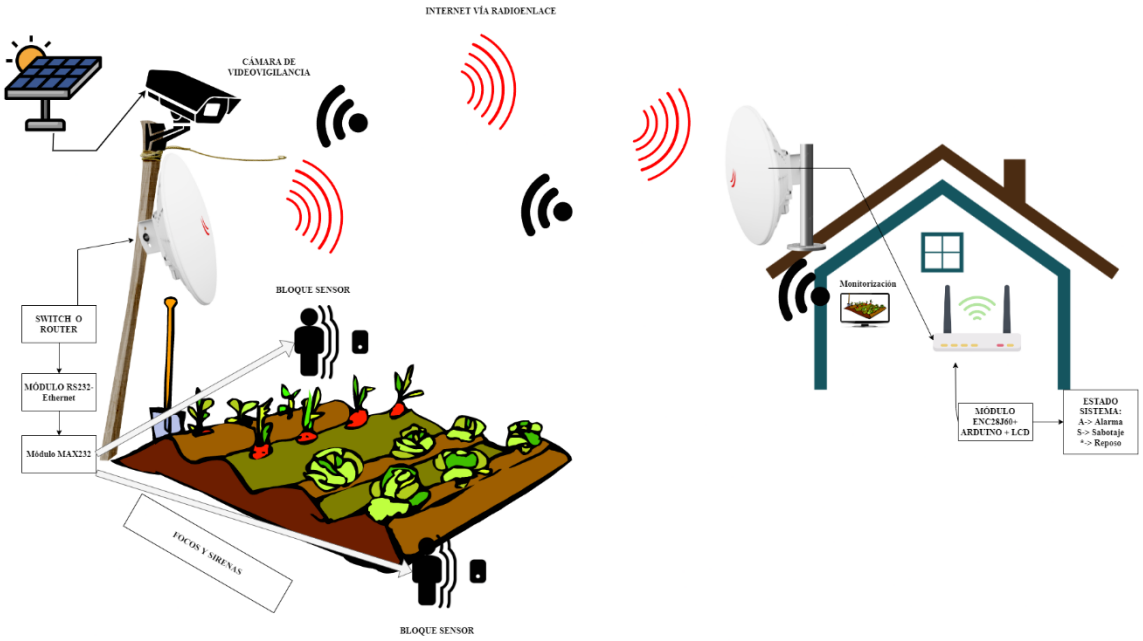
DISEÑO DE UN SISTEMA REMOTO DE ALARMA CONTRA INTRUSIONES



Diseño de un sistema remoto de alarma contra intrusiones

Anaraida García Baigorri
Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación
Diseño de sistemas electrónicos

Consultor: Carlos Gonzalo Moreno Soriano
Profesor responsable de la asignatura: Germán Cobo Rodríguez

Fecha Entrega: 06/2022

Licencias alternativas (elegir alguna de las siguientes y sustituir la de la página anterior)

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Diseño de un sistema remoto de alarma contra intrusiones*
Nombre del autor:	*Anaraida García Baigorri*
Nombre del consultor/a:	*Carlos Gonzalo Moreno Soriano*
Nombre del PRA:	*Germán Cobo Rodríguez*
Fecha de entrega:	06/2022
Titulación:	*Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación*
Área del Trabajo Final:	*Diseño de sistemas electrónicos*
Idioma del trabajo:	*Castellano*
Palabras clave	*Intrusiones, alarma, Wi-Max*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

La idea de este proyecto nace como la necesidad por cubrir una carencia cada vez más extendida entre los agricultores, pues año tras año, el número de hurtos crece exponencialmente. Por todo ello se pretende diseñar un sistema remoto de alarma contra intrusiones, cuyo objetivo principal es la erradicación de estos hurtos.

Cabe destacar que nuestro sistema ha sido desarrollado en un plano teórico, es por ello que todos los resultados que hemos obtenido han sido fruto de simulaciones.

El sensor está conformado principalmente por un microcontrolador + módulo MAX232. El microcontrolador es el núcleo del sistema, pues contendrá cargado en su interior el programa de control previamente programado en MPLAB. Por otro lado, el módulo MAX232 junto con el convertidor Ethernet- RS232, será el elemento que sirva como enlace remoto con la centralita receptora, pues a través de este módulo se conseguirá conocer el estado del recinto. La A simboliza estado de alarma, la S de sabotaje y el asterisco, de reposo.

Así mismo, se han elaborado diseños de fuente de alimentación para convertir la señal de la red eléctrica en la adecuada para los dispositivos, circuito de medidas analógicas, siendo este el elemento testigo que leerá el estado de las entradas, y, por último, control de salidas, que servirán para la activación del sistema de alarma sonoro y óptico.

Finalmente, la forma de conseguir la monitorización en tiempo real será posible al haber elegido un radioenlace punto a punto como forma de conectividad.

Abstract (in English, 250 words or less):

The purpose of this project was born from the need to cover increasingly widespread losses among farmers, because year after year, the number of thefts grows exponentially. Therefore, we intend to design a remote alarm system to warn against intrusions, whose main objective is the eradication of these thefts.

It should be noted that our system has been developed on a theoretical level, which is why all the results we have obtained have been the result of simulations.

The sensor is mainly composed of a microcontroller + MAX232 module. The microcontroller is the core of the system, since it will contain the control program previously programmed in MPLAB. On the other hand, the MAX232 module together with the Ethernet- RS232 converter, will be the element that serves as a remote link with the receiving switchboard, because through this module will get to know the status of the enclosure. The A symbolizes alarm status, the S stands for sabotage and the asterisk for standby.

Likewise, power supply designs have been developed to convert the mains signal into to the appropriate one for the devices, analog measurement circuit, this being the witness element that will read the status of the inputs, and finally, output control, which will be used for the activation of the sound and optical alarm system.

Finally, the way to achieve real-time monitoring will be possible by choosing a point-to-point radio link as a form of connectivity.

Índice

Lista de ilustraciones

Lista de tablas

1. Introducción

¿Qué significa la palabra electrónica? Se conoce que la palabra electrónica, etimológicamente, proviene del griego, significando “relativo a los electrones, ciencia que estudia el almacenamiento y transmisión de la información mediante corrientes eléctricas” [1].

Las últimas incorporaciones tecnológicas brindan la posibilidad de revolucionar el mundo de la electrónica, consiguiendo nuevas formas de interacción entre dispositivos, apareciendo como novedad el término “inalámbrico”, haciendo que cada vez un mayor número de usuarios busquen la comodidad de conseguir dispositivos que puedan instalarse inalámbricamente, pudiendo conseguirlo con tecnologías como: Wi-Fi, Bluetooth, LoRa, LoRaWAN, Zig-Bee, LPWAN, NB-IoT…

El número existente de demandas por parte de los consumidores se suele determinar generalmente por el tipo de edificaciones al que van destinadas, pues algunas no suelen contar con infraestructuras cableadas específicas, por lo que se intenta adoptar una solución que sea conveniente en base a las características, evitando en la medida de lo posible el despliegue de una nueva infraestructura por el coste que esto supone. Como ejemplos de este tipo de soluciones podemos encontrar:

- Sistemas de videovigilancia y seguridad
- Conexión de internet en lugares remotos
- Sistemas de alarma
- Control de sistemas de riego

Para que todos los productos que trabajan de forma inalámbrica puedan coexistir ha sido necesario regular el espectro electromagnético mediante la división de bandas, donde cada una de ellas tiene asignados unos límites de potencia, número de canales, etc…, por lo que se conoce que cada dispositivo deberá cumplir la normativa asociada a la banda de uso pasando por rigurosos controles antes de la comercialización.

1.1 Contexto y justificación del Trabajo

Las personas que han optado por dedicarse a la agricultura como forma de vida necesitan sus cosechas pues son la fuente de su sustento, es por ello, que precisan tener aseguradas toda su producción, pues cada vez, los hurtos en zonas de cultivo son más habituales, por lo que con el diseño de este sistema pretendo abordar esta problemática tan actual.

Después de haber estado realizando una búsqueda general por Internet sobre la existencia de algún sistema similar al que se propone, lo único que se ha encontrado son empresas que se dedican a crear sistemas de seguridad para huertos solares, ya que el precio de las placas solares es bastante elevado, en el que se recomienda el uso de perímetros vallados, cámaras de seguridad, y

sistemas de alarma, donde generalmente se suele avisar directamente al propietario y a los servicios policiales, tal y como podemos ver en [2], sin embargo, si nos ceñimos expresamente a un sistema dedicado para huertos, observamos que no existen sistemas como el que se propone, ofreciendo únicamente consejos para la prevención de estos hurtos, entre los que se destacan, entre otros [3]:

- Uso de alarmas
- Evitar dejar a la vista maquinarias y utensilios de trabajo
- Uso de luces para simular la presencia en el reciento
- Utilizar servicios policiales de la comunidad
- Haciendo vueltas de guardia

Es por todo ello que nace la idea del diseño de un sistema remoto de alarma contra intrusiones, cuyo objetivo principal es la erradicación de los hurtos. Como resultado se pretende obtener el diseño del sistema para poder implementarlo en cualquier huerto, donde no habrá necesidad de poseer ninguna instalación previa compleja, por lo que su implementación podrá estar al alcance de cualquiera.

A lo largo del proyecto se realizará el estudio de forma teórica, sin implementación real del sistema, aunque se tratarán localizaciones reales, para conseguir una mayor objetividad con los resultados que obtengamos de las simulaciones.

1.2 Objetivos del Trabajo

Como objetivos generales del proyecto encontramos la utilidad y relación de todos aquellos conocimientos que se han adquirido a lo largo de estos años en los estudios del Grado en Ingeniería de Tecnologías y Servicios de la Telecomunicación, entre ellos encontramos:

- Realización de un proyecto con todas sus fases
- Capacidad de documentación y justificación del desarrollo del proyecto
- Puesta en práctica de los conocimientos adquiridos en las asignaturas de la titulación, con especial incisión en: Teoría de Circuitos, Circuitos Electrónicos, Comunicaciones Móviles, Redes de distribución y radiodifusión, Electrónica de comunicaciones, …

Como objetivos específicos encontramos:

- Diseño de fuentes de alimentación eficientes
- Diseño de circuitos analógicos que realizan funciones de amplificación, comparación y generación de señal
- Diseño de los circuitos con softwares como EAGLE o PROTEUS
- Elección de los componentes que conformarán el sistema
- Programación del programa de control que se comunicará con el microcontrolador con MPLAB

- Diseño de PCB
- Diseño de circuitos de control de las salidas (señal luminosa, sonora y video cámara)
- Diseño de un sensor remoto de señales analógicas
- Estudio de las bandas ISM
- Aprender a utilizar programas de diseño de circuitos electrónicos
- Comprensión de los datasheets de los componentes

1.3 Enfoque y método seguido

El enfoque de este proyecto se encuentra orientado al diseño de un sistema remoto de alarma contra intrusiones que, aunque cuyo objetivo es evitar intrusiones en los huertos, este sistema puede servir también como un sistema de seguridad contra intrusos instalable en casi cualquier localización que disponga de cobertura de Internet, o en su defecto de cobertura con Wi-Max. Se desarrolla un producto nuevo pues no hay ningún equipo existente en el mercado, aunque el diseño del mismo estará conformado por componentes que se encuentran habitualmente en las tiendas especializadas de electrónica, como, por ejemplo, sensores de presencia adaptados ante posibles falsas presencias, microcontroladores complementados con módulos de radiofrecuencias, entre otros.

El sistema está compuesto por 6 bloques:

1. Circuito de detección (Barreras detectoras infrarrojas)
2. Fuente de alimentación
3. Circuito de medida de señales analógicas
4. Microcontrolador
5. Antenas de radioenlaces
    a. Extremo receptor: En el extremo donde se coloque la antena receptora se instalará el módulo MAX232 junto con el módulo conversor R232 a Ethernet.
    b. Extremo emisor: En el extremo donde se coloque la antena emisora se instalará la centralita para recibir los datos del sistema
6. Circuito de alarma
    a. Circuito activación señal luminosa y sonora

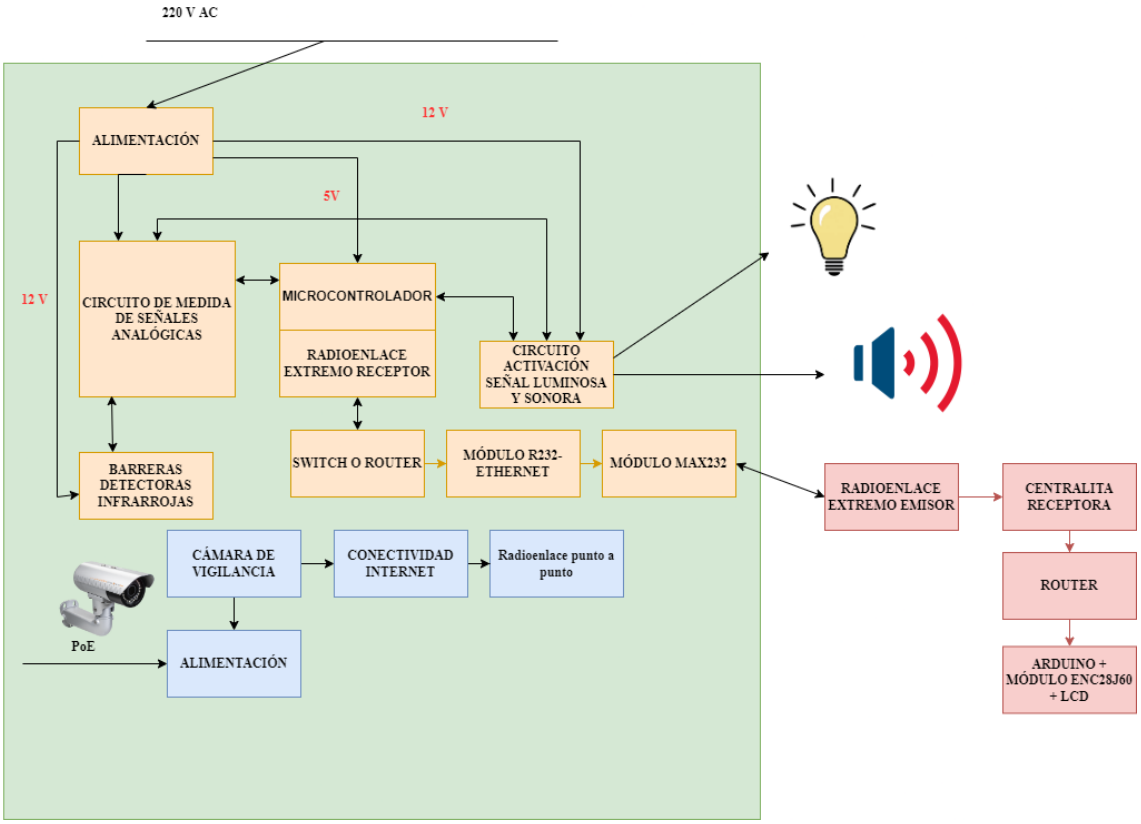


Ilustración 1: Diagrama de bloques del sistema

Para la realización del sistema será necesario documentarse, elegir componentes para la implementación de los circuitos, adaptar esos mismos componentes a las necesidades que requiere el diseño propuesto, así como la realización de simulaciones para la comprobación de que cada bloque funciona adecuadamente, tanto por separado, como en conjunto.

Las tareas que se desempeñarán durante la elaboración del proyecto son las siguientes:

- Tarea 1: Estudio de la banda ISM 868 MHz
- Tarea 2: Estudio del escenario y justificación
- Tarea 3: Estudio de las normativas
- Tarea 4: Estudio de los tipos de alimentaciones para el sistema
- Tarea 5: Estudio de los tipos de sensores de presencia
- Tarea 6: Estudio de los tipos de cámaras de videovigilancia
- Tarea 7: Tecnología Wi-Max, Internet Satelital, Radioenlace
- Tarea 8: Estudio de conexión de las cámaras de videovigilancia
- Tarea 9: Elección del procesador e implementación del programa de control
- Tarea 10: Diseño del circuito de control de las salidas
- Tarea 11: Diseño del circuito de adaptación para la medida de las señales analógicas
- Tarea 12: Diseño de la fuente de alimentación
- Tarea 13: Diseño del layout de la placa PCB

- Tarea 14: Presupuesto del sistema
- Tarea 15: Conclusiones y ampliaciones

1.4 Planificación del Trabajo

En primera instancia, para la planificación del trabajo será necesario establecer cuáles van a ser los hitos del mismo:

Hitos	Fecha
Inicio del Trabajo de Fin de Grado	**17/02/2022**
Definición del Trabajo de Fin de Grado	**17/02/2022**
Entrega del enunciado del trabajo	**04/03/2022**
PEC 1: Entrega de la planificación e inicio de trabajo	**07/03/2022**
PEC 2: Seguimiento del trabajo	**04/04/2022**
PEC 3: Entrega preliminar	**09/05/2022**
PEC 4: Entrega final de la memoria	**13/06/2022**
Defensa del TFG	**Del 21/06/2022 al 23/06/2022**

Tabla 1: Hitos del TFG

Para poder tener una orientación y estimación de la duración del TFG mostramos un plano general del calendario acotado desde febrero hasta junio:

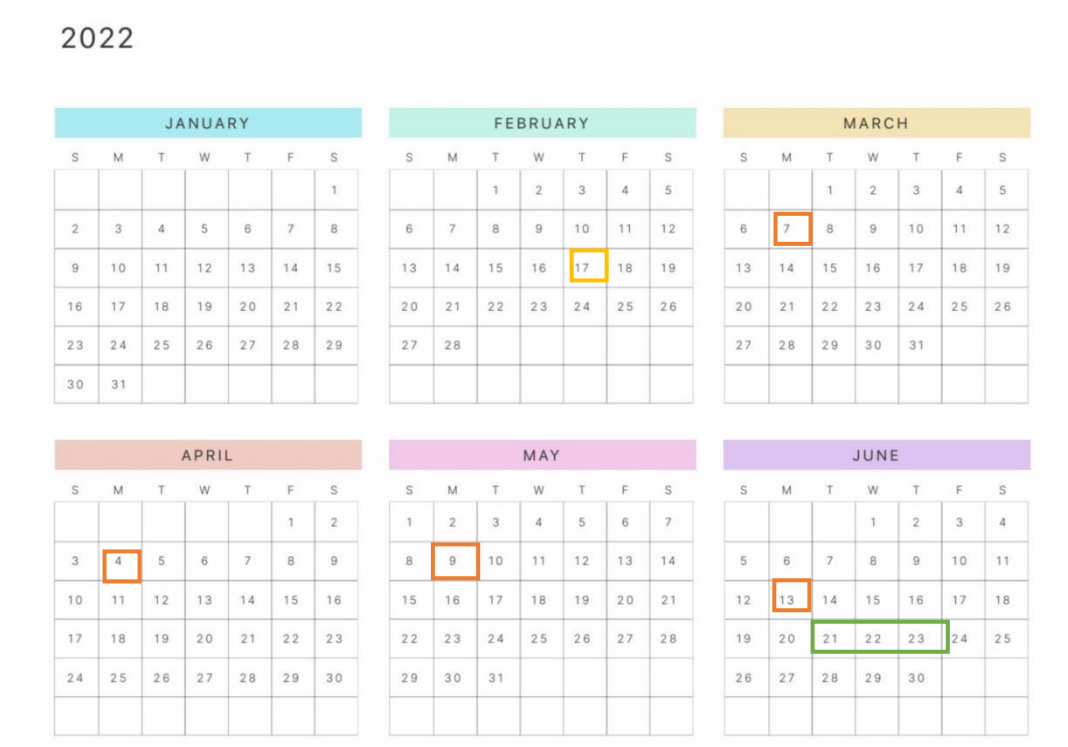


Ilustración 2: Calendario del Trabajo de Fin de Grado

Para realizar una estimación en base al tiempo diario que se va a dedicar al proyecto, primero será necesario realizar la cuenta de los días que se disponen

para la realización del mismo, si realizamos un desglose diferenciando entre días laborables y días no laborables encontramos que:

- **Días laborables (L a V):** Se contabilizan 82 días
- **Días no laborables (S y D):** Se contabilizan 34 días

Como resultado se obtienen 116 días, organizando un horario de 3 horas diarias entre semana, y 4 horas diarias en fines de semana, se consigue un total de 382 horas disponibles para la realización del proyecto, sin embargo, este número de horas se han obtenido de forma teórica, por lo que siendo objetivos, podemos estimar una dedicación semanal de 21 horas, conociendo que la duración del proyecto es de 16 semanas obtenemos un total de 336 horas efectivas de trabajo, obteniendo un margen de 46 horas para la realización de los retoques finales del proyecto, así como la elaboración del vídeo de presentación y la presentación en PowerPoint. Cabe destacar que en esta planificación no se han tenido en cuenta los días de la defensa virtual, contando con 3 días para ello (21/06 al 23/06).

1.4.1 Actividades que se desarrollarán a lo largo del proyecto

N.º Actividad	Descripción de la tarea	Fecha inicio	Fecha final	Número de horas
0	**Inicio de Trabajo de Fin de Grado**	**17/02/2022**	**13/06/2022**	**336**
1	**Definición de Trabajo de Fin de Grado**	**17/02/2022**	**04/03/2022**	**23**
1.1	**Lectura de los enunciados**	**17/02/2022**	**18/02/2022**	**2**
1.2	**Elección y adaptación de enunciado**	**18/02/2022**	**22/02/2022**	**10**
1.2.1	**Búsqueda de información**	**22/02/2022**	**25/02/2022**	**3**
1.2.2	**Elaboración de plan de trabajo**	**25/02/2022**	**04/03/2022**	**4**
1.3	**Instalación de los softwares**	**25/02/2022**	**25/02/2022**	**1**
1.3.1	**Información funcionamiento de los softwares**	**25/02/2022**	**28/02/2022**	**3**
1.4	**Entrega del enunciado del trabajo**	**-**	**04/03/2022**	-
2	**Inicio de PEC 1: "Planificación e inicio del trabajo"**	**01/03/2022**	**07/03/2022**	**13**
2.1	**Contexto y justificación del trabajo**	**01/03/2022**	**02/03/2022**	**2**
2.2	**Objetivos del trabajo**	**01/03/2022**	**02/03/2022**	**0,5**
2.3	**Objetivos específicos del trabajo**	**02/03/2022**	**03/03/2022**	**0,5**
2.4	**Enfoque y método a seguir**	**02/03/2022**	**03/03/2022**	**1**

2.5	Planificación del trabajo	03/03/2022	05/03/2022	4
2.6	Incidencias y riesgos	03/03/2022	05/03/2022	2
2.7	Breve sumario de productos obtenidos	04/03/2022	06/03/2022	1
2.8	Breve descripción de los otros capítulos del trabajo	04/03/2022	06/03/2022	2
2.9	Entrega de PEC1: "Planificación e inicio del trabajo"	-	07/03/2022	-
3	Inicio de PEC 2: "Seguimiento del trabajo"	08/03/2022	04/04/2022	47
3.1	Tarea 1: Estudio de la banda ISM 868 MHz	08/03/2022	11/03/2022	5
3.2	Tarea 2: Estudio del escenario	11/03/2022	15/03/2022	10
3.3	Tarea 3: Estudio de las normativas	15/03/2022	17/03/2022	6
3.4	Tarea 4: Estudio de los tipos de alimentaciones para el sistema	17/03/2022	19/03/2022	5
3.5	Tarea 5: Estudio de los tipos de sensores de presencia	19/03/2022	21/03/2022	5
3.6	Tarea 6: Estudio de los tipos de cámaras de videovigilancia	21/03/2022	24/03/2022	4
3.7	Tarea 7: Tecnología Wi-Max	24/03/2022	28/03/2022	6
3.8	Tarea 8: Estudio de conexión de las cámaras de videovigilancia con Wi-Max	28/03/2022	01/04/2022	6
3.9	Entrega de PEC 2	-	04/04/2022	-
4	Inicio PEC 3: Entrega preliminar del trabajo	05/04/2022	09/05/2022	155
4.1	Tarea 9: Elección del microcontrolador e implementación del programa de control	05/04/2022	11/04/2022	35
4.2.	Tarea 10: Diseño del circuito de control de salidas	11/04/2022	18/04/2022	30
4.3	Tarea 11: Diseño del circuito de adaptación para la medida de las señales analógicas	18/04/2022	25/04/2022	30
4.4	Tarea 12: Diseño de la fuente de alimentación	25/04/2022	02/05/2022	30
4.5	Tarea 13: Diseño del layout de la PCB	02/05/2022	07/05/2022	30
4.6	Entrega de PEC 3	-	09/05/2022	

5	**Inicio PEC 4: Entrega final de la memoria + vídeo presentación**	**10/05/2022**	**13/06/2022**	**81**
5.1	**Tarea 14: Presupuesto del sistema**	**10/05/2022**	**15/05/2022**	**5**
5.2	**Tarea 15: Conclusiones y ampliaciones**	**15/05/2022**	**20/05/2022**	**6**
5.3	**Lectura final del proyecto**	**20/05/2022**	**21/05/2022**	**10**
5.4	**Correcciones del proyecto**	**21/05/2022**	**28/05/2022**	**25**
5.5	**Elaboración presentación del proyecto**	**28/05/2022**	**04/06/2022**	**15**
5.6	**Elaboración vídeo presentación del proyecto**	**04/06/2022**	**10/06/2022**	**20**
5.7	**Entrega PEC 4**	**-**	**13/06/2022**	**-**
6	**Defensa virtual del TFG**	**21/06/2022**	**23/06/2022**	**15**
6.1	**Ronda 1 de preguntas**	**21/06/2022**	**21/06/2022**	-
6.1.1	**Respuesta ronda 1 de preguntas**	**21/06/2022**	**21/06/2022**	**5**
6.2	**Ronda 2 de preguntas**	**22/06/2022**	**22/06/2022**	-
6.2.1	**Respuesta ronda 2 de preguntas**	**22/06/2022**	**22/06/2022**	**5**
6.3	**Ronda 3 de preguntas**	**23/06/2022**	**23/06/2022**	-
6.3.1	**Respuesta ronda 3 de preguntas**	**23/06/2022**	**23/06/2022**	**5**
NÚMERO DE HORAS TOTALES				**319 + 15 = 334**

Tabla 2: Desglose de las actividades desempeñadas durante el proyecto

Como vemos, hemos obtenido un total de 319 horas dedicadas para la realización del proyecto frente a las 336 horas reales que se estimaron, por lo que se consigue un margen de 17 horas frente a posibles retrasos, por otro lado, en las 336 horas no se tuvo en consideración el tiempo necesario para la defensa del TFG, se prevé aproximadamente 15 horas para la contestación de las tres rondas existentes de preguntas, por lo que como suma total del proyecto obtenemos 334 horas.

1.4.2 Detalle del diagrama de Gantt del proyecto

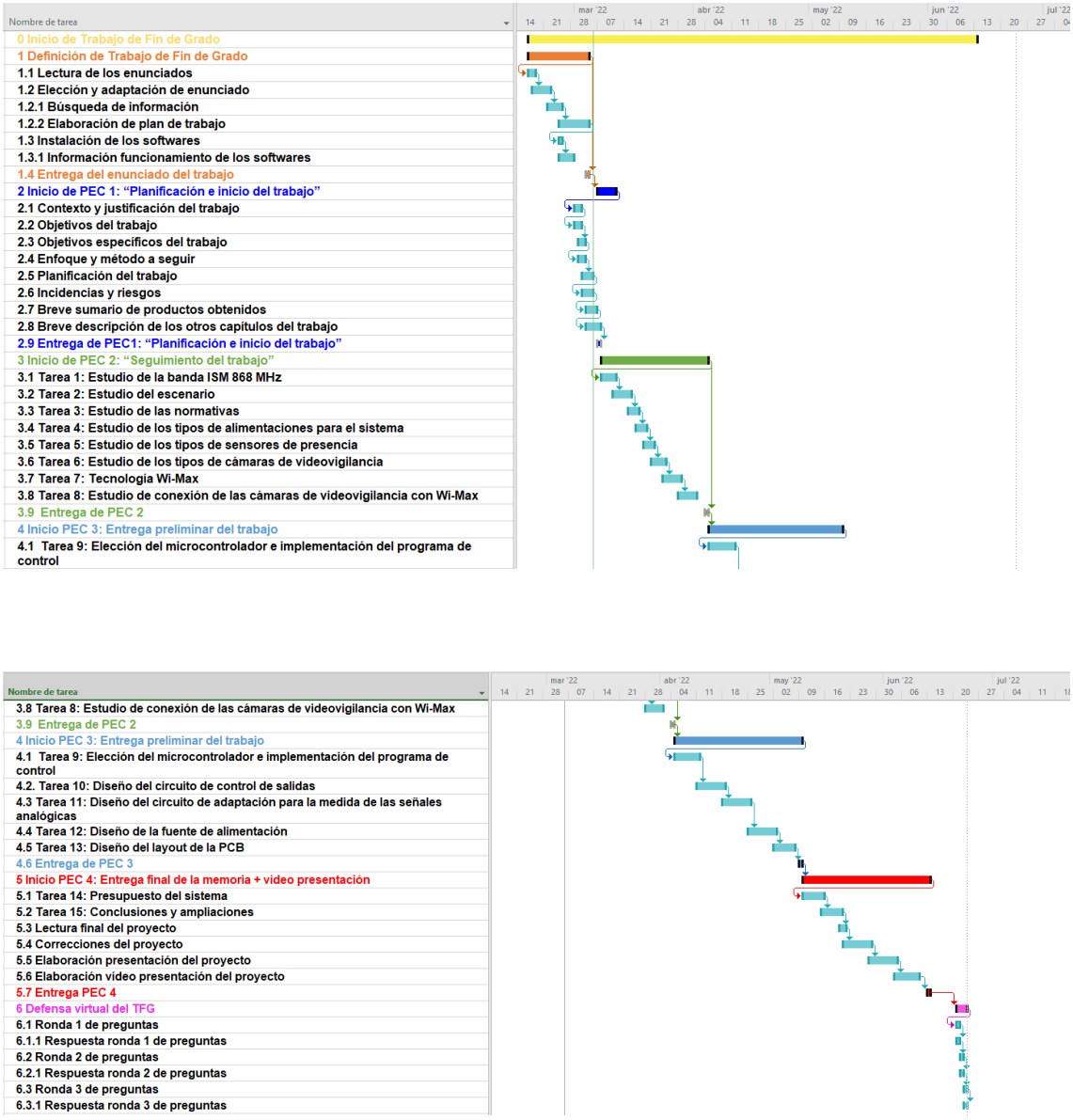


Ilustración 3: Diagrama Gantt TFG

1.5. Análisis de posibles incidencias y riesgos

Durante la realización del TFG pueden aparecer distintas incidencias y riesgos, por lo que es importante que al principio se detecten los posibles riesgos, siendo necesario valorar la probabilidad que existe de que los mismos ocurran considerando de igual forma el impacto que pueden tener en el Trabajo de Fin de Grado. En la tabla 3 se recogen las posibles incidencias y riesgos numerados por código.

Codificación	Descripción	Posible causa	Probabilidad	Posible Impacto
R01	Pérdida de los documentos	Error a la hora de guardar las últimas modificaciones o error en disco duro del equipo	**Media**	**Alto**
R02	Avería del equipo	Alguno de los componentes deja de funcionar	**Baja**	**Medio**
R03	Caída conexión Internet	Avería en la red de la operadora	**Media**	**Alto**
R04	Dificultad manejo softwares	Desconocimiento de los softwares de diseño de circuitos	**Media**	**Alto**
R05	Dificultad implementación programa de control microcontrolador	Aparición de problema a la hora de la implementación del programa de control	**Media**	**Alto**
R06	Mapa de cobertura Wi-Max	Imposibilidad de conseguir mapas de cobertura Wi-Max a través de las operadoras	**Baja**	**Medio**
R07	Enfermedad	Enfermedad propia o de algún familiar	**Baja**	**Alta**
R08	Entregas resto de asignaturas	Posibles retrasos por tener que realizar entregas de otras asignaturas	**Medio**	**Alta**
R09	Componentes	No conseguir componentes que se adapten a nuestras necesidades	**Baja**	**Baja**

Tabla 3: Incidencias y riesgos del proyecto

1.6. Plan de contingencia

En el plan de contingencia se recogen las acciones mitigadoras y/o correctoras que se pueden aplicar a cada riesgo e incidencia, como podemos ver en la tabla 4.

Codificación	Tipo de acción	Acción
A1R01	**Mitigadora**	Realizar copias de seguridad regularmente
A1R02	**Mitigadora**	Realizar mantenimiento del equipo periódicamente
A2R02	**Mitigadora**	Tener a disposición equipos secundarios
A1R03	**Correctora**	Utilizar conexión a través de la tarifa plana de datos móviles
A2R03	**Mitigadora**	Solicitar reparación de la línea con urgencia
A1R04	**Mitigadora**	Búsqueda de manuales de uso
A2R04	**Mitigadora**	Búsqueda de tutoriales
A3R04	**Mitigadora**	Ejecución de ejemplos para comprender funcionamiento
A4R04	**Correctora**	Dedicar más horas de trabajo
A1R05	**Correctora**	Dedicar más horas de trabajo
A2R05	**Mitigadora**	Asesoramiento por parte del tutor de TFG
A1R06	**Correctora**	Elaborar mis propios mapas de cobertura con los datos disponibles en Internet
A2R06	**Mitigadora**	Contactar con el mayor número posible de operadoras que ofrezcan esta tecnología
A1R07	**Correctora**	Se deberá realizar una reorganización en la planificación de las tareas
A1R08	**Correctora**	Se deberá realizar una reorganización en la planificación de las tareas
A1R09	**Correctora**	Búsqueda de componentes en los fabricantes más conocidos
A2R09	**Mitigadora**	Búsqueda de otras alternativas

Tabla 4: Plan de contingencia

1.7 Breve sumario de productos obtenidos

Los productos que se obtendrán al final de la realización del Trabajo de Final de Grado serán:

- La memoria del TFG con una extensión máxima de 60 páginas
- Un vídeo presentando la memoria con una duración máxima de 20 minutos
- Una presentación de diapositivas con lo más reseñable del trabajo
- Código del programa de control del sistema (MPLAB)
- Diseños de los circuitos de:
    - Control de medidas analógicas
    - Control de las salidas
    - Fuente de alimentación
    - Microcontrolador
    - Layout de la placa PCB del sistema remoto de alarma contra intrusiones

1.8 Breve descripción de los otros capítulos de la memoria

La distribución de los capítulos por los que estará conformado el trabajo serán:

- **Capítulo 2: Estudios**

Este capítulo estará conformado por los diferentes estudios que debemos realizar a lo largo del TFG, como, por ejemplo, el escenario en el que se desearía colocar nuestro sistema, las normativas que nuestro sistema debe cumplir en calidad dentro de las áreas de intrusión y videovigilancia, así como el estudio de las diferentes alternativas que tenemos para alimentar nuestro sistema al suponer un escenario en el que no se dispone de instalaciones eléctricas previas. También se tendrá en consideración el estudio de los diferentes modelos de sensores de presencia que nos ofrece el mercado, realizando el análisis de cuál se ajustará mejor a las necesidades de nuestro sistema, será conveniente realizar el mismo procedimiento con las cámaras de videovigilancia.

En resumen, los puntos a tratar serán:

- Espectro electromagnético
- Estudio de la banda ISM
- Escenario de implantación
- Normativas vigentes
    - Sistemas de intrusión
    - Sistemas de videovigilancia
- Tipos y equipos de alimentación
- Tipos de sensores de presencia
    - Modelos de sensores de presencia

- **Capítulo 3: Tecnologías**

En este capítulo se tratará de dar a conocer posibles opciones para conectar nuestras cámaras de vigilancia con Internet, por ejemplo, a través de la tecnología Wi-Max, a través de radioenlaces…

  - Introducción
  - Tecnologías disponibles
  - Ventajas e inconvenientes
  - Decisión final

- **Capítulo 4: Estudio de conexión de las cámaras de videovigilancia**

  - Situación geográfica
  - Estudio de coberturas

- **Capítulo 5: Microcontrolador**

  - Elección del microcontrolador
  - Implementación del programa de control
  - Simulaciones

- **Capítulo 6: Circuito de medidas analógicas**

  - Diseño del circuito de medidas analógicas
  - Simulación del diseño

- **Capítulo 7: Circuito de control de las salidas**

  - Diseño del circuito de control de las salidas
  - Simulación del diseño

- **Capítulo 8: Fuente de alimentación**

  - Diseño del circuito de fuente de alimentación
  - Fuente de alimentación eficiente

- **Capítulo 9: Centralita**

  - Explicación del dispositivo que se va a utilizar para el control del sistema desde casca

- **Capítulo 10: Layout de los circuitos impresos**

  - Diseños del layout de la placa PCB con los elementos que forman el sistema

- **Capítulo 11: Estimación económica del sistema**

  - Realización de un presupuesto

- **Capítulo 12: Conclusiones y ampliaciones**

  - Conclusión sobre el trabajo
  - Problemas surgidos durante el trabajo y las soluciones adoptadas
  - Escalabilidad del sistema

2. Arquitectura del sistema

Este capítulo está dedicado al apartado de estudios, en este realizaremos los estudios de los espectros electromagnéticos, para comprender cómo se comunican los dispositivos por radiofrecuencia; en qué consiste la banda ISM, y cuál es su normativa, así como el escenario que hemos elegido para desarrollar nuestro proyecto, aunque cabe destacar que éste se realizará de forma teórica, pero, no obstante, se tratará de ceñirse lo máximo posible a un escenario real.

Como indica el nombre del proyecto, se realizará el diseño de un sistema de alarma contra intrusiones, en el que las cámaras jugarán un papel fundamental en el sistema de monitorización del entorno, por lo que será importante realizar el estudio de las normativas existentes en el aspecto de los sistemas de intrusión y los sistemas de videovigilancia para conocer los requisitos que debería cumplir nuestro sistema para que se encuentre dentro del marco de la legalidad.

Finalmente, los últimos apartados por los que estará compuesto el capítulo están destinados hacia los tipos y equipos de alimentación, porque se pretende cubrir el mayor número posible de situaciones, como por ejemplo, que el emplazamiento no esté dotado de electricidad, por lo que se tratará de buscar distintas alternativas para dar solución; será necesario realizar una búsqueda de los tipos de sensores de presencia que existen, realizar un estudio de cuál sería más conveniente para nuestro proyecto, y por último, elegir un modelo de sensor de presencia.

2.1. La radiofrecuencia y los espectros electromagnéticos

En la historia de la física existió mucha controversia con la verdadera naturaleza de la luz. Newton en su teoría corpuscular concluyó que la luz era un conjunto de partículas, mientras que otro grupo de eruditos concluyeron por la teoría de ondas, que la luz podría ser una onda. Como se comentó anteriormente, Newton descubrió al usar un prisma triangular de cristal que la luz que penetraba en el prisma se descomponía en 7 colores, sorprendido, decidió poner un segundo prisma que hacía que esos haces de colores se refractasen, por lo que consiguió demostrar que la luz blanca está compuesta por los siete colores del arcoíris, sin darse cuenta, descubrió el rango del espectro visible del espectro electromagnético. [4]

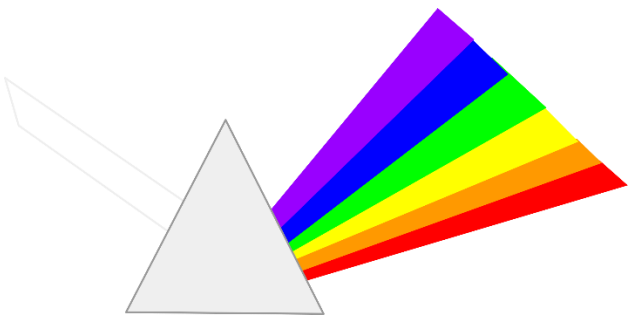


Ilustración 4: Prisma de Newton

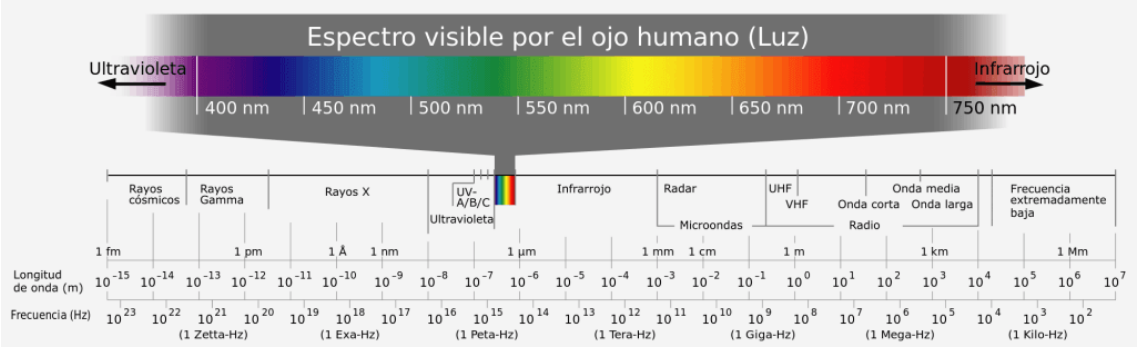


Ilustración 5: Espectro visible

Casi al mismo tiempo, Grimaldi descubrió el fenómeno de la difracción de la luz, por lo que pudo señalar que la luz tiene un comportamiento muy similar al de las ondas, y años más tarde, Huygens estableció la teoría ondulatoria de la luz.

Un siglo después, Fresnel afirmó que las ondas de luz tienen longitudes de onda muy cortas, demostrando la interferencia de la luz, también aportó las leyes físicas para los fenómenos de la reflexión y la refracción de la luz. Fresnel planteó la hipótesis de que el espacio podría estar conformado por una sustancia llamada éter pues las ondas necesitan un medio para poder transmitir.

Young, con su experimento de la doble rendija, siendo la primera comprobación de la teoría ondulatoria de la luz, por lo que demostró que efectivamente la luz se comporta como una onda. Demostrando que existía un patrón de interferencias. [5]

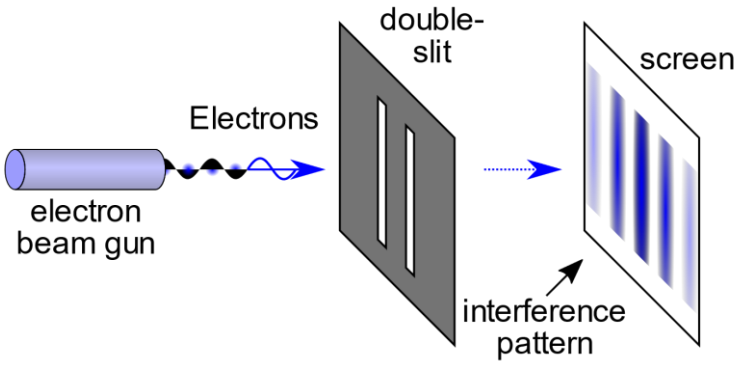


Ilustración 6: Experimento de Young [6]

Finalmente, fue Maxwell quien estableció que la luz es una onda electromagnética, presentando las cuatro ecuaciones para la teoría electromagnética en las que demuestra que los campos magnéticos y los campos eléctricos están vinculados, siendo estas las leyes fundamentales del electromagnetismo: [5]

$$\text{Ley de Faraday} - \text{Lenz: } \boxed{\nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t}}$$

$$\text{Leu de Gauss: } \boxed{\nabla \cdot \vec{E} = \frac{\rho}{\varepsilon_O}}$$

$$\text{Ley de Ampère} - \text{Maxwell: } \boxed{\nabla \times \vec{B} = \mu_O \cdot \varepsilon_O \frac{\partial \vec{E}}{\partial t} + \mu_O \vec{J}}$$

$$\text{Ley de Gauss para el campo magnético: } \boxed{\nabla \cdot \vec{B} = 0}$$

El espectro electromagnético es la distribución energética de todas las ondas electromagnéticas existentes, se encuentran desglosadas en siete categorías, siendo éstas:

- Radiofrecuencia
- Microondas
- Infrarrojo
- Espectro visible
- Ultravioleta
- Rayos X
- Rayos γ

REGIÓN DEL ESPACIO		RANGO DE LONGITUDES DE ONDA	RANGO DE FRECUENCIAS	APLICACIONES MÁS HABITUALES	OBSERVACIONES
RADIO	ONDA LARGA	> 10 m	< 30 MHz	Señales de radio AM Comunicación submarina	Se reflejan en la ionosfera, se pueden utilizar para largas distancias
	ONDA CORTA	10 cm - 10 m	30 MHz - 3 GHz	Señales de radio FM Señales de TV	No se reflejan en la ionosfera por lo que se utilizan para distancias cortas
	MICROONDAS	1 mm - 10 cm	3 - 300 GHz	Radar Redes sin hilos Hornos de microondas	Mucha atenuación en la atmósfera, por lo que se utilizan para distancias muy cortas
INFRARROJOS		700 nm - 1 mm	$3 \cdot 10^{11} - 4 \cdot 10^{14}\ Hz$	Visión nocturna Controles remotos Termografías	Emisiones térmicas
ESPECTRO VISIBLE		400 - 700 nm	$4 \cdot 10^{14} - 7 \cdot 10^{14}\ Hz$	Instrumentos ópticos	Radiación visible por el ojo humano y mayoría de seres vivos
ULTRAVIOLETAS		10 - 400 nm	$7 \cdot 10^{14} - 3 \cdot 10^{16}\ Hz$	Medicina Espectrofotometría	Se conoce que la materia los absorbe muy fácilmente
RAYOS X		0,01 - 10 nm	$3 \cdot 10^{16} - 3 \cdot 10^{19}\ Hz$	Radiografía diagnóstica Cristalografía	Se generan por radiación de ionización, se conoce que su longitud de onda se encuentra dentro de la escala de los átomos
RAYOS GAMMA		10^{-11} m	$> 3 \cdot 10^{19}\ Hz$	Esterilización Radioterapia	Se generan por interacciones subatómicas

Tabla 5: Espectro electromagnético detallado

Donde podemos apreciar que las designaciones de las bandas CCIR es la siguiente:

Número de banda	Intervalo de frecuencias*	Designación
2	30 Hz–300 Hz	ELF (frecuencias extremadamente bajas)
3	0.3 kHz–3 kHz	VF (frecuencias de voz)
4	3 kHz–30 kHz	VLF (frecuencias muy bajas)
5	30 kHz–300 kHz	LF (bajas frecuencias)
6	0.3 MHz–3 MHz	MF (frecuencias intermedias)
7	3 MHz–30 MHz	HF (frecuencias altas)
8	30 MHz–300 MHz	VHF (frecuencias muy altas)
9	300 MHz–3 GHz	UHF (frecuencias ultra altas)
10	3 GHz–30 GHz	SHF (frecuencias super altas)
11	30 GHz–300 GHz	EHF (frecuencias extremadamente altas)
12	0.3 THz–3 THz	Luz infrarroja
13	3 THz–30 THz	Luz infrarroja
14	30 THz–300 THz	Luz infrarroja
15	0.3 PHz–3 PHz	Luz visible
16	3 PHz–30 PHz	Luz ultravioleta
17	30 PHz–300 PHz	Rayos X
18	0.3 EHz–3 EHz	Rayos gamma
19	3 EHz–30 EHz	Rayos cósmicos

*10^0, hertz (Hz); 10^3, kilohertz (kHz); 10^6, megahertz (MHz); 10^9 gigahertz (GHz); 10^{12}, terahertz (THz); 10^{15}, petahertz (PHz); 10^{18} exahertz (EHz)

Tabla 6: Designaciones de las bandas CCIR [7]

Con esta designación de las bandas entra en juego el concepto de la radiofrecuencia, esta simboliza el número de ciclos por segundo que puede transmitir una onda de radio, se conoce que las frecuencias que se utilizan oscilan entre los 300 GHz hasta los 3 KHz, siendo la banda de frecuencias que se utiliza para la transmisión y difusión de las comunicaciones. [8]

La diferencia entre las distintas regiones depende de la longitud de onda y de la frecuencia, a partir de estas, se puede conocer la energía que se desprende de cada una de estas regiones.

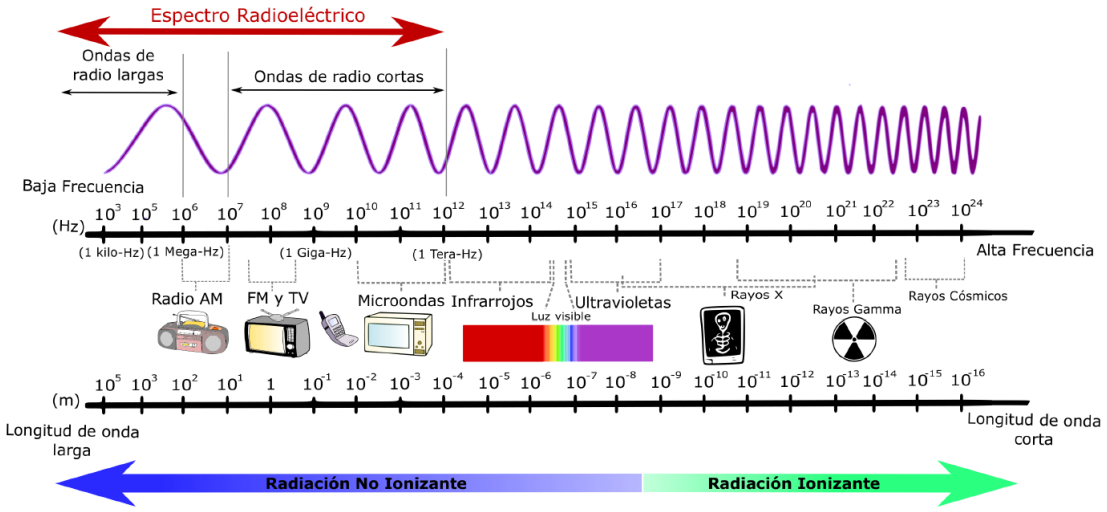


Ilustración 7: Espectro electromagnético [9]

Como podemos observar a partir de la ilustración 7, las longitudes de onda más grandes tienen asociadas frecuencias más bajas, y a su vez, bajas energías, mientras que las longitudes de onda más cortas denotan frecuencias más altas, y como consecuencia, energías más altas, esto es así porque la frecuencia es inversamente proporcional a la longitud de onda.

2.2. Estudio de la banda ISM

Las siglas ISM significan, *Industrial, Scientific and Medical*, y este tipo de bandas son bandas de radiofrecuencia que se especifican según las regulaciones de la ITU, en un principio, estas bandas se reservan para el uso de RF no relacionado con las comunicaciones, aunque son muchos los sistemas de comunicaciones de corto alcance, o sin licencia, los que funcionan dentro de la banda ISM, destacando que es importante respetar las regulaciones y los niveles de potencia que se transmiten [10].

Existen tres bandas ISM [11]:

- **Banda ISM 868 MHz:** Esta banda es para Europa, Asia, África y Oceania. El rango de frecuencias puede variar desde los 863 MHz hasta los 869,9 MHz, pudiendo tener desde 40 canales hasta 140 canales, con una separación entre ellos de 50 KHz o 100 KHz.
- **Banda ISM 902 MHz:** Esta banda se utiliza en América. El rango de frecuencias que se utilizan oscila entre los 902 hasta 928 MHz, puede tener hasta 255 canales con una separación de 100 KHz.
- **Banda ISM 902 MHz e ISM 960 MHz:** Esta banda se utiliza en Japón. Las frecuencias oscilan entre 916.7 MHz hasta 923.5 MHz, los canales guardan una separación de 100 KHz.

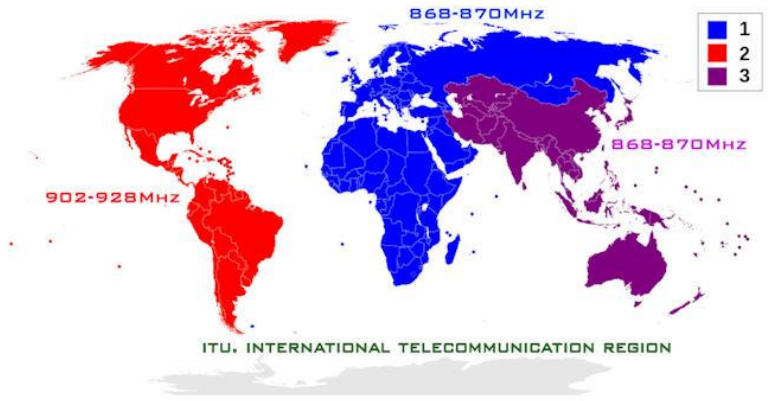


Ilustración 8: Frecuencias bandas ISM en el mundo [11]

Dentro de la recomendación ITU-R SM 1056.1 podemos encontrar que como aplicaciones y equipos que utilicen las bandas ISM encontramos los equipos de calentamiento por inducción por debajo de 1 MHz, el equipo médico, los equipos de microondas que se encuentren por encima de los 900 MHz, laboratorio y equipo científico, equipos de calentamiento dieléctrico RF (1-100 MHz) [12]

Sin embargo, como nuestro proyecto consiste en el diseño de un sistema remoto de alarma contra intrusiones, y se pretende que la alarma sea inalámbrica, según la normativa EN 300 220-3-2 llamada "*Short Range Devices operating in the frecuency range 25 MHz to 1000 MHz […] Wireless alarms operating in designated LDC/HR frecuency bands …"* observamos que nuestro sistema debe cumplir con los siguientes parámetros [13]:

Frequency Band		Maximum radiated power, e.r.p.	Channel access and occupation rules (e.g. Duty cycle or LBT + AFA)	OCW	Band number from EC Decision 2013/752/ EU [i.2]	Class 1 sub-class number according Commission Decision 2000/299/EU [i.5]
A	868,600 MHz to 868,700 MHz	10 mW e.r.p.	≤ 1 % duty cycle	100 kHz or 25 kHz	49	32
B	869,250 MHz to 869,300 MHz	10 mW e.r.p.	≤ 0,1 % duty cycle	25 kHz	52	33
C	869,300 MHz to 869,400 MHz	10 mW e.r.p.	≤ 1 % duty cycle	25 kHz	53	72
D	869,650 MHz to 869,700 MHz	25 mW e.r.p.	≤ 10 % duty cycle	25 kHz	55	34

Tabla 7: Requisitos que debe cumplir el sistema de alarma inalámbrica

Por lo que como vemos, estas frecuencias son las que tenemos disponibles para la banda ISM 868 MHz, por lo que debemos elegir qué frecuencia es la mejor para nuestro sistema, para ello tendremos que tener en cuenta la cantidad de información que es necesario enviar. En nuestro caso, el sistema se encarga de monitorizar constantemente y mandar la información cada 30 segundos con el valor del estado de los sensores de presencia.

Por otro lado, será necesario conocer la potencia que se necesita para poder llegar hasta la centralita, por lo que, en un principio, como únicamente lo que se manda a la centralita son los valores de estado de los sensores de presencia (activo o no activo), consideramos como ideal la banda de **frecuencia de 868.600 – 868.700 MHz,** con una potencia máxima radiada de 10 mW y un ciclo de trabajo inferior o igual al 1%.

Como podemos ver en la siguiente tabla, las frecuencias que más suelen utilizarse para alarmas son [14]:

Clase	Banda de Frecuencia MHz	Potencia e.r.p.	Ciclo de Trabajo	Espaciamiento Canales	Notas
10c	863 – 865	10 mW	100%	200 kHz	Micrófonos Inalámbricos
13a	863 – 865	10 mW	100%	Sin espaciamiento (300kHz para sistemas analógicos)	Audio Inalámbrico
1f	868 – 868,6	25 mW	<1.0%	Sin espaciamiento	SRD no específico
7a	868,6 – 868,7	10mW	<0,1%	25kHz	Alarmas
1g	868,7 – 869,2	25mW	<0,1%	Sin espaciamiento	SRD no específico
7d	869,2 – 869,250	10mW	<0,1%	25 kHz	Alarmas
7b	869,250 – 869,3	10mW	<0,1%	25 kHz	Alarmas
1h	869,3 – 869,4	10mW	Sin restricción	25 kHz	SRD no específico
1i	869,4 – 869,65	500mW	<10%	25 kHz	SRD no específico
7c	869,65 – 869,7	25mW	< 10%	25 kHz	Alarmas
1k	869,7 – 870	5mW	100%	Sin espaciamiento	SRD no específico

Tabla 8: Potencia por banda de frecuencia

2.3. Normativas vigentes

Nuestro sistema va a estar conformado por cámaras de vigilancia y por sensores de presencia, es por ello que será necesario que consultemos las normativas vigentes. En este caso deberíamos consultar las normativas en relación a los sistemas de intrusión y videovigilancia, de esta forma conoceremos las características que debe cumplir todo sistema.

Por otro lado, en nuestro caso, las cámaras que vamos a instalar únicamente servirán como monitorización, por lo que las imágenes no serán grabadas ni guardadas en la nube, diferenciándose de los sistemas de CCTV.

2.3.1. Sistemas de intrusión

Como podemos leer en la orden del 18 de febrero del 2011 en el BOE, sobre el funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, se conoce que únicamente las empresas de seguridad que son autorizadas podrán realizar las operaciones de instalación y mantenimiento de los sistemas de seguridad y alarma, pero en nuestro caso, no será necesario que ninguna empresa de seguridad nos haga instalación de los sistemas de intrusión, seguridad y alarma, pues como alarma utilizaremos una simple sirena, por lo que no hay que confundir con un sistema de alarma como el que existe para las casas, siendo esos más especializados, por lo que deberán ejecutarse por un profesional. [15]

La UNE-EN 50131-1 establece cuatro grados de seguridad en función del riesgo:

- **Grado 1 (riesgo bajo):** Para sistemas de alarma dotados de señalizaciones acústicas que no vayan a conectarse a una central de alarmas o a un centro de control
- **Grado 2 (riesgo bajo a medio):** Está dedicado a viviendas o pequeños establecimientos, en los que se conectan a una central de alarmas o centro de control
- **Grado 3 (riesgo medio/alto):** Para establecimientos obligados a disponer de medidas de seguridad
- **Grado 4 (alto riesgo):** Para infraestructuras críticas como instalaciones militares, materias peligrosas o explosivos… donde se requiere conectar con central de alarmas

En nuestro caso, este sistema se englobaría dentro de grado 2, ya que el sistema tendrá un centro de control, que en este caso será el microcontrolador, pues será el encargado de mandar a los circuitos de activación la señal de alarma para que se active, siendo esta señal proporcionada por los sensores de presencia, o en este caso, barreras de seguridad. [15]

2.3.2. Sistemas de videovigilancia

Dentro de la misma normativa UNE-EN 50131-1 será importante para verificar mediante vídeo, que el subsistema de vídeo sea activado por medio de un

detector de intrusión, o en su defecto, de un video sensor, donde el proceso de verificación mediante vídeo solo podrá comenzar cuando la imagen haya sido visualizada por el operador de la central de alarmas, por lo que el sistema deberá tener al menos una imagen del momento exacto de la alarma, y dos imágenes posteriores a ella, para poder identificar la causa, por lo que los sistemas de grabación utilizados para este tipo de verificaciones no nos permitirán obtener imágenes del lugar que se esté monitorizando, si no se produce alarma, o se exija una grabación permanente [15] .

Aunque será muy importante colocar el cartel de videovigilancia RGPD, porque, aunque nuestras cámaras puedan estar apagadas, podrán ser encendidas cuando salte la alarma, e incluso podemos dejarlas encendidas sin que graben, por lo que es importante dejar visible el cartel para dejar claro que es una zona videovigilada. Si en algún momento se decide grabar permanentemente y dejar el sistema como un CCTV, sí que será necesario grabar las imágenes, y según el reglamento de la LOPD deberán eliminarse cuando haya pasado un mes, y los datos serán siempre confidenciales [16].

Ilustración 9: Cartel de videovigilancia RGPD

2.4. Tipos y equipos de alimentación

Se tiene en cuenta este punto, por si por alguna razón la red eléctrica disponible en el recinto fallase, dejando sin suministro a todo el sistema. Para evitar esto se podrá contar con equipos de aprovisionamiento. Estos equipos podrán utilizar las principales fuentes de electricidad, siendo las más usuales energía solar y energía eólica.

Existen equipos preparados como grupos electrógenos, generadores eléctricos e incluso estaciones de energía portátiles, aunque la mejor opción para un huerto sería un panel solar, pues conseguiríamos almacenar y transformar en energía toda la luz solar incidente en el lugar. Por otro lado, si es una zona en la que existen rachas de viento altas, los molinos también podrían proporcionarnos energía, pues existen aerogeneradores portátiles de hasta 600 W, como por ejemplo el aerogenerador Kitex. [17]

Ilustración 10: Aerogenerador Wind Catcher de Kitex

Dependiendo de las necesidades, será necesario optar por una opción u otra, aunque se ha decidido usar un panel solar porque conseguiríamos tener mucha potencia para nuestro sistema, pues será necesario alimentar las cámaras, la antena de radioenlace, los focos, la sirena, etc…

Aunque es cierto, que existe la posibilidad de que las cámaras tengan integrada su propio panel solar, o que funcionen con batería, o a través de PoE, lo mismo ocurre con los focos, pues existen focos que se cargan con la luz solar, de esta forma conseguiríamos reducir el número de W necesarios para el sistema, y podremos reducir el tamaño del panel solar y el precio.

2.5. Tipos de sensores de presencia

Los sensores o detectores de presencia suelen formar parte de la activación o desactivación de un sistema, siendo los más comunes los detectores por infrarrojos, más conocidos como PIR, en el que la parte fundamental es la variación de temperatura que existe cuando en una zona no hay presencia frente a cuando sí la hay; por otro lado, encontramos los detectores por ultrasonidos, estos son más sensibles y más especializados, cuyo funcionamiento se basa en la diferencia existente entre la frecuencia de la onda que se emite y la que se recibe, siendo poco favorables para su colocación en el exterior, pues son sensibles a vibraciones y ráfagas de aire, por otro lado, existen detectores duales que combinan infrarrojos + ultrasonidos, siendo los más fiables, suelen utilizarse bastante en el ámbito de la seguridad. [18]

Dentro de los sensores de presencia, encontramos los escáneres láser de presencia que son sensores que se utilizan para detectar objetos dentro de un área; las barreras de detección generalmente suelen estar orientadas hacia sectores industriales y de automatización; los sensores inductivos, nos sirven para detectar cualquier tipo de detector metálico, y pueden funcionar incluso en las condiciones más extremas de suciedad y humedad; por otro lado, los sensores fotoeléctricos nos sirven para detectar objetos independientemente del tipo de material que sea. [19]

2.5.1. Modelos de sensores de presencia

Si buscamos sensores de presencia en alguna página especializada, como por ejemplo, Fegemu Solutions, veremos que tenemos distintos productos, entre ellos, escáneres de laser de presencia, barreras de detección, sensores inductivos, sensores fotoeléctricos, sensores y cables de fibra óptica, sensores capacitivos, sensores ultrasónicos, sensores magnéticos, microinterruptores, y dentro de cada categoría, nos proporcionan distintos modelos con sus características más reseñables, sin embargo, para nuestra situación se ha considerado que la opción más recomendable sería optar por barreras infrarrojas, pues son elementos que están compuestos por un extremo emisor y otro receptor, donde el emisor se encarga de generar el haz de luz infrarrojo. [19] Este tipo de dispositivos podemos instalarlos en el exterior, pues nos proporcionarán una fiabilidad superior frente a otro tipo de sensores de presencia, pues con este tipo de dispositivos podremos cubrir espacios más grandes, y además de ello, conseguiremos evitar falsas alarmas si se aproximan animales o si se caen hojas de los árboles, pues únicamente detecta si alguien cruza ese haz de luz infrarrojo, a diferencia de otro tipo de sensores, que en el momento en el que algo entra dentro del ángulo de detección, ya salta alarma, por lo que cualquier tipo de movimiento, e incluso una ráfaga de aire podría hacer que saltase la alarma.

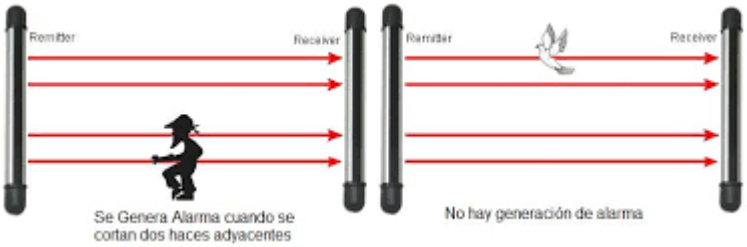


Ilustración 11: Barrera infrarrojo de 4 haces de luz [20]

3. Tecnologías

En este capítulo contemplaremos los distintos tipos de tecnologías existentes en la actualidad para poder dotar de conectividad a las cámaras que se instalarán en el perímetro para monitorizar el escenario.

El escenario elegido no cuenta con instalación de Internet, por lo que nos encontramos con el principal problema que es: ¿Cómo conseguir proporcionar conectividad?

Actualmente las operadoras nos ofrecen tarifas de internet satelital o de internet Wi-Max, aunque como tercer recurso, podemos utilizar un radioenlace para compartir parte de nuestro ancho de banda con el extremo receptor, que en este caso sería el emplazamiento donde se encuentran las cámaras, por lo que la finalidad que se pretende en este capítulo es dar a conocer las alternativas existentes para nuestra problemática, conocer las ventajas e inconvenientes de cada una, y finalmente decidir qué solución es la mejor para nuestra situación.

3.1. Internet satelital

El Internet Satelital es una nueva forma de conectarte a Internet utilizando como medio de enlace una red de satélites, siendo viable este tipo de servicios en zonas sin cobertura, o sin opción de despliegue, como en zonas rurales de montaña. [21]

Actualmente, uno de los servicios de Internet satelital más sonados es Starlink, desarrollado por Space X, cuya idea de proyecto es poner miles de satélites en órbita para conseguir conectividad en cualquier rincón del planeta. Para poder utilizar este tipo de servicios es necesario contratar el servicio e instalar la antena parabólica, donde recibirá las señales que se enviarán al router Wi-Fi que venía con el kit de instalación. Se indica que la antena debe colocarse a ser posible en zonas elevadas y libres de obstáculos [22].

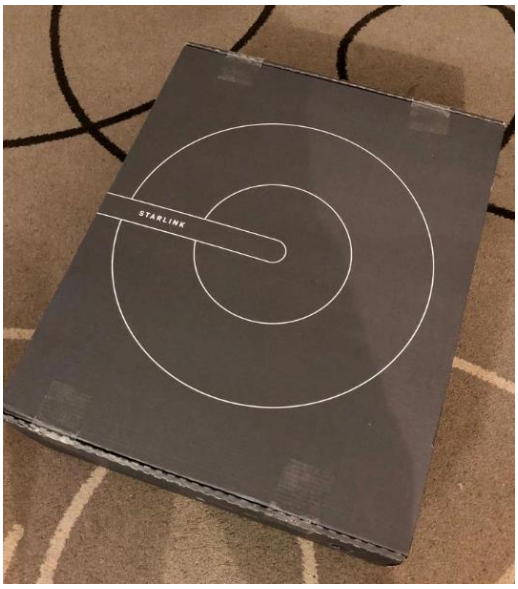


Ilustración 12: Kit instalación Starlink

Ilustración 13: Antena Starlink

La principal ventaja de este sistema es que se puede conseguir Internet en cualquier lugar, sin embargo, sus desventajas son muchas, pues como se puede apreciar en la Ilustración 12 e Ilustración 13 , esta es una antena Starlink real, que actualmente se encuentra instalada en un domicilio de Palma de Mallorca, cuyas imágenes han sido cedidas por el propietario, su tamaño es casi tan grande como el de una mesa de exterior, por lo que puede llegar a ser molesto para tener en ubicaciones pequeñas. Por otro lado, se necesita tener una vista despejada hacia el cielo, y en climas menos favorables, existen problemas en la conexión por las interferencias, por otro lado, el acceso a este tipo de Internet no suele ser inmediato, pues es necesario esperar el tiempo para que se dé la orden, y finalmente, la gran desventaja es el precio que tiene utilizar este tipo de servicios, pues únicamente el kit de la antena roza los 500€, y como tarifa mensual se pagan 99€, por lo que no está teniendo toda la aceptación que esperaban, aunque es cierto que todavía se encuentran en su etapa beta. [22] [23]

3.2. Internet Wi-Max

WiMax es un tipo de conexión de Internet que suele utilizarse en zonas rurales o en zonas en las que es muy difícil realizar una instalación de Internet al ser zonas de difícil acceso, por lo que es una opción que utiliza las ondas de radio, desde los 2.5 GHz hasta los 5.8 GHz, permitiendo conexiones inalámbricas hasta 70 km. Para que funcione es necesario instalar una antena receptora en el lugar donde se desea tener la conexión, no es necesario tener línea de teléfono, esta antena habrá que orientarla hacia el repetidor más cercano, a ser posible con la mayor línea de visión directa, por otro lado, será necesario conectar el cable que viene con la antena al equipo o router, una vez hecho esto, ya se podrá disponer de conexión a Internet.

Como ventajas encontramos que podemos conseguir tener Internet en zonas remotas donde no consiguen llegar otras conexiones, por otro lado, no se necesita una instalación cableada, tampoco es necesario disponer de una línea telefónica, se permite realizar llamadas a través de VoIP, las conexiones ofrecidas con este tipo de servicios pueden llegar a alcanzar hasta 1 Gbps. Se destaca la cobertura de este tipo de dispositivos, y la opción de que sea escalable, permitiendo ampliar en cualquier momento la infraestructura. Por otro lado, como desventajas, encontramos que es necesario contar con una antena que se instale en la fachada del edificio, que únicamente habrá cobertura en las zonas donde las compañías hayan instalado sus propias estaciones de WiMax, la conexión puede tener interferencias por factores externos, además de que la velocidad de navegación es inferior a la fibra óptica, pudiendo perder intensidad en función de la distancia a la que se encuentren los repetidores [24][25]

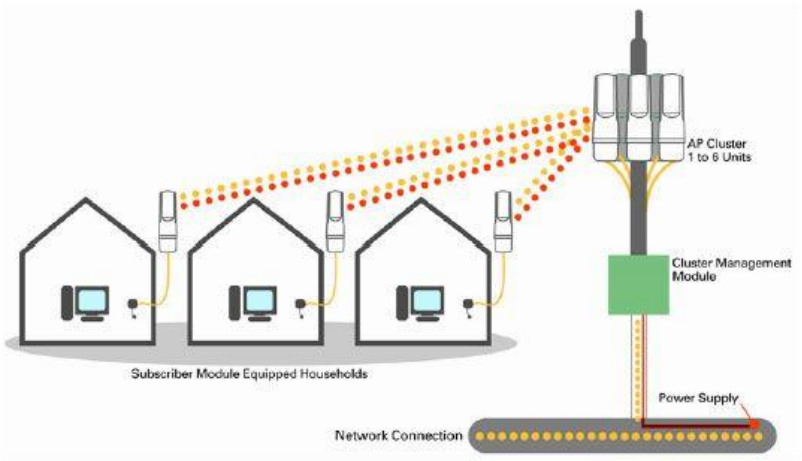


Ilustración 14: Esquema despliegue Wi-Max [26]

A continuación, en la tabla 9 se encuentran las principales diferencias entre Wi-Max e Internet Satelital:

Wi-MAX	Internet Satelital
Señal transmitida desde repetidores	Señal transmitida desde satélite
Se necesitan antenas Wi-Max intermedias	La señal llega al domicilio directamente
Instalación y tarifas más económicas	Existen subvenciones para las instalaciones, por ser mucho más caras
No hay límite de GB de descarga	Existe límite de descarga
No hay saturación al no compartir la señal	Saturación cuando hay mucho tráfico
Gran cobertura en zonas rurales	Cobertura en todo el territorio
Latencia 60 ms	Latencia de 120 ms

Tabla 9: Diferencias entre Wi-Max e Internet Satelital [25]

3.3. Internet a través de radioenlace

Los radioenlaces son considerados sistemas de comunicación, generalmente entre puntos fijos, que se encuentran situados en la superficie terrestre. Entre estos puntos existe una interconexión entre ellos a través de las ondas electromagnéticas, donde lo normal es que sus frecuencias de trabajo vayan desde los 2 GHz hasta los 60 GHz. Suelen emplearse para la transmisión de datos, dar servicios de telefonía móvil, dotar de conectividad de Internet en lugares de difícil acceso…

Para garantizar que un radioenlace funciona correctamente será necesario conseguir una visión directa, *Line of Sight*, y asegurar el 60% de la primera zona de Fresnel, para evitar obstáculos e interferencias, esto podemos conseguirlo con la altura de los mástiles de las antenas, y realizando un estudio del perfil orográfico.

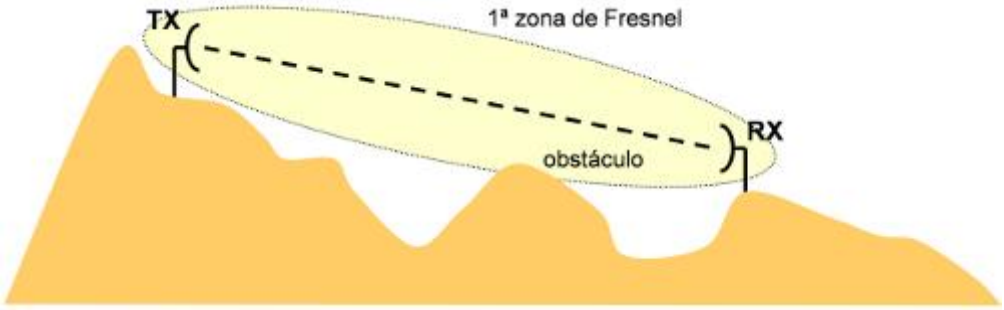


Ilustración 15: Perfil de un radioenlace [27]

Las zonas de Fresnel son elipsoides concéntricos que se definen por las posiciones de las antenas Tx y Rx, donde una onda que sale de la antena transmisora se refleja sobre la superficie elipsoide incidiendo sobre la antena receptora. Generalmente la onda que se refleja suele recibirse con un retardo respecto al rayo directo [27].

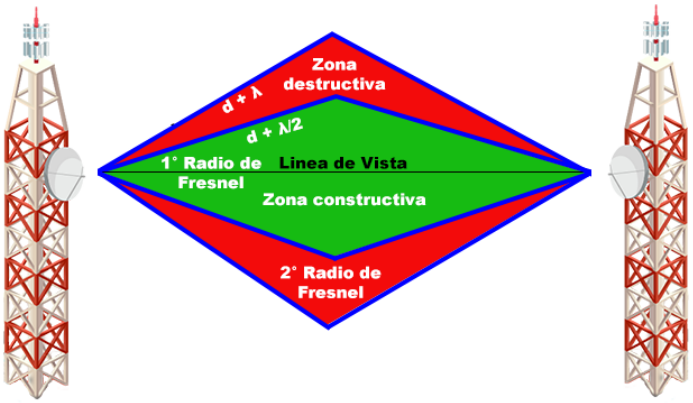


Ilustración 16: Detalle zonas de Fresnel [28]

El radio de las zonas de Fresnel en un punto cualquiera puede calcularse como:

$$R = \sqrt{\lambda \cdot n \cdot \frac{d_1 \cdot d_2}{d_1 + d_2}}$$

Donde:

λ: Es la longitud de onda del radioenlace
n: El número de radio de Fresnel
d_1: Distancia desde antena Tx hasta el punto donde se quiere calcular el radio de Fresnel
d_2: Distancia desde ese punto hasta la antena Rx

En nuestro caso, podemos utilizar un radioenlace para conseguir llevar Internet a una zona donde no hay instalación ni servicio de Internet, para ello lo que se pretende es instalar la antena transmisora en el domicilio donde existe conexión de fibra óptica para compartir el ancho de banda con el extremo receptor que se encontrará situado aproximadamente a 4 km de distancia, por lo que crearíamos un radioenlace punto a punto.

La ventaja de este tipo de radioenlaces es que conseguimos transmitir grandes cantidades de datos a través de las ondas microondas de radio, pues estas tienen la capacidad de transmitir miles de canales de datos entre dos puntos sin necesidad de depender de medios físicos, por otro lado, otra ventaja es que este tipo de sistemas de comunicación son relativamente baratos, siempre y cuando la distancia que deseemos cubrir sea menor, pues para distancias mayores el coste de los equipos se incrementa bastante, pero actualmente, podemos conseguir equipos desde 50 € para cubrir zonas de 2 a 3 km, y 150 € para cubrir zonas que se encuentran hasta 10 km, sin embargo, una característica a tener en cuenta son los fenómenos atmosféricos, pues éstos pueden afectar a la propagación de las ondas electromagnéticas.[29] [30]

3.4. Decisión final

Después de haber tratado los diferentes tipos de conexión, se decide utilizar radioenlaces al permitirnos transmitir Internet desde el domicilio, en este caso, hasta el extremo receptor, de una forma muy sencilla, rápida y económica, en comparación al resto de métodos, porque por ejemplo, con Wi-Max, hubiésemos tenido que contratar una tarifa especial de Internet Wi-Max, aparte de haber pagado por la instalación de los equipos, y este mismo escenario ocurre con el Internet Satelital, pues después de habernos puesto en contacto con varias operadoras de telefonía, como Eurona, nos comentaron que para poder disfrutar de Internet Satelital, es necesario pagar una cuota de suscripción al satélite, que ya costaba 100 € aproximadamente, aunque este pago se pagaba una única vez, el despliegue de la antena + router, eran 450 €, y a eso había que sumarle el pagar la tarifa que se decidiese, siendo la más económica de 28 €, haciendo especial incisión en que con esta tarifa solamente conseguiríamos tener 30 MB, por lo que para nuestro caso, el radioenlace es una opción mucho más económica, con la que conseguiremos mejores resultados, al compartir la

velocidad que tenemos contratada que en este caso son 600 Mbps, y además, como trabajamos en la banda de frecuencias libres, no es necesario pagar licencia por el uso de frecuencias. [31] [32]

TIPOS DE CONEXIÓN	Equipos necesarios	Velocidades	Alcances	Coste
Radioenlace	Antena receptora y transmisora. Si las antenas no llevan router integrado será necesario instalar uno	En nuestro caso podemos llegar a alcanzar una velocidad de 600 Mbps	Existen antenas de radioenlace para transmitir desde pequeños, medios y largos alcances hasta 100 km	En nuestro caso, el radioenlace es la opción más económica al tener que comprar únicamente los equipos, aproximadamente 250 €
Wi-MAX	Antena Wi-MAX y router Wi-MAX + pago tarifa Internet Wi Max	Con las tarifas actuales de Wi-Max se pueden alcanzar velocidades de hasta 100 Mb	Puede alcanzar distancias de hasta 40 o 70 km	Instalación antena Wi-Max + router Wi-Max, aproximadamente unos 300 € + la cuota de 30 Mb unos 30 €
Internet Satelital	Antena de Internet satelital + router , pago suscripción satélite y pago tarifa Internet Satelital	Con las tarifas actuales se pueden alcanzar velocidades de hasta 100 Mb	Para poder disfrutar de Internet Satelital será necesario que exista un despliegue de una red de satélites en el lugar donde se desee la instalación	Pago único suscripción al satélite : 100 € Instalación antena + router: 450€ Tarifa 30 Mb: 28 €

Tabla 10: Comparación entre las diferentes opciones de conexión

4. Estudio de conexión de las cámaras de videovigilancia

En este capítulo realizaremos la descripción de la situación geográfica que se ha elegido para realizar el marco teórico del proyecto. Será importante garantizar a la hora de colocar los equipos transmisores y receptores, una línea de visión directa entre antenas, y, además, deberá asegurarse también que se cumpla al menos el 60% de la primera zona de Fresnel despejada para garantizar el correcto funcionamiento del radioenlace.

A la hora de realizar un radioenlace será necesario que tengamos en consideración todas las pérdidas en el espacio libre, aunque existe otro método mucho más efectivo que es el método de Picquernard, este se utiliza cuando existe la posibilidad de conseguir el perfil rectificado, pues desde ese podremos conocer los obstáculos, y por consiguiente, conseguir un resultado más fiel, por otro lado, también habrá que tener en cuenta las atenuaciones existentes en los cables Tx y Rx, así como las ganancias de los equipos emisor y receptor.

4.1. Descripción de la situación geográfica y distribución de los equipos

Procedemos a obtener unas imágenes a través de la vista aérea que ofrece Google Earth, para poder situar sobre el plano el punto de localización del lugar elegido, así, como poder situar sobre el mismo los puntos en los que se van a localizar los equipos de recepción y emisión del radioenlace, para ello, utilizaremos marcadores, para poder trazar una línea sobre el mapa, para conocer la distancia aproximada entre puntos.

Mostramos el plano detalle del lugar en el que tendremos que realizar el marco teórico de implementación del sistema remoto de alarma contra intrusiones:

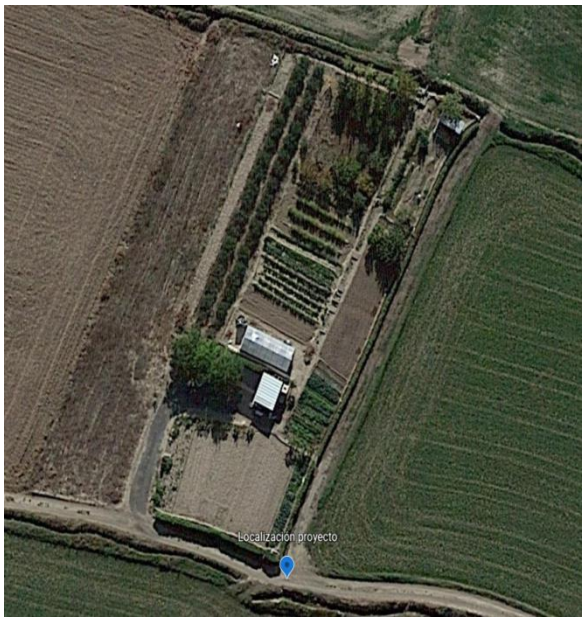


Ilustración 17: Plano detalle del emplazamiento

Procedemos a disponer sobre el mapa el punto donde se encontrará el punto transmisor, que será el punto encargado de transmitir la señal de Internet que conectemos al equipo transmisor, que en este caso será la conexión de fibra óptica existente en el domicilio, al extremo receptor que se encontrará aproximadamente a 4 km del punto. Se dispone de 600 Mbps simétricos, esto significa que se dispondrán de 600 Mbps de subida y 600 Mbps de bajada, aunque estos datos son teóricos, ya que en la realidad llegan aproximadamente 100 Mbps menos.

Por lo que la visión aérea de los dos puntos sería la siguiente:

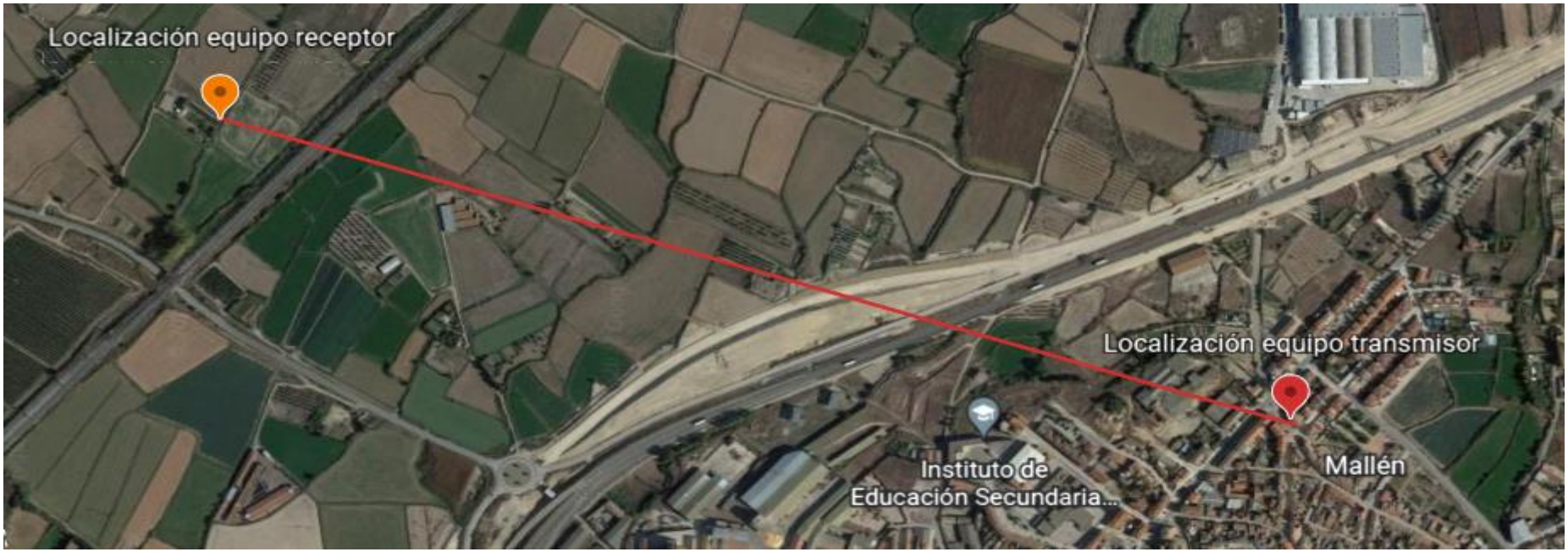


Ilustración 18: Visión aérea de la situación de los equipos Tx y Rx

El equipo receptor como se puede apreciar en las imágenes, en un supuesto, se colocaría en el lado izquierdo al final del campo, pues no existen obstáculos como árboles que puedan impedir una visión directa, y el equipo transmisor se instalaría en el tejado de la vivienda, pues al poseer de instalación de torreta, sobre el mástil en el que tenemos instaladas las antenas de UHF y VHF, podremos colocar la antena del radioenlace transmisor, al poseer suficiente altura para garantizar la conectividad entre antenas.

4.2. Elección de los equipos

Es necesario que elijamos unos equipos que nos garanticen la cobertura del radioenlace, para ello, será importante leer las especificaciones de los mismos para conocer el rango de distancia que pueden cumplir, así como la ganancia de las antenas, además, tendremos que tener en consideración, que unos equipos muy potentes podrán perjudicar la cobertura al existir un exceso de potencia, por lo que se intentará conseguir un sistema equilibrado.

Como especialistas en radioenlaces encontramos marcas como Ubiquiti, Mikrotik, DLink, entre otros, sin embargo, para radioenlaces punto a punto, que es nuestro caso, tenemos actualmente a nuestra disposición los siguientes equipos de Ubiquiti, de los cuales destacamos sus características más relevantes [33]:

Ilustración 19: Equipos radioenlace Ubiquiti

Por otro lado, también tenemos a nuestro alcance equipos de la marca Ligowave, entre ellos podemos destacar los siguientes [34]:

LigoPTP RapidFire 5-23

Es un sistema punto a punto que trabaja a 5 GHz

Ofrece 700 Mbps de salida

Tiene la posibilidad de inclinación de la antena, para aquellas zonas que tengan mucho ruido en el espectro y poder orientarlas mejor

Gracias al radio interno de GHz se puede acceder a la interfaz gráfica de usuario con cualquier dispositivo equipado con Wi-fi

Protección contra sobrecargas y cumple con los requisitos Clase 4

Equipado con dos puertos Gigabit Ethernet, uno con ellos por alimentación PoE

Antena integrada de 23 dBi

LigoPTP RapidFire 6-25

Es un sistema punto a punto que trabaja a 6 GHz

Ofrece 700 Mbps de salida

Diseño resistente a la intemperie y protección contra sobrecargas integrada

Cuenta con el protocolo propietario W-Jet que está diseñado para escenarios PTP de alta demanda y capacidad, minimizando interferencias y estabiliza la latencia en enlaces de larga distancia

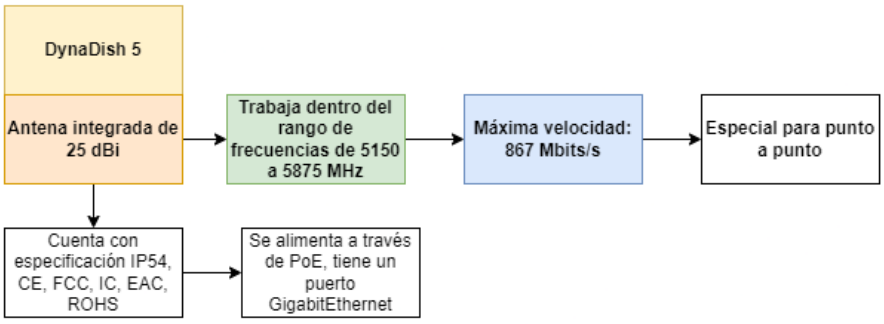
Tiene la opción de ajustar la inclinación de la antena (tilt eléctrico)

Cuenta con un radio de 2.4 GHz para gestión, y está equipado con dos puertos Gigabit Ethernet, uno con paso de PoE

Antena direccional tipo panel de 25 dBi -> Potencia máxima de salida 30 dBm

Ilustración 20: Descripción equipos Ligowave

Por último, como equipos de Mikrotik, entre otros, elegimos los siguientes [35]:



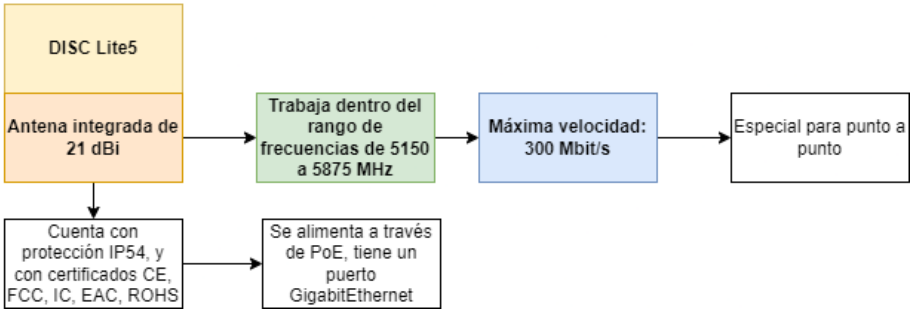


Ilustración 21: Descripción de las características de los equipos de Mikrotik

Aunque existen más fabricantes de antenas para radioenlaces, para nuestro estudio hemos elegido estas marcas, pues se tiene la posibilidad de realizar simulaciones con los equipos descritos anteriormente, por lo que haremos una muestra con algunos de los equipos de cada fabricante.

Finalmente, si hubiera que decidir unos equipos para el despliegue del sistema, la opción más recomendable serían los equipos DynaDish5 de Mikrotik. Dentro del apartado técnico, cuentan con un sistema operativo integrado llamado RouterOS, suponiendo una ventaja al no necesitar conectar router externo. Al poseer este sistema operativo, permite que se realicen todas las configuraciones a través de internet, facilitando el uso de los dispositivos. Por otro lado, estos dispositivos poseen una antena integrada de 25 dBi, siendo capaz de transmitir los datos a largas distancias. Así mismo, la máxima velocidad que pueden transmitir son 867 MBits/s, siendo suficiente para el radioenlace. En cuanto al apartado del coste, estos equipos cuestan alrededor de 150 €, ofreciendo muy buenos resultados calidad-precio.

4.3. Estudio del radioenlace

Procedemos a realizar el estudio del radioenlace a través de las herramientas de simulación de Ubiquiti, Mikrotik y Ligowave. Estas tres herramientas son bastante intuitivas para usar, por lo que no es necesario tener conocimientos muy avanzados sobre realización de radioenlaces, lo único que necesitaremos conocer son las ganancias de los equipos que vamos a utilizar, la frecuencia a la que funcionan, la máxima potencia que transmiten y el umbral de recepción. Todos estos datos será fácil conocerlos a través de las hojas de especificaciones de los equipos que se utilicen.

4.3.1. Estudio del radioenlace punto a punto con Ligowave

Para realizar el estudio del radioenlace, una de las herramientas que podemos utilizar es **Linkcalc** [36] de Ligowave, es muy intuitiva y nos permite realizar un radioenlace rápidamente, eligiendo a través del catálogo de sus antenas la más adecuada para nuestra implementación. Se puede elegir la frecuencia de trabajo, para ello tendremos que leer las especificaciones del equipo con el que realizaremos la simulación:

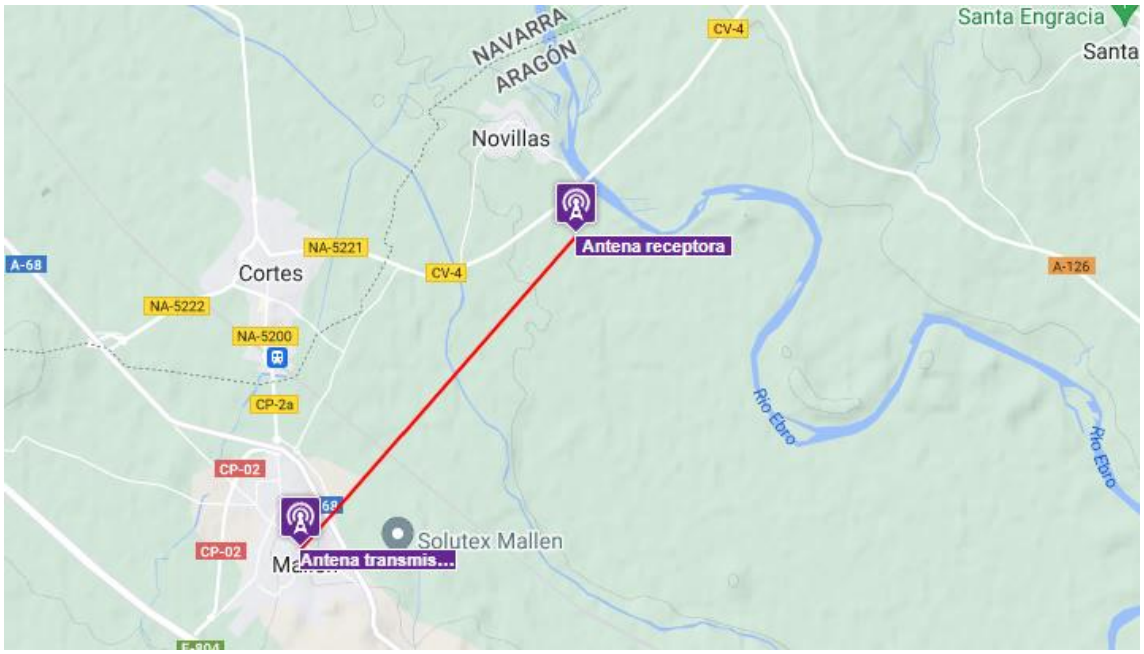


Ilustración 22: Ubicación de los puntos en el simulador Linkcalc

En este ejemplo, estaremos utilizando los equipos **LigoPTP 5-23 RapidFire**, que se caracterizan por tener una ganancia de 23 dBi, alcanzando una potencia máxima de 28 dBm. [37]

Realizando la simulación con una frecuencia de trabajo de 5,8 GHz, obtenemos por resultado:

Resultados			
Pérdida de espacio libre	119 dB	Margen de atenuación térmica	51 dB
Nivel de señal de recepción	-44.86 dBm	Distancia entre los sitios	3.747 km
PIRE	51.0 dBm	Disponibilidad del enlace debido a la	N/A

Ilustración 23: Resultados equipo LigoPTP 5-23 RapidFire

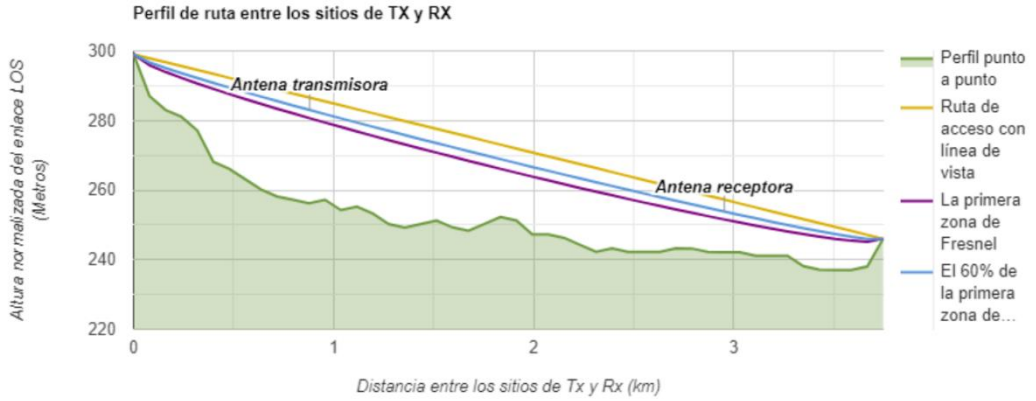


Ilustración 24: Perfil de ruta con equipo LigoPTP 5-23 RapidFire

Como observamos tenemos unas pérdidas por el espacio libre de 119 dB, y obtenemos un nivel de señal de recepción de -44.86 dBm, siendo este un valor excelente, además, también se aprecia el perfil orográfico de ambos extremos transmisor y receptor, lo cual nos ayuda a tener una visión global del escenario, pudiendo afirmar que este radioenlace es viable realizarlo, pues se garantiza el 60% de la primera zona de Fresnel, al no encontrarse con obstáculos que puedan interferir en la señal, cabe destacar que las alturas que se han propuesto para los dos extremos han sido 10 m.

Elegimos realizar otro segundo estudio, con otros equipos, en este caso seleccionamos **LigoPTP 6-25 RapidFire**, estos se caracterizan por tener una ganancia de antena de 25 dBi, la potencia máxima a la que transmiten son 30 dBm, y el umbral de recepción se encuentra en -97 dBm.[38] Introduciendo estos datos en el simulador:

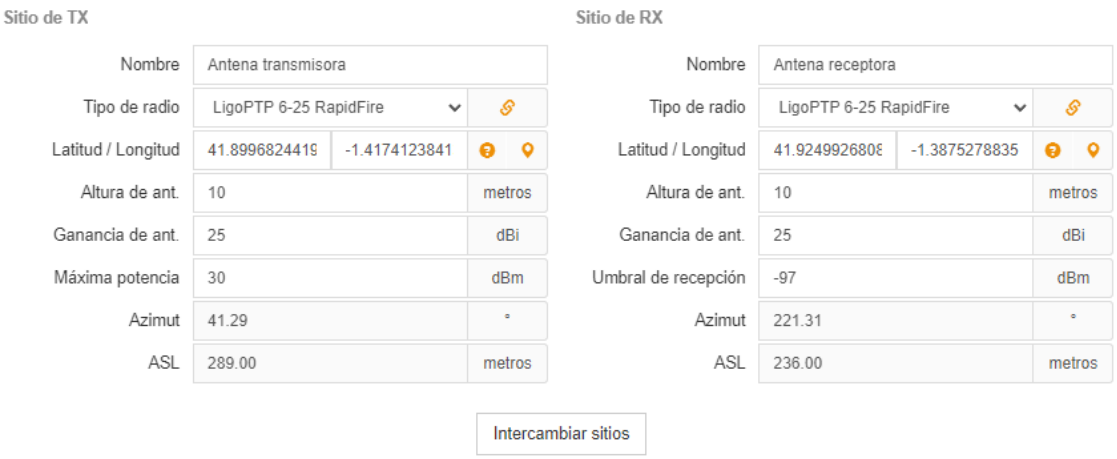


Ilustración 25: Datos equipo LigoPTP 6-25 RapidFire

Obtenemos como resultado:

Pérdida de espacio libre	119	dB	Margen de atenuación tér…	58	dB
Nivel de señal en el sitio d…	-39.16	dBm	Distancia entre los sitios	3.75	km
PIRE	55.00	dBm	Disponibilidad del enlace …	n/a	

Ilustración 26: Resultado equipo LigoPTP 6-25 RapidFire

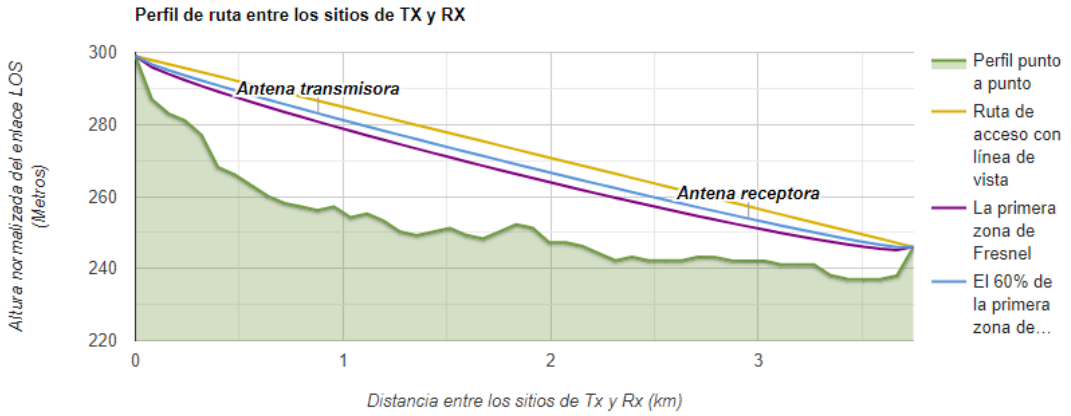


Ilustración 27: Perfil de ruta con equipo LigoPTP 6-25 RapidFire

Como vemos, con estas antenas, la frecuencia de trabajo cambia a 6 GHz, y como la ganancia de las antenas es superior, obtenemos un mejor nivel de señal que con el equipo anterior, -39.16 dBm.

Si realizamos la simulación con el equipo **LigoDLB 2-14** , cuyas características mas reseñables son 14 dBi como ganancia de antena y una máxima potencia de 20 dBm [39], obtenemos unos resultados de cobertura bastante peores respecto a los equipos anteriores:

Sitio de TX			Sitio de RX		
Nombre	Antena transmisora		Nombre	Antena receptora	
Tipo de radio	LigoDLB 2-14		Tipo de radio	LigoDLB 2-14	
Latitud / Longitud	41.8996824419	-1.4174123841	Latitud / Longitud	41.9249926808	-1.3875278835
Altura de ant.	10	metros	Altura de ant.	10	metros
Ganancia de ant.	14	dBi	Ganancia de ant.	14	dBi
Máxima potencia	20	dBm	Umbral de recepción	-75	dBm
Azimut	41.29	°	Azimut	221.31	°
ASL	289.00	metros	ASL	236.00	metros

Intercambiar sitios

Ilustración 28: Datos equipo LigoDLB 2-14

Pérdida de espacio libre	111	dB	Margen de atenuación tér…	12	dB
Nivel de señal en el sitio d…	-63.23	dBm	Distancia entre los sitios	3.75	km
PIRE	34.00	dBm	Disponibilidad del enlace …	n/a	

Ilustración 29: Resultado con equipo LigoDLB 2-14

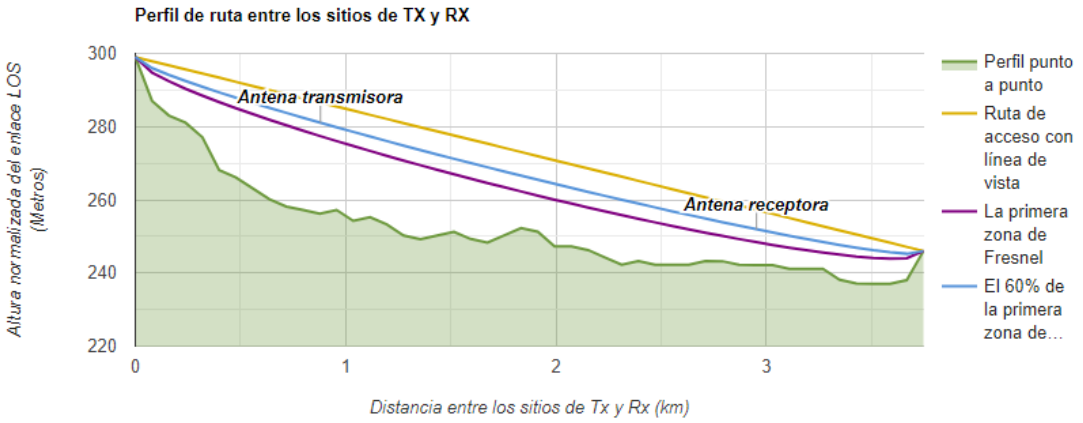


Ilustración 30: Perfil de ruta con equipo LigoDLB 2-14

4.3.2. Estudio del radioenlace punto a punto con Mikrotik

Si realizamos pruebas con el simulador de Mikrotik, éste nos permite al igual que el resto de simuladores, poner a prueba los equipos que ofrecen, para conocer de antemano cuál de ellos se ajusta a nuestras necesidades, en este caso, de Mikrotik seleccionamos los equipos **DynaDish 5** [40]**.** Se ha elegido este modelo porque se han realizado con anterioridad radioenlaces con estos, y el resultado ha sido muy satisfactorio.

El simulador nos permite conocer la distancia, las pérdidas que se pierden debido al espacio libre, y la señal teórica que se espera tener en ambos puntos, además de ello, también nos proporciona información acerca de si ese radioenlace es viable realizarlo; con los parámetros siguientes vemos que sí lo es

Si procedemos a darle a calcular el enlace, nos muestra en el margen superior derecho el perfil orográfico, y en el margen inferior izquierdo nos muestra los valores de la primera zona de Fresnel y el 60% de la primera zona de Fresnel:

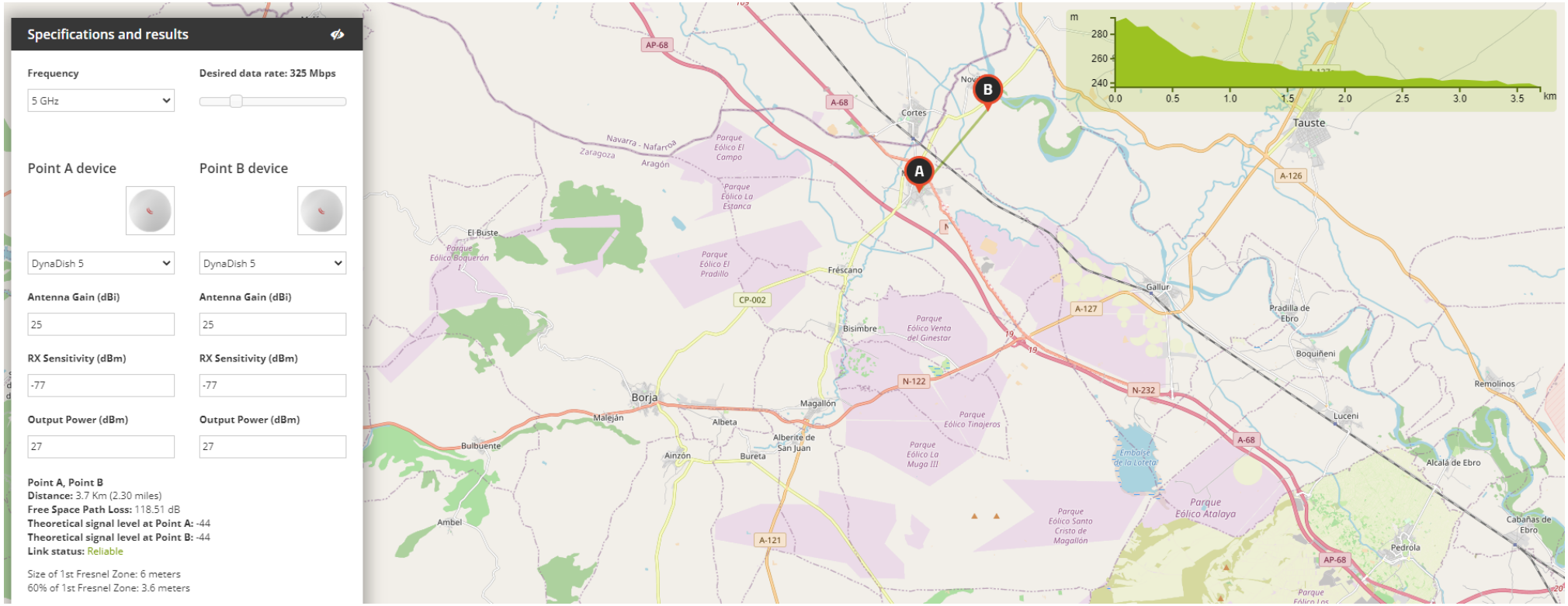


Ilustración 31: Simulación con equipo DynaDish 5

Si realizamos una segunda prueba con los dispositivos **DISC Lite 5** [41], observamos que los niveles de señal, aunque se encuentran dentro de los márgenes aceptables, cuando la situación climática no sea muy favorable, podrán obtenerse valores más pequeños de niveles de señal, pudiendo no garantizar el correcto funcionamiento del enlace

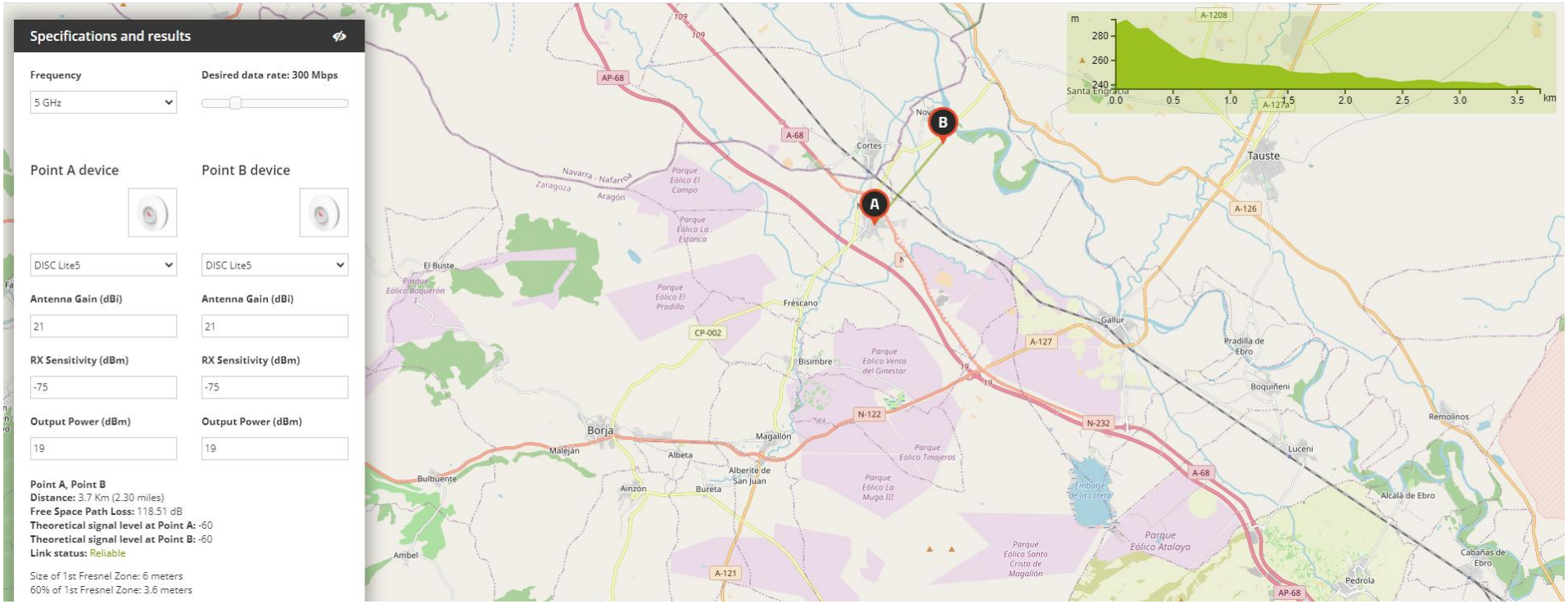


Ilustración 32: Simulación con DISC Lite 5

4.3.3. Estudio del radioenlace punto a punto con Ubiquiti

La ventaja de realizar el estudio del radioenlace desde el simulador de Ubiquiti, es que si nosotros situamos sobre el mapa los puntos desde los que vamos a necesitar cubrir el radioenlace, el propio sistema nos realiza el estudio del radioenlace con los equipos más óptimos para cubrir la distancia del radioenlace, en nuestro caso, como la distancia a cubrir es inferior a 5 km, el equipo que mejor nos iría sería **airFiber 60 LR** [42], además, con estos terminales la señal que se espera recibir es de -46 dBm, por lo que tendríamos una conexión excelente, por otro lado, aunque elige los productos automáticamente, también tenemos la posibilidad de elegirlos manualmente, para observar los distintos cambios en los niveles de señal.

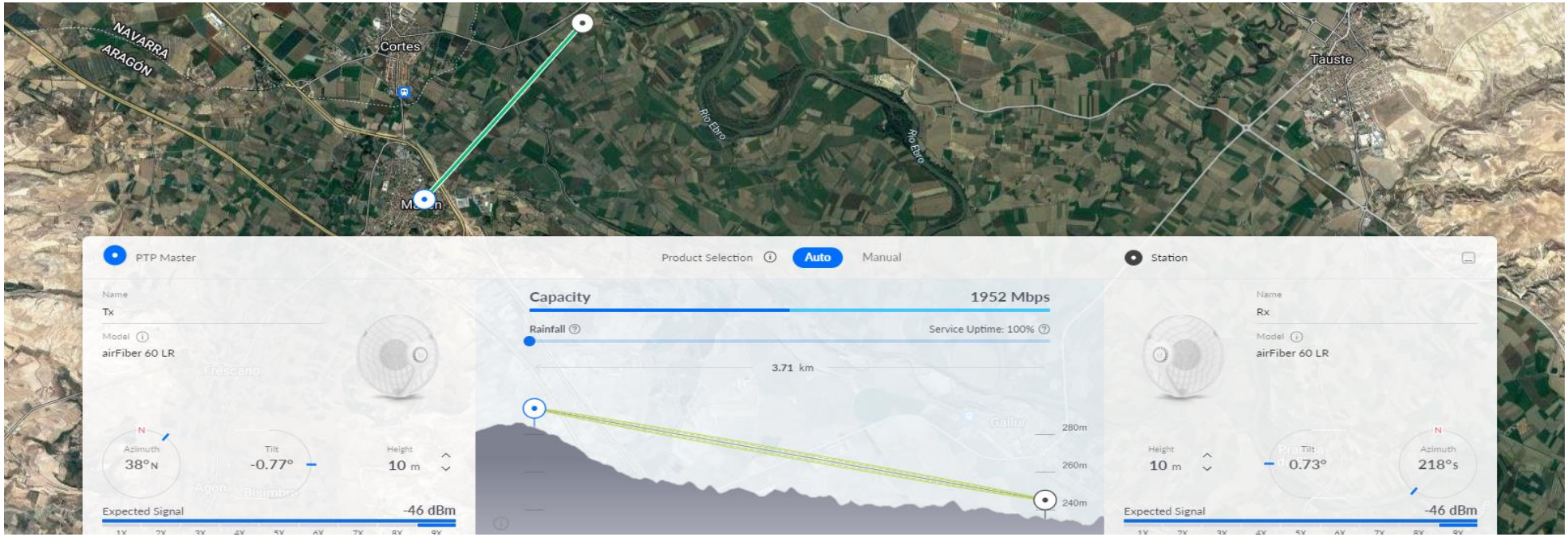


Ilustración 33: Simulación con airFiber 60 LR

Si cambiamos el modelo, observamos que varían los niveles esperados de la señal:

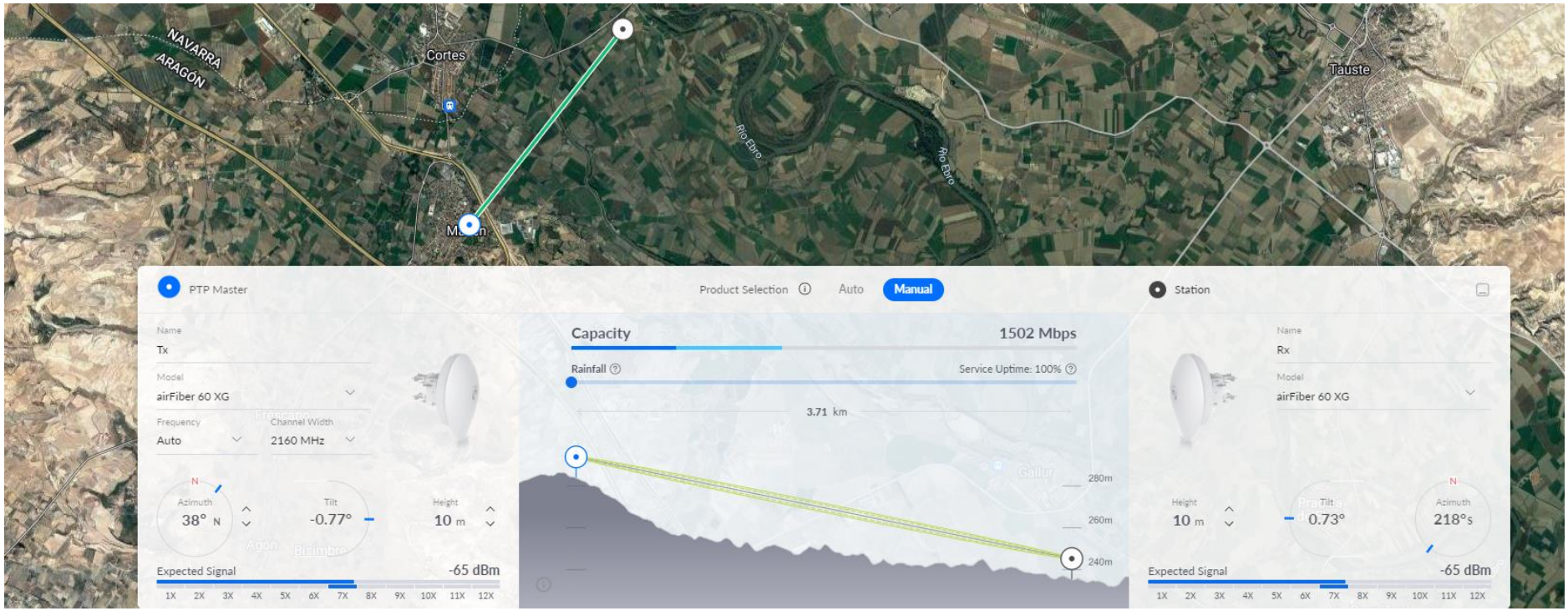


Ilustración 34: Simulación con airFiber 60 XG

Podemos simular incluso, si tuviésemos condiciones de extrema lluvia:

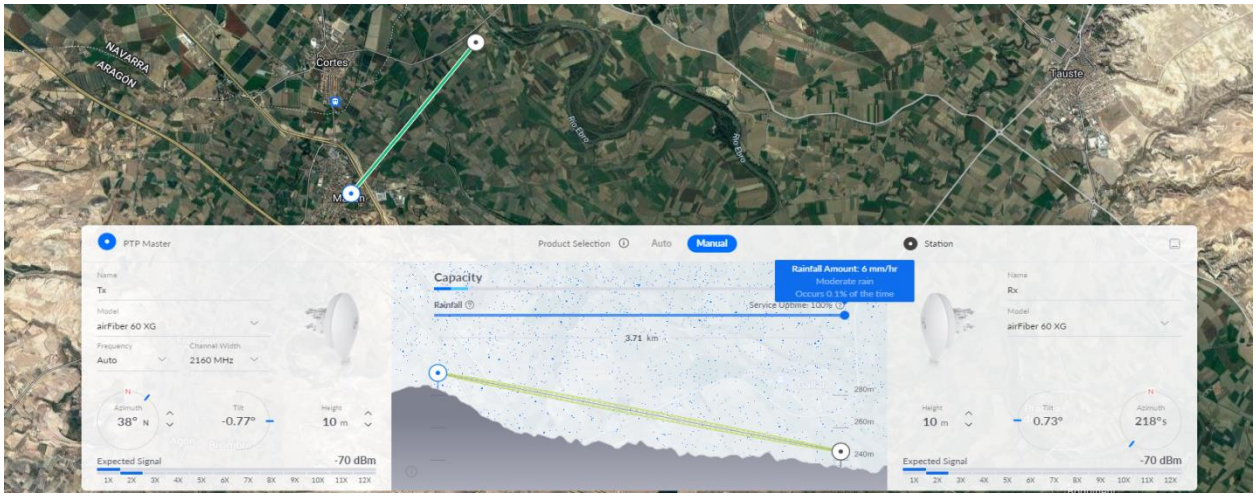


Ilustración 35: Simulación condiciones de extrema lluvia

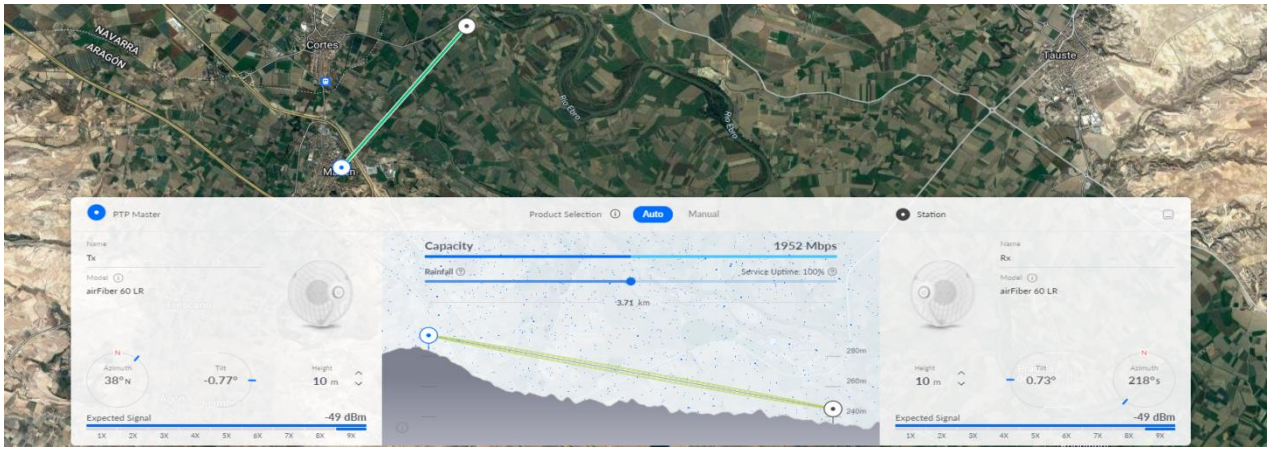


Ilustración 36: Simulación condiciones normales de lluvia

5. Microcontrolador

5.1. Elección del microcontrolador

Para el sistema se ha elegido el microcontrolador de la marca Microchip con referencia PIC 18F26K22, donde las características más reseñables del microcontrolador son [43]:

- Alimentación: desde 1.8 V hasta 5.5 V
- Posee 4 timers de 16 bits
- Permite comunicaciones MSSP y EUSART
- Posee 4 puertos A, B, C, E de I/O que son configurables
- Soporta RS232, RS-485 y LIN 2.0
- Osciladores hasta 64 MHz
- Consumo de 100 nA en modo reposo

Este microcontrolador, además, nos ofrece una resolución de 10 bits, cumpliendo con la mínima precisión que debe tener el sistema. Por otro lado, como vemos, la comunicación que permite este PIC es a través de comunicaciones serie EUSART y MSSP, por lo que utilizando los pines 17 y 18 podremos conectar un módulo de radiofrecuencias, para poder comunicar los datos con la centralita.

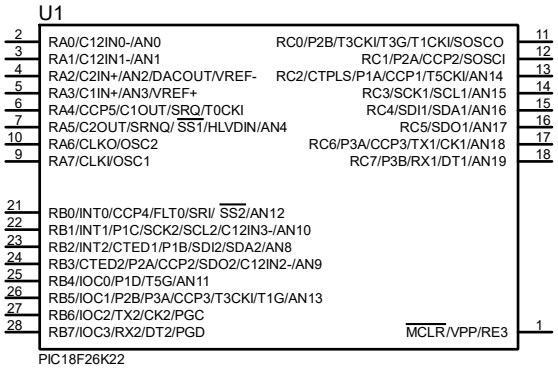
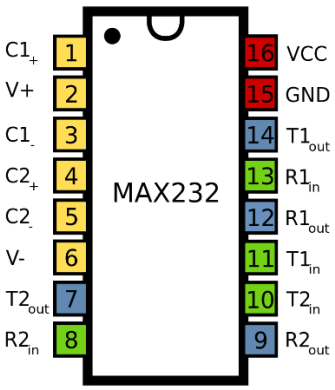


Ilustración 37: PIC18F26K22

Sin embargo, en este caso, como estamos realizando un radioenlace para poder permitir que las cámaras tengan conexión a Internet, en vez de utilizar un módulo de radiofrecuencias que trabaje en la banda ISM como se ha descrito al principio del trabajo, podemos utilizar el propio radioenlace para mandar los datos hasta la centralita. Cabe destacar que, aunque no estemos utilizando la banda ISM, estaremos utilizando la banda de frecuencias libres de 5 GHz, ya que es la frecuencia a la que operan los equipos de radioenlace que se seleccionaron. En el apartado del diseño del microcontrolador, se explicará en detalle el procedimiento.

5.2. Diseño del microcontrolador

Como se ha comentado anteriormente, el microcontrolador en vez de llevar integrado un módulo de radiofrecuencias, lo que se hará será acoplar el circuito integrado MAX232 en los pines 17 y 18 del PIC18F26K22, pues sabemos que este circuito integrado lo que nos permite es convertir las señales del puerto serie en señales que sean compatibles para transmitirlas [44]. Si observamos el diagrama de conexiones de MAX232:



Como vemos, lo que necesitaremos será conectar el pin 17 del microcontrolador (Tx) con el pin 11 de MAX232, y el pin 18 del microcontrolador (Rx) con el pin 12 de MAX232

Ilustración 38: Diagrama de conexiones MAX232

Por lo que ya sabemos que la estructura del microcontrolador debe ser la siguiente:

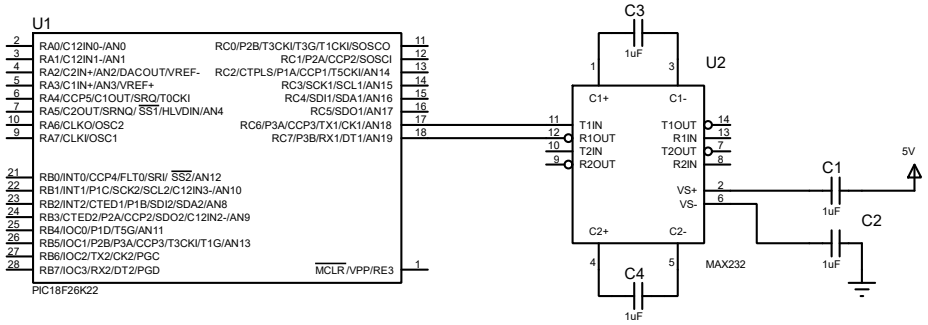


Ilustración 39: Diagrama de conexiones 18F26K22 + MAX232

5.3. Implementación del programa de control

El programa de control que se debe implementar en el microcontrolador es el que se ha definido para el comportamiento del sistema, cuyo funcionamiento es el siguiente:

Emisor:

- Continuamente el sistema estará monitorizando las señales analógicas y cada 30 segundos envía a la centralita la información
- Si durante ese transcurso de 30 segundos se ha detectado presencia, se mandará una señal al microcontrolador para que se activen los circuitos de activación sonora y luminosa, donde en concreto:
    - La sirena se activará (tienen la opción de configurar manualmente los intervalos de intermitencia)

- El foco se encenderá

- Al detectar presencia desencadena la activación del sistema de alarma, por lo que únicamente podrá salirse de ese estado si durante un intervalo de 60 segundos seguidos no se ha cumplido la condición de activación. Será a partir de ese momento cuando la sirena y los focos se apaguen.

Receptor:

- Cuando los datos del emisor lleguen, en el display que tendrá instalado el receptor se mostrará el estado del sistema, donde hemos elegido que:
  - Si muestra A en pantalla, significa que ha saltado alarma
  - Si muestra S en pantalla, significa que ha habido sabotaje
  - Si muestra * en pantalla, significa que el sistema está en reposo, pues no ha detectado presencia

Aunque el código de implementación se adjunta en los anexos, se van a comentar las partes más relevantes.

Como se puede apreciar en la ilustración 40, los pines que se han programado se encuentran coloreados en color verde, y los pines que están en color azul, están libres para poder programarse.

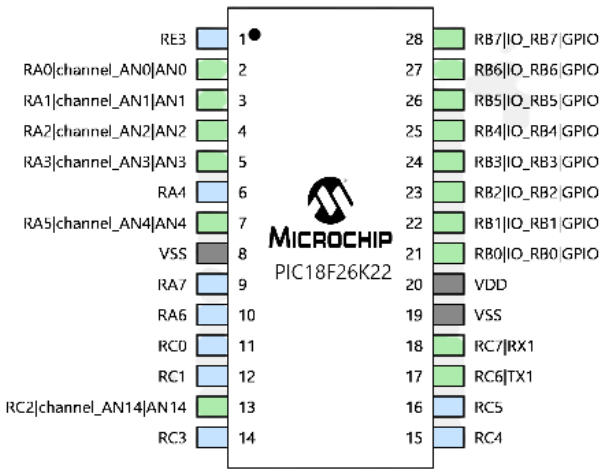


Ilustración 40: Visión general programación pines PIC 18F26K22

En el programa adjuntado en el anexo 15.5, como vemos en el código main.h estamos tratando la declaración de las variables que estamos utilizando en el programa, en nuestro caso las variables que hemos declarado con las etiquetas #define serán las salidas digitales correspondientes a los focos y la sirena. En el código main.c es donde se programa el comportamiento del sistema.

En las líneas 81 hasta 85 estamos programando la entrada digital del receptor Clemsa, para que cambie el estado del sistema en función del estado que tenga en ese momento el sistema cuando se desee apagar o encender la alarma general.

Por otro lado, cabe destacar que hemos asignado la entrada analógica AN0 a la barrera 1, AN1 a la barrera 2, AN2 a la barrera 3, AN3 a la barrera 4, AN 4 al volumétrico, AN14 al contacto magnético del armario de comunicaciones.

La activación de cada una de estas entradas desencadenará la activación de unas determinadas salidas, estas se recogen en la tabla:

ACTIVACIÓN ENTRADA	ACTIVACIÓN SALIDA
Barrera 1	Foco 1 Foco 2 Sirena
Barrera 2	Foco 2 Foco 3 Foco 4 Sirena
Barrera 3	Foco 4 Foco 5 Sirena
Barrera 4	Foco 1 Foco 6 Foco 5 Sirena
Volumétrico	Foco 1 Foco 2 Sirena
Contacto magnético	Foco 1 Foco 2 Foco 3 Foco 4 Foco 5 Sirena
Desactivación alarma	Desactivar las salidas

Tabla 11: Salidas que se activan en función de la entrada activada

6. Circuito de medidas analógicas

Para realizar los circuitos de medidas analógicas, tendremos que conocer el número de entradas que se van a tener. En nuestro caso, tendremos 7 entradas, de las cuales 4 corresponderán a las barreras, 1 al detector volumétrico, 1 al contacto magnético, y otro para el receptor Clemsa.

Después de haber identificado las entradas del sistema, será necesario que consultemos las especificaciones de los equipos que vamos a utilizar para el diseño de los circuitos.

6.1. Barreras detectoras infrarrojas

Para las barreras detectoras infrarrojas utilizaremos el dispositivo ABH-150 L [45]. Como observamos en su datasheet, aparecen las conexiones del extremo transmisor y del extremo receptor. En estos conectores será necesario que físicamente instalemos dos resistencias, que, siguiendo el esquema de conexiones, quedaría de la siguiente forma:

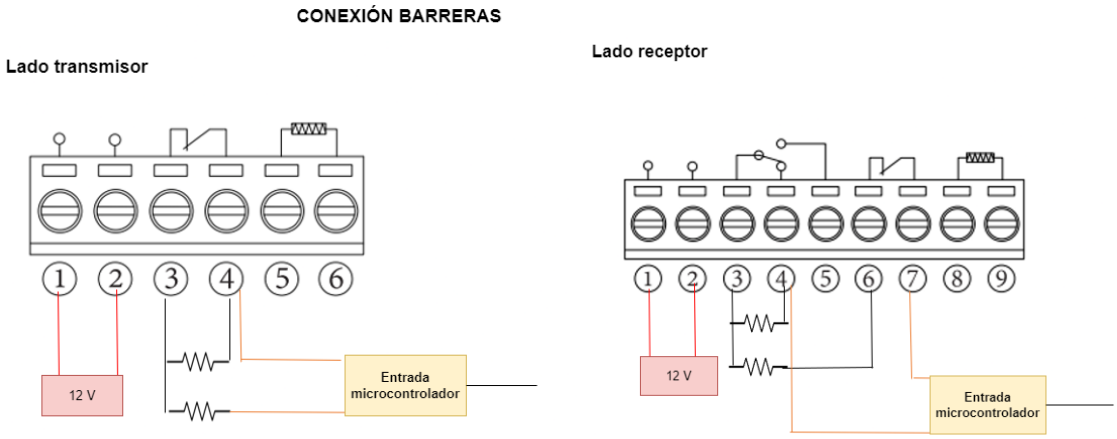


Ilustración 41: Conexión lado transmisor y receptor barreras

En el lado transmisor, las bornas 1 y 2 deberán estar alimentadas con 12 V, pues es el voltaje de funcionamiento de la barrera, por otro lado, deberemos instalar una resistencia en la borna 3 y 4, que es donde se encuentra el tamper, y conectaremos otra resistencia en la borna 3 donde la patilla que se encuentra en el aire irá conectada hacia la entrada analógica del microcontrolador. En este caso, no será necesario que el lado transmisor esté conectado a la entrada del microcontrolador, pues sabemos que las barreras están conformadas por haces de luz, donde el emisor se comporta como un espejo reflejando los haces de luz del lado receptor. Si se tuviese en consideración la entrada del transmisor en el sistema, podrían existir problemas en la lectura al detectar el lado receptor alarma si salta el tamper del transmisor.

En el lado receptor, las bornas 1 y 2 recibirán la alimentación de 12 V, se colocará una resistencia en la borna 3 y 4, y otra resistencia en la borna 3 y 6. Y las bornas 4 y 7 se conectarán hacia la entrada analógica del microcontrolador. Cabe destacar que el lado receptor es el extremo que posee la alarma, es decir, el lado que se encargará de generar la señal de detección de presencia.

El esquema del receptor estará formado por tres resistencias, donde será importante que sean del mismo valor. Como vemos en la ilustración 42, será necesario que utilicemos tres resistencias, porque si no colocásemos la resistencia R3, el sistema no conseguirá obtener la lectura de los estados, pues únicamente se tomaría un valor de 0 V, por la toma de tierra. Además, la resistencia R3 no modificará los resultados del sensor, ya que la entrada al microcontrolador se colocará entre R2 y R3.

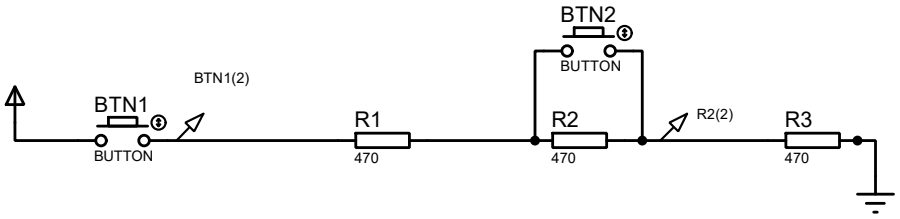


Ilustración 42: Esquema circuito receptor

Como el sistema estará conectado al microcontrolador, introducimos una entrada de 5 V. El botón 1 y el botón 2 nos van a ayudar a simular los tres estados que puede tomar el sistema:

- Si el botón 1 está cerrado y el botón 2 abierto, el sistema habrá detectado presencia
- Si el botón 1 está cerrado y el botón 2 cerrado, el sistema se encontrará en reposo
- Si el botón 1 está abierto, el sistema habrá sido saboteado

Si realizamos la simulación del escenario del lado receptor, podemos ver que funciona correctamente:

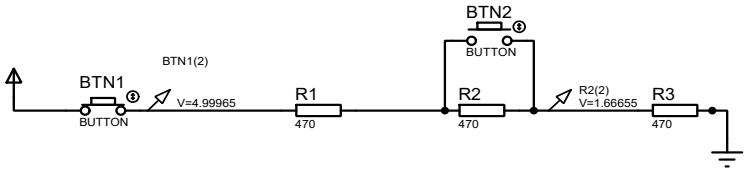


Ilustración 43: Detección de presencia

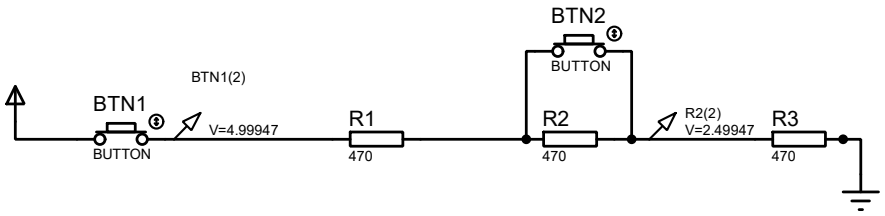


Ilustración 44: Estado de reposo

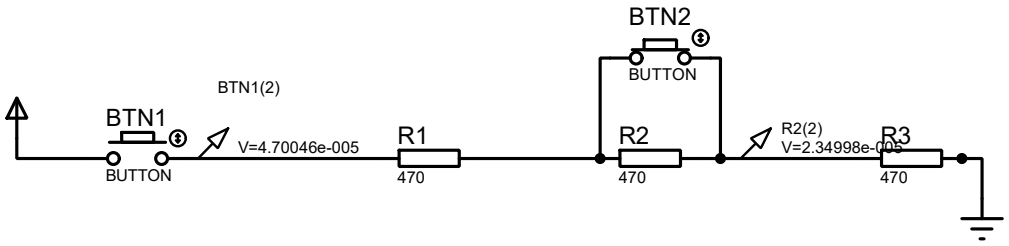


Ilustración 45: Sabotaje de la barrera

Como utilizaremos 4 barreras para cubrir todo el recinto, será necesario que tengamos en cuenta 4 veces el mismo montaje, además, cabe destacar que para realizar las conexiones físicas utilizaremos cables de 4+2, donde 2 cables estarán destinados para la alimentación, y los otros 4 cables serán para la señalización, donde utilizaremos 2 de ellos, quedando como reserva 2 cables más.

6.2. Sensor volumétrico

En nuestro sistema también tendremos en consideración un sensor volumétrico, utilizando un modelo de Optex [46] que estará colocado en la habitación donde instalemos el armario de comunicaciones. De esta forma también controlaremos la presencia en la habitación. En los anexos se adjuntarán los planos de la localización de cada elemento, el armario de comunicaciones, y el cuadro de maniobras.

En la ilustración 46 observamos el esquema de conexiones que deberíamos realizar en el sensor volumétrico. Si nos damos cuenta, el principio de funcionamiento es idéntico al de las barreras infrarrojas, por lo que el estado que puede tomar el sensor también estará determinado por los tres posibles estados, que son alarma, reposo y sabotaje

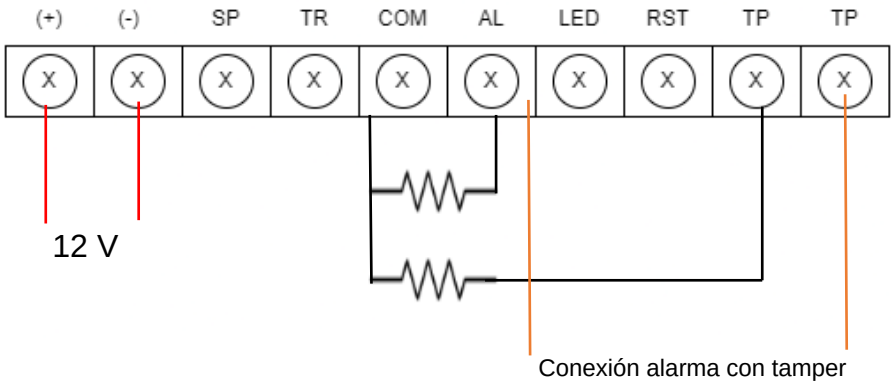


Ilustración 46: Esquema conexiones sensor volumétrico

La simulación del sensor volumétrico es idéntica a las ilustraciones 43, 44 y 45.

6.3. Contacto magnético

Utilizamos el contacto magnético como elemento de seguridad para instalar en la cerradura del armario de comunicaciones. Se ha optado por el modelo MC 470 [47]. Al ser un contacto magnético no necesita alimentación, por lo que únicamente será necesario realizar el montaje del tamper y la señal de alarma. Si nos fijamos, en la representación del elemento, el esquema de conexiones sería igual a los casos anteriores.

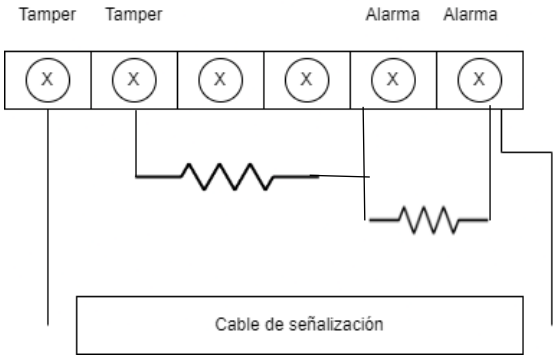


Ilustración 47: Esquema contacto magnético

Como podemos apreciar, el funcionamiento y la simulación va a ser igual al descrito en los apartados 6.1 y 6.2

6.4. Receptor Clemsa

Es necesario contar con un dispositivo que nos permita en un momento determinado apagar y encender de nuevo todo el sistema, para ello, utilizaremos un receptor de la marca Clemsa [48]. Según el esquema de conexiones que observamos en su datasheet, tal y como aparece en la ilustración 48, lo que necesitaríamos para nuestra entrada sería proporcionarle alimentación de 12 V y en la bornera donde aparece RL1 la conectaremos a una salida digital del

microcontrolador, pues el sistema cambiará su estado en dos valores, o en 0 o en 1.

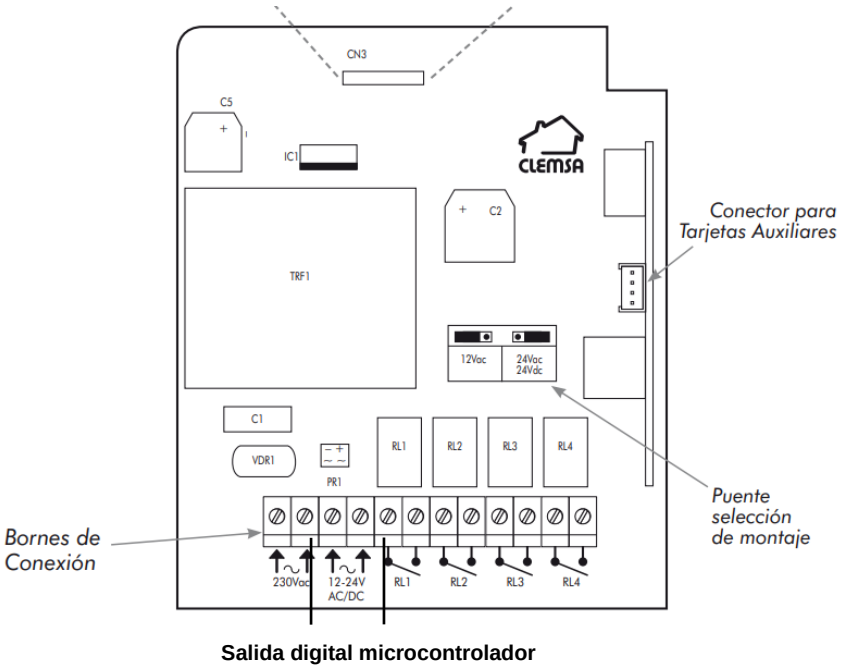


Ilustración 48: Esquema receptor Clemsa

7. Circuito de control de las salidas

Para el circuito de control de las salidas, será necesario conocer el número de salidas que tendrá nuestro sistema, en nuestro caso tendremos 6 focos y una sirena. En el anexo 15.3 se muestra la distribución de todos los elementos. Es importante destacar que como el emplazamiento se ha dividido por zonas, cada entrada tendrá asociadas unas salidas determinadas, éstas se encuentran especificadas en la tabla 11.

Para el diseño del circuito de activación de las salidas, tendremos en cuenta que las salidas serán digitales porque el estado que tomen los focos y la sirena también se encuentra definido por dos estados: encendido o apagado. En otras palabras, cuando en una de las zonas se detecte presencia, el circuito de medida de las entradas, que serán las barreras, enviará el valor del voltaje al pin del microcontrolador en el que se encuentre conectado. El microcontrolador comparará el voltaje recibido con los valores que se han programado en el programa de control, siendo 1.66 V el voltaje asociado a alarma, 2.49 V el valor asociado al reposo del sistema, y finalmente, $2.35 \cdot 10^{-5}$ V cuando el sistema ha sido saboteado. En función del valor obtenido, el microcontrolador mandará un impulso de 5 V, al ser el voltaje del trabajo del microcontrolador, al relé para que éste active o desactive las salidas en función del estado del sistema.

Como vemos en la ilustración 49, este es el diseño que se ha propuesto para verificar que realmente funciona la conmutación de los relés, iluminando y apagando los leds. En el diseño final las salidas que estamos simulando con 0 y 1, irán conectadas a las salidas digitales del microcontrolador.

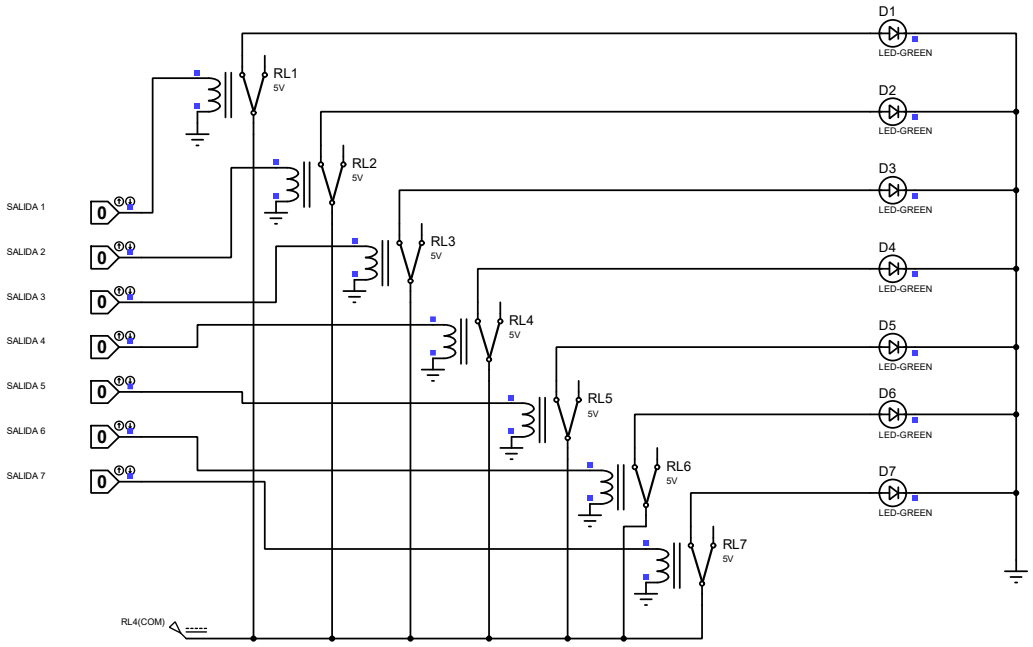


Ilustración 49: Diseño de circuito de las salidas

8. Fuente de alimentación

Para la realización del diseño de la fuente de alimentación del sistema será necesario tener en consideración que ésta debe suministrar los voltajes adecuados a cada elemento del sistema, sabiendo que:

- La alimentación que suministra la red es de 220-230 V de C.A, siendo necesario convertirla a 12 V de C.C y a 5 V de C.C
- Es necesario realizar estas dos transformaciones porque el microcontrolador que hemos seleccionado funciona a una tensión de 5 V de C.C, y las barreras de detección por infrarrojos empiezan a funcionar a partir de 12 V de C.C

Para poder realizar esta conversión de voltaje utilizaremos el transformador existente en la librería de componentes de Proteus 8 Professional, seleccionando concretamente el que tiene por referencia TRAN-2P3S. Al tratarse de un proyecto teórico, y no elegir componentes con referencias reales, a la hora de realizar los cálculos para obtener los valores de los condensadores que actúan como filtro podremos poner un valor orientativo, sin embargo, se puede calcular conociendo la intensidad máxima, el tiempo de descarga y los voltajes que hay antes de la carga y después de la descarga del condensador.

En este caso, estamos convirtiendo la onda sinusoidal de 50 Hz de amplitud de 220 V a 12 V, si asumimos una corriente máxima de 0.5 A, sabremos que el condensador se cargará hasta un voltaje máximo de 12 V en alterna. Como la tensión de salida debe estar en continua, sabremos que realmente obtendremos $12Vca \cdot \sqrt{2} = 16.97\,V$ como tensión máxima en continua. Conocemos que la caída de tensión del puente de Graetz es aproximadamente de 1.4 V. Para averiguar el tiempo de carga sabemos que el periodo es la inversa de la frecuencia, por lo que en este caso $Tc = \frac{1}{f} = \frac{1}{50} = 20\,ms$, y la salida, al estar influida por el rectificador, se obtiene una salida rectificada cuyo tiempo de descarga será de la mitad del periodo de carga, en este caso 10 ms. El voltaje mínimo que se utilizará será el punto de operación de entrada mínima del LM7805. En su datasheet observamos que este valor es de 7 V. Por lo tanto, el condensador que utilizaremos en nuestro diseño tendrá por valor:

$$C = \frac{I_{máx} \cdot T_{descarga}}{V_{máx} - V_{mín\ operación}} = \frac{0.5 \cdot 10 \cdot 10^{-3}}{16.97 - 7} = 501.5\ \mu F$$

En este caso, elegimos el valor comercial más alto que se ajuste al valor calculado, porque cuanto mayor sea este valor más aplanará la tensión de salida del puente de Graetz, es decir, la tensión será más uniforme. Por ejemplo, elegimos un condensador de 1000 μF

El diseño que se propone para la fuente de alimentación es el siguiente:

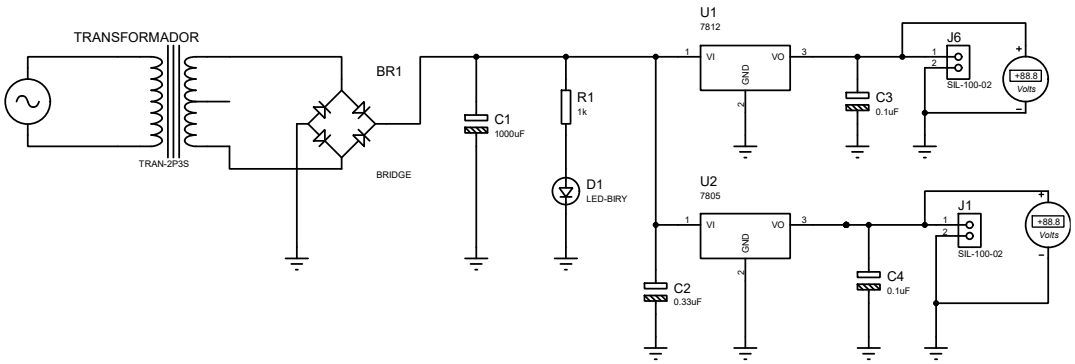


Ilustración 50: Diseño fuente de alimentación

Como se aprecia en la ilustración 50, nuestro diseño está conformado por un transformador de 220 V/ 12 V a 50 Hz y 220 V/ 5 V a 50 Hz, por otro lado, tenemos un puente rectificador de doble onda que estará compuesto por 4 diodos 1N4007. Estos se encargarán de convertir la señal alterna de entrada en una señal de salida pulsante. El condensador C1 como se ha comentado anteriormente, es un condensador de filtro, ya que después de haber realizado la rectificación de la corriente alterna, con el filtrado se obtiene un aplanamiento de la tensión pulsatoria que entrega el rectificador, consiguiendo una tensión con menos ondulación. Sin embargo, los condensadores C2, C3 y C4 evitan los picos de radiofrecuencias, en este caso, se colocan los valores indicados por los fabricantes en el datasheet de los reguladores de voltaje LM7812 y LM7805.
El LED D1 se ha colocado como indicador para conocer el estado de la fuente de alimentación, es importante que vaya acompañado de una resistencia limitadora del diodo, para evitar que el diodo se queme.

En la ilustración 51 se puede observar la simulación de la fuente de alimentación:

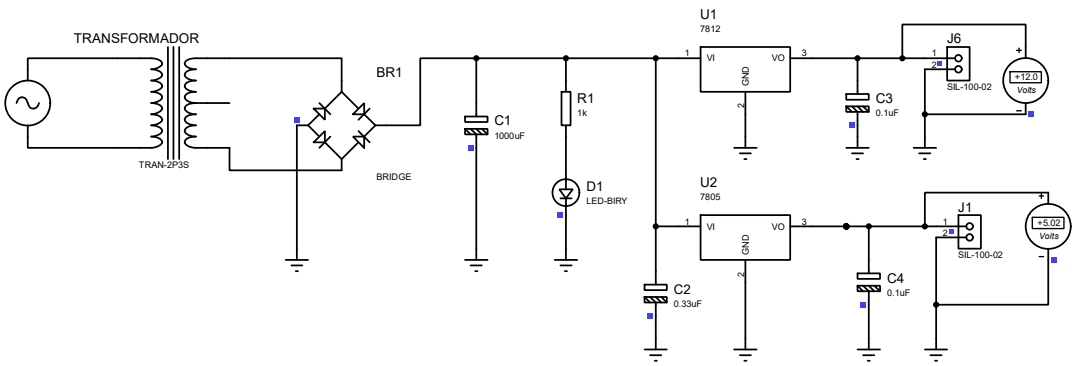


Ilustración 51: Simulación de la fuente de alimentación

Mostramos a continuación las señales de las ondas resultantes de la simulación de nuestra fuente de alimentación, como se puede observar, se obtienen los valores de tensión deseados:

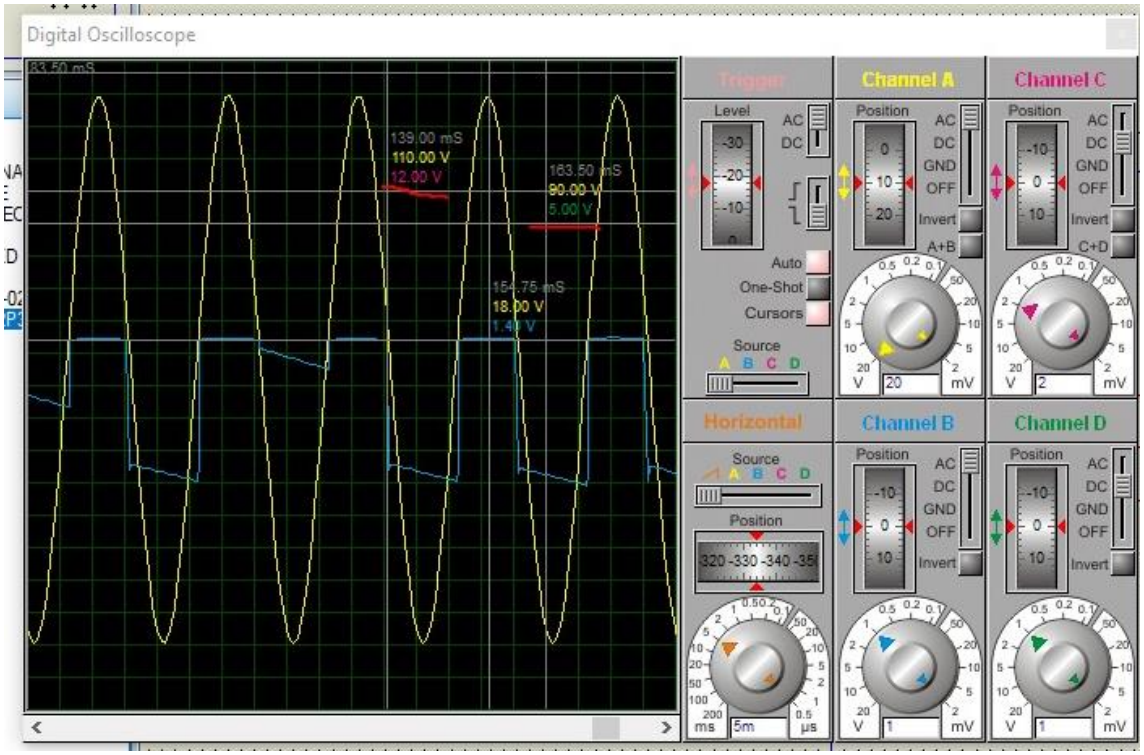


Ilustración 52: Ondas de las señales de salida

9. Centralita

Como se ha comentado anteriormente, nuestro sistema estará monitorizando las señales analógicas constantemente, y en intervalos de 30 segundos irá enviando la información del estado del sistema a la centralita.

Aprovechando que estamos realizando un radioenlace para compartir internet con las cámaras y poder monitorizarlas, se puede utilizar como centralita receptora un Arduino junto con un módulo ENC28J60 [49], al que le podremos acoplar un LCD de 16x2.

La idea es conectar un switch a la antena transmisora del radioenlace que se encontrará en el domicilio, y en ese switch conectar la centralita a través del RJ-45 que posee el módulo ENC28J60, y en el lado donde se encuentra la antena receptora, se encontrará el microcontrolador PIC 18F26K22 + MAX232 al que le acoplaremos un convertidor de la marca Ambetronics [50] que se encargará de convertir la señal del puerto RS232 en Ethernet. Como vemos, este conversor posee un RJ-45 al que lo conectaremos en el switch que vaya a la antena receptora, de esta manera, conseguiremos transmitir los datos del sistema hasta el domicilio remotamente.

El esquema del sistema es el siguiente:

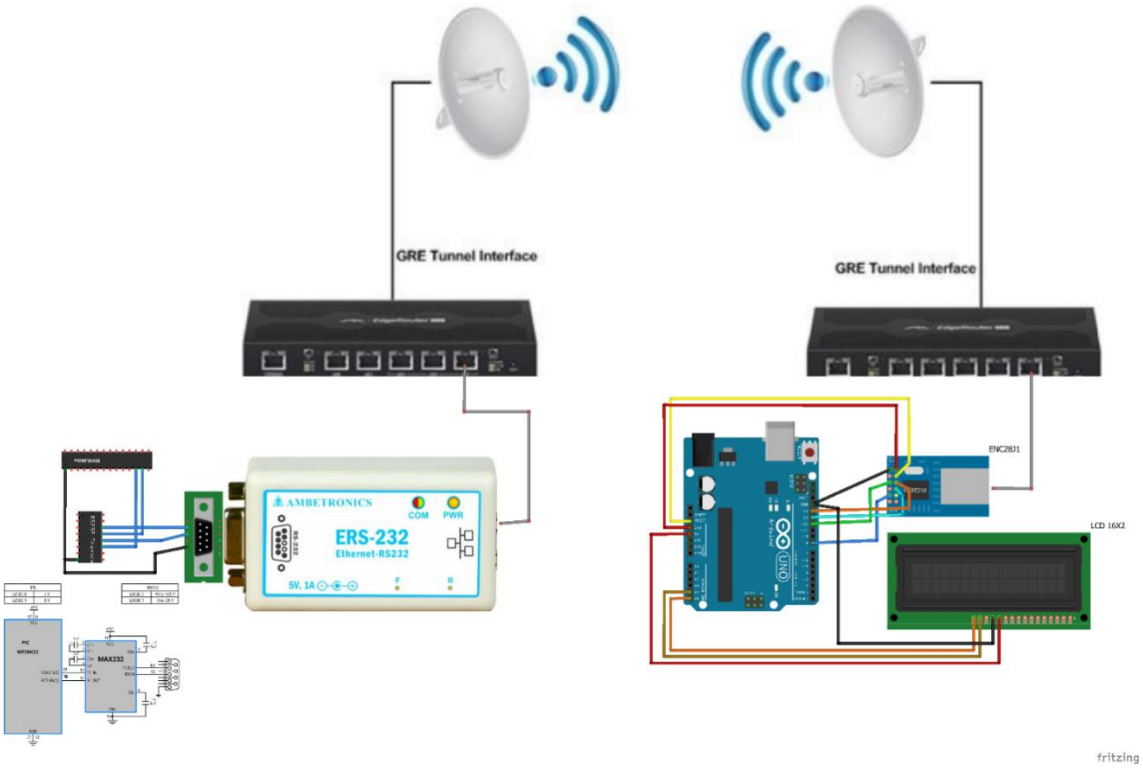


Ilustración 53: Esquema de conexión y elementos de la centralita

Será necesario que realicemos un programa para cargarlo en la placa Arduino. El código de este programa se encuentra en el anexo 15.6

En este caso, en el programa hemos colocado una IP ficticia, pero será importante que introduzcamos la dirección IP de la antena del radioenlace.

10. Layout de los circuitos impresos

Para realizar el diseño de la placa PCB que contendrá todos los elementos del sistema, hemos utilizado Proteus. Para ello ha sido necesario realizar primeramente el esquema de los componentes con todas sus conexiones, después de ello, deberemos ir a la pestaña PCB Layout, en ella en el margen izquierdo nos aparecerá la lista de componentes que hemos utilizado. Será necesario colocarlos en el espacio que nos aparece. Una vez colocados, podemos generar las pistas automáticamente seleccionando la opción Design Rule Manager > Net Classes, en esa pestaña en la opción Net Class seleccionamos Power. Ahí veremos que las pistas coloreadas en color rojo simbolizan que las pistas se encuentran en la cara de arriba, y las de color azul las que se encuentran en la cara de atrás.

Después de haber realizado ese paso, vamos a la pestaña Tools > Auto Router > Begin Routing. Después de que se ejecute este proceso, veremos como aparecen dibujadas todas las pistas de los componentes, tal y como aparece en la ilustración 54.

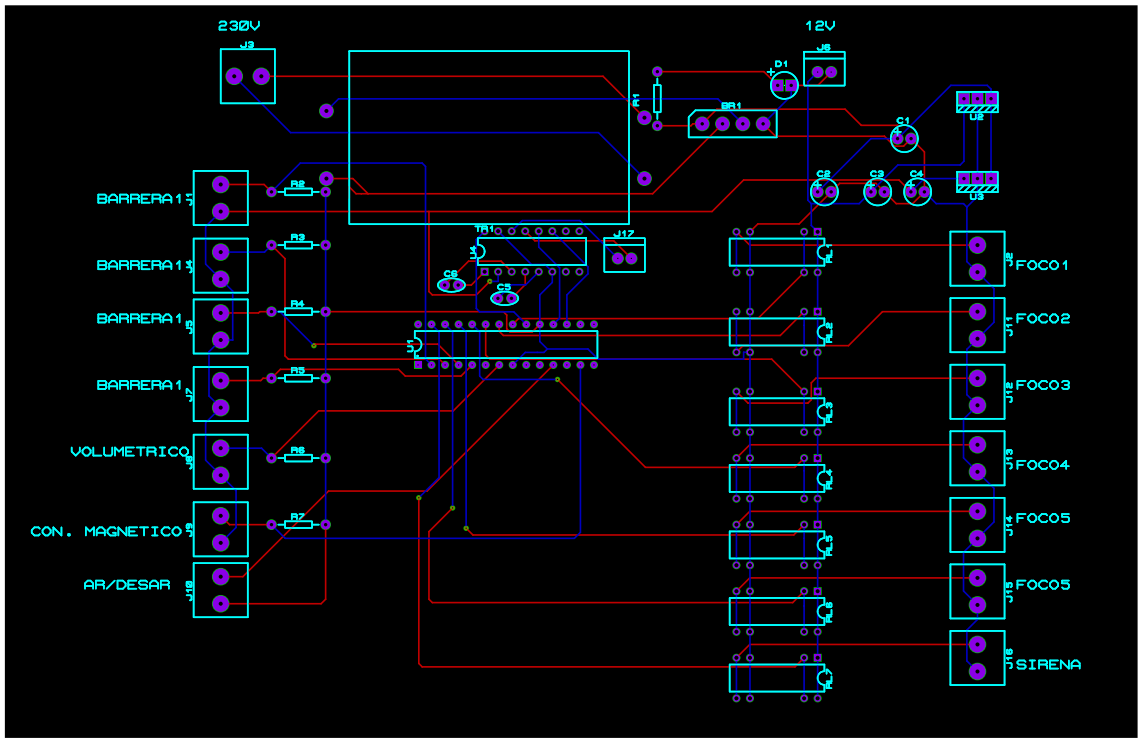


Ilustración 54: Layout del sistema

El esquema general de conexiones se encuentra en el anexo 15.7

11. Estimación económica del sistema

Para realizar la estimación económica del sistema será necesario tener en consideración todos los elementos que intervienen en el sistema. Consideraremos que la placa PCB contiene todos los elementos necesarios para el correcto funcionamiento, por lo que únicamente tendremos que tener en cuenta:

Todos los equipos externos a la placa, como son los equipos de radioenlace, las barreras infrarrojas, los focos, la sirena, el armario de comunicaciones, los magnetotérmicos, el equipo que sirve para controlar apagar o encender todo el sistema, el sensor volumétrico, un Arduino + módulo Ethernet ENC28J60, cámaras de videovigilancia, relés modulares, filas H.480 mm Schneider…

Finalmente, el presupuesto estimado sería el siguiente:

PRESUPUESTO DEL SISTEMA			
Artículo	Cantidad	Precio/ud	Precio total
Equipos de radioenlace	2	147,56 €	295,12 €
Barreras detectoras infrarrojas	4	79,53 €	318,12 €
Focos industriales	6	165,08 €	990,48 €
Sirena/Alarma	1	101,54 €	101,54 €
Armario de comunicaciones	1	622,00 €	622,00 €
Interruptor diferencial 25A	1	43,54 €	43,54 €
Interruptor magnetotérmico 2P-16A	2	13,24 €	26,48 €
Interruptor magnetotérmico 2P-10A	1	12,99 €	12,99 €
Interruptor magnetotérmico 2P-25 A	1	14,49 €	14,49 €
Receptor Clemsa	1	117,00 €	117,00 €
Sensor volumétrico	1	42,90 €	42,90 €
Kit Arduino	1	24,00 €	24,00 €
Módulo Ethernet ENC28J60	1	9,99 €	9,99 €
Cámaras de videovigilancia	3	61,35 €	184,05 €
Placa PCB	1	50,00 €	50,00 €
Relés modulares	7	23,72 €	166,04 €
Cable 4 hilos + 2 alimentación	4	59,29 €	237,16 €
Superficie 2 filas H.480 mm	1	72,84 €	72,84 €
Contacto magnético de superficie	1	21,43 €	21,43 €
Torreta de telecomunicaciones	1	219,74 €	219,74 €
	PRECIO FINAL		3.569,91 €

Ilustración 55: Presupuesto estimado del proyecto

12. Conclusiones y ampliaciones

Después de haber realizado el proyecto, la principal lección que podemos recoger de todas estas páginas, es que, aunque no se hayan hecho nunca diseños de circuitos ni se hayan programado microcontroladores, con determinación, esfuerzo y constancia, todos los retos consiguen superarse. Por otro lado, los factores determinantes para poder haber llevado a cabo el trabajo de final de grado han sido la capacidad de saber gestionar el tiempo, y la capacidad de solucionar los inconvenientes.

Han sido necesarias realizar muchas modificaciones a lo largo del trabajo, como, por ejemplo, cambiar la manera de transmitir los datos desde el microcontrolador hasta la centralita, ya que, en vez de utilizar un módulo de radiofrecuencia, hemos optado por utilizar un módulo MAX232, que, junto con un Arduino, el módulo Ethernet ENC28J60 y un LCD, nos permite la transmisión y recepción de los datos, visionándolos a través del display que se puede instalar en la placa de Arduino. De esta forma estaremos aprovechando la funcionalidad que nos permiten los radioenlaces, al mandar los datos por los mismos. Así mismo, otra de las cosas que han sido necesarias cambiar ha sido la banda de frecuencias de trabajo, ya que al no usar un módulo RF, utilizaremos la banda de frecuencia de trabajo de las antenas de radioenlace, que en este caso ha sido la banda de frecuencias libre de los 5 GHz. Cabe destacar, que en un primer término, las cámaras se contemplaba que estuviesen apagadas y que únicamente estuviesen encendidas cuando se detectase alarma, a lo largo del proyecto, ha sido necesario cambiar esta condición, y establecer que las cámaras permanezcan encendidas de forma constante, pues desde un punto de vista técnico, si la cámara permanece apagada, y se detecta intrusión, no era viable que en ese momento se encendiese ya que le cuesta bastante tiempo hasta que la cámara está lista para mostrar imagen.

Por otro lado, se han logrado gran parte de los objetivos, pues se ha conseguido realizar el diseño de cada uno de los elementos que integran el sistema, se ha conseguido realizar una funcionalidad de 2/3 partes del sistema, de forma simulada, y se ha conseguido desarrollar teóricamente la funcionalidad de transmitir y recibir los datos de forma remota, teniendo en cuenta el código de Arduino. Para todo ello ha sido necesario seguir la planificación y la metodología que nos marcamos en un principio. En la tabla 3 identificamos las posibles incidencias y riesgos del proyecto, y después de haber terminado el proyecto los riesgos que se clasificaron como R04, R05, R06, R08, acabaron teniendo un impacto en cuanto a los plazos establecidos en un inicio en el diagrama de Gantt de la ilustración 3, sin embargo, aunque estos tuvieron un impacto, no afectaron al plazo de fecha final de cada entregable, no siendo necesaria una prórroga.

El diagrama de Gantt que se ha seguido en la realidad se recogerá en la ilustración 55:

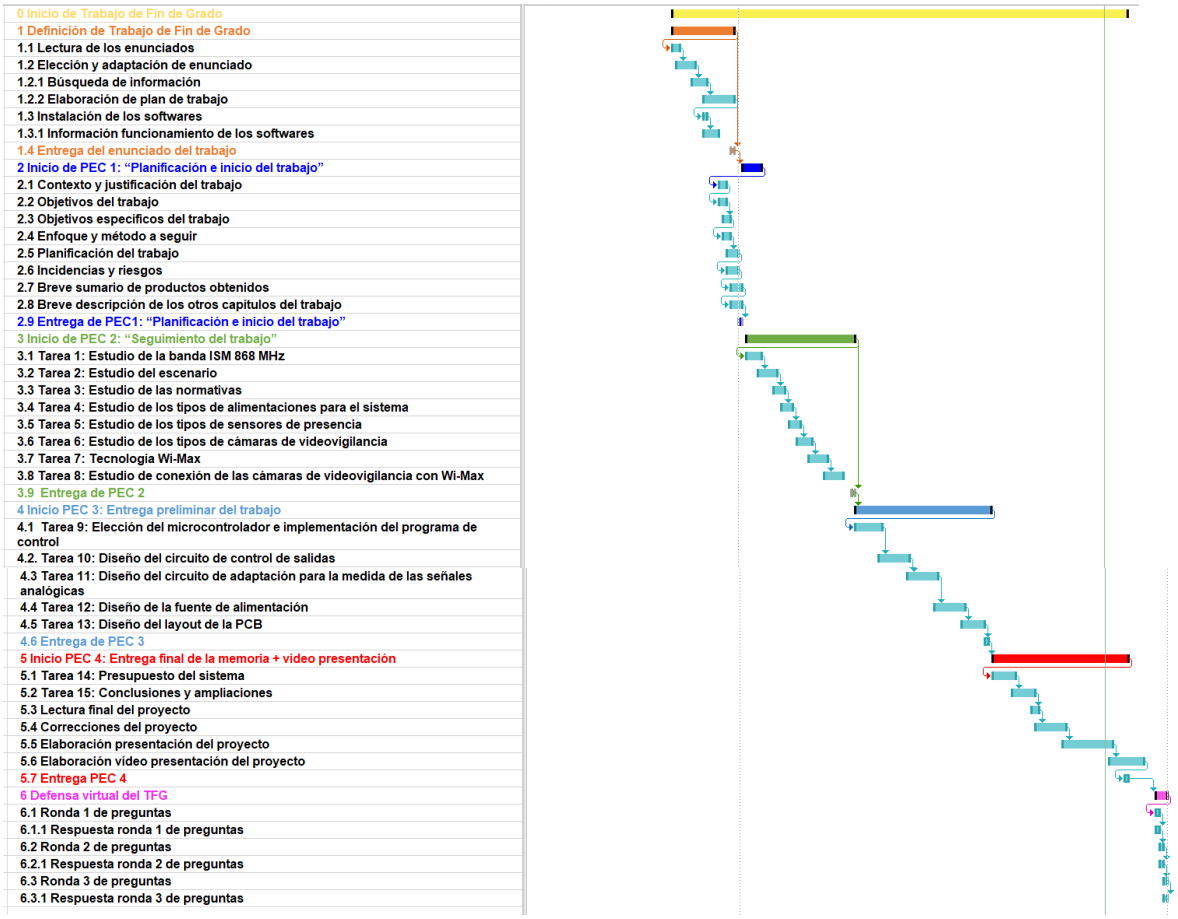


Ilustración 56: Diagrama Gantt final

El desglose por fechas es el siguiente:

Nombre de tarea	Duración	Comienzo	Fin
0 Inicio de Trabajo de Fin de Grado	83 días	jue 17/02/22	lun 13/06/22
1 Definición de Trabajo de Fin de Grado	12 días	jue 17/02/22	vie 04/03/22
1.1 Lectura de los enunciados	2 días	jue 17/02/22	vie 18/02/22
1.2 Elección y adaptación de enunciado	3 días	vie 18/02/22	mar 22/02/22
1.2.1 Búsqueda de información	4 días	mar 22/02/22	vie 25/02/22
1.2.2 Elaboración de plan de trabajo	6 días	vie 25/02/22	vie 04/03/22
1.3 Instalación de los softwares	1 día	vie 25/02/22	vie 25/02/22
1.3.1 Información funcionamiento de los softwares	2 días	vie 25/02/22	lun 28/02/22
1.4 Entrega del enunciado del trabajo	1 día	vie 04/03/22	vie 04/03/22

2 Inicio de PEC 1: "Planificación e inicio del trabajo"	5 días	lun 07/03/22	vie 11/03/22
2.1 Contexto y justificación del trabajo	2 días	mar 01/03/22	mié 02/03/22
2.2 Objetivos del trabajo	2 días	mar 01/03/22	mié 02/03/22
2.3 Objetivos específicos del trabajo	2 días	mié 02/03/22	jue 03/03/22
2.4 Enfoque y método a seguir	2 días	mié 02/03/22	jue 03/03/22
2.5 Planificación del trabajo	3 días	jue 03/03/22	sáb 05/03/22
2.6 Incidencias y riesgos	3 días	jue 03/03/22	sáb 05/03/22
2.7 Breve sumario de productos obtenidos	2 días	vie 04/03/22	dom 06/03/22
2.8 Breve descripción de los otros capítulos del trabajo	2 días	vie 04/03/22	dom 06/03/22
2.9 Entrega de PEC1: "Planificación e inicio del trabajo"	1 día	dom 06/03/22	dom 06/03/22
3 Inicio de PEC 2: "Seguimiento del trabajo"	20 días	mar 08/03/22	lun 04/04/22
3.1 Tarea 1: Estudio de la banda ISM 868 MHz	4 días	mar 08/03/22	vie 11/03/22
3.2 Tarea 2: Estudio del escenario	3 días	vie 11/03/22	mar 15/03/22
3.3 Tarea 3: Estudio de las normativas	3 días	mar 15/03/22	jue 17/03/22
3.4 Tarea 4: Estudio de los tipos de alimentaciones para el sistema	3 días	jue 17/03/22	sáb 19/03/22
3.5 Tarea 5: Estudio de los tipos de sensores de presencia	2 días	sáb 19/03/22	lun 21/03/22
3.6 Tarea 6: Estudio de los tipos de cámaras de videovigilancia	4 días	lun 21/03/22	jue 24/03/22
3.7 Tarea 7: Tecnología Wi-Max	3 días	jue 24/03/22	lun 28/03/22
3.8 Tarea 8: Estudio de conexión de las cámaras de videovigilancia con Wi-Max	5 días	lun 28/03/22	vie 01/04/22
3.9 Entrega de PEC 2	1 día	lun 04/04/22	lun 04/04/22
4 Inicio PEC 3: Entrega preliminar del trabajo	25 días	mar 05/04/22	lun 09/05/22
4.1 Tarea 9: Elección del microcontrolador e	5 días	mar 05/04/22	lun 11/04/22

implementación del programa de control			
4.2. Tarea 10: Diseño del circuito de control de salidas	6 días	lun 11/04/22	lun 18/04/22
4.3 Tarea 11: Diseño del circuito de adaptación para la medida de las señales analógicas	6 días	lun 18/04/22	lun 25/04/22
4.4 Tarea 12: Diseño de la fuente de alimentación	6 días	lun 25/04/22	lun 02/05/22
4.5 Tarea 13: Diseño del layout de la PCB	6 días	lun 02/05/22	sáb 07/05/22
4.6 Entrega de PEC 3	1 día	dom 08/05/22	dom 08/05/22
5 Inicio PEC 4: Entrega final de la memoria + vídeo presentación	25 días	mar 10/05/22	lun 13/06/22
5.1 Tarea 14: Presupuesto del sistema	5 días	mar 10/05/22	dom 15/05/22
5.2 Tarea 15: Conclusiones y ampliaciones	6 días	dom 15/05/22	vie 20/05/22
5.3 Lectura final del proyecto	2 días	vie 20/05/22	sáb 21/05/22
5.4 Correcciones del proyecto	7 días	sáb 21/05/22	sáb 28/05/22
5.5 Elaboración presentación del proyecto	10 días	sáb 28/05/22	jue 09/06/22
5.6 Elaboración vídeo presentación del proyecto	7 días	jue 09/06/22	vie 10/06/22
5.7 Entrega PEC 4	1 día	lun 13/06/22	lun 13/06/22
6 Defensa virtual del TFG	3 días	mar 21/06/22	jue 23/06/22
6.1 Ronda 1 de preguntas	1 día	mar 21/06/22	mar 21/06/22
6.1.1 Respuesta ronda 1 de preguntas	1 día	mar 21/06/22	mar 21/06/22
6.2 Ronda 2 de preguntas	1 día	mié 22/06/22	mié 22/06/22
6.2.1 Respuesta ronda 2 de preguntas	1 día	mié 22/06/22	mié 22/06/22
6.3 Ronda 3 de preguntas	1 día	jue 23/06/22	jue 23/06/22

Tabla 12: Desglose de fechas de inicio y final de cada tarea del proyecto

Finalmente, sobre líneas de trabajo futuras cabe la posibilidad de la implantación real del proyecto en el emplazamiento expuesto, por lo que este proyecto serviría como la guía para la implementación, colocación y programación del programa de control, sin embargo, al haber sido un proyecto íntegramente teórico, es probable que a la hora de una implementación real sean necesarias modificaciones sobre la programación e incluso sobre los diseños de los elementos. Como se ha podido comprobar en la prueba de simulación final, de las funcionalidades del sistema se ha demostrado que funcionan 2/3 partes, no pudiendo simular la desactivación de las salidas cuando al estar la alarma activada, no se cumple la condición de nuevo durante esos 60 segundos. No ha sido posible arreglar el fallo, al no disponer de más tiempo. Por otro lado, como una posible ampliación del proyecto cabe la posibilidad de sustituir la centralita por un dispositivo móvil, de esta forma conseguiríamos obtener por mensaje el estado del sistema.

13. Glosario

Espectro electromagnético: Se conoce por espectro electromagnético al conjunto de frecuencias y/o longitudes de onda de todas las radiaciones electromagnéticas

Radiofrecuencia: La radiofrecuencia es la tasa de oscilación del espectro electromagnético

Radioenlace: Un radioenlace es un sistema electrónico que nos permite realizar comunicaciones inalámbricas a través de ondas de radio

Método Picquernard: Es un método que sirve para calcular las atenuaciones en un radioenlace producidas por los obstáculos existentes entre los equipos transmisor y receptor. Generalmente, los cálculos que se emplean para este método se realizan sobre el perfil orográfico del lugar, obteniendo una mayor precisión respecto al método de pérdidas por el espacio libre.

ITU: La ITU o UIT es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación

14. Bibliografía

[1] *Radicación de la palabra Electrónica*. (s. f.). Etimologías de Chile - Diccionario que explica el origen de las palabras. [Consultado el 1 de marzo de 2022] URL: http://etimologias.dechile.net/?electro.nica#:%7E:text=La%20palabra%20%22electr%C3%B3nica%22%20est%C3%A1%20formada,%2Diko%20(relativo%20a).

[2] S. (2020, 7 noviembre). *Alarmas para huertos solares*. Second Seguridad. [Consultado el 1 de marzo de 2022] URL: https://seguridadsecond.es/alarmas-para-huertos-solares/

[3] de Córdoba, E. D. (2021, 27 enero). *Los hurtos en las zonas de cultivo, cada vez más habituales*. El Día de Córdoba. [Consultado el 1 de marzo de 2022]. URL: https://www.eldiadecordoba.es/cordoba/hurtos-zonas-cultivo-vez-habituales_0_1540346073.html

[4] U. (2022, 28 marzo). *Espectro Electromagnético*. [Consultado el 10 de marzo de 2022] Enredados2012. https://enredados2012.blogspot.com/2013/02/espectro-electromagnetico.html

[5] *Canon : Canon Technology | Canon Science Lab | Light is It a Wave or a Particle?* (s. f.). Canon Global. [Consultado el 10 de marzo de 2022] https://global.canon/en/technology/s_labo/light/001/11.html

[6] colaboradores de Wikipedia. (2022, 11 marzo). [Consultado el 10 de marzo de 2022] *Experimento de Young*. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Experimento_de_Young

[7] *Sistemas de comunicaciones electrónicas*. (s. f.). [Consultado el 11 de marzo de 2022] Google Books. https://books.google.es/books?id=_2HCio8aZiQC&pg=PA6&lpg=PA6&dq=designaciones+de+banda+CCIR&source=bl&ots=vw02L4AOrd&sig=ACfU3U0-bTj3j0dT-XP7IiIsaVSIxtZjfw&hl=es&sa=X&ved=2ahUKEwj5pqHly-

j2AhVLUxoKHXG4DDcQ6AF6BAgkEAM#v=onepage&q=designaciones%20de%20banda%20CCIR&f=false

[8] Alai Secure - Colombia. (2021, 9 diciembre). *Radiofrecuencia en telecomunicaciones - AlaiSecure*. [Consultado el 11 de marzo de 2022] https://alaisecure.co/glosario/radiofrecuencia-en-telecomunicaciones/#:%7E:text=La%20radiofrecuencia%20se%20define%20como,los%203%20kilohercios%20(KHz).

[9] G. (2016, 25 septiembre). *Espectro electromagnético*. [Consultado el 11 de marzo de 2022] Asun Galera. https://asungalera.wordpress.com/2016/09/25/espectro-electromagnetico/

[10] *StackPath*. (s. f.). Militaryaerospace. [Consultado el 12 de marzo de 2022] https://www.militaryaerospace.com/directory/blog/14059677/what-are-the-ism-bands-and-what-are-they-used-for

[11] *Banda_ISM_ICM*. (s. f.). DMD2. [Consultado el 12 de marzo de 2022] https://dmd2.es/banda_ism_icm/

[12] *Frecuency ranges for global or regional harmonization of short-range devices*. (s. f.). ITU. [Consultado el 12 de marzo de 2022] https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.1896-1-201809-I!!PDF-E.pdf

[13] *Short Range Devices operating in the frecuency range 25 MHz to 1000 MHz*. (s. f.). ETSI. [Consultado el 12 de marzo de 2022] https://www.etsi.org/deliver/etsi_en/300200_300299/3002200302/01.01.00_20/en_3002200302v010100a.pdf

[14] *Estudio relativo al uso de equipos de radiocomunicaciones de baja potencia*. (s. f.). Subtel.gob.cl. [Consultado el 12 de marzo de 2022] https://www.subtel.gob.cl/images/stories/articles/subtel/asocfile/informe_final_mod_i.pdf

[15] *Funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada*. (s. f.). BOE. [Consultado el 12 de marzo de 2022] https://www.boe.es/buscar/pdf/2011/BOE-A-2011-3170-consolidado.pdf

[16] Report, R. P. (2022, 6 enero). *Qué hay que poner en el cartel de videovigilancia RGPD*. Protection Report SL. [13 de marzo de 2022] https://www.protectionreport.com/articulos/rgpd/cartel-videovigilancia-rgpd/

[17] Solarat, C. (2021, 7 abril). *Wind Catcher un revolucionario aerogenerador eléctrico portátil que se instala en 15 minutos - Cultura Inquieta*. Cultura inquieta.[13 de marzo de 2022] https://culturainquieta.com/es/sostenibilidad/item/18031-wind-catcher-el-revolucionario-aerogenerador-portatil-que-se-instala-en-15-minutos.html

[18] S. (2021, 7 febrero). *Detector de presencia: cómo funciona y cómo se conecta | S&P*. S&P Sistemas de Ventilación. [Consultado el 13 de marzo de 2022] https://www.solerpalau.com/es-es/blog/detector-de-presencia-como-funciona-y-como-se-conecta/

[19] Fegemu Automatismos S.L. (s. f.). *Sensores de presencia. Productos. Fegemu Solutions*. [13 de marzo de 2022] https://www.fegaut.com/es/productos/sensores-de-presencia/2/

[20] *Barreras infrarrojos exterior por cable,4 haces, alcance 40m.* (2019, 22 marzo). COMPEL. [13 de marzo de 2022] http://www.electronicacompel.es/producto/barreras-infrarrojos-exterior-por-cable4-haces-alcance-40m/

[21] A. (2020, 18 febrero). *Internet Satelital: ¿Que es? ¿Como funciona? Ventajas y desventajas.* OK HOSTING | Hospedaje Web, Dominios, Desarrollo de Software, Marketing Online, SEO. [Consultado el 19 de marzo de 2022] https://okhosting.com/blog/internet-satelital/

[22] Fernández, Y. (2019, 26 julio). *Internet por satélite: qué es, como funciona y las mejores tarifas*. Xataka. [Consultado el 19 de marzo de 2022]

https://www.xataka.com/basics/internet-satelite-que-como-funciona-mejores-tarifas

[23] Fernández, Y. (2021, 9 febrero). *Qué es Starlink, cómo funciona y cuánto cuesta*. Xataka.[19 de marzo de 2022] https://www.xataka.com/basics/que-starlink-como-funciona-cuanto-cuesta

[24] *¿Qué es WiMax? ¿Cómo funciona?* (s. f.). Embou. [19 de marzo de 2022] https://www.embou.com/blog/que-es-el-wimax

[25] W. (2021, 25 enero). *Internet WiMAX: qué es, cómo funciona y ventajas | acomsis*. acomsis |. [19 de marzo de 2022] http://web.acomsis.com/internet-wimax-que-es-y-como-funciona/

[26] *WiMax Que es, Como Funciona, Ventajas, Diferencias WiFi*. (s. f.). Área tecnología. [19 de marzo de 2022] https://www.areatecnologia.com/informatica/wimax.html

[27] *Pérdidas en obstáculos | Radioenlaces*. (s. f.). Radioenlaces. [21 de marzo de 2022] http://www.radioenlaces.es/articulos/perdidas-en-obstaculos/

[28] A. (2020, 29 diciembre). *Zonas de Fresnel*. TODO TELCO. [21 de marzo de 2022] https://todotelco.com/zonas-de-fresnel/

[29] Gilani, N. (2018, 1 febrero). *Ventajas y desventajas de las comunicaciones de radio por microondas*. Geniolandia. [21 de marzo de 2022] https://www.geniolandia.com/13182158/ventajas-y-desventajas-de-las-comunicaciones-de-radio-por-microondas

[30] Soluciones, A. (2021, 23 septiembre). *¿Cuáles son las ventajas de los radioenlaces punto a punto?* Alora Soluciones. [21 de marzo de 2022] https://www.alora-soluciones.es/cuales-son-las-ventajas-de-los-radioenlaces-punto-a-punto/#:%7E:text=Los%20radioenlaces%20ofrecen%20varias%20ventajas,la%20localizaci%C3%B3n%20de%20los%20transceptores.

[31] *Eurona - Internet SatÃ©lite con Datos Ilimitados*. (s. f.). Eurona. [22 de marzo de 2022] https://eurona.es/internet-satelite

[32] Ubierna, O. (2021, 14 julio). *Las bandas libres de frecuencias*. Blog de tecnología wireless. [22 de marzo de 2022] https://www.comunicacionesinalambricashoy.com/wireless/las-bandas-libres-de-frecuencias/

[33] *Ubiquiti | Operator | airFiber PtP Wireless Bridging*. (s. f.). Ubiquiti. [Consultado el 25 de marzo de 2022] https://www.ui.com/uisp/ptp-bridging

[34] *Enlace WiFi Punto A Punto - Serie LigoPTP*. (s. f.). Ligowave. [Consultado el 26 de marzo de 2022] https://www.ligowave.com/es/products-2/ligo-ptp-series-2

[35] *MikroTik*. (s. f.). Mikrotik [Consultado el 26 de marzo de 2022]. https://mikrotik.com/products/group/wireless-systems

[36] *Log in - LigoWave LinkCalc*. (s. f.). LinkCalc Web. [Consultado el 27 de marzo de 2022] https://linkcalc.ligowave.com/Account/login

[37] L.W. (s. f.). *LigoPTP 5-N/ 5–23 RapidFire*. Wni.mx. [Consultado el 27 de marzo de 2022]https://www.wni.mx/images/stories/media/ligowave/pdfs/RAPIDFIRE-5-Series_DS.pdf

[38] *LigoPTP RapidFire 6*. (s. f.). Ligowave.com. [Consultado el 27 de marzo de 2022] https://www.ligowave.com/es/products-2/rapidfire-6

[39] *LigoDLB 2–14n 2.4GHz | IP-66 | router de exterior*. (s. f.). Ligowave. [Consultado el 29 de marzo de 2022] https://www.ligowave.com/es/products-2/dlb-2-14n-3

[40] *MikroTik*. (s. f.). Mikrotik.[Consultado el 29 de marzo de 2022] https://mikrotik.com/product/RBDynaDishG-5HacDr3#fndtn-specifications

[41] *MikroTik*. (s. f.). Mikrotik.[Consultado el 29 de marzo de 2022] https://mikrotik.com/product/rbdisc_5nd#fndtn-specifications

[42] *airFiber 60 LR*. (s. f.). Ubiquiti Inc. [Consultado el 30 de marzo de 2022] https://store.ui.com/collections/operator-airfiber/products/airfiber-60-lr

[43] *Microchip PIC18F26K22*. (s. f.). Microchip.com. [Consultado el 6 de abril de 2022] https://www.microchip.com/en-us/product/PIC18F26K22

[44] colaboradores de Wikipedia. (s.f). *MAX232*. Wikipedia, la enciclopedia libre. [Consultado el 13 de abril] https://es.wikipedia.org/wiki/MAX232#:%7E:text=El%20MAX232%20es%20un%20circuito,niveles%20TTL%20de%20circuitos%20l%C3%B3gicos.

[45] *Detector de barrera por infrarrojos | ABH-150L*. (s. f.). [Consultado el 17 de abril] Visiotechsecurity. https://www.visiotechsecurity.com/es/productos/intrusion/barreras-infrarrojas/abh-150l-detail#tab=prod_0

[46] *Detector PIR Optex cableado de grado 3, 15x15 m, 85º y anti mascotas*. (s. f.). [Consultado el 19 de abril] Tienda de electrónica online - TODOELECTRONICA. https://www.todoelectronica.com/detector-pir-optex-cableado-de-grado-3-15x15-m-85-y-anti-mascotas-p-115335.html

[47] *Contacto magnético de superficie para alarmas cableadas (grado 3)*. (s. f.). [Consultado el 19 de abril] Tienda de electrónica online - TODOELECTRONICA. https://www.todoelectronica.com/contacto-magnetico-de-superficie-para-alarmas-cableadas-grado-3-p-90674.html

[48] *Receptor CLEMSA RV42 MASTERcode 12–24V- 230Vac DC-CA Exterior*. (s. f.). [Consultado el 19 de abril] AUTOMATISMOS W2B.

https://www.webdosb.com/mandos-y-receptores/2383-receptor-clemsa-rv42-mastercode-12-24v-230vac-dc-ca-exterior-.html

[49] *Módulo Ethernet ENC28J60*. (s. f.). Naylamp Mechatronics - Perú. [Consultado el 25 de abril de 2022] https://naylampmechatronics.com/alambrico/87-modulo-ethernet-enc28j60.html

[50] H, S. (2019, 24 diciembre). *RS-232 to Ethernet Converter | One Of The Leading Manufacturer*. Ambetronics Engineers Pvt Ltd. [Consultado el 27 de abril de 2022] https://ambetronics.com/rs-232_to_ethernet_converter/

15. Anexos

15.1. Configuración de las antenas DynaDish 5 de Mikrotik

A continuación, se muestra una configuración real que realicé de unos equipos DynaDish 5 para que puedan transmitir y recibir:

Para programar las antenas del radioenlace para que funcionen en modo emisión y recepción, será necesario realizarlo a través de un ordenador, pero como cada dispositivo tiene su propia IP, será necesario que cambiemos la IP de nuestro ordenador a una dirección que se encuentre en la misma red que las antenas que vamos a configurar:

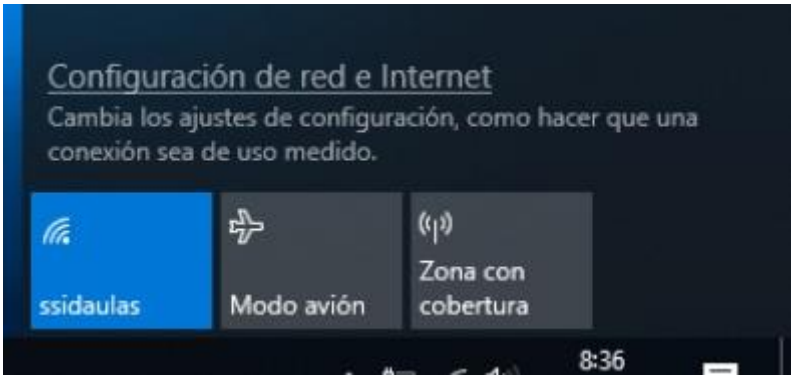


Ilustración 57: Configuración de red e Internet

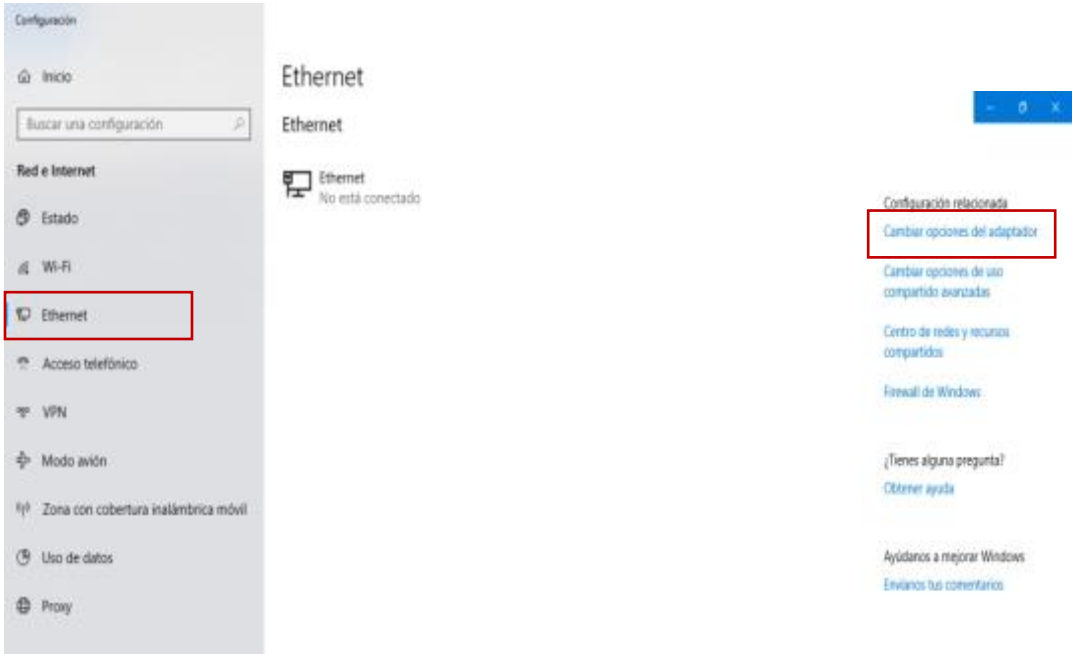


Ilustración 58: Ethernet -> Cambiar opciones del adaptador

Procedemos a seleccionar la conexión Ethernet:

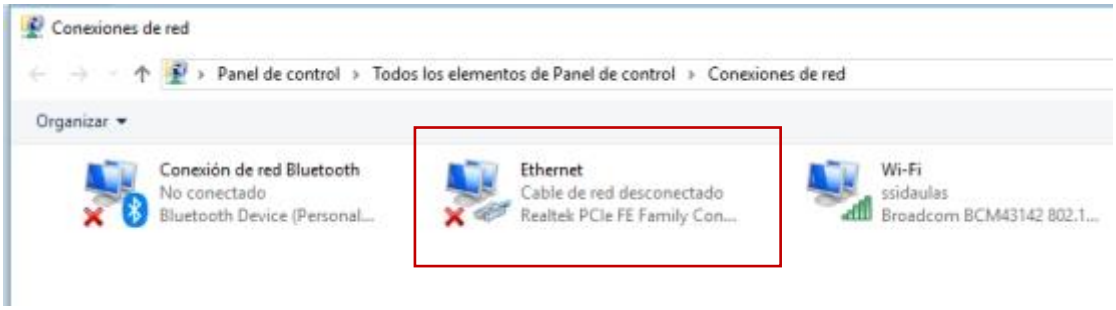


Ilustración 59: Seleccionamos Ethernet

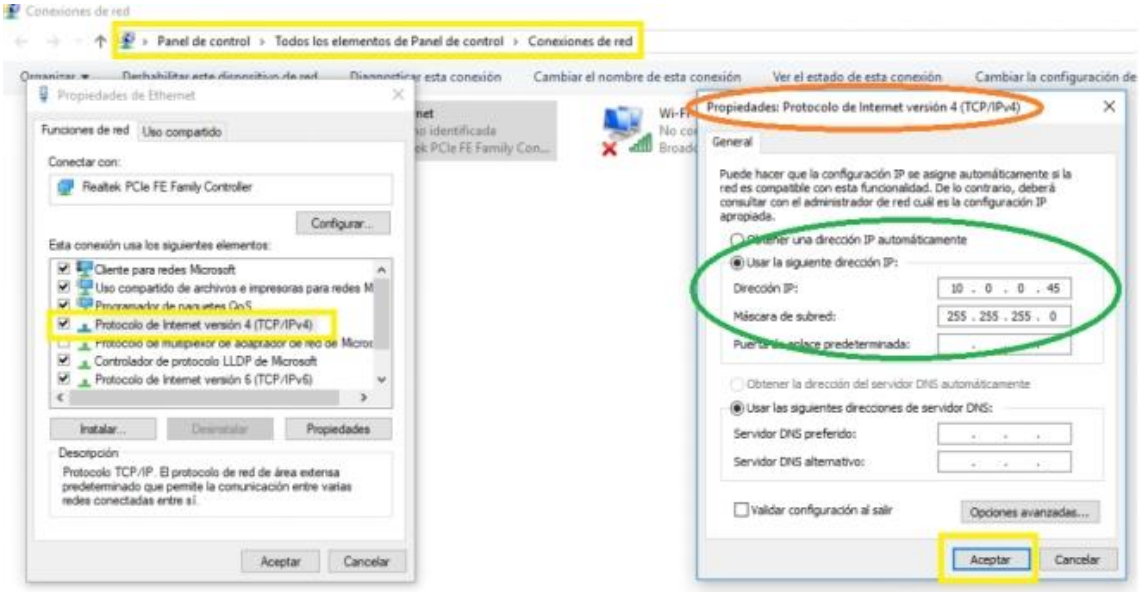


Ilustración 60: Cambiamos el rango IP del PC

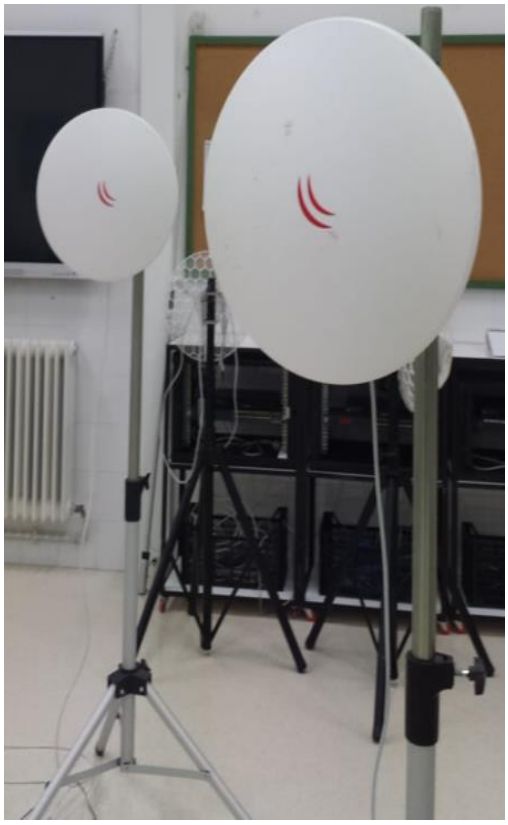


Ilustración 61: Antena Tx y Antena Rx DynaDish 5

Ilustración 62: Dirección IP Rx

Ilustración 63: Dirección IP Tx

Las antenas tienen las direcciones:

-Antena 1: 10.0.0.41
-Antena 2: 10.0.0.42

Se pueden asignar si es Tx o Rx en su configuración
- BRIDGE (EMISORA)
- STATION BRIDGE (RECEPTORA)

Como vemos, hemos asignado la dirección 10.0.0.45 a nuestro ordenador, porque así se encontrará dentro de la misma red que las antenas, siendo la dirección de red 10.0.0.0 y la máscara de subred 255.255.255.0

Para poder configurar la antena transmisora, será necesario conectar al ordenador el adaptador de Ethernet y la alimentación que venía con la antena. Después de este paso, entramos a cualquier navegador, preferiblemente Firefox, ahí introduciremos la dirección de la antena, en este caso, la **dirección de la antena Tx es 10.0.0.42**

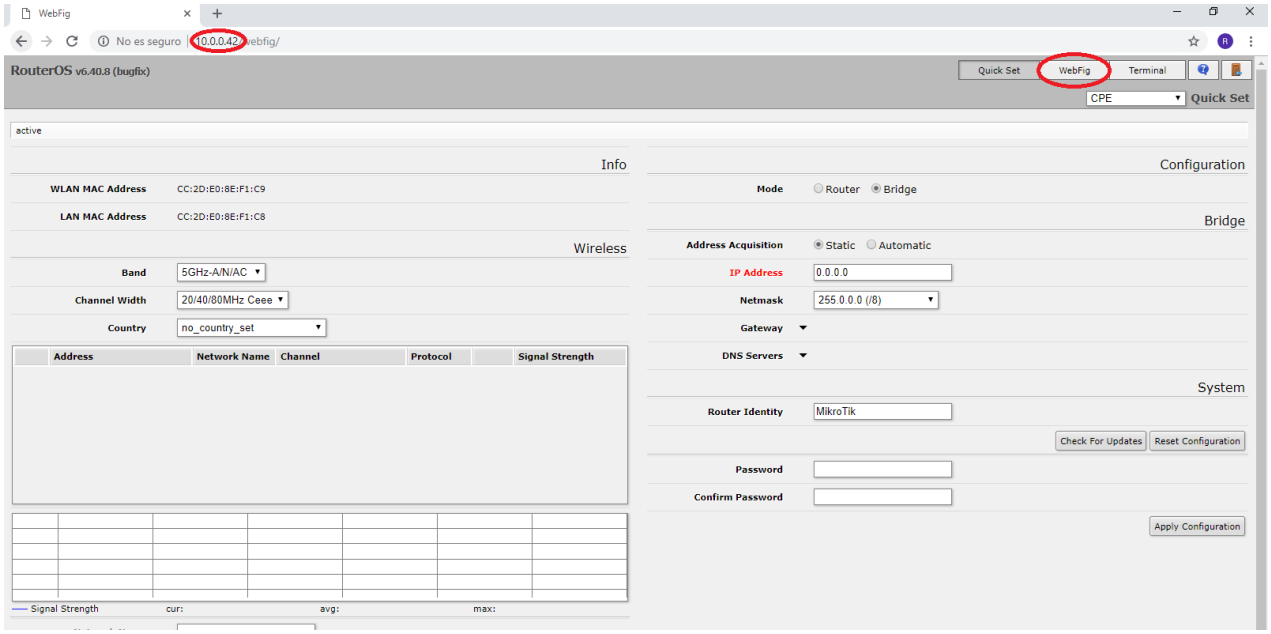


Ilustración 64: Menú principal Antena Tx

En el margen superior derecho encontraremos el apartado Webfig, ingresamos, y nos aparecerá el siguiente menú:

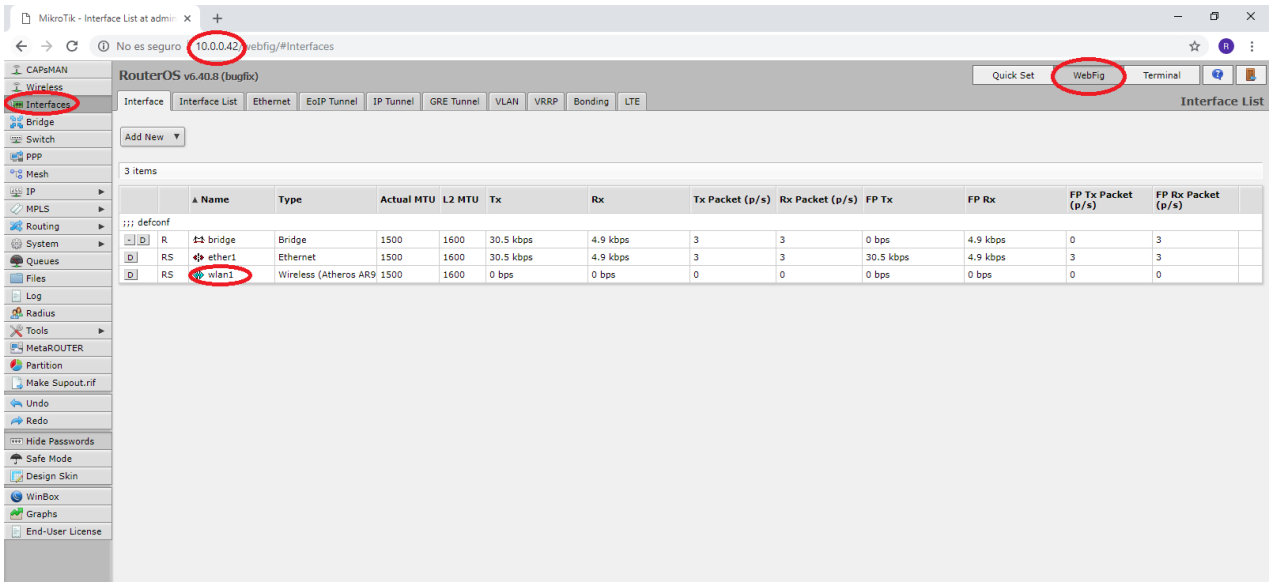


Ilustración 65: Menú Webfig de antena Tx

Será necesario que seleccionemos “wlan1”, para conseguir acceder al siguiente submenú:

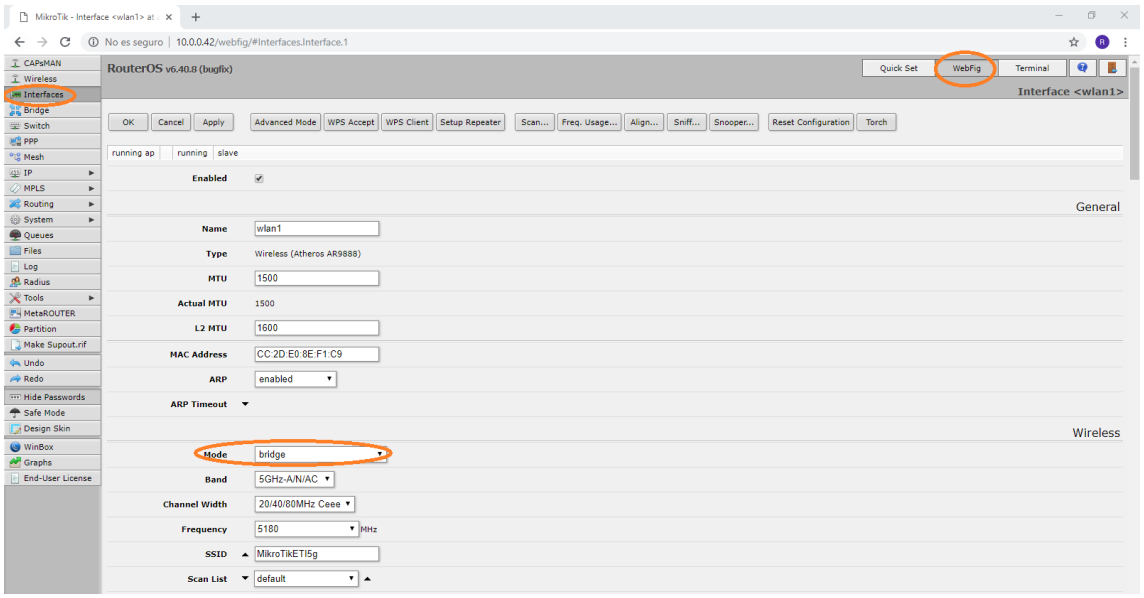


Ilustración 66: Submenú wlan1

Como hemos mencionado anteriormente, para asignarla como EMISORA, debemos configurar su “MODE” como BRIGDE.

Podemos cambiar la SSID(nombre de identificación del dispositivo), aunque esto no es un paso obligatorio. También es importante dejar seleccionadas las bandas en las que trabaja, en este caso dejamos seleccionadas 5GHZ-A/N/AC.

Otro parámetro que debemos cambiar es “Security profile” en nuestro caso tiene asignado el nombre DEFAULT.

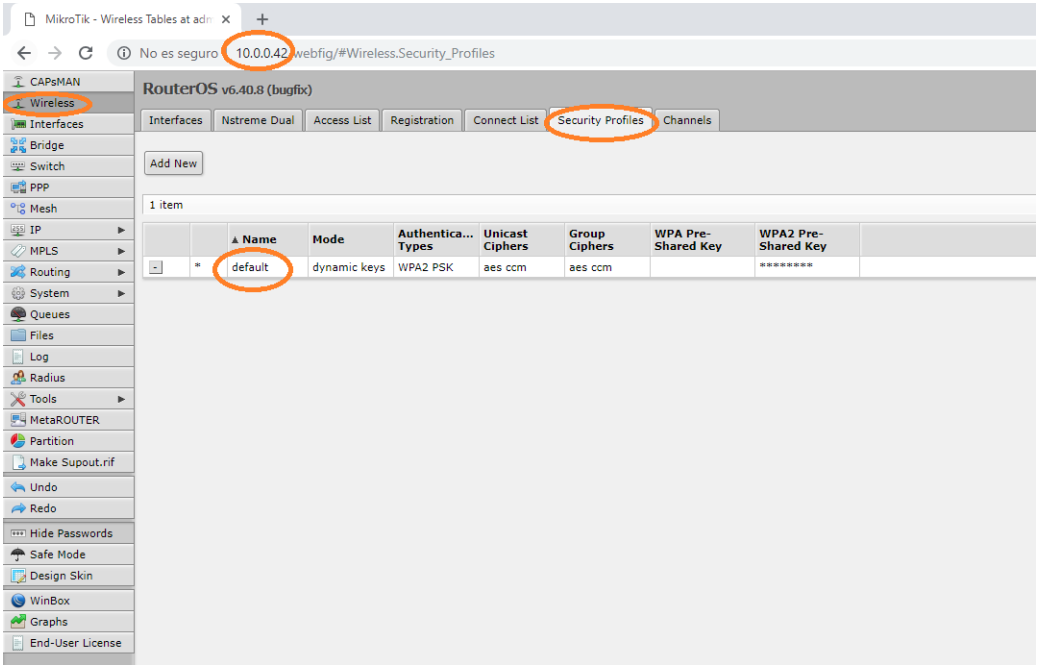


Ilustración 67: Security Profiles

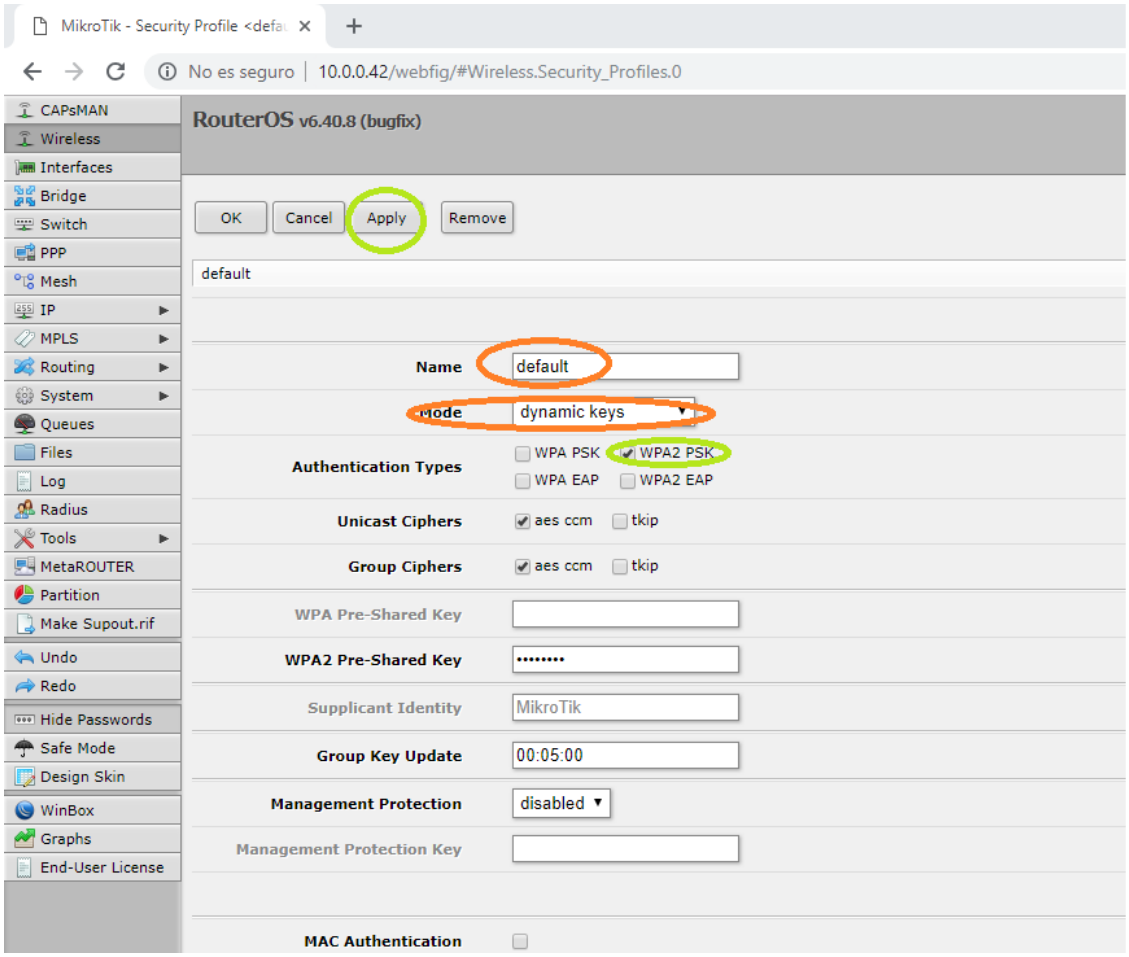


Ilustración 68: Configuraciones realizadas dentro de Security Profile

Para que el radioenlace funcione correctamente será necesario enlazar los puertos de Ethernet y Wlan, para ello tendremos que ir al apartado Brigde, ahí seleccionar el subapartado Ports, y seleccionar “Add new”

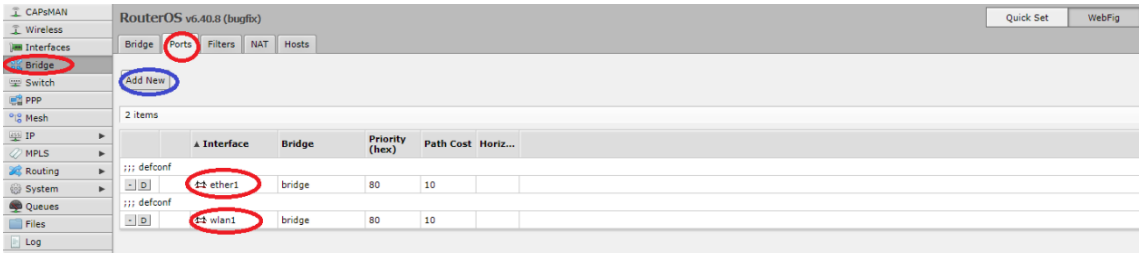


Ilustración 69: Vinculación de los puertos con las interfaces

Lo que nos aparecerá después de darle a “Add new” será lo siguiente:

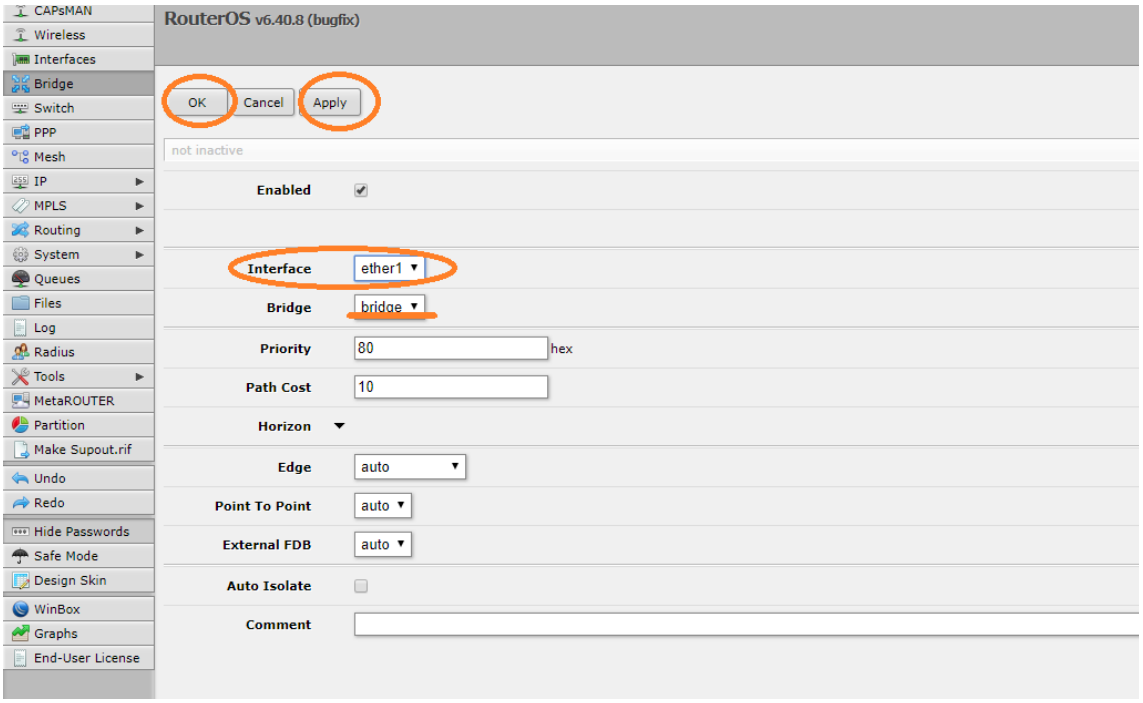


Ilustración 70: Vinculación puerto ether1

Es muy importante que este paso lo realicemos 2 veces, porque en una de las veces tendremos que asignar la interfaz ether1, y en la segunda vez, asignar la interfaz wlan1.

Cuando hayamos terminado estos pasos, la antena transmisora ya estará configurada, por lo que procederemos a configurar la antena receptora. Para ello, debemos conectar la antena receptora al ordenador por medio del adaptador de alimentación y ethernet.

Volveremos a escribir en la barra de direcciones la dirección de la antena, pero en este caso, será 10.0.0.41, pues es la dirección que hemos asignado a la antena receptora.

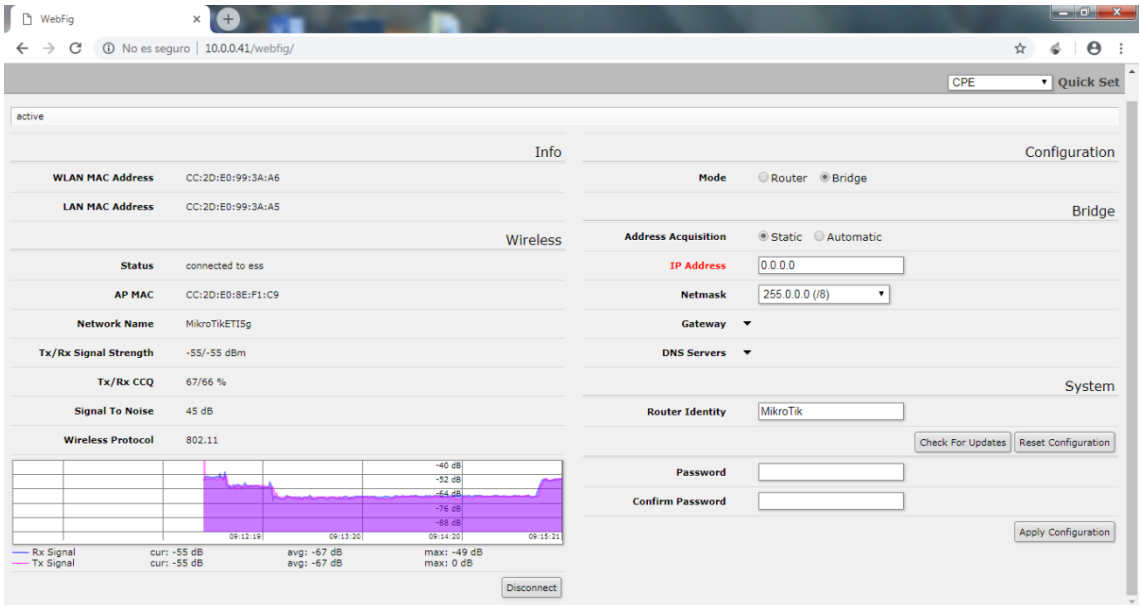


Ilustración 71: Menú antena Rx

Como esta es la antena receptora, deberemos configurarla como "Station bridge", al igual que en la anterior, podemos cambiar el SSID del dispositivo.

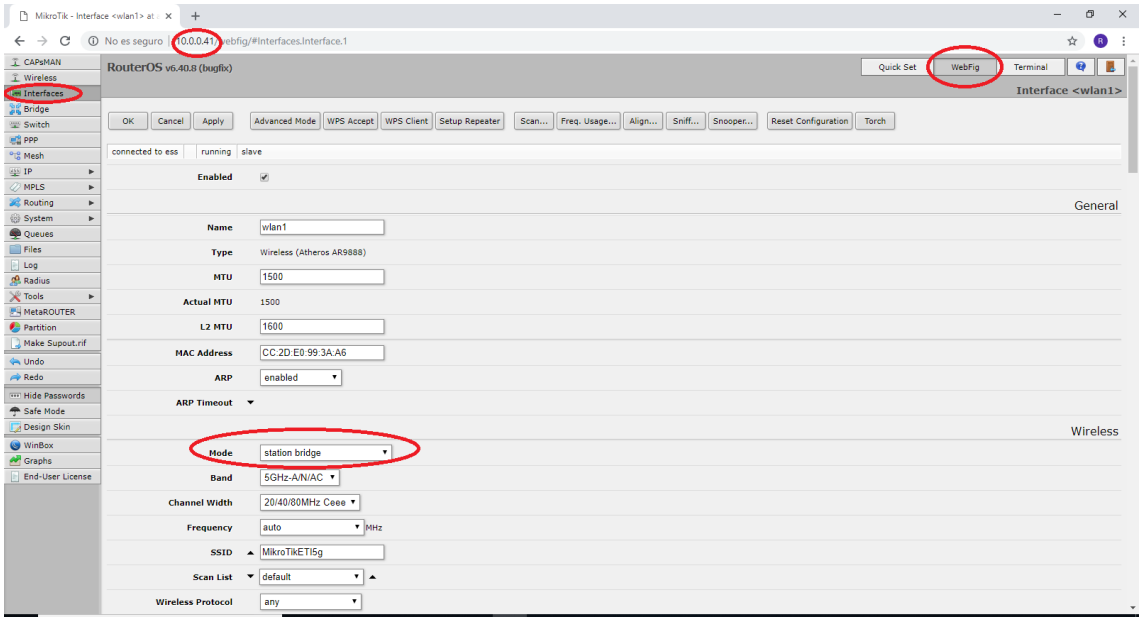


Ilustración 72: Menú webfig antena Rx

También es importante que realicemos las mismas modificaciones que hicimos con la antena emisora en el apartado "Security profile"

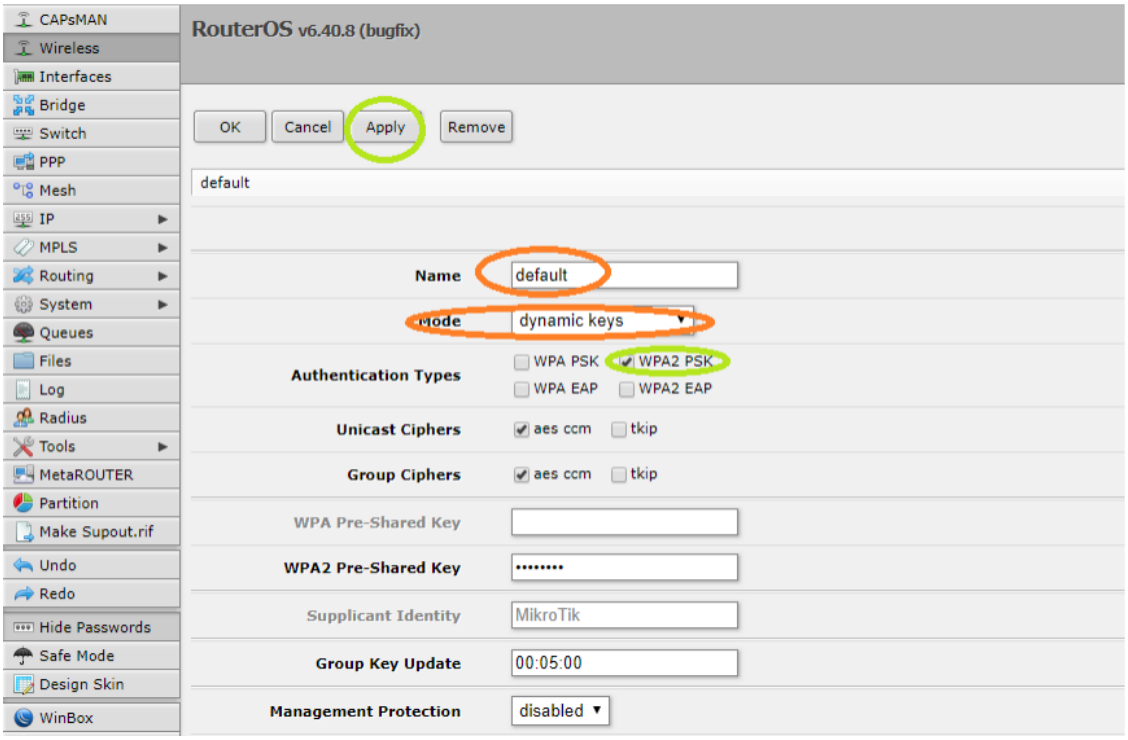
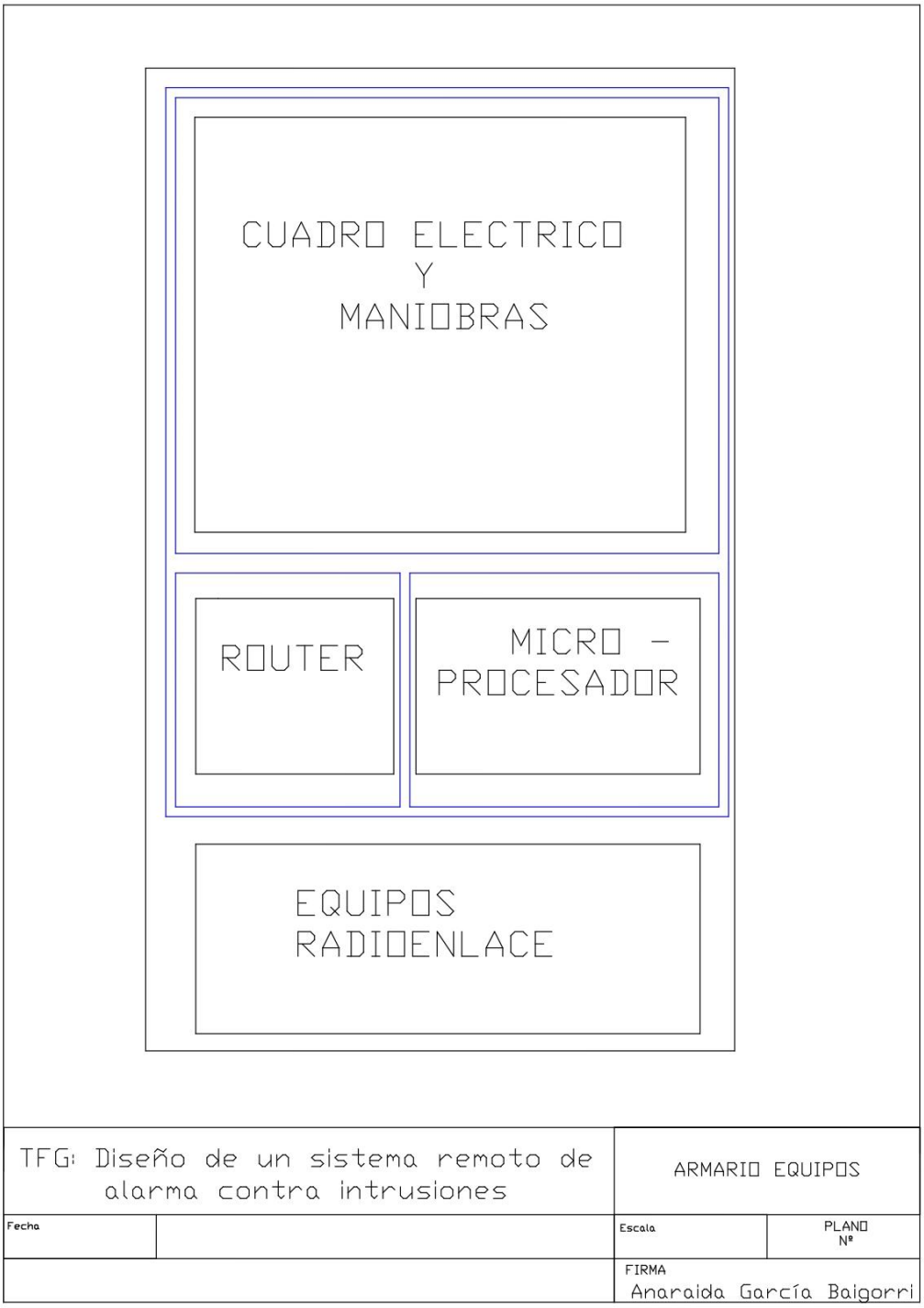


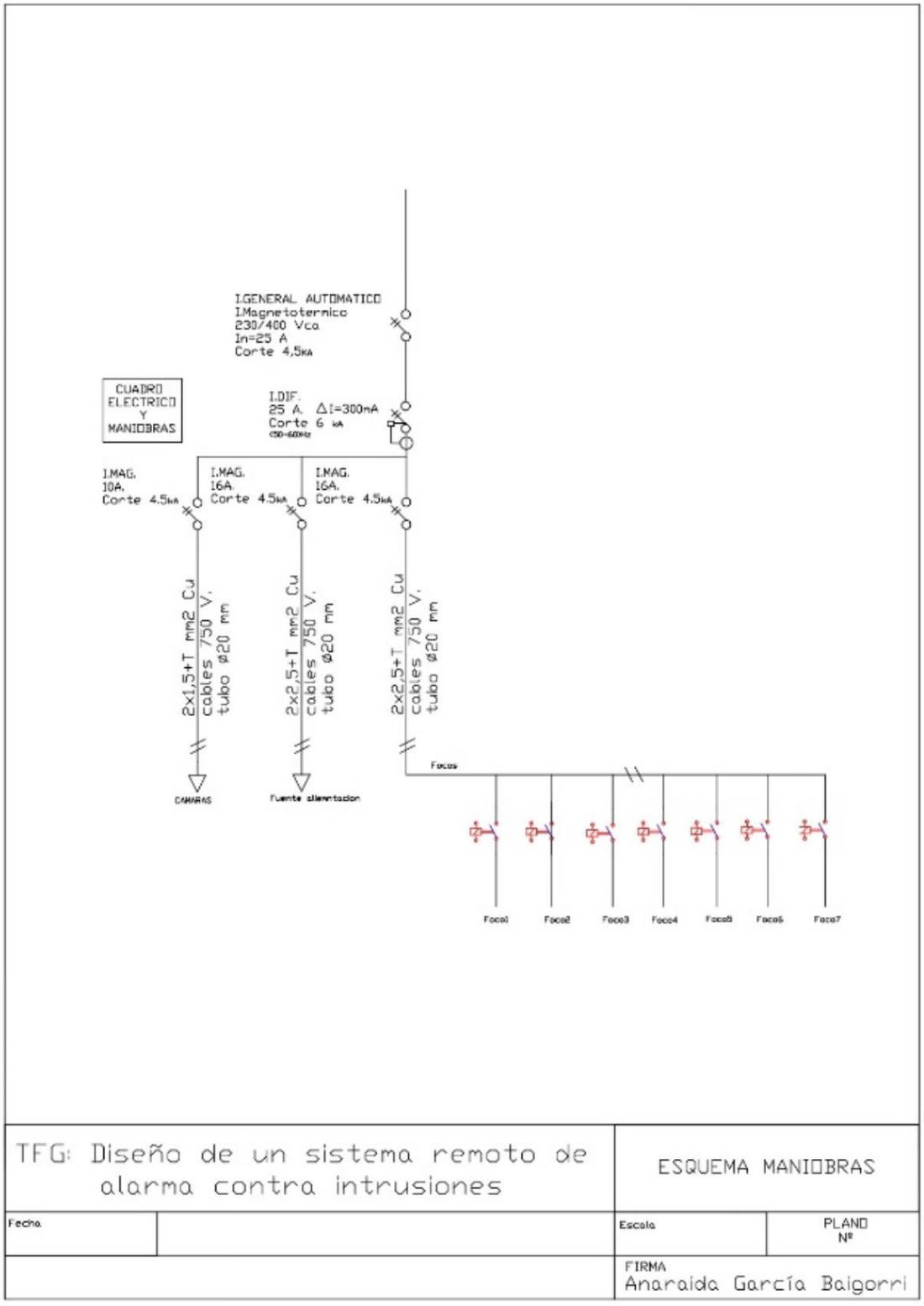
Ilustración 73: Configuración antena Rx en Security Profile

Y enlazamos de nuevo los puertos con la antena receptora, importante, es necesario realizar este paso dos veces, una para la interfaz ether1 y otra para la interfaz wlan1. Después de este último paso, las antenas ya estarán configuradas, por lo que se podrán utilizar para transmitir y recibir.

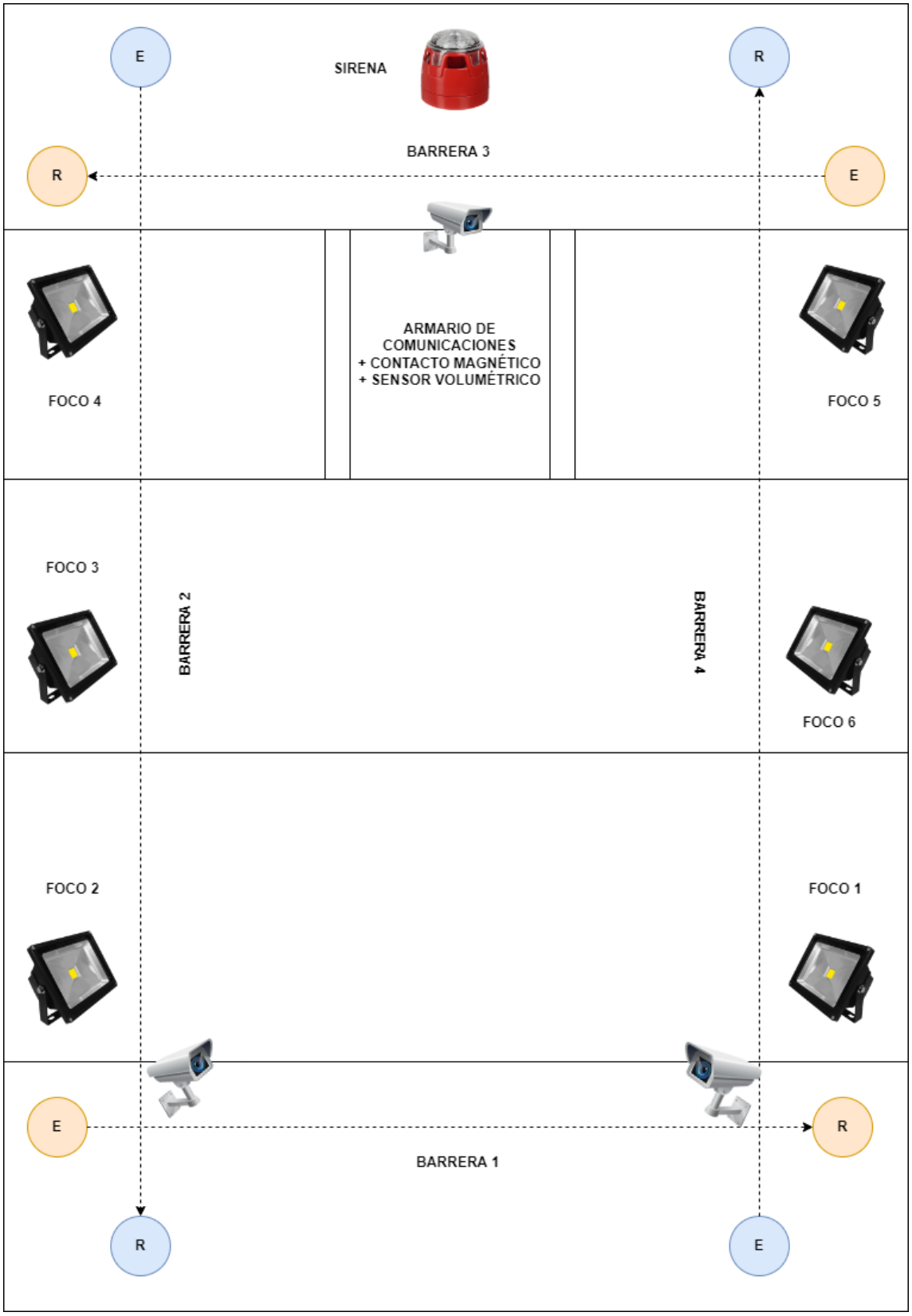
15.2. Esquema del armario de comunicaciones



15.3. Esquema del cuadro de maniobras



15.4. Disposición de los elementos en el recinto



15.5. Código de implementación en MPLAB

15.5.1. Código de main.c

```
#include "mcc_generated_files/mcc.h"
#include "main.h"

/*
                         Main application
 */
void main(void) {
    // Initialize the device
    SYSTEM_Initialize();

    // If using interrupts in PIC18 High/Low Priority Mode you need to enable the Global High and Low Interrupts
    // If using interrupts in PIC Mid-Range Compatibility Mode you need to enable the Global and Peripheral Interrupts
    // Use the following macros to:

    // Enable the Global Interrupts
    //INTERRUPT_GlobalInterruptEnable();

    // Disable the Global Interrupts
    //INTERRUPT_GlobalInterruptDisable();

    // Enable the Peripheral Interrupts
    //INTERRUPT_PeripheralInterruptEnable();

    // Disable the Peripheral Interrupts
    //INTERRUPT_PeripheralInterruptDisable();

    REL1_APAGADO;
    REL2_APAGADO;
    REL3_APAGADO;
    REL4_APAGADO;
    REL5_APAGADO;
    REL6_APAGADO;
    REL7_APAGADO;
    tmp1 = 0;
    while (1) {
        // Add your application code

        if (IO_RC0_GetValue() == 1 && alarma_activada == 0) {
            alarma_activada = 1;
            memoria_estado = 1;
        } else if (IO_RC0_GetValue() == 0) memoria_estado = 0;
        else if (IO_RC0_GetValue() == 1 && alarma_activada == 1 && memoria_estado == 0) alarma_activada = 0;

        __delay_ms(1000);
        if (alarma_activada == 1) {
            if (tmp1 >= 30) tmp1 = 0;
            tmp1 = tmp1 + 1;
            analogicol = ADC_GetConversion(14);

            if (analogicol > (15000) && analogicol < (30000)) {
                tiempo_alarma = 60;
                REL1_ENCENDIDO;
                REL2_ENCENDIDO;
                REL3_ENCENDIDO;
                REL4_ENCENDIDO;
                REL5_ENCENDIDO;
                REL7_ENCENDIDO;
                EUSART1_Write('A');
            } else if (analogicol < 10000) {
                EUSART1_Write('S');
            } else if (tiempo_alarma > 0) {
                --tiempo_alarma;
                REL1_ENCENDIDO;
                REL2_ENCENDIDO;
                REL3_ENCENDIDO;
                REL4_ENCENDIDO;
                REL5_ENCENDIDO;
                REL7_ENCENDIDO;
            } else {
                REL1_APAGADO;
                REL2_APAGADO;
                REL3_APAGADO;
                REL4_APAGADO;
                REL5_APAGADO;
                REL7_APAGADO;
                if (tmp1 >= 30) EUSART1_Write('*');
            }
            analogicol = ADC_GetConversion(0);

```

```
123             if (analogicol > (15000) && analogicol < (30000)) {
124                 tiempo_alarma = 60;
125                 REL1_ENCENDIDO;
126                 REL2_ENCENDIDO;
127                 REL7_ENCENDIDO;
128                 EUSART1_Write('A');
129             } else if (analogicol < 10000) {
130                 EUSART1_Write('S');
131             }  else if (tiempo_alarma > 0) {
132                 --tiempo_alarma;
133                 REL1_ENCENDIDO;
134                 REL2_ENCENDIDO;
135                 REL7_ENCENDIDO;
136             } else {
137                 REL1_APAGADO;
138                 REL2_APAGADO;
139                 REL7_APAGADO;
140                if (tmp1 >= 30) EUSART1_Write('*');
141             }
142             analogicol = ADC_GetConversion(1);
143 
144             if (analogicol > (15000) && analogicol < (30000)) {
145                 tiempo_alarma = 60;
146                 REL2_ENCENDIDO;
147                 REL3_ENCENDIDO;
148                 REL4_ENCENDIDO;
149                 REL7_ENCENDIDO;
150                 EUSART1_Write('A');
151             } else if (analogicol < 10000) {
152                 EUSART1_Write('S');
153             } else if (tiempo_alarma > 0) {
154                 --tiempo_alarma;
155                 REL2_ENCENDIDO;
156                 REL3_ENCENDIDO;
157                 REL4_ENCENDIDO;
158                 REL7_ENCENDIDO;
159             }  else {
160                 REL2_APAGADO;
161                 REL3_APAGADO;
162                 REL4_APAGADO;
163                 REL7_APAGADO;
164                 if (tmp1 >= 30) EUSART1_Write('*');
165             }
167 
168             if (analogicol > (15000) && analogicol < (30000)) {
169                 tiempo_alarma = 60;
170                 REL4_ENCENDIDO;
171                 REL5_ENCENDIDO;
172                 REL7_ENCENDIDO;
173                 EUSART1_Write('A');
174             } else if (analogicol < 10000) {
175                 EUSART1_Write('S');
176             } else if (tiempo_alarma > 0) {
177                 --tiempo_alarma;
178                 REL4_ENCENDIDO;
179                 REL5_ENCENDIDO;
180                 REL7_ENCENDIDO;
181             } else {
182                 REL4_APAGADO;
183                 REL5_APAGADO;
184                 REL7_APAGADO;
185                 if (tmp1 >= 30) EUSART1_Write('*');
186             }
187             analogicol = ADC_GetConversion(3);
188 
189             if (analogicol > (15000) && analogicol < (30000)) {
190                 tiempo_alarma = 60;
191                 REL1_ENCENDIDO;
192                 REL5_ENCENDIDO;
193                 REL6_ENCENDIDO;
194                 REL7_ENCENDIDO;
195                 EUSART1_Write('A');
196             } else if (analogicol < 10000) {
197                 EUSART1_Write('S');
198             } else if (tiempo_alarma > 0) {
199                 --tiempo_alarma;
200                 REL1_ENCENDIDO;
201                 REL5_ENCENDIDO;
202                 REL6_ENCENDIDO;
203                 REL7_ENCENDIDO;
```

```
            } else {
                REL1_APAGADO;
                REL5_APAGADO;
                REL6_APAGADO;
                REL7_APAGADO;
                if (tmp1 >= 30) EUSART1_Write('*');
            }
            analogico1 = ADC_GetConversion(4);

            if (analogico1 > (15000) && analogico1 < (30000)) {
                tiempo_alarma = 60;
                REL1_ENCENDIDO;
                REL2_ENCENDIDO;
                REL7_ENCENDIDO;
                EUSART1_Write('A');
            } else if (analogico1 < 10000) {
                EUSART1_Write('S');
            } else if (tiempo_alarma > 0) {
                --tiempo_alarma;
                REL1_ENCENDIDO;
                REL2_ENCENDIDO;
                REL7_ENCENDIDO;
            } else {
                REL1_APAGADO;
                REL2_APAGADO;
                REL7_APAGADO;
                if (tmp1 >= 30) EUSART1_Write('*');
            }

        }
    }
}
/**
 End of File
 */
```

15.5.2. Código de main.h

```
// This is a guard condition so that contents of this file are not included
// more than once.
#ifndef MAIN_H
#define MAIN_H

#include "mcc_generated_files/pin_manager.h"


#define REL1_APAGADO        IO_RB0_SetLow()
#define REL1_ENCENDIDO      IO_RB0_SetHigh()
#define REL2_APAGADO        IO_RB1_SetLow()
#define REL2_ENCENDIDO      IO_RB1_SetHigh()
#define REL3_APAGADO        IO_RB2_SetLow()
#define REL3_ENCENDIDO      IO_RB2_SetHigh()
#define REL4_APAGADO        IO_RB3_SetLow()
#define REL4_ENCENDIDO      IO_RB3_SetHigh()
#define REL5_APAGADO        IO_RB4_SetLow()
#define REL5_ENCENDIDO      IO_RB4_SetHigh()
#define REL6_APAGADO        IO_RB5_SetLow()
#define REL6_ENCENDIDO      IO_RB5_SetHigh()
#define REL7_APAGADO        IO_RB6_SetLow()
#define REL7_ENCENDIDO      IO_RB6_SetHigh()


// variables

unsigned int analogico1=0, tmp1, tmp2, tiempo_alarma, alarma_activada, memoria_estado; //0-65535


#endif  /* XC_HEADER_TEMPLATE_H */

```

15.6 Código de implementación Arduino

```
#include <EtherCard.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>

static byte mymac[] = {0xDD,0xDD,0xDD,0x00,0x01,0x05};
static byte myip[] = {192,168,1,177}; // es la IP del radioenlace
byte Ethernet::buffer[700];

//Creamos el objeto lcd con la dirección 0x3F, 16 columnas y 2 filas
LiquidCrystal_I2C lcd(0x3F,16,2);

void setup () {

  Serial.begin(9600);
  Serial.println("Test del Modulo  ENC28J60");

  if (!ether.begin(sizeof Ethernet::buffer, mymac, 10))
    Serial.println( "No se ha podido acceder a la controlador Ethernet");
  else
   Serial.println("Controlador Ethernet inicializado");

  if (!ether.staticSetup(myip))
    Serial.println("No se pudo establecer la dirección IP");

  Serial.println("Inicializamos la pantalla LCD");
  lcd.init();
  lcd.backlight();
  lcd.setCursor(0, 0);
}

void loop() {

  word len = ether.packetReceive();
  word pos = ether.packetLoop(len);

  if(pos) {

    if(strstr((char *)Ethernet::buffer + pos, "*") != 0) {
      Serial.println("Mensaje reposo recibido");
      lcd.setCursor(3, 0);
      lcd.print("Reposo (*)  ");
    } else if (strstr((char *)Ethernet::buffer + pos, "A") != 0) {
      Serial.println("Mensaje alarma recibido");
      lcd.setCursor(3, 0);
      lcd.print("Alarma (A)  ");
    } else if (strstr((char *)Ethernet::buffer + pos, "S") != 0) {
      Serial.println("Mensaje sabotaje recibido");
      lcd.setCursor(3, 0);
      lcd.print("Sabotaje (S)");
    }
  }
}
```

15.7. Esquema de conexiones del sistema