PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD INALÁMBRICO CON TECNOLOGÍA BLUETOOTH PARA VIVIENDAS

Tesis para optar el Título de Ingeniero electrónico**,** que presenta el bachiller:

Fernando Wilfredo Ramírez Marocho

ASESOR: Dr. Manuel Augusto Yarlequé Medina

Lima, Noviembre del 2012

RESUMEN

El incremento cuantitativo y cualitativo de la inseguridad y violencia en el Perú, expresada en diferentes formas y resaltando la que tiene un mayor índice de repetitividad, el hurto y robo a las viviendas, ha hecho que la población se encuentre en la búsqueda permanente de medios para protegerse de estas amenazas. Ante esta situación, la presente tesis busca una solución para resguardar el patrimonio de las personas y brindar seguridad a los inmuebles, es por ello que esta tesis lleva como título **"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD INALÁMBRICO CON TECNOLOGÌA BLUETOOTH PARA VIVIENDAS"**.

En el primer capítulo, se detalla la problemática y las tecnologías de seguridad existentes en el medio, las cuales ofrecen diferentes acciones para enfrentar y solucionar el problema de la inseguridad de los inmuebles.

En el segundo capítulo, se describe el lugar donde será instalado el sistema de seguridad y se evalúa las vulnerabilidades del inmueble. Asimismo, se presenta los requerimientos del sistema para realizar el diseño.

En el tercer capítulo, luego de realizar una evaluación y análisis de la mejor opción, se procede con la descripción del diseño e implementación del sistema de seguridad, en donde se detalla las partes y elementos utilizados.

En el cuarto capítulo, se presenta los resultados de las pruebas realizadas, demostrándose la rentabilidad y confiabilidad del sistema

ÍNDICE

INTRODUCCIÓN

A lo largo de la historia, el hombre siempre ha mostrado la necesidad de obtener seguridad para su integridad física y sus pertenencias, en cuyo objetivo buscó medios y recursos para protegerse de las amenazas de toda índole; inventando y construyendo sistemas de seguridad, desde lo más simple hasta lograr infraestructuras portentosas como las edificaciones de fortalezas, que hasta la fecha se mantienen a pesar del tiempo transcurrido.

En los últimos años, el Perú, sobre todo la ciudad de Lima, se caracterizó por ser una ciudad insegura, debido al incremento de los actos ilícitos contra las personas y del patrimonio. Los hurtos y robos a las viviendas denotan un aumento sustancial, por lo que existe un compromiso moral y ético de las autoridades y profesionales de las diferentes ramas para buscar soluciones en los diversos campos de la actividad humana.

Actualmente, vivimos en una sociedad donde la tecnología es un factor muy importante para las personas. La automatización, es un área de la ingeniería que nos brinda la reducción del esfuerzo humano en los diferentes procesos que se necesita; dentro de esta disciplina se observa a la **domótica,** que es básicamente la automatización de los diferentes servicios; ésta aplicada a las viviendas, permitirá implementar diversos sistemas de seguridad confiable sin la presencia física de personas.

Como una forma de contribuir con la sociedad peruana, se ha enfocado la presente tesis en diseñar e implementar un sistema de seguridad inalámbrico para proteger las viviendas contra hurtos y robos. Este sistema podrá ser integrado a futuras tecnologías u otros inventos que contribuyan a la eficiencia para la seguridad total.

CAPÍTULO 1

TECNOLOGÍAS DE SEGURIDAD

1.1. Seguridad

La seguridad consiste en los procedimientos y acciones preventivas que permitan proteger la integridad física de las personas y de sus patrimonios, de amenazas externas que pongan en riesgo su bienestar y el derecho de propiedad.

Actualmente, Lima se ha caracterizado por ser una ciudad violenta e insegura, debido al incremento cuantitativo y cualitativo de los actos ilícitos que afectan a la población en forma general, hechos que se pueden apreciar en las diferentes modalidades como: secuestros, pandillaje, hurto y robo en las calles y viviendas.

Luego de realizar un estudio analítico, sobre la crisis de la seguridad ciudadana; el hurto y robo a las viviendas se encuentra entre los ilícitos más preocupantes para la sociedad, presentando cada vez más un aumento sustancial alarmante. Ante esta situación se orienta este proyecto en la búsqueda de una solución que permita proteger y resguardar el patrimonio de las personas.

1.2 Sistemas de seguridad

Existe una variedad de sistemas de seguridad, desde los más simples que serían los mecánicos, hasta los electrónicos con base y componentes cada vez más complejos.

Un sistema de seguridad electrónico está constituido por un conjunto de elementos electrónicos y de su instalación, que proporcionan a las personas y a su patrimonio protección frente a las agresiones externas, como son: hurtos, robos, sabotajes, incendios, daños materiales por terceros, entre otros. Durante un incidente, el sistema primero lo detectará, luego lo señalizará y finalmente realizará acciones para reducir o eliminar estos actos.

Los sistemas electrónicos de seguridad, según su aplicación, se clasifican en cuatro grupos [1]:

Un sistema de seguridad, está compuesto básicamente por: una unidad de control, sensores y un sistema de aviso o señalización.

1.2.1. Sistemas de control de acceso

Los sistemas de control de acceso se encargan de administrar y supervisar el ingreso de personas a áreas restringidas y evita que personas no autorizadas o indeseables tengan la libertad de acceder a estas zonas. Este sistema de control es mayormente utilizado en empresas, a través del cual se puede tener conocimiento de la asistencia del personal, horarios de ingreso y egreso, además tener un historial de entradas de personas a todas las áreas. Las características más resaltantes de este sistema son: la facilidad de su uso, los empleados lo pueden usar varias veces por día, la identificación por un número asignado (PIN), es el medio más común para autorizar a los empleados el acceso a una determinada área entre otras. [2]

Existe una variedad de sistemas de control de acceso. Entre los más resaltantes podemos mencionar:

1.2.1.1. Control de acceso por teclado

Son sistemas que consisten en digitalizar la clave en un teclado matricial, el cual está conectado con un procesador que verifica la autenticidad de la clave y permite la activación de algún dispositivo, como la apertura de una puerta para el ingreso o egreso. En la Fig.1.1 se muestra una imagen del teclado matricial. [2]

Fig. 1.1 Teclado matricial [3]

1.2.1.2. Control de acceso por sensor biométrico

Estos sistemas son los más utilizados en la actualidad. La tecnología la biométrica autentifica y determina la identidad del individuo utilizando sus características físicas y biológicas para evitar fraudes y restricciones en las entradas y salidas de una edificación. [2]

Los detectores biométricos más usados son: sensor biométrico de huella, sensor biométrico de iris, sensor biométrico de rostro y sensor biométrico de mano.

1.2.1.3. Control de acceso por código de barras

Este control se basa en la identificación de un código de barras para el ingreso de las personas al ambiente que está permitido. La autentificación de personas por el código se basa en conceptos físicos de absorción y reflexión de luz. Este sistema posee un lector que escanea el código de barras a través de un láser, luego decodifica la información con la digitalización de una fuente de luz visible o infrarroja reflejada en tal código, y finalmente es enviada a un procesador para la interpretación, es decir para lo comparación con su base de datos y permitir el acceso. [2]

1.2.2. Sistemas de Circuito Cerrado de Televisión (CCTV)

El circuito cerrado de televisión (CCTV) es una tecnología de video vigilancia visual diseñada para supervisar y controlar una diversidad de ambientes y actividades. El circuito está conformado básicamente por una o más cámaras de vigilancia conectadas a uno o más monitores de video, éstas pueden ser conectadas directamente entre sí o pueden ser enlazadas por red con otros

componentes como videos o computadoras. La mayoría de estos sistemas cuentan con visión nocturna, operaciones asistidas por ordenador y detección de movimiento o presencia, garantizando que el sistema trabaje de manera óptima. Este sistema puede trabajar con los sistemas de control de acceso. En la Fig 1.2 se observa una gráfica del sistema de circuito cerrado de televisión.

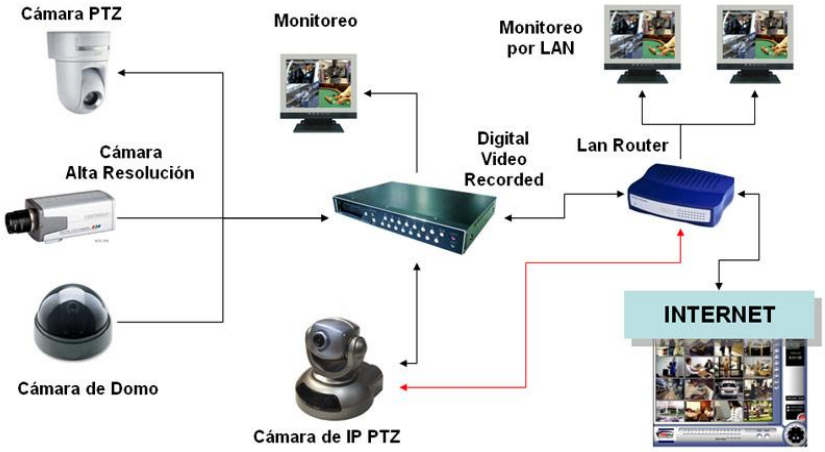

Fig. 1.2 Sistema de CCTV [4]

1.2.3. Sistemas contra incendios

Los sistemas contra incendios alertan a las personas que se encuentran dentro del lugar donde ocurre el incidente, avisándoles la evacuación del lugar por seguridad. Los sistemas de alarma contra incendio pueden ser activadas de distintas formas: detectores de humo, detectores de calor, o manualmente. Al ser activados, los sensores mandan una señal a la unidad de control a fin de poder activar una alerta que puede ser una sirena o una alarma sonora. En la Fig. 1.3 la imagen de un modelo de sistema contra incendios.

Fig. 1.3 Sistemas contra incendio [5]

1.2.4. Sistemas contra hurtos, robos y asaltos a los inmuebles.

Estos sistemas son los más utilizados para detectar y evitar los actos ilícitos en contra de las viviendas. La protección exterior se realiza mediante detectores volumétricos, los cuales se instalan en las afueras del inmueble para detectar la presencia e invasión en un área concreta. En el interior del inmueble se pueden utilizar sensores magnéticos para puertas, sensores de rotura de ventanas y sensores de presencia (PIR). Todos estos dispositivos son controlados por un centro de control el cual genera las órdenes de activación del funcionamiento de los sensores, y viceversa, es decir, capta el mensaje enviado por estos sensores para la activación de una alarma o bocina. El centro de control posee un teclado para poder asignar una clave al sistema de seguridad, con la cual se activa o desactiva el sistema cuando uno lo requiere. [6]

Las partes de este sistema son tres: **conjunto de sensores, centro de control y actuadores.**

1.2.4.1. Sensores

El sensor es un dispositivo capaz de detectar magnitudes físicas o químicas, que se denominarán variables de instrumentación, y transformarlas en variables eléctricas. Para el sistema a implementarse se utilizarán sensores para detectar toda acción que pueda causar daño al patrimonio de las personas. [7]

Los sensores que se utilizan en un sistema de seguridad electrónico contra los hurtos, robos y asaltos se clasifican en:

1.2.4.1.1. Perimetrales
1.2.4.1.2. Volumétricos
1.2.4.1.3. Lineales, entre otros.

1.2.4.1.1. Sensores perimetrales

Se encargan de vigilar el perímetro de una instalación. Se sitúan mayormente en la periferia de la edificación a proteger las puertas, ventanas, etc., estos pueden ser: [7]

- **Sensores de vibración**

Estos se colocan sobre una superficie y cuando reciben un golpe o una vibración se produce una separación de dos masas lo que origina una interrupción del envío de la señal eléctrica, todo esto ocurre en el interior del sensor. [7]

- **Sensores por cinta autoadhesiva conductora**

Es una cinta adhesiva de un material conductor que se adhiere a la superficie del cristal a proteger. La operatividad de este sensor radica en el material que debe actuar como un elemento conductor, éste generará una interrupción al romperse. [7]

- **Sensores por contactos magnéticos**

Estos sensores son usados en puertas, ventanas y persianas. Su funcionamiento se basa en laminillas finas que por la acción de atracción del campo magnético formado por un imán cierran el circuito, lo que al interrumpir generan la apertura de este y activan la alarma. La Fig. 1.4 muestra la imagen del sensor magnético. [7]

Fig.1.4 Sensor magnético [8]

1.2.4.1.2. Sensores volumétricos

Estos son los sensores que actúan por detección de movimiento dentro de un volumen determinado. Son utilizados mayormente en locales cerrados como: viviendas, comercios oficinas, despachos, etc. y pueden ser: [7]

- **Sensores por radar o microondas**

Estos sensores constan de dos partes: emisor y receptor. El emisor emite ondas electromagnéticas que serán reflejadas por los objetos que se encuentren en el área que se protege, luego estas ondas vuelven al receptor. Una de las ventajas de estos sensores es que atraviesan finas superficies como son la madera, cristal, etc., lo que hace más efectivo su detección. [7]

- **Sensores por infrarrojo pasivo (PIR)**

Son sensores que detectan el movimiento de un objeto en una determinada área mediante rayos infrarrojos. Estos rayos son invisibles y se transmiten en línea recta y pueden ser reflejados por cualquier superficie brillante. El sensor detecta el movimiento de un cuerpo humano cuando éste altera la cantidad de rayos infrarrojos en un área, además se sabe que el cuerpo humano emite calor en forma de radiación infrarroja, por ende son captados por los detectores. En la Fig. 1.5 se aprecia la imagen del sensor infrarrojo pasivo. [7]

Fig.1.5 Sensor PIR [9]

1.2.4.1.3. Sensores lineales

Son sensores que actúan al romperse una determinada barrera que es traspasada por un individuo u objeto y se clasifican en: [7]

- **Sensores de barreras infrarrojos**

Al igual que los sensores de presencia (PIR) son sensores que emiten rayos infrarrojos, éstos al presenciar un movimiento alteran la cantidad de haces

infrarrojos. A diferencia de los PIR, los sensores de barreras infrarrojos tienen su emisor y receptor por separado. La Fig. 1.6 representa sensores infrarrojos de barrera. [7]

Fig.1.6 Sensores de barrera infrarrojo [10]

- **Sensores de barreras por microondas**

Se usan para proteger perímetros. Consiste en la colocación de unos cables especiales enterrados que sirven para conectar un emisor y receptor. El emisor emite un impulso de alta frecuencia el cual produce una onda que se propaga a lo largo y fuera del cable transmisor. Cuando se penetra en la zona se produce una variación en la onda que llega al receptor. [7]

1.2.4.2. Unidad central o centro de control

Es un conjunto de dispositivos electrónicos que básicamente se considera como el “cerebro de la instalación”. Su objetivo es interpretar y analizar las señales entregadas por los sensores que indican el intento de agresión y/o penetración en zona protegida. Asimismo avisara a los encargados de la seguridad para generar una alerta o alarma. [11]

En la parte exterior de la carcasa se dispone una serie de indicadores que brindan información sobre el estado del sistema. En el interior posee una fuente recargable, que se alimenta permanentemente de la tensión de la red, en caso de corte de suministro eléctrico, este continúa generando la energía necesaria. [12]

La central se divide en: fuente de alimentación, baterías, teclado, microprocesador, memoria y en algunos casos marcador telefónico.

1.2.4.3. Actuadores (alarmas)

Un actuador es un dispositivo que convierte una magnitud en una señal que puede ser física, química o de otro tipo. El actuador recibe la orden de un controlador y emite una salida necesaria para activar un elemento final de control. [13]

Para un sistema de seguridad, existen varios tipos de actuadores. Estos pueden ser: **ópticos, de llamada y acústicos**.

1.2.4.3.1. Actuadores ópticos

Estos actuadores son dispositivos que generan un tipo de señal visible o luminosa; por ello, en el mercado podemos encontrar gran variedad de este tipo de actuadores. Éstos pueden ser: focos, diodos emisores de luz (leds), matriz de leds, pantallas, etc. [13]

1.2.4.3.2. Actuadores de llamada

Son aquellos dispositivos capaces de realizar un mecanismo de llamada cuando surge un problema con el equipo o ambiente, estos son ordenados a actuar o son activados por un controlador. [13]

1.2.4.3.3 Actuadores acústicos

Los actuadores acústicos son los más comunes para la implementación de un sistema de seguridad y existen varios de este tipo que serán explicados a continuación:

- **Sirena**

Son las más llamativas y poderosas de todos los actuadores acústicos, por lo que se emplean en ambulancias, camiones de bomberos, sistemas de alarmas, etc. Su radio de alcance sobrepasa el kilómetro, en condiciones favorables, y sus tonos elevados sobrepasan prácticamente cualquier otro sonido exterior. En la Fig. 1.7 se observa la imagen de una sirena eléctrica. [13]

Fig. 1.7 Sirena [14]

- **Campanillas**

Es la más versátil de todos los actuadores, se emplean por lo general para alarmas contra ladrones o incendios, para compaginación de códigos y señales de horario. El tono varía del moderado y apacible hasta extremadamente insistente. [13]

- **Zumbadores**

Son transductores electroacústicos que producen un sonido, zumbido continuo o intermitente de un mismo tono. Son populares para las alarmas en los edificios públicos, hospitales y otros lugares donde las demás señales no convienen. [13]

En la Fig. 1.8 se muestra una imagen representativa de las partes del sistema de seguridad contra hurtos, robos y asaltos de un inmueble.

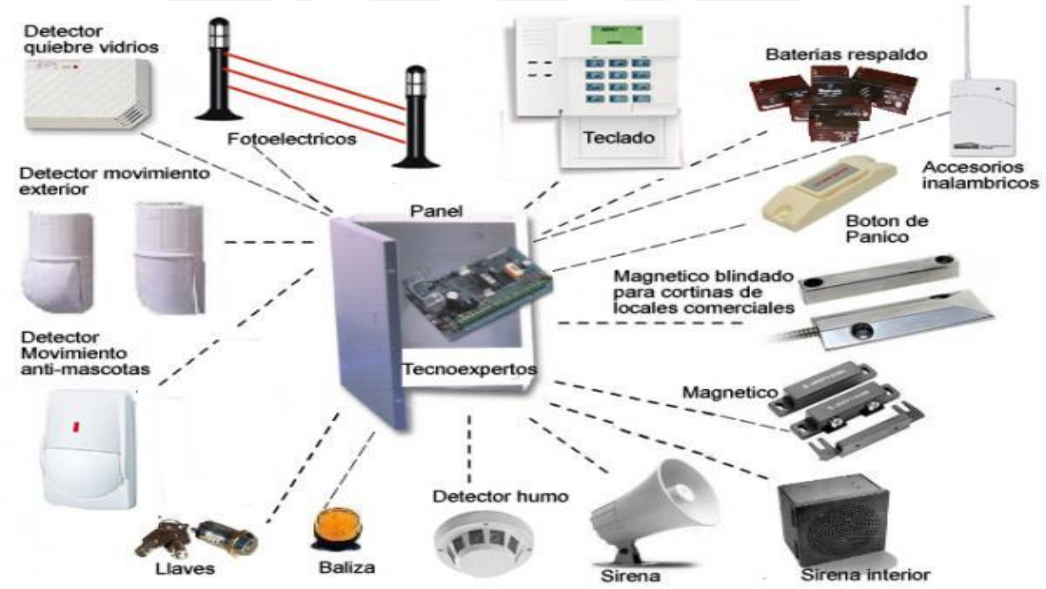

Fig. 1.8 Partes del sistema de seguridad contra hurto, robos y asaltos [15]

1.3. Tecnología de comunicación

Estos sistemas han ido evolucionando y actualmente se pueden apreciar sistemas de seguridad electrónicos inalámbricos. Como estos sistemas serán instalados dentro de una vivienda o edificio, debemos resaltar un área muy importante de la electrónica: la domótica.

La domótica es el conjunto de sistemas capaces de automatizar una vivienda para brindar seguridad, gestión energética y comunicación. La variedad de tecnología inalámbrica en la domótica es inmensa, las más resaltantes para la elaboración de este proyecto son: ZigBee, Wifi, Bluetooth, radio frecuencia, infrarrojos y GPRS.

Una tecnología inalámbrica novedosa y que últimamente se está utilizando con mayor frecuencia es el Bluetooth. Este es un protocolo diseñado especialmente para conexiones que presentan bajo consumo de energía y de medio alcance, el que se adecúa al sistema de seguridad que será planteado posteriormente.

Tecnología Bluetooth

Bluetooth es un sistema de comunicaciones inalámbrica de corto alcance, basados en un estándar global de comunicaciones inalámbricas establecido por la IEEE bajo la especificación 802.15.1, en donde se puede transmitir voz, datos, imágenes, multimedia entre otros, a través de diferentes dispositivos empleando la tecnología de radiofrecuencia. El tipo de redes que opera Bluetooth son las llamadas WPAN (Wireless Personal Area Network) o redes de área personal inalámbricas. [16]

Los principales objetivos de esta tecnología son:

- Facilitar la comunicación entre equipos móviles y fijos
- Eliminar cables y conectores entre dispositivos
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre los equipos personales.

Dentro del desarrollo de bluetooth es necesario conceptualizar su operatividad y composición: [16]

- **Banda de frecuencia libre**

Para poder operar en cualquier parte del mundo es necesaria una banda base de frecuencia abierta a cualquier sistema de radio independientemente del lugar donde se encuentre. La banda ISM (médico científica internacional) cumple con ese requerimiento. Los rangos van de los 2.4 Ghz a los 2.4835 Ghz. El sistema de Bluetooth opera en este rango de banda. [16]

- **Arquitectura de Bluetooth**

La característica más resaltante de Bluetooth, es de proveer un conjunto completo de protocolos, los cuales permiten la intercomunicación de aplicaciones entre dispositivos. En la Fig. 1.9 se muestra un esquema de la arquitectura de Bluetooth.

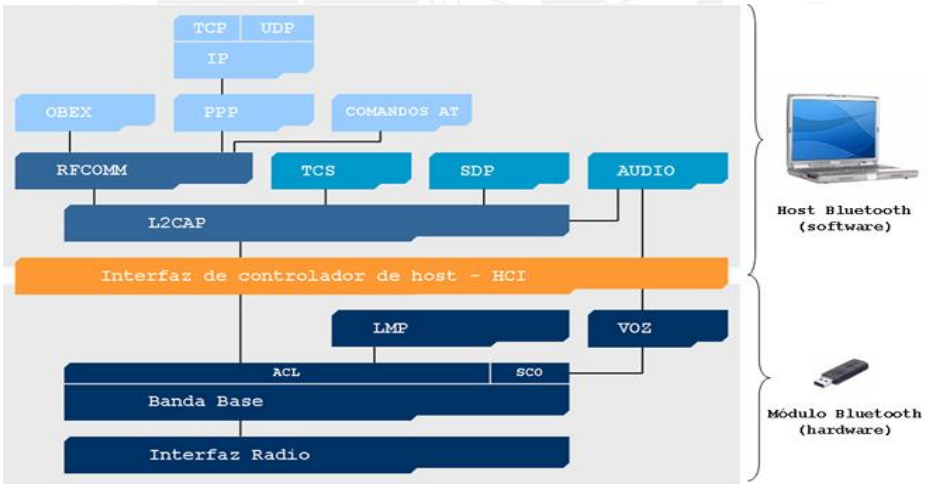

Fig. 1.9 Arquitectura Bluetooth [17]

Dentro de la arquitectura de Bluetooth podemos resaltar las siguientes capas:

- **Capa RF**

En esta capa de radiofrecuencia se encuentra el MODEM de radio que utiliza para la transmisión (Tx) y la recepción (Rx) de la información, en la banda ISM de 2.4 Ghz mediante la modulación de salto de frecuencia (FHSS). [18]

- **Capa Banda Base**

Esta capa es la encargada del control del enlace a nivel de bit y paquetes, asimismo establece la codificación y encriptación, y también las reglas de saltos de frecuencia. [18]

- **Capa de protocolo de manejo de enlace (LMP)**

La capa de protocolo de manejo de enlace está encargada de establecer los enlaces con los otros dispositivos, además es la responsable de conectar los nodos maestros con los esclavos, administra sus modos de operación y vela por el control de potencia. [18]

- **Capa de protocolo de adaptación y control de enlace lógico (L2CAP)**

Es la encargada de brindar servicio de datos orientados a conexión, como los no orientados a conexión de los protocolos de las capas superiores, en conjunto con las facilidades de multiplexación, segmentación y reensamblaje. Además el L2CAP permite que los otros protocolos de capa superiores puedan transmitir y recibir paquetes de hasta 64 Kbytes de longitud. [18]

- **Protocolo RFCOMM**

Este protocolo establece comunicaciones seriales punto a punto, emulando RS232 a través de radio frecuencia, proporcionando la emulación de puertos RS232 mediante el protocolo L2CAP [18]

- **Protocolo de descubrimiento de servicios (SDP)**

Este protocolo permite que las aplicaciones del cliente descubran la existencia de diversos servicios brindados por uno o más “servidores de aplicación” junto con los atributos y propiedades que estos ofrecen. [18]

- **Protocolo de control de telefonía (TCP)**

Este protocolo define la señalización para el control de llamadas de voz para aplicación de telefonía inalámbrica. El audio es transferido directamente de la aplicación a la banda base. El Bluetooth soporta hasta 3 canales de audio full dúplex simultáneamente. [18]

❖ **Clasificación de dispositivos de Bluetooth**

En la actualidad existen dos tipos de clasificaciones para los dispositivos de Bluetooth: **por consumo de energía y ancho de banda**.

Por consumo de energía, los dispositivos pueden clasificarse en clase 1, clase 2 y clase 3.

Tabla 1.1 Clases de Bluetooth [19]

Clase	Potencia máxima permitida (mW)	Potencia máxima permitida (dBm)	Rango (m)
Clase 1	100	20	100
Clase 2	2.5	4	10
Clase 3	1	0	1

Por ancho de banda, puede ser:

Tabla 1.2 Versiones de Bluetooth [19]

Versión	Ancho de banda
Versión 1.2	1 Mbit/s
Versión 2.0 + EDR	3 Mbit/s
Versión 3.0 + HS	24 Mbit/s

CAPÍTULO 2

DESCRIPCIÓN Y REQUERIMIENTO DEL SISTEMA

En el capítulo anterior, se explicó los diferentes tipos de sistemas de seguridad existentes, de los cuales, para la presente tesis se eligió el sistema contra los hurtos, robos y asaltos en los inmuebles.

2.1. Descripción del sistema

2.1.1. Localización del sistema

El sistema diseñado será implementado en un departamento ubicado en el 3er. piso de un edificio residencial, con un área de 103.50 m², el cual consta de 8 áreas: dos dormitorios, una cocina, una sala – comedor, un patio, una lavandería y dos baños. Adicionalmente, presenta dos tragaluces y una jardinera con vista al exterior. En la Fig. 2.1 se observa el bosquejo de la vivienda elegida y la distribución de sus zonas.

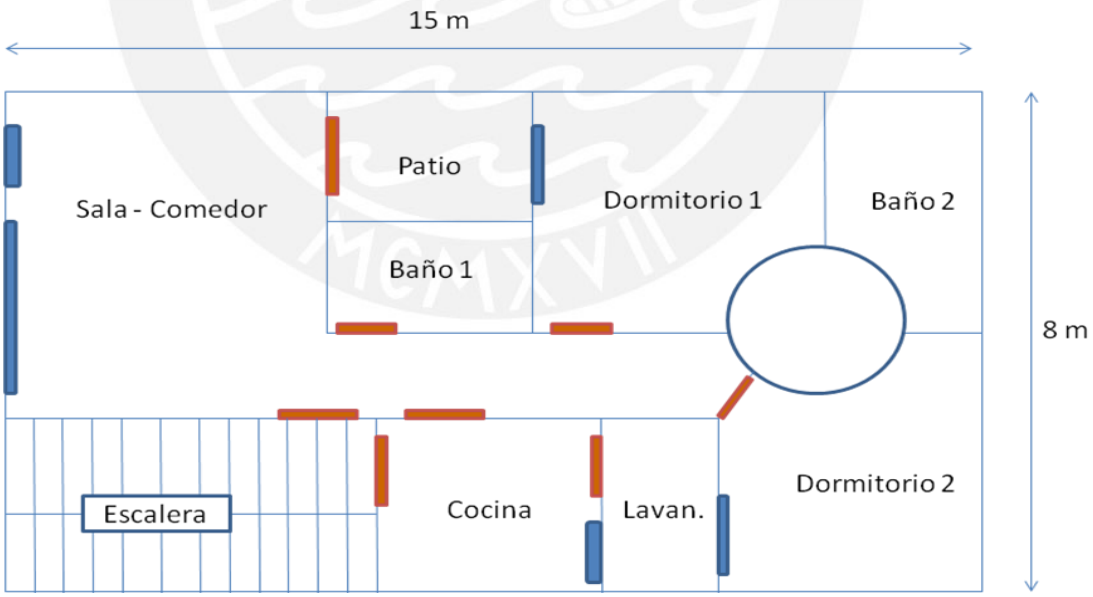

Fig. 2.1 Bosquejo de la vivienda y distribución de las zonas

2.1.2. Vulnerabilidad del área de protección

Realizado el estudio de factibilidades del inmueble a proteger, conforme al bosquejo que se presenta (Fig.2.1); se han determinado las áreas más

vulnerables por donde podrían ingresar individuos para cometer actos ilícitos. Estas áreas son:

- Del patio hacia el primer dormitorio
- Del patio hacia la sala-comedor
- De la lavandería a la cocina
- De la lavandería hacia el 2do dormitorio
- Por las ventanas exteriores hacia la sala-comedor
- Por la puerta principal y de la cocina

Consideraciones importantes

El sistema de seguridad estará diseñando para proteger una vivienda de regulares dimensiones (departamento de 140m² aproximadamente) ubicado en un edificio residencial con ingresos comunes; estas características condicionan a que el sistema tenga un medio de comunicación de pequeño o mediano alcance y que el manejo de éste sea de fácil acceso para el usuario.

Asimismo, es importante adecuar todo el sistema (sensores, medios de comunicación, actuadores) para que el consumo de energía eléctrica sea mínimo con la finalidad de que el usuario no tenga gastos excesivos. Esta consideración debe ser un incentivo para que el uso de este sistema de seguridad esté al alcance de todos los estratos sociales.

2.2. Requerimientos del sistema

De acuerdo al resultado de la evaluación y estudio realizado en el inmueble y conforme al plano presentado para proteger las áreas vulnerables del ingreso externo, el sistema requiere lo siguiente:

Para la sala-comedor:

Dispositivos que detecten el ingreso de intrusos por las ventanas, puerta principal y puerta colindante al patio. Las dimensiones de los accesos de los posibles intrusos son: 3m² (1m x 3m) correspondiente a la ventana principal,

3m² (2m x 1.5m) correspondiente a la puerta colindante al patio y 2.4m² (2m x 1.2m) correspondiente a la puerta principal. Los posibles sensores son:

- Sensores de vibración
- Sensores por cinta autoadhesiva conductora
- Sensores magnéticos
- Sensores por radar o microondas
- Sensores pasivos infrarrojos
- Cámaras de video

Para el dormitorio 1:

Dispositivos que puedan detectar el ingreso de intrusos por las ventanas colindantes al patio. La dimensión del acceso de los posibles intrusos es: 1.5m² (1m x 1.5m). Los posibles sensores son:

- Sensores de vibración
- Sensores por cinta autoadhesiva conductora
- Sensores magnéticos
- Cámaras de video

Para el dormitorio 2:

Dispositivos que puedan detectar el ingreso de intrusos por las ventanas colindantes a la lavandería. La dimensión del acceso de los posibles intrusos es: 2m² (1m x 2m). Los posibles sensores son:

- Sensores de vibración
- Sensores por cinta autoadhesiva conductora
- Sensores magnéticos
- Cámaras de video

Para la cocina:

Dispositivos que puedan detectar el ingreso de intrusos por la ventana y puertas laterales (exterior y lavandería). Las dimensiones de los accesos de los posibles intrusos son: 1m² (1m x 1m) correspondiente a la ventana, 2.4m² (2m x 1.2m) correspondiente a la puerta con acceso a la escalera y 2m² (2m x 1m) correspondiente a la puerta colindante a la lavandería. Los posibles sensores son:

- Sensores por radar o microondas
- Sensores pasivos infrarrojos
- Sensores magnéticos
- Cámaras de video

Para la unidad central se requiere:

Un controlador que reciba la información proporcionada por los sensores y/o cámaras, las que serán analizadas y procesadas para activar una alerta en caso sea necesario.

Tecnología de comunicación a utilizar

Dentro de las comunicaciones existe dos medios de comunicaciones importantes, las inalámbricas y las cableadas. Las diferencias de estas son la portabilidad, el alcance y la variación de precios que puede costar su implementación; sin embargo, el avance de la tecnología ha hecho que estas dos últimas diferencias se disminuyan a una escala notable. Es por ello que para nuestro sistema de seguridad hemos elegido que el medio de nuestra comunicación será inalámbrico. Dentro de los medios inalámbricos que se pueden utilizar para este sistemas se encuentran los siguientes:

- Radio Frecuencia
- Wifi
- Zigbee
- Bluetooth
- Infrarrojo

Para el proyecto del sistema de seguridad se utilizó la tecnología de Bluetooth debido a las características que presenta y cumple con las consideraciones previamente explicadas.

2.3. Características del sistema

De las diferentes características que presenta el sistema de seguridad, se pueden mencionar como las principales las siguientes:

- Posee un interfaz amigable de fácil acceso para el usuario.
- Disposición de cuatro zonas de vigilancia.
- Posee indicadores (leds) de zona y de estado los cuales estarán presentes en el tablero del centro de control.

CAPÍTULO 3

DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD

3.1. Conformación del sistema

Para comprender de manera sencilla y rápida la conformación del sistema de seguridad a implementarse, se ilustra en el siguiente diagrama de bloque (Fig. 3.1), los componentes:

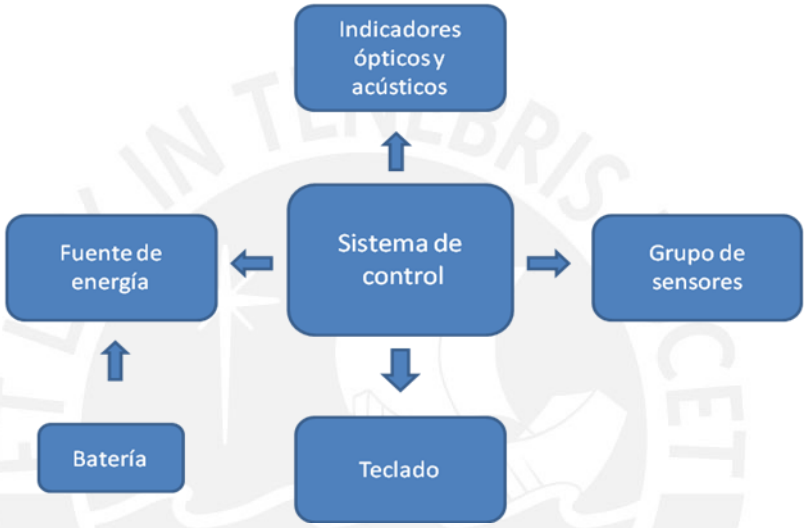

Fig. 3.1 Diagrama de bloques del sistema de alarma

El sistema está conformado por sensores, leds indicadores de estado del sistema, un microcontrolador para el sistema de control, un teclado hexadecimal y una serie de indicadores.

Las partes del sistema de seguridad son:

3.1.1. Fuente de energía.

3.1.2. Los sensores.

3.1.3. Sistema de control

3.1.4. Indicadores o alarmas.

3.1.5. Comunicación inalámbrica.

Como se precisó anteriormente, la comunicación inalámbrica es realizada mediante módulos de bluetooth, por lo cual todos los dispositivos tienen que tienen este módulo son: los sensores PIR, la unidad central y la alarma, a

continuación se presenta un diagrama el cual indica el medio de comunicación utilizado.

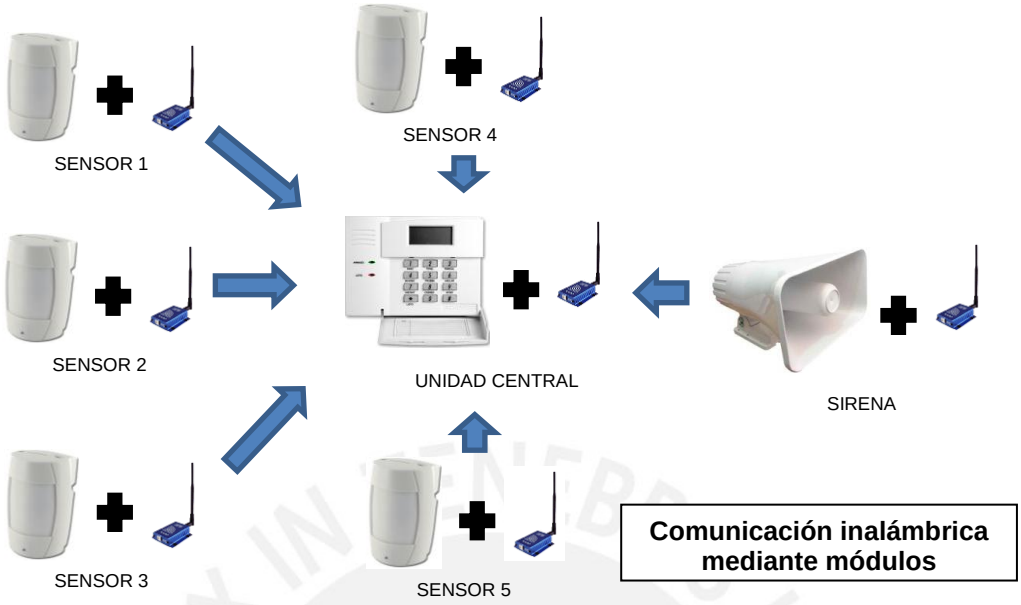

Fig.3.2 Diagrama de comunicación del sistema de seguridad

Requerimientos tecnicos

Para la elaboracion del proyecto de tesis se tuvieron en cuenta los siguientes requerimientos tecnicos:

- Para la unidad central, se necesitó un controlador con pines digitales suficientes para conectarse con el LCD y los indicadores; con comunicación serial para comunicarse con el módulo Bluetooth. Adicionalmente un requerimiento para este fue el bajo costo y accesible en el mercado nacional.
- Los sensores tienen que ser de baja potencia (<0.1w), por los cuales se optaron por sensores PIR modelo MS-360. Para ellos se necesitó diseñar fuentes para su alimentacion. Asimismo estos se encuentran accesibles en el mercado nacional.
- Para la comunicación se necesitó módulos bluetooth de bajo consumo de energia y fáciles de utilización.

3.1.1. Fuente de energía

La fuente de energía desempeña un papel importante en todo sistema electrónico, debido a que realiza la conversión de tensión alterna adquirida por

la red, a tensión continúa, la que debe ser lo más estable posible, para que el funcionamiento de todo el sistema sea óptimo y adecuado.

En la presente tesis se diseñaron 2 diferentes tipos de fuentes, las cuales son: un tipo de fuente para la unidad central y otro tipo de fuente para cada sensor PIR.

Fuente de energía para unidad central

Esta fuente de energía posee las siguientes partes:

- Transformador de entrada
- Rectificador
- Filtro para el control de rizado
- Regulador o estabilizador

A continuación se observa el diagrama de las diferentes etapas de fuente de energía:

Fig. 3.3 Etapas de fuente de energía

- **Etapa de transformación**

En esta etapa se reduce la tensión de entrada a la fuente, en este caso la tensión domiciliaria es de 220v alterna, para lo cual se utiliza un transformador reductor de 220 VAC a 12 VAC y a la salida obtendremos 12 voltios alterna.

- **Etapa de rectificación**

En esta etapa se realiza la conversión del voltaje de alterna de entrada (12 VAC) a un voltaje continuo. En la elaboración de esta etapa se implementó un circuito rectificador conformado por 4 diodos (1N4007), con esto se consigue que el voltaje no sea negativo y se mantenga siempre por encima del nivel de cero.

- **Etapa de filtrado**

Luego de la rectificación, se requiere un voltaje DC uniforme y para ello la etapa anterior pasa por un filtro, que consistirá básicamente de un condensador de 2200 uf a 25 v.

- **Etapa de regulación**

Esta etapa debe lograr mantener constante el voltaje para la carga, independiente de las variaciones que pueden existir en el voltaje de entrada o la corriente que necesita la carga, es por ello que se utiliza un regulador ajustable de voltaje que es el LM317, este componente electrónico ofrece protección total de sobrecargas y limitación de corriente.

En la siguiente imagen (Fig 3.12) se presenta el diagrama esquemático de la fuente de energía.

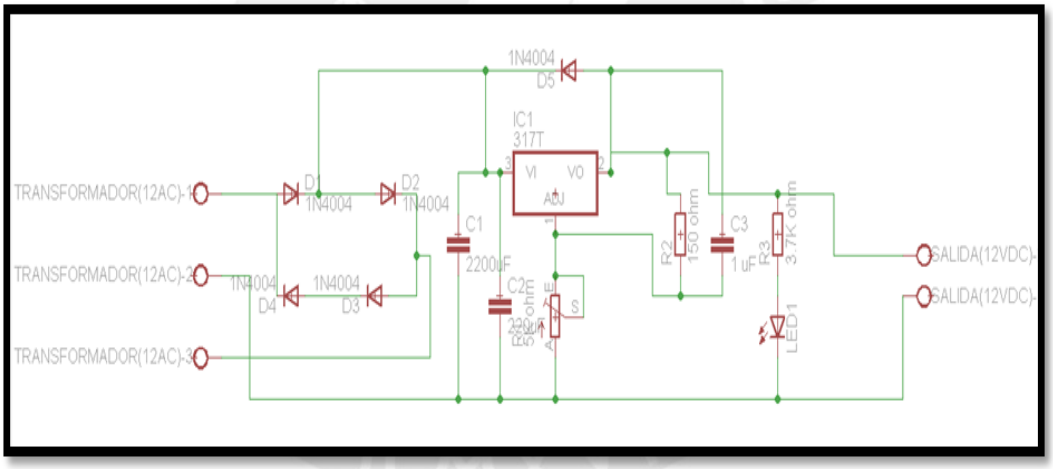

Fig. 3.4 Diagrama esquemático de la fuente de energía de la unidad central

Fuente de energía para los sensores

Cada sensor posee una fuente de energía independiente y para esta se diseñó un circuito que pueda transformar el voltaje 220 VAC a 5 VDC.

En la siguiente figura podemos apreciar un diagrama de cómo estará distribuida la fuente a 5 VDC.

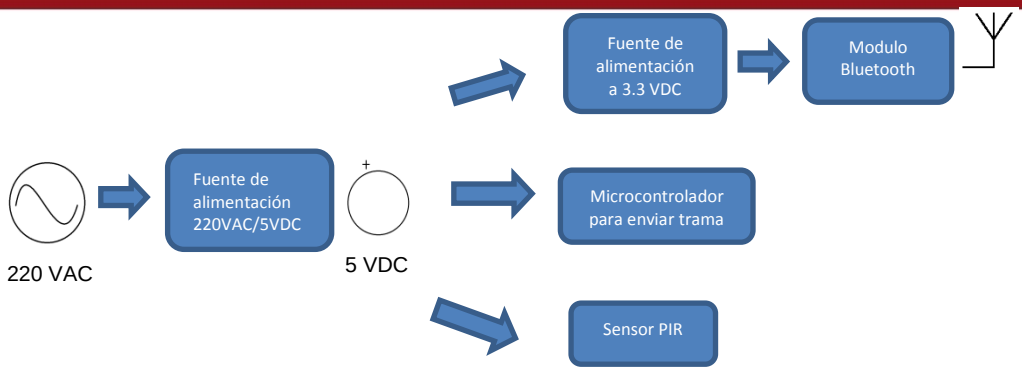

Fig. 3.5 Diagrama de fuente de energía de 5 VDC

A continuación (en la Figura 3.6) se muestra una fuente de voltaje sin transformador de 220 AC a 5VDC. Esta fuente es regulada a través del diodo zener, la cual limita el rango de corriente. El circuito está conformado por dos resistencias (R1 y R2) y un capacitor (C1) que en conjunto sirvió para reducir el voltaje de la entrada a uno aceptable por el diodo zener, posteriormente se encuentran un par de diodos (D1 y D2) los cuales se realizaron una rectificación de media onda antes de la entrada del zener, después se encuentra un condensador (C2) que se encargó de eliminar el rizado de la onda y mantenerla constante. Finalmente se conectó al diodo zener para mantener un voltaje de 9V y adicionalmente se coloca un regulador lineal 7805 para obtener los 5VDC deseados. Este circuito se diseñó debido al pequeño espacio que se tiene y al poco consumo de corriente que se necesitó para la activación de los sensores PIR.

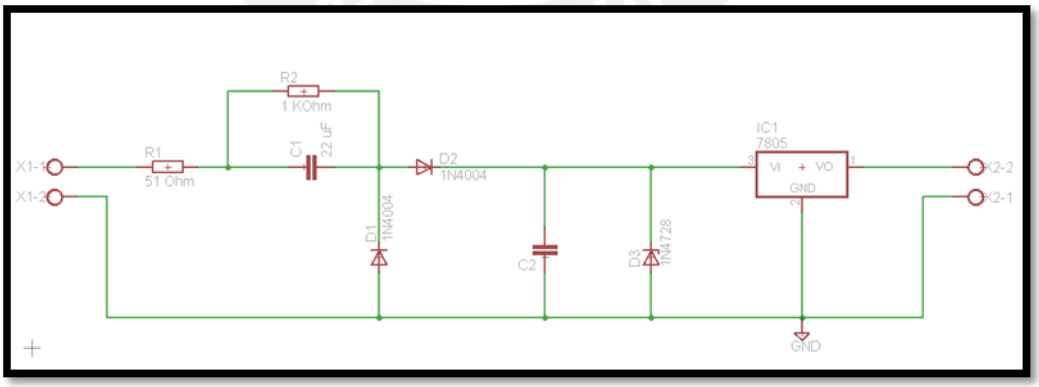

Fig. 3.6 Diagrama esquemático de la fuente de energía de los sensores

Adicionalmente, para que el sistema sea independiente de la tensión eléctrica proveniente del inmueble, se diseñó un circuito con la finalidad de cargar un par de pilas que al corte de la energía eléctrica, el sistema de seguridad funciona sin

ningún inconveniente. Mientras el sistema utilice la tensión eléctrica las pilas se cargarán de energía a fin de poder utilizarse en momentos donde carezca de ésta.

A continuación (Fig 3.7) se presenta el diagrama esquemático del circuito que brinda autonomía al sistema de seguridad.

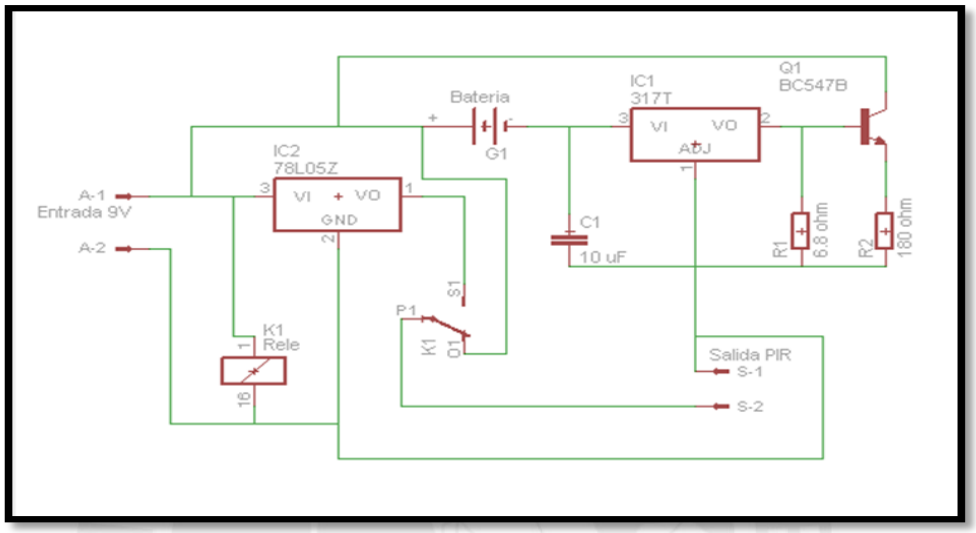

Fig. 3.7 Diagrama esquemático circuito de autonomía y carga de las pilas o baterias

3.1.2. Los sensores

Los sensores son los dispositivos que brindarán la información sobre el ingreso de una persona o intruso en el ambiente de protección, conforme a lo requerido. Para el trabajo de la presente tesis, se utilizan dos tipos de sensores: **Los sensores pasivos infrarrojos,** que se instalan para detectar intrusos en zonas cercanas a las ventanas **y los sensores magnéticos,** que se instalan en las puertas.

3.1.2.1 Sensores pasivos infrarrojos (PIR)

El sensor pasivo infrarrojo o piroeléctrico, es un dispositivo electrónico que mide los cambios de niveles en la radiación infrarroja emitida por objetos que se encuentran a su alrededor. Por lo general, está hecho de un material cristalino o cerámico, que genera una carga eléctrica en la superficie cuando se expone al calor en forma de radiación infrarroja. Por lo tanto, cuando la temperatura del

exterior cambia, la radiación infrarroja que recibe el sensor también lo hará, entonces la carga eléctrica sufrirá una variación que será detectada por un transistor de efecto campo (FET) ubicado dentro del sensor. Los elementos de este sensor son sensibles a un amplio rango de radiación infrarroja, es por ello que se adhiere un filtro que limita el rango entre 5µm y 14µm, en el cual se ubica la radiación promedio de un cuerpo humano que es de 36 grados centígrados.

Está compuesto por dos elementos que captan los cambios de radiación infrarroja colocado en polarización opuesta entre ellos con el fin de anular las señales de interferencia causadas por la luz solar, vibraciones y variaciones de temperatura, mejorando en gran escala la estabilidad de funcionamiento del sensor. En la Fig. 3.8 se aprecia la imagen representativa del funcionamiento del sensor pasivo infrarrojo. [12]

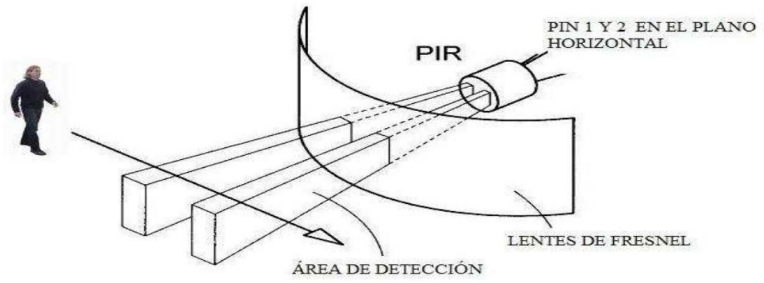

Fig. 3.8 Funcionamiento del sensor PIR [20]

Cuando una persona pasa frente al sensor (área de detección), activa cada uno de los elementos en forma secuencial y genera un cambio de tensión eléctrica, el que puede ser negativo o positivo dependiendo de la dirección por donde pase el intruso. [12]

A diferencia de otros sistemas, como los de microondas o ultrasónicos, los PIR, solo reciben pasivamente la radiación infrarroja proveniente de cuerpos de temperatura superiores al ambiente; además presentan un gran ahorro de energía. Estos sensores son de buena confiabilidad, debido a que actúan en conjunto con programas especializados que los hacen más precisos. La Fig. 3.9 representa el sensor pasivo infrarrojo (PIR) [12]

Fig. 3.9 Sensor PIR [21]

Por criterios de costo y gran oferta en el mercado nacional, se utilizó el circuito del sensor prefabricado PIR de movimiento. Este sensor posee un rango de alcance máximo de 6 metros lo cual es suficiente y que funcionará dependiendo de la ubicación de éste, para detectar un intruso dentro del ambiente al cual se le asigna.

3.1.2.2. Sensores magnéticos

Son dispositivos de apertura integrados por dos unidades hermanadas en una posición determinada y que ante la separación de estas dos piezas genera un cambio mecánico en los contactos de una de ellas, informando el cambio de estado de apertura, el que pasa de estado cerrado al abierto. Una de las dos piezas, consiste en un contacto formado por láminas de metal, que permanecen cerradas o abiertas ante la presencia de un campo magnético circundante y la otra pieza es un imán cerámico de alta coercitividad, que proveerá las necesarias “líneas de fuerza” de un campo magnético, capaz de influenciar directamente en la posición de las láminas de la parte contactual. Los más usuales, son aquellos que en presencia de un campo magnético se mantienen cerradas (unidas entre sí) y que se abren cuando desaparece o disminuye notoriamente el campo magnético. Cuando el sensor magnético se encuentra abierto va a mandar una señal al microcontrolador para ser transmitida por los módulos inalámbricos. [22]

3.1.3. Sistema de Control

Dentro de la unidad central podemos encontrar dos partes importantes: **interfaz del usuario y unidad de control.**

3.1.3.1. Interfaz del usuario

Para la elaboración del interfaz de usuario, se utilizó una pantalla LCD y un teclado matricial, los cuales resultan cómodos en la interacción del interfaz con el usuario.

- **Pantalla de cristal líquido LCD**

Para que la unidad central sea más ilustrativa para el usuario, se utilizó una pantalla que permite visualizar los resultados y las acciones que se están desarrollando. Esta pantalla es un elemento activo que tiene gran variedad de tipos, los cuales varía de acuerdo a su forma y tamaño. La pantalla escogida para la presente tesis es el LCD de dos líneas con dieciséis caracteres cada uno. La gran ventaja de estos dispositivos es que son comerciales y compatibles entre sí.

Esta pantalla, visualiza 16 caracteres en cada fila; sin embargo puede almacenar hasta 20 caracteres por línea, dentro de la programación se especificará que caracteres se desean mostrar.

El LCD posee una matriz de 5x8 pixeles o puntos para representar cada caracter, en total se pueden representar 256 caracteres distintos, de los cuales 248 están grabados en la memoria del LCD y 8 pueden ser implementados por el usuario.[23]

A continuación, en la figura 3.10 se puede apreciar la pantalla LCD 16 x 2 que nos permitirá visualizar la información que envía la unidad de control.

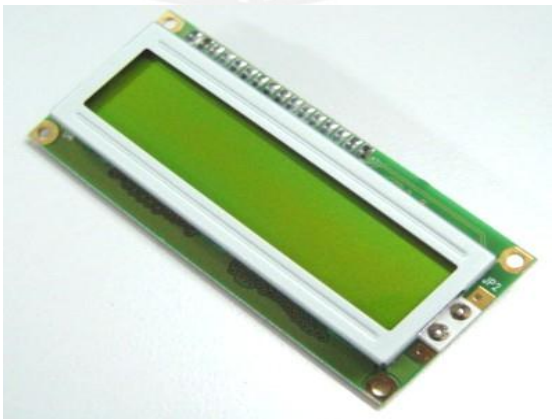

Fig. 3.10 Pantalla LCD 16x2 [23]

- **Teclado matricial**

Es un dispositivo electrónico compuesto por un arreglo de botones conectados en filas y columnas, de modo que se puedan leer con el mínimo número de pines requeridos. Para la presente tesis, se utiliza un teclado matricial de 4x4, el cual ocupa 4 pines de un puerto para las filas y 4 pines para las columnas; es por ello, que se pueden leer 16 teclas utilizando solamente 8 pines del microcontrolador. [24]

En la figura 3.11 se observa el esquemático del teclado matricial.

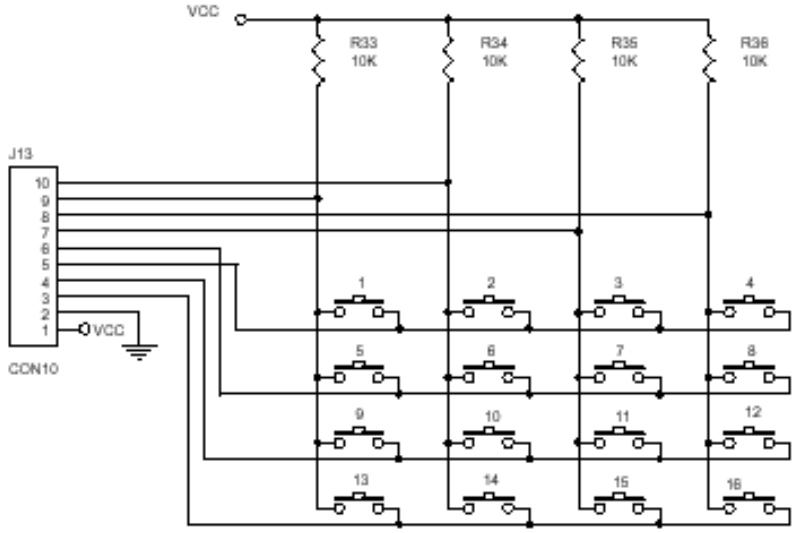

Fig. 3.11 Diagrama del teclado matricial 4x4 [24]

La mayoría de teclados se lee por una técnica de exploración, que consiste en ir leyendo consecutivamente las filas o columnas de éste. Existen circuitos especializados para realizar esta tarea, para la presente tesis se utilizó un microcontrolador.

3.1.3.2. Unidad de control

Microcontrolador PIC16F877A

Para la parte de control de la unidad central se utiliza este microcontrolador, que es un circuito integrado de 8 bits con 5 puertos de entrada y salida, soporta un modo de comunicación serial, posee 2 pines para su funcionamiento (Rx y Tx). También presenta una amplia memoria en comparación de las versiones anteriores para datos y programas, además cuenta con una memoria flash que

se puede borrar eléctricamente y un set de instrucciones reducido de tipos RISC. [25]

Características:

8KB de memoria de programa flash

368 posiciones RAM de datos

256 posiciones EEPROM de datos

14 interrupciones

3 Temporizadores

Comunicación serial USART

A continuación (Fig. 3.12) se puede apreciar el esquema del microcontrolador, éste tiene la finalidad de indicar las diferentes funcionalidades de cada puerto o PIN.

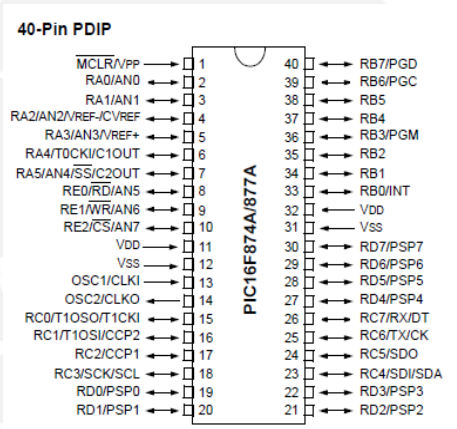

Fig. 3.12 Microcontrolador PIC 16F877A [25]

La unidad de control se encarga de velar por el buen funcionamiento del sistema, dentro de ella se puede apreciar un teclado matricial el que se encarga de brindar la contraseña a nuestro sistema de seguridad; una pantalla LCD que indica la activación o desactivación del sistema de seguridad dependiendo de la contraseña; y el microcontrolador que procesa las señales enviadas por los sensores para la activación de la alarma, asimismo se encarga de procesar y corroborar la contraseña brindada.

En la siguiente figura (Fig. 3.13) se aprecia el diagrama esquemático de la unidad de control.

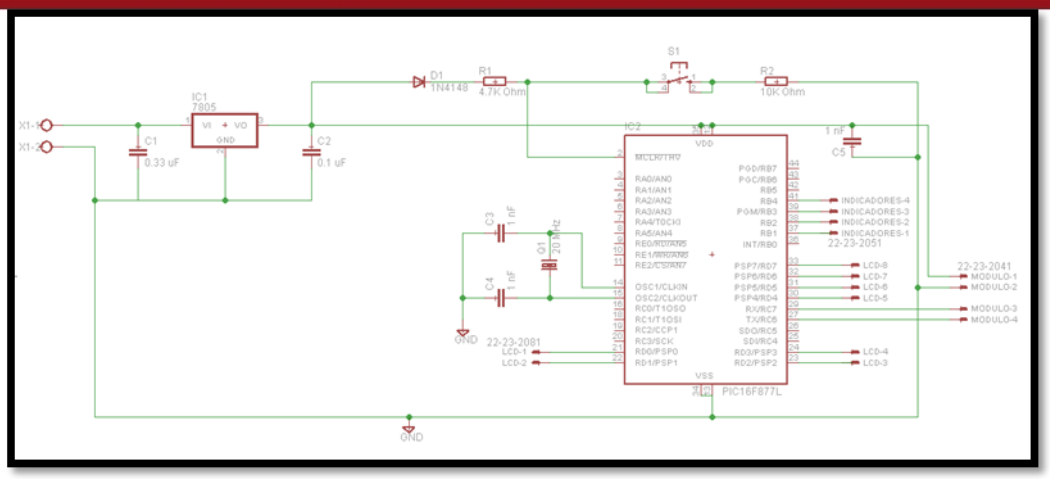

Fig. 3.13 Diagrama esquemático de la unidad central

La unidad central se comunicará por intermedio de los módulos Bluetooth, por lo que se diseñó un circuito especial para su comunicación. La imagen siguiente (Fig. 3.14) representa el diagrama esquemático de lo descrito anteriormente.

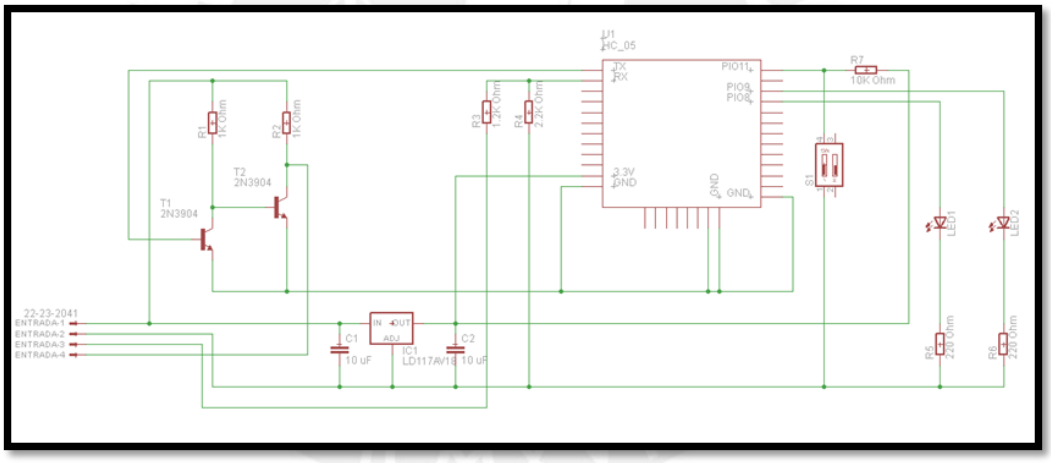

Fig. 3.14 Diagrama esquemático de módulo Bluetooth para la unidad central

3.1.4. Indicadores o alarmas

- **Ópticos**

El sistema cuenta con indicadores visuales que básicamente son diodos de emisión de luz (led), los que indicarán el estado y la función de seguridad. Cada diodo de diferente color corresponde a cada zona resguardada (cuatro zonas), estos diodos se encenderán indicando si alguna de las zonas de seguridad ha sido invadida por intrusos. Asimismo, el sistema cuenta con un led que indica el suministro de energía alterna al sistema de control.

- **Acústicos**

El sistema contiene un dispositivo sonoro que advierte y anuncia cuando se ha violentado cualquiera de las zonas de la vivienda. Este dispositivo es una sirena que funciona con una fuente de alimentación de 12 VDC. Para activar y generar el sonido de la sirena, se diseñó un circuito electrónico, que genera las frecuencias necesarias de ésta. La frecuencia principal de la sirena es de unos 3500Hz o 4000Hz la segunda frecuencia es de unos 400 o 500 Hz.

Para activar la alarma, se requiere de un circuito integrado capaz de generar 2 frecuencias distintas a la vez, por lo que se utilizó un temporizador 555. Como la tensión de las sirenas no es menor que 12 VDC, para el diseño del circuito se utilizaron transistores de alta resistencia. A continuación se observa la figura (Fig. 3.15) del diagrama esquemático del circuito diseñado.

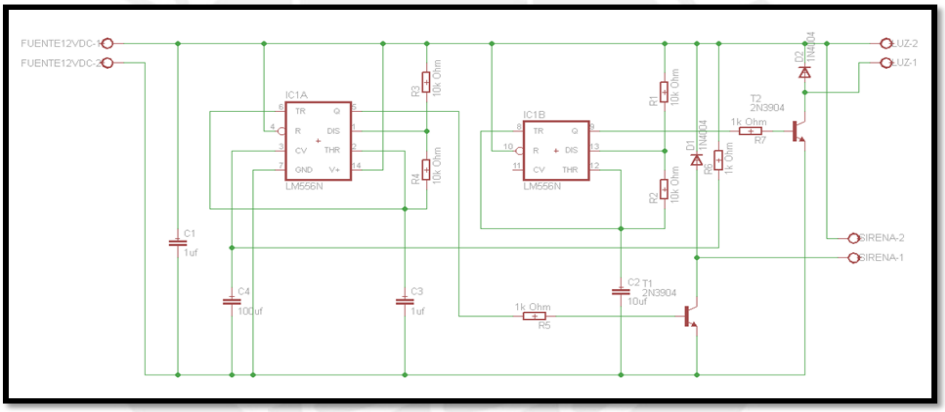

Fig. 3.15 Diagrama esquemático de la sirena

3.1.5. Comunicación inalámbrica.

Como se explicó anteriormente, la tecnología de comunicación que se utilizó para este trabajo de tesis es Bluetooth. Por lo tanto, para la transmisión de datos entre los sensores y la unidad de control, se emplearon los módulos de Bluetooth serial HC05 del fabricante SZHR procedente de China, por su bajo costo, de fácil integración y utilización que tienen estos dispositivos.

- **Módulos Bluetooth serial HC 05**

Los módulos Bluetooth serial HC 05 son módulos “transceiver”; es decir, módulos que transmiten y reciben señal. El módulo bluetooth utiliza el chipsets

CDR BlueCore4 y soporta una fuente de poder de 3.3 VDC. Estos módulos son de clase 2 por lo que la potencia máxima permitida es 2.5 mW y tienen un alcance máximo de 10 metros. La comunicación entre este módulo y un microcontrolador se realizan por los puertos seriales con una pequeña amplificación cuando se transmite del módulo al microcontrolador, por que el módulo trabaja con 0v y 3.3v, donde 0v es “0” lógico y 3.3v es ”1” lógico; se realiza lo inverso para poder transmitir la comunicación del microcontrolador al módulo.[26]

Especificaciones:
Protocolo Bluetooth: Especificación Bluetooth v 2.0 + EDR
Frecuencia: 2.4 GHz ISM Band
Modulación: GFSK (Desplazamiento de frecuencia gausiana)
Sensibilidad: max -84dBm a 0.1% VER
Transmisión de poder: máximo 4dBm, Clase 2
Fuente de alimentación: +3.3 VDC a 8 mA (en comunicación)

A continuación se muestra una figura (Fig. 3.16) del módulo de Bluetooth a utilizar.

Fig. 3.16 Módulo Bluetooth HC05 [26]

Estos módulos han sido configurados previamente, para lograr la comunicación entre el microcontrolador y el módulo (velocidad de transmisión de 9600bits/s, 8 bits de datos, sin bit de paridad). Para la configuración de estos módulos, se utilizaron los comandos AT, los que se han ingresado a través del puerto serial del computador.

- **Comandos AT**

Los comandos AT son instrucciones codificadas que comprenden un lenguaje de comunicación entre el hombre y un terminal modem.
A continuación se presentan los comandos básicos para la configuración:

Maestro/esclavo ajustar y preguntar

Tabla 3.1 Comando de AT de Rol [26]

	Comando	Parámetros	Respuesta
Ajuste	AT+ ROLE=(num)	num: “0” para esclavo, “1” para maestro	OK
Pregunta	AT+ROLE?	NULL	+ROLE=num

UART ajustar y preguntar

Tabla 3.2 Comando AT de UART (Comunicación serial) [26]

	Comando	Parámetros	Respuesta
Ajuste	AT+ UART=(rate),(num1)(num2)	Velocidad de transmisión (rate): 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600, 1382400 num1: bit de parada “0” 1 bit de parada; y “1” 2 bits de parada. num2: paridad. “0” no hay paridad; “1” hay bit de paridad.	OK
Pregunta	AT+ROLE?	NULL	+UART=(rate),(num1), (num2)

Ajustar y preguntar nombre

Ajustar el nombre

AT+NAME=(name)

Preguntar el nombre

AT+NAME?

Ajustar y preguntar contraseña

Ajustar contraseña

AT+PSWD=(password)

Preguntar contraseña

AT+PSWD?

Los módulos Bluetooth trabajan con una tensión de 3.3 VDC y los sensores del presente trabajo brindan 5VDC; por lo que se necesita una etapa reguladora de tensión que disminuya a la adecuada para los módulos.

A continuación se presenta el diagrama esquemático general (Fig. 3.17) del módulo Bluetooth.

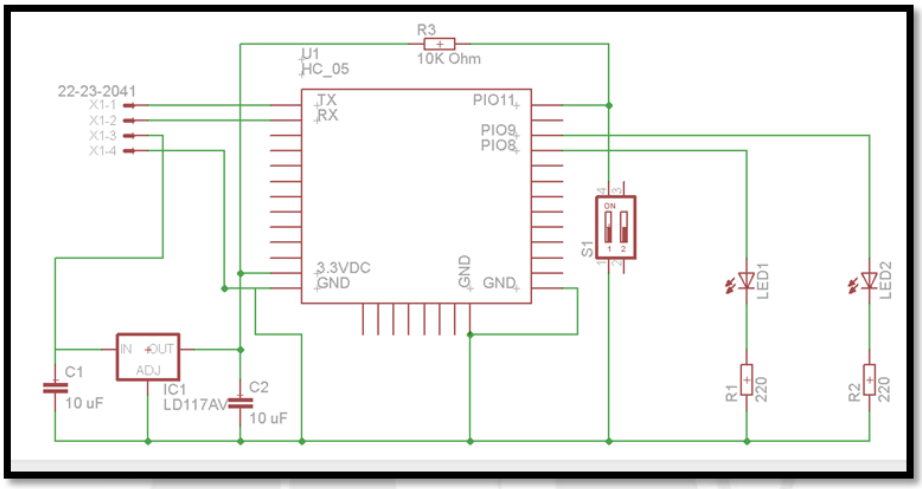

Fig. 3.17 Diagrama esquemático general del módulo Bluetooth

Los módulos (Fig. 3.18) que tienen la finalidad de mandar información a la central requieren de un código o una trama que es enviada a través de los puertos de transmisión del módulo, es por ello que, para generar una trama única por cada sensor, se utilizó un microcontrolador que cumple con lo requerido.

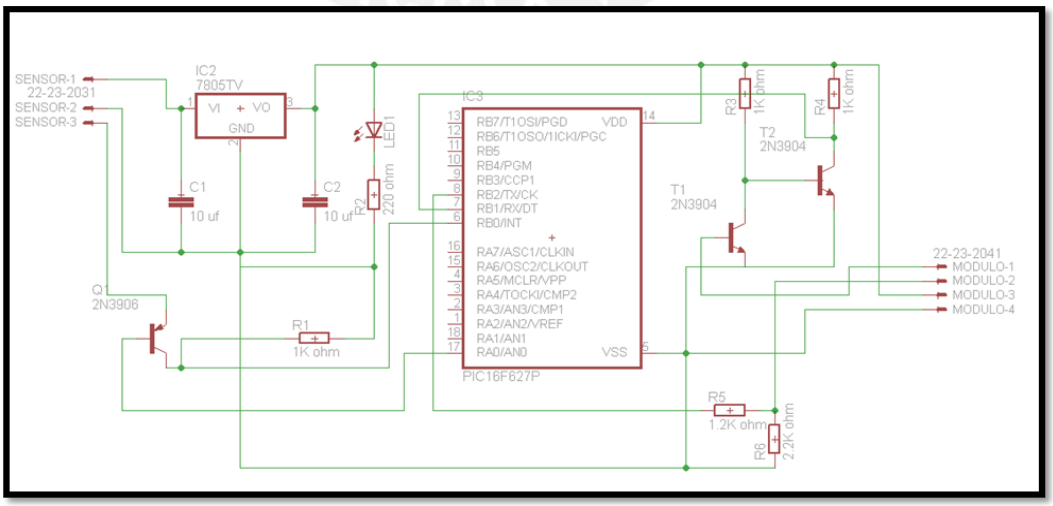

Fig. 3.18 Diagrama esquemático de transmisión de data con microcontrolador

3.2. Implementación del sistema

Como se ha señalado en el Capítulo 2, las zonas más vulnerables para el ingreso de personas indebidas se presentan por las ventanas, el patio, la lavandería, la puerta principal y de cocina; afectando principalmente los dormitorios, la sala – comedor y la cocina.

Según el diseño y dependiendo de las zonas inseguras se implementó lo siguiente:

Para los dormitorios, la detección del individuo por medios de sensores pasivos (PIR).

Para la sala comedor, la detección del individuo cuando ingresa por las ventanas, se realizará por medio de un sensor pasivo (PIR). La detección de ingreso por la puerta principal, de cocina y por la puerta cercana al patio se realizará por sensores magnéticos.

Para la cocina, la detección del individuo se efectuó por medio de un sensor pasivo (PIR) y para la apertura de la puerta se utilizará un sensor magnético.

Por lo tanto, dentro de la vivienda se implementaron cuatro sensores pasivos infrarrojos y tres sensores magnéticos.

Para tener una mejor perspectiva del sistema de seguridad, la implementación será dividida en 3 partes:

3.2.1. Implementación de sensores
3.2.2. Implementación de unidad de control
3.2.3. Implementación de alarma

3.2.1. Implementación de sensores

Dentro de esta implementación se mostrarán las 3 etapas principales:

- Acoplamiento del sensor para trabajar a baja tensión continua.

En la figura Fig 3.19 se muestra la tarjeta de fuente de alimentación para el sensor.

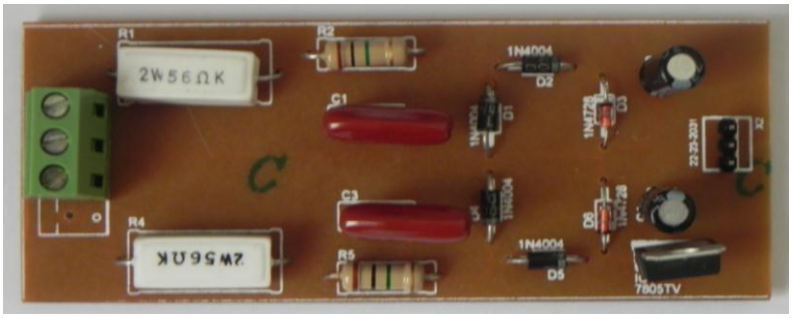

Fig. 3.19 Tarjeta de la fuente de alimentación para el sensor

- Generación de trama para la transmisión de la información.

En la siguiente figura (Fig. 3.20) se aprecia la tarjeta generadora de trama de datos.

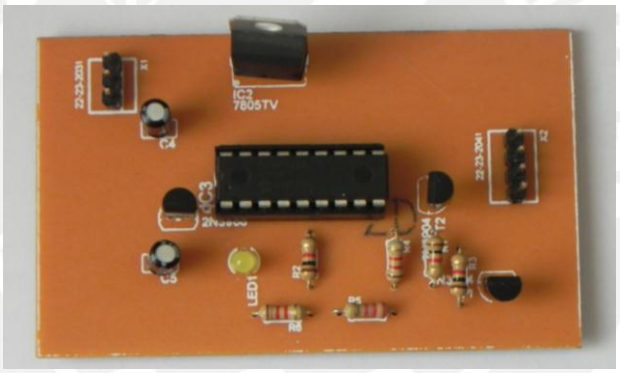

Fig. 3.20 Tarjeta de generación de trama

- Módulo de transmisión.

A continuación se observa la figura Fig 3.21 que es la tarjeta de del módulo bluetooth.

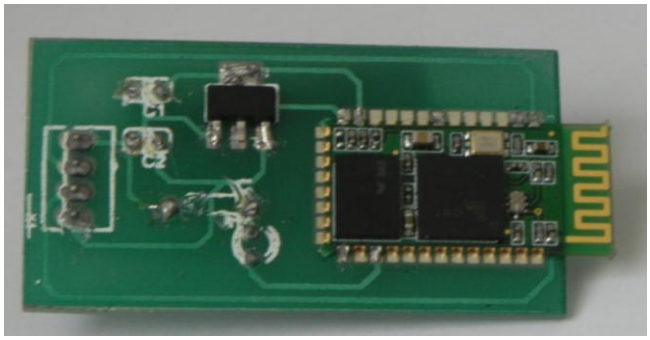

Fig. 3.21 Tarjeta de transmisión

3.2.2. Implementación de sistema de control

Dentro del sistema de control se aprecian 3 etapas:

- Unidad de control.

En la figura Fig. 3.22 se muestra la tarjeta de la unidad de control o central con sus respectivos componentes de interfaz.

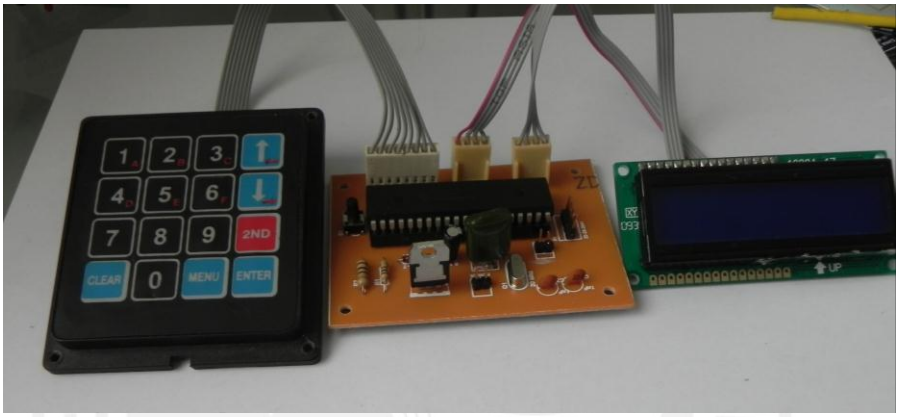

Fig. 3.22 Tarjeta de sistema de control

- Módulo de transmisión.

En la siguiente Figura (Fig 3.23) se aprecia la tarjeta del módulo Bluetooth

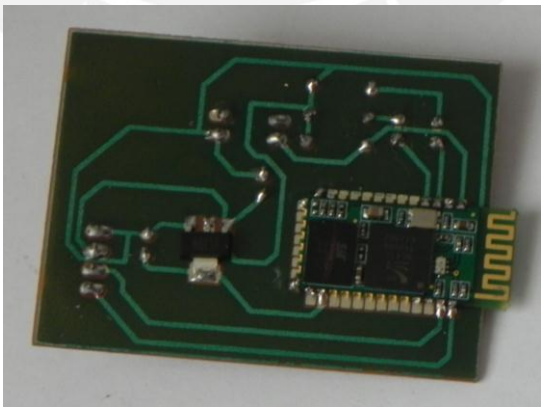

Fig. 3.23 Tarjeta de transmisión de control

- Fuente de poder para el sistema de control.

A continuación se observa en la figura Fig 3.24 la tarjeta de la fuente de energía de la unidad de control.

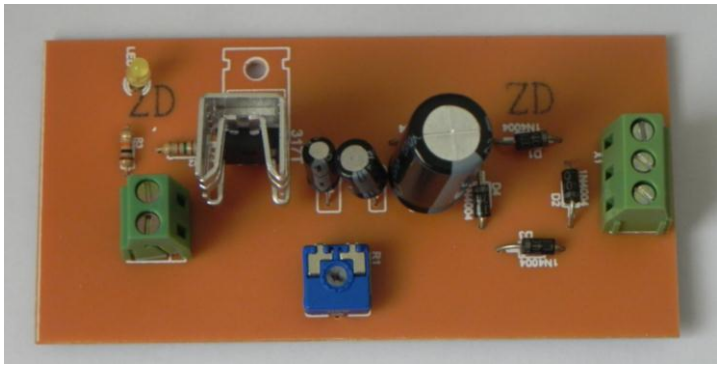

Fig. 3.24 Tarjeta de fuente de poder

3.2.3. Implementación de alarma

Como la alarma (sirena) va a ser instalada cerca del sistema de control, esta implementación consta básicamente del circuito de generación de frecuencias para la activación de la alarma que se aprecia en la siguiente figura (Fig.3.25).

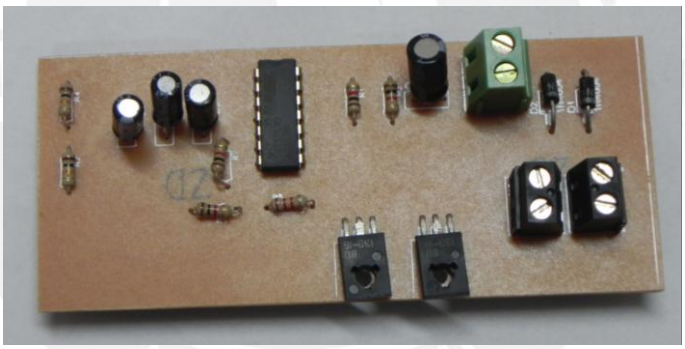

Fig. 3.25 Tarjeta de generación de frecuencia para alarma

CAPÍTULO 4

PRUEBAS Y RESULTADOS

Las pruebas de la implementación del proyecto de tesis se realizaron por etapas.

4.1. Prueba de la etapa de los sensores

En esta etapa se distinguen básicamente dos partes:

4.1.1. Prueba de la tarjeta del sensor

El sensor pasivo infrarrojo tuvo en su interior un sistema de retardo para la activación, es decir una vez que detectó a la persona, se demoró aproximadamente 5 segundos e inmediatamente generó un cambio de estado que llegó a la tarjeta de emisión de trama. Este cambio de estado fue activado en un determinado tiempo de acuerdo a la configuración que se deseó, de los cuales los más comunes fueron: 5 segundos, 10 segundos ó 15 segundos. Para las pruebas del sensor se realizaron 5 mediciones respecto a cada tiempo establecido.

Tabla 4.1 Tabla de muestras a 5 segundos

Nro. Prueba	Tiempo deseado	Tiempo real	Error (%)
1	5	5.5	10
2	5	5.2	4
3	5	5.4	8
4	5	5	0
5	5	5.2	4
Promedio	**5**	**5.26**	**5.2**

Tabla 4.2 Tabla de muestras a 10 segundos

Nro. Prueba	Tiempo deseado	Tiempo real	Error (%)
1	10	10.8	8
2	10	11.2	12
3	10	10.4	4
4	10	11	10
5	10	10.9	9
Promedio	**10**	**10.86**	**8.6**

Tabla 4.3 Tabla de muestras a 15 segundos

Nro. Prueba	Tiempo deseado	Tiempo real	Error (%)
1	15	16	6.66
2	15	15.5	3.33
3	15	15.3	2
4	15	15.7	4.6
5	15	16.5	10
Promedio	**15**	**15.8**	**5.3**

4.1.2. Etapa de transmisión de datos

Una vez que el sensor activó un microcontrolador, transformó la señal de activación por parte del sensor y la envió a través del módulo bluetooth. Para esta etapa se realizaron 10 pruebas y se detallarán los resultados en la siguiente tabla.

Tabla 4.4 Tabla de transmisión de dato

Nro. Prueba	Correcto	Incorrecto	Detalles
1	X		Bien
2	X		Bien
3		X	No envió la información deseada
4	X		Bien
5	X		Bien
6	X		Bien
7	X		Bien
8	X		Bien
9	X		Bien
10	X		Bien
11	X		Bien
12		X	No envió la información deseada
13	X		Bien
14	X		Bien
15	X		Bien
16	X		Bien
17	X		Bien
18	X		Bien
19	X		Bien
20	X		Bien
Porcentaje de error (%)	10		

4.2. Prueba del sistema de control

En esta etapa el controlador se encargó de recibir y analizar la trama de información que fue enviada por los sensores, mientras la señal tenía la información correcta, el controlador realizó la activación de la alarma.

Tabla 4.4 Tabla de recepción de la información

Nro. Prueba	Correcto	Incorrecto	Detalles
1	X		Bien
2	X		Bien
3		X	No recibió la información deseada
4	X		Bien
5	X		Bien
6		X	No recibió la información deseada
7	X		Bien
8	X		Bien
9	X		Bien
10	X		Bien
11		X	Recibió dos veces la información
12	X		Bien
13	X		Bien
14	X		Bien
15	X		Bien
16	X		Bien
17	X		Bien
18	X		Bien
19	X		Bien
20	X		Bien
21	X		Bien
22	X		Bien
23	X		Bien
24	X		Bien
25	X		Bien
26	X		Bien
27	X		Bien
28	X		Bien
29	X		Bien
30	X		Bien
Porcentaje de error (%)	10		

La unidad de control también es encargada de activar el sistema, es decir al inicio el sistema se encontrara en estado suspendido o apagado, que luego de ingresar una contraseña se podrá activar los sensores y se inicializará el sistema de seguridad.

4.3. Prueba de la alarma

Una vez transmitida la información del sensor, el sistema de control analizó si se activó o no la alarma. Cuando la alarma se activó, ésta tuvo que generar un sonido de alerta que fue en frecuencias de 4000Hz y 500Hz para obtener un sonido ruidoso que llamó la atención de las demás personas, avisando el ingreso de un intruso.

4.4. Tabla de costos

Para poder expresar los costos se elaboró una tabla en donde se precisan los costos por unidad y el costo total del sistema.

Tabla 4.5 Tabla de costos del sistema

Material	Cantidad	Precio por unidad (S/.)	Precio total (S/.)
Sensor PIR	5	15	75
Sensor Magnético	2	18	36
Módulo Bluetooth	6	15	90
Estructura del tablero	1	14	14
Teclado Matricial	1	8	8
Display LCD 16x2	1	10	10
Circuito impreso en baquelita	18	6	108
Componentes para el circuito (resistencias, diodos,, etc)	1	30	30
Microcontrolador (Unidad central)	1	18	18
Microcontrolador (Envío de dato)	5	6	30
Pilas recargables	10	7	70
Sirena	1	20	40
Batería (Unidad central)	1	15	15
TOTAL			544

Para la implementación de este sistema de seguridad se generaron gastos que alcanzaron los 544 nuevos soles.

4.5. Consumo del Sistema

El cálculo de consumo de energía del sistema se realizó en las 3 etapas que se presenta: en el envío de datos, recepción de datos (unidad central) y actuadores o sirena.

Para la parte de envío de datos se calculó una potencia de 0.155 W por cada sensor, esto quiere decir que para nuestro sistema se requiere 0.775 W.
Para la parte de recepción de datos se calculó una potencia de 0.8 W.
Para la parte de los actuadores y sirena se obtuvo una potencia de 21W.
Por lo tanto se concluye que el sistema de seguridad tiene una potencia de 22.58 W aproximadamente.

CONCLUSIONES

- Se diseñó e implementó el sistema de seguridad inalámbrico con tecnología Bluetooth, en un departamento ubicado en el 3er piso de un edificio residencial en el distrito de La Molina – Lima; éste sistema alertará sobre la presencia o intento de ingreso a dicho inmueble, de sujetos no autorizados, mediante la activación de dispositivos de seguridad instalados en todas las zonas de posibles accesos.

- En esta tesis se aplicó tecnología existente con dispositivos electrónicos que se encuentran en el mercado nacional; lo que ha permitido la factibilidad del proyecto con la reducción del tiempo y de los costos para la implementación.

- En la etapa de acoplamiento, los resultados demuestran que se presentan errores mínimos. En relación a la configuración del tiempo, se ha visto que a mayor actividad del sensor (cuando se presenta la detección) existe mayor probabilidad de error en promedio; cuando el sensor está calibrado a 15 segundos nos brinda un 6.26% de error, mientras que en 5 segundos resulta 5.2%.

- En las tablas que describen la transmisión y recepción, también existen errores subsanables, con 12% en la emisión de data y 10% en la recepción. Esto ocurre por la falta de precisión en la calibración de los dispositivos entre sí; sin embargo, con la elaboración de más pruebas se reducirá el error.

- El sistema de seguridad diseñado, por sus características de operatividad de alcance mediano o pequeño y por lo económico en su implementación, puede ser requerido por un gran sector de la población en departamentos.

RECOMENDACIONES

Ante el posible porcentaje de error en la transmisión, se debe calibrar con más precisión los módulos de comunicación con el sistema de envío de datos, que es controlado por el microcontrolador.

Para la instalación de los sensores, se debe tener en cuenta el rango de alcance de los sensores PIR, debido a que existen diferentes sensores que poseen ángulos de alcance específico, por lo que unos deben ser colocados en las esquinas, mientras que otros en las paredes.

Se recomienda colocar el sistema de control en un lugar seco, para evitar algún daño del mismo; asimismo la instalación de este debe ser en un lugar donde solo los integrantes de la vivienda conocerán, permitiendo mayor grado de seguridad.

Para que el sistema comunique sobre algún evento o incidente dentro del domicilio, se debe incorporar un módem GSM, a través del cual se enviará mensajes de alerta o llamadas a nuestro celular.

Con la finalidad de mejorar el sistema implementado, se debe motivar el diseño de un software para los celulares capaces de interactuar con el sistema de seguridad, con aplicaciones de bloqueo y desbloqueo.

BIBLIOGRAFIA

[1] Seguridad Electronica *"Clasificacion de los sistemas de seguridad"*. Ecuador.

Disponible en:
<https://sites.google.com/site/seguridadelectronicagcm/capitulo-1/1-2-clasificacion-de-los-sistemas-de-seguridad-electronica>

[2] Escobar, Raúl Tomas. *Protección y seguridad personal, domiciliaria, comercial, electrónica. Contra robos, incendios, catástrofes.* Buenos Aires, 1988.

[3] Empresa Archiexpo "*Teclado numérico con lector de tarjeta de proximidad para control de acceso." Archiexpo*. España.

Disponible en:
<http://www.archiexpo.es/prod/samsung-security/teclados-numericos-con-lectores-de-tarjeta-de-proximidad-para-control-de-acceso-49923-325780.html>

[4] Networking Team. *CCTV*. Montevideo 2002.
Disponible en:
<http://www.networking-team.com/product/cctv/>

[5] Alarmas electrónicas

Disponible en:
<http://alarmasalfaperu.net/nuestros_productos.html>

[6] Prosegur. *Tecnología aplicada a la seguridad*. España

Disponible en:
<http://www.proseguractiva.es/productos_perimetral.php>

[7] Julio Muñoz G. *Sistemas de seguridad*. Madrid, 1995

[8] Empresa de ventas SoloStocks. Barcelona, España
Disponible en:
<http://www.solostocks.com/venta-productos/electronica/seguridad-defensa/camaras/camara-oculta-en-detector-en-pir-simulado-1-3-ccd-sharp-7335958>

[9] Cop-USA. Producto PIR. USA.
Disponible en:
<http://www.cop-usa.com/images/product/image/PIR_PDR.jpg>

[10] Sertek. Alarmas. Buenos Aires.2006.
Disponible en:
<http://www.sertek.com.ar/alarmas.html>

[11] Electrónica práctica. *Central de alarma con microprocesadores. Parte 1*. España, Septiembre 1994, p.51-58.

[12] Electrónica práctica. *Central de alarma con microprocesadores. Parte 2*. España, Octubre 1994, p.49-55.

[13] Horn, Delton T. *Electronic alarm and security systems: a technician's guide.* New York, 1995

[14] Grupo Segutelcom. *Seguridad Electrónica. Sensores contra robo e incendio.* Lima. Peru
Disponible en:
<http://www.gruposegutel.com/index-s-2.html>

[15] Sistemas de Alarmas. *Sistema de seguridad electrónica y automatización*. Buenos Aires, 2006.
Disponible en:
<http://www.sistemadealarmas.net/productos/>

[16] González, Juan José. *Bluetooth : conceptos básicos y nuevas soluciones*. España, Septiembre 2003.

[17] Seguridad mobile. *Arquitectura de protocolos de Bluetooth*. España, 2011.
Disponible en:
<http://www.seguridadmobile.com/bluetooth/especificacion-bluetooth/arquitectura-de-protocolo/index.html>

[18] Bray, Jennifer and Charles F. Sturman. *Bluetooth : connect without cable.* New Jersey, 2002

[19] Bluetooth. Acerca de la Tecnologia Bluetooth. USA, 2011.
Disponible en:

<http://www.bluetooth.com/Pages/Bluetooth-Home.aspx>

[20] Complete Higes Video Solution. Caracteristicas de productos. Ecuador 2009

Disponible en:
<http://mobotixecuador.com/productos.html>

[21] Istore. Caracteristicas del Módulo del sensor PIR. USA.
Disponible en:
<http://iteadstudio.com/store/index.php?main_page=product_info&products_id=5>

[22] Presentación Automatización Integral de Edificios. Generalidades Sobre demótica. España.
Disponible en:
<http://www.slideshare.net/guest0156897/sensores-domtica-3507287>

[23] Hoja técnica del Display de cristal líquido. LCD 16 x 2 Character. China.
Disponible en:
<http://www.dfrobot.com/image/data/FIT0127/datasheet.pdf>

[24] DISCA. Artículo sobre teclado matricial. España.
Disponible en:
<http://www.disca.upv.es/aperles/web51/modulos/teclado/index.htm>

[25] Microchip. *PIC16/17 microcontroller data book*.USA, 1995

[26] Lorenzi, Sergio. *Circuitos para Bluetooth.* Mundo electrónico. España, Noviembre 2002, p.74-77.