FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN

Propuesta Tecnológica, previa a la obtención de Titulo de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

“Implementación de un modelo inteligente con protocolos de comunicación z-wave para el monitoreo y la gestión de zonas seguras.”

AUTOR

Parrales Merino Carlos Alejandro

PROFESOR TUTOR

Ing. Luis Amaya Fariño, Mgt.

LA LIBERTAD – ECUADOR

2024

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de titulación denominado: “Implementación de un modelo inteligente con protocolos de comunicación z-wave y onvif para el monitoreo y la gestión de zonas seguras.” Elaborado por el estudiante **Carlos Alejandro Parrales Merino,** de la carrera de Electrónica y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo a el estudiante para que inicie los trámites legales correspondientes.

La Libertad, ___de _____del 2023

LUIS MIGUEL AMAYA FARINO

Digitally signed by LUIS MIGUEL AMAYA FARINO
Date: 2024.04.11 15:55:18 -05'00'

Ing. Luis Amaya Fariño, Mgtr.

TUTOR

DEDICATORIA.

El presente trabajo de titulación se la dedico a mis padres, mi abuelita, mi tío y mis amistades, ya que ellas fueron un pilar fundamental en mi proceso universitario, brindándome apoyo tanta emocional como económico para poder cumplir con esta etapa en mi vida.

A mi tío Fernando Merino que me llenó de sus consejos cuando la vida universitaria me presentaba un completo problema y debido a eso pude culminar mis estudios.

A mi abuelita que estuvo apoyándome para poder verme como un profesional, ella tanto lo quería y lo logré.

A mi mamá, papá y hermano que a pesar de las diferencias que teníamos me ayudaron y se preocuparon siempre por mí.

Carlos Parrales Merino.

AGRADECIMIENTO.

Agradezco a Dios, mis padres, familiares y amigos por darme la oportunidad de experimentar esta etapa universitaria de la mejor manera.

A Dios por darme vida y oportunidad de experimentar cosas increíbles en cuanto a amistades y aprendizaje respecta en la universidad.

A mis padres les doy gracias por apoyarme económica y emocionalmente en esta etapa.

A mis familiares, mi tío y mi abuelita, gracias por apoyarme con sus consejos de vida, debido a los mismos pude culminar con mi carrera universitaria.

Carlos Parrales Merino.

TRIBUNAL DE GRADO

Firmado electrónicamente por:
WASHINGTON DANIEL TORRES GUIN

Ing. Washington Torres Guin, Mgtr.

Decano de la Facultad

Firmado electrónicamente por:
JOSE MIGUEL SANCHEZ AQUINO

Ing. José Sánchez Aquino, Mgtr.

Director de la Carrera

DANIEL ARMANDO JARAMILLO CHAMBA
Firmado digitalmente por DANIEL ARMANDO JARAMILLO CHAMBA

Ing. Daniel Jaramillo Chamba, Mgtr.

Docente de Área

LUIS MIGUEL AMAYA FARINO
Digitally signed by LUIS MIGUEL AMAYA FARINO
Date: 2024.04.11 15:55:36 -05'00'

Ing. Luis Amaya Fariño, Mgtr.

Docente Tutor

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Ab. María Rivera González, Mgtr.

Secretaria General.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA ELECTRÓNICA Y TELECOMUNICACIONES

“Implementación de un modelo inteligente con protocolos de comunicación z-wave para el monitoreo y la gestión de zonas seguras.”

Autor: **CARLOS PARRALES MERINO**

Tutor: **LUIS AMAYA FARIÑO**

RESUMEN

El presente trabajo de titulación propone desarrollar e implementar un modelo inteligente para monitoreo y gestión en el edificio del Instituto de Investigación y Desarrollo Tecnológico perteneciente a la Universidad Estatal Península de Santa Elena, con el fin de mejorar la seguridad y dar un avance tecnológico en cuanto a esta se refiere.

La etapa de implementación cuenta con dispositivos para monitorear y gestionar diferentes puntos en el edificio, esto es para garantizar una mayor seguridad en cuanto a los equipos que se encuentran en dicha zona, gestionando puntos como luz, movimiento, temperatura, entre otros.

La estructura del modelo inteligente de la implementación está conformada por la etapa en la cual hacemos uso de sensores y controladores. Estas etapas ayudarán a recopilar datos, enviarlos para su gestión y finalmente realizar acciones pertinentes si se presenta anomalía alguna.

El diseño se lo realizó en la plataforma Sketchup para poder ubicar de manera correcta y estratégica los equipos a utilizar, cabe recalcar que gracias a este software podemos crear la infraestructura de la zona segura con las medidas reales,

analizando de la mejor manera las falencias o puntos débiles que tiene esta edificación.

PALABRAS CLAVES: Z-wave, home Assistant, onvif, Monitoreo, Controlador, Raspberry.

ABSTRACT

This degree work proposes to develop and implement an intelligent model for monitoring and management in the building of the Institute for Research and Technological Development belonging to the Peninsula Santa Elena State University, in order to improve security and give a technological advance in this regard.

The implementation stage has devices to monitor and manage different points in the building, this is to ensure greater security in terms of equipment that are in that area, managing points such as light, movement, temperature, among others.

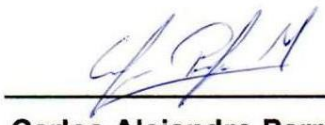
The structure of the intelligent model of the implementation is made up of the stage in which we make use of sensors and controllers. These stages will help to collect data, send them for management and finally take appropriate actions if any anomaly occurs.

The design was made on the Sketchup platform to be able to locate correctly and strategically the equipment to be used, it should be noted that thanks to this software we can create the infrastructure of the safe zone with the real measures, analyzing in the best way the shortcomings or weak points that this building has.

KEYWORDS: Z-wave, Home Assistant, Onvif, Monitoring, Controller, Raspberry.

DECLARACIÓN

El contenido del presente Trabajo de Titulación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de santa Elena.



Carlos Alejandro Parrales Merino

AUTOR

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

ÍNDICE DE ABREVIATURAS

ABREVIATURA	SIGNIFICADO
PTP	Punto a Punto
PTMP	Punto a multipunto
INCYT	Instituto de investigación científica y desarrollo de tecnologías
Iot	Internet de las cosas
SD	Secure digital
POE	Power over ethernet
GPIO	General Purpose Input/Outpu
API	Interfaz de programación de aplicaciones
DBM	Decibelio-milivatio
MA	Mili amperios
V	Voltios
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

HA	Home Assistant
ONVIF	Interface abierta de red de video
DNS	Domain name system
UPNP	Universal plug and play
UUID	Identificador Único Universal

INTRODUCCIÓN

El presente proyecto se planteó como un trabajo práctico orientado a la seguridad de una zona segura perteneciente a la Universidad Estatal Península de Santa Elena con la finalidad de mantener una gestión y monitoreo de los equipos que se encuentran en dicha zona segura, es decir, gestionar factores como videovigilancia, luz, temperatura, movimientos y diversos fenómenos que suceden dentro del edificio.

Este proyecto se implementó con éxito generando diversas opciones a futuro, ya que el sistema quedó totalmente funcional y su configuración es amigable con el usuario, entre las opciones, tenemos que se pueden añadir más dispositivos no solo z wave, sino también robóticos, tales como, sensores (humedad, movimiento, temperatura, etc.), alarmas, cámaras de seguridad, interruptores automáticos, entre otros. La implementación del presente proyecto es el inicio para poder generar un edificio totalmente automatizado y por ende seguro, ya que se controlan de manera remota y con mayor seguridad.

En el capítulo I de la propuesta se habla sobre las generalidades del tema, la problemática existente para la elaboración del presente proyecto, su justificación, su impacto, entre otros. Se mencionan objetivos a cumplir, resultados obtenidos y esperados una vez que finalice la implementación de esta propuesta.

En el capítulo II detalla los elementos y dispositivos utilizados para poder realizar con éxito la gestión y monitoreo de equipos, haciendo referencia a los conceptos generalizados para una mejor implementación. Se trabaja en base a objetivos específicos para poder utilizar equipos, software y herramientas adecuadas para la correcta implementación de esta propuesta.

En el capítulo III se detalla paso a paso la configuración y vinculación de elementos utilizados, adicionalmente la creación y colocación de los materiales que fueron necesarios para colocar el servidor de manera física.

Por último, en el capítulo IV se muestra el funcionamiento del sistema adjuntando datos tomados por los sensores, capturas de las cámaras y la hora en las que sucedió alguna anomalía.

Una vez finalizada dicha explicación se mostrarán pruebas de funcionamiento como mediciones de temperatura, sensores en puertas y ventanas, sensores de movimiento y gestión de los mismos datos tomados para efectuar alguna acción si se presentan anomalías.

.

CAPÍTULO I

GENERALIDADES DE LA PROPUESTA

1.1 ANTECEDENTES

En la actualidad la tecnología juega un papel fundamental en el desarrollo de la vida estudiantil, como diaria. Diversos avances han facilitado el aprendizaje y trabajo de las personas. Cuando se habla de tecnología, hacemos referencia a progreso en diferentes ámbitos de la vida cotidiana, entre los principales esta la seguridad y las telecomunicaciones.

Las telecomunicaciones evolucionan junto a la tecnología, en este caso, hacemos uso del protocolo z-wave que se desarrolló para aplicaciones domóticas, el cual viene de la mano con el monitoreo y gestión. Otro factor relevante en cuanto a protocolos de comunicación y monitoreo hablamos es el protocolo onvif, dicho protocolo es el utilizado en cámaras IP para poder generar una compatibilidad con las diferentes plataformas de video.

A nivel mundial, tenemos a Países Bajos como principal potencia en cuanto a laboratorios y edificios inteligentes se trata, el nombre del edificio es “The Edge”, cuenta con más de 28.000 sensores lo cual facilita el día a día en la oficina de todo el equipo, ya que pueden monitorear y controlar datos como luz, humedad, luminosidad, entre otras. (Integra, Nexus, 2022)

La implementación de nuevas tecnologías es muy importante en este país ya que ayuda a optimizar el tiempo de investigaciones, da una mayor seguridad y ayuda a una mejor colaboración. Las telecomunicaciones se han venido beneficiando de los avances tecnológicos, ya que las mismas ocupan un lugar en el espectro radioeléctrico, debido a esto la contraparte es que se generan saturaciones en las bandas utilizadas. Una ventaja de utilizar protocolos de comunicación como el Z-WAVE es que el mismo trabaja en diferente frecuencia a los equipos inalámbricos monótonos.

En el caso de la implementación realizada se utilizó el protocolo ONVIF y el protocoló Z-Wave, ya que gracias a ellos la información que podemos enviar se hace de manera más eficiente, ya que la banda a trabajar esta menos saturada en las instalaciones, adicionalmente podemos agregar muchos más dispositivos que se encuentren de manera sencilla en el mercado, los elementos utilizados nos ayudaron a mantener una gestión y monitoreo en tiempo real a diferentes aparatos ya sea de uso educativo o uso laboral.

En el Ecuador se han realizado varios proyectos de titulación o investigación sobre la gestión y monitoreo de diferentes zonas seguras, dado está el caso de un tema de titulación presentado en la Universidad Técnica de Ambato que es “Sistema de gestión y monitoreo para mejorar los procesos de administración de los laboratorios de las carreras de Sistemas, Electrónica e Industrial en la FISEIUTA” el cual tiene como objetivo determinar los procesos realizados en la misma para efectuar estudios y plantear propuesta para una mejoría en el área. (Mesias, 2014). Dicho proyecto utiliza varios protocolos de comunicación, entre ellos el Z-Wave, debido a que es un protocolo Wireless que no se encuentra saturado ya que trabaja en otro tipo de frecuencia del espectro radioeléctrico, lo cual beneficia a la UPSE debido a que la red 2.4 GHz se encuentra saturada debido al tráfico de datos que mantiene la universidad.

Otro proyecto que fundamenta el tema es el “Diseño y desarrollo de un laboratorio de pruebas basados en Smart Home aplicando protocolo de comunicación Z-Wave y estándar 802.11” que utiliza el monitoreo y gestión para una creación de un laboratorio de prácticas para dominica. (Moreno Serrano Camilo, 2021). Este tema se enfocó en realizar una casa inteligente y segura, con sensores, alarmas y automatizaciones, esta parte es fundamental para la edificación del INCYT, ya que no posee ningún elemento que monitoree los alrededores e incluso las instalaciones internas del mismo.

En el año 2015 se realizó un proyecto de graduación en la Escuela Superior Politécnica del Litoral titulado “DISEÑO E IMPLEMENTACIÓN DE UN

SISTEMA DOMÓTICO DE RADIOFRECUENCIA PARA BRINDAR GESTIÓN DE NETWORKING, SEGURIDAD Y CONFORT USANDO LOS PROTOCOLOS Z-WAVE Y ZIGBEE". Este tema se centró en crear una red interna que controlara más de 100 dispositivos que trabajan a una frecuencia distinta a dispositivos comunes, adicionalmente brinda una posibilidad de acceder a esta red privada de manera remota. (VELÁSQUEZ, 2015) Con estos puntos mencionados en la tesis antes expuesta, se optó por tomar ideas como el control de los dispositivos, trabajar a una frecuencia diferente para evitar tráfico de redes, crear una red privada y acceder de manera remota al control y monitoreo de los dispositivos implementados.

Un proyecto más que engloba la tecnología z wave es el proyecto de fin de carrera titulado "INTEGRACION DE TECNOLOGIA DOMOTICA Z-WAVE EN LA PLATAFORMA FIBARO", el cual se centró en la utilización de dispositivos FIBARO con la tecnología Z-WAVE, facilitando la configuración y manipulación de los dispositivos en un servidor creado. (García, 2018) De este proyecto se inspiró a utilizar dispositivos FIBARO, para poder dejar una manipulación intuitivo de dispositivos en cuanto a configuración de datos que almacena los mismos se refiere, en el caso del proyecto implementado en la UPSE, hablamos de datos como temperatura, movimiento, entre otros, con este sensor podemos manipular la sensibilidad, el horario y otros factores desde el servidor creado.

1.2 DESCRIPCIÓN DEL PROYECTO

La presente propuesta tecnológica tiene como idea principal evaluar e implementar un modelo domótico basado en un sistema z wave que trabaja bajo la normativa ITU-T G.9959 para mantener la seguridad en el edificio del Instituto de Investigación Científica y Desarrollo de tecnologías. Este proyecto se presenta en dos etapas, la primera es el diseño y simulación del modelo, la segunda etapa es la implementación.

Se realizó de manera satisfactoria la presente propuesta gracias a una simulación del lugar a trabajar. Una vez realizada la simulación de la zona segura a tratar, procedimos a crear una red interna en donde se colocó un equipo Master para poder gestionar los equipos instalados en el edificio. Al utilizar protocolos de comunicación como el Z-Wave y el Onvif trabajamos con sensores, controladores y cámaras de video vigilancia compatibles con los mismos protocolos. Entre la sección de controladores tenemos diversos, para este caso utilizamos el Raspberry PI, esto debido a que este controlador es robusto y el procesamiento de información es más alto que uno convencional, adicionalmente se implementaron dispositivos que permiten realizar la comunicación mediante protocolos asignados a los equipos.

Como se menciona anteriormente, existen una gran cantidad de marcas y modelos en cuanto equipos de procesamiento se refiere, sin embargo, se realizó una comparativa técnica y económica en cuanto al software y hardware utilizado, nos topamos con varias opciones y las mejores debido al procesamiento, velocidad y costo se refiere son en controladores “raspberry pi”, en dispositivos “sensores marca fibaro” y en software servidor “Home Assistant”.

Adicionalmente tendremos una vigilancia en lugares estratégicos del edificio, cabe recalcar que los sensores y cámaras serán enlazados utilizando protocolos antes descritos con su total compatibilidad. En el caso de los sensores, estos utilizaran el protocolo de comunicación Z-Wave y es necesario un Gateway para poder gestionar los mismos, dicha puerta de enlace se verá reflejada en el uso de un USB z-wave plus. Para la parte de la video vigilancia, contaremos con cámaras IP compatibles con el protocolo onvif, ya que dicho protocolo puede ser utilizado en el servidor “Home Assistant” que se creará tal y como mencionamos anteriormente.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Implementar un sistema domótico basado en bandas no licenciadas que monitoree y gestione en tiempo real aplicando protocolos de comunicación Z-wave para la seguridad en el edificio del Instituto de Investigación Científica y Desarrollo de Tecnologías.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analizar los puntos vulnerables del Incyt mediante un diseño digital del mismo para la aplicación de nodos seguros y tecnologías de bajo consumo inalámbrico.
- Desarrollar un sistema electrónico automatizado que monitoree y envíe información a los dispositivos domóticos implementados para la seguridad del edificio.
- Integrar tecnologías que permitan el monitoreo y gestión de redes remotas basadas en software libres desarrollando interfaces gráficas para la instalación.
- Hacer uso de los protocolos z wave para la comunicación efectiva de los dispositivos domóticos implementados con el controlador Raspberry pi 3 y el software Home Assistant.

1.4 RESULTADOS ESPERADOS

Una vez culminado el diseño y la implementación se esperan los siguientes resultados:

- Se espera identificar los puntos vulnerables que tiene el edificio y a su vez cubrirlos y vigilarlos mediante nodos instalados con las diferentes tecnologías antes mencionadas.
- Se espera mantener un monitoreo constante de las personas y equipos que se encuentran en las edificaciones del Incyt, para que, al momento de presentarse una anomalía relacionadas a la seguridad de los bienes, la persona encargada pueda tomar acciones inmediatas ante aquella situación.
- Se espera verificar que la utilización del protocolo Z-wave y el protocolo onvif son las más indicadas debido a los estándares que utiliza y de esta manera facilita y agiliza la interconexión de los sensores y las cámaras utilizadas.
- Se pretende conectar las cámaras y sensores a un mismo controlador utilizando los protocolos antes mencionados, para de esta manera mantener un control global de los mismos.

1.5 JUSTIFICACIÓN

La implementación de este modelo domótico es justificable gracias a que se realizó en base a frecuencias bajas o no licenciadas, teniendo una gran estabilidad en la transmisión y recepción de datos disminuyendo en gran cantidad los paquetes perdidos.

Otro punto a favor para la implementación del modelo es la gestión y el monitoreo que se mantiene dentro de las instalaciones del Incyt, asegurando el bienestar de los equipos que se encuentran dentro de dicha zona segura.

Existen diversos proyectos realizados en la UPSE sobre tecnologías como z wave, zigbee, domótica en general, pero ninguno de ellos han sido implementados en algún edificio o laboratorio, entre los proyectos realizados tenemos “DESARROLLO Y DISEÑO DE UN PROTOTIPO AUTOSOSTENIBLE GEOLOCALIZADO IMPLEMENTANDO UNA RED WSN PARA EL RASTREO DE CAPRINOS EN UN SECTOR AGRARIO DE LA COMUNA ZAPOTAL” (PÉREZ ALTAMIRANO CRISTIAN GEOVANNY, 2022), “IOT APLICADO A LA DOMOTICA” (Luis Miguel Amaya Fariño, 2020), como podemos ver estos proyectos tienen similitudes en cuando a tecnología domótica se habla, son proyectos con temas más cercanos a la implementación que se realizó en el edificio de INCYT.

Al implementar este sistema domótico se previenen hurtos o robos en el edificio a todas horas del día, ya que se mantiene un monitoreo constante y en tiempo real de los equipos que se encuentran en dicha zona, adicionalmente tendremos alertas y señales que serán enviadas a la o las personas encargadas de dicho edificio si se presenta alguna anomalía a todas horas.

1.6 ALCANCE DEL PROYECTO

En lo que concierne la Universidad Estatal Península de Santa Elena cuenta con un sistema de seguridad basado en cámaras de video vigilancia, sin embargo, con la implementación de un modelo domótico con frecuencias bajas podemos monitorear y gestionar diferentes puntos que se encuentran en el edificio con una pérdida de paquetes casi nula, adicionalmente podemos reforzar la seguridad del mismo, ya que contaríamos con un sistema mucho más completo en lo que respecta el bienestar de los equipos que se encuentran en el edificio.

Para la realización del presente proyecto se incluyen los distintos puntos:

- Analizar los diferentes puntos vulnerables de la zona segura para poder realizar el diseño de Master/esclavo para los equipos.
- Integrar tecnologías compatibles a los software y hardware domóticos antes mencionados que trabajen a una frecuencia no licenciada para incluir los protocolos de seguridad correspondientes
- Creación de un servidor amigable para que cualquier persona pueda controlar y monitorear los elementos instalados.
- Configuración de red privada para tener acceso a los puertos utilizados y que no exista una caída o corrupción en el servidor.
- Facilitar el acceso local y remoto a los servidores creados para el monitoreo.
- Instalación de elementos físicos en el edifico de manera correcta para tener señales constantes y continuas de datos tomados como temperatura, audio y video.

1.7 METODOLOGÍA.

La metodología utilizada en el trabajo de titulación fue: diagnostica, descriptiva, aplicada y experimental, a continuación se detallaran cada una de ellas.

INVESTIGACIÓN DIAGNÓSTICA:

Este método es aplicado ya que se debe recurrir a diversas fuentes bibliográficas como libros, artículos científicos, manuales, informes, inclusive otros proyectos, todo esto para recopilar información tanto de la video vigilancia como los sensores y así poder explicar la teoría del proyecto.

INVESTIGACIÓN DESCRIPTIVA:

Esta investigación hace referencia a la relación que existe entre las variables que en este caso son las cámaras de videovigilancia y los sensores para la implementación de este sistema de seguridad basado en IOT.

INVESTIGACIÓN APLICADA:

Esta investigación ayuda a obtener conocimiento sobre la utilización de cámaras y sensores para poder implementar este sistema de seguridad, ayudándonos a cumplir con el objetivo principal de dicho proyecto.

INVESTIGACIÓN EXPERIMENTAL:

A medida que se realiza el proyecto se necesitarán hacer pruebas para poder mantener el correcto funcionamiento del sistema de seguridad.

A continuación, se presenta un esquema general de la realización del proyecto.

Figura 1 Esquema del proyecto

CAPÍTULO II

LA PROPUESTA

2.1 MARCO CONTEXTUAL

El campo de las telecomunicaciones ha evolucionado de manera paulatina con el pasar de los años, esto es debido a que la tecnología crece día a día y se convierte en algo vital para todo tipo de personas en general.

La Universidad Estatal Península de Santa Elena – UPSE es una institución académica que se encarga de brindar conocimiento y saberes a diferentes personas las cuales requieran este servicio, en varios casos estos participantes son personas santaelenenses, ecuatorianos y latinoamericanos en general.

La provincia de Santa Elena y la universidad en general se adaptó a estos cambios en el área de telecomunicaciones y tecnología, a su vez haciendo uso de ella para la creación de laboratorios, sistemas informáticos, sistemas de vigilancia, entre otros.

La seguridad es aquello que aparece y procura mantener la universidad, tanto como en los laboratorios, oficinas, edificios y personas que se encuentren en la misma. Por este motivo se optó por implementar este sistema de seguridad.

El proyecto se desarrollará en un edificio de la institución, el Instituto de Investigación Científica y Desarrollo de Tecnologías, ya que este posee materiales y elementos útiles para el aprendizaje no solo de una carrera en específica, sino también tiene laboratorios de diferentes facultades como Ciencias de ingeniería, Biología Marina y laboratorios de Agropecuaria. Este sistema de seguridad, ayudará a preservar estos materiales, ya que se contará con un monitoreo constante y en tiempo real de los sectores cercanos al edificio e incluso se tomarán datos de los interiores del mismo, gracias a esto podrán mantener un control de las oficinas incluso fuera de horas laborales.

2.2 MARCO CONCEPTUAL

2.2.1 REDES INALÁMBRICAS

Al hablar sobre redes inalámbricas podemos decir que son redes que utilizan ondas de radio para conectar los dispositivos, sin necesidad de utilizar cables de ningún tipo. Los equipos más utilizados en las redes inalámbricas son ordenadores, teléfonos móviles, tablets, dispositivos localizadores, entre otros. Un propósito fundamental de las redes inalámbricas es que se utilizan para proporcionar acceso a datos desde ubicaciones remotas sustituyendo a las redes cableadas. (Salazar, Redes Inalámbricas)

2.2.2 TECNOLOGIAS INALÁMBRICAS

Las redes inalámbricas se clasifican en cuatro grupos específicos según el área de aplicación y alcance de la señal.

- Redes inalámbricas de área personal WPAN
- Redes inalámbricas de área local WLAN
- Redes inalámbricas de área metropolitana WMAN
- Redes inalámbricas de área amplia WWAN

A continuación, mostraremos una figura sobre la clasificación de las redes inalámbricas.

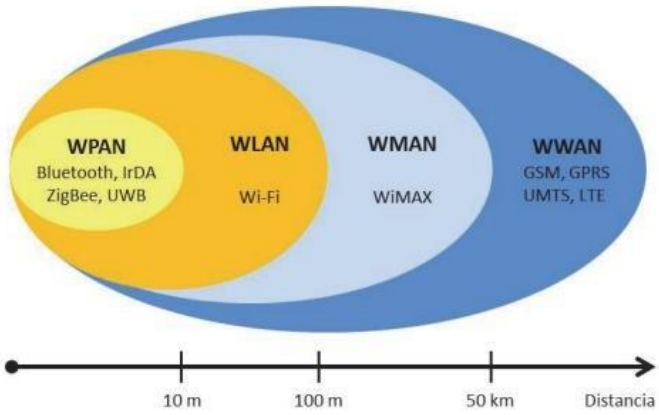


Figura 2 Clasificación de las redes inalámbricas (Salazar, Redes Inalambricas, 2016)

2.2.2.1 SEGURIDAD DE REDES INALÁMBRICA

Al hablar de seguridad de redes inalámbricas podemos decir que se incluyen los controles de seguridad de la capa de red aplicados a redes inalámbricas o WIFI. Este asunto es de vital importancia en los escenarios de trabajo actual. Todo esto es referente a la protección de datos de una entidad, para que personas no autorizadas no puedan poner en peligro los datos pertenecientes a dicha entidad. (F5, s.f.)

2.2.2.2 PROTOCOLOS DE SEGURIDAD INALÁMBRICA

Cuando hablamos de los algoritmos que se utilizan para cifrar toda la comunicación de ese momento en adelante son el WEP, WPA, WPA2 y WPA3. La seguridad es una cuestión de vital importancia cuando se habla de redes inalámbricas, estos protocolos de seguridad antes mencionados cumplen funciones parecidas, sin embargo, su funcionamiento, sus características y nivel de seguridad es diferente. (VADAVO, 2021)

- **PROTOCOLO WEP:** Este protocolo permite ocultar a los intrusos los mensajes que se encuentran codificados y enviándose de una computadora a otra en una red. Esta clave es utilizada para poder conectarse a una red con seguridad inalámbrica.
- **PROTOCOLO WPA:** Este protocolo se encarga de utilizar una clave temporal (TKIP), la cual evita que los intrusos creen una clave de cifrado personal como se podía realizar con el protocolo WEP.
- **PROTOCOLO WPA2:** Este protocolo se basa en el mecanismo de red de seguridad robusta funcionando en dos modos: WAP2-PSK (se basa en uso de códigos de acceso compartido y para usos domésticos) y WPA2-EAP (uso empresarial y para organizaciones).
- **PROTOCOLO WPA3:** Trabaja con cifrado de datos individualizado, protocolo de autenticación simultanea de iguales y protección contra ataques de fuerza bruta más fuerte.

Entre los protocolos de seguridad antes mencionados se utilizó el protocolo WPA y WPA2 para la seguridad de nuestra red inalámbrica, al momento de diseñar nuestra red privada, colocamos un router para poder conectar mediante protocolo ONVIF las cámaras de videovigilancia, estas cámaras se conectan al router colocando la contraseña designada y de esa manera tienen acceso a internet. La razón por la cual se eligieron estos protocolos de seguridad es debido a que trabajan de una manera más segura, ya que el algoritmo estándar de cifrado es más avanzado y gracias a esto podemos evitar que los intrusos generen claves temporales como se puede dar en el caso del protocolo WEP.

2.2.3 SISTEMAS IOT

El internet de las cosas describe la red de objetos físicos que llevan incorporados sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de internet. Cabe recalcar que estos dispositivos tienen una gama amplia de aplicaciones, desde los

objetos domésticos comunes hasta herramientas utilizadas en las industrias sofisticadas. (ORACLE, 2019)

Los sistemas IOT tienen diversas ventajas y desventajas, las cuales se presentan en la tabla 1.

VENTAJAS	DESVENTAJAS
Capacidad de conectarse a la red	Información no cifrada
Intercambio de información	Requiere inversión previa en tecnología
Ahorro energético	Reducción de intimidad
Procesos más sostenibles	Brechas tecnológicas
Comunicación con el entorno	No hay mucha compatibilidad

TABLA 1: VENTAJAS Y DESVENTAS DE SISTEMAS IOT

2.2.3.1 CARACTERISTICAS IOT

Al hablar de Iot tenemos diversas características que hacen relevante e importante este tema, con los avances tecnológicos estas características han ido creciendo para facilitar su uso en diferentes ámbitos de la vida cotidiana.

- **Acceso a la tecnología de sensores de bajo costo y potencia:** Los sensores y tecnología que utilizan los sistemas IOT son de bajo coste ya que se encuentran de manera muy sencilla en el mercado, cabe recalcar que existen diversas marcas las cuales tienen elementos y dispositivos para conectarse a internet, lo cual entra en las aplicaciones IOT. Adicionalmente los elementos son de bajo coste energético, ya que por lo general utilizan baterías de 5V, las cuales poseen una vida útil de casi 2 años.
- **Conectividad:** La conectividad de los dispositivos IOT es muy sencilla e intuitiva, en la actualidad cada elemento viene con su respectivo manual de

instrucciones y adicionalmente con una aplicación, en la cual se detallan pasos para su correcta conexión y configuración.

- **Plataformas de informática en la nube:** Existen diversos softwares en los cuales trabajan estos elementos IOT, entre las más populares tenemos almacenamiento en la nube, por lo general los elementos IOT se encargan de recopilar datos en tiempo real los cuales pueden almacenarse tanto de manera interna en una tarjeta o ser enviados a la nube y almacenar los datos de manera virtual, lo cual nos permite tener acceso a lo almacenado desde cualquier parte.
- **Aprendizaje automático y analítico:** El aprendizaje automático juega un papel muy importante en los sistemas IOT, esto es debido a que la recopilación de información es de gran utilidad para las maquinas, ya que en un futuro puede tomar decisiones por su cuenta, sin necesidad de que el ser humano envíe dicha petición, un ejemplo es la detección de movimiento, podemos detectar un movimiento y que automáticamente se encienda una luz, ese es un pequeño ejemplo del aprendizaje automático y analítico de estos sistemas.
- **Inteligencia artificial convencional:** La inteligencia artificial en el IOT es utilizada de manera industrial, gracias a la toma de datos constante estos pueden ser almacenados y el IA se convierte en un cerebro avanzado que se encarga de la toma de decisiones para controlar un sistema designado.

2.2.4 DOMÓTICA

Según las fuentes bibliográficas el concepto domótica hace referencia al conjunto o agrupación de sistemas y tecnologías capaces de automatizar una vivienda mediante una gestión inteligente de energía. Diferentes parámetros se tratan en una edificación inteligente, entre los cuales tenemos: comunicaciones, iluminación, seguridad, temperatura todo esto se automatiza con el fin de aportar seguridad, bienestar y confort. (Sarachu, 2022)

En la tabla número 2 se presentan las funciones técnicas de la domótica.

FUNCIONES	VENTAJAS	BENEFICIOS
Programación de elementos en el hogar	Mayor control sobre recursos en el hogar	Ahorro de energía
Automatización de diversas acciones	Ahorro energético	Comodidad y simplicidad en el hogar
Conexión a un dispositivo master	Ahorro económico	Control por voz
Control y monitoreo en tiempo real	Instalación automatizada	Prevención de robos
Mejoramiento de seguridad en el hogar	Posee redes eléctricas inteligentes	Monitoreo y almacenamiento de datos en tiempo real

TABLA 2: FUNCIONES TÉCNICAS DE LA DOMÓTICA

2.2.4.1 CARACTERÍSTICAS DE LA DOMÓTICA

La domótica nos permite controlar una serie de sistemas y tecnologías para realizar un uso más racional de la climatización, la electricidad y los sistemas de seguridad. Con la regulación de estos parámetros podemos aportar a las personas residentes o presentes en la edificación bienestar, comodidad y seguridad. (Sarachu, 2022)

Para ser más específicos, la domótica controla diferentes parámetros en el hogar y en las edificaciones.

En la tabla número 3 se describen los parámetros en el hogar que controla la domótica.

PARÁMETROS	FUNCIÓN	PORCENTAJE DE USO
Sistema de iluminación inteligente	Este sistema se encarga de controlar y automatizar elementos como bombillas, lámparas, flashes entre otros.	Según estudios realizados a digital Market Outlook, el 20 % de las casas tienen este sistema inteligente. (PORTAFOLIO, 2022)
Control automático inteligente	Gracias a esto podemos programar acciones para que las mismas sean ejecutadas en un tiempo determinado.	Este concepto es aplicado en diversos lugares, un claro ejemplo es en una planta la cual contiene más de 50% de equipos y acciones automatizadas (Avello, 2021)
Sistema de regulación y control de climatización	Este tipo de sistemas son eficientes en energía pero son implementadas en edificaciones e industrias, cabe recalcar que existen hogares en donde los sistemas de climatización son controlados.	Este sistema ayuda al control de calderas y equipos, hablando industrialmente, según investigaciones tenemos que el 75% de estos equipos están monitoreados y controlados para evitar catástrofes. (Martín, 2018)
Control inteligente de riego	Este sistema es aplicado en el ámbito de la agricultura, incluso se utiliza en universidad, edificios con áreas verdes y en hogares, es el encargado de ejecutar acciones de riego dependiendo de la hora programada.	Según estudios el porcentaje de aplicación de este método en hogares o edificaciones es del 15%, esta tecnología reduce el promedio de uso de agua en estos hogares. (Aguayo, 2021)

TABLA 3: PARÁMETROS CONTROLADOS POR LA DOMOTICA EN EL HOGAR

En base a lo antes mencionado, mostramos a continuación una imagen descriptiva de los elementos y acciones que entran en el control de la domótica.

FIGURE 3 INFOGRAFÍA DE LA DOMÓTICA (Sarachu, 2022)

2.2.4.2 SEGURIDAD DOMÓTICA

Según conceptos la seguridad domótica se basa en la automatización, gestión y control de diversos aspectos de un hogar o edificación que pueden suponer algún peligro.

Gracias a los sensores de todo tipo, un sistema domótico puede alertar a sus usuarios con el objetivo de conocer cualquier tipo de problema o imprevisto dentro de un hogar. Junto a los sensores y sistema vienen apps para mantener seguro el hogar, entre las principales son “Houseinhand KNX”, “Nexho”, “Smart Life”, entre otra. Estas aplicaciones tienen en común el control del hogar desde cualquier parte y de manera rápida e intuitiva, cabe recalcar que estas apps están hechas unas para sistemas IOS y otras para sistemas Android. (MAPFRE, 2023)

La seguridad domótica juega un papel muy importante ya que ayuda a mejorar la prevención de riesgos debido a que se puede obtener información en tiempo real de lo que está sucediendo en el hogar o edificación.

Entre los protocolos más aptos para la domótica tenemos el Zigbee o el Z-wave, esto debido a que no solo evitaríamos problemas de saturación de red, sino

también que aumentaremos la seguridad de la propia red de comunicación domótica. (SIMON, 2021)

2.2.4.3 PROTOCOLOS DE COMUNICACIÓN DOMÓTICA

Existen diversos protocolos de comunicación en la domótica, cada uno de ellos con características específicas, a continuación, mostraremos en una tabla los principales:

PROCOLOS	NORMATIVA	CONCEPTOS O USOS
knx	Normativa mundial iso/iec 14543 (NN, 2022)	Control y automatización de edificios y viviendas mediante sistema de bus
x10	Trabaja bajo la normativa IEEE 80 (Flores, 2007)	Control remoto de dispositivos eléctricos
dali	Trabaja bajo la normativa IEC 62386 (Rojas, 2021)	gestiona iluminación inteligente de manera remota
zigbee	normativa IEEE 802.15.4 (Moreno, 2007)	Trabaja bajo una topología de red malla y su utilización se centra en radiodifusión digital de bajo consumo
z wave	Estandar ITU-T g.9959 (Bernal, 2019)	Tecnología rf de bajo consumo diseñada para productos de domótica.
lonworks	Trabaja la normativa ieee.1473-1999 (DIgital, s.f.)	Sistema de automatización distribuido comunicado a través

TABLA 4: PROTOCOLOS DE COMUNICACIÓN DOMÓTICA

En la tabla anterior se presentaron los principales protocolos de la domótica en el hogar. Con esta información seleccionamos dos protocolos para la aplicación de nuestro sistema, entre los seleccionados tenemos al protocolo zigbee y al protocolo z wave. A continuación, hablaremos sobre ambos protocolos.

2.2.4.3.1 PROTOCOLO ZIGBEE

Zigbee es un estándar que define un conjunto de protocolos para el armado de redes inalámbricas de corta distancia y baja velocidad de datos. Este protocolo opera en las bandas de 868 MHz, 915 MHz y 2.4 GHz y puede transferir datos hasta 250Kbps. (Dignani J. P., 2011)

En la siguiente figura, mostramos un ejemplo controlando luces mediante el protocolo zigbee.

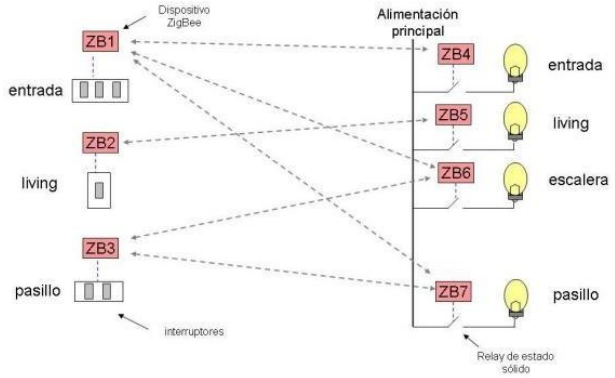


FIGURA 4: CONTROL DE LUCES EN UNA CASA UTILIZANDO PROTOCOLO ZIGBEE (Dignani J. , 2011)

2.2.4.3.1.1 CARACTERÍSTICAS DEL PROTOCOLO ZIGBEE

Este protocolo tiene como características principales las siguientes:

- Ultra bajo consumo que permite usar equipos que funcionen a baterías
- Bajo costo de dispositivos y de instalación
- Alcance corto (menor a 50 metros)
- Optimizado para ciclo efectivo de transmisión
- Velocidades de transmisión menor a 250Kbps

2.2.4.3.1.2 VENTAJAS Y DESVENTAJAS DEL PROTOCOLO ZIGBEE

A continuación, presentaremos en un cuadro las ventajas y desventajas que implica utilizar este protocolo de comunicación.

VENTAJAS	DESVENTAJAS
Es ideal para conexiones PtP y PtMP **(Jimenéz, 2016)**	Tasa de transferencia baja en comparación a otros protocolos (Jimenéz, 2016)
Opera en banda libre de ISM 2.4GHz para conexiones inalámbricas **(Jimenéz, 2016)**	Manipulación de textos pequeños a comparación de otras tecnologías (Jimenéz, 2016)
Óptimo para redes de baja tasa de transferencia de datos **(Jimenéz, 2016)**	Menor cobertura por pertenecer a redes WPAN (Jimenéz, 2016)
Proporciona larga duración a la batería de los equipos **(Jimenéz, 2016)**	No es compatible con bluetooth (Jimenéz, 2016)
Soporta múltiples topologías de red (estática, dinámica, estrella y malla) **(Jimenéz, 2016)**	No tiene mucha capacidad de soporte para nodos (Jimenéz, 2016)

TABLA 5: VENTAJAS Y DESVENTAS DE PROTOCOLO ZIGBEE

2.2.4.3.2 PROTOCOLO Z-WAVE

Z wave es un protocolo el cual tiene como punto fuerte el gran número de diferentes productos de distintos fabricantes, la comunicación robusta, bidireccional y segura. También se compone de chips de baja potencia que consumen 10 mW en el pico y son de bajo coste, ya que fueron diseñados en el 2003 para aplicaciones de viviendas residenciales. Cabe recalcar que Z-wave es un protocolo completo,

seguro, fiable y además ofrece precios competitivos con protección de la inversión para proyectos de todos los tamaños. (Soler, 2014)

A continuación, mostramos una imagen de varios dispositivos interconectados entre sí, mediante el protocolo Z-WAVE como una red tipo mesh.

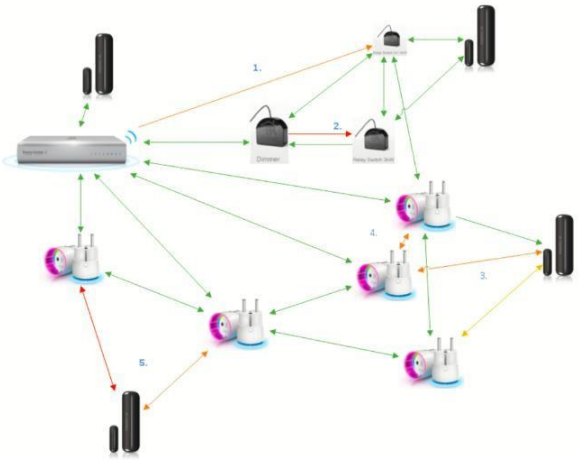


FIGURE 5 RED MALLADA USADA EN PROTOCOLO Z-WAVE (INTERCONEXIÓN DE VARIOS DISPOSITIVOS) (Profesional, 2019)

2.2.4.3.2.1 CARACTERÍSTICAS DEL PROTOCOLO Z-WAVE (Carlos Araya Guzmán, 2018)

Este protocolo cuenta con características similares al protocolo Zigbee, a continuación, nombraremos las suyas que son:

- Frecuencia de trabajo en 868,42 MHz
- Bajo consumo de energía
- Alcance en espacios cerrados es de 45 metros y en espacios libres 150 metros
- Modulación por desplazamiento de frecuencia gaussiana (FSK)
- Potencia de salida de 1MW
- Las velocidades de datos incluyen 9600 bits/s y 40 Kbits/s

2.2.4.3.2.2 VENTAJAS Y DESVENTAJAS DEL PROTOCOLO Z-WAVE

Existen varias ventajas y desventajas cuando hablamos del protocolo de comunicación “z wave”.

A continuación, en la tabla número 6, se muestran las ventajas y desventajas del protocolo z wave.

VENTAJAS	DESVENTAJAS
Trabaja a frecuencia de 900 MHz (evitando frecuencia wifi y bluetooth) **(García, 2018)**	Tasa de transferencia baja (García, 2018)
Instalación sencilla **(García, 2018)**	Utiliza protocolos más sencillos (García, 2018)
No requiere ningún nuevo cableado eléctrico **(García, 2018)**	Distancia de funcionamiento limitadas (García, 2018)
Utiliza el mismo cifrado que la banca en línea **(García, 2018)**	Precios más altos (García, 2018)
Inversión mínima y deja abierta la entrada a nuevos dispositivos inteligentes. **(García, 2018)**	La fiabilidad y estandarización no son gratuitas (García, 2018)

TABLA 6: VENTAJAS Y DESVENTAS DE PROTOCOLO Z WAVE

2.2.4.3.3 PROTOCOLO ONVIF

Uno de los protocolos utilizados para la comunicación de las cámaras de videovigilancia instaladas es el protocolo ONVIF (Open Network Video Interface Forum). Este protocolo es un estándar para los sistemas de videovigilancia, ya que permiten la interoperabilidad entre distintos equipos de varios proveedores. El

objetivo de este protocolo es que cualquier equipo compatible con ONVIF pueda comunicarse con algún otro dispositivo que también sea compatible, en el caso del presente proyecto tenemos las cámaras con protocolo ONVIF y el servidor creado en nuestro Raspberry que también es compatible con dicho protocolo. (Seguridad, 2022)

2.2.4.3.3.1 CARACTERÍSTICAS DEL PROTOCOLO ONVIF

El protocolo ONVIF posee diversas características, a continuación, hablaremos de las principales y las que hacen diferente a este protocolo de comunicación comparado con otros.

- Normalización de comunicación entre los dispositivos IP
- Interoperabilidad entre equipos de video
- Facilidad de configuración y trabajo de las cámaras
- Acceso a todas las empresas y organizaciones

2.2.4.3.3.2 VENTAJAS Y DESVENTAJAS DEL PROTOCOLO ONVIF

Existen varias ventajas y desventajas cuando hablamos del protocolo de comunicación “ONVIF”.

A continuación, en la tabla número 7, se muestran las ventajas y desventajas del protocolo onvif.

VENTAJAS	DESVENTAJAS
Escalabilidad (puede usarse en proyectos de varios tamaños)	Es un protocolo antiguo
Compatibilidad con varios dispositivos	Es menos seguro para sistemas grandes
Flexibilidad para elegir cámaras de seguridad	Depende de la velocidad de internet
Fácil configuración	El sistema es vulnerable a ataques mediante hacks

TABLA 7: VENTAJAS Y DESVENTAS DE PROTOCOLO ONVIF

2.2.4.4 TIPOS DE DOMÓTICA

La tecnología domótica se clasifica en dos grupos, los sistemas inalámbricos y los sistemas cableados.

- **DOMÓTICA INALÁMBRICA:** En estas aplicaciones se utilizan señales de radiofrecuencia en las cuales se transportan los datos según protocolos de transmisión inalámbrica como lo son WIFI, Z-wave, etc. (TECNOSEGURO, s.f.)
- **DOMÓTICA CABLEADA:** Este sistema tiene dos subclases, transmisión de datos con cableado dedicado y transmisión de datos con uso de la infraestructura eléctrica. Estos trabajan por medio de un conductor específico para el envío y comunicación de los datos, entre los protocolos tenemos: BacNet, LonWorks, etc. (TECNOSEGURO, s.f.)

2.2.4.5 ARQUITECTURA EN LA DOMÓTICA

En la domótica existen dos tipos de arquitectura, la arquitectura distribuida y la arquitectura centralizada.

- **SISTEMAS CON ARQUITECTURA DISTRIBUIDA:** En este sistema, cada equipo puede funcionar como un sensor o un actuador, incluye la unidad de procesamiento y se comunica con el software de manera independiente. (TECNOSEGURO, s.f.)

A continuación, en la figura 4 se muestra un diagrama como ejemplo de la arquitectura distribuida para apreciar de mejor manera el funcionamiento.

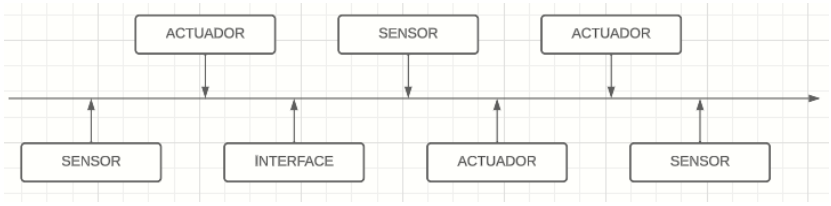


FIGURE 6 ARQUITECTURA DISTRIBUIDA

Como podemos observar en el diagrama anterior, esta arquitectura trabaja de manera independiente, esto envía información según el tipo de programación y configuración, dicha información se capta por sí mismo y recibe otra información de otros elementos del sistema.

- **SISTEMAS CON ARQUITECTURA CENTRALIZADA:** En estos sistemas hay un controlador al cual se conectan los sensores y/o actuadores del sistema. (TECNOSEGURO, s.f.)

A continuación, en la figura 5 se muestra un diagrama como ejemplo de la arquitectura centralizada para apreciar de mejor manera el funcionamiento.

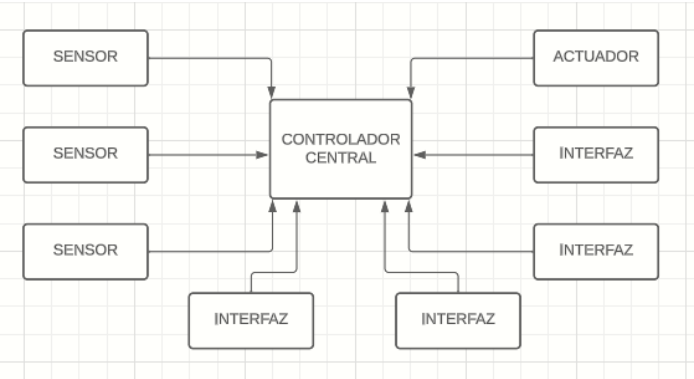


FIGURE 7 ARQUITECTURA CENTRALIZADA

Como podemos observar en el diagrama de flujo, esta arquitectura trabaja de manera cooperativa, es decir que los sensores, la interfaz y los actuadores van dirigidos a un mismo controlador central, el cual dependiendo de la codificación o configuración va a realizar acciones dependiendo de los datos enviados.

2.2.5 RADIOFRECUENCIAS

Las radiofrecuencias, hacen énfasis al espectro radioeléctrico que son los niveles de Hertz que se encuentran en el espacio para ser utilizados, existen diversos tramos de frecuencias las cuales tienen subdivisiones.

Según definiciones generales, la radiofrecuencia es la tasa de oscilación del espectro de radiación electromagnético u ondas de radio electromagnéticas, estas frecuencias van desde los 300 gigahercios (GHz) hasta los 3 kilohercios (KHz). Gracias a diferentes tipos de antes y/o transmisores, se los utilizan en diferentes aspectos de la comunicación inalámbrica. (alaisecure, s.f.)

A continuación, en la figura 6 mostramos el espectro electromagnético con ejemplos de las ondas de radio y las aplicaciones que tienen.

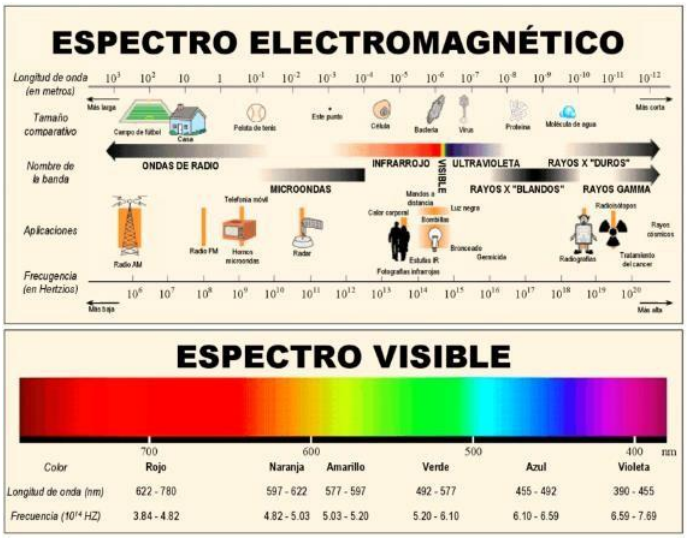


FIGURE 8 ESPECTRO ELECTROMAGNÉTICO (ESQUEMA, 2021)

2.2.5.1 FRECUENCIAS LICENCIADAS Y NO LICENCIADAS

En el espectro radio eléctrico tenemos dos divisiones en las frecuencias, ya sean altas o bajas, entre las mismas están las frecuencias licenciadas y las no licenciadas.

- **Frecuencias licenciadas:** En este tipo de frecuencias se requieres de una validación por parte del organismo regulador para su uso. Para la utilización de un espacio del espectro requiere una documentación que conlleva a una larga inversión de tiempo, ya que el organismo regulador requiere detalles sobre el uso que se le dará a este espacio. (Martínez, 2012)
- **Frecuencias no licenciadas:** Dicho de esta forma, las frecuencias no licenciadas son aquellas que no requieren de permisos espectrales para ser utilizadas, hablando a nivel mundial, las bandas 2.4 GHz y 5 GHz son las más utilizadas con diferentes variaciones y restricciones dependiendo del país en el que se encuentren. Estas frecuencias son utilizadas mediante WiFi, el estándar 802.11 y por ser libres las podemos encontrar en puntos de acceso. (Martínez, 2012)

2.2.6 HARDWARE LIBRE

Al hablar de hardware libre nos referimos a los dispositivos en las que sus especificaciones y diagramas esquemáticos son de acceso público, tenemos una gran variedad de ellos, entre los más utilizados son:

- Arduino
- Raspberry
- RepRap
- E-puck
- Open Source Ecology
- Uzebox
- Cubieboard

2.2.6.1 VENTAJAS Y DESVENTAJAS DE UTILIZAR HARDWARE LIBRE

En esta etapa hablaremos sobre las ventajas y desventajas que tenemos al utilizar hardware libres. En la tabla número 8 se muestran las ventajas y desventajas de los hardware antes mencionados

HARDWARE LIBRE	VENTAJAS	DESVENTAJAS
ARDUINO REPRAP E-PUCK OPEN SOURCE ECOLOGY UZEBOX CUBIEBORAD RASPEBRRY	• Flexibles • Económicos • Código Abierto • Mucha información • fácil de programar • Sostenibilidad • Funcionalidad • Mayor precisión • Mayor velocidad	• No hay mantenimiento del proveedor • No tiene la misma precisión de un equipo propietario • No tiene la misma robustez de un equipo propietario • Propenso a hacks • Mala programación

TABLA 8: VENTAJAS Y DESVENTAS DEL USO DE HARDWARE LIBRE

En base a las características y aplicaciones antes mencionadas, las tarjetas con más funciones cercanas a lo que se necesita son “Arduino” y “raspberry”, a continuación, hablaremos más a fondo de estas dos tarjetas controladoras para evaluar sus ventajas y desventajas.

2.2.7 SOFTWARE LIBRE

El software libre es un software o programa que puede ser utilizado, copiado y distribuido de manera libre, es decir no es necesario pagar una suscripción o un precio fijo para usarlos. Existen diversos programas que se pueden utilizar todo dependiendo de lo que se necesite, entre las principales aplicaciones tenemos:

- Ofimática
- Navegadores Web
- Gestores de correo
- Sistemas operativos
- Sistema de gestión de cursos

A continuación, en la tabla número 9, hablaremos sobre las ventajas y desventajas que poseen los softwares libres.

VENTAJAS	DESVENTAJAS
Accesibilidad	Falta de soporte técnico
Personalización	Curva de aprendizaje según sea el caso
Colaboración	Problemas de seguridad
Reducción de costos	Problemas de estabilidad
Innovación tecnológica	No posee garantía
Requisitos de Hardware menores	Algunas configuraciones no son intuitivas

TABLA 9: VENTAJAS Y DESVENTAS DEL USO DE SOFTWARE LIBRE

2.2.7.1 SOTFWARE LIBRE EN LA DOMÓTICA

Los softwares libres en la domótica se han visto influenciados por un movimiento llamado Maker, los cuales sugieren alternativas basadas en Linux. Estas opciones buscan integrar varios elementos que tienen las instalaciones domóticas con APIs de internet. (Vega, 2017)

A continuación, en la tabla número 10 explicaremos los softwares principales y las características que poseen cada uno de ellos.

Software Libre	Características y funcionamiento
Domoticz	• Compatibilidad con Windows y Linux • Trabaja bajo protocolos como Ocean, x10, Z wave • Programación en C++
Jeedom	• Posee arquitectura interna modular • Gran parte de la información se encuentra en francés
OpenHab	• Es compatible con Windows y Linux • Su arquitectura es totalmente modular • Es compatible con varios protocolos de comunicación
Home Assistant	• Compatibilidad con Windows y Linux • Es adaptable para dispositivos móviles y de escritorio • Compatibilidad hardware con z. wave, P1 smart, Ocean

TABLA 10: CARACTERISTICAS DE LOS PRINCIPALES SOFTWARE LIBRES EN LA DOMOTICA

Una vez indicadas las características principales de los softwares libres en la domótica, podemos decir que 2 de ellos se asemejan más al uso que le dimos en la implementación del sistema de monitoreo, los cuales son “Home Assistant” y “Domoticz”. A continuación, hablaremos más sobre ambos softwares para indicar su funcionamiento, ventajas y características.

2.2.7.1.1 DOMOTICZ

Domoticz es un sistema el cual nos permite configurar y supervisar varios dispositivos domóticos como luces, interruptores, sensores, entre otros. En

cuestiones de aplicaciones, este sistema es compatible con un gran numero como Raspberry, Cubieboard, Unix, Apple, Windows. (Peters, 2015)

A continuación, en la tabla número 11 se presentan las características de este sistema.

CARACTERISTICAS	DESCRIPCION
Compatible con varios protocolos	Z-Wave, Mqtt, Zigbee
Facilidad de instalación	Es compatible con Windows, Linux
Puertos utilizados	8080
Certificado	SSL
Configuración	Cuenta con comandos para automatización
Lenguaje de programación	C++

TABLA 11: CARACTERISTICAS DE SISTEMA DOMOTICZ

2.2.7.1.1.1 VENTAJAS Y DESVENTAJAS DEL SISTEMA DOMOTICZ

Como todas las aplicaciones y programas poseen diversas características para su uso, también poseen ventas y desventajas, saber cuándo cada sistema es el indicado a usar es conveniente, a continuación, en la tabla número 12 presentamos las principales.

VENTAJAS	DESVENTAJAS
Es eficiente para dispositivos de baja potencia	Interfaz un poco compleja
Tiene soportes para varios protocolos	Sus integraciones son limitadas
Amplia gama de personalización	Compatibilidad con protocolos limitada
Rendimiento estable y confiable	Costos en dispositivos para su compatibilidad
Fácil instalación	Configuración del servidor compleja
Lenguaje de programación basado en C++	Manipulación de comandos menos intuitiva

TABLA 12: VENTAJAS Y DESVENTAJAS DEL SISTEMA DOMOTICZ

2.2.7.1.2 HOME ASSISTANT

Home Assistant es una plataforma de código abierto que se ejecuta en Python 3, este sistema permite rastrear y controlar dispositivos del hogar para gestionar su automatización. Este tipo de sistemas son muy comunes instalarlos en hardware como Raspberry, Orange hasta incluso Pi Zero. Lo que se consigue con esto es gestionar el control de los dispositivos de la domótica. (Fernandez, 2018)

Su uso varía dependiendo el dispositivo a controlar, entre los cuales están:

- Apagado y encendido
- Mediciones
- Envío de mensajes y alertas
- Control
- Comandos de voz

A continuación, en la tabla número 13 presentamos las características principales que posee esta plataforma.

CARACTERISTICAS	DESCRIPCION
Integración de diferentes protocolos	Z wave, Linux, Mqtt
Usos de variedades de APIs	HUE, Xiaomi, Nest
Distintas reglas de automatización	Trigger, Condition, Action
Interfaz amigable	Es fácil de entender
Facilidad de instalación y configuración	Se puede instalar en raspberry, Windows, Linux
Compatibilidad con varios dispositivos	Luces, termostatos, cámaras, sensores

TABLA 13: CARACTERISTICAS DE LA PLATAFORMA HOME ASSISTANT

2.2.7.1.2.1 VENTAJAS Y DESVENTAJAS DE LA PLATAFORMA HOME ASSISTANT

Para esta plataforma al igual de la de Domoticz existen diversas ventajas y desventajas, esta se caracteriza por ser de configuración sencilla e interfaz simple, esto ayuda a personas que no tienen conocimiento informático o de redes configurar y ejecutar diversas aplicaciones que posee la plataforma

A continuación, en la tabla número 14 se presentan las ventajas y desventajas principales que posee esta plataforma, en base a las presentadas, podemos darnos una idea del por qué se utilizó este sistema en la implementación del proyecto.

VENTAJAS	DESVENTAJAS
Interfaz sencilla de utilizar	Curva de aprendizaje para configuración avanzada
Amplia compatibilidad con los dispositivos y marcas	Requiere un cantidad considerable de recursos en el sistema
Opciones de automatización mediante reglas	No se puede instalar integraciones que no se encuentren en el catálogo
Comunidad Activa	No se tiene acceso a su sistema operativo
Bajo coste en dispositivos	Para utilizar herramientas como Docker se necesita conocimiento
Facilidad para instalación y configuración	Capacidad limitada para ejecutarlo en macro proyectos

TABLA 14: VENTAJAS Y DESVENTAJAS DE LA PLATAFORMA HOME ASSISTANT

2.2.8 ARDUINO

El Arduino es una plataforma de prototipos electrónica de código abierto que se basa en hardware y software flexibles y sencillos de usar. Este consiste en una placa microcontroladora, la cual soporta entrada y salida de datos y señales. (Pedrera, 2017)

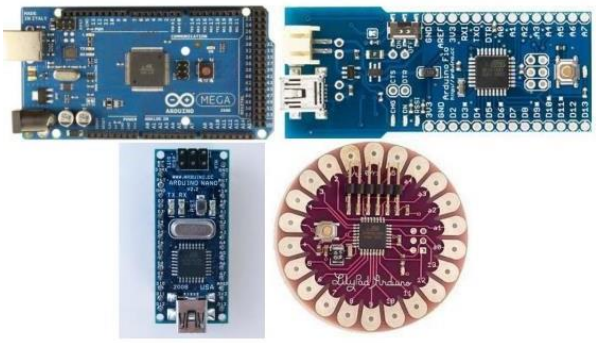


FIGURE 9 IMAGEN DE VARIOS MODELOS DE "ARDUINO" (Pedrera, 2017)

2.2.7.1.1 TIPOS DE ARDUINO

Existe una variedad inmensa en lo que a modelos de arduinos se refiere, cada uno de ellos se adapta al uso y al lugar en donde se los requiera, debido a que algunos modelos son de proporciones más altas o bajas, tienen distintos puertos de entradas y salidas. Entre los modelos de Arduino más comunes y utilizados tenemos los siguientes:

Arduino UNO: Arduino de gama básica, cuenta con 14 pines de entrada y salida, 6 de los mismos se pueden usar como PWM, 6 entradas analógicas, I2C, SPI y UART. (Acceso, 2022)

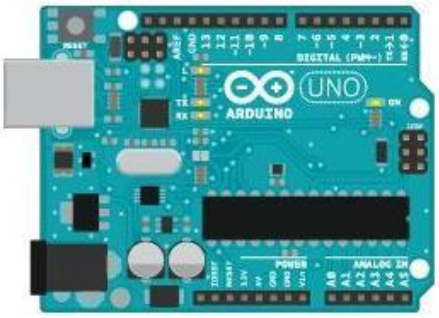


FIGURE 10 IMAGEN DE ARDUINO UNO (ARDUINO, Arduinon UNO R3 , 2023)

Arduino UNO R3: Este tipo de Arduino es el más utilizado, cuenta con características similares y su diseño es más robusto.

FIGURE 11 IMAGEN DE ARDUINO UNO R3 (ARDUINO, Arduinon UNO R3 , 2023)

Arduino DUE: Este Arduino está basado en un microcontrolador de 32 bits, cuenta con 54 entradas.

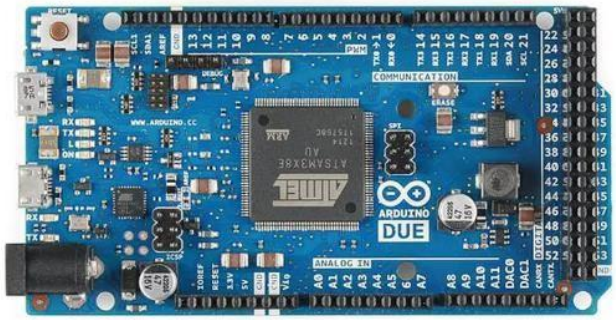


FIGURE 12 IMAGEN DE ARDUINO DUE (ARDUINO, docs.arduino.cc, 2022)

ARDUINO LEONARDO: Es un Arduino básico con características similares, la diferencia es que este no posee un controlador adicional para controlar el USB.

FIGURE 13 IMAGEN DE ARDUINO LEONARDO (ARDUINO, Arduino Leonardo, 2022)

ARDUINO MEGA 2560: Este tiene 54 puertos (entradas y salidas digitales), cuenta con 6 interrupciones externas y es compatible con todos los shields de Arduino.

FIGURE 14 IMAGEN DE ARDUINO MEGA (ARDUINO, Arduino Leonardo, 2022)

ARDUINO MICRO: Este tipo de Arduino es similar al modelo Leonardo, pero la diferencia es el tamaño que este tiene.

FIGURE 15 IMAGEN DE ARDUINO NANO (ARDUINO, Arduino Leonardo, 2022)

2.2.7.1.2 CARACTERÍSTICAS GENERALES DEL ARDUINO

Como vimos anteriormente, Arduino cuenta con varios modelos, cada uno de ellos adaptándose al uso que se le quiere dar, sin embargo, tomaremos como referencia el más común que es el “Arduino UNO”, ya que este es el más utilizado para diferentes proyectos y trabajos.

CARACTERÍSTICAS	DESCRIPCIÓN
Microcontrolador	ATmega168
Voltaje de operación	5V
Tensión de entrada recomendada	7 - 12 V
Tensión de entrada limite	6 - 20 V
Pines digitales E/S	14
Pines de entrada analógico	6
Corriente DC por pin E/S	40 mA
Memoria Flash	16 KB
SRAM	1 KB
EEPROM	512 Bytes
Frecuencia de reloj	16 MHz

TABLA 15: CARACTERISTICAS DEL ARDUINO

2.2.9 RASPBERRY PI

El Raspberry Pi es un dispositivo que tiene la capacidad de realizar labores de computación de propósito general. Estos dispositivos son una placa computadora u ordenador de tamaño reducido, es de bajo costo y se basa en la arquitectura ARM. Cabe recalcar que este dispositivo es una opción muy buena junto al Arduino, sin embargo, este miniordenador tiene el poder para ejecutar un sin número de aplicaciones y tareas que se le asigne, este dispositivo viene sin sistema operativo y su instalación va en una tarjeta SD para su respectiva ejecución y programación. (Viera, 2017)

A continuación, mostraremos unas imágenes de algunos modelos que existen de este miniordenador.

FIGURE 16 IMAGEN DE ALGUNOS MODELOS DE RASPBERRY PI (MOLLOY)

2.2.9.1.1 TIPOS DE RASPBERRY

En la actualidad, existen varios tipos o modelos de este miniordenador, todo de acorde a las necesidades que se presentan y al uso que se le quiera dar, a continuación, hablaremos brevemente de los modelos más comunes y más utilizados en el ámbito de la informática y la electrónica.

RASPBERRY PI 1: Este modelo de Raspberry tiene 512 de memoria RAM, una salida HDMI, salida de audio, salida de video RCA, puerto USB.

FIGURE 17 IMAGEN DE RASPBERRY PI 1 (RASPBERRY, 2022)

RASPBERRY PI 2: Este modelo de Raspberry ofrece mayor capacidad en comparación con la versión anterior, muy aparte de contar con las características mencionadas en la versión anterior este es más rápido debido a que cuenta con un procesador Broadcom de 4 núcleos que funciona a 900 MHz.

FIGURE 18 IMAGEN DE RASPBERRY PI 2 (RASPBERRY, 2022)

RASPBERRY PI ZERO: Este modelo de Raspberry es mucho más avanzado que los anteriores, tiene la ventaja de que su tamaño es más reducido, su CPU funciona a una frecuencia de 1GHz, posee Bluetooth, conector mini HDMI, micro USB y WLAN.

FIGURE 19 IMAGEN DE RASPBERRY PI ZERO (RASPBERRY, 2022)

RASPBERRY PI 3: Este modelo tiene un procesador de cuatro núcleos de 64 bits que trabajan a 1,4 GHz, doble banda (2,4 GHz y 5 GHz), Bluetooth, Ethernet y capacidad PoE.

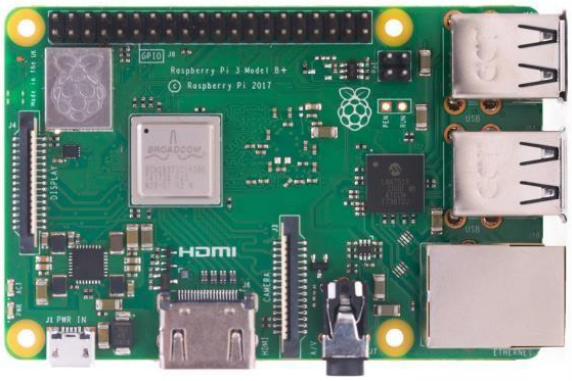


FIGURE 20 IMAGEN DE RASPBERRY PI 3 (RASPBERRY, 2022)

RASPBERRY PI 4: Este modelo es de los más recientes ya que cuenta con un procesador que trabaja a una frecuencia de 1,4 GHz, posee una memoria RAM de 1, 2 o 4 Gb, 4 puertos USB, su alimentación es mediante un puerto tipo C y tiene 40 pines GPIO.

FIGURE 21 IMAGEN DE RASPBERRY PI 4 (RASPBERRY, 2022)

2.2.6.3.2 CARACTERISTICAS GENERALES DE RASPBERRY

Como mencionamos anteriormente, existen una gran variedad de modelos en lo que a Raspberry se refiere, para hablar de características generales, tomaremos como referencia la versión Raspberry PI 3 que es la más utilizada y la más comercializada, ya que cuenta con mejoras de las versiones anteriores y las diferentes funciones y puertos que posee son de ayuda para ejecutar casi cualquier función que se le dé.

En la siguiente tabla se muestran las características técnicas y generales del raspberry.

CARACTERÍSTICAS	DESCRIPCIÓN
Procesador	ARM v8
Núcleos del procesador	4 núcleos
Frecuencia de funcionamiento	1,4 GHz
Procesador Gráfico	Video Core IV
Conector HDMI	1
Conexión Ethernet	Si (10/100/1000 Mbps)
Puertos USB	4
Pines GPIO	40
Lector de tarjeta SD	Si (micro)

TABLA 16: CARACTERISTICAS DEL RASPBERRY

2.2.6.3.3 VENTAJAS Y DESVENTAJAS DE RASPBERRY

Existen varias ventajas y desventajas en cuanto al Raspberry se refiere, cabe recalcar que todo dependerá del uso que se le quiera dar a esta minicomputadora.

VENTAJAS	DESVENTAJAS
Es una minicomputadora	No soportan tareas con muchos gráficos
Posee puerto ethernet para fácil conexión	Capacidad de computo reducida
Su sistema operativo va en una tarjeta SD	No posee suficientes interfaces para conexión de sensores externos
Permite una expansión debido a su placa	

TABLA 17: VENTAJAS Y DESVENTAS DEL RASPBERRY

2.2.7 TECNOLOGÍAS MIMO

Según conceptos de varios artículos científicos MIMO (múltiples entradas múltiples salidas) es una tecnología de radio comunicaciones que se refiere a enlaces de radio que utilizan múltiples antenas tanto del lado del transmisor y lado del receptor con el fin de lograr un mejor rendimiento en la transferencia de datos de manera inalámbrica, es decir, nos ayuda a una mejor estabilidad en la señal. (TACO, 2009)

2.2.7.1 FUNCIONAMIENTO DE LA TECNOLOGÍA MIMO

La tecnología MIMO utiliza funciones de ondas de radio de múltiples rutas, gracias a esto la información que viaja puede rebotar en las paredes y llega a la

antena receptora. Esta tecnología es capaz de aumentar la potencia de la captura de señales ya que permite que las antenas combinen distintos flujos de datos.

A continuación, en la imagen número 22 se muestra un esquema del funcionamiento de la tecnología MIMO.

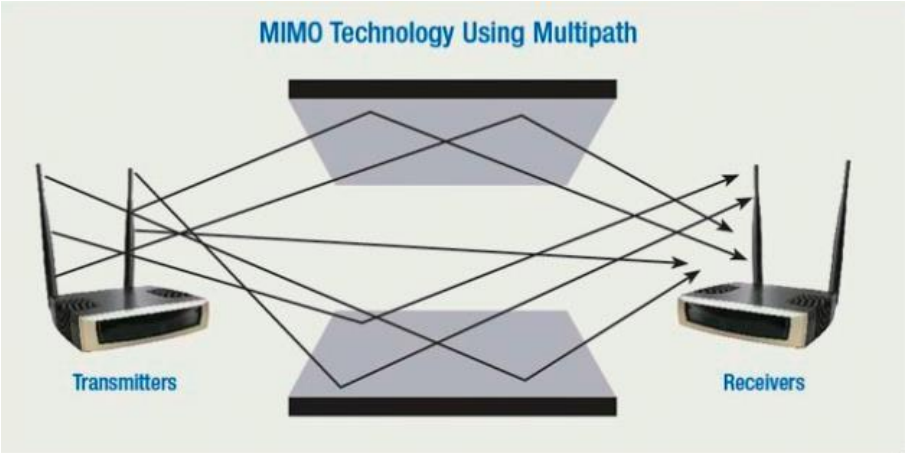


Figure 22 FUNCIONAMIENTO DE TECNOLOGÍA MIMO (GARCIA, 2015)

2.2.8 MAESTRO Y ESCLAVO

El sistema Maestro y esclavo es un protocolo de comunicación en el cual tenemos un dispositivo que hace una función principal y envía órdenes previamente programadas a un dispositivo esclavo, el cual se encarga de ejecutar y a la vez enviar y recibir datos a su maestro.

Al hablar de maestro y esclavo podemos decir que el nodo “maestro” es aquel que asume el control de acceso en términos de intercambio de información de datos. Si hablamos de “esclavo” es aquel que ejecuta las órdenes recibidas por el nodo maestro. (ANDRANGO, 2007)

Una de las ventajas que tenemos al utilizar este tipo de conceptos es la simplicidad, el tiempo de latencia que tiene el bus para poder enviar y recibir información. (ANDRANGO, 2007)

Para hablar de una manera más precisa, el maestro administra la red y actúa de mediador, de esta forma pregunta a cada dispositivo conectado al mismo (esclavo) para ver si necesita realizar alguna reacción, si este es el caso, el mismo la enviará y el nodo o dispositivo esclavo responderá a esas peticiones. (Pineda, 2015)

A continuación, mostraremos un diagrama de la secuencia que sigue el “maestro” y “esclavo”.

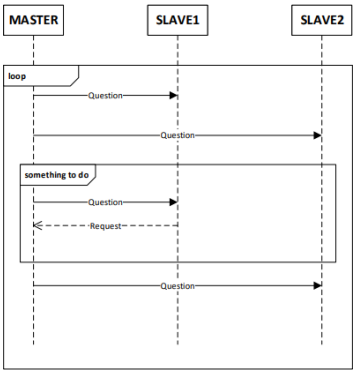


FIGURE 23 DIAGRAMA DE SECUENCIA MAESTRO-ESCLAVO (GARCIA, 2015)

2.2.9 VIDEOVIGILANCIA

Según la definición del artículo científico tomado, la videovigilancia se refiere a la tecnología con la finalidad de observar, detectar, copiar o registrar movimientos, imágenes, sonidos o el estado de una persona. Esta es utilizada para la erradicación de la violencia, la seguridad de las personas y de bienes materiales, todo esto sirve para poder grabar imágenes y sonidos, es utilizada tanto en lugares públicos debido a que la ley lo permite y en lugares privados, dependiendo de su requerimiento. (FERNANDO BANDÉS, 2009)

2.2.9.1 TIPOS DE SISTEMAS DE VIDEOVIGILANCIA

Existen diversos tipos de sistemas de videovigilancia, desde los completamente analógicos, hasta los completamente digitales. A continuación, hablaremos sobre ellos para evaluar sus ventajas y desventajas.

2.2.9.1.1 SISTEMAS DE CCTV ANALÓGICOS

Este sistema utiliza cámaras analógicas que se conectan a un reproductor de video (VCR) para poder guardar la grabación. Estas cámaras se conectan mediante un cable coaxial y sus grabaciones duran alrededor de ocho horas ya que no se utilizan funciones de compresión de video. (Toro, 2015)

A continuación, en la figura 24 se muestra un sistema CCTV análogo.

FIGURE 24 SISTEMA CCTV ANALÓGICO (Toro, 2015)

2.2.9.2 SISTEMAS DE VIDEO DE RED

Este tipo de cámaras tienen una conexión de red donde su video es transportado mediante una vía haciendo uso de una IP, todo lo que se graba es guardado en un servidor que viene de la mano de un software el cual permite su gestión.

En la figura 25 podemos apreciar que este sistema es totalmente digital, ya que no posee elementos analógicos.

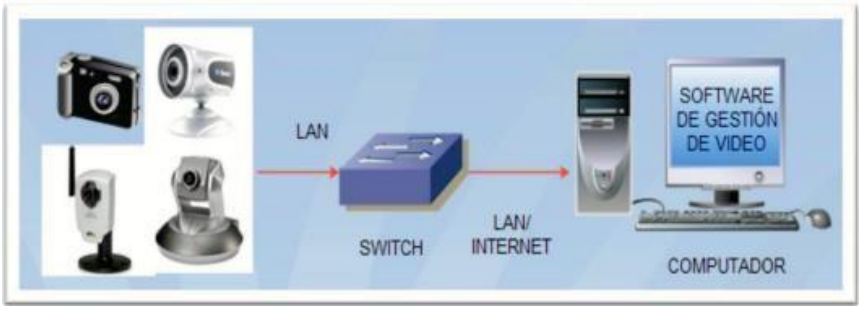


FIGURE 25 SISTEMA CCTV DIGITAL (Toro, 2015)

2.2.10 CÁMARAS DE VIGILANCIA

Las cámaras de vigilancia son aquellas que captan videos de manera profesional, las cuales proveen una imagen de alta calidad, debido a esto son robustas y fiables, capaces de durar años. Existen diversos tipos de cámaras de vigilancia lo cual permite una adecuación pertinente sea el caso. Estas cámaras son utilizadas para disuadir el robo de agentes externos a un establecimiento o inclusive a los agentes internos. Al mantener una imagen clara de las personas que transitan por dicho edificio podemos salvaguardar los bienes materiales y en algunos casos extremos salvaguardamos la vida de las personas que se encuentran dentro de la misma. (ZAPATA, 2014)

2.2.10.1 TIPOS DE CÁMARAS

En la actualidad se han desarrollado diversas técnicas de grabación y compresión, gracias a esto se pueden transmitir señales de audio y video mediante redes LAN y WAN.

Existen diferentes tipos de cámaras y se debe tener en cuenta el contexto o situación en la cual la vamos a utilizar, entre los diferentes tipos de cámaras tenemos:

2.2.10.1.1 CAMARAS DE INTERIOR

Estas cámaras son las más básicas, sencillas y económicas que podemos encontrar, las mismas no necesitan una carcasa robusta o visión nocturna ya que su uso es en aquellos lugares en donde la iluminación está presente constantemente. (ZAPATA, 2014)

FIGURE 26 CÁMARA DE INTERIORES (unnotekno.com, 2023)

2.2.10.1.2 CÁMARAS CON INFRARROJO

Este tipo de cámaras son muy utilizadas en lugares con poca iluminación, una característica especial que tienen es que a horas en donde la luz es escasa, se activa automáticamente una “visión nocturna” la cual permite grabar en blanco y negro, mientras que cuando hay iluminación estas graban a todo color normalmente. (ZAPATA, 2014)

Este tipo de cámaras en específico, poseen lentes los cuales permiten detectar un cambio mínimo de temperatura, adicionalmente poseen un campo de visión distinto a las demás cámaras.

En la figura 24 observamos el campo de visión y funcionamiento del lente para detectar los cambios de temperatura.

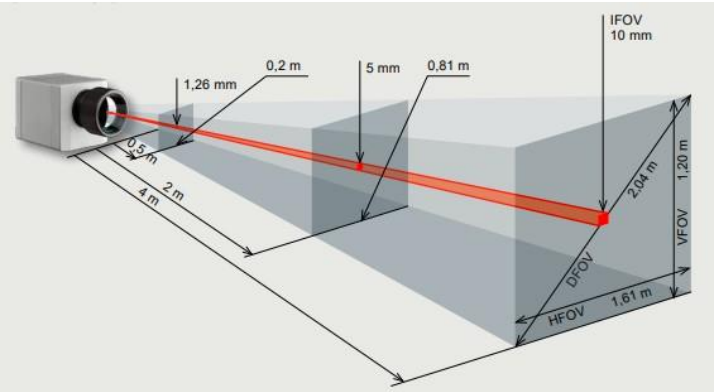


FIGURE 27 CÁMARAS CON INFRARROJOS (Optris, 2022)

2.2.10.1.3 CÁMARAS ANTI VANDALICAS

Una de las características principales de este tipo de cámaras es la carcasa que tienen, debido a que son robustas son perfectas para grabar lugares en donde hay mucho tránsito, debido a esto las cámaras comunes y corrientes son expuestas a robos o agresiones a las mismas. (ZAPATA, 2014)

Otra característica de estas cámaras son los MP, la compresión, la iluminación, entre otras. Cabe recalcar que estas cámaras son resistentes a exteriores y son ideales para ambientes desafiantes.

FIGURE 28 CÁMARA ANTI VANDÁLICA (VICON, 2023)

2.2.10.1.4 CÁMARAS IP

Este tipo de cámaras son de las más completas que existen en la actualidad, debido a que se conectan directamente al internet y muestran imágenes del lugar donde se encuentra colocada. Cabe recalcar que con este tipo de cámaras podemos utilizar el móvil o computadora para ver la escena de grabación desde cualquier parte del mundo. (ZAPATA, 2014)

FIGURE 29 CÁMARA IP (FOSCAM, 2011)

2.2.10.1.5 CÁMARAS CON MOVIMIENTO Y ZOOM

Este tipo de cámaras son perfectas para instalaciones de CCTV que tienen una persona monitoreando las cámaras o para superficies grandes que se mantienen en constante vigilancia siguiendo una ruta específica de movimiento. (ZAPATA, 2014)

FIGURE 30 CÁMARA CON MOVIMIENTO Y ZOOM (trendnet, 2023)

2.2.10.1.6 CAMARAS OCULTAS

Estas cámaras pueden ser colocadas en algún lugar y graban con una gran discreción, estas son conocidas como cámaras espías. Este tipo de cámaras son de un tamaño minúsculo y suelen colocarse en sensores de movimiento, sensores de humo, espejos, entre otros. (ZAPATA, 2014)

FIGURE 31 CÁMARA ESPÍA (MANUALS, 2022)

Una vez explicada brevemente las características y funcionamiento de las cámaras, podemos optamos por dos opciones entre las cuales tenemos, cámaras con movimiento y cámaras IP.

En la actualidad existen las llamadas “cámaras robóticas” o “cámaras PTZ”, las cuales poseen apps para su configuración y control, adicionalmente estas cámaras poseen conexión Wireless y su campo de visión es de 360 °.

A continuación, hablaremos a fondo sobre la cámara a utilizar, sus caracterizas, usos, ventajas y desventajas.

2.2.10.2 CAMARA ROBÓTICA PTZ

Este tipo de cámara de videovigilancia tienen diversas cualidades, entre ellas esta que poseen distintos métodos de comunicación, van desde sistemas cableados para conectarse a internet hasta protocolos como el ONVIF el cual utilizamos para la comunicación con el servidor.

Esta cámara PTZ (Pan, Tilt, Zoom) es la más adecuada para el monitoreo constante del edificio, a continuación, en la tabla número 12 mostraremos las características técnicas que posee la cámara seleccionada.

Características	
COMUNICACIÓN	Posee protocolos como ONVIF, comunicación cableada mediante RJ45 y comunicación inalámbrica, fácil comunicación con app (Carecampro), P2P
GENERALIDADES	Posee sensor de movimiento, zoom, Entrada de audio con micrófono incorporado, protección IP66
CARACTERISTICAS DE VISION	Esta cámara posee un angulo de visión de 83°, resolución de grabación de 1080P, compresión H264, 5 Mp, distancia de visión nocturna 30 m
COMPATIBILIDAD CON SISTEMAS	Es compatible con sistemas IOS, Android, adicionalmente es compatible con navegadores como Safari, Google Chrome, Internet explorer
GRABACION Y ALMACENAMIENTO	Esta cámara posee puertos para memoria SD (soporta una tarjeta de 128 Gb), almacenamiento contratado en la nube

TABLA 18: CARACTERISTICAS DE CAMARA PTZ

2.2.10.1 COMUNICACIÓN DE CAMARAS PTZ

Una vez mencionadas las características principales de las cámaras PTZ, procedemos a explicar la comunicación que estas cámaras poseen.

Entre las cámaras PTZ tenemos diferentes tipos de comunicación y conexión, entre las más comunes están:

- Comunicación por puerto RS485
- Comunicación mediante protocolo ONVIF
- Comunicación mediante puerto RJ45

En la tabla número 13, explicamos las características que tienen cada una de estas comunicaciones.

COMUNICACIÓN POR PUERTO RS485	COMUNICACIÓN MEDIANTE PROTOCOLO ONVIF	COMUNICACIÓN MEDIANTE PUERTO RJ45
Utiliza un software especial como RS485 Data Logger	Su comunicación es inalámbrica	Mantenimiento sencillo
Se basa en la normativa EIA/TIA 485	Utiliza protocolos de seguridad basados en su IP	Su comunicación es cableada
Su comunicación es mediante un cable par trenzado	Facilita integración de distintas marcas de equipos de video	Tiene un mayor rendimiento
La distancia máxima de comunicación es de 1200 metros	Fácil instalación y configuración	No es compatible con varios sistemas
No puede transmitir y recibir datos al mismo tiempo	Puede enviar y recibir datos al mismo tiempo	Dificultad para localizar daños
Su velocidad de transmisión es alta	Almacenamiento de video sencillo	Su distancia de transmisión es menor a 80 metros debido a las perdidas

TABLA 19: CARACTERISTICAS DE LAS COMUNICACIONES QUE POSEEN LAS CAMARAS PTZ

2.2.11 SENSORES

Una definición formal de los sensores es el equipo o dispositivo el cual se encarga de proporcionar una acción o respuesta a algún estimulo, una señal física o inclusive a una señal química. Es considerado en la actualidad un elemento muy importante no solo en el campo de la domótica, sino también en otros campos, ya que existen una gran variedad de los mismos. (ARENY, 2005)

Los sensores son elementos que miden parámetros frecuentes en el lugar a vigilar o a ubicar como lo son: humos, temperatura, movimiento, gases, humedad e iluminación. A continuación, en la tabla número 14 se muestran las aplicaciones que tienen los sensores en la domótica.

TIPOS DE SENSORES	CARACTERÍSTICAS	APLICACIONES
SENSORES DE HUMO	Precisión en la alerta de humo y calor Se basan en la normativa CE	Este tipo de sensores es utilizado en conductos de aire (viviendas, centros comerciales, supermercados, cárceles o bodegas).
SENSORES DE GAS	Poseen electrodos 2 los cuales tienen propiedades catalíticas para su reacción química Existen sensores para distintos tipos de gas (Dióxido de carbono, Propato, butano)	Se instalan en talleres de soldadura, plantas nucleares (dependiendo del tipo de sensor de gas). A su vez existen sensores de gas que pueden ser instalados en el hogar (sensores de gas LP)
SENSORES DE PRESENCIA	Algunos trabajan de los sensores trabajan de forma distinta. Su detección es mediante línea de vista	Estos sensores son los más comunes en los hogares, pueden ser instalados en Bancos, Centros comerciales, entre otros lugares concurridos.
SENSORES DE LUMINOSIDAD	No es necesario tener contacto con el objeto a medir Son ajustables en el rango de medición de luz	Empresas en general Industrias dedicadas a la electrónica Bancos Universidades Hogares

TABLA 20: SENSORES Y SUS APLICACIONES

2.2.11.1 SENSORES EN LA DOMOTICA

En el campo de la domótica se utilizan una gran variedad de sensores, los mismos que cuentan con una característica especifica debido a lo que van a medir, entre las que tenemos dos: (Gijón, 2018)

Características estáticas: Son aquellas que describen el comportamiento del sensor en base a cambios según sea la variable a medir.

En la tabla número 15 se presentan las variables a medir y la definición de los mismos.

CARACTERISTICAS	DEFINICION Y USOS
Resolución	Esta variables es configurable y se comporta como un máximo y mínimo a medir, la encontramos en sensores de Luz, temperatura.
Precisión	Esta variable es un aproximado, ya que el sensor cuenta con una salida real y una ya configurada que es llamada salida teórica, esto aplica en sensores de gas, humedad, entre otros.
Linealidad	Son aquellos que se basan en una posición dada para enviar información, un claro ejemplo de linealidad serían los sensores lineales.
Sensibilidad	Esta variable depende de la magnitud de entrada, ya que si es mayor el sensor se comportará más sensible, un claro ejemplo es el sensor de movimiento, tanto en cámaras de celulares y videocámaras.
Ruido	Esta variable depende de perturbaciones en el sistema. Entre los principales aparece en sensores de imagen, sensores de sonido, entre otros.

TABLA 21: CARACTERISTICAS ESTATICAS DE LOS SENSORES

Características dinámicas: En este caso los sensores muestran una actuación en base transitoria, esto es debido a estímulos de magnitud física que se le dan, entre ellos.

En la tabla número 16, mencionamos los 4 tipos de características dinámicas de los sensores y su definición.

CARACTERISTICAS	DEFINICION Y CARACTERISTICS
Tiempo de respuesta	Es aquel tiempo que pasa desde la entrada de la señal hasta su salida, el valor correspondiente es del 96% (MecatrónicaLATAM, 2021)
Constante de tiempo	Es el tiempo que tarda en actuar por los cambios en la entrada, la mayoría de sensores actuar en cuestión de ms. (MecatrónicaLATAM, 2021)
Tiempo de levantamiento	Tiempo que se requiere para lograr una salida en un estado estable (MecatrónicaLATAM, 2021)
Tiempo de asentamiento	Tiempo que tarda en alcanzar un valor establecido (cabe recalcar que depende de la configuración del sensor) (MecatrónicaLATAM, 2021)

TABLA 22: CARACTERISTICAS DINAMICAS DE LOS SENSORES

2.2.11.2 TIPOS DE SENSORES EN LA DOMÓTICA

Existen diferentes tipos de sensores en la domótica, estos son aquellos que se encargan de recopilar información para luego ser procesada y ejecutar alguna acción en específica, entre los más comunes y principales tenemos. (PENTADOM, s.f.)

En la tabla número 17, se hablan de los sensores más comunes en la domótica y su uso.

SENSORES	USO
Sensor de climatización	Este tipo de sensor se encarga de medir la humedad en el ambiente que no supera el 55% y no está por debajo de 25% (Ventilación, 2022)
Sensor detector de humo	Este tipo de sensores creció de manera rápida desde el 2020 y se prevé un CAGR del 8.3% en el 2026, Este tipo de sensores son los encargados de detectar incendios tempranos en varios lugares. (mordorintelligence, mordorintelligence, 2021)
Sensor de color	Según estudios, estos sensores tendrán un CAGR del 8.63% (mordorintelligence, mordorintelligence, 2021)
Sensor de movimiento	En base a estudios realizados, se espera que los sensores de movimiento tengan un aumento en su uso del 6.5%. (mordorintelligence, mordorintelligence.com, 2021)

TABLA 23: TIPOS DE SENSORES EN LA DOMOTICA Y SU USO

CAPÍTULO III

DESARROLLO DE LA PROPUESTA

3.1 COMPONENTES DE LA PROPUESTA

En el capítulo III, una vez explicado los distintos modelos y las características de los posibles elementos y dispositivos a utilizar, seleccionaremos uno en específico que cumpla con los requisitos y se adapte de mejor manera al edificio del INCYT.

Entre los dispositivos principales que vamos a utilizar para cumplir con la comunicación Z WAVE y ONVIF son los siguientes.

- Raspberry PI 3 B+
- USB z stick gen 5
- Sensor FIBARO
- Cámaras PTZ

3.1.1 CONTROLADOR RASPBERRY PI 3 MODELO B+

En el capítulo anterior, nombramos varias tarjetas controladoras, las cuales tenían diferentes funciones y aplicaciones, luego de mencionar sus características y ventajas se optó por trabajar con el controlador "Raspberry PI 3 B+", ya que con este elemento podemos cumplir con los requisitos necesarios para formar la interconexión de los equipos y hacer uso del protocolo Z wave, con la ayuda de un dispositivo que funcionará como Gateway el cual explicaremos con más detalles a lo largo del capítulo.

La tarjeta utilizada para crear el servidor Home Asistan es la Raspberry Pi 3 Modelo B+ ya que cuenta con un procesador de cuatro núcleos de 64 bits que trabajan a una frecuencia 1,4 GHz. Esta tarjeta funciona a doble banda (2,4 GHz y 5 GHz), esta tarjeta se escogió debido a que se pensó en futuras generaciones que quieran

utilizar otro tipo de protocolos de comunicación con estos equipos (Zigbee). (raspberrypi.org)

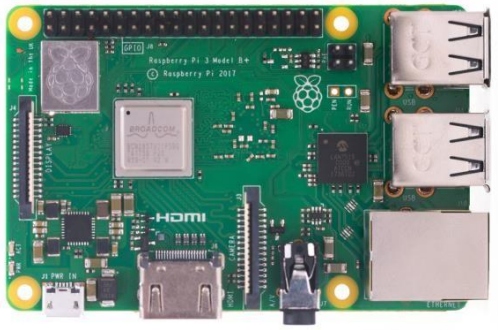


Figure 32 RASPBERRY PI 3 MODELO B+ (RASPBERRY, 2022)

3.1.1.1 CARACTERISTICAS RASPBERRY PI 3 MODELO B+

A continuación, en la tabla número 18 mostraremos las características principales por el cual esta tarjeta fue la elegida para realizar la implementación del sistema.

Características	
MARCA	Raspberry PI 3
CONECTIVIDAD	Bluetooth Doble banda Cuatro puertos USB Puerto Gigabit Ethernet (300Mbps max)
VOLTAJE DE ENTRADA	Micro USB a 5 y 2.5 V
ACCESOS	40 Pines GPIO
COMPATIBILIDAD CON TARJETAS SD	Es compatible con micro SD
VIDEO Y SONIDO	Puerto HDMI Puerto de cámara

TABLA 24: CARACTERISTICAS DEL RASPBERRY PI 3 MODELO B+

3.1.2 COMUNICACIÓN Z WAVE CON RASPBERRY

Para poder realizar la comunicación con el protocolo Z wave entre el Raspberry y los sensores a utilizar, se debe utilizar un dispositivo intermediario que funcione como Gateway, esto es debido a que Raspberry no cuenta con una interfaz Z wave, debido a esto se hará uso del dispositivo USB Z-Stick Gen 5. Todo esto es posible gracias a las librerías que se pueden utilizar con este protocolo, las cuales son conocidas como “OpenZWave”

3.1.2.1 OPEN Z WAVE

Open Z Wave es un conjunto de librerías que mantienen un código abierto el cual trabaja en el lenguaje de programación C++. El fin de esto es dar el soporte a la comunicación con varios dispositivos z wave sin tener conocimiento avanzado sobre esta tecnología, dicho en otras palabras, estas librerías nos ayudan a mantener una conexión sencilla con los dispositivos y el servidor.

A continuación, en la tabla número 25 mencionaremos la compatibilidad que existe entre los controladores USB y OpenZWave

FABRICANTE	TIPO DE CONEXIÓN
Tricklestar	USB
ACT ZCS101	RS232
Z toller	RS232
Aeon Zstick	USB
Seluxit Viasens	USB
Z wave.me Z stick	USB

TABLA 25: COMPATIBILIDAD ENTRE OPENZ WAVE Y CONTROLADORES USB (Solís, 2014)

Como podemos ver en la tabla anterior, los distintos modelos poseen tipos de conexión, en el caso tenemos RS232 y USB, para el caso del presente proyecto, nuestro raspberry PI elegido posee puertos USB, entonces entre los distintos fabricantes se optó por el AEON ZSTCIK, a continuación, hablaremos sobre las características que este posee.

3.1.2.1 ¿QUÉ ES EL USB AEON Z-STICK GEN 5?

Este dispositivo es un adaptador USB desarrollado para controlar actuadores y sensores mediante el protocolo Z wave. Este dispositivo posee tres modos de funcionamiento, entre los cuales tenemos: modo inclusión, modo de eliminación y modo Serial API. (aeotec.freshdesk, 2022)

FIGURE 33 AEOTEC Z-STICK GEN 5 (AEOTECH, 2023)

3.1.2.2 CARACTERÍSTICAS Z STICK GEN 5

A continuación, en la tabla número 20 mostraremos las especificaciones y características de este dispositivo USB utilizado.

NOMBRE	Z-STICK GEN 5
MODELO	ZW090
ALIMENTACION	USB de 4,75 V a 5,25 V Batería de litio recargable
CORRIENTE MAXIMA DE FUNCIONAMIENTO	98 mA en modo PA 40 mA en modo normal
NODOS MAX Z WAVE	232 dispositivos
POTENCIA DE TRANSMISION	2,91 dBm
DISTANCIA DE FUNCIONAMIENTO	150m aire libre 400m en exteriores modo PA 75m en interiores con megafonía

TABLA 26: CARACTERISTICAS DEL USB Z-STICK GEN 5

3.1.3 SENSOR DE MOVIMIENTO FIBARO Z-WAVE PLUS FGMS-001 ZW5

Para detección de movimiento, utilizaremos el sensor FIBARO compatible con el protocolo de comunicación Z wave, este sensor permite monitorear temperatura, movimiento, luz y vibración.

Este sensor una vez conectado a la puerta de enlace mencionada anteriormente, emitirá notificaciones por mensaje de texto o correo electrónico si el sensor detecta un movimiento inesperado en las instalaciones.

FIGURE 34 SENSOR FIBARO Z-WAVE PLUS (FIBARO, www.fibaro.com, 2023)

Como podemos observar en la figura 34, el dispositivo se compone de un circuito de trabajo, una bacteria de alimentación y un sensor, el cual es multi función,

adicionalmente su carcasa en forma circular la cual ayuda al campo de detección, a continuación, explicaremos su funcionamiento.

3.1.3.1 FUNCIONAMIENTO DEL SENSOR FIBARO Z WAVE PLUS

Este modelo de sensor trabaja de manera que ayuda a detectar la temperatura, el movimiento y la intensidad de luz del lugar en donde se lo instala, este sensor posee sensibilidad ajustable, lo cual permite ser adaptado a distintos lugares del hogar, en el caso del proyecto se lo colocó dentro del edificio del INCYT.

Adicionalmente, la forma de “ojo” de este sensor ayuda a la detección de algún intruso según sea configurado, emitiendo una alerta en aplicaciones o servidores, ya que su tecnología es compatible con aplicaciones o configurable con servidores como el caso del presente proyecto.

3.1.3.2 DETECCION Y AREA DE TRABAJO DEL SENSOR

Para la instalación se recomienda hacerla en una esquina de la habitación, ya que posee un buen campo de visión y detección, a continuación, en la figura número 35 se puede apreciar el rango en el que trabaja este sensor.

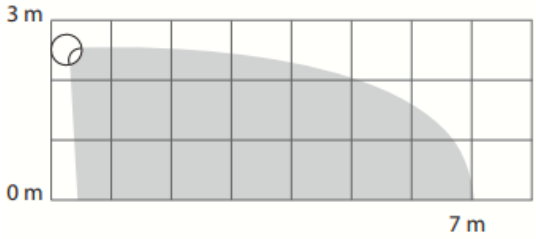


Figure 35 RANGO FRONTAL DE TRABAJO DEL SENSOR FIBARO (FIBARO, manuals.fibaro.com, 2014)

Como podemos observar, el rango de trabajo de este sensor es de 3 metros de alto y 7 metros de largo, lo cual es conveniente ya que las habitaciones promedias mantienen esas dimensiones, para el edificio del INCYT se analizaron distintos puntos estratégicos para la colocación de estos sensores y se optó por

colocarlos de modo que detecte con mayor facilidad las ventanas ya que estas conectan las oficinas con el exterior y no se encuentran aseguradas.

En la figura número 36 observamos cómo sería el área de trabajo del sensor en una oficina promedio.

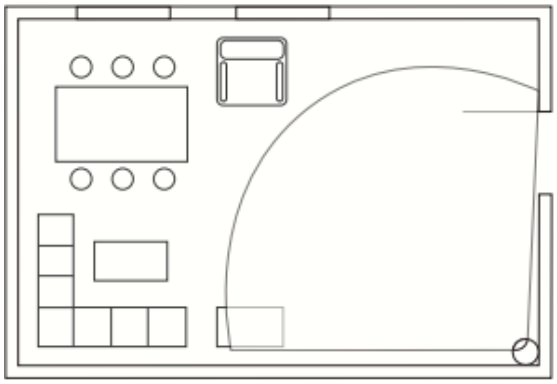


Figure 36 AREA DE TRABAJO DEL SENSOR EN OFICINA PROMEDIO (FIBARO, manuals.fibaro.com, 2014)

Como podemos observar, el sensor cubra una buena área de la oficina, cabe recalcar que este sensor debe ser colocado en dirección la cual el ingreso a la oficina sea totalmente cubierto, tal y como se muestra en la figura anterior.

3.1.3.3 CARACTERÍSTICAS SENSOR FIBARO Z WAVE PLUS

El modelo de sensor utilizado posee varias características las cuales fueron importantes al momento de elegirlo, entre ellas está, la vida útil, la comunicación, entre otras.

A continuación, en la tabla número 27, se presentan las características principales del sensor “FIBARO Z WAVE PLUS”.

Características	
NOMBRE	Fibaro z-wave plus
FRECUENCIA DE ONDA Z	908, 42 MHz
ALIMENTACION	1 pila de 3,6 V
RANGO DE DETECCION DE MOVIMIENTO	23 pies
TEMPERATURA DE FUNCIONAMIENTO	(0- 40 °C)
RANGO DEL SENSOR DE TEMPERATURA	Mide -4 °F (-20 °C) a +212 °F (100 °C)
RANGO DEL SENSOR DE LUZ	0–32000 LUX
ALCANCE INALÁMBRICO	30 metros

TABLA 27: CARACTERISTICAS DEL SENSOR FIBARO Z WAVE PLUS

3.1.4 CAMARA IP WIFI EXTERIOR ROBÓTICA 1080P HD 8 LEDS SEGURIDAD MICRÓFONO

Para la parte del monitoreo o vigilancia del edificio, utilizamos la cámara IP para exteriores, precisamente como características la movilización remota mediante el celular, detección de audio, alertas de detección y wifi, siendo compatible con la red y cumpliendo la función de vigilar y alertas si sucede alguna anomalía en el edificio.

Este tipo de cámaras son PTZ y poseen diferentes características, las cuales explicaremos a continuación, debido a esto fue la seleccionada.

- Medio de la cámara (exteriores o interiores)
- Sensibilidad a la luz

- Resolución
- Tipo de lente
- Funcionamiento en la red

Estas 5 características fueron las claves para poder elegir esta cámara ya que debido al lugar a colocar era la precisa.

3.1.4.1 MEDIO DE LA CAMARA PTZ

Debido a que las cámaras de seguridad eran necesarias en la parte externa de las instalaciones del INCYT, la cámara tenía que soportar intemperie y debe tener funcionalidad con todos estos cambios. La cámara que se colocó tiene protección IP66 y es perfecta ya que es aprueba de agua, precisa para días lluviosos.

A continuación, en la figura número 37 podemos apreciar las partes que tiene la cámara PTZ colocada.

Figure 37 AREA DE TRABAJO DEL SENSOR EN OFICINA PROMEDIO (SHOP, 2023)

3.1.4.2 SENSIBILIDAD A LA LUZ

Para la elección del modelo de cámara a colocar se tuvieron en cuenta varios aspectos en cuanto a la sensibilidad a la luz se refiere, la cámara debe funcionar de una manera óptima en el día y en la noche. Actualmente existen distintos formatos (tamaño de la porción utilizable del sensor), entre los cuales están 2/3”, 1/2”, 1/3”,1/4”. El formato que se eligió para el sensor es el 1/4” ya que su campo de vista se encuentra desde 27 hasta 72 mm, de esta manera podemos evitar alguna distorsión en el campo de visión de cámara.

3.1.4.3 RESOLUCIÓN

En cuestión a resolución, tenemos distintos puntos de vista, en el campo de la videovigilancia se considera optimo el rango entre 70 a 100 pixeles. Como buscamos la seguridad del edificio y queremos identificar rostros de personas, optamos por una resolución alta, la cual posee la cámara instalada, ya que cuenta con 2 megapíxeles, lo cual permite identificar de mejor manera al sujeto que la cámara detecte, adicionalmente debido a esta alta resolución que tiene, la cámara viene con sensores de detección de movimiento y detección humana, incluye un zoom de 4x máximo.

3.1.4.4 TIPO DE LENTE Y DISTANCIAL FOCAL

Existen diversos tipos de lentes en las cámaras de videovigilancia, en el caso de la cámara que se colocó en el edificio, es el lente auto iris, este lente va de la mano con el sensor de imagen que este modelo de cámara posee, ya que la cantidad de luz que recibe el mismo se ajusta automáticamente. Gracias a esto la calidad de imagen será la más óptima y el sensor se encontrará seguro cuando la luz del sol sea intensa ya que se encuentra en el exterior

Cabe recalcar que cada modelo de cámaras tiene una distancia focal distinta, en este caso realizamos una ecuación para poder identificar la que necesitamos.

$$Longitud\ Focal = \frac{Distancia\ x\ Formato\ de\ la\ camara}{Objeto}$$

Para utilizar la ecuación, le damos valores estándar, el formato elegido fue de ¼" el cual tiene como medidas 3,6 mm en horizontal y 2,7 mm en vertical.

3.1.4.5 FUNCIONAMIENTO EN LA RED Y COMUNICACIÓN

Este modelo de cámaras posee varias funciones en cuanto a comunicación y red se refiere, a continuación, en la tabla número 22 vamos a colocar las características principales que la cámara posee.

Características y funciones	
Alimentación	Esta cámara se alimenta a través de puerto POE bajo el estándar 802.3af
Seguridad	Utiliza DHCP cifrada con HTTPS
Comunicación	Posee comunicación cableada por cable de par trenzado o comunicación inalámbrica
Conectores	Estos conectores permiten la entrada y salida de datos
Protocolo de comunicación	Posee protocolo ONVIF
Topología	Se pueden implementar en topología de bus o topología estrella.

TABLA 28: CARACTERISTICAS DE LA CAMARA PTZ COLOCADA

3.1.5 ROUTER A UTILIZAR

Para poder brindarle conexión a internet a nuestro servidor instalado en el raspberry, debemos crear una red interna en el edificio, para esto hacemos uso de un Router, esto para conectar de manera cableada nuestro servidor a internet y ejecutar el protocolo z wave de manera satisfactoria y para conectar de manera inalámbrica las cámaras y ejecutar el protocolo ONVIF. El modelo del router que se utilizó es el TP link TL-WR840N.

La ventaja de este router es que tiene diferentes métodos de configuración, entre los cuales están:

- Modo Router
- Modo Access Point
- Modo extensor o repetidor
- Modo WISP

A continuación, en la imagen número 38, presentamos la conexión de cada modo.

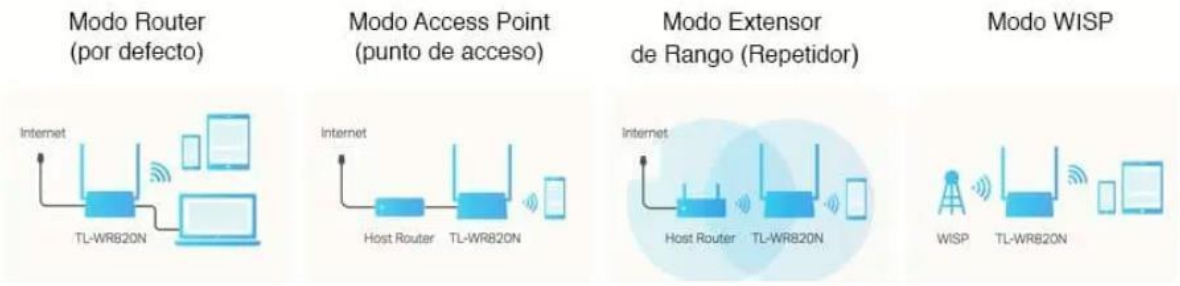


Figure 38: MODOS DE OPERACIÓN DEL ROUTER TP LINK TL-WR820/840 N

Para el sistema instalado en el edifico del INCYT se utilizó el modo Router, esto porque nos comunicamos directamente a los dispositivos instalados sea inalámbricamente con el protocolo ONVIF o de manera cableada con el controlador Raspberry.

A continuación, en la tabla número 29, se presentan las características y definiciones de cada modo de operación del router.

MODO DE OPERACION	DEFINICION Y APLICACIONES
Modo Router	Este modo de operación es el que viene por defecto y se conecta a internet para poder utilizar el router de manera normal, es decir de manera inalámbrica o cableada. Este modo comparte funciones como Qos, ancho de banda, NAT, VPN e IPV6
Modo Access Point	El Modo Access Point es para conectar dispositivos de manera inalámbrica, esto se utiliza para cubrir grandes áreas de conexión que tengan una distancia de 30 a 100 metros
Modo extensor de rango	Este modo del router permite replicar una señal WIFI y alargar su alcance , entre las velocidades más habituales esta 300Mbps.
Modo WISP	Este modo es especial en su uso ya que sirve para instalar el servicio de internet en los distintos hogares, el router crea una subred privada para poder configurarla y manipularla, cabe recalcar que la conexión no es cableada sino mediante wifi

TABLA 29: CARACTERISTICAS DE LOS MODOS DE OPERACIÓN DEL ROUTER TL-WR840N

3.2 COMPONENTES Y COMPLEMENTOS DE IMPLEMENTACION

Una vez mencionadas las características y funciones de los dispositivos principales del proyecto, vamos a nombrar los componentes, elementos y complementos extras que vienen de la mano para poder implementar los equipos antes mencionados.

Como mencionamos en el capítulo I el proyecto se dividía en dos partes, la primera es la simulación y la segunda la implementación.

Para la parte de simulación se tomaron fotos y se utilizó el programa Sketchup, gracias a este programa podemos visualizar de manera digital el edificio y de esta manera colocar las cámaras y los sensores en el lugar más óptimo tomando a consideración lo explicado en el capítulo II, ángulos, distancia focal, distancia de trabajo, entre otros.

Para la parte de implementación utilizamos distintos elementos, a continuación, en la tabla número 30 se presentan los principales y sus funciones.

ELEMENTOS UTILIZADOS	**PORCENTAJE Y APLICACION**
Home Assistant	Como servidor de nuestro sistema domótico utilizamos la plataforma Home Assistant, esto gestiona el 100% de nuestra implementación, ya que es el centro de operaciones del servidor.
Protocolo de comunicación ONVIF y Z wave	Para ejecutar estos protocolos en nuestro servidor, utilizamos complementos tales como Z wave Js y ONVIF que se encuentran en el catálogo de Home Assistant .
Alertas y automatizaciones	Para poder ejecutar y configurar estas alertas y automatizaciones, instalamos el complemento File Editor.
Acceso remoto al servidor	Para la comunicación y acceso remoto a nuestro servidor, utilizamos el protocolo IPV6
Puerto utilizados	Para el protocolo onvif se utilizó el puerto 580
App Fing	Es una aplicación, la cual permite leer que IPs se encuentran ocupadas en nuestra red

TABLA 30: ELEMENTOS UTILIZADOS EN LA IMPLEMENTACION DEL SISTEMA

Una vez mencionados los elementos principales con sus definiciones, vamos a explicarlos de manera más concreta, el uso que le dimos a cada uno de ellos y adicionalmente como influye en nuestro sistema de seguridad.

3.2.1 SOFTWARE HOME ASSITANT

Como hablamos en el capítulo II, teníamos dos sistemas que trabajaban de manera similar y eran el Domoticz y el Home Assistant. Entre las características que se buscaban era la compatibilidad con el protocolo Z Wave y Onvif, los cuales ambos poseían, se eligió la plataforma Home Asistan gracias a la facilidad de su interfaz, una vez configurado el servidor, creadas las interfaces de los sensores y cámaras, cualquier persona tenga o no conocimiento informático podrá acceder y ejecutar las diversas funciones.

Una clara diferencia que tiene Home Assistant con Domoticz es la configuración de código abierto que posee, ya que Home Assistant tiene acceso al código fuente de cada aplicativo, es decir, si nosotros queremos ejecutar distintas acciones bajo las reglas de Z wave u ONVIF podemos realizar alteraciones en el código que se encuentra en el lenguaje Python.

3.2.1.1 COMUNICACIÓN HOME ASSISTANT

Para la comunicación de la plataforma y los respectivos protocolos se utilizaron distintos dispositivos antes mencionados.

COMUNICACIÓN Z WAVE: Para esta comunicación se necesitó de dos elementos principales, la antena z wave antes mencionada “USB z Stick” y el complemento “z wave Js”.

Esta antena ejecuta ondas electromagnéticas que están entre 919.8 MHz y 921 MHz, debido a que estas ondas se encuentran en un rango distinto a las tecnologías utilizadas comúnmente en la UPSE, el envío y recepción de información

será mucho menor, ya que este fragmento del espectro radioeléctrico no se encuentra saturado.

A continuación, en la figura número 39 se presenta un diagrama para explicar la conexión física de nuestra antena y nuestro controlador.

Figure 39: CONEXIÓN FISICA ENTRE ANTENA Z WAVE Y CONTROLADOR

En la figura número 40 se presenta un diagrama explicando el funcionamiento que tiene la antena cuando se encuentra conectada.

Figure 40: GENERACION DE ONDAS DE RADIO DE 920 MHz

Como podemos observar nuestra antena z wave, genera ondas electromagnéticas constantes que se encuentran entre los 920 MHz, de esta manera no tendrá interferencias de dispositivos que trabajan a otras frecuencias como routers, celulares, entre otros.

Una vez creada nuestra red Z wave, tendremos espectro electromagnético libre para poder enlazar dispositivos que trabajen a esta frecuencia, en este caso los sensores elegidos.

A continuación, en la figura número 41 se presentan de manera más puntual el funcionamiento de nuestro sistema. Siendo el controlador nuestro Raspberry con la antena Z wave y los nodos que son nuestros sensores que trabajan en la misma frecuencia.

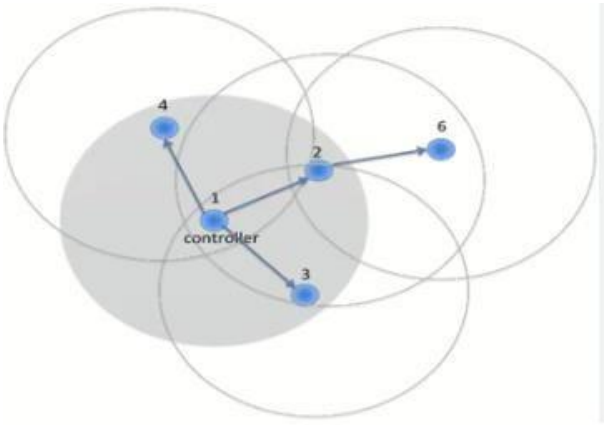


Figure 41: DIAGRAMA DE TRABAJO RED Z WAVE

3.2.2 PROTOCOLO ONVIF

Para la comunicación de las cámaras a nuestro Raspberry con el servidor Home Assistant, utilizaremos el protocolo ONVIF. Este protocolo es un estándar abierto que permite a diferentes dispositivos IP ser compatibles entre sí. Esta es una gran ventaja ya que nos proporciona flexibilidad a la hora de elegir los productos, por este motivo utilizamos el mismo, su instalación es sencilla, simplemente usaremos IP del dispositivo y el puerto del protocolo ONVIF que utiliza el mismo. (argos, s.f.)

El protocolo ONVIF trabaja en nuestra red creada mediante topología estrella, en el caso de las cámaras de videovigilancia las 4 cámaras se conectan al mismo router antes configurado.

A continuación, en la figura número 42 se muestra un diagrama de conexión entre las cámaras y nuestro servidor mediante IP.

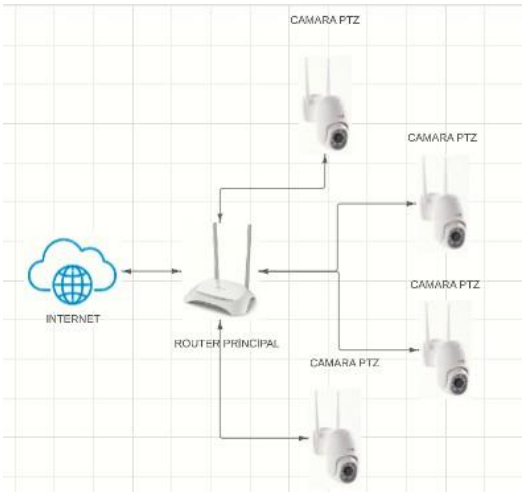


Figure 42: DIAGRAMA DE CONEXIÓN ENTRE LAS CAMARAS Y EL RPOUTER PRINCIPAL

Una vez conectadas las cámaras mediante IP, procedemos a utilizar el protocolo ONVIF para poder enlazarlas a nuestro Home Assistant. El protocolo se encarga de ejecutar funciones para que las cámaras compatibles ingresen a un solo servidor creado, en el caso del proyecto, la información de las cámaras de videovigilancia ingresan al servidor creado en nuestro raspberry.

A continuación, en la imagen número 43 se muestra un diagrama de conexión entre la información de video y audio a nuestro servidor mediante protocolo ONVIF.

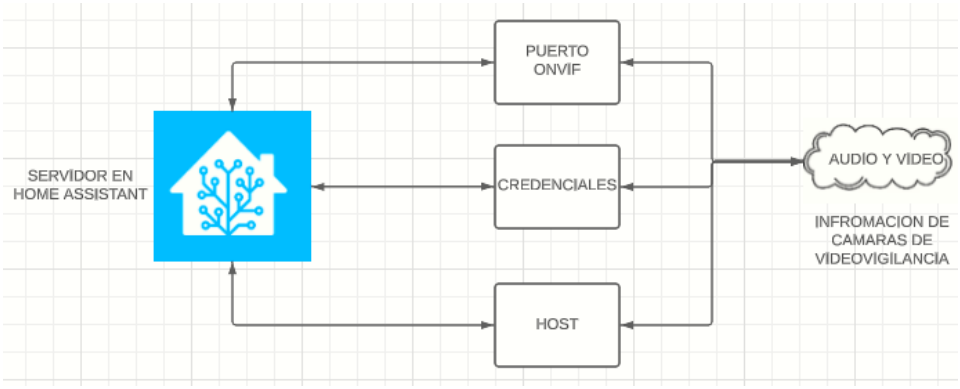


Figure 43: DIAGRAMA DE SEGUIMIENTO DE LA INFORMACION CAPTADA POR LAS CAMARAS HASTA EL SERVIDOR

Como podemos observar en la figura anterior, los datos viajan mediante dirección IP y pasan el puerto ONVIF que en este caso es el puerto 6688, colocando las credenciales enviamos nuestros datos al servidor.

3.2.3 DISEÑO ELÉCTRICO PARA ALIMENTACIÓN DE CÁMARAS DE SEGURIDAD

Para poner a funcionar el sistema de cámaras, necesitaremos conectarlas a la energía eléctrica, este es un trabajo adicional que se debe realizar, debido a que las edificaciones del Incyt no cuentan con energía eléctrica en las zonas en donde se colocarán las cámaras de seguridad, este tipo de cámaras mencionadas anteriormente trabajan con energía AC a 120 V, por este motivo haremos extensiones a cada uno de los puntos para poder ponerlas a trabajar.

A continuación, en la figura número 44 se presenta un esquema electrico sencillo, el cual es la base para la conexión externa de las cámaras de videovigilancia.

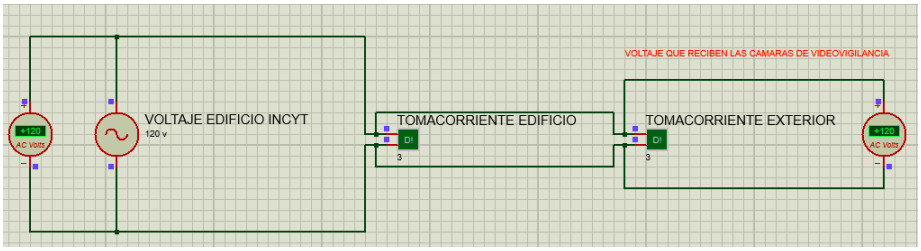


Figure 44: ESQUEMA ELECTRICO PRINCIPAL

Como podemos observar en la figura anterior, este es el esquema que se siguió para la instalación de las distintas extensiones eléctricas en cada punto, en el caso del presente proyecto fueron 4 puntos, los cuales se ubicaron en cada esquina del edificio.

Una vez teniendo en cuenta los puntos eléctricos y la conexión que se realiza, procedemos a colocarla en nuestra simulación en Sketchup.

A continuación, en la figura número 45, se presenta una captura de la simulación con los puntos de energía eléctrica que utilizan las cámaras de seguridad.

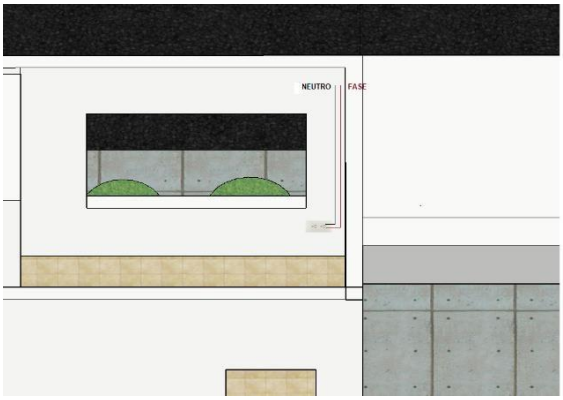


FIGURE 45: DIGITALIZACIÓN DE CABLES QUE SALEN DEL INCYT

En la figura anterior, se observa que el cable neutro y el de fase salen de un tomacorriente que se encuentra dentro de la oficina del INCYT, dichos cables alimentarán la extensión que se encuentra en la parte externa de las instalaciones.

A continuación, en la figura 46, se muestra la parte exterior de la instalación.

FIGURE 46: DIGITALIZACIÓN DE PUNTOS ELÉCTRICOS PARA CÁMARAS DE SEGURIDAD

Como podemos observar en la imagen anterior, la cámara se conecta directamente a un tomacorriente externo que se encuentra en una caja de paso para que la misma funcione de manera continua.

3.2.4 SOFTWARE SKETCHUP

Para ubicar de una mejor manera las cámaras de seguridad y los sensores, optamos por digitalizar la edificación del Incyt, en este caso, se digitalizó la planta baja, debido a que es la zona de entrada y la zona con más fácil acceso al lugar, ya que esta se encuentra descubierta tanto en la puerta de entrada y en las ventanas de la misma, dicho esto la planta alta de la edificación estará monitoreada por las cámaras de seguridad que nos permitirán tener una visión amplia del edificio controlando los 4 flancos de dicha edificación.

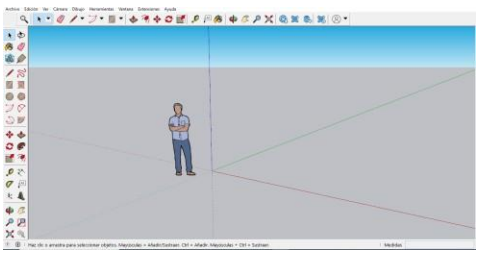


Figure 47 INTERFAZ SOFTWARE SKETCHUP

Una vez mencionado el software con el que se digitalizó la planta baja del edificio, procedemos a mostrar las perspectivas del plano simulado.

VISTA SUPERIOR DE LA PLANTA BAJA DEL INCYT

Como podemos apreciar en la figura número 48 la vista superior del edificio, las divisiones y distancias del mismos serán más sencillas de tomar, ya que en los capítulos II y III, se habló del rango de acción que tienen los sensores. Gracias a esto podemos tomar a consideración este rango y en base a la simulación, colocar el sensor de manera más óptima.

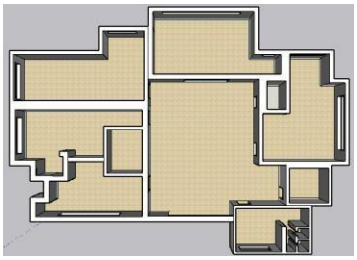


Figure 48 VISTA SUPERIOR DE LA PLATANA BAJA DEL INCYT

PLANO LATERAL IZQUIERDO DE LA PLANTA BAJA DEL INCYT

En la imagen número 49, podemos observar el plano izquierdo del Incyt, el cual tiene distintos puntos de ingreso, ya sea ventanas o ventanillas. Cabe recalcar que estas ventajas no cuentan con relajas y ninguna protección.

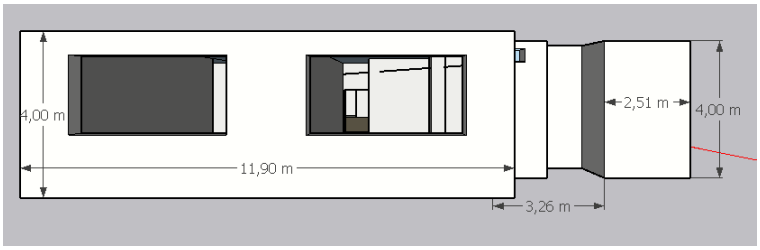


FIGURE 49 FLANCO LATERAL IZQUIERDO

PLANO POSTERIOR DE LA PLANTA BAJA DEL INCYT

En la imagen número 50 se muestra la parte posterior del edificio y cómo podemos apreciar no tiene puertas, pero si tiene ventanas y este ingreso debemos monitorearlo.

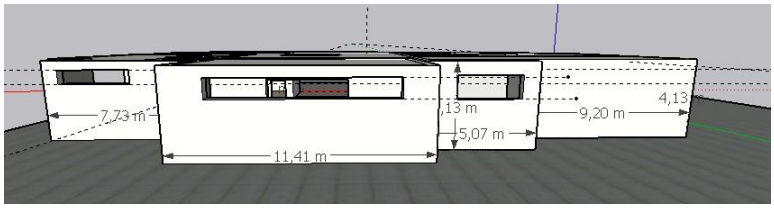


FIGURE 50 PLANO POSTERIOR DE LA PLANTA BAJA DEL EDIFICIO

PLANO LATERAL DERECHO DE LA PLATANA BAJA DEL INCYT

En la figura numero 51 se muestra la parte lateral derecha del edificio y podemos ver que existen accesos que debemos cubrir ya sea con sensores o camaras.

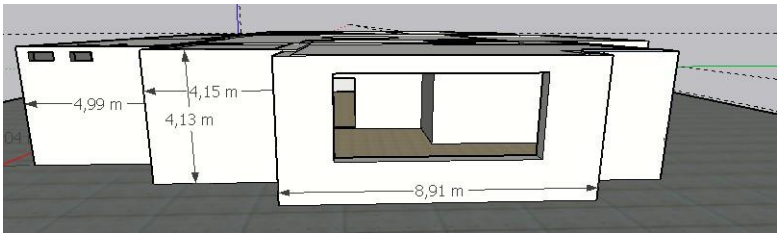


FIGURE 51 PLANO LATERAL DERECHO DE LA PLANTA BAJA DEL EDIFICIO

PARTE FRONTAL

En la figura número 52, se muestra el plano frontal de la digitalización del INCYT, el cual nos permite ver los distintos accesos que se tiene.

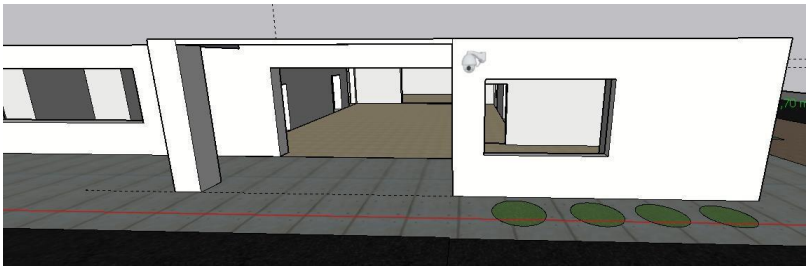


Figure 52 CAMARA EN LA PARTE FRONTAL DE LA PLANTA BAJA

PLANO INTERNO DEL ACCESO PRINCIPAL AL EDIFICIO

A continuación, en la figura número 53 se presenta una vista general del interior del edificio, como podemos observar se tienen varias puertas de distinto tamaño pertenecientes a distintas oficinas.

Figure 53 PLANO INTERNO DE LA ENTRADA PRINCIPAL AL EDIFICIO

3.3 IMPLEMENTACIÓN Y CONSTRUCCIÓN

En el presente capitulo se hablará sobre los puntos en donde se instalaron las cámaras, el servidor principal y los sensores, todo esto se basa en el objetivo de mantener la seguridad, en cuanto a las cámaras de videovigilancia, fueron colocadas en puntos estratégicos en donde su campo de visión cubra las entradas al edificio (puertas y ventanas).

A continuación, en la figura número 54 se presenta la parte frontal del edificio en donde colocamos la cámara con su respectivo rango de visión.

PARTE FRONTAL

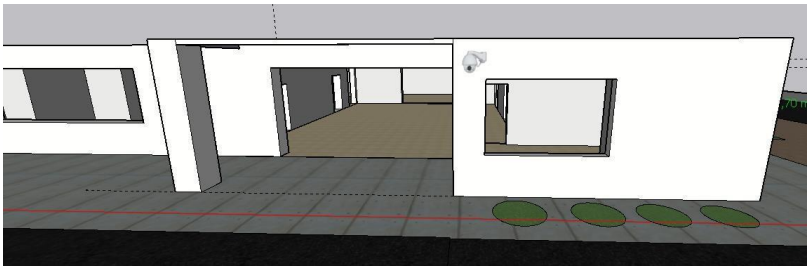


Figure 54 CAMARA EN LA PARTE FRONTAL DE LA PLANTA BAJA

Como observamos en la imagen anterior, ese es el lugar en donde se colocó la cámara, en el capítulo II explicamos que la cámara tiene distintos ángulos de visión, lo cual le permite a la cámara ver hacia ambas direcciones.

A continuación, en la figura número 55, se muestra el rango de visión que tiene la cámara en este punto.

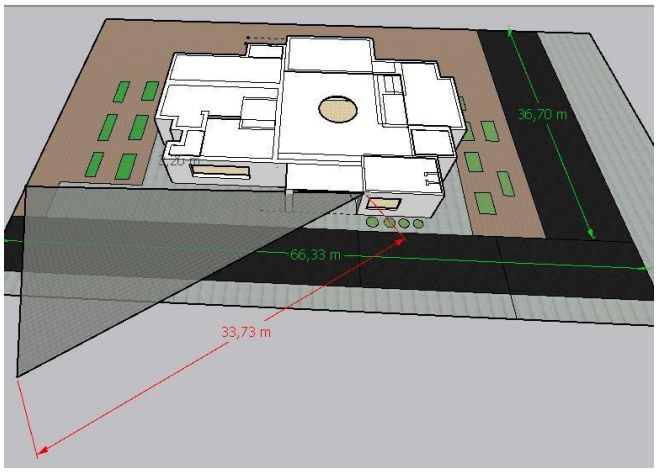


Figure 55 DISTANCIA DE VISION DE LA CAMARA COLOCADA

En la figura anterior se puede apreciar la distancia que se cubre con la cámara en ese punto, cabe recalcar que el modelo colocado puede abarcar hasta 100m, en el caso de la digitalización se hace el ejemplo de las áreas aledañas que miden 30m, la misma distancia se repite al momento de girar la cámara.

A continuación, en la figura número 56 se marca el rango total que puede cubrir la cámara con los movimientos que ejecuta.

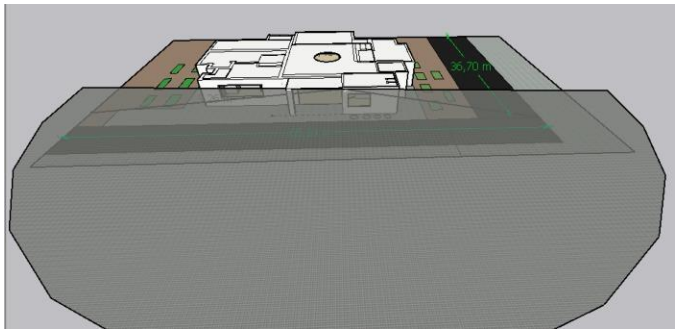


Figure 56 VISION CUBIERTA POR LA CAMARA COLOCADA

Siguiendo el mismo razonamiento se colocó las cámaras laterales en distintos puntos para poder cubrir todos los ángulos cerca del edificio.

RANGOS LATERALES.

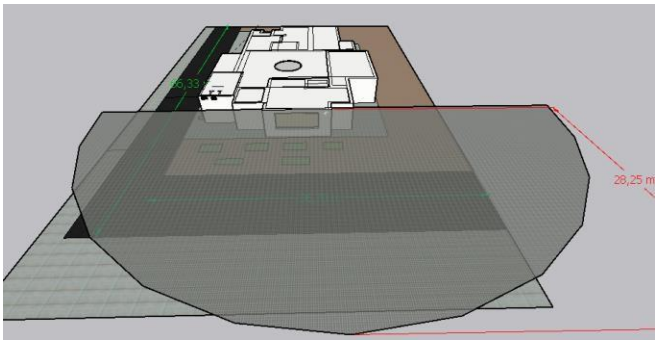


FIGURE 57 RANGO LATERAL DERECHO

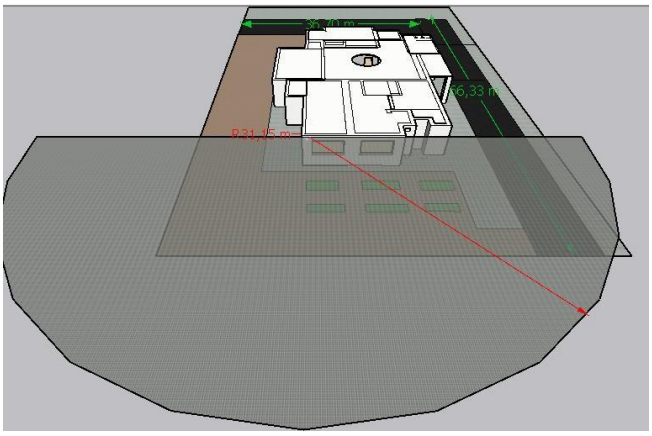


FIGURE 58 TANGO LATERAL IZQUIERDO

RANGO POSTERIOR

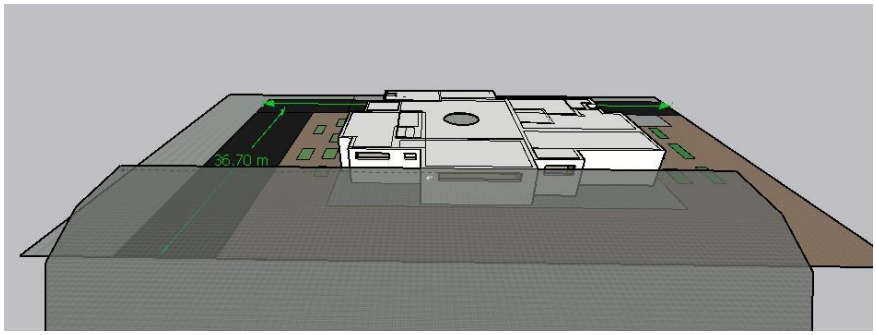


Figure 59 RANGO POSTERIOR

En el caso del rango posterior es un caso especial, ya que un edificio aledaño se encuentra a menos de 10 metros del INCYT, por lo cual nos sobra mucha distancia de grabación.

3.3.1 UBICACIÓN DE CONTROLADORES

Como etapa de controlado tenemos que este trabaja en un servidor creado en Home Assistant, el cual ejecuta ordenes mediante nuestro raspberry que es el encargado de contener todo el proyecto. Los sensores y cámaras van enlazados a nuestro servidor mediante protocolos de comunicación que indicamos en el capítulo II al hablar de la comunicación del sistema. Antes de colocar los controladores que son el Raspberry y el dispositivo USB para la comunicación Z wave, vamos a explicar la configuración de este, como mencionamos anteriormente el controlador Raspberry será el cerebro que reciba y envíe las señales a las cámaras y sensores.

A continuación, en la figura número 60 se mostrará el diseño jerárquico que se utiliza en esta implementación.

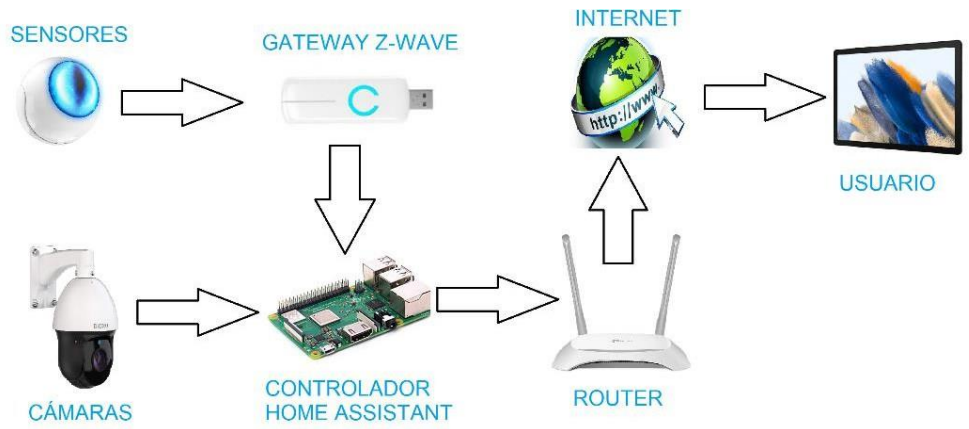


Figure 60 DISEÑO GENERAL DE CONEXIÓN UTILIZADO

Para explicar de mejor manera el diseño, se presentan partes del mismo, el cual se compone de protocolo Z wave para la comunicación de los sensores con nuestro raspberry y el protocolo onvif para la comunicación de las cámaras a nuestro controlador.

DISEÑO DE COMUNICACIÓN Z WAVE CON RASPBERRY

Para la comunicación de los sensores y nuestro controlador, necesitamos una antena Z wave mencionada en capítulos anteriores, esto ayuda a que nuestro controlador trabaje con OpenZWave y de esta manera puede comunicarse y hablar el mismo lenguaje que los sensores.

En la figura número 61 podemos ver la conexión que se ejecuta entre los sensores, la antena y el controlador.

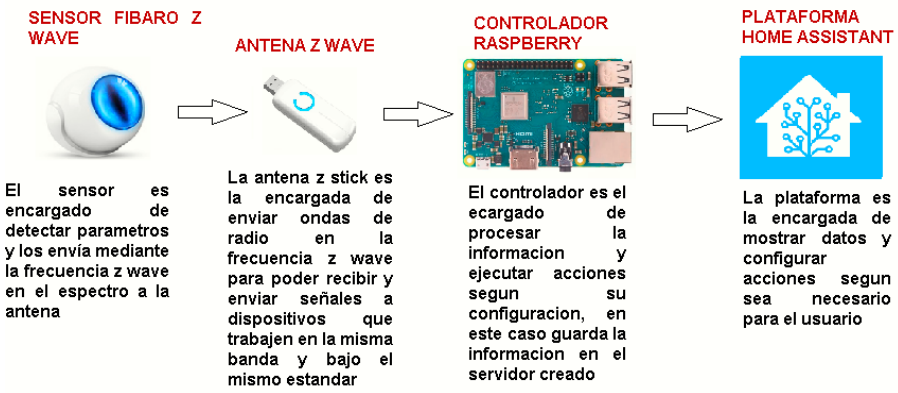


Figure 61 DISEÑO Y EJECUCION DEL PROTOCOLO Z WAVE

DISEÑO DE COMUNICACIÓN ONVIF CON RASPBERRY

Para la comunicación de las cámaras de videovigilancia con el servidor Home Assistant y el controlador se utilizó el protocolo ONVIF, en capítulos anteriores hemos hablado del trabajo que realiza este protocolo, que parámetros utiliza, bajo que licencias trabaja, la frecuencia que utiliza para el envío y recepción de los datos tomados.

A continuación, en la figura número 62 presentamos la conexión que ejecuta este protocolo y permite la conexión de las cámaras con el controlador raspberry y luego a nuestro servidor en Home Assistant.

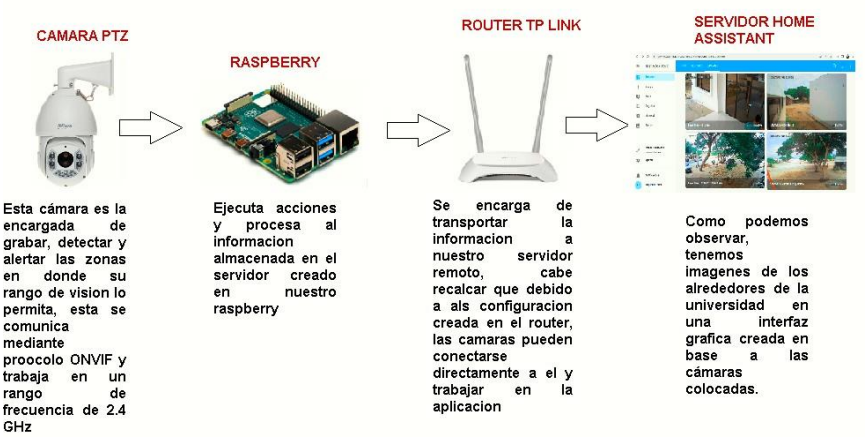


Figure 62 DISEÑO Y EJECUCION DEL PROTOCOLO Z WAVE

3.3.1.1 INSTALACIÓN DE SOFTWARE HOME ASSISTANT EN RASPBERRY

Para la ejecución y creación del servidor en la plataforma Home Assistant en raspberry pi necesitamos instalar el sistema operativo con el que trabaja que en este caso es “Home Assistant OS”, este sistema puede ser grabado en una memoria SD la cual va a leer nuestro controlador.

Para grabar este sistema operativo tenemos dos opciones, utilizar el programa “Raspberry Pi Imager” o el programa “BalenaEtcher”. Toda esta información se encuentra en la página oficial de Home Assistant, en el caso del presente proyectó se eligió el programa “BalenaEtcher” para instalar el sistema operativo, esto es debido a que este programa no tiene restricción sobre versiones de raspberry utilizadas, al contrario, el programa “Raspberry Pi Imager” tiene restricciones de modelos y versiones, ya que las opciones sobre ciertos modelos no son admitida, adicionalmente este programa no es compatible con ciertas plataformas.

1) Antes de poder instalar el home Assistant en nuestro Raspberry vamos a necesitar de un programa que nos permita grabar el sistema en la micro SD, este programa ser llama “BalenaEtcher”. Este programa será el encargado de descargar (según se elija la opción) nuestro sistema operativo de HA y lo grabará en la tarjeta SD colocada.

A continuación, en la figura número 63 se presenta la interfaz del programa BalenaEtcher

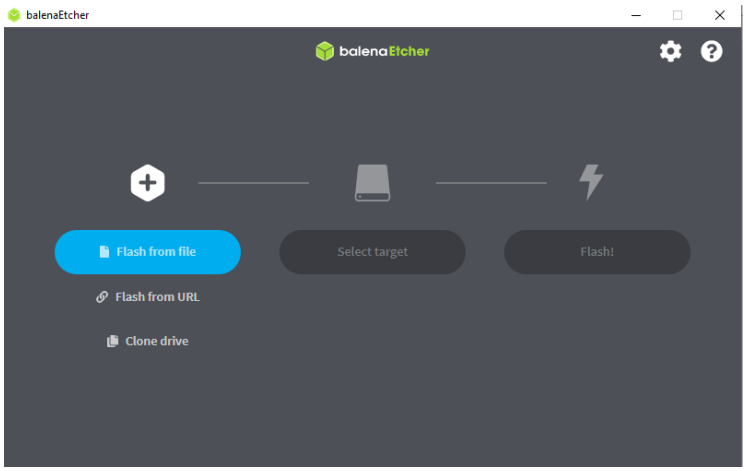


Figure 63 INTERFAZ DE SOFTWARE BALENA ETCHER

2) Una vez abierto el programa, el mismo nos va a dar dos formas de grabar un sistema operativo y es por medio de carpeta o por medio de URL, en el caso de seleccionar la opción “carpeta” tenemos que tener el sistema operativo descargado y almacenado en la computadora. En el caso del proyecto utilizamos la opción URL, la cual permite al software que al ingresar una URL este se redirigirá y descargará el sistema que se encuentra en la misma. Una vez hecho esto podemos instalar el sistema operativo HA a la micro SD, dicha URL se encuentra en la página web de home Assistant en donde descargaremos el instalador para Raspberry. Elegimos la versión de Raspberry ya sea 4 o 3.

A continuación, en la figura número 64 se presenta la interfaz de la página de Home Assistant, y podemos apreciar las diferentes URL que se presentan, elegimos la indicada, para el proyecto elegimos el modelo “Raspberry Pi 3”.

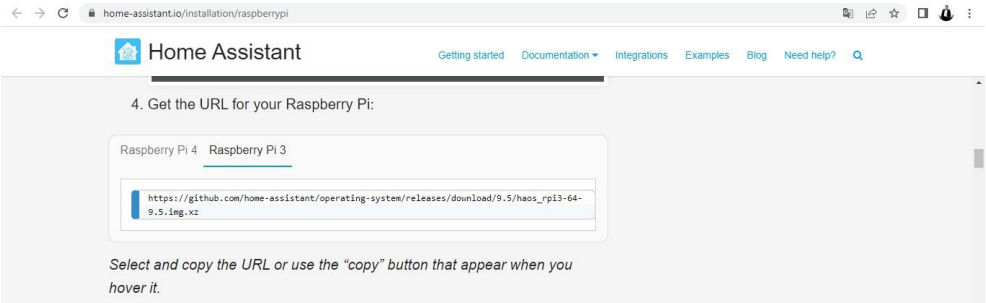


FIGURE 64 PÁGINA OFICIAL DE HOME ASSISTANT

3) Una vez copiado el URL, procedemos a pegarlo en la opción que seleccionamos en el programa anterior y seleccionamos el dispositivo conectado, en este caso la micro SD.

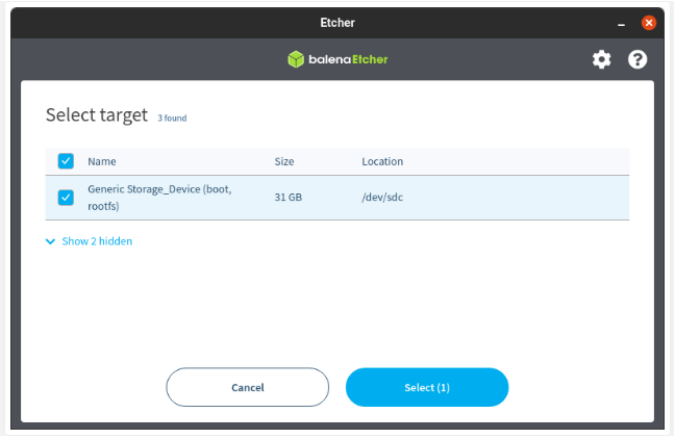


Figure 65 INTERFAZ DEL SOFTWARE SELECCIONANDO EL DISPOSITIVO INSERTADO

4) Una vez seleccionado el dispositivo a almacenara (en el caso del proyecto es la memoria SD insertada en la computadora), procedemos a colocar “siguiente”, lo que hará el software es empezar a grabar en la memoria el sistema operativo de Home Assistant, el cual lo encuentra en la pagina del mismo, cabe recalcar que este proceso es posible a que la computadora se encuentra conectada a internet.

A continuación, en la figura número 66 podemos observar que el software grabó exitosamente el sistema operativo en nuestra memoria SD.

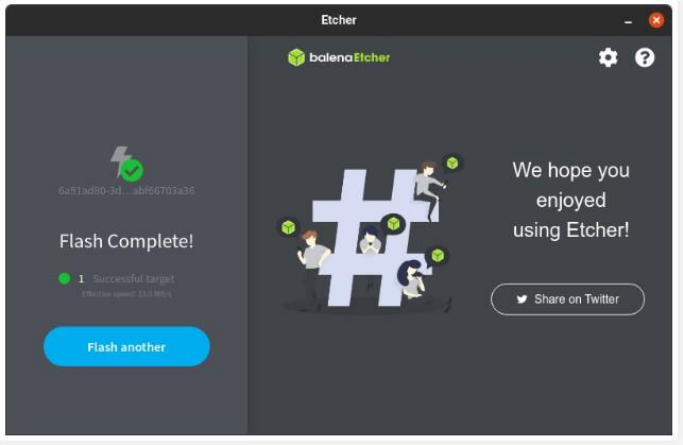


FIGURE 66 INTERFAZ DEL SOFTWARE FINALIZANDO LA INSTALACIÓN DEL HOME ASSISTANT

3.3.1.2 CONFIGURACIÓN DEL HOME ASSISTANT EN EL RASPBERRY PI

Para poder ejecutar el sistema operativo, se necesita controlar y ejecutar distintos parámetros, estos son.

- Dirección IP
- Tipo de conexión
- UUID
- ID de la red

Estos parámetros son los que vamos a crear según sea el caso. Como se tiene una red creada, vamos a utilizar direcciones que se encuentren en la misma.

Esta información la vamos a ingresar a nuestro raspberry mediante un dispositivo USB, para que el controlador lea la información y la interprete creando el servidor en la plataforma con los valores asignado (dirección IP, tipo de conexión, entre otras).

A continuación, en la figura número 67 se presenta una imagen de los parámetros antes mencionados colocados.

```
[connection]
id=my-network
uuid=
type=802-3-ethernet

[ipv4]
method=manual
address=
dns=8.8.8.8;8.8.4.4

[ipv6]
addr-gen-mode=stable-privacy
method=auto
```

FIGURE 67 CONFIGURACIÓN DEL SERVIDOR HOME ASSISTANT

A continuación, explicaremos que acción ejecuta cada línea de configuración.

ID: Para crear una IP fija en nuestro raspberry debemos colocar el ID de nuestro archivo, esto es para que el Raspberry pueda leer el mismo, en este caso lo colocamos como “my-network”

UUID: El UUID es un identificador universal único, este lo sacamos de una página que genera este tipo de parámetros “uuidgenerato”, lo que hace el mismo es identificar y comprobar el servidor HA.

TYPE: Esto se basa en el protocolo IEEE 802.3 y es el encargado de ejecutar la tecnología cableada que existe entre nuestro raspberry y el internet.

ADDRESS: Este parámetro nos permite colocar una red IP para acceder a nuestro servidor creado.

DNS: Este dominio es el utilizado para convertir las solicitudes en redes IP, en este caso utilizamos las de google, ya que son muy estables y no reportan caídas de manera continua.

IPV6: en el caso de IPV6 colocamos parámetros automáticos, de esta manera nuestro servidor detectará acciones que necesitan IPV6 y pueda funcionar debido a que no tiene restricciones, en el caso del acceso remoto que se basa en protocolo IPV6

3.3.1.3 CREACION DEL SERVIDOR HOME ASSISTANT

Para la creación del servidor utilizamos parámetros que fueron descritos en el capítulo II al hablar del software a utilizar, estos son importantes, ya que sin ellos no tendríamos acceso a un servidor en la plataforma HA.

Una vez configurado el Raspberry con los parámetros insertados en el USB, procedemos a iniciarlo y entrar a la IP antes puesta, esto va a depender de la IP que maneje la universidad, cabe recalcar que debemos ingresar una IP que se encuentre en la red, podemos utilizar aplicaciones como “Fing” para poder ver que redes tenemos disponibles y utilizar una de ellas.

A continuación, en la figura numero 68 presentamos la interfaz que nos da nuestro servidor al ser creado.

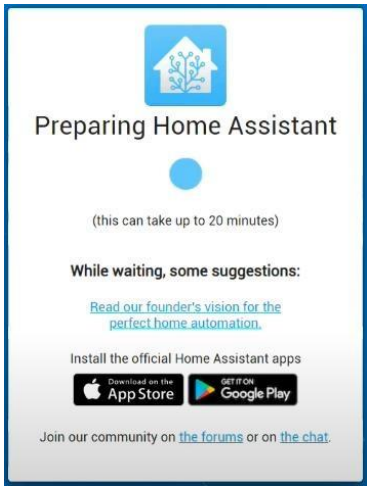


FIGURE 68 INTERFAZ DE CREACIÓN DE SERVIDOR HOME ASSISTANT (Assistant, 2023)

Al crear el servidor en la plataforma HA, debemos esperar que se ejecuten las configuraciones respectivas, esto lo hará la plataforma mediante parámetros que configuramos anteriormente, el tiempo de espera para la ejecución varía entre 10 y 20 minutos máximo, en este caso tardó un promedio de 15 minutos en crear el servidor completamente.

Cuando esperemos el tiempo indicado en la página, procedemos a crear un usuario y una contraseña para poder ingresar a nuestro servidor, una vez hecho esto nuestro servidor estará listo para poder ingresar complementos y poder vincular diferentes dispositivos.

A continuación, en la figura numero 69 presentamos la interfaz que nos da la plataforma para crear un usuario y contraseña

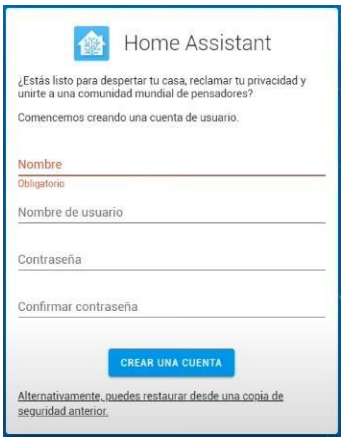


FIGURE 69 INTERFAZ HOME ASSISTANT PARA CREACIÓN DE USUARIO Y CONTRASEÑA DEL SERVIDOR (Assistant, 2023)

Cuando tengamos el servidor creado, procedemos a instalar los aplicativos necesarios para poder trabajar con las cámaras y los sensores.

Como complementos principales y necesarios para la comunicación entre nuestro controlador y los dispositivos instalados están:

- Complemento ONVIF
- Complemento Z wave JS
- Complemento UPNP

A continuación, en la tabla número 31 se presentan los complementos instalados en nuestro servidor y el lugar en donde lo utilizamos para nuestro proyecto.

COMPLEMENTOS INSTALADOS	USO Y APLICACIÓN
COMPLEMENTO ONVIF	Este complemento es el encargado de crear la comunicación mediante el protocolo ONVIF y se utiliza para enlazar las cámaras con nuestro servidor
COMPLEMENTO UPNP	Este complemento ejecuta acciones que permiten a los dispositivos compatibles configurar reglas de re direccionamiento, de esta manera ningún dispositivo no tendrá problemas para poder ingresar y controlar el servidor
COMPLENTO Z WAVE JS	Este complemento es el que dará las credenciales y ejecutará acciones para que nuestro controlador se vincule con la antena y los dispositivos raspberry

TABLA 31: COMPLEMENTOS INSTALADOS EN EL SISTEMA

3.3.1.3.1 INSTALACION DE COMPLEMENTOS UTILIZADOS EN EL SERVIDOR

En título anterior, mencionamos los complementos que necesita nuestro servidor en HA para que pueda ejecutar los diferentes protocolos utilizados (ONVIF y Z WAVE). Estos protocolos ayudan a la comunicación efectiva entre los modelos de dispositivos utilizados (cámaras y sensores).

A continuación, vamos a explicar cómo instalamos los protocolos para que ejecuten las funciones designadas en el servidor.

COMPLEMENTO ONVIF

El complemento ONVF es el encargado de crear la integración de la cámara, gracias a esto se puede utilizar un dispositivo compatible en este caso la cámara ptz en nuestro Home Assistant. Este complemento admite perfiles de audio y video, proporcionando imágenes de las cámaras conectadas. Esta integración agrega entidades a los perfiles compatibles con la codificación configurada en H.264. El mecanismo que utiliza para transporte RTSP varía entre.

- Tcp
- Udp
- udp_multicast
- http

1. Para la instalación de este complemento, nos dirigimos a la configuración del servidor.

   A continuación, en la figura número 70 se presenta la interfaz de configuración de nuestro servidor.

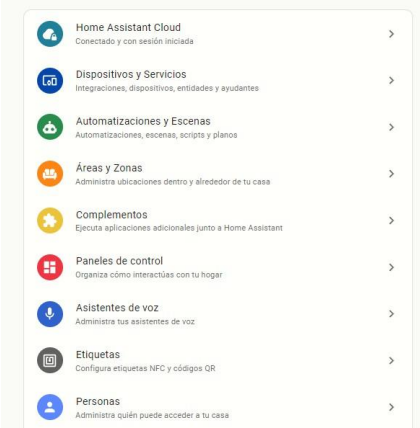


FIGURE 70 INTERFAZ "CONFIGURACIÓN" DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

2. Cuando nos encontremos en las configuraciones, ingresamos a la pestaña de "Dispositivos y Servicios".

A continuación, en la imagen número 71 se muestra la interfaz de opciones que tenemos en nuestro servidor.

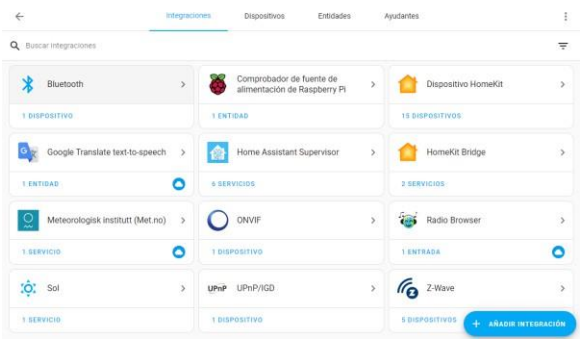


FIGURE 71 INTERFAZ "DISPOSITIVOS Y SERVICIOS" DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

3. Una vez ingresado, le damos a "añadir nueva integración" y nos presentará un menú que contiene diferentes complementos e integraciones.
   A continuación, en la figura número 72 presentamos el menú de las distintas marcas, complementos e integraciones presentadas en el servidor.

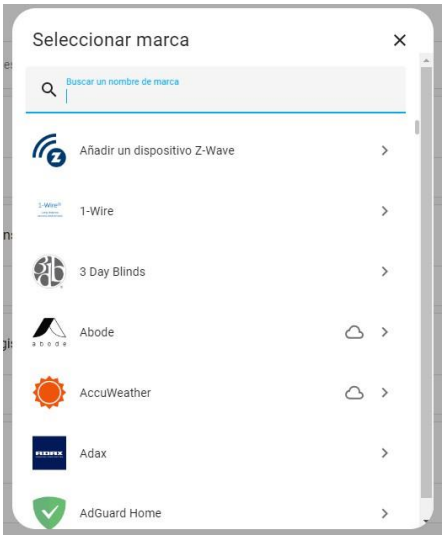


FIGURE 72 INTERFAZ "NUEVA INTEGRACIÓN" DE NUESTRO SERVIDOR HOME ASSISTANT

4. En este menú, debemos buscar el complemento que necesitamos instalar, en este caso es el “ONVIF”, el cual nos ayuda a la comunicación de las cámaras colocadas.

   A continuación, en la imagen número 73 se muestra el complemento dado en el menú de servidor.

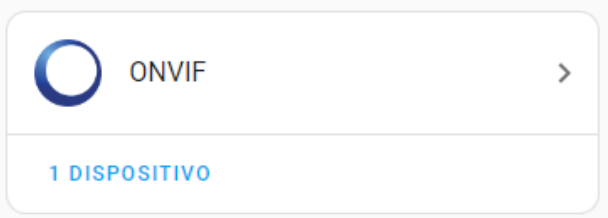


FIGURE 73 INTERFAZ “ONVIF” DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

COMPLEMENTO Z WAVE JS

El raspberry es compatible con distintos protocolos de comunicación, en este caso hablaremos del z wave, si bien es cierto, el controlador no tiene una antena integrada para la comunicación z wave con dispositivos, es compatible con una extensión que trabaja bajo OpenZWave, esta extensión o complemento ejecuta credenciales que permiten vincular dispositivos a un Gateway instalado en el raspberry que en el presente caso es nuestro “USB Z STICK”. El funcionamiento de esta extensión es hacer que la antena z wave cree una red mallada en donde los dispositivos compatibles que trabajen a la misma frecuencia puedan ser emparejados, el escaneo que ejecuta la red z wave permitirá emparejarlos, sin embargo, la forma dependerá de cada dispositivo utilizado, en el caso del proyecto tenemos los sensores, los cuales leerán la red z wave y se emparejaran.

Una vez mencionado lo que realiza este complemento y bajo que frecuencias trabaja, podemos presentar los pasos para instalarlo, los cuales son muy similares al protocolo ONVIF ya que se encuentran en la misma librería.

1. Para la instalación de este complemento, nos dirigimos a la configuración del servidor.

A continuación, en la imagen número 74 se presenta la interfaz de configuración del servidor Home Assistant con las diferentes opciones que este tiene.

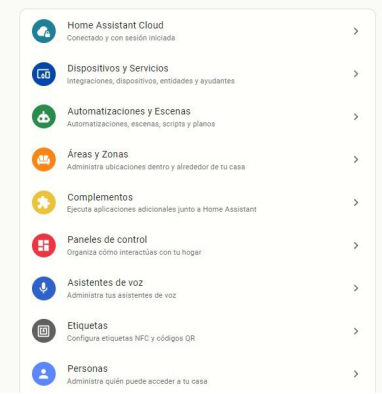


FIGURE 74 INTERFAZ "CONFIGURACIÓN" DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

2. Cuando nos encontremos en las configuraciones, ingresamos a la pestaña de "Dispositivos y Servicios". En esta pestaña nos muestra los complementos y servicios que tenemos instalados en nuestro servidor HA.
   A continuación, en la figura número 75 se presenta la interfaz de "dispositivos y servicios" de nuestro servidor

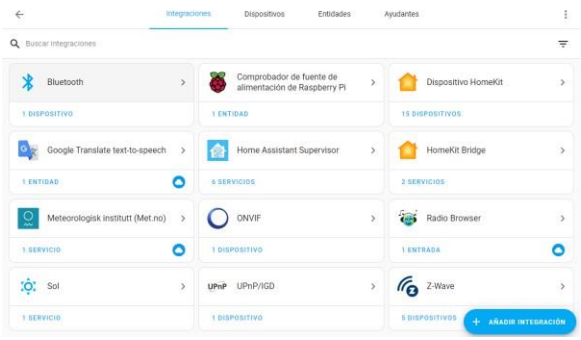


FIGURE 75: INTERFAZ "DISPOSITIVOS Y SERVICIOS" DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

3. Una vez ingresado, le damos a “añadir nueva integración” y nos presentará un menú que contiene diferentes complementos e integraciones.

   A continuación, en la figura número 76 presentamos el menú de las distintas marcas, complementos e integraciones presentadas en el servidor.

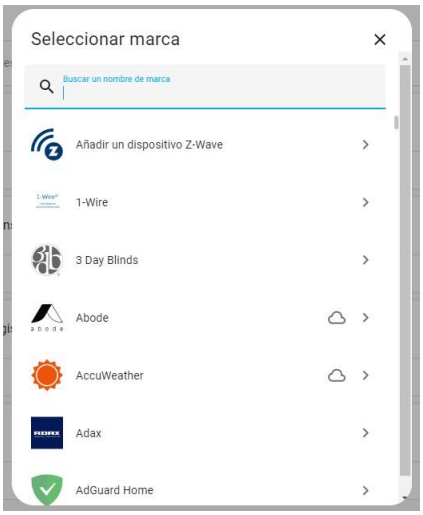


FIGURE 76 INTERFAZ “NUEVA INTEGRACIÓN” DE NUESTRO SERVIDOR HOME ASSISTANT

4. En este menú, debemos buscar el complemento que necesitamos instalar, en este caso es el “Z WAVE”, el cual nos ayuda a la comunicación de los sensores mediante protocolo z wave.

   A continuación, en la imagen número 77 se muestra el complemento dado en el menú de servidor.

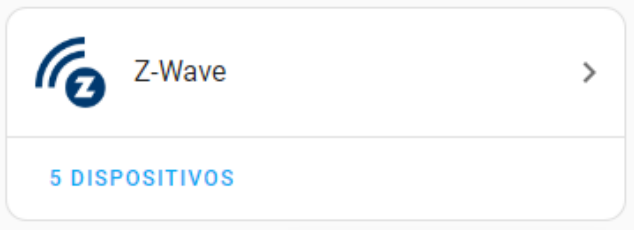


FIGURE 77 INTERFAZ “Z WAVE” DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

COMPLEMENTO UPNP

El complemento UPNP es de suma importancia para nuestra red, ya que es el encargado de hacer que los dispositivos configuren reglas de redirección a los puertos, ya que los sensores y las cámaras utilizan puertos de red distintos para el paso de información. Adicionalmente este complemento nos ayuda a abrir puertos a utilizar, de esta manera no tendremos problemas si el usuario manipula el servidor mediante distintos sistemas operativos como por ejemplo IOS.

1. Para la instalación de este complemento, nos dirigimos a la configuración del servidor.

   A continuación, en la imagen número 78 se presenta la interfaz de configuración del servidor Home Assistant con las diferentes opciones que este tiene.

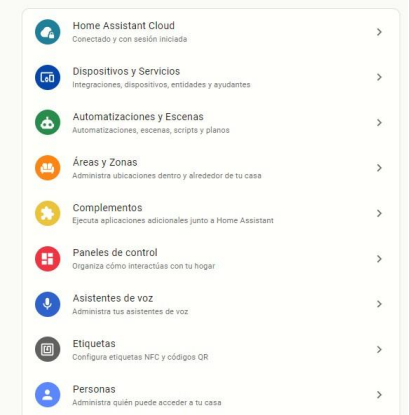


FIGURE 78 INTERFAZ "CONFIGURACIÓN" DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

2. Cuando nos encontremos en las configuraciones, ingresamos a la pestaña de "Dispositivos y Servicios". En esta pestaña nos muestra los complementos y servicios que tenemos instalados en nuestro servidor HA.

   A continuación, en la figura número 79 se presenta la interfaz de "dispositivos y servicios" de nuestro servidor

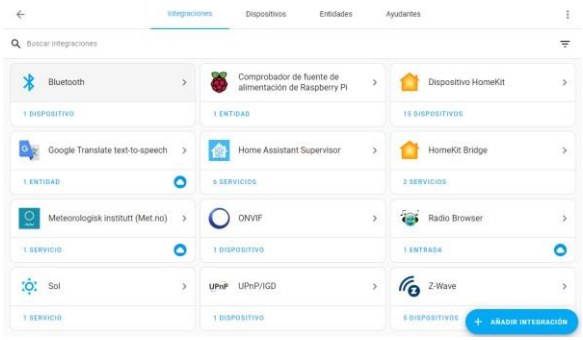


FIGURE 79 INTERFAZ "DISPOSITIVOS Y SERVICIOS" DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

3. Una vez ingresado, le damos a "añadir nueva integración" y nos presentará un menú que contiene diferentes complementos e integraciones.
   A continuación, en la figura número 80 presentamos el menú de las distintas marcas, complementos e integraciones presentadas en el servidor.

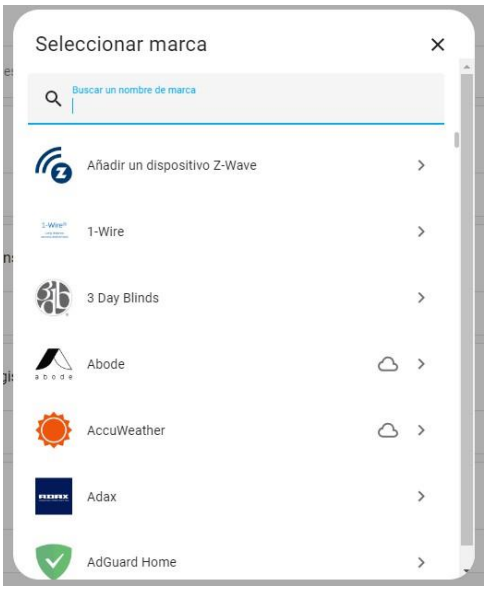


FIGURE 80 INTERFAZ "NUEVA INTEGRACIÓN" DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

4. En este menú, debemos buscar el complemento que necesitamos instalar, en este caso es el "UPNP/IGD", el cual nos ayuda a la comunicación de los dispositivos mediante el uso y configuración de puertos automáticamente.

A continuación, en la imagen número 81 se muestra el complemento dado en el menú de servidor.

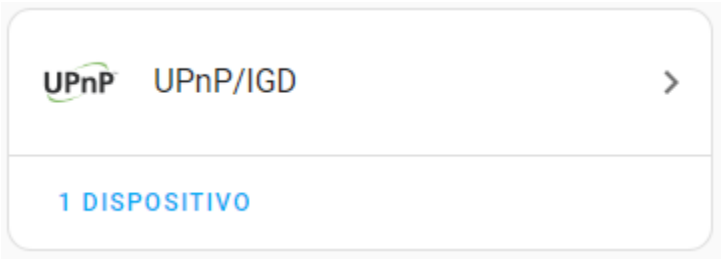


FIGURE 81 INTERFAZ "UPNP" DE NUESTRO SERVIDOR HOME ASSISTANT (Assistant, 2023)

3.3.1.4 UBICACIÓN DEL RASPBERRY Y ROUTER CON SERVIDOR HOME ASSISTANT EN EDIFICIO DEL INCYT

En este capítulo hablamos sobre la ubicación física de nuestro controlador y router principal, el cual es el encargado de brindar internet a nuestro sistema. El controlador Raspberry se conecta de manera cableada mediante un cable UTP a nuestro router principal, para que este pueda utilizar los puertos correspondientes para la creación y funcionamiento del sistema de monitoreo. Adicionalmente el controlador estará enlazado a la antena Z wave para poder generar la red mallada y los dispositivos puedan conectarse entre sí.

A continuación, en la figura número 82 se presenta el esquema que se realizó en el HeadEnd para el funcionamiento del mismo.

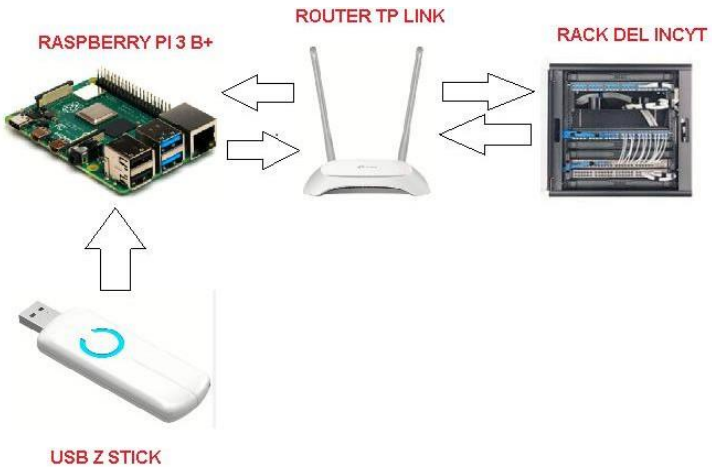


FIGURE 82 CONEXIÓN PARA HEADEND DEL SERVIDOR

Como podemos observar en la figura anterior, esa es la conexión que se realizó en el HeadEnd del proyecto, cabe recalcar que las conexiones fueron realizadas mediante el uso de cable UTP categoría 5e para interiores. La conexión entre nuestro Gateway y controlador es de manera USB.

En el cable UTP se utilizó la conexión de cable directa, este se basa en el estándar T568B, el cual nos indica que es utilizado para conectar equipos en una red de área local como lo es el caso del sistema de vigilancia.

A continuación, en la figura número 83 mostraremos la normativa que se utilizó para la conexión de internet de forma cableada y el porqué de la misma.

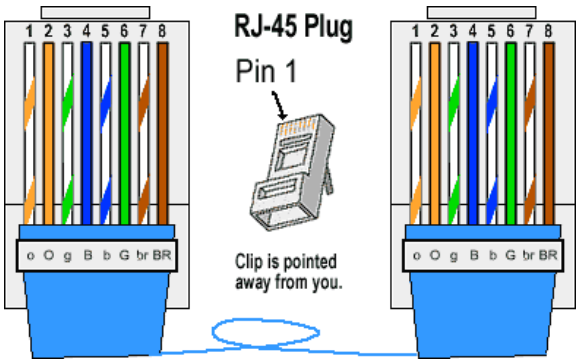


FIGURE 83 CONEXIÓN CABLE DIRECTO UTP T568B (Telectronika, 2022)

Una vez indicada las normativas de nuestra conexión, procedemos a conectar el Rack principal del INCYT a nuestro router principal, el cual tendrá internet y hará el funcionamiento de ser el equipo madre de nuestra red local.

A continuación, en la figura número 84 se presenta un esquema entre el rack principal y el router de área local.

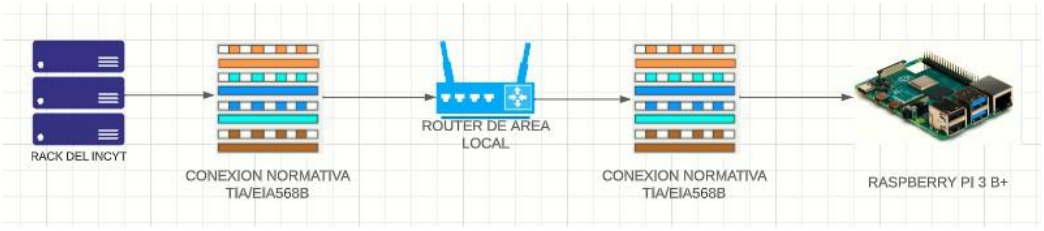


FIGURE 84 CONEXIÓN DE RED ENTRE RACK, ROUTER Y RASPBERRY (Telectronika, 2022)

Una vez mencionadas las conexiones que se realizaron en el INCYT, presentamos los pasos a seguir para la colocación de nuestro HeadEnd en un punto del edificio y explicamos el motivo por el cual se lo colocó en ese lugar.

3.3.1.4.1 UBICACIÓN DE HEADEND EN EL EDIFICIO DEL INCYT

Para este tema, se optó por elegir un punto céntrico y visible del edificio, esto debido a motivos de seguridad y de conectividad. Al tener nuestro enrutador en un punto céntrico la señal inalámbrica del mismo será repartida de manera equitativa y llegará a los equipos con mayor velocidad y menos latencia.

1. Como HeadEnd colocamos una caja de paso de plástico color blanca, la cual nos ayudará a mantener dentro los equipos principales del servidor, esta caja está colocada en un punto céntrico del edificio debido al alcance wifi que necesita tener y adicionalmente está en un punto visible con un punto de electricidad a su lado.

   A continuación, en la figura número 85 se presenta una imagen la caja colocada en el edificio.

Figure 85 HEADEND PARA EQUIPOS

En la imagen número 86 mostramos en la simulación el lugar exacto donde se colocó la caja para poder trabajar desde otra perspectiva.

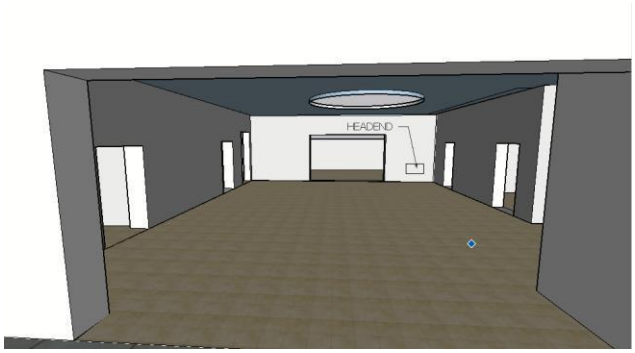


Figure 86 HEADEND EN LA DIGITALIZCIÓN

Como podemos observar en la simulación, este es el lugar elegido para la colocación de los equipos que controlan al servidor, esto se realizó debido al alcance WIFI que tiene nuestro Router (20 m aproximadamente según especificaciones del mismo), gracias a esto podemos obtener un buen alcance de señal para cubrir casi toda el área del edificio.

A continuación, en la figura número 87 se presenta el rango de señal WIFI que abarca el router elegido para el área local.

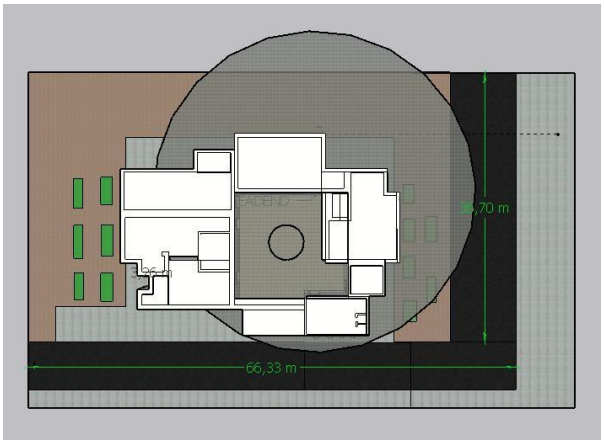


Figure 87 AREA DE ALCANCE WIFI

2. Una vez colocada la caja, se procedió a solicitar un punto de internet del SW administrable a las oficinas de Tic's del INCYT. Los Ingenieros encargados de sistema y redes, mostraron los puertos que se pueden utilizar y los que dejaron libres del Rack principal.

   A continuación, en la figura número 88 se presenta evidencia de la conversación con el Ingeniero de Tics para el uso de un puerto de Rack. En este caso se asignó el puerto número 3 y 4 de SW para la utilización.

Figure 88 EXPLICACIÓN DEL SW PRINCIPAL POR PARTE DEL DEPARTAMENTO DE TIC'S

Una vez dado el puerto del SW principal el edificio, lo utilizamos para la conexión, cabe recalcar que nuestro HeadEnd se encuentra ubicado en una zona céntrica del

edificio, el SW principal del INCYT está ubicado en una oficina lateral, debido a esto se optó por realizar una conexión cableada desde el Rack hasta el HeadEnd de área local.

3. Para la conexión cableada se procedió a ponchar un cable UTP que va desde el Rack principal hasta nuestro HeadEnd, para cuidar la estética del edificio, se colocaron canaletas en las esquinas del mismo, de esta manera el cable pasará por las mismas y cuidará la imagen del INCYT.
   A continuación, en la imagen número 89 se presenta el ponchado del cable UTP siguiendo la normativa EIA/TIA568B.

Figure 89 PONCHADO DE CABLE UTP

A continuación, en la imagen número 90 se presenta la colocación de las canaletas en las esquinas que van desde el Rack hasta el HeadEnd.

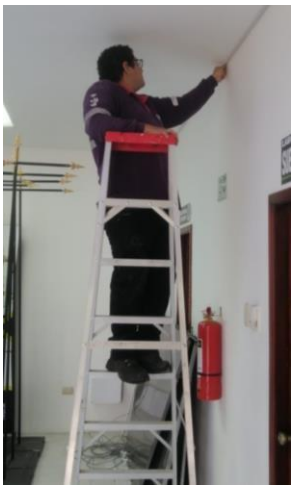


Figure 90 COLOCACION DE CANALETAS PARA CABLE UTP

A continuación, en la figura número 91 se aprecia en la digitalización el camino marcado de color rojo por donde fueron colocadas las canaletas.

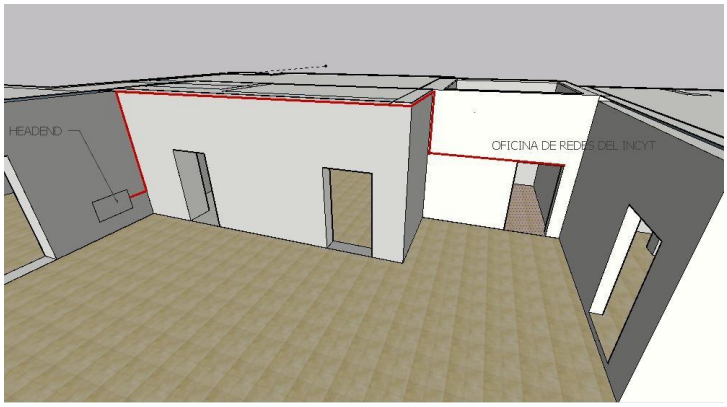


Figure 91 DIGITALIZACION DE LA COLOCACION DE CANALETAS

3.3.1.5 CONFIGURACIÓN DE ROUTER COMO AP

Para poder darle conexión a internet a nuestro Raspberry se decidió implementar un router independiente para conectar las cámaras de forma inalámbrica y el Raspberry de forma cableada mediante un puerto LAN. Esta red de área local creada será la que le brinde internet a todo nuestro sistema, en el capítulo anterior mencionamos el tipo de conexión que se hará para la mismo. Una vez realizada la conexión, vamos a explicar el por qué se configuro la red de tal manera que los puertos que se utilizan se encuentren libres, adicionalmente que el protocolo IPv6 se encuentre activo, ya que este nos ayudará a realizar la conexión remota al HA.

Para la configuración de nuestro Router vamos a ejecutar los siguientes pasos.

1) Conectamos nuestro router a la PC mediante un cable ethernet, entramos a nuestro navegador a la página “http://tplinkwifi.net” e ingresamos una contraseña para este ingreso, en este caso “SeguridadUpse2023”. Estas

credenciales serán las que el router tendrá y mediante su acceso podemos configurar lo que se requiera del equipo.

A continuación, en la imagen número 92 se presenta la interfaz del router que se utilizó

FIGURE 92 INTERFAZ DEL ROUTER PARA CREACIÓN DE CONTRASEÑA

2) Una vez ingresada la contraseña, entramos a configuración automática y colocamos el SSID y contraseña para la red. Este paso se puede realizar de forma manual, colocando el router en modo predeterminado y seguir con los pasos correspondientes.

   A continuación, en la figura número 93 se presenta la interfaz de "configuración rápida" que nos brinda el equipo-

Figure 93 INTERFAZ DEL ROUTER PARA CREACIÓN DE SSID Y CONTRASEÑA PARA LA RED

3) Una vez seleccionado el modo predeterminado del router e ingresada las credenciales, configuramos la red mediante DHCP, la cual ayudará a que nuestro router detecte la IP y la máscara de red automáticamente. Esto ayudará a que no sea necesario asignarle una IP de la red al dispositivo.

   A continuación, en la figura número 94 se presenta la interfaz de la configuración del tipo de LAN

Figure 94 INTERFAZ DEL ROUTER PARA EL USO DE DHCP

3.3.1.6 UBICACIÓN DE EXTENSORES WIFI

Una vez ubicado los equipos y el router principal, se realizaron pruebas y cálculos para llegar a la conclusión de que se necesitaban extensores WIFI para cubrir el edificio en su totalidad, esto es debido a que la potencia que emitía el router principal no era la suficiente para llegar a las cámaras de videovigilancia que se colocaron en distintos puntos, cabe recalcar que esto trabaja en la bando 2.4 GHz y necesita una potencia optima de transmisión y recepción para que la conexión entre las cámaras y el internet sea la más óptima. Para poder realizar en enlace

exitoso de las cámaras de seguridad, se realizaron extensiones WIFI con una red tipo MESH para tener mayor alcance en la señal.

Se utilizaron extensores WIFI de la marca Xiaomi, el modelo específico es “Mi Wi-Fi Range Extender Pro”, esto debido a que cuenta con una opción de configurar el mismo nombre al repetidor, entonces se crea una red tipo mesh.

Antes de configurar los equipos, tenemos que tener en cuenta como trabaja la banda 2.4 GHz, la banda 5GHz la vamos a excluir ya que los equipos no trabajan en esa banda.

A continuación, en la tabla número 32 se presentan las características principales de la banda 2.4 GHz que es donde trabaja en router y los repetidores.

Características	
Banda ISM	Pocas reglamentaciones al ser una banda libre
Interferencia	Los 2.4 GHz se encuentra saturada en todo el territorio
Estándares	Trabaja bajo estándar 802.11b, 802.11g, 802.11n
Canales	Existen 13 canales con ancho de banda de 20MHz
Longitud de onda	Su longitud de onda esta entre 0.12m y 1.125m

TABLA 32: CARACTERÍSTICAS DE LA BANDA 2.4 GHZ

Una vez mencionadas las características principales de esta banda, notamos que se rige a distintos estándares y la saturación de la misma es alta, debido a esto existe un parámetro principal e importante que es denominado “Link Budget”, el cual nos dice que existe la potencia de transmisión que tiene el equipo (con la tecnología en la que está trabajando) y una potencia aproximada que recibe el usuario a una

distancia aproximada, esto trabaja bajo perdidas que se producen en el camino y atenuaciones causadas por paredes.

A continuación, se presenta una fórmula para poder calcular las pérdidas y atenuaciones que existe en el edificio del INCYT, tomando valores aproximados en base a los equipos.

CÁLCULO DE POTENCIA APROXIMADA

1. Para el primer paso debemos calcular la ganancia que existe entre nuestro AP y el cliente más alejado.

$$Ganancia\ Total = Tx\ Power\ AP + Ganancia\ de\ la\ Antena - Perdidas\ por\ cable\ AP + Ganancia\ Antena\ Host - Perdidas\ por\ cable\ Host$$

Este tipo de parámetros los encontramos explicados en el capítulo II cuando mencionamos las características de los equipos a utilizar.

2. Como indica la formula, debemos encontrar las perdidas y atenuaciones, esto se realiza con la siguiente formula.

$$Perdidas = 20\log d + 20\log f - 27.55 + Atenuaciones\ por\ paredes$$

Los valores a utilizar en las formulas son los siguientes:

- d 23m (Dispositivo más lejano al router principal)
- f 2.4GHz
- Atenuaciones por paredes 19.5 dB (tres paredes)
- Ganancia Host 5dBi
- Ganancia de Antena 13 dBi
- Tx power 20 dBm

Teniendo en consideración los valores antes mencionados, podemos calcular las perdidas y la ganancia total que dan como resultado lo siguiente.

Para poder configurar los extensores, realizamos los siguientes pasos.

GANANCIA TOTAL: 38 dBm

PERDIDAS: 201.13 dBm

DIFERENCIA ENTRE AMBAS: -163 dBm

Considerando que la sensibilidad de recepción WIFI promedio para una buena cobertura es de -76 dBm, podemos concluir que la señal solo con el router principal es muy mala, debido a esto utilizamos amplificadores WIFI para mejorar la señal.

Una vez mencionado los motivos por lo cual se necesitan extensores WIFI, procedemos a configurarlos respectivamente. A continuación, se muestran los pasos utilizados para su configuración.

1) Primer descargamos la aplicación “Mi Home” desde la play store, esta es la aplicación con la que trabaja el modelo de extensor WIFi seleccionado. Se muestra la figura número 95 con la interfaz de descarga.

Figure 95 CAPTURA DE APLICACIÓN “MI HOME” (Xiaomi)

2) Como segundo paso, debemos conectar el equipo a la electricidad para su respectiva configuración, tal y como se muestra en la figura número 96.

FIGURE 96 IMAGEN DE AMPLIFICADOR WIFI INSTALADO

3) Como tercer paso configuramos el repetidor WIFI para emparejarlo con la red creada y colocamos la opción de “Roaming WIFI”, la cual le dará el mismo nombre y la misma contraseña a la red. En la figura número 97 podemos observar la interfaz del equipo con los dBm respectivos.

Figure 97 CAPTURA DEL EXTENSOR WIFI CONFIGURADO

Una vez configurados los dispositivos debemos colocarlos en puntos estratégicos para que la señal sea efectiva, en el caso del modelo matemático, tomamos como ejemplo el punto más alejado de la señal, por lo tanto, esta era mala.

A continuación, en la figura número 98 se presenta la cobertura de los extensores WIFI.

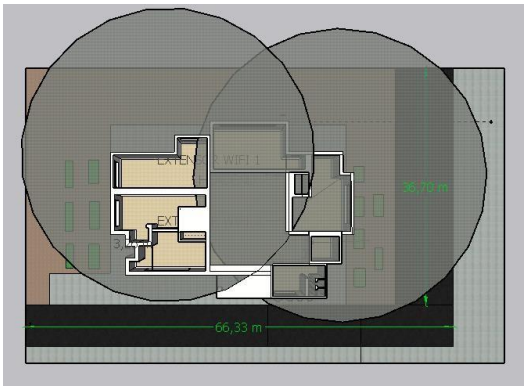


Figure 98 COBERTURA DE EXTENSORES WIFI COLOCADOS

3.3.2 UBICACIÓN DE CÁMARAS

Para la ubicación de las cámaras nos debemos fijar en la digitalización que se realizó en el software Sketchup e identificar los puntos más vulnerables que se encuentran en el edificio, una vez identificados estos puntos, procedemos a configurar las cámaras PTZ que se van a instalar.

Anteriormente hablamos sobre el rango de visión y la distancia focal que tienen las cámaras seleccionadas. Con los datos de la digitalización, podemos corroborar que los puntos elegidos son correctos para cubrir los ángulos del INCYT.

CÁLCULO MATEMATICA PARA LA VISION DE LA CÁMARA

A continuación, explicaremos cálculos matemáticos para verificar los puntos ciegos que tiene las cámaras, para eso nos ayudaremos de la digitalización del sistema.

En la figura número 99 tenemos la cámara frontal con la medida de la altura en la que se encuentra colocada.

Figure 99 CÁMARA FRONTAL

En base a esto podemos utilizar los siguientes datos de la cámara y calcular su funcionamiento bajo un objeto a una distancia “x”. Los parámetros a tomar en cuenta son los siguientes:

- Distancia máxima
- Longitud de lente
- Altura colocada
- Tamaño del sensor
- Distancia focal

Todos estos parámetros están mencionados en capítulos anteriores bajo el modelo utilizado. A continuación, vamos a calcular la resolución que se necesita para detectar un objeto a una distancia “x”, comprobando que los pixeles que tiene la cámara son los necesarios para cumplir esta función.

Los datos necesarios para el cálculo son los siguientes.

- Máximo ancho de la cámara
- Distancia de objeto
- Tamaño del sensor de la cámara
- Necesidad a satisfacer

Bajo estos datos calculamos la resolución que se necesita, en este caso la necesidad a satisfacer es la detección de un objeto a una distancia “x”.

Para una mejor representación y entendimiento, realizamos un gráfico con los distintos datos. A continuación, en la imagen número 100 se presentan gráficamente los datos tomados como ejemplo.

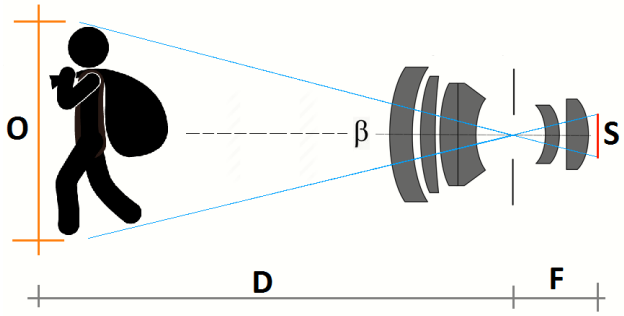


Figure 100 MODELADO MÁTEMATICO DE VISION DE LA CÁMARA

Donde:

O: Altura o anchura de la escena

D: Distancia entre la cámara y el objeto

F: Distancia Focal

S: Tamaño del sensor de la cámara

B: Angulo resultante entre la distancia focal y sensor de la cámara

Calculando las variables podemos decir que:

$$\beta = 2.arctan\left(\frac{S}{2F}\right)$$

$$\tan\left(\frac{\beta}{2}\right) = \frac{O/2}{D}$$

Reemplazando la primera ecuación en la segunda se obtiene que

$$D.S = O.F$$

En base a las ecuaciones, colocamos parámetros para comprobar el modelo y obtenemos los siguientes resultados.

- Máximo que verá al cámara 2m

- Distancia de objeto 5 m
- Tamaño del sensor ¼”
- Necesidad Monitoreo (Estándar para satisfacer esta necesidad 12.5p por metro)

Con esto obtenemos los siguientes resultados.

- **Resolución Necesario: 30 pixeles**
- **Ángulo necesario: 28.1°**
- **Distancia Focal necesaria: 8.5 mm**

Esta tarea se puede satisfacer con un lente que utilice un zoom x2 o superior, debido a los parámetros, en este caso la cámara elegida cuenta con un lente que utilizar un zoom superior, por esto es utilizable en estos casos, el mismo procedimiento se realiza con las demás cámaras y obtendremos resultados satisfactorios.

Una vez aclarada que las cámaras son adecuadas y su colocación es la mejor, vamos a explicar cómo fue la parte física, en la cual se colocaron las cámaras.

Para esta explicación pondremos los puntos paso a paso de una ubicación de la cámara ya que se realizó el mismo procedimiento en todas y el resultado fue positivo.

1) Primero procedimos a identificar un punto de electricidad dentro del edificio del Incyt e hicimos la perforación con el taladro para pasar el cable. A continuación, en la imagen número 101 se presenta una imagen realizando trabajo físico para la colocación de las cámaras.

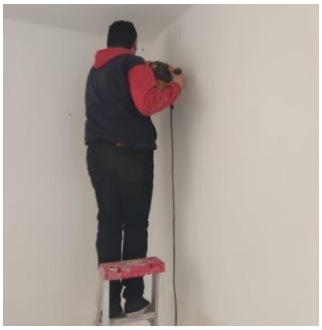


Figure 101 IMAGEN REALIZANDO LA PERFORACIÓN PARA LOS PUNTOS ELÉCTRICOS DE LAS CÁMARAS

2) Luego procedimos a realizar la extensión eléctrica armando el conector que va dentro del edificio. En la imagen número 102 presentamos el armado de las extensiones eléctricas.

FIGURE 102 IMAGEN REALIZANDO EL ARMADO DEL TOMACORRIENTE QUE VA DENTRO DEL EDIFICIO

3) Luego se procedió a pasar el cable y colocar las canaletas para mantener la estética del edificio. En la imagen número 103 se presenta la colocación de canaletas para mantener la estética del edificio.

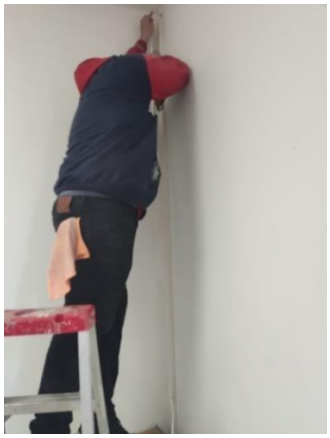


Figure 103 IMAGEN REALIZANDO EL MONTAJE DE LA CANALETA Y PASO DE CABLE ELÉCTRICO

4) Luego de realizar la conexión interna, se realizó el armado de la caja de paso en la cual se colocaría la parte eléctrica de la cámara, su punto de alimentación y su fuente de poder. En la imagen número 104 apreciamos la colocación de las cajas para mantener el POE seguro.

Figure 104 IMAGEN REALIZANDO EL MONTAJE DE LA CAJA DE PASO PARA UBICAR LA FUENTE DE ENERGÍA

5) Al final se colocaron las canaletas y se mejoró la estética dando como resultado la siguiente imagen. En la figura número 105 se presenta la imagen resultante de la instalación eléctrica para la cámara.

Figure 105 IMAGEN DE LA EXTENSIÓN FINALIZADA

6) Luego de tener los puntos eléctricos se procedió a la colocación y encendido de las cámaras de seguridad. En la imagen número 106 se presenta la finalización de la instalación de la cámara.

Figure 106 IMAGEN DE LA CÁMARA INSTALADA Y FUNCIONAL

3.3.2.1 CONFIGURACIÓN DE CÁMARAS

Este tipo de cámaras poseen tres tipos de conexión, alámbrica, por punto de acceso y conexión en la misma red.

En este caso elegimos la conexión en la red, que es mediante WIFI, ya que esta red creada estará conectada al controlador y por lo tanto formaran parte de la misma. Cabe recalcar que para la configuración de estas cámaras debemos descargar la aplicación de las mismas, la cual podemos encontrar en “google play store”.

1) Una vez descargada la aplicación, procedemos a abrirla y nos da la opción de ingresar mediante número de teléfono o por un correo de Gmail, para las pruebas ingresamos con nuestra cuenta Gmail, obteniendo la siguiente interfaz gráfica. En la figura número 107 se presenta la interfaz de la aplicación que utilizan las cámaras de vigilancia

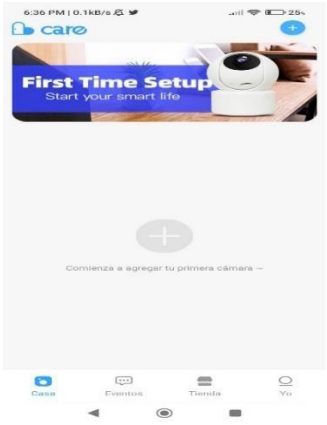


Figure 107 INTERFAZ DE APP “CARECAMPRO”

2) Una vez creada la cuenta, vamos a elegir uno de los modos de conexión, en este caso el de red inalámbrica, por lo tanto, vamos a insertar la clave WIFI en la cámara y esta podrá escanear un código QR para su respectivo enlace. A continuación, en la figura número 108 se presenta la interfaz de emparejamiento que existe entre las cámaras y la app, la cual presenta 3 medios para emparejar.

Figure 108INTERFAZ PARA AGREGAR CÁMARAS A LA APLICACIÓN

3) Escaneamos el código QR y seguimos los pasos para que nuestra cámara se enlace. En la imagen número 109 se presenta el código QR que nos da la app para el emparejamiento de la cámara.

Figure 109 CÓDIGO QR QUE DEBE SER ESCANEADO POR LA CÁMARA

4) Una vez escaneado el código, tendremos en nuestra interfaz gráfica las imágenes que proporciona la cámara. En la imagen número 110 se presenta la interfaz y las imágenes que da la cámara una vez emparejada a la red.

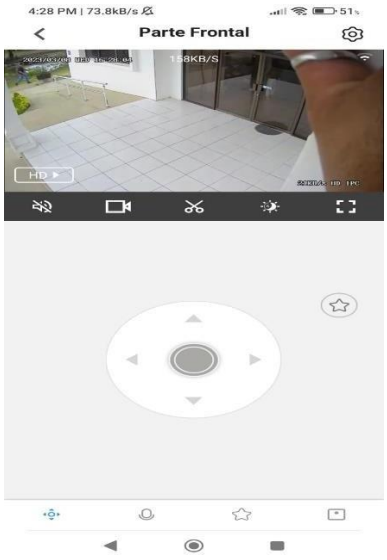


Figure 110 IMAGEN PROPORCIONADA POR LA CÁMARA EN LA APLICACIÓN

5) Realizamos el mismo procedimiento con las demás cámaras obteniendo el siguiente resultado. En la figura número 111 podemos ver todas las cámaras emparejadas y funcionales del INCYT.

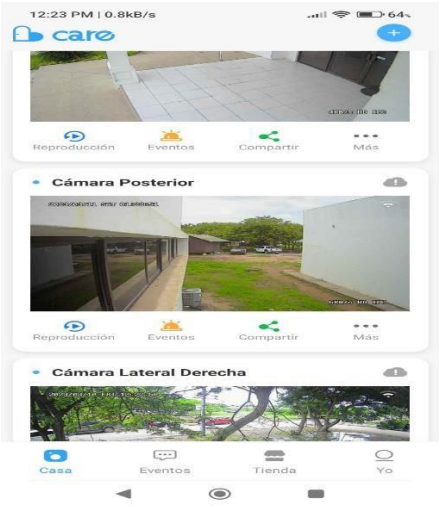


Figure 111 INTERFAZ DE LA APLICACIÓN CON TODAS LAS CÁMARAS ENLAZADAS

3.3.2.2 CONFIGURACIÓN DE ALERTAS PARA LAS CÁMARAS

Las cámaras utilizadas para el sistema inteligente cuentan con movimientos robóticos, sensores de movimiento y seguimiento cuando son configuradas de manera correcta, para este caso, vamos a habilitar las diferentes alertas que esta tiene.

1) Como primer paso una vez vinculadas las cámaras a la APP vamos a ir a la configuración de cada una de ellas y activaremos las alarmas que contienen. A continuación, en la imagen número 112 se presenta la interfaz gráfica de las alertas que tiene la cámara instalada.

Figure 112 INTERFAZ DE LA APLICACIÓN "CARECAMPRO" CONFIGURACIÓN DE ALERTAS

2) Una vez ingresamos a la opción de alertas ajustamos la sensibilidad de las cámaras a la que se desea. En la figura número 113 vemos la configuración de sensibilidad que tiene la cámara.

Figure 113 INTERFAZ DE LA APLICACIÓN "CARECAMPRO" CONFIGURACIÓN DE SENSIBILIDAD DE MOVIMIENTO

3.3.2.3 CONEXIÓN DE CÁMARAS AL CONTROLADOR Y SERVIDOR DE HOME ASSISTANT

Como se mencionó en el capítulo II y III la comunicación de las cámaras a nuestro servidor se realizará mediante protocolo ONVIF, el cual trabaja con la interoperabilidad de varios dispositivos independientemente de la marca, es decir que, con el aplicativo de este protocolo, vamos a poder enlazar cámaras de manera futura, ya sea que sean necesarias más de ellas dentro del edificio. Este tipo de protocolo utiliza el puerto 580, puerto mediante el cual los clientes ONVIF envían solicitudes para flujos de video, adicionalmente el protocolo ONVIF viene de la mano con RTSP que es el protocolo de transmisión en tiempo real, cabe recalcar que las cámaras colocadas en el edificio pueden configurarse mediante este protocolo, ya que es muy similar. El trabajo del protocolo ONVIF es acceder al puerto RTSP de manera directa, utilizando un navegador para recuperar y mostrar video, en el caso del proyecto, utilizamos un navegador para entrar al servidor de HA y monitorear lo que muestran las cámaras.

Para realizar la correcta comunicación entre las cámaras y el servidor, vamos a utilizar el protocolo ONVIF, ya que este nos ayudará a mantener una imagen constante de lo que está sucediendo a los alrededores.

1) Para poder enlazar de manera correcta las cámaras vamos a añadir el complemento "ONVIF" en el servidor de Home Assistant. En la imagen número 114 se presenta la interfaz que nos brinda HA para el uso del protocolo ONVIF.

Figure 114 Interfaz de la configuración "ONVIF" de nuestro servidor (Assistant, 2023)

2) Una vez instalado e iniciado, vamos a colocar la IP de la cámara, el puerto ONVIF con el que trabaja y por ultimo las credenciales que utiliza el fabricante. Usuario: admin, Contraseña: admin12345. Cabe recalcar que el HOST y el puerto a utilizar puede variar según la cámara que se utiliza y el dispositivo en a la red, ya que cada uno de estos mantiene una IP (HOST) diferente.

   A continuación, en la imagen número 115 se presenta la interfaz de configuración del protocolo ONVIF.

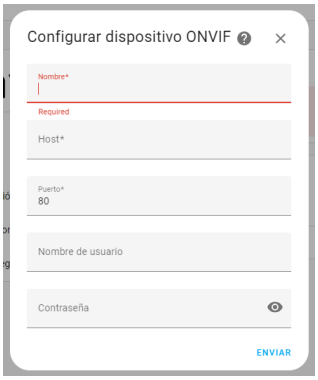


Figure 115 INTERFAZ DE LA CONFIGURACIÓN PARA AÑADIR DISPOSITIVOS MEDIANTE PROTOCOLO ONVIF DE NUESTRO SERVIDOR (Assistant, 2023)

3) Luego procedemos a ingresar las cámaras a nuestra interfaz principal, la cual se mostrará al ingresar al servidor, estas imágenes de video pasan por el puerto utilizado por la cámara y viajan al servidor HA y son presentadas junto con otras acciones que ejecuta la cámara, es decir podemos vincular el protocolo ONVIF a HA a tal punto que podemos controlar y detectar los parámetros de la cámara, como apagado, encendido, reinicio y sensor de movimiento.

   Toda la vinculación de las cámaras se dirigió a una pestaña en la cual el usuario puede ver de una mejor manera las cámaras enlazadas al sistema, que en este caso fueron mencionadas anteriormente.

A continuación, en la figura número 116 se presenta la interfaz de la pestaña “cámaras” que tiene nuestro servidor HA.

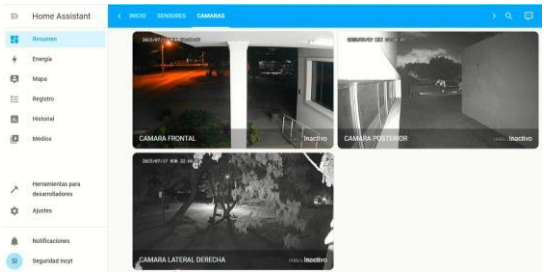


Figure 116 INTERFAZ DE LA PESTAÑA DE “CAMARAS” DE NUESTRO SERVIDOR

3.3.3 UBICACIÓN DE SENSORES

Para la ubicación de los sensores, trabajamos bajo el rango de actuación que tienen los mismo, lo cual fue expuesto en capítulo III, bajo este parámetro, se pudo utilizar la digitalización y colocar los sensores en un punto estratégico el cual puede cubrir zonas internas en el edificio.

Adicionalmente, estos sensores utilizan la tecnología Z wave para la comunicación con el servidor, debido a esto el envío constante de la información será rápido y eficaz, gracias a que esta tecnología utiliza otra frecuencia, el funcionamiento del sistema entre las cámaras y sensores no se verá afectado por el mismo.

A continuación, en la imagen número 117 se presenta el rango en el cual actúa el sensor en la digitalización y en base a eso podemos ver que cubre la entrada principal y las oficinas con fácil acceso al edificio.

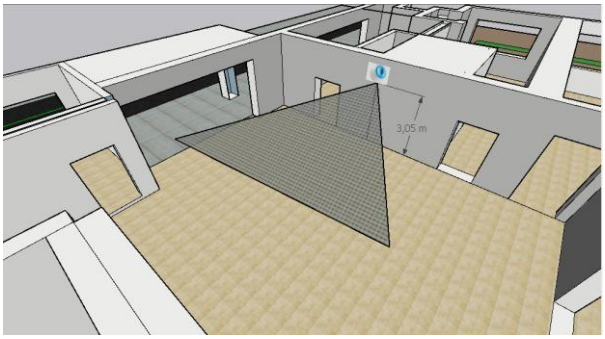


Figure 117 COBERTURA DEL SENSOR COLOCADO EN LA ENTRADA PRINCIPAL

Como podemos observar en la digitalización, el espacio que cubre el sensor es el indicado para detectar movimientos que se producen en el ingreso principal del edificio y adicionalmente el movimiento que se detecta en la mitad del lobby del edificio. A continuación, en la imagen número 118 se presenta el rango de acción que mantiene el sensor en una de las oficinas.

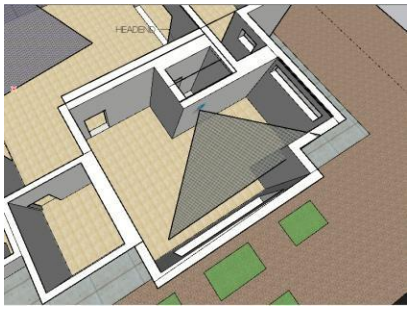


Figure 118 COBERTURA DEL SENSOR COLOCADO EN LA OFICINA DERECHA

Como podemos observar se cubre gran parte de la oficina en la cual se encuentran diversos equipos de trabaja del INCYT como microscopios, máquinas de trabajo, entre otros.

Una vez aclarado el tema de la ubicación en la digitalización, procedemos a explicar el paso a paso de la colocación física de los sensores.

1) Primero se procedió a realizar las perforaciones respectivas en los lugares donde va colocado el sensor, cabe recalcar que los sensores utilizados funcionan a batería y no necesitan estar conectados a la energía eléctrica.

A continuación, en la imagen número 119 se presenta el sensor apuntando a la entrada de la oficina que es la ventana.

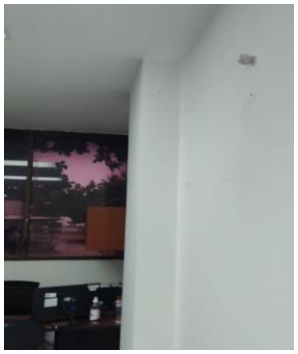


Figure 119 IMAGEN DE NUESTRO SENSOR COLOCADO EN OFICINAS

2) Una realizadas las perforaciones, se procedió a colocar los sensores en su respectivo lugar. Tal y como se muestra en la simulación, los sensores fueron colocados en los puntos clave para cubrir el mayor rango de acción de los mismos. A continuación, en la imagen número 120 se presenta el sensor colocado en la entada principal.

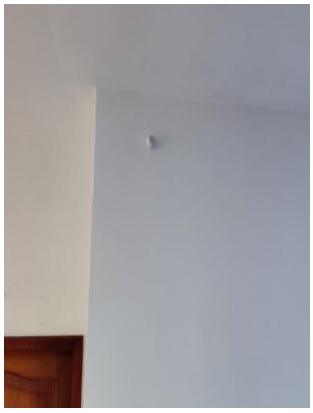


Figure 120 IMAGEN DE NUESTRO SENSOR FUNCIONANDO

3.3.3.1 CONFIGURACION Y COMUNICACIÓN DE SENSORES

Estos sensores FIBARO, funcionan con tecnología Z WAVE, para esto ya debemos tener nuestra red z wave creada, tal y como lo hablamos en capítulos anteriores, con la creación y la instalación del complemento en nuestro HA, esta red

se encuentra lista para ejecutar lecturas y detectar dispositivos que trabajen bajo esta frecuencia.

Para poder configurar los sensores con el servidor creado en nuestro raspberry, debemos tener instalado los complementos a utilizar, lo cual se explicó previamente en el documento, junto a la parte de “creación del servidor”.

1) Primero debemos colocar nuestro sensor en modo inclusión para que nuestro servidor pueda detectarlo y emparejarlo, cabe recalcar que el modo inclusión puede varían en cada dispositivo, en este caso, los sensores ingresan a dicho modo oprimiendo el botón que tiene por 4 veces seguidas.
   A continuación, en la imagen número 121 se presenta la imagen del sensor utilizado.

Figure 121 IMAGEN DEL SENSOR UTILIZADO

2) Cuando nos encontramos en modo inclusión, procedemos a utilizar el complemento instalado en nuestro Home Assistant, el cual escaneará y reconocerá el dispositivo colocado en dicho modo. La red z wave enviará pulsos en su frecuencia para detectar dispositivos que estén a la misma, en este caso son los sensores. A continuación, en la figura número 122 se presenta la interfaz de la red z wave para añadir un dispositivo.

Figure 122 IMAGEN DE CONFIGURACIÓN MEDIANTE PROTOCOLO Z WAVE

3) Una vez reconocido el dispositivo z wave, añadimos el sensor a nuestro servidor, para una mejor perspectiva visual, lo colocamos en nuestro panel principal. Como podemos observar en la imagen número 123 el sensor z FIBARO nos muestra el estado de la batería, la temperatura y si detectó o no un movimiento.

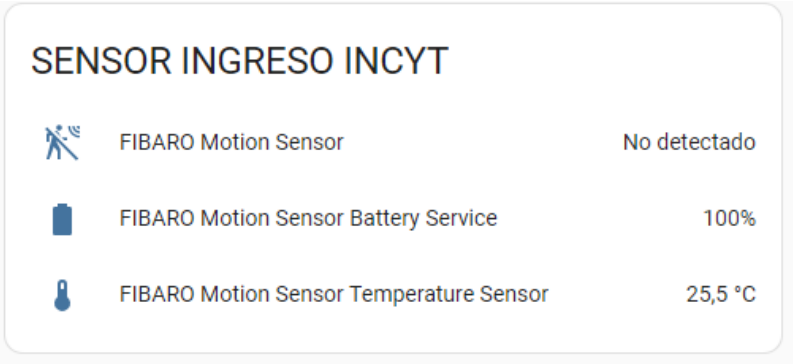


Figure 123 IMAGEN DE DATOS QUE MUESTRA EL SENSOR TRABAJANDO

3.4 ~~ESTUDIO DE~~ FACTIBILIDAD de la propuesta

3.4.1 FACTIBILIDAD TÉCNICA

Este proyecto es un sistema de monitoreo basado en tecnologías z wave y onvif para salvaguardar la seguridad no solo de los bienes, sino también de las personas que se encuentran en el INCYT. Con este proyecto se planteó mantener un monitoreo constante de los alrededores del edificio para generar un ambiente seguro y tecnológico.

Los dispositivos colocados debido a su tecnología son comunes en el mercado de la tecnología, ya que trabajan bajo protocolos que son conocidos, en este caso es el ONVIF y el Z WAVE, la integración de esta tecnología en la universidad abre puertas a futuras implementaciones tecnológicas basadas en los mismos protocolos, existen dispositivos distintos como alarmas, sensores de puertas, sensores de humos que pueden ser emparejados con el sistema actual del HA.

Estos productos se encuentran a la mano económicamente, ya que los dispositivos utilizados no son costosos debido a su tecnología, es lo que lo diferencia de otros equipos más avanzados, sin embargo, podemos obtener resultados buenos utilizando productos que mantienen un coste constante en el mercado, tal y como lo son los sensores, raspberry, antenas y videocámaras.

Debido a lo antes mencionado, el sistema con esta tecnología es eficaz ya que trabajan en frecuencias diferentes a los equipos que mantiene el INCYT, adicionalmente se puede tener un monitoreo constante y unificado de varios aspectos cercanos al edificio, gracias a la integración que nos brinda nuestro servidor en HA.

CAPÍTULO IV

RESULTADOS DE LA PROPUESTA

4.1 PRUEBAS

Para cumplir con los resultados esperados que fueron escritos en el capítulo I, se realizaron distintas pruebas y simulaciones, a continuación, se muestran las mismas divididas en secciones.

COBERTURA DE PUNTOS VULNERABLES EN LAS INSTALACIONES DEL INCYT

Para poder visualizar de una mejor manera los puntos vulnerables que existen en la edificación se realizó una digitalización del mismo en el software Sketchup, tal cual se mostró en el capítulo III del presente documento. Esto nos llevó a encontrar puntos vulnerables a los exteriores del edificio, debido a esto se optó por instalar cámaras de videovigilancia para mantener una visión constante de dichos puntos. En el caso de la parte interna, se instalaron sensores de movimiento, temperatura y luz. Todos estos nodos instalados envían datos al servidor creado en Home Assistant para mantener la información unificada y que tenga una interfaz amigable con el usuario.

A continuación, en la imagen número 124 se presenta la interfaz de las cámaras en el servidor Home Assistant, las cuales cubren los ingresos al edificio. La tecnología de comunicación de las cámaras con el servidor es mediante el protocolo ONVIF, el cual fue explicado a más detalle en el capítulo III cuando se habló de la configuración del mismo.

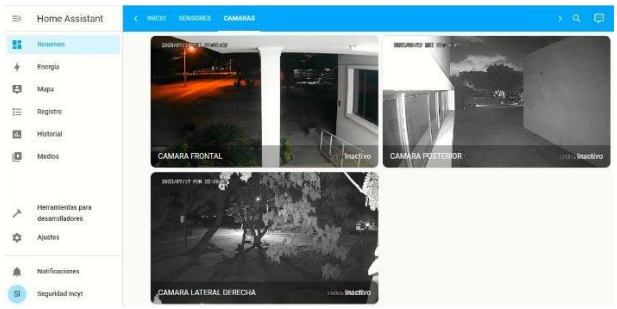


FIGURE 124 IMAGEN DE VIDEO TOMADAS POR LAS CÁMARAS INSTALADAS

Para los puntos vulnerables y mayor vigilancia de la parte interna del edificio, se colocaron sensores para mantener una vigilancia complementando las cámaras de seguridad. Como se habló en el capítulo III, estos sensores están colocados de tal manera que cumplan con la función de detectar cambios en los parámetros del mismo (detección de movimiento, cambios en la intensidad de luz y cambios en la temperatura).

A continuación, en la imagen 125 se presenta la interfaz de los sensores en el servidor Home Assistant, las cuales ayudan a cubrir los ingresos más vulnerables del edificio. La tecnología de comunicación de los sensores con el servidor es mediante el protocolo Z-WAVE, el cual fue explicado a más detalle en el capítulo III cuando se habló de la configuración del mismo.

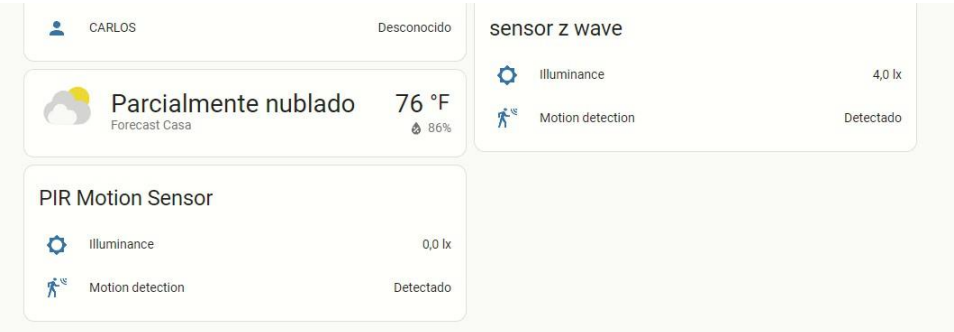


FIGURE 125 IMAGEN DE LA INTERFAZ DE LOS SENSORES FUNCIONALES EN HOME ASSISTANT

MONITOREO DE PUNTOS VULNERABLES Y PARÁMETROS DE LAS CÁMARAS Y SENSORES

Para mantener un monitoreo correcto y óptimo de las instalaciones del INCYT, se configuraron las cámaras y sensores de tal manera de que estos sean sensibles a cambios en especial a altas horas de la noche, esto debido a que en este periodo de tiempo el edificio no cuenta con personas que se encarguen de su seguridad y las entradas que tienen son de fácil acceso.

Las cámaras de videovigilancia cuentan con detección de movimiento, comunicación bidireccional y visión nocturna, estas características y muchas más fueron indicadas en el capítulo III, gracias a esto podemos configurar opciones para mantener en alerta a las mismas.

Los sensores cuentan con parámetros que se pueden alterar, ya sea la sensibilidad tanto de movimiento como de luz. Para un mejor entendimiento de los parámetros mencionados se explicarán a continuación.

En la imagen número 126 podemos observar los distintos parámetros que se manejan tanto en las cámaras como en los sensores.

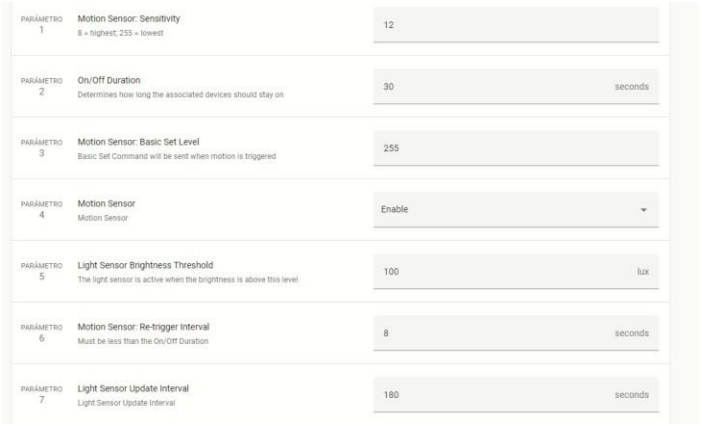


FIGURE 126 PARÁMETROS MANEJADOS EN EL PROYECTO

UNIFICACIÓN DE DATOS DE LOS DISTINTOS NODOS EN UN SOLO SERVIDOR

Para poder monitorear de una mejor manera y aplicar conceptos de domótica al proyecto se optó por unificar los datos de entrada y salida de los nodos en un solo servidor, gracias a esto se aplicaron conceptos para mejorar la interfaz final de usuario. En el capítulo III, se explica la forma de crear y unificar los datos enviados por la cámaras y sensores instalados en el INCYT.

A continuación, en la imagen 127 se muestra una captura de pantalla de la aplicación WhatsApp, enviada por nuestro servidor en Home Assistant.

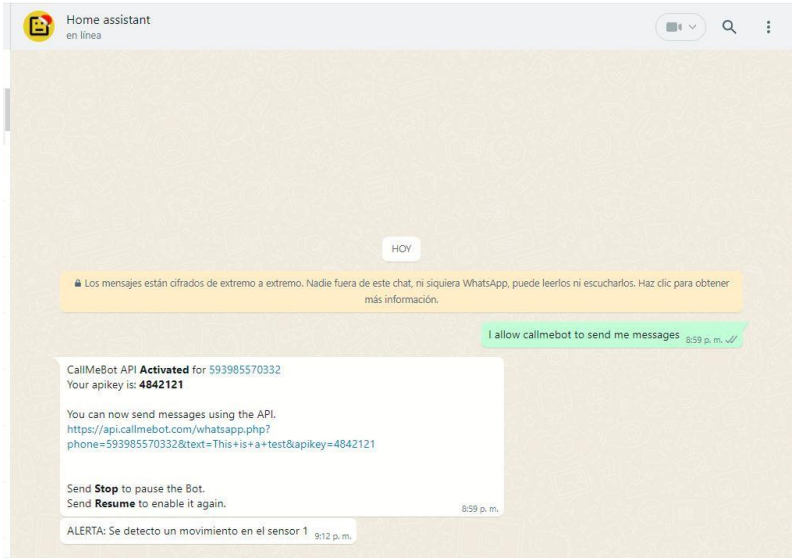


Figure 127 ALERTA ENVIADA POR EL SERVIDOR

Como se ve en la imagen anterior, el sensor detectó un movimiento y el servidor mandó un mensaje al número de WhatsApp registrado, en este caso para las pruebas utilicé mi número personal. Este tipo de configuraciones son aplicables gracias a la parte domótica en el proyecto, podemos estar alertas e informados en cualquier momento.

A continuación, en la imagen 128 se presenta una imagen del código para que las alertas del servidor puedan ser efectuadas.

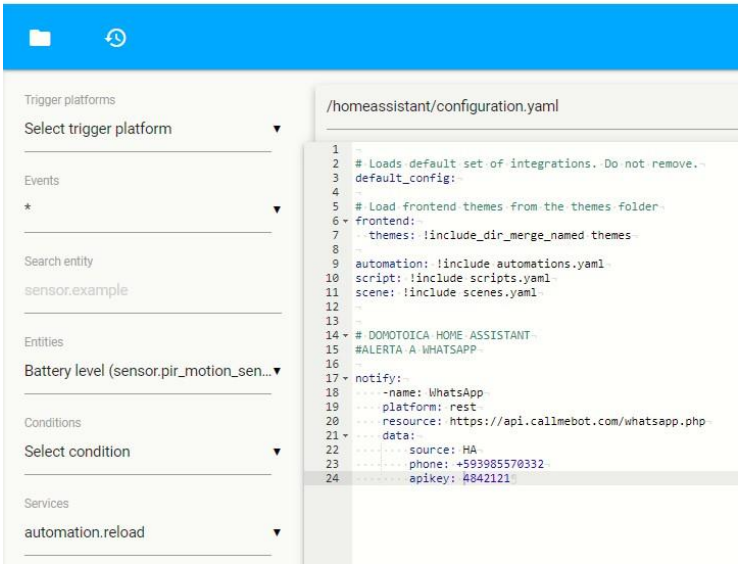


Figure 128 CODIGO PARA DOMOTICA

En la figura anterior podemos observar el código para que el servidor envíe alertas a WhatsApp. A si mismo podemos utilizar variaciones en el código para recibir alertas por distintas maneras.

Este proyecto queda abierto y como pionero para que futuras generaciones puedan trabajar en la parte domótica y el servidor pueda tener mejoras continuas según sea necesarias.

COMUNICACIÓN DE LOS NODOS INSTALADOS MEDIANTE PROTOCOLO Z-WAVE

Como se explica en el capítulo II y el capítulo III, el protocolo de comunicación principal es el Z-WAVE, una vez enlazados los nodos con el servidor creado en Home Assistant, la tecnología Z-WAVE se encarga de enviar y recibir datos, en este caso se toma los datos de los sensores instalados como ejemplo.

A continuación, en la figura 129 se muestra el comportamiento de un sensor instalado.

Figure 129 DATOS TOMADOS POR EL SENSOR FIBARO

Como podemos observar tenemos dos estados del sensor, “detectado” y “no detectado”, estas pruebas se realizan en un lapso de tiempo para verificar el correcto funcionamiento del sensor.

Una vez teniendo claro que el sensor envía y recibe datos, vamos a comprobar que la transmisión mediante el protocolo Z-WAVE es la más óptima, debido a que el envío y recepción de datos se maneja en una frecuencia distinta a la 2.4GHz y 5 GHz.

A continuación, en la imagen 130 se muestra una captura de la configuración Z-WAVE que tiene el servidor para los sensores.

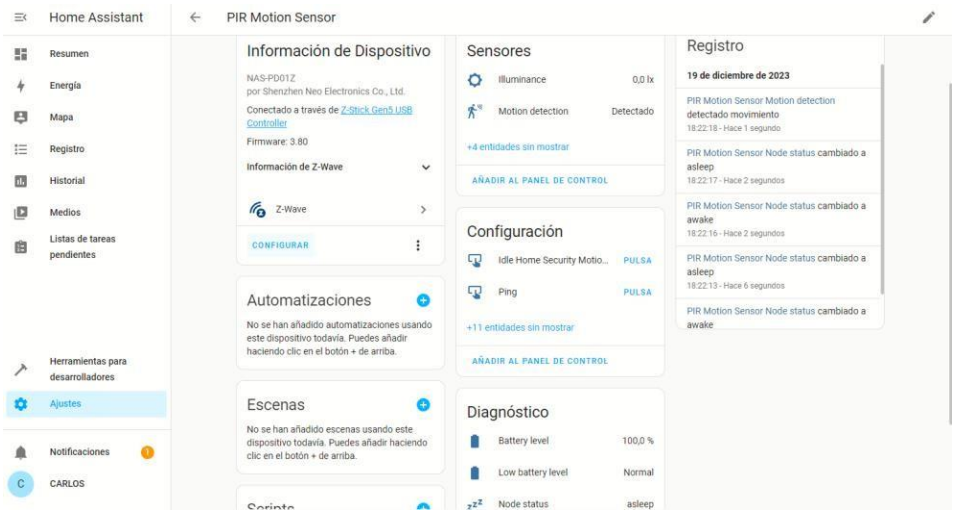


Figure 130 REGISTRO DE DATOS DEL SENSOR Z-WAVE

Como podemos ver en la imagen anterior, se muestra la configuración de la pestaña Z-WAVE adjuntando una pestaña de registro en la cual se realizan pruebas y el envío y recepción de datos son constantes. Se observa en la figura el estado del sensor, este varia en “asleep” y “awake”, estos dos datos son enviados de

manera constante para el cambio que tendrá el sensor, una vez detectado un movimiento o cambio de parámetro, el registro lo recibirá como “movimiento detectado”. Todos estos datos son enviados por el nodo Z-WAVE y recibidos por el servidor mediante la antena colocada “Z STICK” mencionada en el capítulo III.

Otra prueba adjunta para la comunicación Z-WAVE son los datos y mensajes que envía el sensor al controlador.

A continuación, en la imagen número 131 se muestra una captura de datos enviados por un sensor.

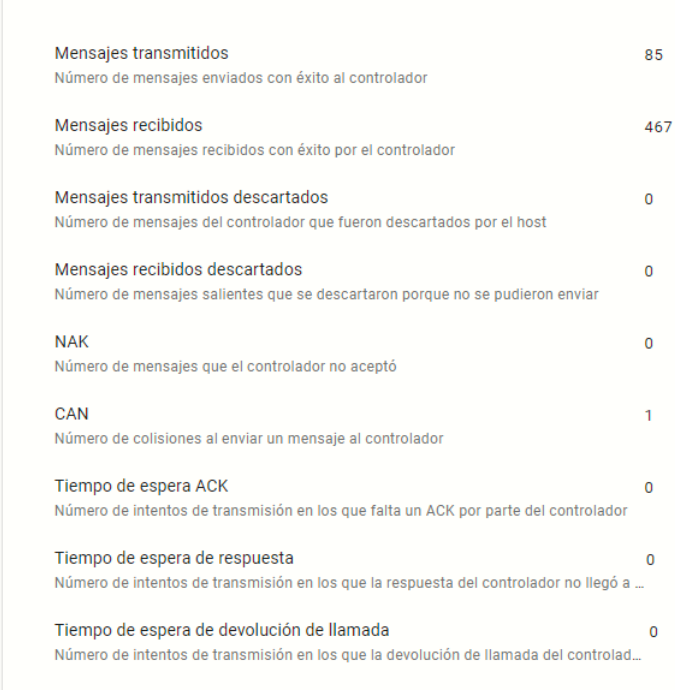


Figure 131 MENSAJES DEL SENSOR Z-WAVE

Como podemos observar en la imagen anterior el sensor transmitió 85 mensajes con éxito al controlador que este caso es el servidor creado, se detallan mensajes recibidos por el mismo, cabe recalcar que el número es mayor debido a las pruebas realizadas. Estos parámetros nos ayudan a comprobar el funcionamiento correcto del envío de datos mediante la tecnología Z-WAVE, como se habló en el capítulo III el servidor puede recibir distintos datos, pero en esta

imagen se aprecia que son pocos aquellos datos que se envían mediante esta frecuencia especifica.

Toda esta información se encuentra detallada en el servidor y es de fácil acceso para el usuario final.

4.2 CONCLUSIONES Y RECOMENDACIONES

4.2.1 CONCLUSIONES

- Para la implementación de las cámaras y sensores fue necesario realizar una digitalización para poder centrarse en los puntos vulnerables que existían en el edificio, cabe recalcar que no se podían cubrir en su totalidad esos puntos, pero si se podían cubrir zonas de fácil acceso y zonas aledañas a los mismos, gracias a esto se eligieron equipos que cubran con esas necesidades, en conclusión se obtuvo que la implementación de los equipos fue de gran ayuda para mejorar la seguridad no solo del edificio, sino también de zonas aledañas al mismo. Bajo este criterio podemos decir que se cubrió el 80% se zonas de fácil ingreso al edificio.
- Existen variedades de protocolos de comunicación compatibles con la plataforma Home Assistant, sin embargo, al realizar investigaciones sobre los dispositivos encontramos varias ventajas y desventajas, las cuales explicamos en el documento, debido a este elegimos los protocolos ONVIF y Z-WAVE para la comunicación según sus características.
- Al utilizar Home Assistant como plataforma para el servidor se desbloquearon varias funciones e inclusive sirven para en algún futuro integrar más tecnologías compatibles, ya que el mismo funciona con varias tecnologías las cuales explicamos en el documento. El 100% del proyecto se centra en el servidor ya que este es el encargado de unificar los equipos utilizados y

según las pruebas realzadas podemos decir que la implementación fue exitosa.

- En cuanto a la comunicación Z WAVE y el controlador, podemos concluir que fue realizada de manera correcta, tal y como se muestra en el sensor y su envío de información constante, lo cual nos indica que la comunicación mediante el uso de este protocolo es estable y segura. Con esto podemos indicar que el 50% de comunicación es realizada con éxito.

4.2.2 RECOMENDACIONES

- Se recomiend~~o~~a a futuras generaciones mantener un diagrama digitalizado del edificio, ya que gracias a esto podrán verificar alguna zona nueva o fundamental para colocar otros tipos de elementos que trabajen bajo esta misma tecnología.
- Debido a la demanda de protocolos y puertos de internet que requiere este sistema, se recomienda mantener actualizado los puertos de los switches que posee el edificio, esto es necesario para que nuestro servidor se mantenga actualizado y funcional.
- Se recomienda segmentar la cola de redes para darle prioridad a funciones que utiliza el sistema z wave, la transmisión remota de los dispositivos en tiempo real, necesita de protocolos tales como IPV6 y UPNP los cuales se encargan de ejecutar acciones para poder mantener funcional el sistema.
- Se recomienda darles mantenimiento a los equipos instalados, con esto se refiere a reiniciar, actualizar ya sea el caso, cabe recalcar que la red que se deja en las instalaciones es de fácil manipulación, ya que la interfaz de usuario es intuitiva y amigable con el mismo.

4.3 BIBLIOGRAFIA

1 Acceso, G. (06 de 06 de 2022). *rayte.com*. Recuperado el 28 de 01 de 2023, de https://rayte.com/blog/post/5-tipos-de-arduino

2 aeotec.freshdesk. (03 de 06 de 2022). *aeotec.freshdesk.com*. Recuperado el 20 de 01 de 2023, de https://aeotec.freshdesk.com/support/solutions/articles/6000056439-z-stick-gen5-user-guide-

3 AEOTECH. (2023). *https://www.aotech.es/*. Recuperado el 12 de SEPTIEMBRE de 2023, de https://www.aotech.es/

4 Aguayo, H. (junio de 2021). *casainteligentewifi*. Recuperado el 02 de Septiembre de 2023, de https://casainteligentewifi.com/riego-inteligente/

5 alaisecure. (s.f.). *alaisecure*. (Grupo Ingenium Tecnologia) Recuperado el 01 de Diciembre de 2022, de https://alaisecure.co/glosario/radiofrecuencia-en-telecomunicaciones-que-es-y-como-funciona/#:~:text=La%20radiofrecuencia%20se%20define%20como,los%203%20kilohercios%20(KHz).

6 ANDRANGO, M. L. (2007). *ESTUDIO DEL PROTOCOLO CAN (CONTROLLER AREA.* QUITO.

7 ARDUINO. (2022). *Arduino Leonardo.*

8 ARDUINO. (ENERO de 2022). *docs.arduino.cc*. Recuperado el 08 de SEPTIEMBRE de 2023, de https://docs.arduino.cc/hardware/due

9 ARDUINO. (2023). *Arduinon UNO R3 .*

10 ARENY, R. P. (2005). *SENSORES Y ACONDICIONADORES DE SEÑAL (4ª ED.).* MARCOMBO.

11 argos. (s.f.). *argos.red*. Recuperado el 01 de 03 de 2023, de https://argos.red/protocolo-onvif/#:~:text=El%20protocolo%20ONVIF%20es%20un,instalaci%C3%B3n%20y%20desarrollo%20de%20software.

12 Assistant, H. (25 de Agosto de 2023). *192.168.100.27*. Recuperado el 18 de Septiembre de 2023, de https://192.168.100.27:8123

13 Avello, A. J. (Noviembre de 2021). *automaticaeinstrumentacion*. (automaticaeinstrumentacion) Recuperado el 28 de Agosto de 2023, de

https://www.automaticaeinstrumentacion.com/texto-diario/mostrar/3293017/control-inteligente-procesos

14 Bernal, B. (2019). *El protocolo Z-Wave desde la.* Cartagena.

15 Camilo Moreno Serrano, J. O.-M. (2021). *Diseño y desarrollo de un laboratorio de pruebas basados en Smart Home aplicando protocolo de comunicación Z-Wave y estándar 802.11.* Milagro.

16 Carlos Araya Guzmán, G. G. (2018). *Implementación de niveles de ciberseguridad.* San José, Costa Rica.

17 Controls, J. (s.f.). *www.johnsoncontrols.com*. (Jhonson Controls) Recuperado el 15 de 08 de 2022, de https://www.johnsoncontrols.com/es_es

18 DIgital, H. (s.f.). *hogardigitalaccesible*. Recuperado el 05 de Septiembre de 2023, de https://hogardigitalaccesible.etsist.upm.es/tecnologias/tecnologias-lonworks/

19 Dignani, J. (2011). *postgrado.info.unlp.edu.ar.* Obtenido de https://postgrado.info.unlp.edu.ar/wp-content/uploads/2014/07/Dignanni_Jorge_Pablo.pdf

20 Dignani, J. P. (2011). *http://sedici.unlp.edu.ar/.* Recuperado el 20 de 01 de 2023, de http://sedici.unlp.edu.ar/bitstream/handle/10915/18349/Documento_completo_.pdf?sequence=1&isAllowed=y

21 ESQUEMA. (Junio de 2021). *esquema.net*. Recuperado el 08 de Septiembre de 2023, de https://esquema.net/espectro-electromagnetico-2/

22 F5. (s.f.). *www.f5.com*. (F5) Recuperado el 22 de Noviembre de 2022, de https://www.f5.com/es_es/services/resources/glossary/wireless-network-security

23 Fernandez, D. (19 de Julio de 2018). *tecnonucleous.com*. Recuperado el 16 de Septiembre de 2023, de https://tecnonucleous.com/2018/07/19/que-es-home-assistant/#:~:text=Home%20Assistant%20se%20encargar%C3%A1%20de,WeMo%20y%20incluso%20dispositivos%20Xiaomi.

24 FERNANDO BANDÉS, S. D. (2009). *TOMO VI BIOMEDICINA Y DERECHO SANITARIO.* ADEMAS.

25 FIBARO. (2014). *manuals.fibaro.com.* Recuperado el 14 de SEPTIEMBRE de 2023, de https://manuals.fibaro.com/content/manuals/us/FGMS-001/FGMS-001-USA-A-v1.01.pdf

26 FIBARO. (2023). *www.fibaro.com*. Recuperado el 13 de SEPTIEMBRE de 2023, de https://www.fibaro.com/cl/products/motion-sensor/

27 Flores, J. S. (Marzo de 2007). *bibdigital.epn.* Recuperado el 06 de Septiembre de 2023, de https://bibdigital.epn.edu.ec/bitstream/15000/391/1/CD-0798.pdf

28 FOSCAM. (2011). *CAMARAS IP FOSCAM MANUAL DE USUARIO.*

29 GARCIA, A. J. (2015). *Comunicacion multimaestro a traves de partrenzado RS-485.*

30 García, C. J. (2018). *Integración de tecnología domótica Z-Wave en la plataforma FIBARO.* Sevilla.

31 Gijón, E. I. (FEBRERO de 2018). *isa.uniovi*. Recuperado el 05 de ENERO de 2023, de http://isa.uniovi.es/docencia/AutomEdificios/transparencias/sensores.pdf

32 Integra, Nexus. (2022). *Nexus Integra.io*. Recuperado el 18 de Agosto de 2023, de https://nexusintegra.io/es/5-edificios-mas-inteligentes-del-mundo/

33 Jimenéz, J. M. (2016). *El protocolo zigbee como recurso a la tecnología en la agricultura de.* Recuperado el 21 de 01 de 2023, de https://repository.unicatolica.edu.co/bitstream/handle/20.500.12237/806/FUCLG0016629.pdf?sequence=1&isAllowed=y

34 Luis Miguel Amaya Fariño, A. T. (2020). El IoT aplicado a la Domótica. *Revista Científica y Tecnológica UPSE, 1*, 8.

35 MANUALS. (ABRIL de 2022). *manuals.plus*. Recuperado el 11 de Septiembre de 2023, de https://manuals.plus/es/arebi/hidden-cameras-for-home-security-1080p-hd-mini-spy-camera-wifi-wireless-complete-features-instruction-guide-2#axzz8DCab8AX3

36 MAPFRE. (Febrero de 2023). *MAPFRE*. Recuperado el 03 de Septiembre de 2023, de https://www.mapfre.es/particulares/seguros-de-hogar/articulos/aplicaciones-domotica-para-un-hogar-seguro/

37 Martín, A. (2018). *OVACEN*. Recuperado el 01 de Septiembre de 2023, de https://ovacen.com/tipos-sistemas-de-climatizacion-ejemplos/

38 Martínez, T. (Diciembre de 2012). *telequismo*. (telequismo) Recuperado el 02 de Diciembre de 2022, de https://www.telequismo.com/2012/12/banda-libre-vs-banda-licenciada.html/

39 MecatrónicaLATAM. (04 de Mayo de 2021). *MecatrónicaLATAM*. Recuperado el 11 de Septiembre de 2023, de

https://www.mecatronicalatam.com/es/tutoriales/sensores/#:~:text=distancia%20y%20vibraci%C3%B3n.-,Caracter%C3%ADsticas%20din%C3%A1micas%20de%20un%20sensor,su%20valor%20de%20estado%20estable.

40 Mesias, G. D. (2014). *“Sistema de control y monitoreo para mejorar los procesos de administración de.* Ambato-Ecuador.

41 MOLLOY, D. (s.f.). *Raspberry Pi a fondo para desarrolladores.*

42 mordorintelligence. (2021). *mordorintelligence*. Recuperado el 12 de Septiembre de 2023, de https://www.mordorintelligence.com/es/industry-reports/color-detection-sensor-market-growth-trends-forecast-2019-2024

43 mordorintelligence. (2021). *mordorintelligence.com*. Recuperado el 12 de Septiembre de 2023, de https://www.mordorintelligence.com/es/industry-reports/motion-sensor-market

44 Moreno Serrano Camilo, O. M. (2021). *Diseño y desarrollo de un laboratorio de pruebas basados en Smart Home aplicando protocolo de comunicación Z-Wave y estándar 802.11.* Milagro-Ecuador.

45 Moreno, M. (2007). *Informe Técnico: Protocolo ZigBee.* Alicante.

46 NN. (2022). *blog.gruponovelec*. Recuperado el 05 de Septiembre de 2023, de https://blog.gruponovelec.com/blog/automatizando-supervisando-calidad-vida-knx/#:~:text=El%20sistema%20KNX%20es%20un,(ISO%2FIEC%2014543).

47 Optris. (2022). *www.mesurex.com.* Recuperado el 10 de Septiembre de 2023, de https://www.mesurex.com/wp-content/uploads/2018/04/folleto-camaras-infrarrojas-1.pdf

48 ORACLE. (2019). *ORACLE*. (ORACLE) Recuperado el 22 de Noviembre de 2022, de https://www.oracle.com/ar/internet-of-things/what-is-iot/

49 Pedrera, A. C. (2017). *Arduino para principiantes.* España.

50 PENTADOM. (s.f.). *PENTADOM*. Recuperado el Junio de 2023, de https://pentadom.com/tipos-de-sensores-para-domotica/

51 PÉREZ ALTAMIRANO CRISTIAN GEOVANNY, V. T. (2022). *repositorioupse.* Recuperado el AGOSTO de 2023

52 Peters, R. (Febrero de 2015). *usermanual.wik.* Recuperado el 15 de Septiembre de 2023, de https://usermanual.wiki/Pdf/DomoticzManuales.606702014/html

53 Pineda, Á. d. (DICIEMBRE de 2015). *riuma.uma.* Recuperado el 3 de ENERO de 2023, de https://riuma.uma.es/xmlui/bitstream/handle/10630/11444/A.J.%20Garc%C3%ADa%20Pineda_TFG.pdf?sequence=1#:~:text=Maestro%2Desclavo%20(Master%2Dslave,conocidos%20como%20esclavos%20o%20slaves).

54 PORTAFOLIO. (Septiembre de 2022). *PORTAFOLIO.CO*. Recuperado el 25 de Agosto de 2023, de https://www.portafolio.co/tendencias/mas-del-20-de-hogares-tendran-dispositivos-inteligentes-en-el-2025-571374

55 Profesional, T. (26 de Noviembre de 2019). *tdtprofesional*. Recuperado el 07 de Septiembre de 2023, de https://www.tdtprofesional.com/blog/z-wave-vs-knx/

56 RASPBERRY. (DICIEMBRE de 2022). *datasheets.raspberrypi.com*. Recuperado el 09 de SEPTIEMBRE de 2023, de https://datasheets.raspberrypi.com/

57 raspberrypi.org. (s.f.). *raspberry pi 3 Modelo B+ datasheet.*

58 Ricardo Alfonso Pinto García, A. F. (2004). *Sistemas de comunicaciones ópticas.* Bogota.

59 Rojas, G. (2021). *Sistema de iluminacion DALI.* Caracas.

60 Salazar, J. (2016). *Redes Inalambricas.*

61 Salazar, J. (s.f.). *Redes Inalámbricas.* Republica Checa.

62 Sarachu, E. (05 de Mayo de 2022). *e-ficiencia.com.* Recuperado el 25 de Noviembre de 2022, de https://e-ficiencia.com/domotica-que-es-y-como-funciona/

63 Seguridad, R. (21 de Enero de 2022). *revistaseguridad360.com*. Recuperado el 07 de Septiembre de 2023, de https://revistaseguridad360.com/destacados/que-es-onvif/

64 SHOP, C. (2023). *claroshop.com*. Recuperado el 14 de SEPTIEMBRE de 2023, de https://www.claroshop.com/producto/14420666/camara-de-seguridad-domo-wifi-ptz-vigilancia-ir-2mp-1080p-ip66

65 SIMON. (30 de Junio de 2021). *simonelectric.com.* Recuperado el 26 de Noviembre de 2022, de https://www.simonelectric.com/blog/que-puede-aportar-la-seguridad-domotica-un-hogar#:~:text=%C2%BFQu%C3%A9%20es%20la%20seguridad%20dom%C3%B3tica,un%20peligro%20para%20las%20personas.

66 Soler, A. B. (2014). *https://upcommons.upc.edu/.* Recuperado el 22 de 02 de 2023, de https://upcommons.upc.edu/bitstream/handle/2099.1/22360/PROYECTO%20FINAL%20DE%20CARRERA.pdf?sequence=4&isAllowed=y

67 Solís, D. S. (2014). *biblus.us.es.* Recuperado el 13 de SEPTIEMBRE de 2023, de https://biblus.us.es/bibing/proyectos/abreproy/90064/fichero/TFG+-+Daniel+Sierra+Sol%C3%ADs.pdf

68 TACO, I. S. (JULIO de 2009). *bibdigital.epn.* Recuperado el 27 de DICIEMBRE de 2022, de https://bibdigital.epn.edu.ec/bitstream/15000/4170/1/CD-2515.pdf

69 TECNOSEGURO. (s.f.). *tecnoseguro.com*. (TECNOSEGURO) Recuperado el 28 de NOVIEMBRE de 2022, de https://www.tecnoseguro.com/faqs/domotica/que-es-domotica-tipos

70 Telectronika. (20 de Septiembre de 2022). *telectronika.com*. Recuperado el 20 de Septiembre de 2023, de https://www.telectronika.com/tutoriales/como-hacer-un-cable-de-red-ethernet-utp/

71 Toro, D. L. (Mayo de 2015). *bibdigital.epn.edu.ec.* Recuperado el 09 de Septiembre de 2023, de https://bibdigital.epn.edu.ec/bitstream/15000/10770/1/CD-6313.pdf

72 trendnet. (2023). *trendnet.com*. Recuperado el 10 de Septiembre de 2023, de https://www.trendnet.com/langsp/products/3MP-PTZ-ip-cameras/TV-IP420P

73 unnotekno.com. (2023). *unnotekno.com*. Recuperado el 10 de Septiembre de 2023, de https://unnotekno.com/es/product/smart-wifi-indoor-camera-cam8cm1408wt

74 VADAVO. (5 de Noviembre de 2021). *www.vadavo.com*. (VADAVO) Recuperado el 2022 de Noviembre de 22, de https://www.vadavo.com/blog/protocolos-seguridad-inalambrica-wep-wpa-wpa2-wpa3/

75 Vega, R. (08 de Febrero de 2017). *ricveal.com*. Recuperado el 14 de Septiembre de 2023, de https://ricveal.com/blog/domotica-libre

76 VELÁSQUEZ, G. A. (2015). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DOMÓTICO DE.* Recuperado el 25 de JULIO de 2023, de https://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/30126/D-100156.pdf?sequence=1&isAllowed=y

77 Ventilación, S. (2022). *siberzone.es*. Recuperado el 12 de Septiembre de 2023, de https://www.siberzone.es/blog-sistemas-ventilacion/sensor-humedad/

78 VICON. (2023). *vicon-security.com.* Recuperado el 10 de Septiembre de 2023, de https://www.vicon-security.com/wp-content/uploads/2020/05/4.8-2020-Vicon-Camera-Guide-SP-web.pdf

79 Viera, G. (2017). *PROCESAMIENTO DE IMÁGENES.* Piura.

80 Xiaomi. (s.f.). Mi Home.

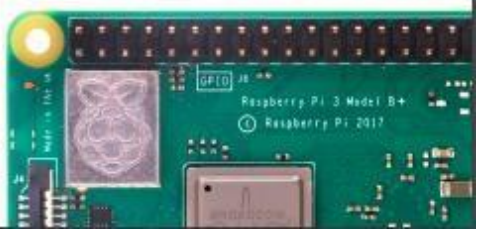
81 ZAPATA, J. A. (2014). *ESTUDIO Y DISEÑO DE UN SISTEMA DE CÁMARAS DE SEGURIDAD PARA LA I.E.S.T.P.* TALARA.

4.4 ANEXOS

DATASHEET RASPBERRY PI 3 B+

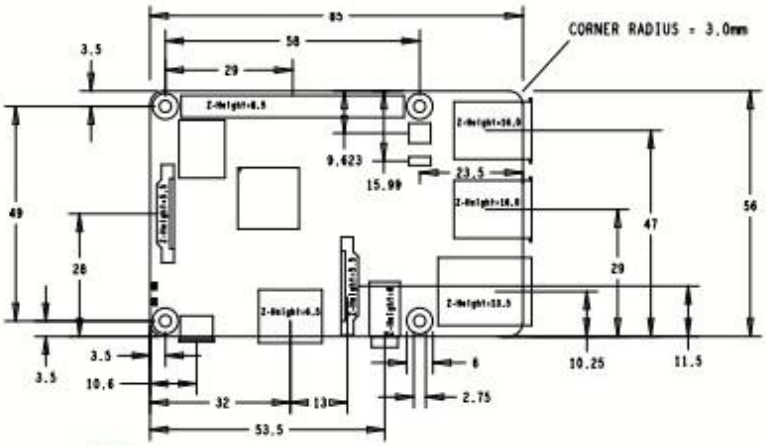
Specifications

Processor:	Broadcom BCM2837B0, Cortex-A53 64-bit SoC @ 1.4GHz
Memory:	1GB LPDDR2 SDRAM
Connectivity:	■ 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE ■ Gigabit Ethernet over USB 2.0 (maximum throughput 300Mbps) ■ 4 × USB 2.0 ports
Access:	Extended 40-pin GPIO header
Video & sound:	■ 1 × full size HDMI ■ MIPI DSI display port ■ MIPI CSI camera port ■ 4 pole stereo output and composite video port
Multimedia:	H.264, MPEG-4 decode (1080p30); H.264 encode (1080p30); OpenGL ES 1.1, 2.0 graphics
SD card support:	Micro SD format for loading operating system and data storage
Input power:	■ 5V/2.5A DC via micro USB connector ■ 5V DC via GPIO header ■ Power over Ethernet (PoE)–enabled (requires separate PoE HAT)
Environment:	Operating temperature, 0–50°C
Compliance:	For a full list of local and regional product approvals, please visit www.raspberrypi.org/products/raspberry-pi-3-model-b+
Production lifetime:	The Raspberry Pi 3 Model B+ will remain in production until at least January 2023.



raspberrypi.org

Physical specifications



Warnings

- This product should only be connected to an external power supply rated at 5V/2.5 A DC. Any external power supply used with the Raspberry Pi 3 Model B+ shall comply with relevant regulations and standards applicable in the country of intended use.
- This product should be operated in a well-ventilated environment and, if used inside a case, the case should not be covered.
- Whilst in use, this product should be placed on a stable, flat, non-conductive surface and should not be contacted by conductive items.
- The connection of incompatible devices to the GPIO connection may affect compliance, result in damage to the unit, and invalidate the warranty.
- All peripherals used with this product should comply with relevant standards for the country of use and be marked accordingly to ensure that safety and performance requirements are met. These articles include but are not limited to keyboards, monitors, and mice when used in conjunction with the Raspberry Pi.
- The cables and connectors of all peripherals used with this product must have adequate insulation so that relevant safety requirements are met.

Safety instructions

To avoid malfunction of or damage to this product, please observe the following:

- Do not expose to water or moisture, or place on a conductive surface whilst in operation.
- Do not expose to heat from any source; the Raspberry Pi 3 Model B+ is designed for reliable operation at normal ambient temperatures.
- Do not expose the printed circuit board to high-intensity light sources (e.g. xenon flash or laser) whilst in operation.
- Take care whilst handling to avoid mechanical or electrical damage to the printed circuit board and connectors.
- Whilst it is powered, avoid handling the printed circuit board, or only handle it by the edges to minimise the risk of electrostatic discharge damage.

MANUAL DE USUARIO SENSOR FIBARO

USA

Distributed by Fibaro
1540 East Lake Ave. Glenview, IL 60025, USA
www.fibaro.com

OPERATING MANUAL
FIBARO MOTION SENSOR
FGMS-001-USA-A-V1.01

The Fibaro Motion Sensor is a universal Z-Wave multi-sensor. Along with detecting motion the device measures the temperature and light intensity. The sensor has a built-in accelerometer to detect any tampering of the device. The Fibaro Motion Sensor is battery powered device and designed to be installed quickly and easily on any surface. The LED indicator signals motion, temperature level, operating mode and can be used to see if device is within the Z-Wave network. The motion sensor can be used for lighting scenes and presence monitoring systems.

SPECIFICATIONS

Power Supply:	CR123A battery, 3.0V DC
Recommended installation height:	2.4m
Operational Temperature:	0-40°C
Measured Temperature Range:	-20 to 158°C
Temperature Measuring Accuracy:	0.5°C (within 0°C-40°C range)
Light Intensity Measuring Range:	0-32000 LUX
Radio Protocol:	Z-Wave
Radio Frequency:	868 MHz EU; 908 MHz US; 921 MHz ANZ; 869 MHz RU;
Range:	up to 50 m outdoors up to 30 m indoors (depending on terrain and building structure)

TECHNICAL INFORMATION

- Compatible with any Z-Wave controller.
- Detects motion using a passive IR sensor.
- Measures the temperature.
- Measures the light intensity.
- Easy installation on a wall or any surface.
- Protected against tampering and theft - once vibrations are detected, the notification is sent to the main controller.
- Alarms of movement and temperature are signaled by LED diode blinking.
- Simple earthquake detector mode.

CAUTION
Read this manual before attempting to install the device. Failure to observe recommendations included in this manual may be dangerous or cause a violation of the law. The manufacturer, Fibar Group Sp. z o.o., will not be held responsible for any loss or damage resulting from not following the instructions of operating manual.

CAUTION
When handled carelessly or used in non-specified environment conditions, the device may not function properly. It's highly recommended to take all safety precautions to ensure safety and property protection.

I. Z-WAVE NETWORK INCLUSION

The Fibaro Motion Sensor can be included into the Z-Wave network by using the B-button.

1) Open the sensor's casing.
2) Unlock battery by removing 'I'm ready' stripe.
3) Make sure the device is located within direct range of main controller.
4) Set the main controller into learning mode (see main controller's operating manual).
5) Quickly, triple click the B-button - LED diode will glow blue.
6) Fibaro Motion Sensor will be detected and included into the Z-Wave network. Wait for the main controller to configure the sensor.
7) If necessary, wake up the Motion Sensor by triple clicking the B-button. LED diode will glow blue to confirm the sensor wake-up.
8) Close the sensor's casing. Enclosure lock is marked with dots.

Diagram 1 - B-button.

II. EXCLUDING SENSOR FROM THE Z-WAVE NETWORK

1) Make sure the sensor's battery is unlocked.
2) Set the main controller into learning mode (see main controller's operating manual).
3) Quickly, triple click the B-button, located inside Fibaro Motion Sensor's casing.
4) LED diode will glow blue confirming that the device has sent the Node Info Z-Wave command frame.

III. SENSOR INSTALLATION

1) Include the device into the Z-Wave network (see p.II). Note that the inclusion process may be performed ONLY in direct range of the main controller.
2) Install the sensor's holder in desired location.
3) If the sensor is already included in the Z-Wave network, wake it up by triple clicking the B-button.
4) Insert the Motion Sensor in its holder.
5) Test the sensor's operation - check whether the LED diode indicates motion detection.
6) Test the Z-Wave network assuring the device is within range.

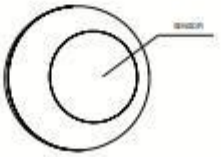
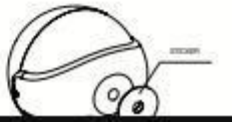


Diagram 2 - Motion detector, light sensor, LED diode.

DICTIONARY:
- **INCLUSION** (Adding) - a device sends "Node Info" command frame which allows it to be included into existing Z-Wave network.

Diagram 3 - preparing Fibaro Motion Sensor for operation.



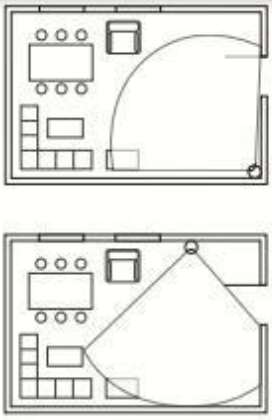


Diagram 5 - Fibaro Motion Sensor's proximity area.

IV. DETECTION AREA AND WORKING CONDITIONS

Fibaro Motion Sensor's detection area is shown in diagram 6b.
Fibaro Motion Sensor has to be installed in a corner of the room or perpendicularly to the doors.
Actual range of the sensor can be influenced by environment conditions. Should false motion alarms be reported, check for any moving objects within the sensor's detection area, such as trees blowing in the wind, cars passing by, windmills. False motion alarms may be caused by moving masses of air and heat as well. If the device keeps on reporting false alarms, despite all of the above-mentioned factors have been eliminated, install the device in another place or adjust the advanced parameters.

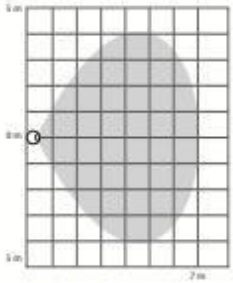


Diagram 6 - Fibaro Motion Sensor's motion detection area.

How to eliminate pet-triggered false alarms:
Fibaro Motion Sensor should be installed 2-3m above the floor, pointed parallelly to the floor level. If wandering pets trigger false alarms it's recommended to modify parameters 1 and 2 settings. The value of parameter 1 can depend on pet's size and environment conditions. It's good to experiment with settings, increasing the parameter value by 5 at each attempt until the desired effect is reached. If parameter 1 settings modifications will not produce

V. INSTALLATION NOTES

Fibaro Motion Sensor cannot be pointed at any source of heat (e.g. radiators, fireplaces, coolers, etc.) or at any source of light (direct sunlight, lamps).
It's not recommended to install the motion sensor in places prone to drafts. Sensor can be mounted using screw or the sticker.

VI. RESETTING THE FIBARO MOTION SENSOR

The Fibaro Motion Sensor reset erases the memory, including all information on the Z-Wave network and the main controller.

Fibaro Motion Sensor reset procedure:
1) Make sure the battery works and is in place.
2) Press and hold the tilt-button for 4-6 seconds until the LED glows yellow signaling the 2nd option of the menu mode.
3) Release the tilt-button.
4) Again, press the tilt-button briefly.
Successful reset will be confirmed with the LED changing colour to red and fading.

NOTE
Device reset will not remove it from the Z-Wave network main controller's memory. However, removing the device from the Z-Wave network will reset Fibaro Motion Sensor automatically.

VII. OPERATING WITHIN THE Z-WAVE NETWORK

Fibaro Motion Sensor has a built in motion detector, temperature sensor and light intensity sensor, which make it a multi-channel device. In the Home Center 2 menu it will be presented as three devices, depending on the main controller software version.

NOTE
Fibaro Motion Sensor capabilities will vary depending on the Z-Wave network controller. Certain functionalities of the Fibaro Motion Sensor may not be supported by some controllers. To make sure your Z-Wave network controller supports the Fibaro Motion Sensor, get in touch with its manufacturer.

Motion, temperature and light intensity values are presented in Home Center 2 menu with the following icons.

VIII. ASSOCIATIONS

By using association with Fibaro's devices the Fibaro Motion Sensor may control another Z-Wave network device, e.g. a Dimmer, Relay Switch, Roller Shutter, RGBW Controller, Wall Plug, or a scene (scene only through the Home Center 2 main controller).

NOTE
Association allows for direct communication between Z-Wave network devices. Main controller does not take part in such communication. Using this mechanism, Fibaro Motion Sensor may communicate with other devices even when the main controller is damaged, e.g. in case of fire.

Fibaro Motion Sensor allows for the association of three groups.
1st Association Group is assigned to the device status - sending the BASIC SET control frame to the associated devices having detected motion.
2nd Association Group is assigned to the tamper alarm. Alarm frame will be sent to the associated devices once tampering is detected.
3rd Association Group reports the device status and allows for assigning a single device only (the main controller by default - the device reports its status to the main controller). It's not recommended to modify this association group.

The Fibaro Motion Sensor allows for controlling up to five regular and up to five multi-channel devices per an association group. However the 3rd association group is recommended for the Z-Wave network main controller (e.g. Fibaro Home Center 2).

IX. EARTHQUAKE DETECTOR MODE

Fibaro Motion Sensor can be configured to work as a simple earthquake detector by setting the Parameter 24 value to 4. Reports with scale of the vibrations (dimensionless) will be sent at the time intervals specified in Parameter 22. First report will be sent immediately after vibrations have been detected. The minimum value of the vibrations, resulting in report being sent, can be defined in Parameter 20. Once the vibrations cease, reports will stop being sent. The Home Center 2 menu presents the earthquake detector measurements in the following way:

X. SENSOR'S ORIENTATION IN SPACE

The Fibaro Motion Sensor has a built-in accelerometer. When the value of parameter 24 is set to 2 or 3, Z-Wave network controller will be informed on the sensor's orientation in space.

XI. LED VISUAL INDICATORS AND SETTINGS

The Fibaro Motion Sensor is equipped with a LED diode for indicating sensor's operating modes and alarms. In addition the LED indicator may inform of the Z-Wave network range and the current temperature.

LED indicator modes:
1) Motion Alarm's colour will vary depending on the temperature. The colour and the signaling mode can be set in parameter 80.
2) Tamper alarm is signaled with an alternating blinking in red - blue - white.
3) The Z-Wave Node Info command frame is signaled with glowing in blue.

To enter MENU press and hold the tilt-button for 3 seconds. MENU levels will be signaled with the LED colours:
- VIOLET - Z-Wave network range tester
- YELLOW - sensor reset

XII. Z-WAVE RANGE TEST

The Fibaro Motion Sensor has a built in Z-Wave network main controller's range tester. Follow the below instructions to test the main controller's range:

1) Press and hold the tilt-button for 2 to 4 seconds until the LED glows violet.
2) Release the tilt-button.
3) Press the tilt-button again, briefly.
4) LED will indicate the Z-Wave network's range (range signaling modes described below).
5) To exit Z-Wave range test, press the tilt-button briefly.

Z-Wave range tester signaling modes:
LED indicator pulsing green - Fibaro Motion Sensor attempts to establish a direct communication with the main controller. If a direct communication attempt fails, sensor will try to establish a routed communication, through other modules, which will be signaled by LED indicator pulsing yellow.
LED indicator glowing green - Fibaro Motion Sensor communicates with the main controller directly.
LED indicator pulsing yellow - Fibaro Motion Sensor tries to establish a routed communication with the main controller through other modules (repeaters).
LED indicator glowing yellow - Fibaro Motion Sensor communicates with the main controller through the other modules. After 2 seconds the sensor will retry to establish a direct communication with the main controller, which will be signaled with LED blinking in green.
LED indicator pulsing violet - Fibaro Motion Sensor does communicate at the maximum distance of the Z-Wave network. If connection proves successful it will be confirmed with a yellow glow. It's not recommended to use the sensor at the range limit.
LED indicator glowing red - Fibaro Motion Sensor is not able to connect to the main controller directly or through another Z-Wave network device (repeater).

XIII. BATTERY USAGE TIPS

The Fibaro Motion Sensor's battery life is approximately 2 years at factory default settings. The current battery level is displayed in a Home Center 2 interface. Red battery icon means the battery needs replacement. In order to avoid tamper detection while replacing the battery remove association of the 2-nd association group and reduce tamper sensitivity (parameter 20 value set to 0). If battery discharges quickly, please check for the following conditions which may result in reducing the battery life:
- Wake up interval is too short - it's recommended to lengthen the interval.
- Temperature and light intensity reports are sent too frequently - modify the advanced configuration settings to decrease the frequency.
- If associated devices or the Z-Wave network main controller are disconnected from the power source it will cause the sensor to frequently attempt to reconnect to those devices which will result in shortening the battery life.

ESPECIFICACIONES CAMARA PTZ

Especificaciones de cámara	
Sensor de imagen (pulgadas)	1/2,8 Inch CMOS
Número de Sensores	1
Mega Pixels	2.07M
Min. Illumination	0.5 Lux
Velocidad de obturación	Shutter speed: 1/30 to 1/10000
Especificaciones ópticas	
Zoom óptico X veces	20
Zoom dinámico X veces	8
Número F de óptica	1,8 a 2,8
Relación de lente desde / hasta	4,42mm a 88,5mm
Auto Focus	Si

Características de la cabeza PTZ	
AN Ángulo en grado +/-	170
Velocidad de PAN con adaptador de CA max degree / sec.	100
Velocidad PAN con POE + grado máximo / seg.	100
TILT Ángulo en grado	-30 a 90
Velocidad de INCLINACIÓN con adaptador de CA grado máximo / seg.	69,9
Velocidad de INCLINACIÓN con POE + grado máximo / seg .	69,9
Posiciones preestablecidas	255

Conexiones ENTRADA-SALIDA	
Salida HDSDI	Si, 3G HDSDI
Salida HDSDI Formato máx.	1080/60p,50p
Salida HDMI	Si
Salida HDMI Formato máx.	1920x1080 60/50p
Salida Audio LINE	Si, 1 unidad mini jack 3,5mm
Interfaz serie PTZ RS-232C in/out	Si, más de 8 PIN mini DIN
Protocolos compatibles con PTZ	Serie, PelcoD, IP JVC, IP otros
Especificaciones de potencia y entorno	
Alimentación DC	Si, 12 Volt or 42V to 57V POE+ over Network LAN
Consumo	12W
Temperatura de funcionamiento	0 a 40
Temperatura de almacenamiento	-40 a 60

Información Mecánica	
Peso en kilos	1.7
Dimensiones (AnxAlxFo) en mm	An 142 x Al 164 x Fo 169
Accesorios incluidos	
Adaptador CA/DC	Si
Cable 2	Si, RS232 Cable
Adicionales	Si, Ceiling mounting bracket
Soporte de montaje en el techo	Si

FOTOGRAFIAS DE LAS CAMARAS COLOCADAS

FOTOS DE LOS SENSORES COLOCADOS

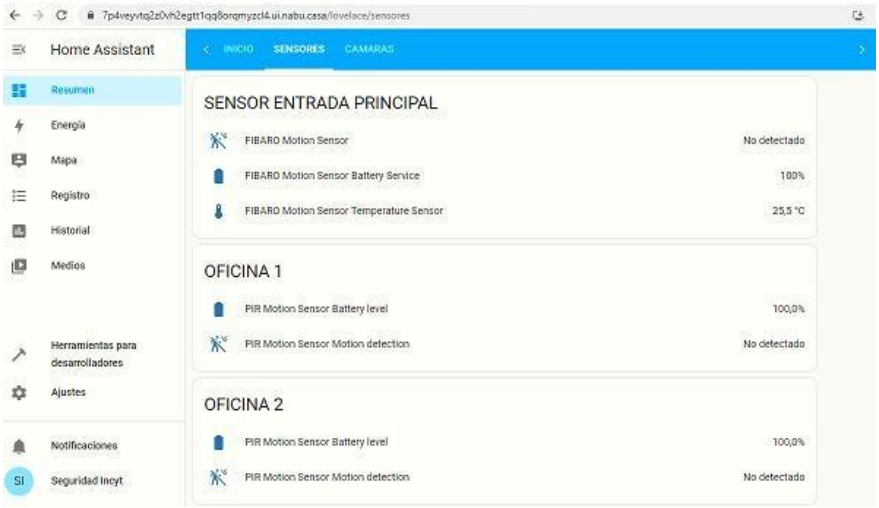
FOTOS DE EXTENSORES WIFI

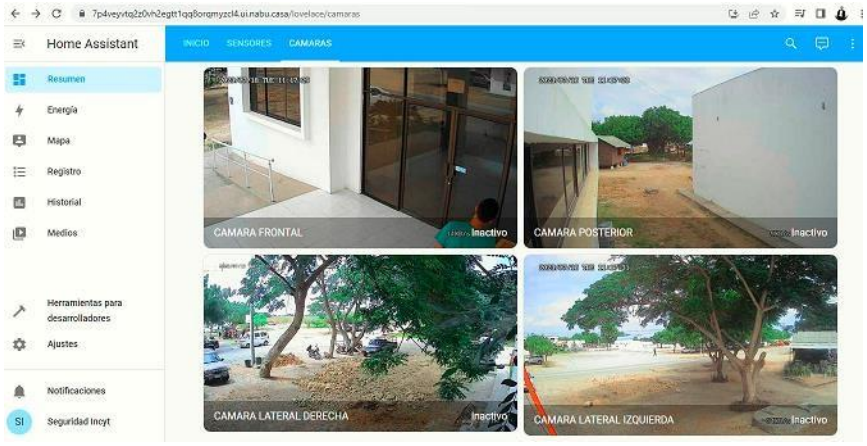
FOTOS DE HEADEND COLOCADO

FOTOS DE LA COLOCACION DE LAS CANALETAS

FOTOS DE ANTENA Z WAVE UTILIZADA

FOTOS DE SERVIDOR FUNCIONAL




Home Assistant
INICIO
SENSORES
CAMARAS
Resumen
Energía
Mapa
Registro
Historial
Medios
Herramientas para desarrolladores
Ajustes
Notificaciones
Seguridad Incyt
CAMARA FRONTAL
Inactivo
CAMARA POSTERIOR
Inactivo
CAMARA LATERAL DERECHA
Inactivo
CAMARA LATERAL IZQUIERDA
Inactivo