



This is the **published version** of the bachelor thesis:

Limarino Rivero, Anthony. *La casa del futuro*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Enginyeria Informàtica)

This version is available at <https://ddd.uab.cat/record/334461>

under the terms of the  license.

La casa del futuro

Anthony Limarino Rivero

Resumen — En este documento se presenta el diseño conceptual de una vivienda inteligente e interconectada bajo el modelo Edge Computing, el cual está orientado a optimizar la seguridad, la privacidad y la eficiencia energética. Utilizando una placa Raspberry Pi 5 con almacenamiento SSD NVMe y el sistema operativo Home Assistant OS como nodo de procesamiento local, se unifica el control de los subsistemas más básicos en un hogar domótico, como son la climatización, iluminación, electrodomésticos de línea blanca y accesos a la vivienda. El diseño destaca por incluir una segmentación de red estricta mediante VLANs, un túnel cifrado WireGuard para el acceso remoto seguro y la adopción del estándar Matter sobre Thread para la interoperabilidad nativa sin dependencias de la nube. También se presentan ciertos KPI que son útiles para validar la eficiencia y factibilidad del sistema. Finalmente, para comprobar la viabilidad práctica de la arquitectura y su comportamiento asíncrono basado en eventos, se ha implementado un prototipo de alarma por detección de movimiento con un microcontrolador ESP32, un sensor PIR y una máquina virtual con Home Assistant OS.

Palabras clave— Domótica, hogar digital, Edge Computing, Home Assistant, Raspberry Pi, Estándar Matter, Thread, Zigbee, segmentación de red, privacidad, Internet de las cosas, interoperabilidad, sensores, microcontrolador, YAML

Abstract— This document presents the conceptual design of a smart and interconnected home under the Edge Computing paradigm, which is aimed at optimizing security, privacy and energy efficiency. Using a Raspberry Pi 5 board with NVMe SSD storage and Home Assistant OS as a local processing node, the control of the most fundamental subsystems in a home automation environment — such as climate control, lighting, major home appliances and residential access — is unified. The design stands out for incorporating a strict network segmentation through VLANs, a WireGuard encrypted tunnel for secure remote access and the adoption of the standard Matter-over-Thread to ensure native interoperability without cloud dependencies. Additionally, certain KPIs are presented to validate the system's efficiency and feasibility. Finally, to verify the practical viability of the architecture and its asynchronous event-based behavior, a motion-detection alarm prototype has been implemented using an ESP32 microcontroller, a PIR sensor and a virtual machine running Home Assistant OS.

Index Terms— Home automation, digital home, Edge Computing, Home Assistant, Raspberry Pi, Matter Standard, Thread, Zigbee, network segmentation, privacy, Internet of Things, interoperability, sensors, microcontroller, YAML



1 INTRODUCCIÓN

En los últimos años, la evolución tecnológica ha cambiado la manera en la que interactuamos con los espacios donde vivimos. Gracias al despliegue de tecnologías inteligentes en el entorno doméstico, una casa puede responder a nuestras necesidades, permitiéndonos controlar distintos dispositivos e incluso anticipar nuestro comportamiento frente al uso de estos. Este concepto conocido como domótica u hogar digital, se refiere a la automatización y control inteligente de funciones y sistemas de una vivienda para mejorar la calidad de vida de sus habitantes.

El concepto de hogares inteligentes se empezó a esparcir en la década de 1930, bajo el nombre de “hogares del futuro”. Este nombre se debe al deseo que se tenía de conseguir una alta eficiencia en la vivienda. El *Intelligent Building Institute* (IBI) creó el concepto de “hogar inteligente” en la década de 1970, pensando en un edificio que ofreciera un uso eficiente y productivo del espacio de trabajo[1]. La palabra domótica proviene de la combina-

ción del latín *domus* (casa) y el término griego *αὐτόνομος* (autónomo), reflejando la idea de hogares que son capaces de “gobernar a sí mismos” utilizando sistemas tecnológicos, permitiendo gestionar tareas como la iluminación, climatización, electrodomésticos, entre otros. Dichos sistemas utilizan redes de comunicación, sensores, actuadores y un controlador normalmente centralizado que permite la coordinación inteligente según condiciones ambientales, rutinas del usuario y criterios de eficiencia energética y seguridad[2].

Estudios recientes demuestran que la domótica permite reducir notablemente el consumo energético al coordinar el funcionamiento de los sistemas de climatización, iluminación y electrodomésticos, favoreciendo un uso más razonable y adaptado a las necesidades reales del hogar[3]. La seguridad y el bienestar del habitante también son dos aspectos destacables. Para estos casos, se incorporan sensores de movimiento, detectores de humo y gas que pueden enviar alertas en tiempo real a los dispositivos del usuario, o incluso activar respuestas automáticas.

Una “casa del futuro” incluye el uso tecnologías emergentes como el Internet de las cosas (*IoT*) o la inteligencia artificial (*IA*), debido a que son elementos que aumentan la capacidad de automatización y adaptación de los sistemas domésticos. Esto quiere decir que los dispositivos no solo responderán a órdenes de control del usuario, sino que pueden aprender de los hábitos y determinar unos patrones de uso [4].

- E-mail de contacte: Anthony.Limarino@autonoma.cat
- Menció: *Enginyeria de Computadors*
- Treball tutoritzat per: *Jordi Castilla Miró (Microelectrònica i Sistemes Electrònics)*
- Curs 2025/26

No obstante, el despliegue de estas tecnologías enfrenta desafíos críticos en términos de interoperabilidad entre fabricantes y la seguridad de los datos del usuario. La transición hacia el estándar *Matter* (conectividad de código abierto para hogares inteligentes) y la implementación de sistemas *Edge Computing* aparecen como soluciones clave para garantizar que los hogares inteligentes sean privados y escalables[5].

Por lo cual, la “casa del futuro” se presenta como un proyecto que emplea tecnologías avanzadas y define un entorno inteligente e interconectado, buscando el confort, la seguridad y la eficiencia. La integración de todos estos elementos convierte la vivienda en un espacio dinámico que “redefine” la experiencia de habitar un hogar.

2 ESTADO DEL ARTE

La domótica ha experimentado un crecimiento notable en los últimos años debido al desarrollo de nuevas tecnologías de comunicación y al auge del IoT. Lo que antes se consideraba una tecnología reservada para proyectos de “alta gama”, se ha transformado en un ecosistema accesible y masivo. Se han desarrollado diversas aproximaciones tecnológicas y enfoques para automatizar elementos del hogar, que varían principalmente en su arquitectura, tecnologías utilizadas y nivel de complejidad.

2.1 Evolución de los sistemas de control

Tradicionalmente, la domótica utilizaba protocolos principalmente cableados, con el estándar KNX como referente, el cual requería de reformas estructurales en el edificio. Actualmente, el mercado está repleto de dispositivos inalámbricos de bajo coste que utilizan protocolos como Wi-Fi o Zigbee, por lo que el propio usuario puede instalar un aparato sin necesidad de hacer una obra ni requerir de un profesional (*Retrofitting*)[6].

La interfaz de usuario también ha cambiado. Los smartphones son los cuadros de mando universal predominantes, ya que son ordenadores de bolsillo que nos permiten realizar muchas funciones. Sin embargo, la tendencia actual se está desplazando hacia el control utilizando la voz, lo que se conoce como control por lenguaje natural o VUI (*Voice User Interface*). Tenemos como líderes de mercado a *Amazon Alexa*, *Google Assistant* y *Apple Siri*, los cuales han evolucionado más allá de su función como interfaces de audio para convertirse en nodos centrales de gestión [7].

Cabe mencionar que actualmente estamos en proceso de pasar de casas automatizadas que simplemente siguen órdenes, a “casas cognitivas”. Gracias al *Machine Learning*, los sistemas actuales pueden analizar datos históricos para anticiparse a nuestras necesidades. Por ejemplo, el sistema no solo enciende el aire acondicionado cuando el usuario está en casa y la temperatura ha superado cierto umbral, sino que también aprende a qué hora vuelve del trabajo y se inicia automáticamente para enfriar el hogar antes de que regrese.

2.2 Protocolos de comunicación

El correcto funcionamiento de una instalación domótica se basa en su capacidad para comunicarse de manera fiable, segura y eficiente. Los protocolos de comunicación definen reglas y formatos para intercambiar datos. La domótica inalámbrica se basa en redes de bajo consumo y corto alcance. Entre las destacadas tenemos:

- **Zigbee:** destaca por su topología de malla, donde cada dispositivo actúa como un repetidor, extendiendo el alcance de la red, garantizando la redundancia y sin aumentar el consumo energético.
- **Z-Wave:** trabaja en bandas de frecuencia por debajo del GHz para reducir interferencias con el Wi-Fi, que es ampliamente utilizado, y mejora la penetración de materiales de construcción[8].

Sin embargo, en la actualidad se está optando por la convergencia hacia un estándar universal, como lo es *Matter*. Este se apoya en Thread (protocolo de transporte de malla basado en IP y con baja latencia) para proporcionar interoperabilidad “nativa” entre fabricantes[9]. A diferencia del Wi-Fi (destinado a transferir gran cantidad de datos) o Bluetooth Low Energy (destinado a la configuración inicial de dispositivos), *Matter* permite gestionar localmente los datos, lo cual reduce la latencia y garantiza el control sin conectividad a la nube, siendo esto un factor crítico para la seguridad y la privacidad del hogar.

Esta evolución hacia el control local se traduce en una arquitectura de *Edge Computing*, donde el procesamiento de los datos se realiza en el propio hogar donde se han generado. Esto reduce las vulnerabilidades de privacidad asociadas al almacenamiento en la nube y mejora los tiempos de respuesta.

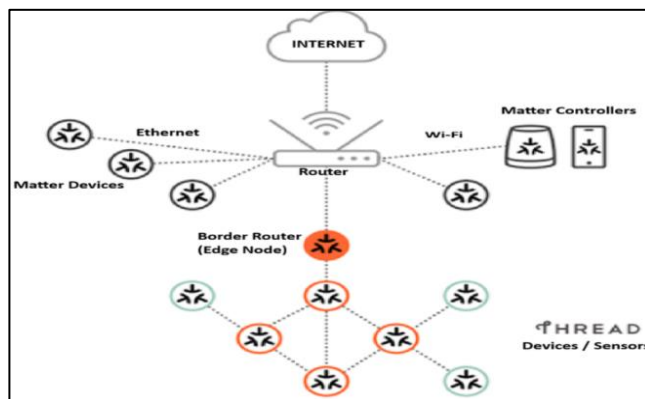


Ilustración 1. Esquema de red Thread, Wi-Fi y Ethernet

2.3 Tecnologías actuales

La arquitectura física de una casa del futuro se divide principalmente en tres capas: capa de percepción (sensores), capa de ejecución (actuadores) y capa de procesamiento (control). Estas capas permiten que el hogar pase de un entorno estático a uno dinámico que comprende el contexto y las necesidades del usuario.

En el ámbito de los sensores, la mayor innovación es el uso de radares de ondas milimétricas (*mmWave*), con las que se puede detectar presencia humana estática, como la respiración[10]. Los sensores de calidad del aire modernos monitorizan CO₂, partículas contaminantes (PM_{2.5}) y compuestos orgánicos volátiles (VOC) para gestionar la automatización de la ventilación.

Por otra parte, el núcleo de procesamiento y control ha evolucionado hacia el *Edge Computing*, implementado con microprocesadores como Raspberry Pi que requieren una configuración inicial, o con procesadores dedicados “plug-and-play” como Home Assistant Green. Estas herramientas permiten que el control esté centralizado de forma local (cerraduras, relés y climatización). Al proce-

sar la información dentro del propio hogar, se reduce notablemente la latencia y se protege la privacidad del usuario, además de permitir en funcionamiento ante fallos de la conexión a internet.

2.4 Seguridad y privacidad

La seguridad de las viviendas inteligentes ha evolucionado de un enfoque principalmente físico (alarmas y sensores) hacia un modelo ciber-físico. La interconexión de dispositivos a través de *IoT* introduce vulnerabilidades críticas, como el acceso no autorizado a datos personales o control malintencionado de los dispositivos del hogar[11].

Uno de los desafíos actualmente es mantener la privacidad de los datos, ya que el uso de cámaras y asistentes de voz genera información sensible, que tradicionalmente se procesaba en la nube exponiendo al usuario a posibles fallos de seguridad. La tendencia actual se basa en el principio de *Privacy by Design*, donde los sistemas se diseñan para minimizar la exposición de los datos.

En este contexto, el estándar *Matter* es clave, ya que impone requisitos de seguridad, como el cifrado de extremo a extremo y la autenticación de dispositivos mediante certificados digitales. En adición al *Edge Computing*, garantiza que la información y hábitos de uso no salgan de la red doméstica, fortaleciendo la confianza del usuario en materia de privacidad[12].

3 OBJETIVOS

Este proyecto busca proponer el desarrollo de una vivienda inteligente basada en la integración de sistemas domóticos para el control de electrodomésticos, climatización, iluminación, seguridad, sensores ambientales y automatización de apertura y cierre, partiendo desde un enfoque más teórico hacia uno más práctico/funcional. La idea es poder ejecutar órdenes localmente o en remoto sobre los siguientes elementos del hogar:

- Climatización
- Iluminación
- Frigorífico, horno, cafetera, lavadora, lavavajillas
- Sensores: movimiento, temperatura, humedad, humo, calidad del aire y fugas de agua
- Alertas como respuesta los sensores
- Persianas y ventanas

El enfoque principal del sistema se centra en la seguridad integral de la vivienda, teniendo en cuenta tanto la seguridad física como la seguridad ambiental y la supervisión del estado de los dispositivos. Además, realizaré una implementación de un sensor de movimiento para simular su funcionamiento en un entorno “real” controlado y comprobar su rendimiento.

4 METODOLOGÍA

La estructura de trabajo para realizar el proyecto la he dividido en cuatro fases secuenciales e incrementales:

4.1 Búsqueda de información inicial

Estudio en profundidad sobre las arquitecturas de domótica actuales para entender la situación del mercado y justificar las decisiones tecnológicas que se toman en este proyecto:

- Arquitecturas *IoT* para smart homes
- Sistemas de control embebidos

- Protocolos de comunicación adecuados
- Plataformas que ofrecen sistemas de domótica

4.2 Análisis de soluciones existentes

En esta fase, se investigan las soluciones comerciales existentes con el fin de:

- Evaluar las características técnicas
- Establecer criterios de selección de tecnologías
- Determinar ventajas y limitaciones

4.3 Diseño del sistema

En esta fase, se define la estructura y la interconexión de los elementos necesarios para implementar el sistema:

- Arquitectura general del sistema
- Descripción funcional de los subsistemas
- Diagrama de estados del sistema
- Selección de dispositivos, sensores y actuadores
- Flujo de comunicación de los dispositivos

4.4 Evaluación de viabilidad y simulación con sensor de movimiento

En esta fase, se realiza un análisis teórico sobre la viabilidad técnica del proyecto, así como la definición de métricas de rendimiento para monitorizar la eficacia de la solución propuesta.

- Viabilidad tecnológica
- Comunicación entre sistemas
- Limitaciones y riesgos

Además, realizo una implementación con un microcontrolador y un sensor de movimiento para simular un dispositivo *IoT* de alarma.

5 PLANIFICACIÓN DEL PROYECTO

En el **Anexo 1** se muestra el **diagrama de Gantt** del proyecto, con la duración aproximada de cada fase. Considerando que el proyecto tiene cinco entregas y la duración total es de aproximadamente veinte semanas, he definido los siguientes hitos:

Hito	Fecha (máx)	Descripción
Definición del proyecto	8/03/2026	Planificación inicial
Estado del arte	12/04/2026	Bibliografía sobre smart home, <i>IoT</i> y conectividad
Diseño conceptual	24/05/2026	Propuesta de un diseño de vivienda inteligente con diagramas y casos de uso
Documento en fase final	14/06/2026	Propuesta de documento en fase muy avanzada o final
Propuesta de presentación	28/06/2026	Primera versión de la presentación final para la defensa del trabajo

Tabla 1. Hitos propuestos para el desarrollo del proyecto

6 DESARROLLO DE LA SOLUCIÓN

En este apartado se detalla el diseño y la implementación técnica de la propuesta de “Casa del futuro”. La solución se basa en una arquitectura de control local para garantizar la privacidad, utilizando estándares de interoperabilidad modernos que permiten la gestión integral de la vivienda

tanto de forma presencial como remota.

6.1 Definición general de la arquitectura

La propuesta de este proyecto no se limita a la instalación de dispositivos aislados, sino que se requiere un ecosistema que trabaje en conjunto. Para ello, he optado por utilizar una arquitectura *Edge Computing* para garantizar latencia mínima y que los datos del usuario no dependan de servidores de terceros.

6.1.1 Edge Computing: nodo central

En este modelo, el procesamiento, el almacenamiento y la toma de decisiones críticas se ejecutan localmente dentro de la red doméstica. Esto aporta las siguientes ventajas [13]:

- El sistema sigue funcionando sin conexión a Internet. Las automatizaciones no dependen de servidores eternos.
- Al procesar datos sensibles dentro de la red, se elimina la exposición de la información a terceros.
- Se reduce la latencia en la comunicación.

6.1.2 Hardware del nodo central

Para poder aplicar el modelo de *Edge Computing*, he seleccionado una *Raspberry Pi 5* como unidad de procesamiento central. Esta elección está justificada debido a su bajo consumo energético (entre 10 y 15W) y su potencia de cálculo [14]. Sus características más relevantes son:

- **Procesador:** SoC Broadcom BCM2712 con CPU Quad-core a 2.4 GHz. Permite gestionar las automatizaciones y base de datos sin retardos significativos.
- **Memoria:** he optado por la opción de 16 GB de RAM LPDDR5 para asegurar la fluidez al ejecutar varias automatizaciones de forma simultánea.
- **Almacenamiento:** una unidad SSD NVMe para garantizar lecturas y escrituras rápidas, y asegurar la integridad de los datos.
- **Conectividad:** la placa solo dispone de Bluetooth y Wi-Fi de forma nativa. Para utilizar los protocolos Zigbee 3.0 y Thread es necesario incorporar un adaptador de radio dual (USB Dongle).

En los **Anexos 2 y 3** se muestran las imágenes de la *Raspberry* y del adaptador de radio dual respectivamente. Para complementar el Edge Device basado en la Raspberry Pi 5, se añadirán interfaces físicas de control:

- **Interfaces de control táctil:** se integrarán al menos cuatro pantallas táctiles que actuarán como estaciones de control fijas. Se colocará una en cada habitación y la última en el salón principal. Estas pantallas ejecutarán el *Dashboard* de Home Assistant, permitiendo gestionar los subsistemas de forma cómoda.

6.1.3 Software del nodo central: Home Assistant OS

El sistema operativo elegido es *Home Assistant OS (HassOS)*, el cuál es una distribución de Linux minimalista optimizada para la domótica [15]. Se basa en el uso de contenedores para aislar los procesos críticos del sistema de las aplicaciones de terceros. La ventaja de este entorno es su capacidad de **abstracción de hardware**, es decir, que permite unificar dispositivos de distintos fabricantes en una única interfaz de control. La imagen siguiente muestra el diagrama de conexión de la

arquitectura de borde (Edge), a nivel de IoT.

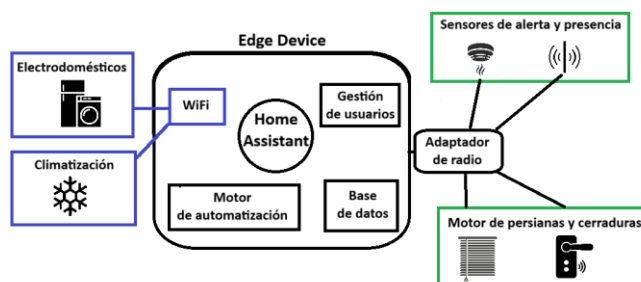


Ilustración 2. Diagrama de conexión de la arquitectura Edge

Actualmente, Home Assistant ofrece una interfaz visual para poder configurar cada dispositivo sin tener que escribir líneas de código en formato YAML (YAML Ain't Markup Language). Cabe mencionar que no se requiere un bucle infinito que consuma recursos, sino que cuando un sensor envía un dato, se dispara un evento y se activa un actuador, siguiendo la estructura *Triggers-Conditions-Actions*.

Como ejemplo, este es el código YAML para realizar el corte de agua por "inundación" en un determinado sistema. Aunque sería más cómodo tener todos los sensores agrupados en la misma automatización, he optado por separarlos para poder identificar la zona donde se ha detectado la fuga.

```
- alias: "Corte automático de agua por inundación"
  trigger:
    - platform: state
      entity_id: binary_sensor.cocina_fugas_water_leak
      to: "on"
  condition: []
  action:
    - service: switch.turn_off
      target:
        entity_id: switch.cocina_electrovalvula_principal
    - service: notify.mobile_app_usuario
      data:
        title: "¡Alerta de inundación!"
        message: "Fuga detectada en la cocina. Suministro de agua cortado."
```

Ilustración 3. Código YAML para cortar el suministro de agua

6.2 Definición de los subsistemas

Una vez definido el núcleo del sistema, procedo a agrupar los dispositivos en subsistemas funcionales que interactúan entre sí a través del nodo central.

6.2.1 Seguridad ambiental

Este es uno de los subsistemas más críticos, ya que tienen la función de proteger la integridad física del habitante y de la edificación [16]. Los elementos incluidos aquí utilizan principalmente el protocolo Zigbee 3.0, debido a su alta fiabilidad y bajo consumo.

- **Sensores de humo y gas:** se ubicará uno en la cocina, ya que es una zona de riesgo, y otro en el pasillo de la planta superior. Estarán configurados como dispositivos siempre activos, los cuáles dispararán una alarma sonora local y enviarán una notificación al smartphone del habitante.
- **Detección de fugas de agua:** consistirá en una electroválvula inteligente y sensores de inundación colocados en el suelo

de la cocina, en el cuarto de la colada que es donde está ubicada la lavadora, y uno por cada cuarto de baño, ubicados estratégicamente. En caso de detección, el sistema enviará una orden a la válvula inteligente para cortar el suministro de agua.

- **Calidad del aire interior:** a través de una red de sensores este sistema monitorizará la temperatura, la humedad y los niveles de CO2. Si los niveles superan los umbrales aceptables, el sistema podrá activar la ventilación forzada abriendo ventanas, y en tal caso notificará al usuario.

6.2.2 Climatización inteligente

Este subsistema es el encargado de garantizar el confort térmico del habitante. A diferencia de los sistemas con termostatos aislados, esta solución integra la climatización con otros sensores para poder gestionar automáticamente la eficiencia energética [17].

- **Control:** se utilizará un termostato inteligente Wi-Fi, y se comunicará con el Edge Device. Su funcionamiento dependerá de la red de sensores de temperatura y humedad mencionados en el punto anterior. Esto permite gestionar la temperatura del hogar por zonas.
- **Eficiencia proactiva:** si el sistema detecta que hay ventanas abiertas, puede suspender la climatización en esa zona.

6.2.3 Seguridad perimetral

Aquí se agrupan las medidas diseñadas para proteger el perímetro físico del hogar. Actúan como primera línea de defensa, buscando prevenir accesos no autorizados y robos. En este caso, el subsistema es una mezcla de seguridad física tradicional y seguridad digital.

- **Sensores de movimiento y presencia:** se utilizarán sensores de **onda milimétrica** (mmWave) en el salón y en los dormitorios para detectar personas, aunque se mantengan inmóviles. Esto también evita que las luces inteligentes se apaguen accidentalmente [18]. Utilizarán el protocolo Zigbee 3.0.
- **Tecnologías de autenticación:** la apertura de puerta con llave tradicional se complementará con un sistema de cerradura inteligente que utiliza **biometría capacitiva** [19] (huella dactilar con medición de variación eléctrica) y **NFC** (*Near Field Communication*). Esto permite que el morador pueda utilizar tanto su huella como su móvil o reloj inteligente como llaves digitales. Además, el sistema permitirá generar códigos **PIN temporales** para que otros usuarios puedan acceder. Todo quedará registrado en el nodo central.
- **Cifrado de autenticación:** relacionado con la apertura de la puerta biométrica, debido a la criticidad de este elemento, la comunicación se realizará mediante el estándar Matter-over-Thread. Este protocolo proporciona una latencia muy baja e impone capas de cifrado para evitar ataques *man-in-the-middle*.
- **Seguridad activa:** la cerradura inteligente también contará con un sensor que detecte los intentos de manipulación (*anti-tamper*). Si se detecta un intento de apertura forzado, se envía una alerta inmediatamente al dueño del hogar.

A continuación, se muestra una tabla con los métodos de acceso a la vivienda y su nivel de fiabilidad.

Método	Tecnología	Nivel de seguridad	Propósito
Biometría	Sensor capacitivo	Muy alto	Acceso principal
NFC	Radio frecuencia	Alto	Acceso de respaldo o invitados
Código PIN	Teclado	Medio	Acceso temporal o emergencia
Llave física	Cerradura cilíndrica	Medio - Bajo	Fallo del hardware o emergencia

Tabla 2. Métodos de acceso al domicilio

6.2.4 Iluminación, persianas y ventanas

En este punto se explica la automatización de elementos que son principalmente de confort. Se utilizará el estándar Matter-over-Thread, principalmente porque su red en malla es muy útil para conectar los dispositivos y su tiempo de respuesta es muy bajo.

- **Iluminación inteligente:** las luces adaptarán su intensidad y temperatura (frío a cálido) en función de la hora del día. También se podrán encender o apagar las bombillas en función de la presencia o ausencia de personas. Podrán encenderse aleatoriamente cuando el morador se encuentre de viaje para disuadir a posibles delincuentes.
- **Persianas y ventanas motorizadas:** además de responder a ordenes manuales, se podrán abrir o cerrar en función del tiempo exterior, de la temperatura interior o como respuesta a una alerta de los sensores ambientales [20]. El propio sistema automatizado de la persiana o ventana indica si está abierta o cerrada.

6.2.5 Electrodomésticos de línea blanca

Este punto agrupa los grandes electrodomésticos, generalmente fijos, duraderos y esenciales en el hogar. El protocolo para estos elementos habitualmente es Wi-Fi, y esto suele implicar fragmentación en sistemas propietarios [21].

- **Refrigerador:** tendrá monitorización continua de temperatura, con notificación al habitante si se detectan anomalías en la temperatura, por ejemplo, si se deja la puerta abierta durante varios minutos.
- **Horno:** además de poder encenderlo o apagarlo a distancia, notificará el modo de cocción, temperatura y tiempo restante.
- **Cafetera:** se integrará con la rutina del usuario. Las cafeteras inteligentes permiten adaptar la temperatura del agua, la cantidad de café y la cantidad de agua, y guardar modos de funcionamiento. También notifican cuando se requiere una limpieza o descalcificación.
- **Lavadora y lavavajillas:** además de programar un horario fijo, permiten iniciar, pausar o detener los lavados de forma remota, siempre que la puerta esté correctamente cerrada. También notifican el consumo eléctrico y de agua.

6.3 Infraestructura de red y conectividad

La eficacia de una arquitectura *Edge Computing* depende de

la robustez de su infraestructura de red. En esta propuesta, la red doméstica será un ecosistema estructurado en niveles de criticidad.

6.3.1 Segmentación de red y seguridad

Para garantizar la integridad del sistema, se dispondrá de una segmentación mediante VLANs (Virtual Local Area Networks). Esta técnica permite aislar el tráfico de los elementos IoT de los dispositivos personales y de invitados, con el objetivo de mejorar la seguridad[22].

- **VLAN de gestión:** acceso exclusivo para el nodo central (Raspberry Pi 5), con permisos para administrar el resto de VLANs.
- **VLAN IoT (Dispositivos Wi-Fi):** aquí se conectarán los electrodomésticos, el termostato, la electroválvula y las pantallas táctiles de gestión. Por seguridad, esta VLAN solo podrá comunicarse con la VLAN de gestión. El tráfico hacia internet estará restringido y el acceso a datos personales de la vivienda estará bloqueado.
- **VLAN de residentes:** incluirá tanto la conexión por cable como la red Wi-Fi para los habitantes. Tendrá acceso completo de entrada y salida a Internet.
- **VLAN de invitados:** red Wi-Fi para visitantes. Permitirá el acceso a Internet, pero tendrá bloqueado el acceso a cualquier recurso local del hogar.

En la siguiente tabla, se muestra división de cada VLAN, con sus rangos y número máximo de hosts.

VLAN ID	Nombre	Dispositivos	Rango IP	Hosts
10	Gestión	Nodo central	10.10.0.0/28	14
20	IoT	Pantallas táctiles, termostato, línea blanca	10.20.0.0/24	254
30	Residentes	Equipos cableados y Wi-Fi	10.30.0.0/26	62
40	Invitados	Conexiones temporales Wi-Fi	10.40.0.0/27	30

Tabla 3. Tabla de direccionamiento de las subredes del hogar

La justificación del tamaño de cada VLAN es la siguiente:

Gestión: esta subred es crítica, por lo que limitarla reduce el riesgo frente intrusiones, pero dejando un margen para escalabilidad.

IoT: es la más grande, ya que se podrían tener muchos dispositivos que requieran una dirección IP, pero he considerado que tener más de 254 es algo poco probable.

Residentes: pueden tener muchos dispositivos personales como ordenadores de sobremesa, portátiles, móviles, tabletas, entre otros.

Invitados: he optado por limitar esta subred, ya que he considerado que no es común tener más de 30 invitados simultáneamente.

6.3.2 Topología y protocolos de comunicación

El sistema utilizará una topología híbrida que combina una estructura en estrella (Wi-Fi) con estructuras en malla (Zigbee y Thread).

- **Red IP:** utilizará Wi-Fi 6[23] y Ethernet. Estará reservada para dispositivos que quieren alimentación permanente y transferir muchos datos, como el nodo central y los electrodomésticos de línea blanca.
- **Redes de malla:** utilizarán Zigbee 3.0 y Thread[24]. Son necesarias para conectar los sensores y la iluminación. En este tipo de red, cada dispositivo actúa como un repetidor de señal, lo cual elimina los “puntos muertos” del hogar, de manera que, si un nodo falla, se utilizarán rutas alternativas para llegar al nodo central.

6.3.3 Interoperabilidad: Matter over Thread

Matter es una capa de lenguaje común que corre sobre el protocolo Thread (basado en IPv6) para tener controlados todos los dispositivos posibles bajo un “mismo idioma”. Esta combinación permite que, por ejemplo, un sensor de movimiento de un determinado fabricante pueda encender una bombilla de otro de forma instantánea, sin pasar por ninguna nube, reduciendo la latencia. Los dispositivos Zigbee 3.0 también funcionan como nodos de una red en malla, distinta a la de Thread.

6.3.4 Acceso remoto seguro

Para cumplir con el requisito de la gestión remota sin comprometer la seguridad local, se implementará un túnel de cifrado mediante el protocolo WireGuard, considerado el más seguro y eficiente actualmente. WireGuard crea una conexión punto a punto cifrada (VPN o Virtual Private Network) entre un dispositivo del usuario y la Raspberry Pi 5. De esta forma, el usuario puede manejar los dispositivos de su hogar desde el exterior como si estuviera conectado a la red doméstica.

El nodo central funciona como servidor WireGuard y como extremo del túnel de la VPN, y crea una subred privada para el túnel. Se necesitan claves criptográficas públicas y privadas en ambos extremos de la comunicación para poder validar su identidad al iniciar la conexión[25]. Una vez conectado el dispositivo remoto, puede enviar órdenes a los elementos inteligentes de la casa, ya que el sistema interpreta que está dentro de la red doméstica. En la siguiente imagen se puede observar el esquema de la comunicación mediante la VPN.

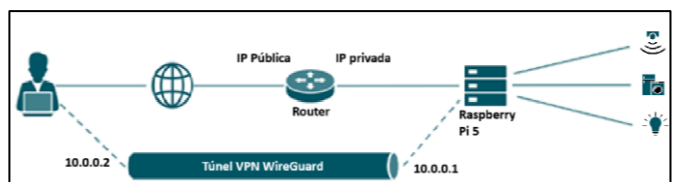


Ilustración 4. Esquema de funcionamiento de WireGuard

6.3.5 Distribución de los dispositivos

En el **anexo 4** se muestra en una imagen el plano de la casa con las distintas habitaciones y con los distintos dispositivos que forman parte del sistema inteligente, además de los protocolos de comunicación que utilizan. En la parte inferior se puede observar una leyenda con cada tipo de dispositivo y tipo de conexión.

6.4 Diagramas de estados de los dispositivos

Estos diagramas muestran el comportamiento operacional de los dispositivos, donde la Raspberry Pi 5 actúa como núcleo central de control, para ejecutar acciones automáticas en función de la información recibida por los sensores o por peticiones del usuario[26].

6.4.1 Sensor de presencia

Este sensor se mantiene en estado inactivo (IDLE) hasta que detecta una señal. En ese momento, el sistema envía una alerta al usuario. Una vez enviada la alerta, vuelve al estado inactivo.

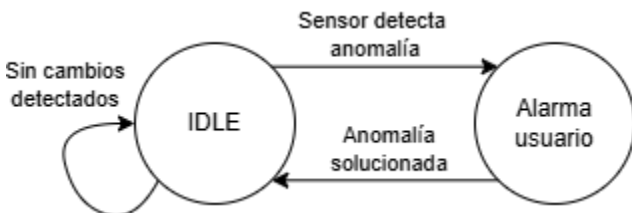


Ilustración 5. Diagrama de estados del sensor de presencia

6.4.2 Sensor de inundación

Este sensor se mantiene inactivo hasta que detecta agua constante. En ese momento, el sistema envía una alerta al usuario e inmediatamente envía una señal para corta el suministro de agua. Cuando el sensor ya no detecte la fuga, se enviará otra señal para reestablecer el suministro y volverá al estado inactivo.

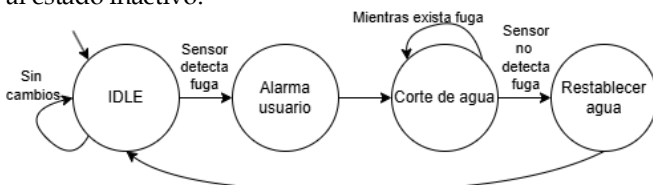


Ilustración 6. Diagrama de estados del sensor de inundación

6.4.3 Sensores de humo, gas y temperatura

Estos sensores monitorizan constantemente el ambiente, mientras el sistema está en estado de lectura. Cuando detectan una anomalía, envían una alarma al usuario. Si el usuario ha habilitado la opción de ventanas automáticas, el sistema enviará una señal para abrir las ventanas de la zona afectada. Una vez que la anomalía ha terminado, el sistema enviará otra señal para cerrar las ventanas y volverá al estado de lectura.

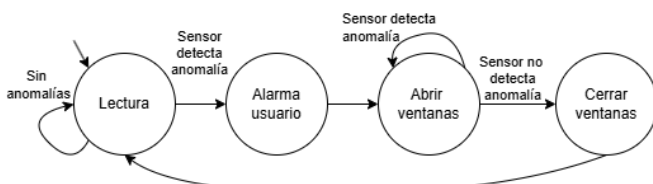


Ilustración 7. Diagramas de estado de sensor ambiental

6.4.4 Cerradura inteligente

Este elemento se encontrará bloqueado hasta que el usuario lo desbloquee mediante un sistema de apertura permitido. Si el desbloqueo se realiza correctamente, la cerradura permanecerá abierta durante 30 segundos, tiempo tras el cual se cerrará. Por otra parte, si se detecta un intento de apertura fallido o manipulación, se enviará una alarma al usuario y se mantendrá en estado bloqueado.

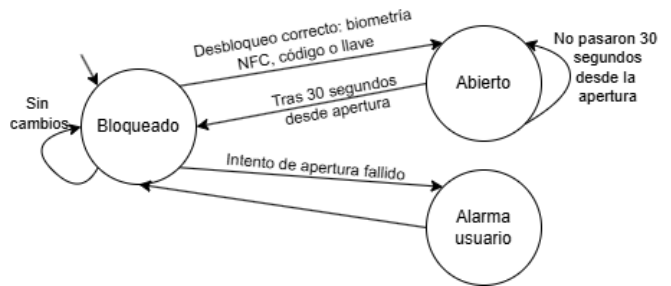


Ilustración 8. Diagrama de estados de la cerradura inteligente

6.4.5 Termostato

Este sistema permanece apagado hasta que el usuario lo active manualmente o hasta que detecta una temperatura anómala. Si la temperatura alcanza un valor definido, se quedará en modo espera hasta que el usuario lo apague o hasta que la temperatura no sea la deseada, volviendo al estado activo. Por otra parte, si el sistema detecta una ventana abierta en la zona, se pausará la climatización en dicha zona hasta que se cierre la ventana o hasta que el usuario apague el termostato.

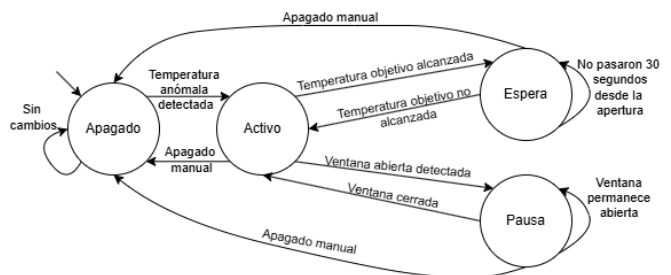


Ilustración 9. Diagrama de estados del termostato

6.4.6 Ventanas, persianas y válvula de agua

Estos sistemas permanecerán cerrados hasta que algún sensor emita una señal para abrirlos o el usuario lo indique. Permanecen abiertos hasta que el sistema reciba otra señal para cerrarlos o el usuario envíe la orden.

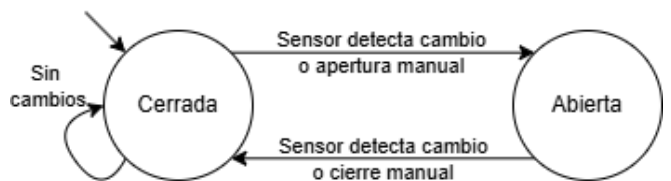


Ilustración 10. Diagrama de estados de ventanas, persianas y válvula de agua

6.5 Almacenamiento y gestión de la información

En una vivienda inteligente se generan datos constantemente: cada apertura de puerta, cambio de temperatura o lectura de sensor. Por ello, he estructurado la gestión de la información en capa física y lógica.

6.5.1 Capa física (Hardware)

Como se definió en la arquitectura del nodo central, el sistema operativo y las bases de datos residen en una unidad SSD NVMe conectada vía PCIe. He elegido este medio debido a que las tarjetas microSD sufren una degradación más rápida por las constantes operaciones de lectura y escritura. En cambio, el almacenamiento NVMe asegura la integridad de datos a largo plazo.

6.5.2 Capa lógica (Base de datos)

El componente de Home Assistant que se encarga de guardar los

datos, eventos y estados que generan los dispositivos inteligentes en una base de datos se denomina Recorder[27]. Para tener un sistema eficiente, el almacenamiento se divide conceptualmente en dos partes:

1. **Base de datos operacional:** el motor predeterminado es SQLite. Almacena los estados recientes de todos los dispositivos conectados y registra los eventos de automatización. Se utiliza principalmente para la toma de decisiones en tiempo real y visualización en pantallas táctiles.
2. **Base de datos de series temporales:** se utilizará para almacenar grandes volúmenes de datos para hacer análisis a largo plazo, como el consumo de los electrodomésticos o los niveles de CO₂. Se integrará con InfluxDB[28] para evitar que la base de datos principal ralentice el sistema.

6.5.3 Ciclo de vida de los datos

Tanto para que el sistema no se sature y para mantener la seguridad de la información, la gestión de la información tendrá un ciclo de vida cerrado[29]. El soporte de almacenamiento se ha calculado para conservar los datos históricos durante 1 año permitiendo analizar tendencias de consumo y eficiencia. El flujo de los datos se estructura en cuatro fases bien definidas.

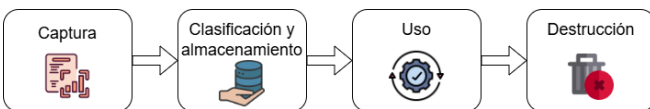


Ilustración 11. Ciclo de vida de los datos del sistema

1. **Captura:** los sensores recolectan información continuamente. Estos datos se envían de forma asíncrona hacia el nodo central.
2. **Clasificación y almacenamiento:** al recibir la información, el componente Recorder aplica un filtro usando YAML y descarta los valores que no aportan un valor analítico útil (ej. datos repetitivos del sensor de presencia, el porcentaje de batería que envían algunos sensores Zigbee) y selecciona solo métricas de valor (alertas, temperaturas, etc) y estos datos se escriben en la base de datos del SSD.
3. **Uso:** la información almacenada se utiliza para ejecutar acciones locales inmediatas, como cortar el agua ante una fuga, y para generar gráficos de consumo y uso en la interfaz de usuario.
4. **Destrucción:** para evitar que el rendimiento se reduzca debido al crecimiento de la base de datos, los datos que no estén incluidos en la ventana de retención son eliminados durante las horas de menor actividad de la vivienda. De esta forma, eliminamos los patrones de hábito antiguos del usuario.

6.6 Interfaz de usuario

La interfaz de usuario representa la capa de interacción entre el sistema y los habitantes de la vivienda o los invitados. Al tener todo el sistema localmente, se garantizará una respuesta visual con una latencia mínima, en comparación a soluciones basadas en la nube.

La interfaz se desarrollará con el propio Home Assistant, utilizando la librería de diseño modular Mushroom Cards[30], la cual permite crear un entorno visual minimalista y optimizado para lo que queremos ver. En el **anexo 5** se muestra un ejemplo

de la interfaz de usuario que se podría ver en las pantallas táctiles. Los íconos cambian de color y estado según los botones activados, proporcionando *feedback* visual.

Las pantallas táctiles estarán destinadas exclusivamente a la gestión del hogar, por lo que tendrán bloqueadas cualquier otra actividad. Estos dispositivos están integrados en la VLAN 20 y están conectados a la alimentación.

Es importante definir perfiles de acceso para cada tipo de usuario. Home Assistant permite la creación de perfiles y modificar las vistas de cada perfil. De esta manera, una persona que se encuentre en una habitación solamente podrá interactuar con los dispositivos de esa habitación. Además, los perfiles de invitados solo podrán controlar la iluminación y la climatización. En contraste, el *dashboard* de los habitantes incluirá todos los dispositivos del hogar.

6.7 Casos de uso: modos de gestión

Los casos de uso describen los escenarios de interacción del sistema mediante la ejecución de escenas. La ejecución de estos modos demuestra la capacidad del nodo central como orquestador para coordinar varios dispositivos simultáneamente, y especifican los actores que intervienen en cada uno de ellos. En el **anexo 6** se adjunta una imagen con los casos de uso detallados.

6.8. Key Performance Indicators (KPI)

Para evaluar la viabilidad de la arquitectura Edge Computing, he definido tres Indicadores Clave de Rendimiento (KPI). Estas métricas permiten demostrar empíricamente la eficiencia del diseño.

6.8.1 Latencia de eventos End-to-End

El objetivo es conseguir un tiempo de respuesta inferior a 150 ms para los dispositivos inteligentes, en especial para los más críticos como los sensores ambientales[31]. La forma de verificarlo sería analizando el archivo log de Home Assistant y calcular la diferencia de tiempo entre la marca de tiempo (timestamp) de entrada del evento (ej. cambio de estado de sensor) y el timestamp de salida del actuador (ej. encendido de luz).

6.8.2 Disponibilidad y autonomía

El objetivo es conseguir la disponibilidad de cinco noes (99,999%) en las funciones locales esenciales durante fallos de conectividad a Internet[32], lo que implicaría que como máximo, el sistema no estaría disponible durante 25,92 segundos cada mes. En la realidad, esto es muy complicado de conseguir, ya que con las redes IoT podemos tener muchas interferencias. El método de demostración de la disponibilidad consiste en realizar pruebas de estrés desconectando la red durante varias horas y comprobando que los dispositivos locales siguen funcionando correctamente y sin tiempos de espera.

6.8.3 Concurrencia del nodo central

El objetivo de este indicador es evaluar la capacidad del nodo central de adaptarse a los picos de demanda antes de comprometer el correcto funcionamiento. En vez de estimar un rendimiento ideal, establezco los siguientes límites máximos tolerables bajo condiciones de estrés:

- **Uso de CPU:** se considerará eficiente siempre que no supere el umbral del 85% durante la máxima concurrencia. Puede haber picos transitorios temporales que no se prolonguen

más de unos segundos.

- **Uso de RAM:** se considerará eficiente si se mantiene por debajo del 80% de uso de la capacidad total (12.8 GB). Esto asegura que el sistema no tenga que recurrir al uso de memoria de intercambio (*swap*) en el SSD.
- **Disipación térmica:** la temperatura del procesador debe estabilizarse por debajo de los 65°C durante instantes de alta demanda, ya que la Raspberry Pi 5 entra en modo de protección al superar los 80°C debido al *thermal throttling* (estrangulamiento térmico)[33].

Para validar estos puntos, se activará el “Modo fiesta” presentado en los casos de uso y se **simulará el tráfico de 30 usuarios** en la red de invitados (VLAN 40). Además, se ejecutarán peticiones concurrentes desde todas las pantallas táctiles. Los datos de uso se extraerán numéricamente utilizando System Monitor, que es una integración de Home Assistant para monitorear el rendimiento.

7 RESULTADOS: SIMULACIÓN DEL SENSOR DE PRESENCIA

A modo de evaluar la viabilidad práctica de la solución diseñada, he desarrollado un prototipo del sensor de presencia que, cuando detecta movimiento, enciende un LED azul en el microcontrolador y envía un mensaje al usuario a través de un bot de Telegram.

7.1. Material

A continuación, presento los materiales físicos y lógicos utilizados para el desarrollo de este sistema:

- 1 placa ESP32 WROOM-32 con conectividad Wi-Fi integrada y un LED azul.
- 1 sensor infrarrojo pasivo (PIR) HC-SR501, que detecta movimiento midiendo la radiación (calor) de los cuerpos.
- 3 cables dupont hembra-hembra
- Virtual Box para crear una máquina virtual
- Home Assistant OS

7.2. Implementación

El primer paso ha sido crear una máquina virtual en Virtual Box y utilizar como disco de arranque el proporcionado por la web oficial de Home Assistant. Una vez iniciada, desde un navegador local he accedido al panel de administración de Home Assistant, donde inicialmente he creado una cuenta de administrador.

Luego, he instalado los complementos Telegram Bot y ESPHome en la tienda, siendo este último para poder comunicar la placa que tiene el sensor con la máquina virtual. Después de instalar el complemento, he añadido como un nuevo dispositivo la placa ESP32, le he asignado el nombre “sensor-movimiento” y he añadido el ssid y la contraseña de la red a la que se va a conectar, que debe ser la misma que la que utiliza la máquina virtual.

Una vez añadido el dispositivo, lo siguiente que hice fue configurar los pines para poder indicarle a Home Assistant la entrada de datos del sensor y la salida hacia el LED azul. En el anexo 7 muestro la conexión del sensor de movimiento con la placa, y en el anexo 8 adjunto el código YAML utilizado para esta configuración. Después de añadir estos ajustes, Home Assistant ha creado un ejecutable para descargar e instalar en la placa, por lo que la he conectado por USB al ordenador y la he instalado.

Por último, he creado las automatizaciones para hacer que cuando el sistema reciba una señal del sensor de movimiento, se

conmute el estado del LED azul y se envíe un mensaje a un bot de Telegram previamente creado.

7.3. Comportamiento

La lógica replica un comportamiento asíncrono y una estructura de interrupciones. Durante las pruebas se han obtenidos los siguientes resultados:

- **Detección:** al pasar la mano por delante del sensor, este conmuta su estado de 0 a 1 (high), y este dato binario lo envía el ESP32 a través de Wi-Fi a la máquina con Home Assistant.
- **Automatizaciones:** cuando el sistema recibe un 1 del dispositivo “sensor-movimiento”, en aproximadamente 200 ms envía a través de Wi-Fi una señal a la placa ESP32 para encender el LED azul y también envía un mensaje al bot de Telegram establecido durante la configuración de la automatización.
- **Tolerancia:** el sistema mantiene el LED encendido mientras sigue detectando movimiento. Cuando deja de detectar movimiento, la luz se apaga.

Este resultado demuestra que el modelo es altamente fiable. El acoplamiento físico entre sensores y actuadores controlados por un nodo local garantiza una velocidad de respuesta óptima. Cabe resaltar que esto es un prototipo para simular físicamente la implementación de la alarma por movimiento, ya que en este ejemplo utilicé el protocolo Wi-Fi en lugar de Zigbee, y en un entorno real no sería buena idea alertar al intruso con la luz LED, sino que el sistema solo nos enviaría un aviso. A continuación, se muestra una imagen del LED azul encendido al acercar la mano y otra imagen con el mensaje recibido en Telegram.

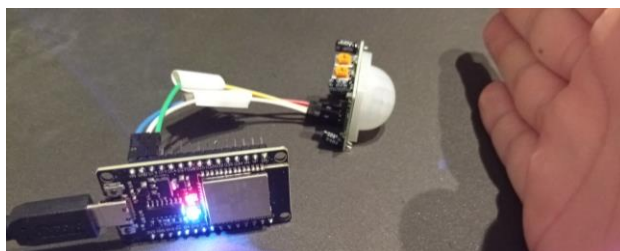


Ilustración 12. Comprobación del LED azul indicando detección



Ilustración 13. Comprobación del mensaje en Telegram

8 CONCLUSIONES Y TRABAJO FUTURO

La realización de este Trabajo de Fin de Grado me ha permitido analizar la viabilidad técnica y operativa de una arquitectura domótica basada en Edge Computing para el control integral de una vivienda inteligente. A lo largo de la investigación y el diseño de la solución, he cumplido con el objetivo de unificar bajo un ecosistema local el control de la iluminación, climatización, seguridad ambiental, seguridad perimetral y electrodomésticos comunes. Se ha demostrado que, aunque esta solución requiere más tiempo de configuración, es factible evitar la dependencia de

las infraestructuras en la nube, garantizando tiempos de respuesta más bajos e interoperabilidad entre fabricantes gracias al estándar Matter y a la plataforma Home Assistant OS.

Desde la perspectiva de la mención de Ingeniería de Computadores, la principal aportación de este proyecto está en la optimización de la infraestructura física y lógica de los sistemas propuestos. La selección del hardware óptimo sirve para contar con disponibilidad, durabilidad y alto rendimiento a lo largo del tiempo. La implementación de un ciclo de vida cerrado para los datos y la segmentación de la red mediante la técnica de subnetting protegen el sistema ante amenazas cibernéticas y permiten seguir el principio de Privacy by Design. Además, los indicadores de rendimiento evaluados aseguran que la experiencia del usuario sea satisfactoria y que el sistema funcione de manera predecible bajo ciertos escenarios.

A pesar de que la arquitectura propuesta sea robusta, la tecnología se encuentra en constante evolución en el ámbito del IoT, lo que abre un abanico de posibilidades para expandir este proyecto. Un primer punto a tratar en el futuro sería la integración de modelos de inteligencia artificial y Machine Learning, ejecutados de forma nativa en el nodo central. Esta característica permitiría acercar el proyecto hacia una casa "cognitiva", permitiendo al sistema predecir fallos, necesidades y rutinas, tal como se explicó en el estado del arte. Así mismo, eventualmente aparecerán en el mercado dispositivos con Matter-over-Thread nativo, sustituyendo a los nodos Zigbee 3.0, lo cual simplificará la topología física de la red al trabajar bajo una misma red unificada.

USO DE LA IA GENERATIVA

El uso de la inteligencia artificial se ha limitado a:

- Consultas sobre detalles técnicos de los protocolos de comunicación
- Mejoras en la redacción del informe
- Mejoras en la calidad de algunas imágenes
- Consultas sobre detalles técnicos de KPIs en domótica
- Consultas sobre errores al descargar código en la placa ESP32

AGRADECIMIENTOS

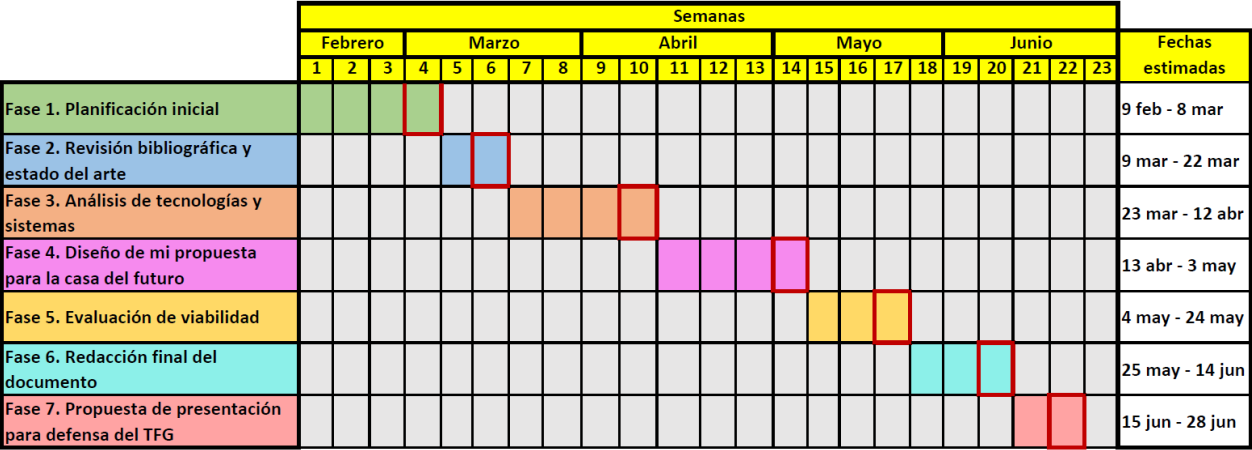
Quiero agradecer al profesorado de la UAB por todas las enseñanzas a lo largo de los años de estudio. También a mi tutor Jordi Castilla por ayudarme a enfocar este último trabajo de la carrera y aconsejarme para mejorarlo continuamente. Por último, a mis padres y a mi pareja, que confiaron en mí desde el primer momento, incluso en los momentos en los que yo no confiaba en mí mismo.

BIBLIOGRAFIA

- [1] Smart Home Based on IoT - Architecture and Practices. Disponible: <https://ieeexplore.ieee.org/document/10156739>
- [2] Domótica, Casas inteligentes. Disponible: <https://www.hogar-sense.es/domotica/casa-inteligente>
- [3] Introducción a la domótica. Disponible: <https://sites.google.com/site/ejldcdomotica/Home/tema-1-introduccion-a-la-domotica>
- [4] La sinfonía de la domótica y la climatización: El futuro de los hogares inteligentes. Disponible: <https://www.daikin.es/es-es/hogar/notas-de-prensa/2024/nota-de-prensa-485-climatizacion-domotica.html>
- [5] Smart Buildings y domótica. Disponible: <https://www.fundaciondesa.org/es/educacion/endsa-educar/recursos/smart-building-casa-domotica>
- [6] Vaishnavi S. Gunge, Pratibha S. Yalagi, Smart Home Automation: A Literature Review, RTDM 2016. Disponible: <https://research.jica-online.org/rtdm2016/number1/rtdm2568.pdf>
- [7] Daiva Stanelytė, Birutė Rataitė, Algimantas Andriūsis, Aleksas Narščius, Gintaras Kučinskas and Jelena Dikun, Development of a Solution for Smart Home Management System Selection Based on User Needs, 2025. Disponible: <https://www.mdpi.com/2571-5577/8/5/139>
- [8] Carles Gomez, Josep Paradell, Wireless Home Automation Networks: A Survey of Architectures and Technologies. Disponible: <https://rob-ertdick.org/esaca/papers/gomez-home-automation.pdf>
- [9] Thread Network Fundamentals. Disponible: https://www.threadgroup.org/Portals/0/documents/support/Thread%20Network%20Fundamentals_v3.pdf
- [10] Millimeter-wave radar for intelligent sensing: A comprehensive review of techniques, applications, and challenges. Disponible: <https://www.sciencedirect.com/science/article/pii/S0045790625006391>
- [11] IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Disponible: <https://www.sciencedirect.com/science/article/pii/S2542660518300477>
- [12] IoT and Privacy by Design in the Smart Home. Disponible: https://web-assets.esetstatic.com/wls/en/papers/re-sources/ESET_MWC2018_IoT_SmartHome.pdf
- [13] Edge Computing For Smart Home Devices. Disponible: <https://course.ece.cmu.edu/~ece500/projects/s20-teama6/wp-content/uploads/sites/80/2020/05/Final-Report.pdf>
- [14] The Raspberry Pi 5 is the best Home Assistant hub you can get for cheap. Disponible: <https://www.xda-developers.com/raspberry-pi-5-best-home-assistant-hub-cheap/>
- [15] Estudio y desarrollo de sistema domótico para vivienda privada con Home Assistant. Disponible: https://oa.upm.es/74970/1/TFM_ENRIQUE_REBOLLO_GON-ZALEZ.pdf
- [16] IoT-Based Indoor Air Quality Management System for Intelligent Education Environments. Disponible: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10877861>
- [17] Smart Thermostats for Home Automation Systems and Energy Savings from Smart Thermostats. Disponible: <https://ieeexplore.ieee.org/document/8751790>
- [18] Indoor Personnel Detection Method Based on Millimeter-Wave Radar. Disponible: <https://dl.acm.org/doi/10.1145/3718491.3718620>
- [19] A secure authentication scheme for smart home environments: a biometric-driven approach. Disponible: <https://www.researchgate.net/publication/401322729>
- [20] IoT-Enabled Smart Window System for Environmental Adaptation in Home 4.0. Disponible: <https://ieeexplore.ieee.org/document/11172091>
- [21] A review of Internet of Things for smart home: Challenges and solutions. Disponible: <https://www.sciencedirect.com/science/article/pii/S095965261631589X>
- [22] Planifica tu red local doméstica para instalar dispositivos de domótica. Disponible: <https://www.redeszone.net/tutoriales/domotica/planificacion-red-local-domotica-casa/>
- [23] ¿Qué es Wi-Fi 6? Disponible: <https://www.monolithic.com/cual-es-la-mejor-tecnologia-wifi-para-desarrollos-iot/>
- [24] Comparative Analysis of Mesh and Thread Networks and their Application Possibility in the "Smart Home" Systems. Disponible: <https://ieeexplore.ieee.org/document/9396680>
- [25] Wireguard. Fast, modern, secure VPN Tunnel. Disponible: <https://www.wireguard.com/>
- [26] How State Machine Diagrams Are Evolving in Next-Gen IoT Architecture. Disponible: <https://www.archimetric.com/future-outlook-state-machine-diagrams-next-gen-iot-architecture/>
- [27] Home Assistant Recorder. Disponible: <https://www.home-assistant.io/integrations/recorder/>
- [28] Home Assistant InfluxDB. Disponible: <https://www.home-assistant.io/integrations/influxdb/>
- [29] Data Lifecycle Management: A Simple and Complete Explanation. Disponible: <https://www.cicdata.com/blog/complete-guide-data-lifecycle-management/>
- [30] Mushroom Cards para Home Assistant. Disponible: <https://ayudadomotica.com/mushroom-cards-home-assistant-guia/>
- [31] IoT Latency: The Power of Real-Time Communication. Disponible: <https://www.nabto.com/iot-latency-the-power-of-real-time-communication/>
- [32] High Availability Architecture: Requirements & Best Practices. Disponible: <https://www.couchbase.com/blog/high-availability-architecture/>
- [33] Heating and Cooling Raspberry. Disponible: <https://www.raspberrypi.com/news/heating-and-cooling-raspberry-pi-5/>

ANEXOS

Anexo 1. Diagrama de Gantt del proyecto



 Semana límite

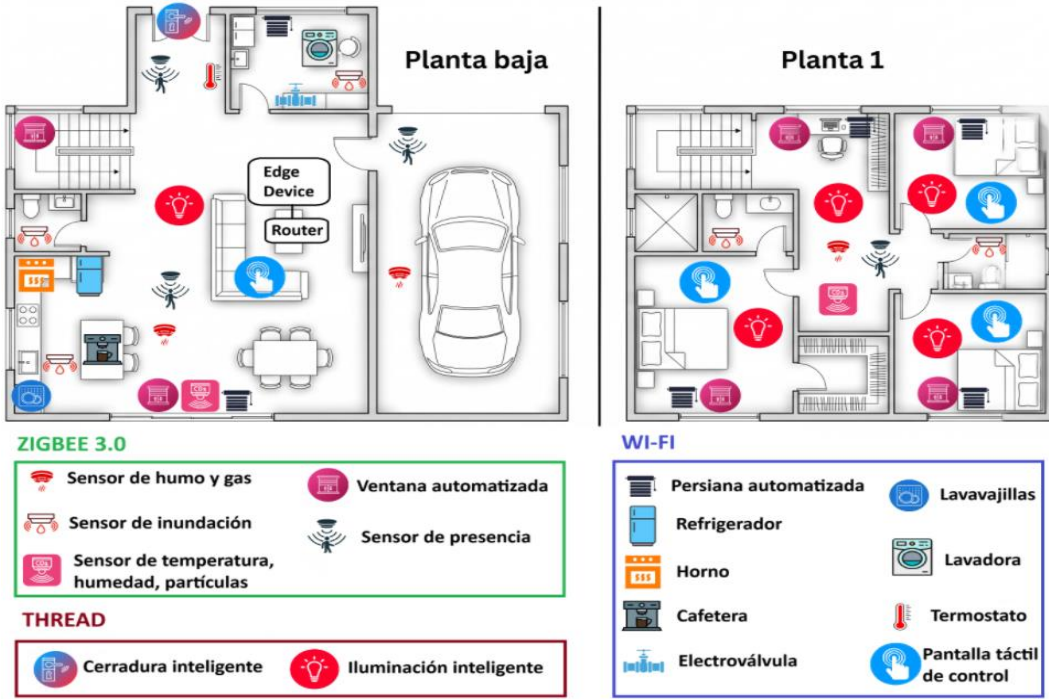
Anexo 2. Raspberry Pi 5



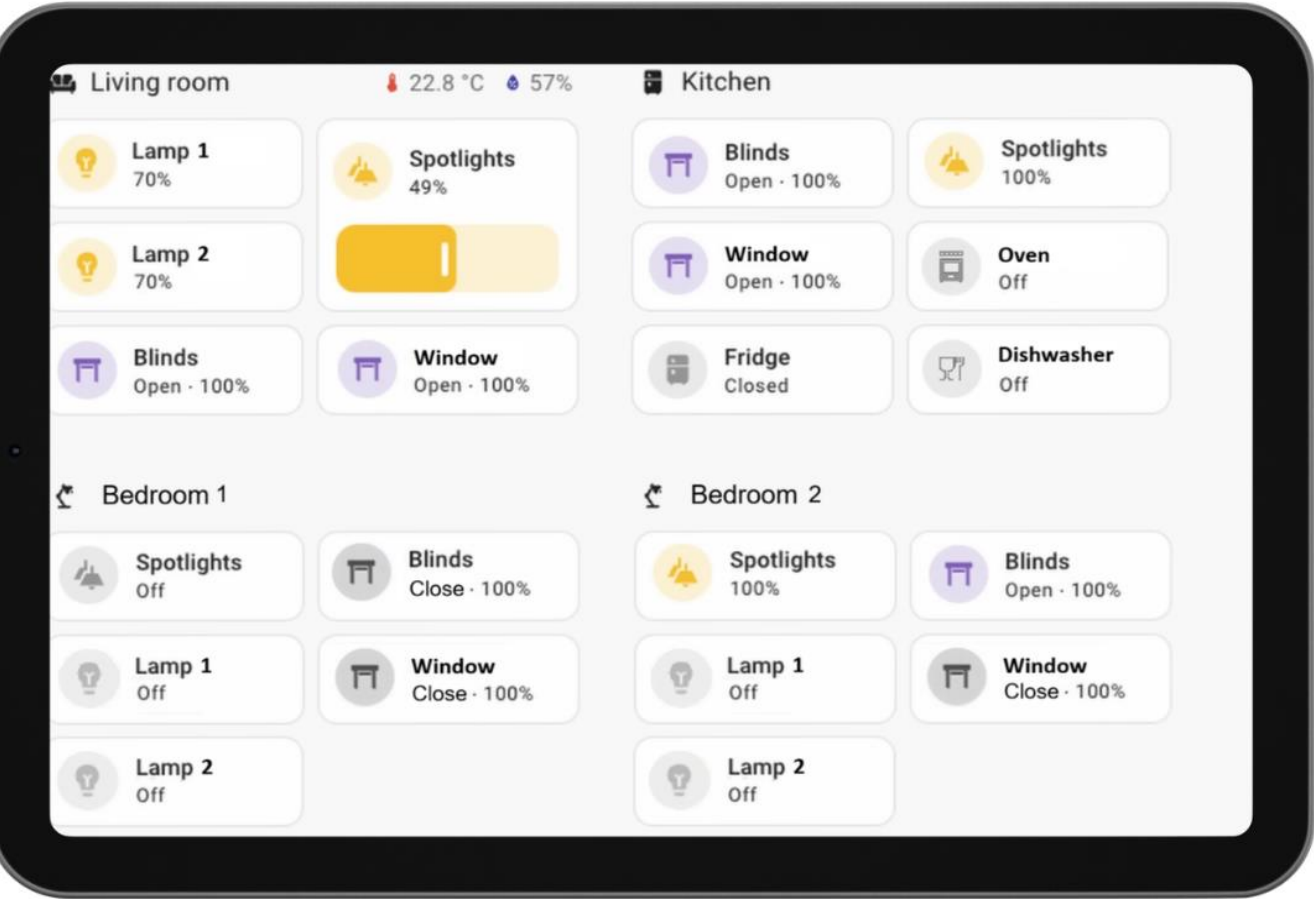
Anexo 3. Adaptador de radio zigbee y thread



Anexo 4. Plano de las plantas de la casa



Anexo 5. Mockup de las pantallas táctiles de control local



Anexo 6. Casos de uso

Modo noche

Este escenario se activa durante las horas de descanso (23:00 - 7:00), siempre que los habitantes se encuentren en el hogar.

Los actores involucrados son los residentes.

Se comprueba que la cerradura inteligente esté bloqueada. Se cierran todas las ventanas y persianas. Se ajusta la temperatura de las habitaciones ocupadas. Se apagan todas las luces.

Si durante la noche el sensor de presencia detecta movimiento en el pasillo, activa una iluminación tenue en esa zona.

Modo vacaciones

Este escenario se activa para proteger la vivienda cuando los habitantes están ausentes durante largos periodos.

El actor es el usuario que activa el modo.

Se comprueba que la cerradura inteligente, la válvula de agua, las ventanas y las persianas estén cerradas. Los sensores de presencia continúan activos para avisar de intrusiones.

Se ejecutan simulaciones de presencia dinámica, utilizando los datos históricos almacenados para replicar hábitos de iluminación y persianas, para disuadir a posibles delincuentes.

Modo despertar

Este caso gestiona la transición del modo nocturno hacia las rutinas matutinas de los residentes (a partir de las 7:00).

Los actores son los residentes.

Cuando este modo se activa, se encienden las luces de la habitación ocupada de manera progresiva para no molestar al usuario. Al cabo de 15 minutos, se apagan las luces y se abren las persianas.

Se enciende la cafetera y se prepara el café para el usuario.

Modo confort

Este modo consiste en la preparación del hogar antes de la llegada de los habitantes.

Los actores son los smartphone de los residentes.

Este modo se activa cuando el dispositivo móvil del usuario cruza un radio geográfico preconfigurado, el cuyo caso se activa el termostato para conseguir una temperatura óptima en el momento de la llegada.

Si es de noche, las luces del pasillo de entrada se encienden automáticamente al abrir la cerradura inteligente.

Modo evento social

Este modo está optimizado para la recepción de visitas, de manera que los invitados puedan realizar algunas gestiones.

Los actores son los invitados.

Cuando se activa el modo, se pausan los sensores de presencia para evitar transiciones constantes de luz. Las pantallas táctiles de control cambian a una interfaz de invitados, con funciones limitadas a iluminación, climatización y multimedia.

Opcionalmente se puede dejar desbloqueada la cerradura inteligente durante el evento.

Modo ventilación

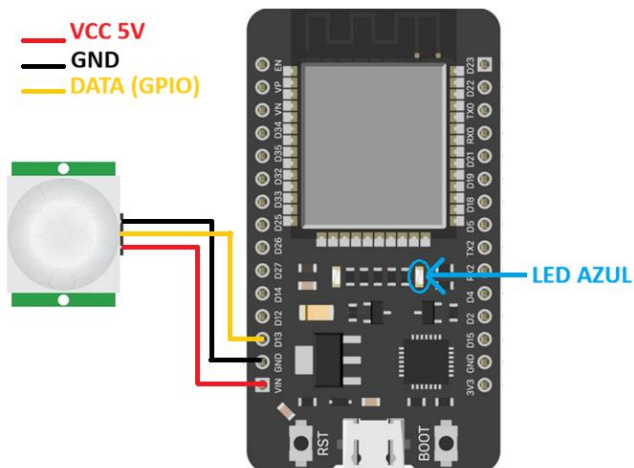
Este modo se activa cuando los sensores de humo o gas detectan anomalías críticas.

Los actores son las ventanas y persianas.

Cuando se activa el modo, automáticamente se abren las ventanas y persianas para ventilar el hogar. En caso de que el usuario se encuentre en la vivienda, se desbloquea la cerradura inteligente para facilitar la salida.

Además de enviar una alerta al usuario, las luces del hogar se encienden y empiezan a parpadear como alerta de que algo está ocurriendo.

Anexo 7. Esquema de conexiones placa ESP32



Anexo 8. Código YAML para configurar pines

```
# Configuración del sensor de movimiento físico en el pin 13
binary_sensor:
  - platform: gpio
    pin: GPIO13
    name: "Movimiento Pasillo TFG"
    device_class: motion

# Configuración del LED azul integrado de la placa en el pin 2
output:
  - platform: ledc
    pin: GPIO2
    id: led_azul

# Entidad visual vinculada al led_azul
light:
  - platform: binary
    name: "LED Alerta"
    output: led_azul
```