org/wp-content/uploads/2025/10/onvif-overview-20251009.pdf

ONVIF (2025) *ONVIF Overview Driving the Future of Interoperability* https://www.onvif.org/wp-content/uploads/2025/06/onvif-overview-20250602.pdf

Orfanos, V. A., Kaminaris, S. D., Papageorgas, P., Piromalis, D., & Kandris, D. (2023). *A Comprehensive Review of IoT Networking Technologies for Smart Home Automation Applications. Journal of Sensor and Actuator Networks, 12(2), Article 2.*
https://doi.org/10.3390/jsan12020030

Orfanos, V., Kaminaris, S. D., Piromalis, D., & Papageorgas, P. (2019). *Trends in home automation systems and protocols. AIP Conference Proceedings, 2190(1), 020049.*
https://doi.org/10.1063/1.5138535

Pastor, Javier (2019) *Qué es Cloudflare, cómo funciona y por qué cuando "se cae" parte de internet se viene abajo*
https://tinyurl.com/4jysr92e

Patterson, D. A.; Hennessy, J. L. (2021) *Computer Organization and Design MIPS EDITION THE HARDWARE/SOFTWARE INTERFACE SIX EDITION*
https://tinyurl.com/ms429u3w

Pearson, Daniel (2025) *Why the '3-2-1' backup rule is still key to modern cybersecurity*
https://tinyurl.com/wxfvwv88

Pelco (2026) *What is ONVIF? A complete guide to ONVIF cameras and profiles*
https://www.pelco.com/blog/onvif-guide

Pérez, J., & Merino, M. (2025). *Definicion de Domótica*.
https://definicion.de/domotica/

Perumal, T., Ramli, A. R., Leong, C. Y., Samsudin, K., & Mansor, S. (2010). *Interoperability Among Heterogeneous Systems in Smart Home Environment. En Web-Based Information Technologies and Distributed Systems (Vol. 2, pp. 141-157). Atlantis Press.*
https://doi.org/10.2991/978-94-91216-32-9_7

Pratchaya Jaisudthi, Pachara Threerapat Sridee Natthakran Phungkoed, Kanyaphak Srisuk, Vasupon Phueaknumpol (2025) *Comparative Study of Modern VPN Solutions: Impact of Cloudflare, ZeroTier, and WireGuard on Network and Server Performance*
https://ph01.tci- thaijo.org/index.php/lej/article/download/260843/174520

Prieto, M., Bañeres, D., & Serra, M. (2025). *Implantación de un proxy inverso en un entorno empresarial [Trabajo final de grado, Universität Oberta de Catalunya].*
https://tinyurl.com/4bepmp48

Promart (2026) *Cámara Inalámbrica Wifi 360º C6N Full HD - Ezviz* https://tinyurl.com/4rn4fb7s

Raspberry Pi 4. (2026). *Raspberry Pi 4 Model B.* https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

Reddit (2024) *SMlight Vs Sonoff ZigBee dongle* https://tinyurl.com/4jjr9k9b

RenierM26 (2026) *EZVIZ* https://www.home-assistant.io/integrations/ezviz/

Robert, D., & Istvan, S. (2011). *SNMP protocol based home automation system. 2011 RoEduNet International Conference 10th Edition: Networking in Education and Research, 1-4.* https://doi.org/10.1109/RoEduNet.2011.5993697

Romero Cabrera, S. (2019). *Estudio de la plataforma domótica Home Assistant e integración en Raspberry Pi [Trabajo Fin de Grado, Universidad de Sevilla].* https://biblus.us.es/bibing/proyectos/abreproy/92598/fichero/TFG-

Romero, D., Hermosillo, G., Taherkordi, A., Nzekwa, R., Rouvoy, R., & Eliassen, F. (2010). *RESTful Integration of Heterogeneous Devices in Pervasive Environments. En Distributed Applications and Interoperable Systems (Vol. 6115, pp. 1-14). Springer Berlin Heidelberg.* https://doi.org/10.1007/978-3-642-13645-0_1

Rákay, R., & Galajdová, A. (2019). *Comparison of communication protocols for smart devices. TECHNICAL SCIENCES AND TECHNOLOGIES, 3(17), 146-154.* https://doi.org/10.25140/2411-5363-2019-3(17)-146-154

Schulzrinne H., Rao A., Lanphieret R. (1998) *Real Time Streaming Protocol (RTSP)* https://datatracker.ietf.org/doc/html/rfc2326

Schulzrinne, H. (2003) *RTP: A Transport Protocol for Real-Time Applications* https://www.ietf.org/rfc/rfc3550.pdf

Segurilatam (2021) *Autenticación de doble o múltiple factor: una capa adicional de seguridad* https://tinyurl.com/ewnbj998

SigmaOS (2024) *Internet of Things (IoT) Terms Explained: Network Topology* https://tinyurl.com/4s653jpf

Silva, D., Carvalho, L. I., Soares, J., & Sofia, R. C. (2021). *A Performance Analysis of Internet of Things Networking Protocols: Evaluating MQTT, CoAP, OPC UA. Applied Sciences, 11(11), Article 11.* https://doi.org/10.3390/app11114879

SmartHomeScene (2025) *How To Build a Stable and Robust Zigbee Network* https://tinyurl.com/33d9h3vr

SODIMAC (2026) *Cable GPT 16 AWG Azul 100 Metros*

https://tinyurl.com/54c29umh

SONOFF. (2026). *SONOFF ZBMINIR2 Zigbee Extreme Smart Switch (Neutral Wire Required).*
https://tinyurl.com/44pn9vtn

SONOFF. (2026b). *SONOFF ZBDongle Plus-P Zigbee 3.0 USB Dongle-P.* https://tinyurl.com/49d7sw8x

SONOFF (2023) *SNZB-06P(EN) User Manual V1.0* https://tinyurl.com/km4abxzv

Sonoff (2024) *ZBMINIR2 Quick Guide V1.1* https://tinyurl.com/3ex9vfks

Stateofsurveillance (2025) *Home Network VLANs* https://tinyurl.com/yfdmwxsv

Steane, T. N. E., & Radcliffe, P. J. (2019). *IOT status communication for home automation. International Journal of Computing, 240-248.* https://doi.org/10.47839/ijc.18.3.1516

Stepanov, M. S., Poskotin, L. S., Shishkin, D. V., Turgut, T., & Muzata, A. R. (2021). *The using of ZigBee protocol to organize the «Smart Home» system for aged people. T-Comm, 15(10), 64-70.* https://doi.org/10.36724/2072-8735-2021-15-10-64-70

Sujatha, E., Shanthasheela, S., Rajarajeswari, H., Kannan, R., & Anurada, T. (2025). *Optimizing browsing security: AdGuard's influence on privacy and user experience across devices. In Web Intelligence and Human-Machine Interaction (ICWIHI 2025), Advances in Intelligent Systems and Computing (pp. 47–64). Springer Nature.* https://link.springer.com/chapter/10.1007/978-981-96-8563-9_4

Sørensen, J. (2024) *HACS 2.0: La mejor manera de compartir proyectos creados por la comunidad ahora es aún mejor* https://tinyurl.com/4wm7pzt4

Tailscale (2026) *Networking should be simple* https://tailscale.com/kb/1151/what-is-tailscale

Tailscale (2026) *WireGuard® vs. Tailscale | Which VPN Alternative is Better for You?* https://tailscale.com/compare/wireguard

Tecnoyfoto (2025) *Segmentar Red Doméstica: Métodos Efectivos y Seguros* https://www.youtube.com/watch?v=vSVWuuSv09w

Thetechmunk (2026) *Home Automation Zigbee vs WiFi* https://thetechmunk.com/home-automation-zigbee-vs-wifi/

Tiendamia (2026) *Aqara Zigbee Motion Sensor P1, Detector de Movimiento Inteligente, Requiere AQARA HUB, Batería de 5 Años, Tiempo de detección configurable, para Sistema de Alertas y Automatizaciones, Compatible con HomeKit, Alexa, IFTTT* https://tiendamia.com/pe/producto?amz=B09QKVMMTB

TONGOU. (2026). *Tuya Zigbee Din Rail Smart Circuit Breaker with Metering TO-Q-SY1-JZT.* https://tinyurl.com/2dbzvxt7

TONGOU (2024) *¿Qué es Zigbee2MQTT: cómo conectarlo con TONGOU* https://www.tongou.com/es/que-es-zigbee2mqtt-como-conectarlo-con-tongou/

Torres Tello J. W. (2008) *Estudio comparativo entre las arquitecturas isa y diffserv en una pasarela residencial con servicios de voz, datos y video para el dimensionado de una red domótica* https://bibdigital.epn.edu.ec/bitstream/15000/4200/1/CD-1324.pdf

Touch J., Lear E., Ono K., Eddy W., Trammell B., Iyengar J., Scharf M. (2025) *Service Name and Transport Protocol Port Number Registry* https://tinyurl.com/2e2e9xmm

TP-LINK (2024) *TAPO CAMERA RTSP GUIDE* https://www.tp-link.com/tapo-camera-rtsp-guide

TP-LINK (2025) *Cómo ver la cámara Tapo en el PC a través del flujo RTSP* https://www.tp-link.com/es/support/faq/2680/

TP-LINK (2025) *How to view Tapo camera on PC/NAS/NVR through RTSP/Onvif Protocol*
https://www.tp-link.com/us/support/faq/2680/

TP-LINK. (2026). *Tapo C200 V3.20 Specifications.* https://www.tp-link.com/pe/home-networking/cloud-camera/tapo-c200/v3.2/

TP-Link. (2026). *Tapo C310 Specifications.* https://www.tp-link.com/pe/home-networking/cloud-camera/tapo-c310/

TP-LINK (2026) *Pan/Tilt Home Security Wi-Fi Camera* https://tinyurl.com/38rmbx53

Tp-Link (2026) *TL-WR841HP*

https://www.tp-link.com/pe/home-networking/high-power-router/tl-wr841hp/

Tran, W (2025) *Step-By-Step OneDrive File Recovery for Office 365 Admins* https://spin.ai/blog/onedrive-file-recovery/

Van Steen, M.; Tanenbaum, A.S. (2023) *SISTEMAS DISTRIBUIDOS.NET* https://www.distributed-systems.net/index.php/books/ds4/

Veesion (2025) *ONVIF: ¿cuáles son las ventajas del equipo de vigilancia en tienda?* https://veesion.io/es/onvif-cuales-son-las-ventajas-del-equipo-de-

Vidal, S. (2023) *¿Cómo puedo segmentar mi red WiFi doméstica con un router?* https://tinyurl.com/bdh6u94t

Viserco. (2023). *Seguridad domótica, qué es y cómo aprovecharla. Viserco Seguridad.* https://www.viserco.com/seguridad-domotica-que-es

VueVille (2025) *Hands-on Review: SONOFF ZigBee 3.0 USB Dongle Plus https://tinyurl.com/4datmxp3*

Wendy (2025) *ZHA vs. Zigbee2MQTT: The Best Zigbee Integration for Home Assistant?* https://tinyurl.com/5x37m8zn

WizzDev (2026) *Overview of IoT Network Topologies* https://wizzdev.com/blog/overview-of-iot-network-topologies/

Zapatero, Carlos (2025) *Qué es CG-NAT y por qué se comparte la IP pública* https://www.adslzone.net/reportajes/operadores/que-es-cg-nat-operadores/

Zigbee2MQTT. (2025). *Getting started. Zigbee2MQTT.* https://www.zigbee2mqtt.io/guide/getting-started/

Zigbee2MQTT (2025) *Supported Adapters* https://www.zigbee2mqtt.io/guide/adapters/

Zigbee Alliance (2015) *ZigBee Specification* https://tinyurl.com/2sntc4wb

ANEXOS

Anexo 1. MATRIZ DE CONSISTENCIA

<table>
<tr><th>Problema</th><th>Objetivos</th><th>Variables</th><th>Indicadores</th><th>Metodología</th></tr>
<tr><td>Problema general

¿Cómo el diseño e implementación de un sistema híbrido de comunicación Zigbee–WiFi contribuye a la automatización eficiente, segura y accesible de una vivienda urbana en la ciudad de Tacna durante el año 2025-2026?</td><td>Objetivo general

Diseñar e implementar un sistema híbrido de comunicación Zigbee–WiFi que contribuya a la automatización eficiente, segura y accesible de una vivienda urbana en la ciudad de Tacna durante el año 2025</td><td rowspan="2">Sistema domótico</td><td rowspan="2">- Índice de heterogeneidad funcional (IHF)
- Índice de estabilidad de integración (ISI)
- Ratio de adaptadores necesarios (RAN)

- Tiempo medio de retardo
- Consumo total
- Consumo promedio por dispositivo
- Máximo número de dispositivos funcionando sin fallos

- Número de puertos abiertos
- Intentos de acceso bloqueados
- DNS filtrados o bloqueados
- Uso de HTTPS y certificación de autentificación habilitada</td><td rowspan="2">Tipo de investigación:

Aplicada, porque busca resolver un problema técnico específico que tiene implicancias prácticas en la eficiencia energética y operativa de hogares inteligentes.

Nivel de investigación:

Aplicativo, busca intervenir directamente en la realidad para resolver un problema práctico o mejorar una condición existente.

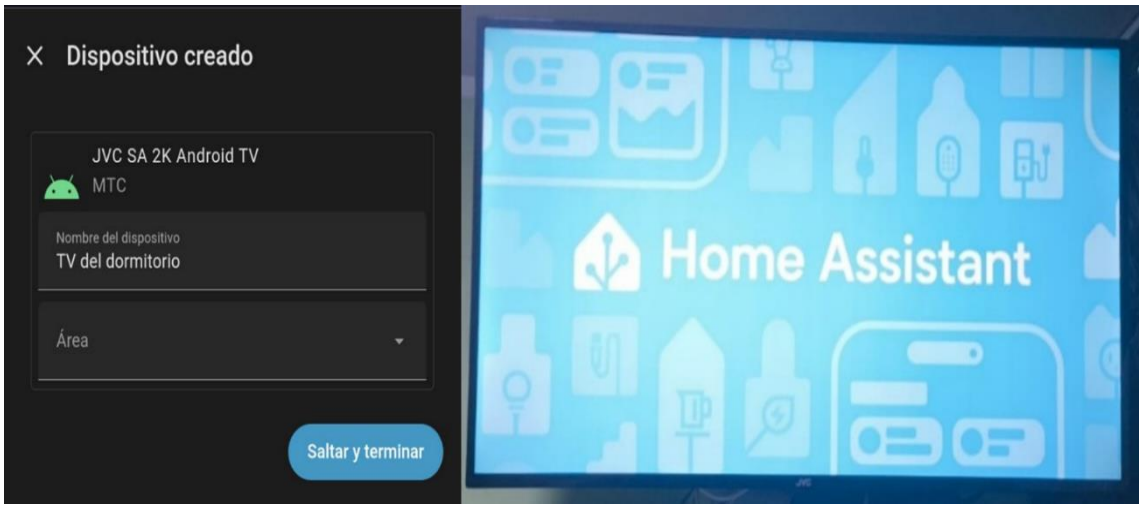
Diseño de investigación

La investigación es experimental, su propósito es construir, implementar y evaluar un sistema domótico híbrido Zigbee–WiFi y explicar las relaciones causales entre la marca de dispositivos y las variables como: consumo energético, interoperabilidad, estabilidad y seguridad.</td></tr>
<tr><td>Problemas específicos

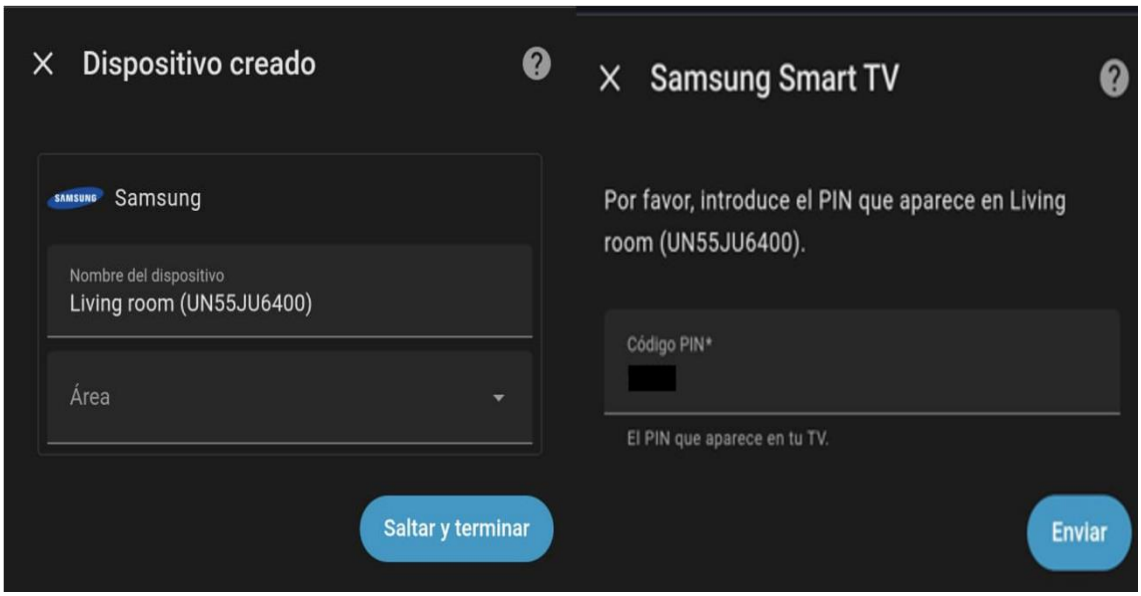
a. ¿Cómo diseñar una arquitectura híbrida Zigbee–WiFi que permita un control remoto confiable de los dispositivos domóticos, sin depender de plataformas o hubs propietarios?
b. ¿En qué medida la automatización de la iluminación y de los actuadores mediante la arquitectura híbrida propuesta reduce el consumo energético en comparación con el uso convencional de dichos dispositivos?
c. ¿Cómo implementar un sistema de control remoto que garantice la seguridad de las comunicaciones y una exposición controlada a Internet en un entorno doméstico basado en IoT?</td><td>Objetivos específicos

a. Diseñar una arquitectura híbrida Zigbee–WiFi que permita un control remoto confiable de los dispositivos domóticos, sin depender de plataformas o hubs propietarios
b. Determinar que la automatización de la iluminación y de los actuadores mediante la arquitectura híbrida propuesta reduce el consumo energético en comparación con el uso convencional de dichos dispositivos
c. Implementar un sistema de control remoto que garantice la seguridad de las comunicaciones y una exposición controlada a Internet en un entorno doméstico basado en IoT</td></tr>
</table>

Anexo 2: INTEGRACIÓN DEL TELEVISOR JVC UBICADO EN LA HABITACIÓN REY

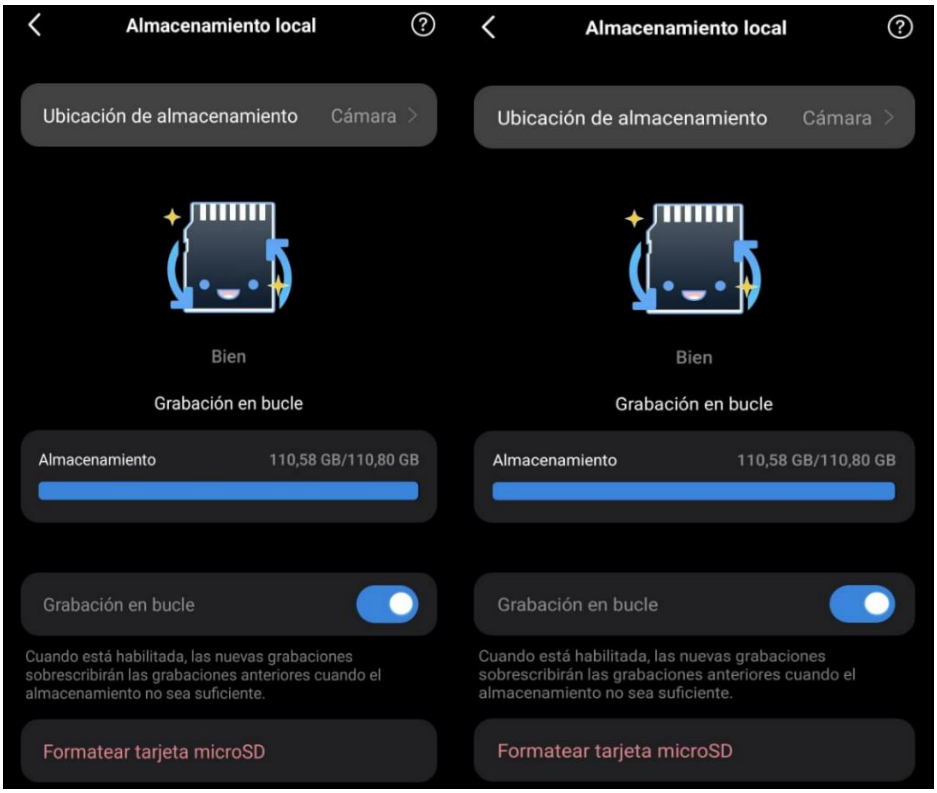


Anexo 3: INTEGRACIÓN DEL TELEVISOR SAMSUNG UBICADO EN LA SALA DEL SEGUNDO PISO

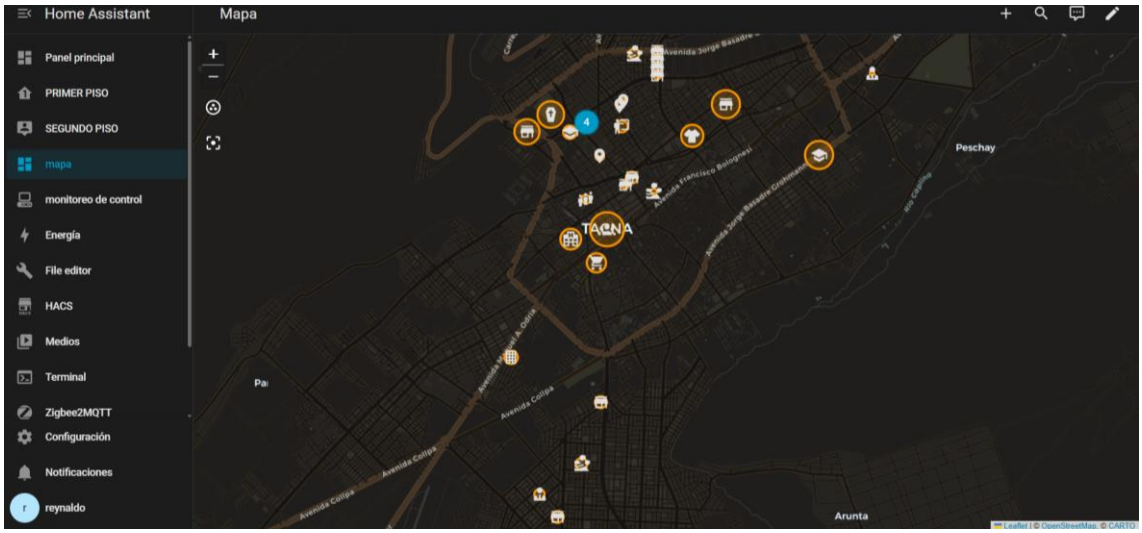


Anexo 4: ESTADO DE ALMACENAMIENTO PARA LA TARJETA MICRO SD DE LA CÁMARA EZVIZ C6N

Anexo 5: ESTADO DE LAS TARJETAS MICRO SD PARA CÁMARA TAPO C310 Y C200



Anexo 6: DESIGNACIÓN DE ZONAS COMÚNMENTE TRANSITADAS/ÚTILES



Anexo 7: NOMBRES DE TODAS LAS ZONAS EN EL APARTADO DE MAPA