PONTIFICIA **UNIVERSIDAD CATÓLICA** DEL PERÚ

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE SEGURIDAD BASADO EN UNA RED ACTUADOR – SENSOR ZIGBEE CON SOPORTE EN LA WLAN DE UN EDIFICIO DE DEPARTAMENTOS

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

Roberto Iberico Acosta

ASESOR: Luis Ángelo Velarde Criado

Lima, setiembre del 2010

RESUMEN

Actualmente, los sistemas de seguridad para edificios de departamentos no han sido ampliamente adoptados, debido a los elevados costos de implementación y mantenimiento asociados, siendo el factor humano el más utilizado para prevenir y afrontar los diferentes tipos de incidentes que pudiesen ocurrir dentro de dichas instalaciones. Por otro lado, los dispositivos electrónicos usados para el monitoreo automático de los sistemas de seguridad, hacen que los residentes deban seguir ciertas reglas para el adecuado funcionamiento del sistema. Asimismo, es importante resaltar que, hoy en día, existe un gran número de viviendas que cuenta con redes locales inalámbricas y dispositivos compatibles con la tecnología Wi-Fi, capaces de interconectarse dentro de una WLAN.

En la presente tesis se realizará el diseño de un sistema de seguridad basado en una WLAN bajo la tecnología Wi-Fi para el control y monitoreo del sistema, así como el protocolo Zigbee para la interconexión inalámbrica de los sensores y actuadores. La solución integrará sensores de detección de movimiento, detectores de humo, alarmas contra robos e incendios, control de accesos y manejo de la iluminación de las instalaciones. Asimismo, se propone la selección y ubicación de los elementos del sistema considerando los costos y la distribución de los ambientes, para de este modo optimizar el área de cobertura.

De esta manera, se logró diseñar un sistema de seguridad, realizando la selección de los dispositivos y ubicándolos de manera eficiente dentro de un departamento. Asimismo, se diseñó una red actuador – sensor basada en el protocolo Zigbee, desde la cual se interconectarán los dispositivos finales a la WLAN de soporte. Finalmente, con el desarrollo de una aplicación, se realizó el control y monitoreo del sistema desde la red local basada en la tecnología Wi-Fi, enviando los comandos de control a un nodo de acceso, que actuaba como el enlace entre ambas redes, sin experimentar pérdida de información.

ÍNDICE

ÍNDICE DE TABLAS Y FIGURAS

INTRODUCCIÓN

La seguridad de la vivienda ha jugado un rol importante en la vida de las personas, es por esto que cada día más, los sistemas de seguridad vienen formando parte esencial del hogar. Hoy en día, estos sistemas se conforman de una combinación de medidas preventivas por parte de los usuarios, y de dispositivos electrónicos como controladores, sensores y actuadores, que permiten la detección de un incidente.

Actualmente, en nuestro medio, los sistemas de seguridad para edificios de departamentos representan unidades con bajos niveles de eficiencia e integración, siendo el factor humano el componente principal, el cual se encarga de vigilar las instalaciones y que, en la mayoría de las veces, no cuenta con las herramientas necesarias para prevenir y alertar un incidente.

Asimismo, los elementos internos de una vivienda como las instalaciones eléctricas y de gas son un peligro potencial para la seguridad en casa; del mismo modo, ocurren con los factores externos como la delincuencia. Sin embargo, es necesario tomar medidas preventivas frente a un incidente que pueda ser ocasionado por estos factores, y que pueda atentar contra la integridad física de las personas y producir pérdidas materiales. Es por esto que los sistemas de seguridad son una buena alternativa para prevenir grandes pérdidas causadas por estos incidentes.

Dado que los mecanismos y sistemas de seguridad implementados, hoy en día, cuentan con bajos niveles de eficiencia, debido al costo de los elementos adicionales. Entonces, el diseño de un sistema de seguridad, que cuente con sensores y actuadores interconectados inalámbricamente, que permitan detectar y alertar incidentes como intrusiones e incendios, y que a la vez, estos dispositivos sean controlados desde la red local inalámbrica previamente instalada en el departamento, es la solución más adecuada para resolver este problema.

En el presente trabajo, se desarrolla el diseño de un sistema de seguridad para edificios de departamentos, utilizando una WLAN (Wireless Local Area Network) bajo la tecnología Wi-Fi para el control y monitoreo, así como el protocolo Zigbee para la comunicación inalámbrica de los sensores y actuadores del sistema, generando así una solución con buenas características de eficiencia y flexibilidad.

CAPÍTULO 1: LOS SISTEMAS DE SEGURIDAD PARA EDIFICIOS DE DEPARTAMENTOS Y SU PROBLEMÁTICA

En la actualidad, los sistemas de seguridad para edificios de departamentos no han sido ampliamente adoptados, principalmente, debido al costo de implementación y mantenimiento que involucran. Por esta razón, la gran mayoría de residentes optan tan sólo por la vigilancia de una persona, para prevenir cualquier incidente que pueda afectar su seguridad y la de sus bienes.

Sin embargo, lo anterior, se contrasta con el alto índice de robos a viviendas, según datos de la Encuesta de Opinión en Lima Metropolitana sobre Temas de Seguridad realizado por la Pontificia Universidad Católica del Perú en el 2009. Por ejemplo, el 27% de encuestados afirma haber sido víctima de algún delito en el último año, siendo los robos a viviendas, el 20% del total de las situaciones [1]; del mismo modo, representa el cuarto problema que causa mayor preocupación en la ciudad de Lima, según datos de la encuesta de IMASEN sobre la Percepción Sobre la Seguridad Ciudadana del 2007 [2]. De esta manera, las personas se han visto en la obligación de instalar mecanismos de protección contra robos como seguros reforzados, rejas, etc., y en algunos casos sistemas de seguridad electrónicos provistos por diferentes empresas en el rubro, como ayuda a la vigilancia externa del edificio.

Estas soluciones cuentan con alarmas y sensores distribuidos por la vivienda. Por el contrario, ofrecen poca flexibilidad, puesto que no se adapta a las necesidades de cada usuario, ocasionando molestias, debido a las reglas que se deben tener en cuenta para el correcto funcionamiento de estos sistemas de seguridad.

Finalmente, los niveles de escalabilidad de este tipo de soluciones son bajos, puesto que si a largo plazo se decidiera realizar una mejora o expansión del sistema, se requeriría la actualización de la mayoría de los componentes, dado que la tecnología para entonces sería obsoleta o incompatible.

1.1. Análisis de la Situación Actual a Nivel Local

El sector construcción ha venido experimentando un crecimiento importante dentro del ámbito económico en los últimos años, según datos del INEI [3], proyectando las principales obras para edificios de departamentos. Este rápido crecimiento ha empezado a captar la atención de personas inescrupulosas, que aprovechando la

poca vigilancia en la mayoría de los edificios, se introducen en los departamentos para extraer las pertenencias de las personas que allí habitan.

Es por esto que los residentes se han visto obligados a instalar sistemas de seguridad contra robos que se encuentren a su alcance económico. Sin embargo, en muchos casos, estos sistemas no ofrecen una flexibilidad adecuada a la infraestructura, es decir, las soluciones no se adaptan a la distribución de ambientes de cada departamento dentro del edificio.

Por otra parte, los sistemas contra incendios significan una inversión adicional y, por lo general, no se encuentran integrados con otros sistemas disponibles en la vivienda, es por eso que, análogamente a un control remoto para cada equipo electrónico, éste debe contar con su propio controlador independiente, lo cual no es muy eficiente y confortable para los usuarios finales.

En la actualidad, en el Perú, no existe una normativa legal aprobada para los sistemas domóticos que automatizan la vivienda. Sin embargo, el Código Nacional de Electricidad tiene declarado algunas normas que se deben cumplir al momento de instalar sistemas de alarmas contra incendios y emergencias en general [4]. Asimismo, el Reglamento General de la Ley de Telecomunicaciones “establece que aquellos servicios cuyos equipos, utilizando las bandas de 902-928MHz, 2400-2483,5MHz y 5725-5850MHz transmiten con una potencia no superior a 100mW en antena (potencia efectiva irradiada), y no sean empleados para efectuar comunicaciones en espacios abiertos, están exceptuados de concesión alguna” [5].

1.2. Análisis de la Situación Actual a Nivel Global

En el contexto global, la seguridad de la vivienda ha sido un tema de mucha importancia para el desarrollo de las nuevas tecnologías. Es así que todo sistema domótico debe presentar características tales como flexibilidad, seguridad, ahorro energético y comunicación con el usuario final, para de esa manera cumplir con los estándares mundiales existentes hoy en día.

Actualmente, existen diferentes organizaciones internacionales que se encargan de publicar normas y recomendaciones para la correcta aplicación de los sistemas domóticos en general, incluyendo a los de seguridad como ISO, IEC, UIT, etc. [6]. Sin embargo, dichas normas se aplican según el criterio voluntario de las empresas

que proveen estas soluciones, con lo cual no permite una regulación obligatoria que asegure el correcto funcionamiento de los sistemas.

Finalmente, una de las principales características de toda vivienda con aplicaciones domóticas es la gestión de la energía de manera eficaz para contribuir a la protección del medio ambiente, ya que permite reducir significativamente las emanaciones de gases que contribuyen con el calentamiento global que las empresas generadoras de electricidad producen.

1.3. Problemática y Situación Actual de los Sistemas de Seguridad

En la actualidad, los sistemas de seguridad para departamentos generalmente involucran la vigilancia de una persona y cercos eléctricos instalados en los alrededores de los edificios. Sin embargo, el control de acceso en todo momento lo tienen los residentes y en algunas ocasiones el vigilante manualmente. Sin embargo, dentro de estos mecanismos de seguridad se reconocen algunas deficiencias que vuelven a este tipo de soluciones vulnerables frente a cualquier incidencia. De esta manera, se pueden identificar los siguientes puntos de vulnerabilidad dentro del flujo normal de acciones para cualquier incidente.

- Los incidentes son detectados por la persona encargada de la vigilancia. En caso contrario, la persona no los haya detectado, la incidencia sigue su curso, originando en el mejor de los casos sólo pérdidas materiales.
- Al no contar con un sistema automático de alerta, cualquier incidente podría eventualmente pasar desapercibido, lo cual significa un peligro inminente para el bienestar de las personas que allí habitan.
- Los métodos para controlar un incidente, generalmente incluyen la intervención de la persona encargada de la vigilancia, arriesgando así su seguridad física, al no encontrarse totalmente capacitada para estas tareas.

CAPÍTULO 2: ASPECTOS TEÓRICOS Y ANTECEDENTES DE LOS SISTEMAS DE SEGURIDAD

2.1. El Estado del Arte

2.1.1. Presentación del Asunto de Estudio

El avance de la tecnología y la aparición de la domótica, ha generado el desarrollo de diferentes dispositivos como detectores de presencia, sensores de temperatura, detectores de humo, entre otros; así como controladores y actuadores que permiten integrar todos estos componentes en un solo sistema de seguridad eficiente, flexible y de bajo consumo de energía.

En la actualidad, los sistemas de seguridad para el hogar ofrecen una solución tecnológica de prevención ante situaciones como robos, incendios, fuga de fluidos, etc., y de esta manera, las personas pueden proteger, controlar y hasta monitorear sus hogares ante la presencia de un incidente.

Por otro lado, se busca que las redes domóticas sean seguras y confiables, con una baja tasa de transmisión y un reducido consumo de energía; y además, que no tengan un alto costo de inversión. A continuación, se presenta un análisis de las diferentes tecnologías existentes en el mercado que se emplean para aplicaciones en redes domóticas.

2.1.2. Estado de la Investigación

Actualmente, los sistemas de seguridad son implementados como redes de datos, que involucran componentes como controladores, encargados principalmente de gestionar las tareas de los dispositivos instalados en la red. Por otro lado, los sensores, se ocupan de enviar la información necesaria sobre el estado de la casa en todo momento. Por último, los actuadores son los encargados de recibir información por parte de los controladores y/o sensores para ejecutar los comandos solicitados por éstos.

Asimismo, dichos sistemas pueden ser configurados en tres tipos de arquitecturas. Los sistemas centralizados poseen un solo componente de control que se encarga de recibir y procesar toda la información que es enviada por los sensores y enviar órdenes hacia los actuadores. La ventaja de esta arquitectura está en que una vez instalado el controlador principal, todas las funciones del sistema pueden ser utilizadas, y además el costo del sistema es menor al contar con un único

dispositivo inteligente. No obstante, la desventaja que se presenta es que si el controlador principal falla, entonces todo el sistema dejará de operar, y además la inversión inicial es elevada, ya que se tiene que adquirir un dispositivo complejo, capaz de gestionar toda la red [7].

Por otra parte, los sistemas distribuidos tienen la capacidad de procesar la información en cada módulo de sensores y actuadores. La ventaja que posee esta arquitectura es el bajo costo inicial para implementar el sistema, y además la falla de algún componente no afecta a otros dispositivos del sistema. Sin embargo, la desventaja de estos sistemas está en que las expansiones son mucho más costosas que en los sistemas centralizados [7].

Por último, los sistemas mixtos tienen las características de ambas arquitecturas anteriores, es decir, involucran pequeños módulos con inteligencia propia, distribuidos por toda la red, capaces de controlar los componentes asociados a cada uno. Asimismo, involucran las ventajas y desventajas de ambos sistemas [7].

Las nuevas tecnologías han permitido el uso de diferentes medios de transmisión de datos para las redes domóticas. Es así que los fabricantes emplean medios cableados que transportan corrientes portadoras para aprovechar las líneas del cableado eléctrico instaladas en la vivienda y transmitir la información. Las señales codificadas se insertan desde algún punto del cableado eléctrico a muy baja potencia, para luego ser decodificadas por los respectivos receptores. De esta manera, se reduce la inversión de cualquier sistema a ser instalado, ya que no hay necesidad de adquirir el medio de transporte físico. Sin embargo, un problema que se presenta al utilizar la red eléctrica es el ruido que otros equipos eléctricos producen, afectando a cualquier sistema de seguridad de alta sensibilidad. Por este motivo es conveniente instalar filtros para disminuir la interferencia [8].

Por otro lado, los medios inalámbricos son una alternativa que brinda mucha flexibilidad en cuanto a la portabilidad de los componentes que integran las redes. La comunicación inalámbrica está siendo comúnmente desarrollada para trabajar en la banda de 2,4 GHz, debido a su libre uso en la mayoría de los países, y las bandas de 800 MHz y 900 MHz, para aplicaciones dentro de los Estados Unidos y Europa, respectivamente. No obstante, uno de los inconvenientes a que se enfrentan las tecnologías que emplean este medio, es la interferencia que se puede generar por otras tecnologías que operan sobre estas bandas de frecuencia. A

continuación, se presentan algunas tecnologías desarrolladas para sistemas domóticos en general.

a) Zigbee

Zigbee es un protocolo inalámbrico desarrollado por la Alianza Zigbee, de libre uso y está basado en el estándar IEEE 802.15.4, el cual ofrece una baja complejidad, consumo mínimo de energía, bajo costo de dispositivos, instalación y mantenimiento. Asimismo, soporta una alta densidad de nodos dentro de la red gracias a su direccionamiento de capa de red de 16 bits que permite manejar hasta 65536 nodos, ofreciendo alta flexibilidad, coexistencia con otras tecnologías de radiofrecuencia, transferencia segura de la información e incluso puede cubrir grandes áreas dependiendo de la topología usada por la red, soportando los tipos estrella, malla y árbol. En la figura 2.1, se muestran las diferentes capas que conforman este protocolo.

<table>
<tr><td>Aplicación/Perfiles</td><td>Definido por el usuario</td></tr>
<tr><td>Aplicación del Framework</td><td rowspan="2">Definido por la Alianza Zigbee</td></tr>
<tr><td>Capas de Red/Seguridad</td></tr>
<tr><td>Capa MAC</td><td rowspan="2">Definido por la IEEE</td></tr>
<tr><td>Capa Física</td></tr>
</table>

Figura 2.1. Modelo de capas de la tecnología Zigbee [9].

Zigbee opera en la banda libre de 2.4 GHz y en las bandas de 868/915 MHz. En la tabla 2.1, se presentan las características de transmisión del protocolo.

Tabla 2.1. Características de transmisión de Zigbee [9].

Frecuencia	Tasa de Transmisión	Alcance Máximo
868 MHz	20 Kbps	75 m
915 MHz	40 Kbps	75 m
2.4 GHz	250 Kbps	75 m

Asimismo, las redes Zigbee diferencian tres tipos de componentes. El coordinador Zigbee es el encargado de controlar toda la red y direccionar la información de los demás componentes, existiendo sólo uno dentro de cada red. Los routers Zigbee se encargan de interconectar los componentes que se encuentran fuera del alcance del coordinador, y los dispositivos finales Zigbee se ocupan de recibir las órdenes de su controlador y sólo son capaces de comunicarse con el coordinador o algún router Zigbee cercano [9].

b) Z-Wave

Z-Wave es un protocolo cerrado desarrollado por la compañía Zensys, de bajo ancho de banda, con comunicación half duplex, confiable para comunicación

inalámbrica en una red de control de bajo costo. El principal propósito de este protocolo es intercambiar pequeños mensajes de control entre los diferentes nodos.

El protocolo está conformado por cuatro capas. La capa MAC controla los datos que se envían inalámbricamente a través de radiofrecuencia; la capa de transferencia controla el transporte de las tramas; la capa de ruteo direcciona las tramas de la red y la capa de aplicación controla la carga de las tramas a ser transferidas. En la figura 2.2, se muestra la conformación de las capas correspondientes a Z-Wave.

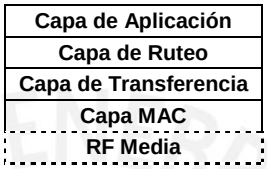


Figura 2.2. Modelo de capas de la tecnología Z-Wave [10].

Z-wave opera en las bandas 868/915 MHz para evitar interferencia con los equipos de comunicación dentro de la vivienda, que transmiten en la banda de 2.4 GHz. En la tabla 2.2, se presentan las características de transmisión del protocolo.

Tabla 2.2. Características de transmisión de Z-Wave [10].

Frecuencia	Tasa de Transmisión	Alcance Máximo
868 MHz	40 Kbps	75 m
915 MHz	40 Kbps	75 m

Zwave tiene dos tipos de dispositivos. Los controladores están encargados de enviar comandos a otros nodos y los esclavos se ocupan de ejecutar y replicar los comandos a nodos fuera de alcance del controlador.

Otra característica de este protocolo es el home ID y node ID. El primero es una identificación única de 32 bits que separa redes diferentes, es así que todos los controladores necesitan ser programados con su respectivo home ID y los esclavos serán programados por éstos. El node ID sirve para direccionar nodos diferentes dentro de una misma red [10].

c) INSTEON

Es una tecnología de baja complejidad desarrollada por SmartLabs, Inc., y cuenta con dispositivos de bajo costo. Utiliza el cableado eléctrico de la vivienda como medio físico para enviar la información a través de las corrientes portadoras. Asimismo, emplea ondas de radio como medio inalámbrico, y hasta incluso permite

aprovechar ambos medios para darle una mayor flexibilidad a los sistemas. Por otro lado, todos los componentes basados en INSTEON son capaces de transmitir, recibir o repetir otra información, realizando una comunicación punto a punto, y eliminando así la necesidad de contar con un controlador principal y complejo.

INSTEON ha sido diseñado para ser compatible con cualquier equipo que funcione bajo el protocolo X10 desarrollado por Pico Electronics y que fue muy utilizado en los primeros sistemas domóticos, puesto que la idea es que INSTEON sea el sucesor de éste, mejorando así la poca confiabilidad y flexibilidad de X10.

Los productos con esta tecnología se caracterizan principalmente por tener tiempos de respuesta rápidos, ser fáciles de instalar, simples de usar y confiables. Además, los dispositivos dentro de una red INSTEON pueden ser direccionados por el ID Code de 24 bits, que se asigna al momento de su fabricación.

Por otro lado, INSTEON está basado en las capas del modelo OSI, lo que representa buenas características de escalabilidad y eficiencia. En la figura 2.3, se muestran las capas del modelo OSI.

Capa de Aplicación
Capa de Presentación
Capa de Sesión
Capa de Transporte
Capa de Red
Capa de Enlace de Datos
Capa Física

Figura 2.3. Modelo de capas de la tecnología INSTEON [11].

La seguridad en las redes INSTEON se presenta en dos niveles. Por control de vinculación, que evita la creación de vínculos con redes externas y por encriptación, que permite una comunicación segura para las aplicaciones que así lo requieran. Asimismo, esta tecnología opera en la banda de 900MHz, de libre uso en los Estados Unidos. En la tabla 2.3, se presentan las características de las señales de radiofrecuencia para la transmisión de datos bajo la tecnología INSTEON [11].

Tabla 2.3. Características de transmisión de INSTEON sobre RF [11].

Frecuencia	Tasa de Transmisión	Alcance Máximo
904 MHz	2.88 Kbps	50 m

d) LonWorks

Es un protocolo abierto basado en el estándar ANSI/EIA 709.1 y fue desarrollado por Echelon Corporation, el cual inventó el Neuron Chip para ser instalado por cualquier fabricante en los equipos LonWorks como su componente principal. Asimismo, posee buenos niveles de eficiencia, confiabilidad y seguridad, utilizando una arquitectura descentralizada para ser implementada con dispositivos de bajo costo.

Esta tecnología provee una serie de servicios que permiten aplicaciones para intercambiar información sin la necesidad de conocer la topología de la red, los nombres, las direcciones o las funciones de los elementos que la conforman, proporcionando ventajas sobre la escalabilidad de los sistemas bajo esta tecnología.

Por otro lado, LonWorks es un protocolo que ofrece transmisión de datos punto a punto, basado en las capas del modelo OSI, lo que asegura la escalabilidad y eficiencia del estándar. En la figura 2.4, se muestran las capas del modelo OSI.

Capa de Aplicación
Capa de Presentación
Capa de Sesión
Capa de Transporte
Capa de Red
Capa de Enlace de Datos
Capa Física

Figura 2.4. Modelo de capas de la tecnología LonWorks [12].

No obstante, el modelo de comunicaciones es independiente del medio de transmisión, permitiendo a los dispositivos interconectarse sobre muchos medios físicos, tales como cable de par trenzado, cable coaxial, fibra óptica, líneas eléctricas, radiofrecuencia e incluso infrarrojo. En la tabla 2.4, se presentan las características de transmisión sobre cable de par trenzado.

Tabla 2.4. Características de transmisión de LonWorks en par trenzado [12].

Tasa de Transmisión	Alcance Máximo
1.25 Mbps	125 m

Otra característica importante es que el protocolo soporta diferentes direccionamientos; es así que cada dispositivo cuenta con un Neuron ID, que es asignado al momento de su fabricación y un ID de dispositivo para ser identificado dentro de la red [12].

e) Wi-Fi

Es una tecnología de comunicación inalámbrica basada en el estándar IEEE802.11, que presenta mayor difusión en la actualidad, debido a su compatibilidad con los servicios de las redes de área local o LAN's. Es así que la mayoría de equipos de uso cotidiano como computadoras portátiles, celulares, PDA's, etc. poseen tarjetas de red inalámbricas compatibles con Wi-Fi, beneficiando la portabilidad y flexibilidad para la transferencia de información a través de la red.

Wi-Fi utiliza ondas de radio en las bandas de frecuencia de 2.4 GHz y 5 GHz como medio de transporte de datos. En la tabla 2.5, se presentan los protocolos basados en el estándar IEEE 802.11 más conocidos actualmente [13].

Tabla 2.5. Características de transmisión de protocolos IEEE 802.11 [13].

Protocolo	Frecuencia	Tasa de Transmisión
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz	100 Mbps

Wi-Fi es un estándar que ofrece transferencia de datos basada en las capas del modelo OSI, lo que asegura la escalabilidad y eficiencia del estándar. En la figura 2.5, se muestran las capas del modelo OSI.

Capa de Aplicación
Capa de Presentación
Capa de Sesión
Capa de Transporte
Capa de Red
Capa de Enlace de Datos
Capa Física

Figura 2.5. Modelo de capas de la tecnología Wi-Fi [13].

Asimismo, el estándar IEEE 802.11 proporciona tres mecanismos diferentes de cifrado para el transporte seguro de la información. WEP (Wired Equivalente Privacy) es un método de cifrado basado en el algoritmo RC4, que utiliza llaves de 64 bits para la encriptación de los datos, haciéndolo actualmente vulnerable debido a su baja complejidad. Por otro lado, WPA (Wi-Fi Protected Access) es un mecanismo de cifrado temporal que proporciona una encriptación más compleja con el protocolo TKIP (Temporal Key Integrated Protocol), utilizando un algoritmo del tipo hash. Por último, WPA2 o estándar IEEE 802.11i es el último mecanismo de cifrado adoptado por la Alianza Wi-Fi, el cual está implementado con un método complejo de cifrado conocido como AES (Advanced Encryption Standard), el cual

utiliza un bloque simétrico encriptado para procesar la información en bloques de 128 bits con llaves de diferentes longitudes [14].

2.1.3. Síntesis sobre el Asunto de Estudio

El actual desarrollo de nuevas tecnologías para el control domótico está generando soluciones con buenos resultados en cuanto a flexibilidad y eficiencia. Es así que cada vez más son los sistemas que incluyen componentes para la interconexión con Internet, con ayuda de dispositivos como gateways y routers ADSL inalámbricos, proporcionando un importante valor agregado para los usuarios finales.

Asimismo, la integración de muchos sistemas del hogar como entretenimiento, seguridad, iluminación, etc., se está volviendo una realidad, tal como menciona el estudio sobre las tendencias domóticas realizado por Fujitsu y Siemens, “El concepto del hogar digital ya está bien establecido y se está viendo impulsado hacia una única unidad en la que almacenar y desde la que se pueda acceder a todo el contenido del hogar digital” [15].

Finalmente, se está tomando mucha importancia a la conservación del medio ambiente, puesto que los fabricantes siguen innovando en nuevos dispositivos más eficientes, que cuenten con un manejo eficiente de la energía y reduzcan el uso de elementos que degradan la naturaleza.

2.2. Conceptualizaciones Generales

2.2.1. Sistemas de Seguridad

Son sistemas implementados para la protección de las personas e instalaciones ante cualquier acto, incidente o fenómeno que sugiera un tipo de peligro.

2.2.1.1. Elementos

a) Sensores

Son dispositivos que transforman magnitudes físicas o químicas, en magnitudes eléctricas que los controladores del sistema puedan interpretar y procesar [16].

b) Actuadores

Son dispositivos capaces de generar la fuerza necesaria para mover o actuar sobre algún elemento mecánico, de acuerdo a los comandos de control enviados por un controlador [16].

c) Controladores

Son los encargados de llevar el control del sistema, procesando la información enviada por los sensores o algún medio externo, para luego tomar una decisión y, finalmente, transmitir los comandos de control necesarios a los actuadores, y de esa forma modificar las variables del sistema [16].

2.2.1.2. Subsistemas

a) Sistema de Seguridad Contra Incendios

Estos sistemas están diseñados para alertar y proteger a las personas ante la presencia de fuego, ya sea con algún tipo de alarma, las cuales son activadas por detectores de humo o gas, permitiendo a los residentes tomar las medidas preventivas de evacuación. Asimismo, permiten minimizar los daños materiales de las viviendas, activando dispositivos para extinguir el fuego [7].

El componente principal de estos sistemas es el detector de humo, que está conformado por un dispositivo de detección de humo y una alarma, existiendo dos tipos de detectores de acuerdo al tipo de mecanismo de sensado. Los detectores ópticos poseen internamente una cámara donde se localizan perpendicularmente sin línea de vista el emisor y receptor de un haz de luz infrarrojo; de esta manera, al ingresar las partículas de humo, la luz se refracta hacia el emisor, provocando la activación de la alarma. Por otro lado, los detectores iónicos están compuestos de un elemento radiactivo ubicado cerca a una cámara abierta con dos electrodos polarizados, permitiendo que la radiación genere un pequeño flujo de corriente; de este modo, al ingresar partículas de humo, se reduce dicho flujo ocasionando la activación de la alarma. En la figura 2.6, se muestra el mecanismo de sensado de un detector óptico [17].

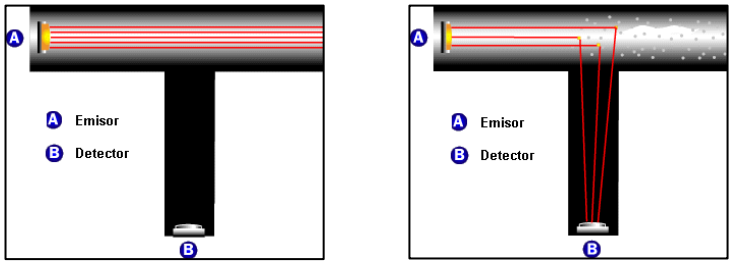


Figura 2.6. Mecanismo de sensado de un detector óptico [17].

b) Sistema de Seguridad Contra Robos

Estos sistemas están diseñados para alertar ante cualquier intento de intrusión de vivienda no deseado, haciendo uso de dispositivos como sensores de movimiento

dentro y fuera de la casa, sensores magnéticos para puertas y ventanas, y en ocasiones cámaras de vigilancia monitoreadas. Asimismo, los componentes para el control de acceso poseen medios de autentificación y son implementados para permitir el ingreso sólo a personas autorizadas [7].

El componente principal de estos sistemas es el sensor de movimiento, que está conformado por un mecanismo detección de movimiento y un dispositivo de alerta como una luz o un relé, existiendo tres tipos de sensores según el tipo de mecanismo de detección. Los detectores infrarrojos o PIR (Passive InfraRed sensor) utilizan un sensor que detecta la radiación que emiten los objetos, de esta manera, al detectar el calor emitido por una persona, se activará el mecanismo de alerta. Por otro lado, los detectores de microondas emiten pulsos de ondas, que al ser perturbados por un objeto en movimiento, ocasionará que se active el mecanismo de alerta. Finalmente, los detectores ultrasónicos emiten pulsos de ultrasonido con mucha precisión, que al ser reflejados en un objeto en movimiento, provocará que se active el mecanismo de alerta [18].

2.2.1.3. Elementos de Interconexión para el Control desde una WLAN

a) Gateway

Es un dispositivo de red que permite interconectar redes con protocolos y arquitecturas diferentes, siendo la tasa de transmisión un parámetro importante al momento de seleccionar uno, para no afectar la eficiencia de la red local [13].

b) Router ADSL Inalámbrico

Es un dispositivo que permite la comunicación inalámbrica entre los equipos de una red local Wi-Fi, proporcionando acceso a Internet a través de la línea telefónica mediante la tecnología ADSL. Asimismo, provee funciones de un gateway, generando una puerta de enlace para la conexión entre los elementos inalámbricos y los componentes de la red cableada local bajo el protocolo IP [13]. En la figura 2.7, se muestra un router ADSL inalámbrico en una red de área local con Internet.

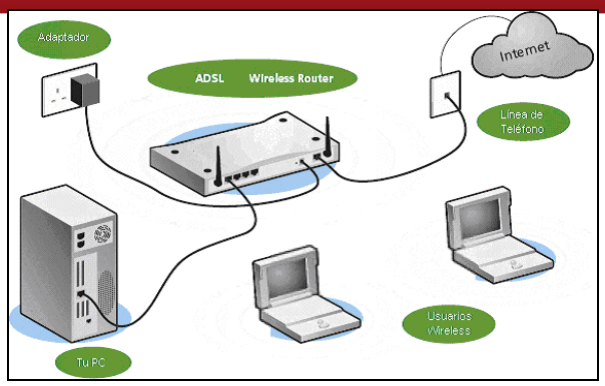


Figura 2.7. Router ADSL inalámbrico en una WLAN con Internet.

2.2. Modelo Teórico

Los nuevos sistemas de seguridad han evolucionado hacia tecnologías inteligentes, de bajo costo y con un alto grado de integración, que son capaces de adaptarse a las necesidades de cada usuario, generando así resultados con buenos niveles de eficiencia, flexibilidad y seguridad.

Para la implementación de esta solución, es importante conocer las características de los diferentes componentes que conforman un sistema de seguridad, como son los sensores y actuadores, puesto que el rendimiento del sistema dependerá del desempeño de estos dispositivos. Asimismo, es necesario estudiar las características de los dispositivos de transmisión inalámbrica que serán empleados en la red actuador – sensor, para conocer el alcance y eficiencia de las transmisiones. Por otra parte, dicho sistema debe incluir una red de soporte inalámbrica bajo el protocolo Wi-Fi, que permita el control y monitoreo desde un computador portátil compatible y/o servidor dentro de la red local, para lo cual será importante realizar un estudio del gateway a utilizar para interconectar las redes. Del mismo modo, la solución incluirá un sistema de respaldo de energía para preveer cualquier corte que pueda generar la desactivación del sistema.

Finalmente, el diseño de este sistema de seguridad debe buscar la integración de las tecnologías empleadas, la eficiente ubicación de los dispositivos dentro de los ambientes de los departamentos y el confort de las personas que allí residen, para de esa manera obtener óptimos resultados.

CAPÍTULO 3: DEFINICIÓN DE LAS CARACTERÍSTICAS DE LA WLAN DE SOPORTE Y DE LA RED ACTUADOR – SENSOR BASADA EN ZIGBEE SEGÚN LOS REQUERIMIENTOS DEL MEDIO

3.1. Hipótesis

3.1.1. Hipótesis Principal

Dado que los sistemas de seguridad para edificios de departamentos no han sido ampliamente adoptados, debido a los elevados costos de implementación y mantenimiento, siendo el factor humano el de mayor utilización al momento de prevenir los incidentes que pudiesen ocurrir dentro de estas instalaciones. Por otro lado, los dispositivos electrónicos que vienen siendo implementados en los sistemas de seguridad, hacen que los residentes deban seguir ciertas reglas para el correcto funcionamiento de éstos. Asimismo, actualmente, existe un gran número de viviendas que cuenta con redes locales inalámbricas, las cuales no vienen siendo aprovechadas para aplicaciones de seguridad dentro de edificios de departamentos. Entonces, el diseño de un sistema de seguridad inalámbrico, que integre sensores y actuadores, controlados desde un sistema de monitoreo automático, y que además pueda ser adaptado a la medida de la distribución de los ambientes del edificio, es la solución más adecuada para resolver este problema, debido al alto rendimiento que las nuevas tecnologías de comunicación pueden brindar en cuanto a eficiencia, flexibilidad, escalabilidad y accesibilidad del usuario desde cualquier dispositivo que sea compatible con la tecnología Wi-Fi, gracias al uso de mecanismos de traducción de protocolos entre la red domótica y la red local inalámbrica de las viviendas.

3.1.2. Hipótesis Secundarias

- Un sistema de seguridad basado en tecnologías para redes domóticas provee un alto grado de integración con otros sistemas como iluminación, entretenimiento, etc., si así fuera requerido por el usuario.
- Los dispositivos como sensores y actuadores electrónicos se caracterizan por tener una buena flexibilidad para adaptar su comportamiento según los requisitos de los usuarios.
- Para que los residentes puedan monitorear el sistema de seguridad, se deben incluir mecanismos de traducción de protocolos dentro del diseño del sistema, y de esa manera interconectar la red domótica con las redes locales del edificio.

3.2. Objetivos

3.2.1. Objetivo General

Diseñar un sistema de seguridad para un edificio de departamentos basado en una WLAN bajo la tecnología Wi-Fi para el control y monitoreo del sistema, así como el protocolo Zigbee para la interconexión de los sensores y actuadores, asegurando la escalabilidad y flexibilidad del mismo. La solución integrará sensores de movimiento, detectores de humo, alarmas contra robos e incendios, control de accesos y manejo de la iluminación de las instalaciones, que serán integrados para formar parte de los componentes del sistema como la seguridad contra robos, seguridad contra incendios, control de accesos y control de la iluminación, y asimismo un dispositivo de respaldo de energía.

3.2.2. Objetivos Secundarios

- Establecer los requerimientos del sistema de seguridad, según el área de cobertura y funcionalidades del mismo.
- Seleccionar los dispositivos para el sistema de seguridad, considerando costos, disponibilidad en el mercado y cumplimiento de los requisitos de diseño.
- Diseñar una red de sensores y actuadores basado en el protocolo Zigbee, que cuente con interconexión a una red local Wi-Fi para el control y monitoreo del sistema.
- Validar el funcionamiento del sistema de seguridad con pruebas y simulaciones.

3.3. Consideraciones para el Diseño del Sistema de Seguridad

3.3.1. Identificación de los Requerimientos del Sistema de Seguridad

Para el diseño del sistema de seguridad es necesario considerar los requerimientos del medio, teniendo en cuenta las funcionalidades que serán implementadas y la distribución de los ambientes en el interior de los departamentos para obtener la mayor cobertura dentro de los mismos. Asimismo, existen requerimientos intrínsecos a los sistemas domóticos, los cuales permiten evaluar los resultados obtenidos para dichas soluciones y que se detallan a continuación.

a) Flexibilidad

La flexibilidad del sistema de seguridad es muy importante para futuras modificaciones que puedan surgir dentro del mismo, es así que a largo plazo esta característica involucra en su mayoría modificaciones de los componentes físicos. Por otro lado, la flexibilidad a corto plazo toma en cuenta los cambios en las aplicaciones que controlan los dispositivos instalados en el sistema [7].

b) Comunicación

La comunicación dentro del sistema de seguridad es una de las características más importantes para el correcto funcionamiento de éste, puesto que dependerá de su disponibilidad para respaldar la adquisición de la información necesaria para el control de los dispositivos del sistema [7].

c) Seguridad

La seguridad del sistema es una característica intrínseca de la solución planteada, debido a que se debe tomar en cuenta la seguridad interna de la implementación, considerando que el control de las funciones estará siendo supervisado desde un equipo remoto inalámbricamente. Para esto es necesario habilitar mecanismos de encriptación para reducir la vulnerabilidad del sistema ante posibles ataques [7].

d) Consumo de Energía

El consumo de energía es una característica que viene tomando mucha importancia actualmente, debido a que la implementación de un sistema de seguridad automatizado requiere reducir el costo energético para de esa manera validar la inversión inicial por parte de los usuarios. Es por esta razón que el diseño de la solución debe integrar diversos componentes de bajo consumo de energía, para de esa manera reducir los costos operativos y contribuir con el medio ambiente [7].

3.3.2. Identificación de los Componentes del Sistema de Seguridad

a) Seguridad Contra Robos

El diseño de este componente integrará los sensores de movimiento, las alarmas sonoras y el control de la iluminación. Una vez activado el sistema, los sensores detectarán cualquier movimiento dentro del departamento y se encenderán luces como primer mecanismo de disuasión contra robos. Después de unos segundos, se verificará si los sensores continúan activados; de ser así se pasará al siguiente nivel, donde la alarma alertará a todos los que se encuentren en los interiores y alrededores del departamento.

b) Seguridad Contra Incendios

El diseño de este componente integrará los detectores de humo y alarmas sonoras. Al activarse el sistema, los sensores podrán detectar cualquier presencia de humo, con lo cual se procederá a activar la alarma, alertando a las personas en los alrededores. Después de unos segundos, se verificará si los detectores continúan activados y se enviará un mensaje de confirmación con el estado de los detectores.

c) Control de Accesos

El diseño de este componente integrará la cerradura eléctrica de la entrada a cada departamento y una base de datos incluida en el sistema de control, donde se registrarán diferentes códigos de acceso de acuerdo a la cantidad de miembros del hogar. Una vez activado el sistema, para ingresar a la vivienda, cada miembro deberá digitar su código en un teclado matricial que se encontrará en la parte externa del departamento y se validará dicho código en la base de datos. Si éste es correcto, la cerradura se abrirá automáticamente. Asimismo, se llevará el registro de todos los intentos, sean éstos válidos o no, permitiendo a los usuarios realizar consultas cuando así lo requieran.

d) Control de Iluminación

El diseño de este componente integrará la seguridad contra robos y parte de la iluminación de la vivienda. Es así que al activarse los sensores de movimiento, el sistema de control encenderá las luces de la sala y los pasadizos automáticamente como mecanismo de disuasión de intrusos, debido a que estas áreas comprenden las zonas comunes y se encuentran cerca de la entrada principal, siendo éste el punto de acceso más vulnerable.

3.3.3. Identificación del Edificio de Departamentos Donde Será Instalado el Sistema de Seguridad

Los sistemas de seguridad se instalarán en seis departamentos de un edificio de tres pisos, que cuenta con una escalera principal, la cual proporciona el acceso a cada uno de ellos. El interior de cada vivienda cuenta con una puerta de acceso principal que conduce directamente a la sala y áreas comunes. El segundo acceso conduce a la cocina y, asimismo, existe un pasadizo que comunica a las habitaciones y baños con las áreas comunes. De esta manera, los componentes del sistema de seguridad estarán ubicados en el interior de cada departamento y para efectos de diseño, se tomará en cuenta uno de éstos. En la figura 3.1, se muestra la vista de planta del departamento seleccionado ubicado en el tercer piso.

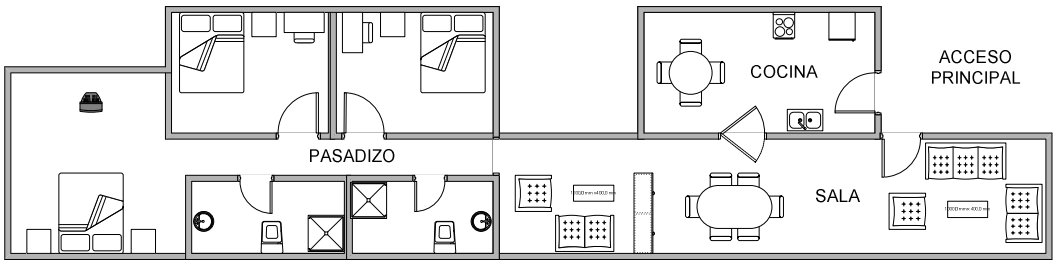


Figura 3.1. Vista de planta del departamento seleccionado ubicado en el tercer piso.

3.3.4. Coexistencia de Zigbee y Wi-Fi

Actualmente, la banda de 2.4GHz es compartida por diferentes tecnologías como Wi-Fi, Bluetooth y más recientemente Zigbee. Es por esta razón que, para asegurar un buen comportamiento, dichas tecnologías necesitan coexistir de manera pacífica y sin ningún tipo de interferencia que pueda perjudicar la comunicación de dispositivos con protocolos diferentes. Sin embargo, los diferentes niveles de potencia y según los canales utilizados por cada una de estas tecnologías, ocasionan que en situaciones específicas pueda existir interferencia.

Se han implementado algunas técnicas sobre Zigbee para disminuir el impacto por interferencia y de ese modo asegurar la coexistencia con otras tecnologías de comunicación. El estándar IEEE 802.15.4, que define la capa física y el control de acceso al medio del protocolo Zigbee, utiliza una modulación de espectro disperso, con lo cual se utiliza un ancho de banda mayor a lo necesario para la transmisión de información. Asimismo, dicho estándar divide la banda de 2.4GHz en 16 canales no traslapados, con un ancho de canal de 2MHz y una banda de guarda de 5MHz, de los cuales cuatro de ellos no se superponen a los canales más usados para tráfico Wi-Fi. En la figura 3.2, se observa que los canales 15, 16, 21 y 22 no se superponen a los comúnmente utilizados canales 1, 7 y 13 en los estándares IEEE 802.11b/g de la tecnología Wi-Fi.

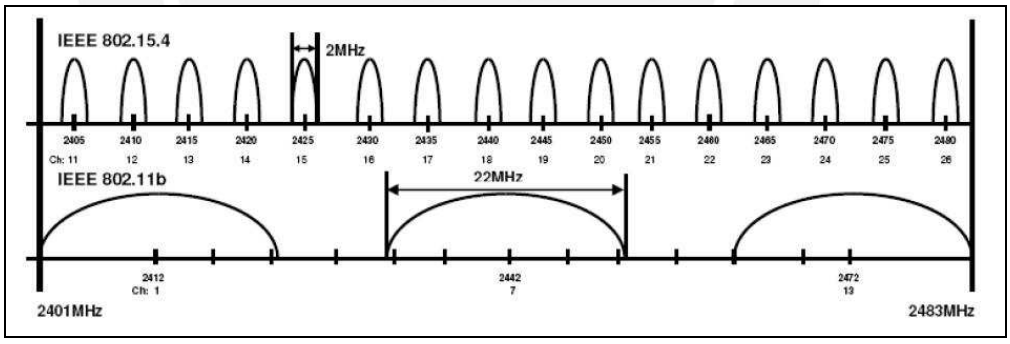


Figura 3.2. Interferencia de IEEE 802.15.4 y IEEE 802.11b/g [19].

Por otro lado, antes del establecimiento de una nueva red, los dispositivos Zigbee muestrean todos los canales y de esa manera pueden elegir el canal que presente menor interferencia. Del mismo modo, Zigbee incluye comandos de confirmación de los datos enviados por parte del receptor, por lo que la información es retransmitida hasta que se confirme la recepción sin errores. Por último, Zigbee es una tecnología diseñada bajo la topología tipo malla, con lo cual es posible transmitir los paquetes a través de múltiples rutas, en caso de que alguna de ellas no se encuentre disponible por interferencia. En la figura 3.3, se muestra el mecanismo que utilizan

los dispositivos basados en Zigbee implementados en una red tipo malla, los cuales automáticamente generan otra ruta al encontrar interferencia en alguno de los tramos de la red.

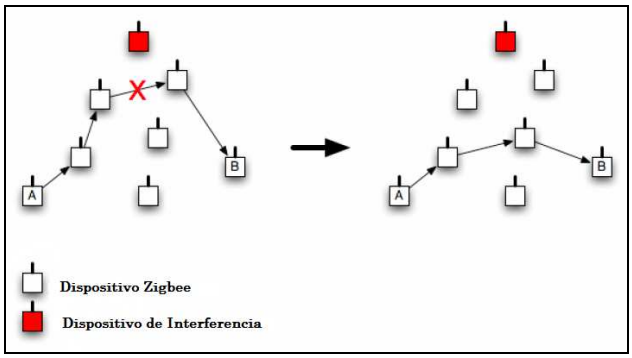


Figura 3.3. Topología tipo malla e interferencia [19].

Finalmente, del estudio realizado por la empresa Schneider Electric, se concluye que en presencia de aplicaciones reales sobre Wi-Fi; Zigbee puede operar satisfactoriamente sin experimentar pérdidas de paquetes. No obstante, en ocasiones se podría experimentar un incremento del retardo en la comunicación, debido al alto número de retransmisiones de los datos por parte de los dispositivos Zigbee [19].

3.3.5. Selección de los Protocolos de Comunicación

a) Protocolo de la Red de Soporte

La red de soporte será implementada bajo el protocolo Wi-Fi, puesto que actualmente existe un gran número de viviendas con redes locales inalámbricas configuradas bajo este protocolo. De esta manera, se podrá aprovechar este recurso para el control y monitoreo de los dispositivos que conforman el sistema de seguridad. Por otro lado, la implementación sólo tomará en cuenta los estándares IEEE 802.11b/g, debido a que la mayor parte de los equipos comercializados en nuestro medio trabajan en la banda de libre uso de 2.4GHz. Finalmente, el uso de Wi-Fi permitirá el acceso a la red desde cualquier dispositivo compatible, previamente registrado, ya que se encriptará la información dentro de la red con el tipo de seguridad conocido como WAP2 y tipo de encriptación AES, reduciendo de esa manera la vulnerabilidad de la red frente a un ataque.

b) Protocolo de la Red Actuador – Sensor

La red actuador – sensor será implementada bajo el protocolo Zigbee, debido a las características inalámbricas que posee sobre la banda de libre uso de 2.4GHz. De

esta manera, la coexistencia de este estándar con la tecnología Wi-Fi proporcionará la disponibilidad de comunicación en todo momento. Asimismo, la escalabilidad del protocolo permitirá realizar ampliaciones en el sistema de manera sencilla, sin importar la cantidad de nuevos dispositivos, gracias a su capacidad para manejar una alta densidad de nodos. Finalmente, el uso de Zigbee proporcionará un reducido consumo de energía y la transmisión segura de la información, puesto que los paquetes serán encriptados con el Estándar Avanzado de Encriptación o AES.

c) Protocolo de Interconexión de Redes

La interconexión entre el nodo coordinador Zigbee y el nodo de acceso a la WLAN de soporte será mediante comunicación serial asíncrona o UART (Universal Asynchronous Receiver/Transmitter), debido a que se encuentra ampliamente difundido para la transferencia de datos serialmente entre dispositivos electrónicos, proporcionando comunicación punto a punto de manera simple y eficiente. La versión menos compleja de comunicación a través de un puerto UART sólo necesita de tres líneas Tx., Rx. y línea común de tierra. Por otro lado, UART no proporciona señal de reloj, por lo que se requiere configurar ambos dispositivos con los mismos parámetros de velocidad, control de flujo, bits de datos, bit de paridad y bits de parada, para evitar errores que ocasionen la pérdida de información [20]. En la figura 3.4, se muestra la trama que conforma la comunicación serial asíncrona.

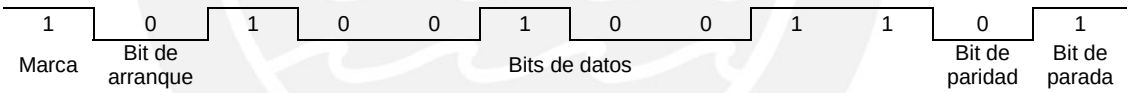


Figura 3.4. Trama que conforma la comunicación serial asíncrona.

3.3.6. Selección de los Dispositivos del Sistema de Seguridad

a) Módulos Zigbee

La red actuador - sensor requerirá que los módulos Zigbee sean de alta flexibilidad para modificaciones futuras y de bajo consumo, permitiendo el manejo eficiente de la energía. Por otro lado, dichos componentes deberán proporcionar una amplia cobertura para la comunicación eficiente dentro del área del departamento, permitiendo la coexistencia con otras tecnologías que puedan generar interferencia. Del mismo modo, se requerirá que los módulos Zigbee puedan realizar la adquisición de datos a través de puertos digitales, para leer el estado ON-OFF de los sensores y activación de los actuadores. Además deberán contar con un puerto UART que permita la comunicación serial entre el módulo coordinador y el módulo Wi-Fi, proporcionando la interconexión desde la red actuador - sensor hacia la

WLAN de soporte bajo la tecnología Wi-Fi. En la tabla 3.1, se presentan las especificaciones técnicas de algunos módulos Zigbee.

Tabla 3.1. Especificaciones técnicas de algunos módulos Zigbee.

Especificación	Xbee ZB	ZigBit Amp	MRF24J40MB
Fabricante	Digi	ATmel	Microchip
Tecnología	Zigbee	Zigbee	Zigbee
Frecuencia	2.4GHz	2.4GHz	2.4GHz
Tasa de Tx.	250kbps	250kbps	250kbps
Potencia de Tx.	17dBm	20dBm	20dBm
Voltaje DC	2.1-3.6V	3-3.6V	2.4-3.6V
Corriente de Rx.	40mA	23mA	25mA
Corriente de Tx.	40mA	50mA	130mA
Puerto Serial	UART	USART, SPI	SPI
DI/O	10	9	6
Precio (USD)	24.15	48.38	26.58

De esta manera, se seleccionarán los módulos Xbee ZB, debido a que cuentan con todos los requisitos antes mencionados para la implementación dentro del sistema de seguridad. Es así que poseen diez pines digitales y un puerto UART para la comunicación con otros dispositivos seriales. Asimismo, estos dispositivos se comunican en la banda ISM no licenciada de 2.4GHz y el protocolo Zigbee proporciona flexibilidad, seguridad y bajo consumo de energía a estos componentes. Finalmente, el costo de los módulos Xbee ZB es reducido y la Pontificia Universidad Católica del Perú actualmente cuenta con ellos, otorgando ventajas sobre la disponibilidad de los mismos para el desarrollo de la solución.

b) Módulo Wi-Fi

El módulo Wi-Fi deberá interconectarse con la WLAN de soporte bajo la tecnología Wi-Fi, la cual servirá para el monitoreo del sistema y, a su vez, generará los comandos de control para los diversos componentes que conforman la red actuador - sensor. De esta manera, este dispositivo deberá contar con una amplia cobertura, permitiendo la flexibilidad en cuanto a la ubicación del mismo. Asimismo, el módulo Wi-Fi deberá ser de baja complejidad para su fácil configuración, además de contar con los mecanismos de encriptación WEP, WPA y WPA2 para prevenir ataques, así como con un puerto UART para la comunicación serial con el módulo Xbee ZB coordinador. En la tabla 3.2, se presentan las especificaciones técnicas de algunos módulos Wi-Fi.

Tabla 3.2. Especificaciones técnicas de algunos módulos Wi-Fi.

Especificación	ConnectCore	Airborne	Secure Socket iWiFi
Fabricante	Digi	Quatech	Connect One
Tecnología	Wi-Fi	Wi-Fi	Wi-Fi
Frecuencia	2.4GHz	2.4GHz	2.4GHz
Tasa de Tx.	11Mbps (802.11b) 54Mbps (802.11g)	11Mbps (802.11b) 54Mbps (802.11g)	11Mbps (802.11b) 54Mbps (802.11g)
Alcance	45m	45m	45m
Voltaje DC	3.3V	3.3V	3.3V
Corriente Rx.	443mA	420mA	190mA
Corriente Tx.	554mA	620mA	260mA
Puerto Serial	UART	UART	UART
Encriptación	WEP, WPA, WPA2	WEP, WPA, WPA2	WEP, WPA, WPA2
Precio (USD)	414.00	89.00	56.00

De esta manera, se seleccionará el módulo Secure Socket iWiFi, debido a que cumple con todos los requisitos antes mencionados, siendo un dispositivo compatible con la tecnología Wi-Fi. Asimismo, cuenta con un alcance de hasta 45m en interiores y es posible configurarlo de manera rápida, con ayuda de la aplicación gratuita desarrollada por el fabricante. Del mismo modo, permite establecer conexión con las diversas WLAN sin importar el tipo de encriptación, debido a que posee compatibilidad con la mayoría de protocolos de seguridad. Por otra parte, este módulo posee un puerto UART, manejando niveles de voltaje de 3.3VDC, lo cual lo hace compatible para la comunicación serial con los módulos Xbee ZB. Finalmente, la Pontificia Universidad Católica del Perú ha adquirido este módulo para su uso en diferentes proyectos, proporcionando ventajas sobre la disponibilidad del mismo.

c) Microcontrolador

El microcontrolador es uno de los elementos del control de accesos, debido a que la lectura de los dígitos del teclado matricial tendrá que realizarse a través de ocho pines; cuatro de ellos serán configurados como entradas; y cuatro, como salidas. Asimismo, dichos dígitos ingresados deben ser incluidos dentro de una trama Zigbee para la comunicación entre los módulos Xbee ZB, por lo cual el microcontrolador deberá tener un puerto UART para la comunicación serial, manejando niveles de voltaje de 3.3VDC para ser compatible con los módulos Zigbee. En la tabla 3.3, se presentan las especificaciones técnicas de algunos microcontroladores.

Tabla 3.3. Especificaciones técnicas de algunos microcontroladores.

Especificación	ATmega8L	PIC16F873
Fabricante	ATmel	Microchip
Velocidad	0-8MHz	0-20MHz
Voltaje DC	2.7-5.5V	2.0-5.5V
Bits de Registros	8 bits	8 bits
Puertos Digitales	B,C,D	A,B,C
Puerto Serial	USART, SPI	USART, SPI
Precio (USD)	5.90	5.20

De esta manera, se seleccionará el microcontrolador ATmega8L, debido a que cumple con todos los requisitos antes mencionados. Es así que cuenta con dos puertos de 8 bits y un puerto de 7 bits, los cuales pueden ser configurados fácilmente como entradas y salidas. Del mismo modo, este dispositivo cuenta con un puerto serial USART configurable, manejando niveles de voltaje de 2.7VDC – 5.5VDC. Finalmente, el ATmega8L es un dispositivo de buena disponibilidad en el mercado local y, asimismo, los estudiantes de Ingeniería Electrónica estamos familiarizados con este dispositivo, por cursos previos dentro del plan de estudios.

d) UPS

El sistema de seguridad requerirá de un UPS como respaldo de energía para evitar desactivaciones ante un corte de energía [21]. De esta manera, el UPS deberá proveer una potencia mínima de 300W, necesaria para el funcionamiento de los principales elementos conectados a la línea eléctrica como los Xbee ZB, Secure Socket iWiFi, microcontrolador, computador, pantalla, y router ADSL inalámbrico. Asimismo, deberá contar con un mínimo de 6 conectores con voltaje de salida de 220-240VAC/60Hz. En la tabla 3.4, se presentan las especificaciones técnicas de algunos UPS.

Tabla 3.4. Especificaciones técnicas de algunos UPS.

Especificación	BR550GI	AVRX750U
Fabricante	APC	Tripp Lite
Voltaje AC	230V	230V
Frecuencia	50/60Hz	50/60Hz
Potencia	330W	450W
Conectores	6	6
Autonomía	9min	10min
Precio (USD)	133.42	143.93

De esta manera, se seleccionará el UPS BR550GI de APC, puesto que cuenta con los 6 conectores con un voltaje de salida de 230VAC/60Hz. Asimismo, provee una potencia superior a la requerida de 330W con una autonomía de 9 minutos. Finalmente, el costo de este dispositivo es reducido, en comparación con otros existentes en el mercado.

CAPÍTULO 4: DISEÑO DEL SISTEMA DE SEGURIDAD BASADO EN UNA RED ACTUADOR – SENSOR ZIGBEE CON SOPORTE EN LA WLAN DE UN EDIFICIO DE DEPARTAMENTOS

El diseño de la solución tomará en cuenta la distribución de los ambientes del edificio de departamentos elegido previamente. Sin embargo, este sistema de seguridad inalámbrico puede ser fácilmente adaptado a la mayoría de edificios, debido a la flexibilidad con la que cuentan los dispositivos que integran la solución. Asimismo, se tendrá en cuenta que actualmente existe un gran número de viviendas que tienen implementadas redes locales inalámbricas basadas en la tecnología Wi-Fi, con un área de cobertura igual o mayor a las áreas de descanso dentro de la residencia, como son la sala y las habitaciones, desde donde los usuarios acceden a los servicios proporcionados por dicha red.

La implementación del sistema de seguridad a menor escala para las pruebas servirá para la validación del funcionamiento de la misma, contando con la mínima cantidad de elementos para la correcta operación de la solución. No obstante, a esta pequeña implementación, podrá adicionarse un número mayor de elementos, gracias a la alta densidad de nodos que permite manejar el protocolo Zigbee, haciendo más eficiente el sistema respecto de las funcionalidades y los requerimientos del medio. A continuación, se detalla el proceso de diseño del sistema de seguridad, así como la validación de la implementación de la solución.

4.1. Diseño de la Red Actuador - Sensor

4.1.1. Consideraciones Preliminares

La red actuador - sensor contará con un módulo Xbee ZB configurado como coordinador, el cual se conectará mediante comunicación serial con el módulo Secure Socket iWiFi, que proporcionará acceso a la WLAN de soporte. Asimismo, se comunicará inalámbricamente con los demás módulos Xbee ZB configurados como router, que incrementarán el alcance de la red Zigbee.

El módulo coordinador establecerá la red actuador - sensor y enviará todos los comandos de control hacia los dispositivos finales del sistema, que son generados desde el servidor dentro de la WLAN. Por último, se debe tener en cuenta que todos los sensores y actuadores deben conectarse físicamente a los módulos Xbee ZB mediante tarjetas de acondicionamiento de señal, que permitan el manejo de niveles de voltajes de 3.3VDC con los que operan los módulos.

4.1.2. Diseño del Acondicionamiento de Señal de los Sensores y Actuadores

El diseño del acondicionamiento de señal de los sensores y actuadores, necesita tomar en cuenta los niveles de voltaje que corresponderán a los valores lógicos de activación y desactivación de éstos, debido a que los módulos Xbee ZB tomarán lectura del estado de los sensores y, asimismo, activarán los actuadores, operando con 3.3VDC para el nivel 1 lógico y 0VDC para el 0 lógico. A continuación, se describe el diseño de cada tarjeta para el acondicionamiento de los dispositivos finales que conforman el sistema de seguridad.

a) Acondicionamiento de Señal del Sensor de Movimiento

El sensor de movimiento para techos de la marca Visonic fue seleccionado para las pruebas, debido a que cuenta con un detector infrarrojo que permite un amplio rango de cobertura de 10.8m de diámetro a 3.6m de altura, lo cual permite monitorear espacios amplios en los departamentos. Asimismo, se tomó en cuenta su buena disponibilidad en el mercado. En la figura 4.1, se muestran las especificaciones técnicas del sensor de movimiento.

Fabricante	Visonic
Voltaje DC	9-15.5V
Tipo de Contacto	NC
Corriente de Alarma	100mA
Precio	$ 20.70

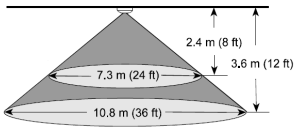


Figura 4.1. Especificaciones técnicas del sensor de movimiento [22].

El sensor de movimiento cuenta con una salida de un relé N.C. o normalmente cerrado, que se activa o desactiva, dependiendo del estado del sensor. Por otro lado, posee una entrada para la alimentación con un rango de 9VDC – 15.5VDC y una segunda salida de un relé N.C. TAMP que se activa manualmente con un interruptor ubicado en la parte superior del sensor, y que a su vez puede ser utilizado para efectos de prueba [22].

La tarjeta de acondicionamiento de señal del sensor de movimiento estará conformada por una compuerta lógica IC1 CMOS AND CD4081, la cual será alimentada por un regulador de voltaje de 3.3VDC IC2 LM1117. De esta manera, se garantizará la compatibilidad de los niveles lógicos con los módulos Xbee ZB, puesto que el circuito integrado CD4081 proporcionará voltajes lógicos de salida de GND y VDD. Asimismo, por recomendaciones del fabricante se adiciona una resistencia R1 de 1kΩ a la salida del relé N.C. para limitar la corriente a través de ésta. Finalmente, el bajo consumo de energía de los circuitos integrados basados en la tecnología CMOS, ayudará a prolongar la vida de la batería de 9VDC con la

cual se alimentará la tarjeta. En la figura 4.2, se muestra el diagrama esquemático y la tarjeta de acondicionamiento de señal del sensor de movimiento.

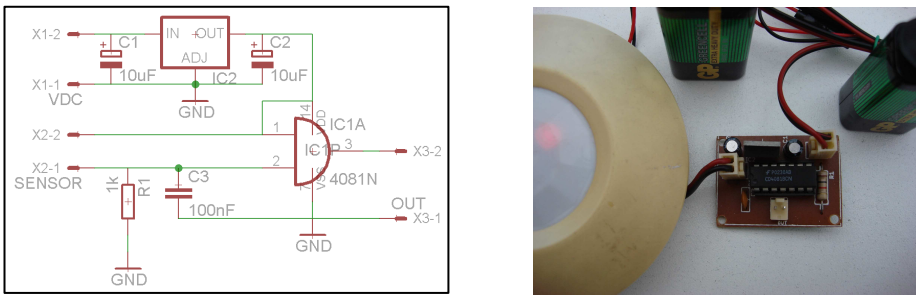


Figura 4.2. Tarjeta de acondicionamiento de señal del sensor de movimiento.

Durante las pruebas, la batería de 9VDC se conectará a la entrada VDC para energizar la tarjeta; asimismo, el relé N.C. estará conectado a la entrada SENSOR para detectar los cambios de estado. Finalmente, la salida OUT será conectada a una entrada digital del Xbee ZB para enviar los cambios al servidor del sistema.

b) <u>Acondicionamiento de Señal del Detector de Humo</u>

El detector de humo de la marca GE Security fue seleccionado, debido a que cuenta con un detector de calor y un sensor óptico con una sensibilidad de 3.1%, permitiendo detectar pequeñas partículas de humo. Asimismo, se tomó en cuenta su buena disponibilidad en el mercado. En la figura 4.3, se muestran las especificaciones técnicas del detector de humo.

Fabricante	GE Security
Voltaje DC	6-12V
Tipo de Contacto	NO
Corriente de Alarma	60mA
Precio	$ 13.18

Figura 4.3. Especificaciones técnicas del detector de humo [23].

El detector de humo cuenta con una entrada para la alimentación con un rango de 6VDC – 12VDC, y por otro lado posee una salida de un relé N.O. o normalmente abierto, que se activa o desactiva dependiendo del estado del detector [23].

La tarjeta de acondicionamiento de señal del detector de humo estará conformada por una compuerta lógica IC1 CMOS INVERSORA CD4069, la cual será alimentada por un regulador de voltaje de 3.3VDC IC3 LM1117. De esta manera, se garantizará la compatibilidad de los niveles lógicos con los módulos Xbee ZB, puesto que el circuito integrado CD4069 proporciona voltajes lógicos de salida de GND y VDD. Asimismo, por recomendaciones del fabricante se adiciona una resistencia R1 de 1kΩ a la salida del relé N.O. para limitar la corriente a través de ésta. Finalmente, el

bajo consumo de energía de los circuitos integrados basados en la tecnología CMOS, ayudará a prolongar la vida de la batería de 9VDC con la cual se alimentará la tarjeta. En la figura 4.4, se muestra el diagrama esquemático y la tarjeta de acondicionamiento de señal del detector de humo.

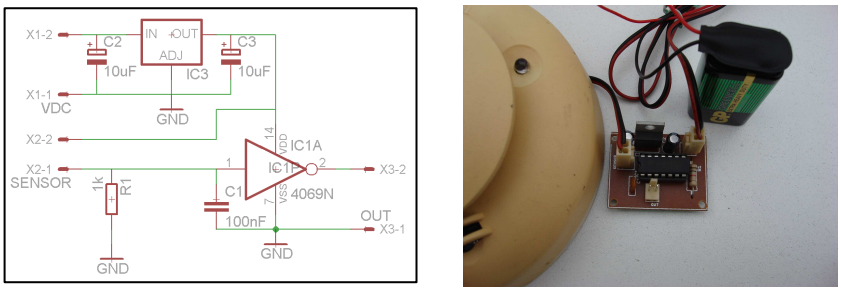


Figura 4.4. Tarjeta de acondicionamiento de señal del detector de humo.

Durante las pruebas, la batería de 9VDC se conectará a la entrada VDC para energizar la tarjeta; asimismo, el relé N.O. estará conectado a la entrada SENSOR para detectar los cambios de estado. Finalmente, la salida OUT será conectada a una entrada digital del Xbee ZB para enviar los cambios al servidor del sistema.

c) <u>Acondicionamiento de Señal de la Cerradura Eléctrica</u>

La cerradura eléctrica cuenta con una entrada de 12VAC para su activación o apertura. De esta manera, bastará aplicar un impulso eléctrico en la entrada de la cerradura para abrir la puerta.

La tarjeta de acondicionamiento de señal de la cerradura eléctrica estará conformada por un optoTRIAC MOC3021, que aislará la etapa de control de la etapa de potencia. En la etapa de control, el módulo Xbee ZB generará voltajes lógicos de salida de 0VDC y 3.3VDC para la activación de la cerradura, por esta razón se adiciona una resistencia en serie de 500Ω para limitar la corriente de activación del MOC3021. La etapa de potencia estará conformada por un TRIAC BTA08 de 8A, que se activa con el TRIAC interno del MOC3021 y dos resistencias de 360Ω para limitar la corriente en el “gate” del BTA08, y la alimentación será una fuente de 12VAC para activar la cerradura. Finalmente, se adiciona un circuito “snubber” de 39Ω y 10nF en paralelo con el BTA08, según recomendación del fabricante, con lo que se evita dañar el TRIAC con los sobrepicos de corriente que pueda generar la cerradura, debido a su equivalente circuito inductivo. En la figura 4.5, se muestra el diagrama esquemático y la tarjeta del circuito de activación de la cerradura eléctrica.

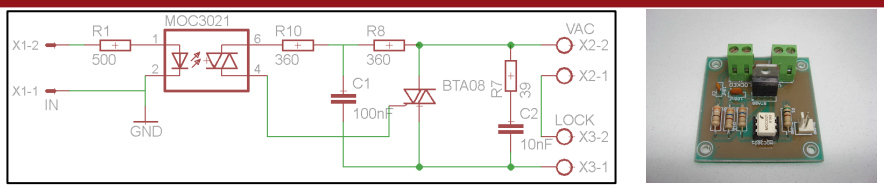


Figura 4.5. Tarjeta del circuito de activación de la cerradura eléctrica.

Durante las pruebas, una salida digital del Xbee ZB será conectada a la entrada IN para disparar el optoTRIAC desde el servidor. Por otro lado, la entrada VAC estará conectada a una fuente de 12VAC para energizar la cerradura y activarla. Finalmente, la salida LOCK se conectará a la cerradura eléctrica para activarla.

d) <u>Acondicionamiento de Señal de las Luces</u>

Para el encendido de las lámparas incandescentes de los departamentos, es necesario conectarlas manualmente a la línea eléctrica de 220VAC mediante un interruptor en serie. No obstante, en el diseño del acondicionamiento de señal para la activación de las luces, se reemplazarán dichos interruptores por un circuito conformado de un optoTRIAC MOC3021, que aislará la etapa de control de la etapa de potencia alimentada con la línea eléctrica de 220VAC para el encendido de las lámparas. En la etapa de control, el módulo Xbee ZB generará voltajes lógicos de salida de 0VDC y 3.3VDC para el encendido de las luces, por esta razón se adiciona una resistencia en serie de 500Ω para limitar la corriente de activación del MOC3021. La etapa de control estará conformada por un TRIAC BTA08 de 8A, que se activa con el TRIAC interno del MOC3021 y una resistencia de 360Ω para limitar la corriente en el "gate" del BTA08. Finalmente, en este diseño no es necesario incluir un circuito "snubber", debido a que estas lámparas tienen un equivalente circuito resistivo y no generan sobrepicos de corriente. En la figura 4.6, se muestra el diagrama esquemático y la tarjeta del circuito de activación de las lámparas incandescentes de los departamentos.

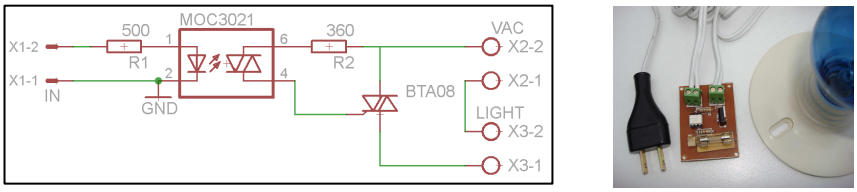


Figura 4.6. Tarjeta del circuito de activación de las lámparas incandescentes.

Durante las pruebas, una salida digital del Xbee ZB se conectará a la entrada IN para disparar el optoTRIAC desde el servidor. Por otro lado, la entrada VAC estará conectada a la línea eléctrica de 220VAC para energizar las lámparas cuando éstas

sean activadas. Finalmente, la salida LIGHT será conectada a las lámparas incandescentes para activarlas.

e) Acondicionamiento de Señal del Teclado Matricial

El teclado matricial cuenta con ocho pines de conexión, de los cuales cuatro corresponden a las columnas y cuatro a las filas. De esta manera la combinación de una columna con una fila proporcionará la ubicación exacta de cualquier botón presionado.

La tarjeta del acondicionamiento de señal del teclado matricial a través de la cual se insertará la clave de acceso, estará conformada por un microcontrolador ATmega8L, conectando los ocho pines del puerto B con los ocho pines del teclado matricial. La tarjeta será energizada con un adaptador de 9VDC conectado a la entrada VDC y los componentes serán alimentados por un regulador de voltaje de 3.3V LM1117, debido al nivel de voltaje con el que operan los módulos Xbee ZB. Los pines conectados a las filas del teclado matricial serán configurados como entradas en el microcontrolador, por esta razón se adicionarán resistencias de 10kΩ entre la conexión de los pines del puerto B y la salida del regulador de voltaje LM1117 para evitar la lectura de datos erróneos generados por ruido. Las columnas del teclado se conectarán directamente con los pines del microcontrolador configurados como salidas. Por otro lado, no se incluye ningún circuito “antirrebote” adicional para los pines configurados como entradas, debido a que cualquier “rebote” detectado en la lectura del teclado será eliminado internamente por software desde el microcontrolador, aprovechando así los recursos de este dispositivo. Asimismo, la conexión será directa para la comunicación UART entre el ATmega8L y el módulo Xbee ZB. En la figura 4.7, se muestra la conexión serial entre el ATmega8L y el módulo Xbee ZB, y en la figura 4.8; el diagrama esquemático y la tarjeta de acondicionamiento de señal del teclado matricial.

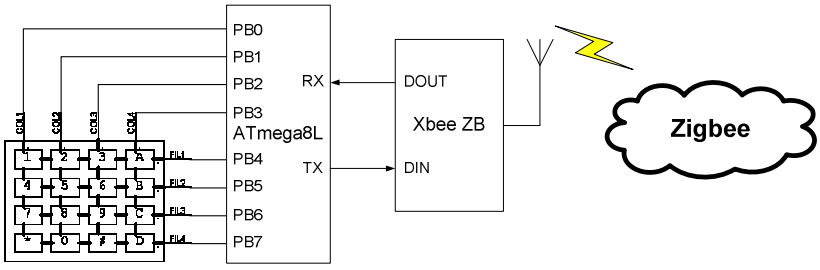


Figura 4.7. Conexión serial entre el ATmega8L y el Xbee ZB.

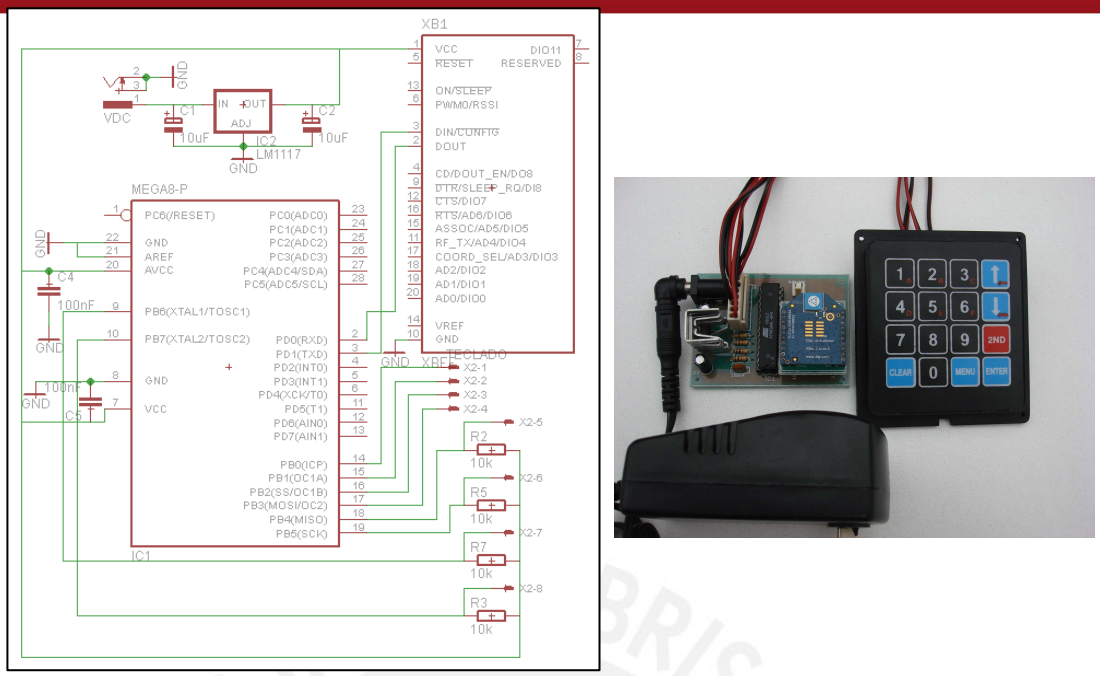


Figura 4.8. Tarjeta de acondicionamiento de señal del teclado matricial.

Se ha desarrollado un programa en lenguaje ensamblador, el cual se grabará en el ATmega8L y que se incluye en los anexos. Los números serán ingresados a través del teclado matricial y leídos desde el microcontrolador hasta que se presione la tecla ENTER; luego, se enviarán los datos en una trama Zigbee en formato hexadecimal al módulo Xbee ZB a través del puerto serial. Durante las pruebas, se configurará la velocidad de transmisión a 19200bps, puesto que es la mínima tasa con la que no se experimentó pérdida de paquetes. En la tabla 4.1, se muestra la trama Zigbee donde se incluirá la clave ingresada.

Tabla 4.1. Trama Zigbee para enviar datos a través del Xbee ZB.

Trama para enviar datos recibidos por el puerto UART									
7E	00 13	10	01	00 13 A2 00 40 54 41 72	00	00	00 00	05 06 07 08 7E	5A
Arranque	Longitud de Trama	Tipo de Trama	ID de Trama	Dirección de Destino de 64 bits	Radio de Broadcast (Máxima Cantidad de Saltos)	Opciones	Dirección de Destino de 16 bits	Datos a Enviar (Clave)	Checksum

4.1.3. Diseño del Nodo Coordinador de la Red Actuador - Sensor

La tarjeta donde se ubicará el nodo coordinador de la red Zigbee está conformada por un módulo Xbee ZB configurado como coordinador, el cual será alimentado por un regulador de voltaje de 3.3VDC LM1117. Asimismo, este dispositivo se conectará serialmente con el módulo Secure Socket iWiFi a través de sus pines DIN y DOUT conectados a borneras, proporcionando acceso a la WLAN de soporte. En

la figura 4.9, se muestra la conexión serial entre el módulo Xbee ZB coordinador y el módulo Secure Socket iWiFi, y en la figura 4.10, se muestra el diagrama esquemático y la tarjeta del módulo Xbee ZB coordinador.

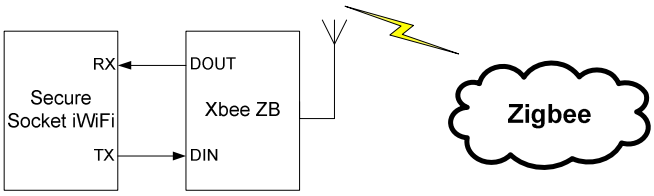


Figura 4.9. Conexión serial (UART) entre el Xbee ZB y el Secure Socket iWiFi.

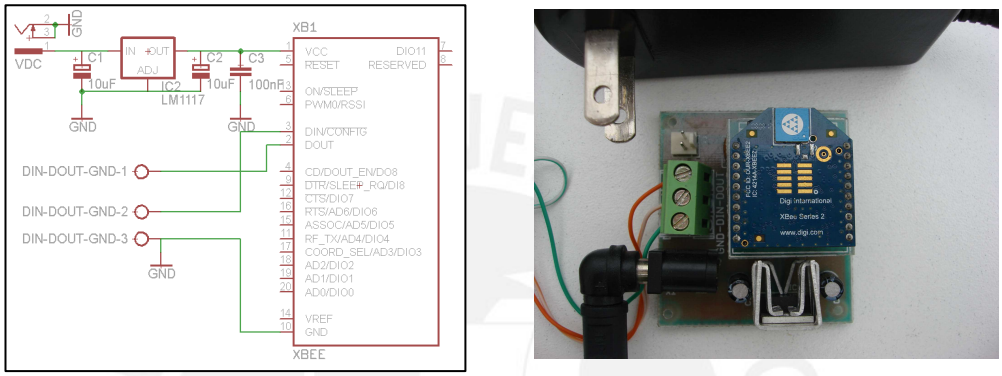


Figura 4.10. Tarjeta del nodo Zigbee coordinador.

Durante las pruebas, los pines DIN, DOUT y GND del Xbee ZB se conectarán con los pines de TX1, RX1 y GND del Secure Socket iWiFi, respectivamente. Por otro lado, la tarjeta del Zigbee coordinador se energizará con un adaptador de 9VDC conectado a la entrada VDC.

4.2. Diseño de la WLAN de Soporte

4.2.1. Consideraciones Preliminares

La WLAN de soporte estará conformada por la red local inalámbrica basada en el protocolo Wi-Fi e implementada en el departamento por el proveedor de Internet, como se muestra en la figura 4.11. En el nodo de acceso, se localizará el módulo Secure Socket iWiFi, el cual proporcionará acceso a la WLAN de soporte y establecerá la conexión con el servidor desde donde se realizará el control y monitoreo del sistema de seguridad. Es necesario tener en cuenta que cada departamento cuenta con un WLAN propia, es por esto que se implementará un sistema de seguridad independiente para cada vivienda, disminuyendo de esa manera la vulnerabilidad en la seguridad. Asimismo, cada WLAN tendrá una llave única basada en el cifrado AES de WPA2, garantizando la seguridad en la comunicación dentro de la red. Finalmente, el nodo de acceso se conectará

mediante comunicación serial con el nodo coordinador de la red actuador – sensor, manejando niveles de voltaje de 3.3VDC.

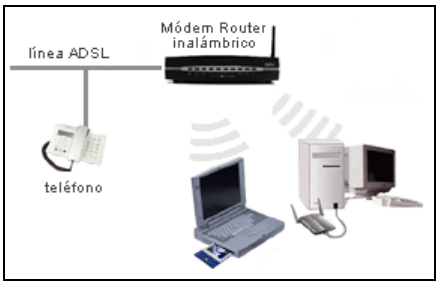


Figura 4.11. WLAN para hogar implementada por el proveedor de Internet [24].

4.2.2. Diseño del Nodo de Acceso de la Red Actuador – Sensor a la WLAN de Soporte

La tarjeta donde se ubicará el nodo de acceso a la WLAN de soporte estará conformada por el módulo Secure Socket iWiFi, el cual será alimentado con el regulador de voltaje de 3.3VDC LM1117. Asimismo, este dispositivo se conectará serialmente con el módulo Xbee ZB coordinador a través de sus pines de TX y RX conectados a borneras. No obstante, en caso dicha comunicación no requiera el uso de los pines CTS y RTS, éstos deberán ser cortocircuitados desde sus respectivas borneras por recomendaciones del fabricante. Por otro lado, se adiciona el integrado FT232RL de montaje superficial, que proporcionará un interfaz USB a serial (UART) para la programación del Secure Socket iWiFi a través del puerto USB de un computador. De esta manera, se deberá cambiar la ubicación de los jumpers a la salida de los pines TX, RX, CTS y RTS, para seleccionar entre comunicación con algún dispositivo serial externo o, en caso contrario, con un computador a través del puerto USB. También, se conecta un LED con una resistencia en serie de 330Ω al pin RF LED del módulo para conocer su estado de conectividad con la WLAN. Finalmente, se debe tener en cuenta que el FT232RL será alimentado por el mismo puerto USB, debido a su bajo consumo de energía. En la figura 4.12, se muestra la conexión serial entre el módulo Secure Socket iWiFi y el módulo Xbee ZB coordinador; y en la figura 4.13, el diagrama esquemático y la tarjeta del nodo de acceso a la WLAN de soporte.

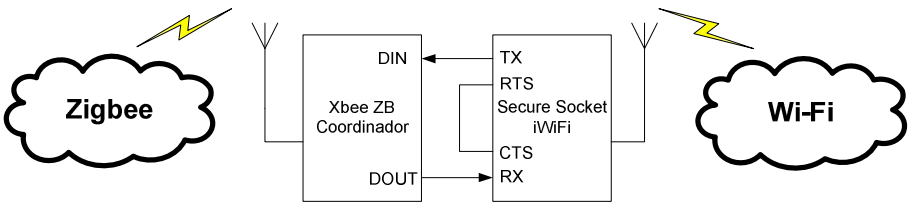


Figura 4.12. Conexión serial entre el Secure Socket iWiFi y el Xbee ZB coordinador.

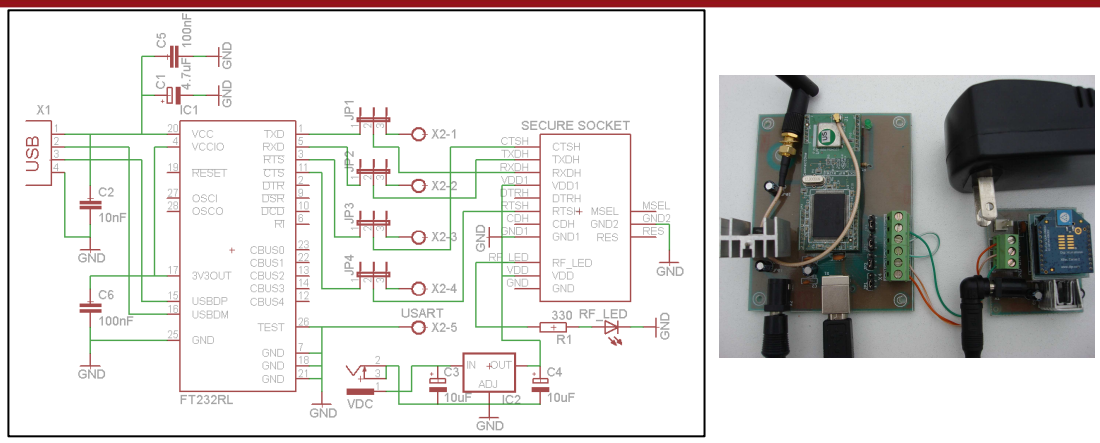


Figura 4.13. Tarjeta del nodo de acceso a la WLAN de soporte.

Durante las pruebas, los pines TX1, RX1 y GND del Secure Socket iWiFi se conectarán con los pines DIN, DOUT y GND del Xbee ZB, respectivamente. Por otro lado, se conectará un adaptador de 9VDC a la entrada VDC para energizar la tarjeta del nodo de acceso a la WLAN de soporte.

4.3. Interconexión de la Red Actuador – Sensor con la WLAN de Soporte

La interconexión de la red actuador – sensor con la WLAN de soporte se realizará mediante comunicación serial entre el nodo de acceso a la WLAN de soporte conformado por el Secure Socket iWiFi y el nodo coordinador donde se encuentra el módulo Xbee ZB coordinador, a través de borneras adicionadas a las respectivas tarjetas. Por otro lado, el Secure Socket iWiFi estará configurado en modo SerialNET para transmitir las tramas Zigbee de manera transparente y sin modificaciones. Asimismo, se debe tener en cuenta que la solución planteada incluye redes independientes para cada departamento, mejorando así la eficiencia de cada sistema de seguridad.

La red actuador – sensor basado en el protocolo Zigbee estará conformada por tres módulos Xbee ZB configurados en modo router para incrementar el alcance de los dispositivos dentro de la vivienda, y los puertos digitales configurados como entradas y salidas estarán conectados a los sensores y actuadores, respectivamente mediante tarjetas de acondicionamiento de señal. Por otro lado, el teclado matricial donde se digitará la clave para permitir el ingreso de las personas desde el exterior, estará conectado a un microcontrolador ATmega8L programado para recibir los dígitos ingresados e incluirlos en una trama Zigbee. De esta manera, todos los nodos router enviarán información al nodo coordinador y

viceversa, ya que éste será el encargado de transmitir todos los comandos de control del servidor.

Finalmente, los comandos de control y monitoreo automático serán generarados desde una aplicación desarrollada en Visual Basic 6.0, la cual se ejecutará en un computador de escritorio con sistema operativo Windows XP, que actuará como servidor del sistema, proporcionando la compatibilidad especificada por Microsoft. Del mismo modo, esta aplicación servirá como interfaz de usuario para control y monitoreo manual del sistema de seguridad. Por otro lado, se ha desarrollado en Visual Basic 6.0, una segunda aplicación que servirá únicamente para el monitoreo del sistema desde cualquier computador portátil con sistema operativo Windows XP en adelante. En la figura 4.14, se muestra el diseño de la interconexión de los elementos del sistema de seguridad.

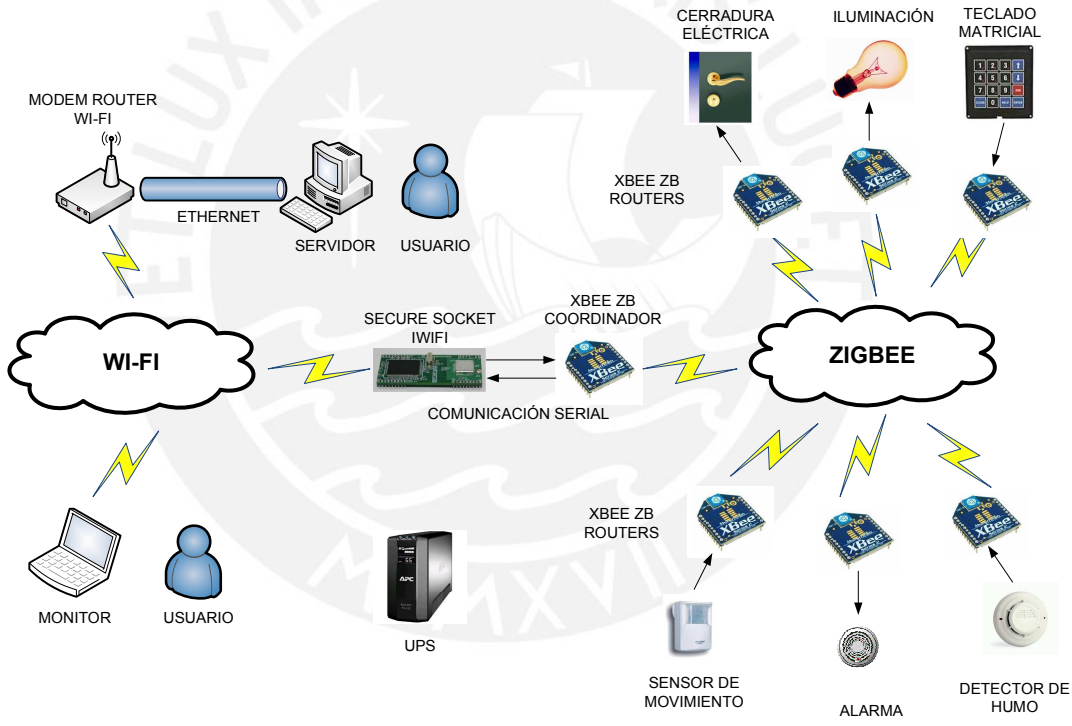


Figura 4.14. Diseño de la interconexión del sistema del seguridad.

4.4. Ubicación de los Dispositivos del Sistema de Seguridad

En primer lugar, se debe tener en cuenta que la mayor parte de los dispositivos que conforman el sistema de seguridad estarán localizados en el interior de cada departamento, debido a que cada vivienda contará con una red actuador - sensor independiente, y de esa manera otorgar mayor eficiencia y seguridad al interior de cada residencia. Asimismo, cabe resaltar que cada departamento cuenta con una

WLAN propia, lo cual proporciona aún mayor independencia para la implementación de la solución final de cada vivienda.

Un sensor de movimiento y un detector de humo estarán localizados en el pasillo de acceso a las habitaciones y en la sala principal de cada departamento, con lo cual se podrá monitorear las áreas de mayor vulnerabilidad en el departamento, debido al alcance de dichos sensores. Asimismo, se instalará un sensor de movimiento en la cocina para cubrir todos los puntos de acceso a la vivienda. Del mismo modo, se instalarán dos alarmas, una de ellas estará localizada en la cocina, por ser el lugar con mayor ocupación durante el día, y de esa manera se podrá tener una rápida respuesta por parte de los miembros del hogar. La segunda alarma estará ubicada en el pasillo de acceso a las habitaciones al igual que los sensores, ya que son los lugares de mayor estancia durante las noches.

Por otro lado, el control de la iluminación se realizará en las luces de la sala principal, debido a que en caso se detecte algún intruso, automáticamente éste pueda ser disuadido con el encendido de las luces principales. Sin embargo, el control de accesos estará dividido en dos etapas. La primera se conformará por el teclado matricial, el cual estará ubicado en la parte externa de la vivienda para el ingreso de las personas con sus respectivas claves y la segunda etapa conformada por la cerradura eléctrica, que a su vez será activada después de que la clave de acceso sea validada por la aplicación ejecutada en el servidor.

No obstante, el sistema de seguridad estará dividido en tres zonas, cada una de ellas contará con un módulo Xbee ZB configurado en modo router, para incrementar la capacidad de alcance dentro del departamento. La alarma, el detector de humo y el sensor de movimiento ubicados en el pasillo de las habitaciones estarán conectados al Xbee ZB de la primera zona. La segunda zona estará conformada por la alarma y el sensor de movimiento localizados en la cocina, la cerradura eléctrica de la puerta principal, el sensor de movimiento, el detector de humo y el control de iluminación que están localizados en la sala, y al igual que en la primera zona, éstos elementos del sistema estarán conectados a otro Xbee ZB router. El último Xbee ZB router, que conforma la tercera zona, sólo estará conectado con el teclado matricial que se encuentra en la parte externa de la vivienda, para de esa manera proteger ante cualquier tipo de sabotaje físico del hardware que pueda aperturar erróneamente la puerta principal.

Finalmente, el módulo Xbee ZB configurado como coordinador se encontrará ubicado a pocos centímetros del Secure Socket iWiFi, que proporcionará el acceso a la WLAN de soporte. Ambos estarán conectados físicamente y localizados en un punto intermedio de la vivienda, proporcionando una mayor cobertura para controlar a todos los dispositivos del sistema. En la figura 4.15, se muestra la vista de planta del departamento con la ubicación de cada dispositivo.

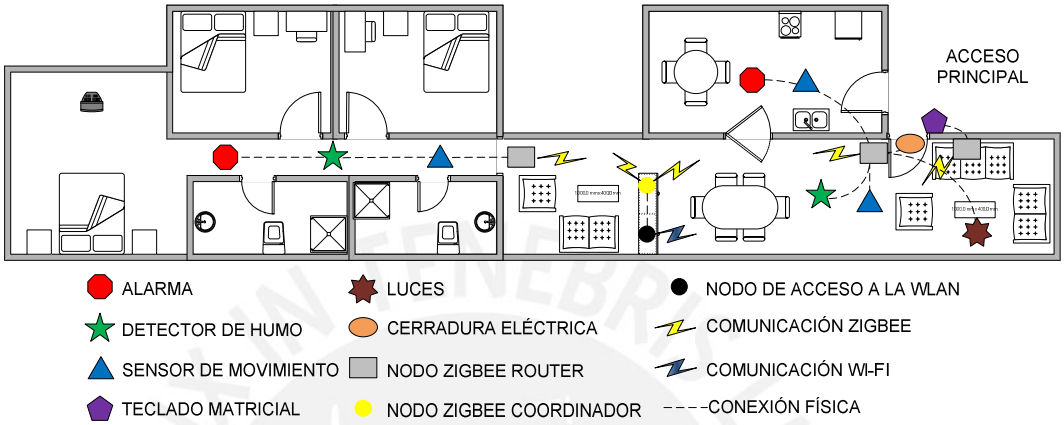


Figura 4.15. Vista de planta del departamento con la ubicación de los dispositivos.

4.5. Diseño del Interfaz de Usuario para el Control y Monitoreo del Sistema de Seguridad

El diseño del interfaz de usuario para el control y monitoreo del sistema de seguridad está basado en una aplicación Seguridad desarrollada en Microsoft Visual Basic 6.0. Se eligió este lenguaje de programación por su baja complejidad y flexibilidad para manejar los diferentes puertos de un computador con sistema operativo Windows XP en adelante. Esta aplicación será ejecutada en el servidor del sistema de seguridad desde donde se realizará el control y monitoreo automático del sistema. Por otro lado, se ha desarrollado una aplicación Monitoreo Portátil únicamente para el monitoreo, que podrá ser ejecutada en cualquier computador portátil que cuente con Windows XP en adelante. En este programa, sólo se recibirán mensajes de alerta cuando se detecte alguna incidencia y no se podrá realizar ningún tipo de control, para de esa manera evitar sabotajes en el sistema. Asimismo, estas aplicaciones se incluyen en los anexos.

Finalmente, una vez desarrolladas las aplicaciones en Visual Basic, será posible ingresar al programa Seguridad y Monitoreo Portátil, haciendo clic sobre los respectivos íconos ubicados en el escritorio. En la figura 4.16, se muestran las ventanas de interfaz de usuario de las aplicaciones Seguridad y Monitoreo Portátil.

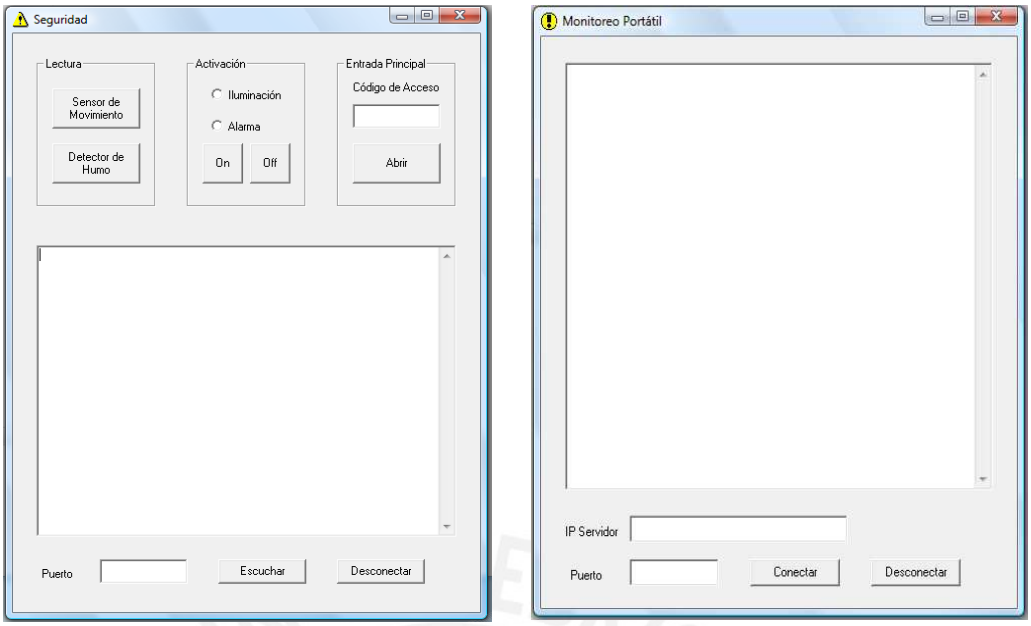


Figura 4.16. Interfaces de usuario de los programas Seguridad y Monitoreo Portátil.

4.6. Instalación de las Aplicaciones de Programación y Configuración de los Dispositivos Inalámbricos para las Pruebas del Sistema de Seguridad

Para el manejo de los dispositivos inalámbricos como el Xbee ZB y el Secure Socket iWiFi, es necesario contar con aplicaciones como el X-CTU y el iChip Config Utility, respectivamente. Estos programas gratuitos proporcionan una interfaz gráfica al usuario, permitiendo la fácil programación de los dispositivos desde cualquier computador que cuente con un sistema operativo compatible. A continuación, se detalla el procedimiento para la configuración de los módulos, y de esa manera interactuar eficientemente con ellos.

4.6.1. Configuración de los Xbee ZB con el X-CTU

Esta aplicación gratuita fue desarrollada por la compañía Digi y es compatible con Windows 2000 en adelante. A continuación, se detalla el procedimiento para la configuración del módulo Xbee ZB.

1. Descargar la aplicación de la dirección indicada e instalarlo.
   http://www.digi.com/support/productdetl.jsp?pid=3430&osvid=0&s=365&tp=5
2. Conectar el módulo de programación a un puerto USB del computador con el Xbee ZB montado sobre los sockets como se muestra en la figura 4.17.

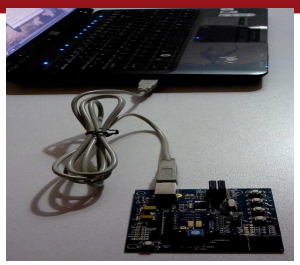


Figura 4.17. Módulo de programación del Xbee ZB.

3. Ingresar al programa, haciendo clic sobre el ícono del X-CTU ubicado en el escritorio.
4. En la pestaña PC Settings, configurar los parámetros para la comunicación serial, 19200bps, sin control de flujo, 8bits de datos, sin paridad y 1bit de parada. Asimismo, seleccionar el modo API (Application Programming Interface), debido a que el modo API del Xbee ZB nos permite interactuar a nivel de aplicación con el dispositivo, utilizando directamente las tramas Zigbee definidas para la programación local y remota, que se muestran en los anexos. En la figura 4.18, se muestra la configuración especificada para la comunicación serial.

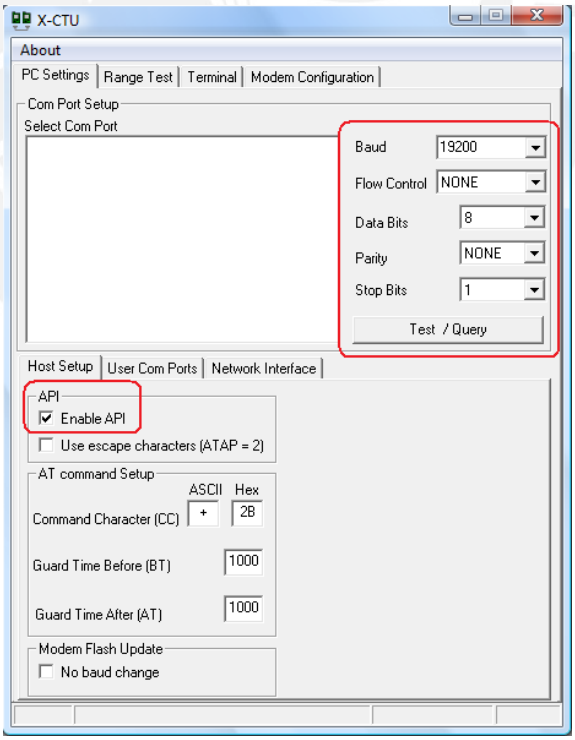


Figura 4.18. Configuración del Xbee ZB para la comunicación serial.

5. En la pestaña Modem Configuration, descargar las últimas versiones de firmware disponibles con el botón Download new versions. Seguidamente, leer

la última configuración almacenada con el botón Read. Luego, proceder a seleccionar en Baud Rate la tasa de baudios a 19200bps para la comunicación serial y verificar que el tipo de dispositivo sea el correcto en Function Set. En este caso, configurar el coordinador como Zigbee Coordinador API y los routers como Zigbee Router API. Finalmente, guardar los cambios con el botón Write. En la figura 4.19, se muestra la configuración detallada.

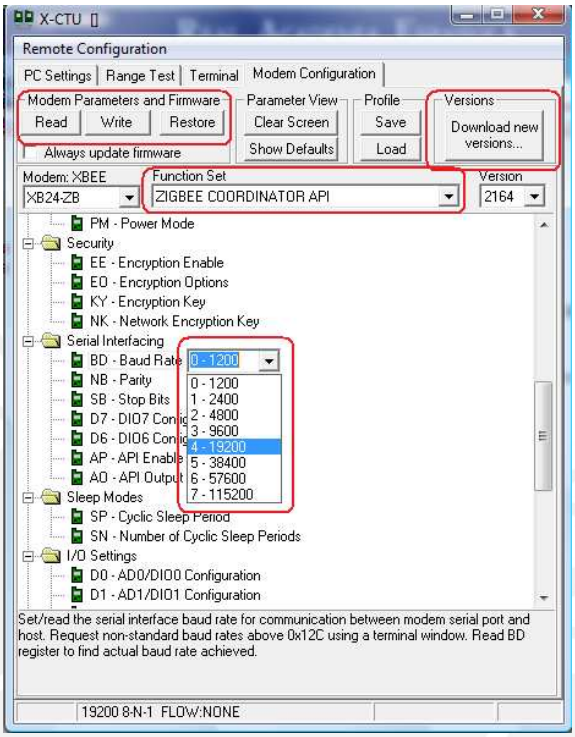


Figura 4.19. Configuración del Xbee ZB.

6. En el Xbee ZB router que estará conectado a los sensores y las lámparas incandescentes, habilitar los puertos D0 y D1 como entradas digitales; y el puerto D2 y D3, como salidas digitales en baja. Tomar en cuenta que en las entradas, las resistencias pull-up están habilitadas por defecto, así que estarán en nivel 1 lógico en estado de reposo. Asimismo, habilitar el muestreo por detección de cambio para detectar los cambios de estado de los sensores en las dos entradas, escribiendo el número hexadecimal 0x03, lo cual significa que se habilita dicho parámetro para los puertos D0 y D1. Por otro lado, en el Xbee ZB router que transmitirá los datos del teclado matricial, no es necesario realizar ninguna configuración adicional, puesto que no se usarán los puertos digitales. Finalmente, verificar que la versión de firmware de los módulos sea la última y proceder a guardar los cambios con el botón Write. En la figura 4.20, se muestra la configuración detallada.

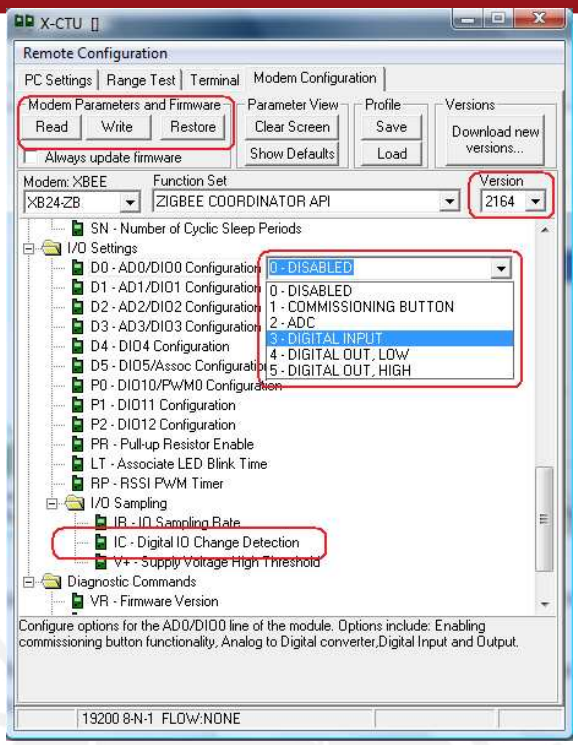


Figura 4.20. Configuración de los puertos digitales del Xbee ZB.

4.6.2. Configuración del Secure Socket iWiFi con el iChip Config Utility

Esta aplicación gratuita fue desarrollada por la compañía Connect One y es compatible únicamente con Windows XP. A continuación, se detalla el procedimiento para la configuración del módulo Secure Socket iWiFi.

1. Descargar la aplicación de la dirección indicada e instalarlo.
   http://www.connectone.com/support.asp?did=30
2. Conectar la tarjeta de programación a un puerto USB del computador con el Secure Socket iWiFi montado sobre los sockets, como se muestra en la figura 4.21. Verificar que los jumpers estén ubicados en los pines de programación.

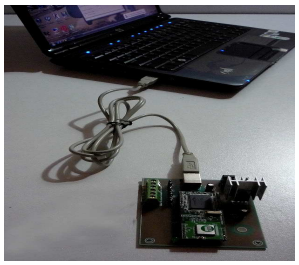


Figura 4.21. Tarjeta de programación del Secure Socket iWiFi.

3. Ingresar al programa, haciendo clic sobre el ícono del iChip Config Utility ubicado en el escritorio.

4. En la ventana principal, ingresar a la opción Serial Ports, seleccionar la velocidad deseada a 19200bps y el puerto para la comunicación serial. Luego, ingresar a Full Configuration y seleccionar los parámetros para registrar el dispositivo en la WLAN de soporte y, posteriormente, ingresar al ícono de Dumb Terminal para establecer la conexión con la WLAN y activar el modo SerialNET. En la figura 4.22, se muestra la ventana principal del iChip Config Utility.

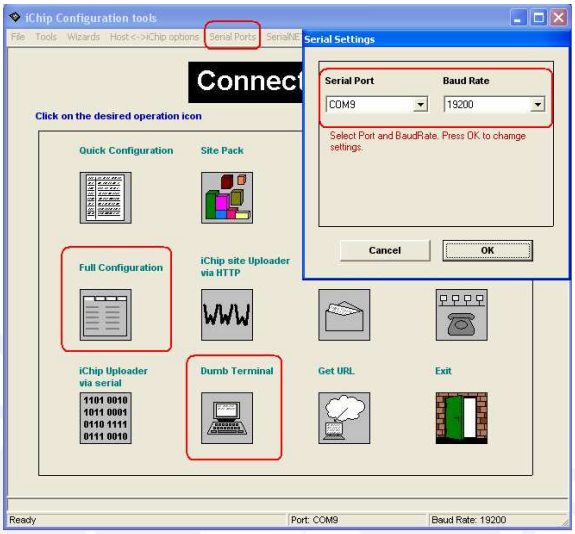


Figura 4.22. Ventana principal del iChip Config Utility.

5. En Full Configuration, seleccionar la pestaña Wireless LAN para los datos de la red inalámbrica como el nombre en SSID, el tipo de encriptación en WEP Mode 64bit, sólo para efectos de prueba, ya que se usará WPA2, cuya configuración está en los anexos. Asimismo, en Key Index seleccionar la llave que se desea utilizar, y del mismo modo ingresar en formato ASCII hexadecimal, la clave de la red en la llave que corresponde a la selección. Finalmente, en la parte inferior elegir la opción Apply para guardar los cambios. En la figura 4.23, se muestra la configuración para registrar el dispositivo en la WLAN de soporte.

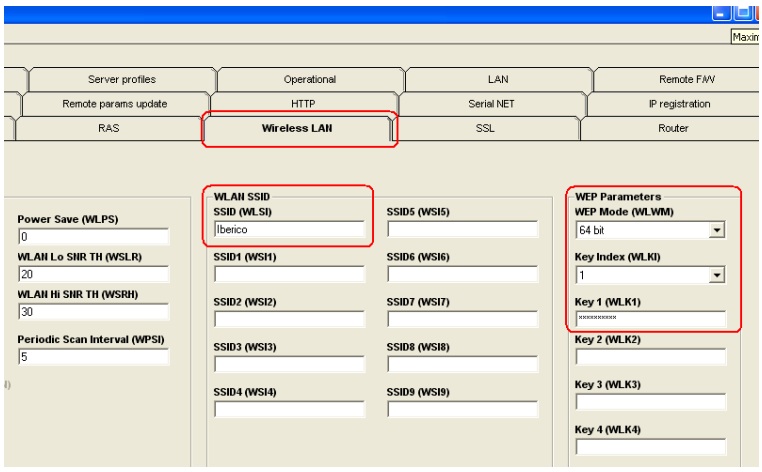


Figura 4.23. Configuración para registro del dispositivo en la WLAN.

6. Seguidamente, seleccionar la pestaña SerialNET e ingresar los parámetros de configuración. En FCHR ingresar el carácter que permitirá enviar la información almacenada en el buffer, en este caso, se seleccionará 0x7E, debido a que se encuentra presente en el arranque de todas las tramas Zigbee. Asimismo, en la opción SNSI, ingresar los parámetros para la comunicación serial, 19200bps, 8bits de datos, sin paridad, 1bit de parada, sin control de flujo. Luego, en la opción HSRV, ingresar la dirección IP del servidor, así como el puerto de comunicación, en este caso la 192.168.1.33:5100. Se debe tener en cuenta que lo recomendable es seleccionar puertos a partir del 1024 de los 65536 disponibles, puesto que los primeros están reservados para la comunicación del sistema operativo mediante diferentes protocolos. Finalmente, en la parte inferior de la ventana, seleccionar Save para guardar los cambios y cerrar la ventana. En la figura 4.24, se muestra la configuración para activar el modo SerialNET del dispositivo.

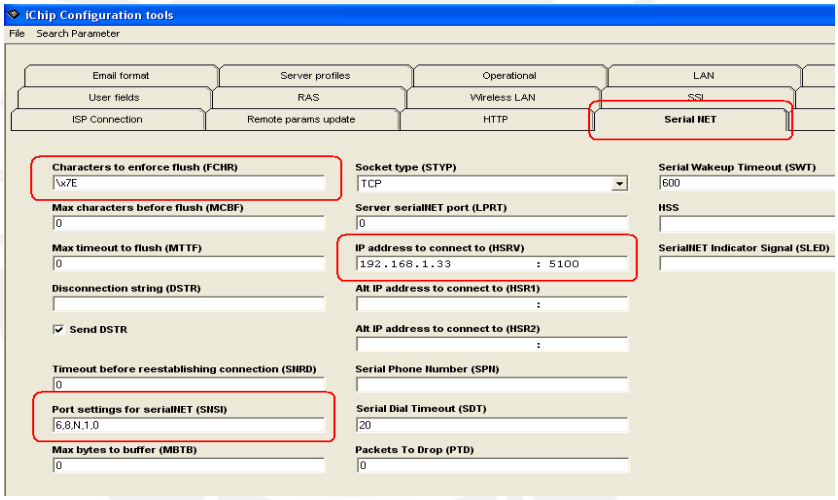


Figura 4.24. Configuración para activar el modo SerialNET.

7. Por último se debe ingresar al Dumb Terminal de la ventana principal, para establecer la conexión con WLAN y activar el modo SerialNET del dispositivo, escribiendo los comandos AT+iDOWN y AT+iSNMD, respectivamente. Finalmente, una vez recibida la confirmación del dispositivo con el mensaje I/ONLINE, se puede iniciar la comunicación con el servidor. En la figura 4.25, se muestra el ingreso de los comandos desde el Dumb Terminal.

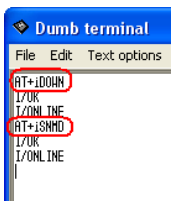


Figura 4.25. Comandos ingresados desde el Dumb Terminal.

4.7. Pruebas del Funcionamiento de los Componentes del Sistema de Seguridad

Las pruebas del sistema de seguridad se realizaron a menor escala, simulando los diferentes incidentes que pudiesen ocurrir dentro del departamento. De esta manera, se utilizó un sensor de movimiento y un detector de humo, así como dos lámparas incandescentes para simular la alarma en el primer caso; el control de la iluminación y apertura de la cerradura eléctrica, en el segundo. Asimismo, se utilizó un teclado matricial desde donde se ingresaba la clave de acceso a la vivienda. Por otro lado, se ejecutó la aplicación Seguridad y Monitoreo Portátil en un computador portátil con sistema operativo Windows 7. En la figura 4.26, se muestra el diagrama de pruebas del sistema. A continuación, se detallan las pruebas realizadas.

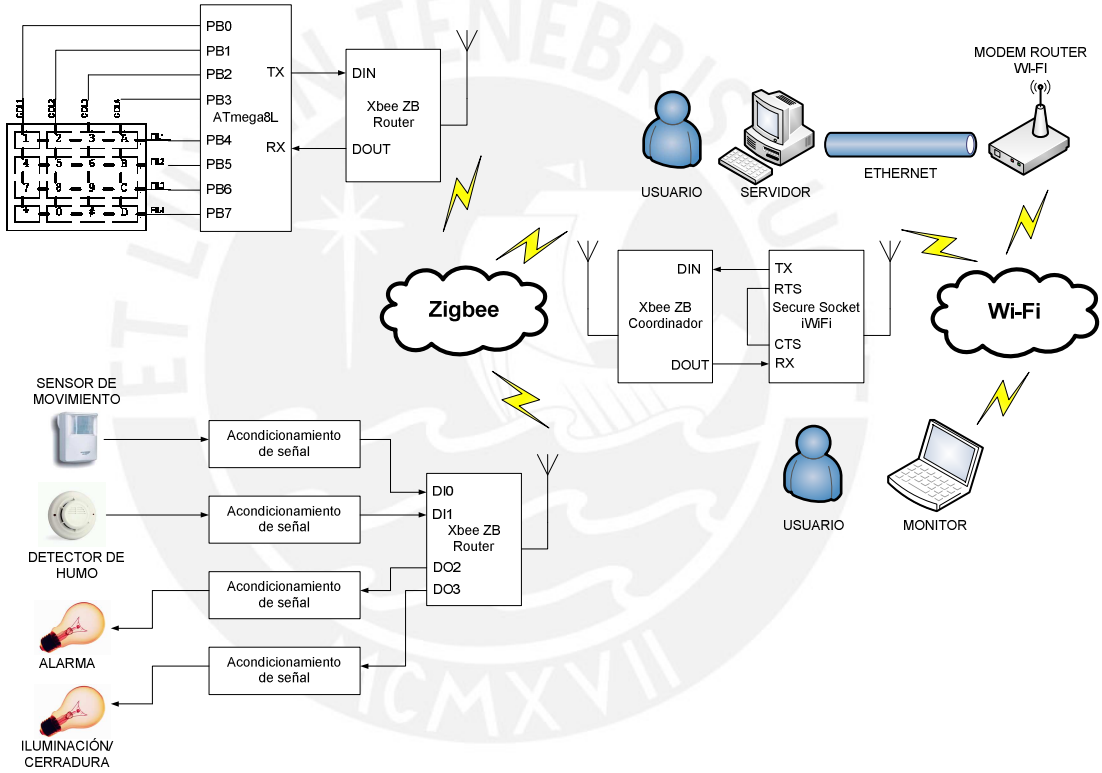


Figura 4.26. Diagrama de pruebas del sistema de seguridad.

1. Se conectó el sensor de movimiento, el detector de humo y las lámparas incandescentes a sus respectivas tarjetas de acondicionamiento. Asimismo, estas tarjetas fueron conectadas a los puertos digitales DI0, DI1, DO2 y DO3, respectivamente de un Xbee ZB router, cuya configuración se detalló anteriormente. La conexión se realizó directamente a una de las tarjetas de programación que proporciona salida de los cuatros primeros puertos digitales.

En la figura 4.27, se muestra el modelo de pruebas y la conexión de los dispositivos con el Xbee ZB router.

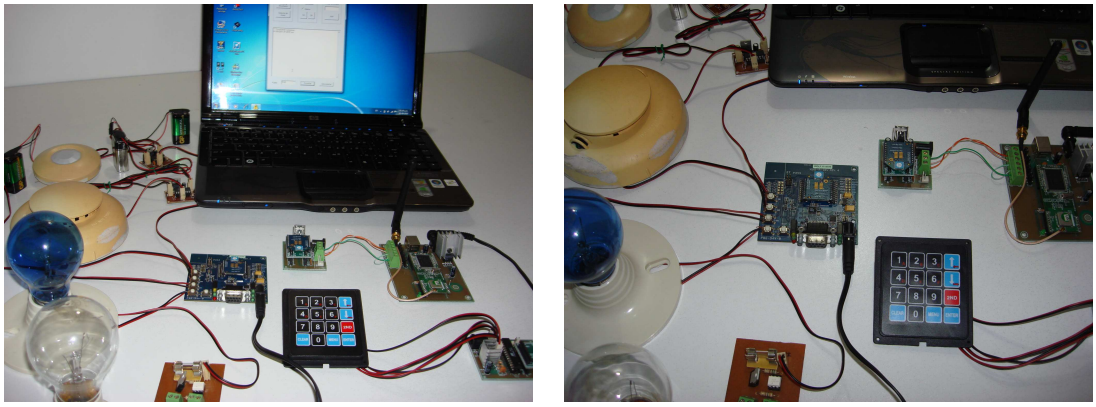


Figura 4.27. Modelo de pruebas y conexión de los dispositivos con el Xbee ZB.

2. Seguidamente, se energizaron todas las tarjetas y dispositivos del sistema de seguridad, para seguidamente ingresar a la aplicación Seguridad que se encargará del control y monitoreo automático. Después de ingresar el puerto 5100 y presionar el botón Escuchar, se estableció la conexión con el sistema. Una vez realizada la conexión, observaremos un mensaje de confirmación y, asimismo, podremos realizar diferentes solicitudes para activar, desactivar y leer los dispositivos que conforman la solución. Por ejemplo, al solicitar el estado del sensor de movimiento presionando el botón del mismo nombre, recibimos la confirmación de que el sensor de no está activo; no obstante, al solicitar el estado del detector de humo presionando el botón del mismo nombre, recibimos una mensaje de ALERTA de activación. Manualmente, se activó y desactivó la iluminación y la alarma, respectivamente; seleccionando la opción del mismo nombre, y presionando el botón On y Off. Finalmente, se solicitó la apertura de la cerradura eléctrica, ingresando la clave en Código de Acceso y presionando el botón Abrir, con lo que se recibe un mensaje de validez de la clave al abrir la puerta. En la figura 4.28, se muestra la pantalla de la aplicación Seguridad con los resultados de las pruebas descritas. Estas pruebas se incluyen en los anexos.

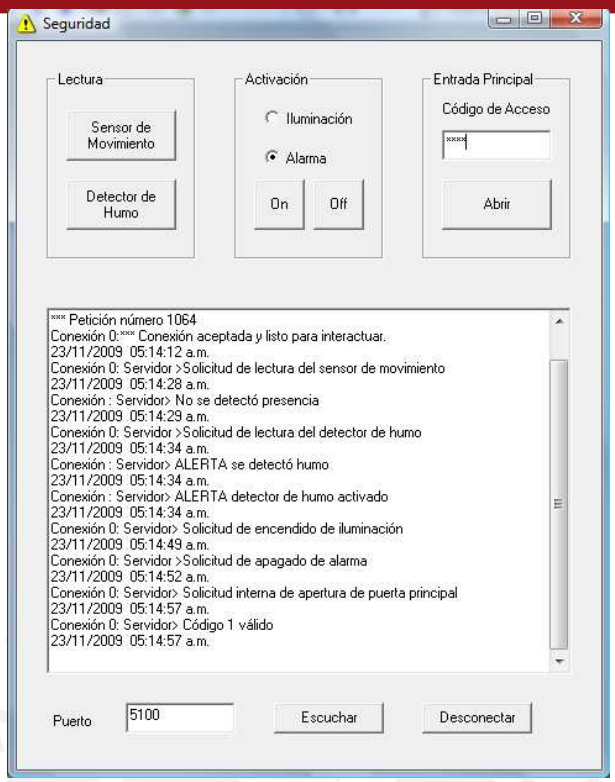


Figura 4.28. Aplicación Seguridad y solicitudes realizadas por el usuario.

3. En caso se registre algún incidente dentro del departamento, observaremos mensajes de alerta, y asimismo la aplicación ejecutará los procedimientos de prevención y disuasión de incidentes descritas en Identificación de los Componentes del Sistema de Seguridad. Por ejemplo, cuando el sensor detectó movimiento, se encendieron las luces automáticamente; después de 45 segundos, la aplicación envía una trama al Xbee ZB router para leer nuevamente el estado del sensor. En este caso, al confirmar la activación del sensor, se encendió la alarma para alertar a los usuarios. Por otro lado, al activarse el detector humo, se encendió la alarma; después de 45 segundos, se envió una trama al Xbee ZB para leer nuevamente el estado del detector. En este caso, se recibió la confirmación de que el dispositivo había retornado a su estado de reposo. En la figura 4.29, se muestra la pantalla de la aplicación Seguridad con los resultados de las pruebas descritas. Estas pruebas se incluyen en los anexos.

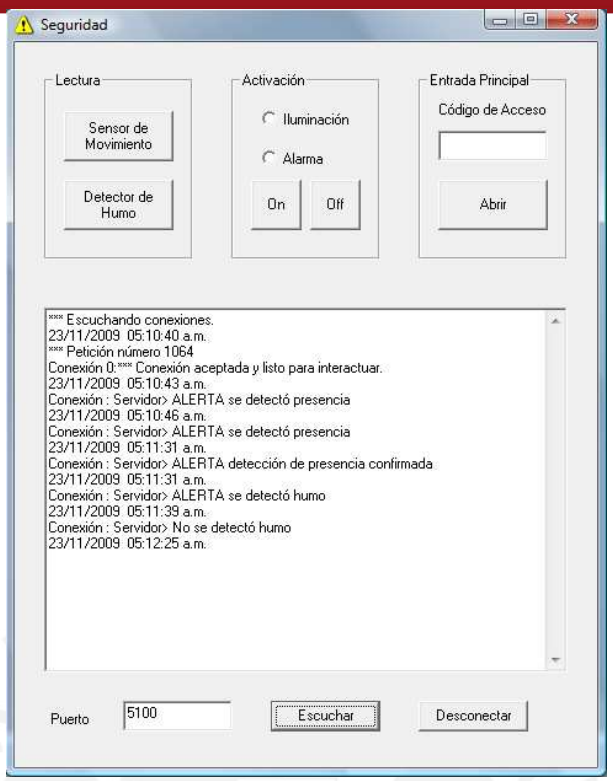


Figura 4.29. Aplicación Seguridad y detección de incidentes.

4.8. Costos de Materiales

En la tabla 4.2, se detalla los costos de los elementos y la implementación para el desarrollo de la solución.

Tabla 4.2. Costos de los materiales para el desarrollo de la solución.

Producto	Distribuidor	Cantidad	Costo Inc. IGV (USD)
Xbee ZB	Digi-Key	4	193.20
Secure Socket iWiFi	Mouser Electronics	1	112.00
Tarjeta de Secure Socket iWiFi	Varios	1	23.10
Tarjeta de Sensor de Movimiento	Varios	2	6.20
Tarjeta de Detector de Humo	Varios	2	6.20
Tarjeta de Cerradura Eléctrica	Varios	1	3.50
Tarjeta de Alarma	Varios	1	3.50
Tarjeta de Luces	Varios	1	3.40
Tarjeta de Teclado Matricial	Varios	1	17.70
ATmega8L	Varios	1	5.20
Tarjeta de Coordinador	Varios	1	9.10
Cerradura Eléctrica	Maestro	1	34.50
Sensor de Movimiento	RadioShack	3	31.05
Detector de Humo	RadioShack	2	13.80
Sirena 30W (Alarma)	Elektro Security	2	23.80
UPS	Amazon	1	266.84
Diseño e Implementación	-	1	300.00
Total			**1053.09**

CONCLUSIONES

- En el diseño de la solución se logró establecer los requerimientos del sistema de seguridad, distribuyendo de manera eficiente los elementos en el interior del departamento. Asimismo, se determinaron las funcionalidades de la seguridad contra robos, seguridad contra incendios, control de accesos y control de iluminación, ejecutando el flujo de acciones integrado en un solo sistema.
- Se seleccionaron los dispositivos que integrarán el sistema de seguridad, teniendo en cuenta el costo, disponibilidad y cumplimiento de los requisitos de diseño, generando una solución eficiente y accesible para nuestro medio.
- Se realizó el diseño de la red actuador – sensor, conformada por nodos router Zigbee que permiten incrementar el alcance de la red, los cuales se conectan a los sensores y actuadores a través de tarjetas de acondicionamiento de señal. Asimismo, se diseñó la interconexión mediante comunicación serial entre el nodo coordinador Zigbee y el nodo de acceso a la WLAN de soporte, proporcionando conectividad con la red inalámbrica Wi-Fi de cada departamento. Esta característica permite la portabilidad del equipo encargado del control y monitoreo al interior de cada departamento.
- Se desarrollaron dos aplicaciones de control y monitoreo en Visual Basic, que permitieron verificar el funcionamiento de la solución. Asimismo, se obtuvo resultados satisfactorios, detectando las variables de sensado y enviando comandos de control a los dispositivos finales desde la aplicación instalada sobre un computador portátil.
- Se verificó el correcto funcionamiento del sistema, operando de acuerdo a lo configurado para cada componente y contando con una cobertura total de la red actuador - sensor y WLAN de soporte dentro del departamento. Asimismo, se comprobó la alta disponibilidad de la comunicación, experimentando en ambas redes una tasa nula de pérdida de paquetes.

RECOMENDACIONES

- Un sistema de seguridad de este tipo puede ser adaptado a edificios con diferentes características, debido a que los elementos que conforman el sistema operan de manera inalámbrica, proporcionando flexibilidad con respecto de su ubicación. De esta manera, será posible aprovechar las redes inalámbricas del edificio que son implementadas en este tipo de locaciones, para realizar las tareas de control y monitoreo desde un centro de vigilancia, sin importar su ubicación dentro del mismo.
- Por otro lado, esta solución permite adicionar una gran cantidad de dispositivos, puesto que la implementación del sistema de seguridad bajo el protocolo Zigbee permite manipular hasta 65536 nodos, contribuyendo a la escalabilidad del sistema. De esta manera, se puede adaptar este sistema de seguridad a locaciones que cuentan con amplias áreas para aprovechar las ventajas de este protocolo.
- Por otra parte, a esta solución se pueden integrar diversos componentes con tareas específicas, siendo un factor importante la aplicación de control del sistema, es por esto que con el desarrollo de un programa de gestión de vivienda, podría integrarse otros componentes, y de esa manera automatizar el hogar en su conjunto.

BIBLIOGRAFÍA

[1] INSTITUTO DE OPINIÓN PÚBLICA
2009 Temas de seguridad. Consulta: 25 de abril de 2010. <http://www.pucp.edu.pe/iop/files/sondeo_41.pdf>

[2] SEGURIDAD CIUDADANA
2007 Encuesta sobre seguridad ciudadana en Lima Metropolitana y el Callao. Consulta: 27 de marzo de 2010. <http://www.seguridadidl.org.pe/destacados/2007/12-02/texto.htm>

[3] INEI
2010 Perú en Cifras. Consulta: 15 de mayo de 2010. <http://www.inei.gob.pe/>

[4] MINISTERIO DE ENERGÍA Y MINAS
2006 Sección 370 del Código Nacional de Electricidad Utilización. 30 de enero.

[5] MINISTERIO DE TRANSPORTES Y TELECOMUNICACIONES
2004 Artículo 28° del Texto Único Ordenado del Regl amento General de la Ley de Telecomunicaciones. 25 de junio.

[6] CEDOM
2008 Instalaciones Domóticas. 2da. edición. Madrid: AENOR. Consulta: 11 de enero de 2010. <http://www.cedom.es/fitxers/documents/publicacions/InstalDomot_Cuadernbuenaspract_CEDOM_2ed.pdf>

[7] KASIER, Guy
2008 eCourse on Integrated Home Systems. Consulta: 20 de enero de 2010. <http://www.leonardo-energy.org/drupal/node/3048>

[8] DOMÓTICA VIVA
2003 “Bricolaje X-10 Curso de Domótica a través de la red eléctrica”. Consulta: 18 de marzo de 2010.
<http://www.domoticaviva.com/X-10/X-10.htm>

[9] KINNEY, Patrick
2003 ZigBee Technology: Wireless Control that Simply Works. Consulta: 10 de febrero de 2010.
<http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=5162>

[10] ZENSYS, INC.
2006 Z-Wave Protocol Overview. Consulta: 11 de febrero de 2010.
<http://www.eilhk.com/en/product/Datasheet/Zensys/SDS10243-2%20-%20Z-Wave%20Protocol%20Overview.pdf>

[11] SMARTLABS, INC.
2005 INSTEON The Details. Consulta: 20 de febrero de 2010.
<http://www.insteon.net/pdf/insteondetails.pdf>

[12] ECHELON CORPORATION
1999 Introduction to the LonWorks System. Consulta: 25 de febrero de 2010.
<http://www.isep.pw.edu.pl/ZakladNapedu/Instrukcje/lon-echelon.pdf>

[13] PETERSON, Larry
2007 Computer networks: a systems approach. 4th ed. Amsterdam: Elsevier.

[14] HABIBI, Arash, et. al.
2009 A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i). Consulta: 15 de abril de 2010.
<http://www.ivanescobar.com/survey%20wifi.pdf>

[15] FUJITSU SIEMENS COMPUTERS
2007 “El Futuro del Hogar Digital”. CASADOMO.com. Consulta: 10 de marzo de 2010.
<http://www.casadomo.com/noticiasDetalle.aspx?id=9914&c=6&idm=10&pat=10>

[16] PÉRTIGA
2005 Sistemas de control: elementos componentes, variables, función de transferencia y diagrama funcional. Material de enseñanza. Consulta: 15 de enero de 2010.
<http://www.jmrivas.es/pdf/tecnologia.pdf>

[17] BRAIN, Marshall
2008 “How Smoke Detectors Work”. HowStuffWorks. Consulta: 25 de marzo de 2010.
<http://home.howstuffworks.com/home-improvement/household-safety/fire/smoke1.htm>

[18] EHOW
2007 “Types of Motion Detectors”. Consulta: 15 de abril de 2010.
<http://www.ehow.com/about_5373497_types-motion-detectors.html>

[19] ALLARD-JACQUIN, Patrick, et. al.
2008 ZigBee – WiFi Coexistence. Consulta: 23 de febrero de 2010.
<http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=13184>

[20] FREEBSD
2004 “Serial and UART Tutorial”. Consulta: 25 de mayo de 2010.
<http://www.freebsd.org/doc/en_US.ISO8859-1/articles/serial-uart/>

[21] STEVEN, Eric
2007 “UPS HOWTO”. TLDP. Consulta: 28 de mayo de 2010.
<http://www.tldp.org/HOWTO/UPS-HOWTO/>

[22] VISONIC
2008 Disc Miniature 360 Ceiling Mount PIR Detector. Consulta: 11 de marzo de 2010.
<http://www.visonic.com/Products/Wired-Detectors/Disc>

[23] GE SECURITY
2009 Smoke Detector, NetworX PID, Photo, 2-wire, CleanMe®, 12-24VDC. Consulta: 13 de marzo de 2010.
<http://www.gesecurity.com/portal/site/GESecurity/menuitem.f76d98ccce4cabed5efa421766030730?selectedID=7267&seriesyn=true&seriesID=>

[24] MOVISTAR
2010 "Línea ADSL RDSI". Consulta: 27 de mayo de 2010.
<http://www.movistar.es/qx/Nav/qxTONavFichProdImp/0,,v_producto+18162+v_idioma+es+v_segmento+AHOG,00.html>

[25] TING-PAT SO, Albert
1999 Intelligent building systems. Boston: Kluwer Academic.

[26] AULACLIC
2005 "Wi-Fi. La Comunicación Inalámbrica". Consulta: 15 de enero de 2010.
<http://www.aulaclic.es/articulos/wifi.html>

[27] IEC Intelligent Technologies
2004 "A LonWorks Techonology Tutorial". Consulta: 27 de enero de 2010.
<http://www.ieclon.com/LonWorks/LonWorksTutorial.html>

[28] HOME CONTROLS
2010 "Why Automate Your Home". Consulta: 5 de febrero de 2010.
<http://www.homecontrols.com/why_automate>

ANEXOS

Anexo A

Tramas Zigbee Enviadas para el Control del Sistema de Seguridad

Trama para leer el estado del sensor de movimiento conectado a DI2								
7E	00 0F	17	01	00 13 A2 00 40 54 41 71	FF FE	02	49 53	51
Arranque	Longitud de Trama	Tipo de Trama	ID de Trama	Dirección de Destino de 64 bits	Dirección de Destino de 16 bits	Comando Remoto (Aplicar Cambios)	Comando AT (Muestreo de Puertos)	Checksum

Trama para leer el estado del detector de humo conectado a DI3								
7E	00 0F	17	02	00 13 A2 00 40 54 41 71	FF FE	02	49 53	50
Arranque	Longitud de Trama	Tipo de Trama	ID de Trama	Dirección de Destino de 64 bits	Dirección de Destino de 16 bits	Comando Remoto (Aplicar Cambios)	Comando AT (Muestreo de Puertos)	Checksum

Trama para activar la lámpara incandescente conectada a DO0								
7E	00 10	17	03	00 13 A2 00 40 54 41 71	FF FE	02	44 30 05	72
Arranque	Longitud de Trama	Tipo de Trama	ID de Trama	Dirección de Destino de 64 bits	Dirección de Destino de 16 bits	Comando Remoto (Aplicar Cambios)	Comando AT (Configurar DO0 en Alta)	Checksum

Trama para desactivar la lámpara incandescente conectada a DO0								
7E	00 10	17	05	00 13 A2 00 40 54 41 71	FF FE	02	44 30 04	71
Arranque	Longitud de Trama	Tipo de Trama	ID de Trama	Dirección de Destino de 64 bits	Dirección de Destino de 16 bits	Comando Remoto (Aplicar Cambios)	Comando AT (Configurar DO0 en Baja)	Checksum

Anexo B

Comparación de Costos con Otras Soluciones del Mercado Local

Producto BOXER	Cantidad	Costo inc. IGV (USD)
Controlador	1	
Teclado Digital	1	
Batería 12V 4A	1	
Sirena 30W	1	
Sensor Magnético	2	
Sensor de Movimiento	3	
Detector de Humo	2	
Instalación y cableado	1	
Total		**1075**

Producto ORUS	Cantidad	Costo inc. IGV (USD)
Controlador	1	
Teclado Digital	1	
Batería 12V 4A	1	
Sirena 30W	1	
Sensor Magnético	2	
Sensor de Movimiento	3	
Detector de Humo	2	
Instalación y cableado	1	
Total		**562.36**

Producto	Cantidad	Costo Inc. IGV (USD)
Xbee ZB	4	193.20
Secure Socket iWiFi	1	112.00
Tarjeta de Secure Socket iWiFi	1	23.10
Tarjeta de Sensor de Movimiento	2	6.20
Tarjeta de Detector de Humo	2	6.20
Tarjeta de Cerradura Eléctrica	1	3.50
Tarjeta de Alarma	1	3.50
Tarjeta de Luces	1	3.40
Tarjeta de Teclado Matricial	1	17.70
ATmega8L	1	5.20
Tarjeta de Coordinador	1	9.10
Cerradura Eléctrica	1	34.50
Sensor de Movimiento	3	31.05
Detector de Humo	2	13.80
Sirena 30W (Alarma)	2	23.80
UPS	1	266.84
Diseño e Implementación	1	300.00
Total		**1053.09**

Se observa la implementación del sistema de seguridad tiene un costo comparativo con la solución de la empresa BOXER. Sin embargo, el costo de la solución de ORUS es mucho menor al sistema desarrollado.

Anexo C

Diagrama de Flujo de la Aplicación Seguridad para el Control y Monitoreo Automático

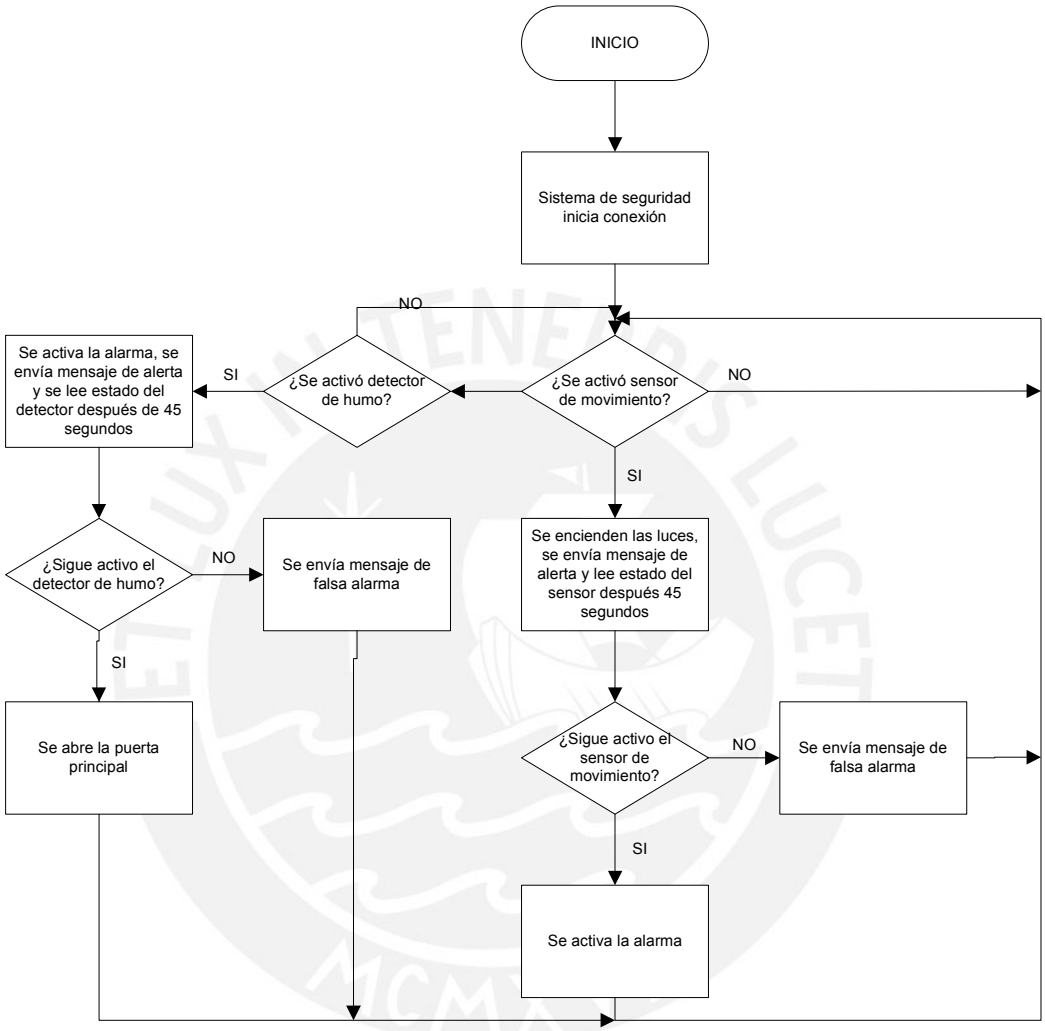
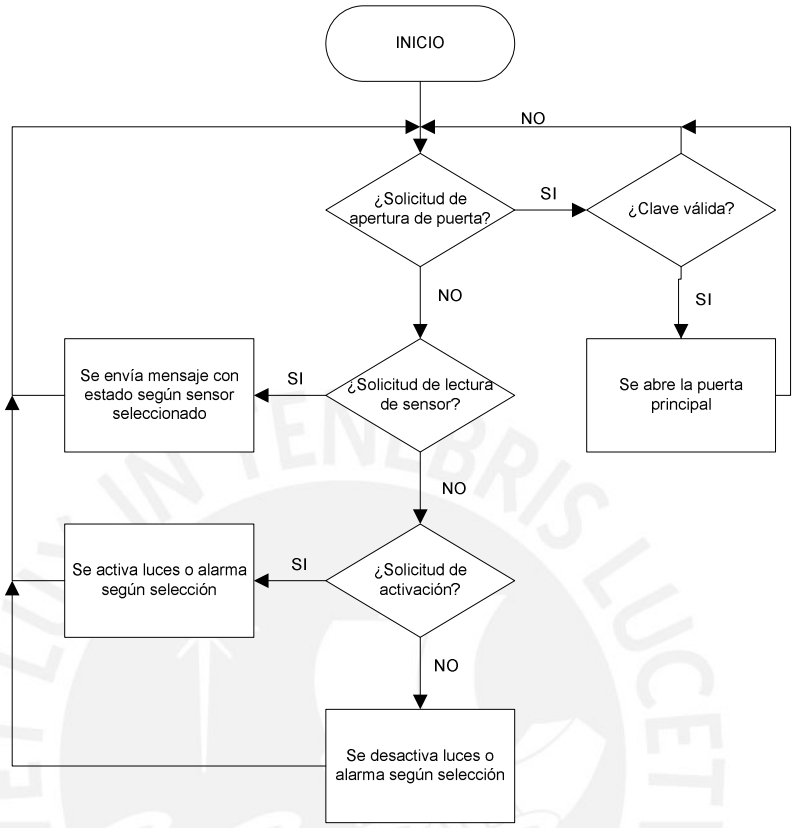


Diagrama de Flujo de la Aplicación Seguridad para el Control y Monitoreo Manual



Anexo D

Programa Seguridad de Control y Monitoreo

```
'Lee Detector de Humo
Private Sub Command1_Click()
Dim numElementos As Integer 'numero de sockets
Dim i As Integer 'contador
'obtiene la cantidad de Winsocks que tenemos
numElementos = Winsock2.UBound
'recorre el arreglo de sockets
For i = 0 To numElementos
'si el socket se encuentra conectado...
If Winsock2(i).State = sckConnected Then
'enviamos la trama para leer el detector de humo ID 02
Winsock2(i).SendData
        hex2ascii("7E000F17020013A20040544171FFFE02495350")
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor >" & "Solicitud de lectura del
        detector de humo" & vbCrLf & Date & "  " & Time & vbCrLf  'mostramos los
        datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
'generamos un retardo de 1 seg para poder enviar nuevamente la trama y leer los
datos correctos
delay (1)
Winsock2(i).SendData
        hex2ascii("7E000F170F0013A20040544171FFFE02495343")
End If
Next
End Sub

'Lee Sensor de Movimiento
Private Sub Command4_Click()
Dim numElementos As Integer 'numero de sockets
Dim i As Integer 'contador
```

```
'obtiene la cantidad de Winsocks que tenemos
numElementos = Winsock2.UBound
'recorre el arreglo de sockets
For i = 0 To numElementos
'si el socket se encuentra conectado...
If Winsock2(i).State = sckConnected Then
'enviamos la trama para leer el sensor de movimiento ID 01
Winsock2(i).SendData
        hex2ascii("7E000F17010013A20040544171FFFE02495351")
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
        obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor >" & "Solicitud de lectura del
        sensor de movimiento" & vbCrLf & Date & "  " & Time & vbCrLf   'mostramos
        los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
'generamos un retardo de 1 seg para poder enviar nuevamente la trama y leer los
        datos correctos
delay (1)
Winsock2(i).SendData
        hex2ascii("7E000F170F0013A20040544171FFFE02495343")
End If
Next
End Sub
```

'Desactiva Iluminación(Opción1) o Alarma(Opción2)

```
Private Sub Command5_Click()
Dim numElementos As Integer 'numero de sockets
Dim i As Integer 'contador
'obtiene la cantidad de Winsocks que tenemos
numElementos = Winsock2.UBound
'recorre el arreglo de sockets
For i = 0 To numElementos
'si el socket se encuentra conectado...
If Winsock2(i).State = sckConnected Then
If Option2.Value = True Then
'enviamos la trama para desactivar la alarma
```

```
Winsock2(i).SendData
        hex2ascii("7E001017060013A20040544171FFFE0244300470")
'apuntamos al final del contenido del TextBox e
'insertamos los nuevos datos obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor >" & "Solicitud de apagado
        de alarma" & vbCrLf & Date & "  " & Time & vbCrLf  'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Else
'enviamos la trama para desactivar las luces
Winsock2(i).SendData
        hex2ascii("7E001017050013A20040544171FFFE0244300471")
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & "Solicitud de apagado
        de iluminación" & vbCrLf & Date & "  " & Time & vbCrLf  'mostramos los
        datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
End If
End If
Next
End Sub

'Activa Iluminación(Opción1) o Alarma(Opción2)
Private Sub Command6_Click()
Dim numElementos As Integer 'numero de sockets
Dim i As Integer 'contador
'obtiene la cantidad de Winsocks que tenemos
numElementos = Winsock2.UBound
'recorre el arreglo de sockets
For i = 0 To numElementos
'si el socket se encuentra conectado...
If Winsock2(i).State = sckConnected Then
If Option2.Value = True Then
'enviamos la trama para activar la alarma
```

```
Winsock2(i).SendData
        hex2ascii("7E001017040013A20040544171FFFE0244300571")
'apuntamos al final del contenido del TextBox e
'insertamos los nuevos datos obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & "Solicitud de encendido
        de alarma" & vbCrLf & Date & "  " & Time & vbCrLf  'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Else
'enviamos la trama para activar las luces
Winsock2(i).SendData
        hex2ascii("7E001017030013A20040544171FFFE0244300572")
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & "Solicitud de encendido
        de iluminación" & vbCrLf & Date & "  " & Time & vbCrLf  'mostramos los
        datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
End If
End If
Next
End Sub

'Activa la cerradura
Private Sub Command7_Click()
Dim Clave As String
Dim mensaje As String
Dim numElementos As Integer 'numero de sockets
Dim i As Integer 'contador
'obtiene la cantidad de Winsocks que tenemos
numElementos = Winsock2.UBound
'recorre el arreglo de sockets
For i = 0 To numElementos
'si el socket se encuentra conectado...
If Winsock2(i).State = sckConnected Then
```

```
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & "Solicitud interna de
        apertura de puerta principal" & vbCrLf & Date & "  " & Time & vbCrLf
        'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Clave = Text2.Text
Text2.Text = ""
Select Case Clave
Case 1234
mensaje = "Código 1 válido"
valido = 1
Case 5678
mensaje = "Código 2 válido"
valido = 1
Case 9876
mensaje = "Código 3 válido"
valido = 1
Case 5432
mensaje = "Código 4 válido"
valido = 1
Case Else
mensaje = "Código inválido"
valido = 0
End Select
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & mensaje & vbCrLf &
        Date & "  " & Time & vbCrLf  'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
If valido = 1 Then
'enviamos la trama para apertura la puerta
Winsock2(i).SendData
        hex2ascii("7E001017070013A20040544171FFFE024431056D")
delay (2)
```

```
'enviamos la trama para detener apertura de puerta después de 2 seg
Winsock2(i).SendData
        hex2ascii("7E001017080013A20040544171FFFE024431046D")
End If
End If
Next
End Sub

'Recibe datos
Private Sub Winsock2_DataArrival(Index As Integer, ByVal bytesTotal As Long)
Dim Buffer As String 'variable para guardar los datos
'obtenemos los datos y los guardamos en una variable
Winsock2(Index).GetData Buffer
'verificamos el contenido de la trama
ValidaTrama (HexString(Buffer))
End Sub

'Escucha Conexiones
Private Sub Command2_Click()
'cerramos cualquier conexion previa
Winsock1.Close
'asignamos el puerto local que abriremos
Winsock1.LocalPort = Text3.Text
'deja el socket escuchando conexiones
Winsock1.Listen
'desplegamos un mensaje en la ventana
Text1.SelStart = Len(Text1.Text)
Text1.Text = Text1.Text & "*** Escuchando conexiones." & vbCrLf & Date & "  " &
        Time & vbCrLf
Text1.SelStart = Len(Text1.Text)
End Sub

'Cierra Conexiones
Private Sub Command3_Click()
'cierra la conexion
Winsock2(Index).Close
'desplegamos un mensaje en la ventana
```

```
Text1.SelStart = Len(Text1.Text)
Text1.Text = Text1.Text & "*** Conexión cerrada por el usuario." & vbCrLf & Date &
        "  " & Time & vbCrLf
Text1.SelStart = Len(Text1.Text)
End Sub
Private Sub Winsock2_Close(Index As Integer)
'cierra la conexión
Winsock2(Index).Close
'desplegamos un mensaje en la ventana
Text1.SelStart = Len(Text1.Text)
Text1.Text = Text1.Text & "Conexión " & Index & ":*** Conexión cerrada por el
        cliente." & vbCrLf & Date & "  " & Time & vbCrLf
Text1.SelStart = Len(Text1.Text)
End Sub
```

'Muestra Ventana de Error

```
Private Sub Winsock2_Error(Index As Integer, ByVal Number As Integer,
        Description As String, ByVal Scode As Long, ByVal Source As String, ByVal
        HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
'cerramos la conexion
Winsock2(Index).Close
'mostramos información sobre el error
MsgBox "Error numero " & Number & ": " & Description, vbCritical
End Sub
```

'Acepta Peticiones de Conexiones

```
Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long)
Dim numSocket As Integer 'el numero del socket
'mostramos un mensaje en la ventana
Text1.SelStart = Len(Text1.Text)
Text1.Text = Text1.Text & "*** Petición número " & requestID & vbCrLf
Text1.SelStart = Len(Text1.Text)
'creamos un nuevo socket
numSocket = NuevoSocket
'aceptamos la conexión con el nuevo socket
Winsock2(numSocket).Accept requestID
'desplegamos un mensaje en la ventana
```

```
Text1.SelStart = Len(Text1.Text)
Text1.Text = Text1.Text & "Conexión " & numSocket & ":*** Conexión aceptada y
        listo para interactuar." & vbCrLf & Date & "  " & Time & vbCrLf
Text1.SelStart = Len(Text1.Text)
End Sub

'Carga un nuevo socket al arreglo y devuelve su indice
Private Function NuevoSocket() As Integer
Dim numElementos As Integer 'numero de sockets
Dim i As Integer 'contador
'obtiene la cantidad de Winsocks que tenemos
numElementos = Winsock2.UBound
'recorre el arreglo de sockets
For i = 0 To numElementos
'si algun socket ya creado esta inactivo
'utiliza este mismo para la nueva conexión
If Winsock2(i).State = sckClosed Then
NuevoSocket = i 'retorna el índice
Exit Function 'abandona la función
End If
Next
'si no encuentra sockets inactivos
'crea uno nuevo y devuelve su identidad
Load Winsock2(numElementos + 1) 'carga un nuevo socket al arreglo
'devuelve el nuevo indice
NuevoSocket = Winsock2.UBound
End Function

'Convierte datos en hexadecimal string
Public Function HexString(EvalString As String) As String
Dim intStrLen As Integer
Dim intLoop As Integer
Dim strHex As String
EvalString = Trim(EvalString)
intStrLen = Len(EvalString)
For intLoop = 1 To intStrLen
strHex = strHex & " " & Hex(Asc(Mid(EvalString, intLoop, 1)))
```

```
Next
HexString = strHex

End Function

'Convierte valor hexadecimal en ASCII
Public Function hex2ascii(ByVal hextext As String) As String
For y = 1 To Len(hextext)
    num = Mid(hextext, y, 2)
    Value = Value & Chr(Val("&h" & num))
    y = y + 1
Next y
hex2ascii = Value
End Function

'Genera retardo en el programa
Public Function delay(ByVal valor As Integer)
 retraso = valor + Timer
    While retraso >= Timer
        DoEvents
    Wend
End Function

'Valida Tramas Recibidas
Public Function ValidaTrama(ByVal trama As String)
Dim FrameID As String
FrameID = Mid(trama, 7, 2)
Select Case FrameID
Case "90"
Acceso (trama)
Case "92"
Incidente (trama)
Case "97"
If Mid(trama, 10, 1) = "1" Or Mid(trama, 10, 1) = "A" Then
LeeMovimiento (trama)
ElseIf Mid(trama, 10, 1) = "2" Or Mid(trama, 10, 1) = "C" Then
LeeHumo (trama)
```

```
End If
End Select
End Function

'Genera acciones para la seguridad contra robos
Public Function LeeMovimiento(ByVal movimiento As String)
Dim message2 As String
If Mid(movimiento, 10, 1) = "1" And (Mid(movimiento, 57, 1) = "8" Or
Mid(movimiento, 57, 1) = "9" Or Mid(movimiento, 57, 1) = "0" Or Mid(movimiento,
57, 1) = "1") Then
message2 = "ALERTA sensor de movimiento activado"

ElseIf Mid(movimiento, 10, 1) = "A" And (Mid(movimiento, 57, 1) = "8" Or
Mid(movimiento, 57, 1) = "9" Or Mid(movimiento, 57, 1) = "0" Or Mid(movimiento,
57, 1) = "1") Then
message2 = "ALERTA detección de presencia confirmada"
'enviamos la trama para activar la alarma
Winsock2(i).SendData
        hex2ascii("7E0010170B0013A20040544171FFFE024430056A")
Else
message2 = "No se detectó presencia"
End If
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & message2 & vbCrLf &
        Date & "  " & Time & vbCrLf  'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
End Function

'Genera acciones para la seguridad contra incendios
Public Function LeeHumo(ByVal humo As String)
Dim message3 As String
If Mid(humo, 10, 1) = "2" And (Mid(humo, 57, 1) = "4" Or Mid(humo, 57, 1) = "5" Or
Mid(humo, 57, 1) = "0" Or Mid(humo, 57, 1) = "1") Then
message3 = "ALERTA detector de humo activado"
```

```
ElseIf Mid(humo, 10, 1) = "C" And (Mid(humo, 57, 1) = "4" Or Mid(humo, 57, 1) = "5"
Or Mid(humo, 57, 1) = "0" Or Mid(humo, 57, 1) = "1") Then
message3 = "ALERTA detección de humo confirmada"
Else
message3 = "No se detectó humo"
'enviamos la trama para desactivar la alarma
Winsock2(i).SendData
hex2ascii("7E001017060013A20040544171FFFE0244300470")
End If
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & message3 & vbCrLf &
        Date & "  " & Time & vbCrLf  'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
End Function
```

'Valida clave ingresada desde el teclado matricial

```
Public Function Acceso(ByVal password As String)
Dim valido As Integer
Dim mensaje As String
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & "Solicitud externa de
        apertura de puerta principal" & vbCrLf & Date & "  " & Time & vbCrLf
        'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Select Case Mid(password, 39, 7)
Case "1 2 3 4"
mensaje = "Código 1 válido"
valido = 1
Case "5 6 7 8"
mensaje = "Código 2 válido"
valido = 1
Case "9 8 7 6"
mensaje = "Código 3 válido"
```

```
valido = 1
Case "5 4 3 2"
mensaje = "Código 4 válido"
valido = 1
Case Else
mensaje = "Código inválido"
valido = 0
End Select
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
        obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & mensaje & vbCrLf &
        Date & "  " & Time & vbCrLf  'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
If valido = 1 Then
'enviamos la trama para apertura la puerta
Winsock2(i).SendData
        hex2ascii("7E001017070013A20040544171FFFE024431056D")
delay (2)
'enviamos la trama para detener apertura de puerta después de 2 seg
Winsock2(i).SendData
        hex2ascii("7E001017080013A20040544171FFFE024431046D")
End If
End Function
```

'Valida Incidente

```
Public Function Incidente(ByVal alerta As String)
Dim alertahumo As Integer
Dim alertamov As Integer
Dim message As String
Select Case Mid(alerta, 49, 1)
'se activó el sensor de movimiento
Case "8"
alertahumo = 0
alertamov = 1
message = "ALERTA se detectó presencia"
Case "9"
```

```
alertahumo = 0
alertamov = 1
message = "ALERTA se detectó presencia"
'se activó el detector de humo
Case "4"
alertahumo = 1
alertamov = 0
message = "ALERTA se detectó humo"
Case "5"
alertahumo = 1
alertamov = 0
message = "ALERTA se detectó humo"
'se activó el sensor de movimiento y detector de humo
Case "0"
alertahumo = 1
alertamov = 1
message = "ALERTA se detectó presencia y humo"
Case "1"
alertahumo = 1
alertamov = 1
message = "ALERTA se detectó presencia y humo"
End Select
Winsock2(i + 1).SendData message 'envia mensaje a equipos de monitoreo
If alertahumo = 1 Or alertamov = 1 Then
'apuntamos al final del contenido del TextBox e insertamos los nuevos datos
obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Conexión " & i & ": Servidor> " & message & vbCrLf &
        Date & "  " & Time & vbCrLf  'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
End If
If alertamov = 1 Then
'enviamos la trama para encender las luces
Winsock2(i).SendData
        hex2ascii("7E001017090013A20040544171FFFE024430056C")
delay (3)
'enviamos la trama para leer el sensor de movimiento
```

```
Winsock2(i).SendData
        hex2ascii("7E000F170A0013A20040544171FFFE02495348")
'generamos un retardo de 2 seg para poder enviar nuevamente la trama y leer los
        datos correctos
delay (1)
Winsock2(i).SendData
        hex2ascii("7E000F170F0013A20040544171FFFE02495343")
ElseIf alertahumo = 1 Then

'enviamos la trama para activar la alarma
Winsock2(i).SendData
        hex2ascii("7E0010170B0013A20040544171FFFE024430056C")
delay (3)
'enviamos la trama para leer el detector de humo
Winsock2(i).SendData
        hex2ascii("7E000F170C0013A20040544171FFFE02495346")
'generamos un retardo de 2 seg para poder enviar nuevamente la trama y leer los
        datos correctos
delay (1)
Winsock2(i).SendData
        hex2ascii("7E000F170F0013A20040544171FFFE02495343")
End If
End Function
```

Anexo E

Programa Monitoreo Portátil de Monitoreo

```
'Recibe datos
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
Dim Buffer As String 'variable para guardar los datos
'obtenemos los datos y los guardamos en una variable
Winsock1.GetData Buffer
'apuntamos al final del contenido del TextBox e
'insertamos los nuevos datos obtenidos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
Text1.Text = Text1.Text & "Servidor >" & Buffer & vbCrLf & Date & "  " & Time &
        vbCrLf 'mostramos los datos
Text1.SelStart = Len(Text1.Text) 'coloca el cursor al final del contenido
End Sub

'Muestra Ventana de Error
Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal
        Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal
        HelpContext As Long, CancelDisplay As Boolean)
'cerramos la conexión
Winsock1.Close
'mostramos información sobre el error
MsgBox "Error numero " & Number & ": " & Description, vbCritical
End Sub

'Solicita Conexión
Private Sub Command2_Click()
'asignamos los datos de conexion
Winsock1.RemoteHost = Text3.Text
Winsock1.RemotePort = Text4.Text
'conectamos el socket
Winsock1.Close
Winsock1.Connect
End Sub
```

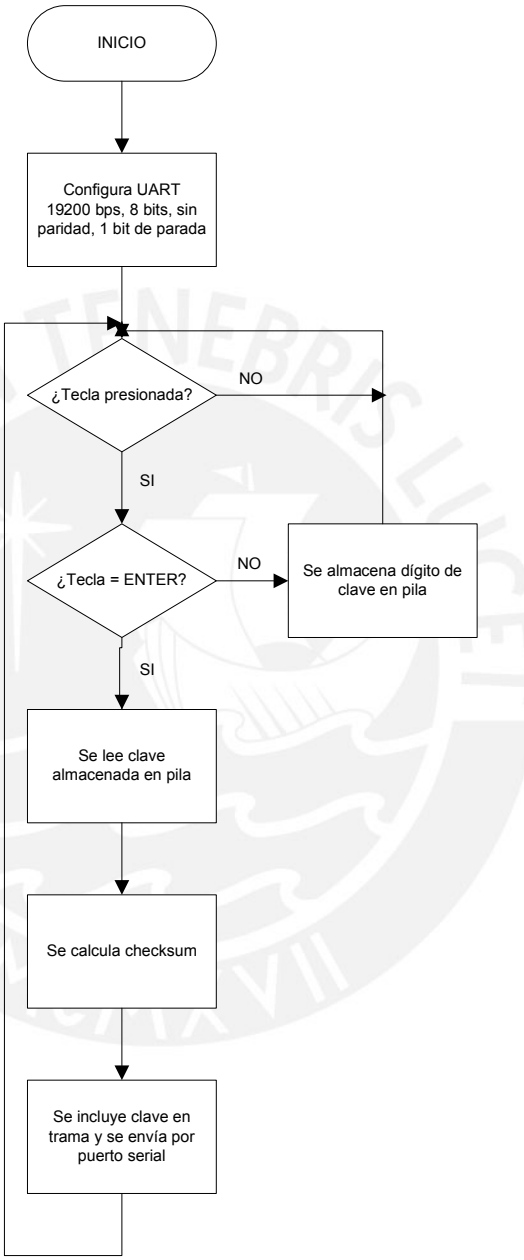
```
'Cierra Conexión
Private Sub Command3_Click()
'cierra la conexión
Winsock1.Close
'desplegamos un mensaje en la ventana
Text1.Text = Text1.Text & "*** Conexión cerrada por el usuario." & vbCrLf
'desplazamos el scroll
Text1.SelStart = Len(Text1.Text)
End Sub

'Establece conexión
Private Sub Winsock1_Connect()
'desplegamos un mensaje en la ventana
Text1.Text = Text1.Text & "*** Conexión establecida." & vbCrLf
'desplazamos el scroll
Text1.SelStart = Len(Text1.Text)
End Sub

'Cierra Conexión
Private Sub Winsock1_Close()
'cierra la conexion
Winsock1.Close
'desplegamos un mensaje en la ventana
Text1.SelStart = Len(Text1.Text)
Text1.Text = Text1.Text & "*** Conexión cerrada por el servidor." & vbCrLf
Text1.SelStart = Len(Text1.Text)
End Sub
```

Anexo F

Diagrama de Flujo del Programa Matriz para la Lectura y Envío de Clave del Teclado Matricial



Anexo G

Programa Matriz de Lectura y Envío de Clave Ingresada en el Teclado Matricial

```
; ****************************************************
;PROGRAMA: MATRIZ
;DESCRIPCIÓN: LEE LOS DÍGITOS INGRESADOS EN EL TECLADO MATRICIAL
;Y LOS ENVÍA POR EL PUERTO USART EN UNA TRAMA ZIGBEE
; ****************************************************

.include "C:\VMLAB\include\m8def.inc"

.def     checksum1=r22
.def     checksum=r21
.def  digito=r23          ;  guarda el valor de la tecla presionada que será enviada
.def     dato = r24     ;  se almacena dato a ser enviado por USART
.def     anterior = r25; se almacena el valor anterior de la tecla presionada

.dseg
          .org $60
          indice: .byte 1     ;      desplazamiento del contador
          columna: .byte 1     ;  columna
          clave:  .byte 8

.cseg
          .org $0
          rjmp inicio

;*************************************************************************************************
;INICIO DE PROGRAMA:

inicio:

;Configuración de pila, puertos I/O
          ldi       R16,high(RAMEND)          ;Se configura la Pila
          out       sph,r16
          ldi       r16,low(RAMEND)
```

```
        out     spl,r16

        rcall   ConfiguraSerial     ;configuro USART

        ldi     r16,0b00001111              ;Configuración de puertos para el
        teclado matricial
        out     ddrb,r16            ;pc7-pc4 son filas ,pc3_pc0 columnas.
        clr     digito          ;inicializo registros
        ldi     anterior,$FF

limpia:
        ldi     XL,low(clave)       ;inicializo la ram para guardar digito
        ldi     XH,high(clave)

leer:
        rcall LecturaTeclado    ;Leo el Teclado MATRICIAL y en r17 se guarda el
        valor de la tecla presionada
        cpi     r17,0b11110000
        breq    leer

        ldi     ZH,high(TablaTeclado*2);busco la posición en la tabla
        ldi     ZL,low(TablaTeclado*2); para conocer la tecla presionada
        add     ZL,r17
        clr     r16
        adc     ZH,r16
        lpm     digito,Z                    ;guardo verdadero valor de la tecla

        cp              digito,anterior ;verifico que no sea rebote del teclado
        breq    leer
        mov     anterior,digito         ; guardo la ultima tecla presionada

        cpi     digito,20                       ; verifico que la tecla sea valida
        breq    leer

        cpi     digito,10       ;verifico que no se desee limpiar la clave
        breq    limpia
```

```
        st    X+,digito        ;almaceno en RAM digito hasta completar la clave

        cpi     digito,$7E                      ;verifico que se presione ENTER
        breq    trama

        rjmp    leer            ; leemos siguiente digito

trama:
   ldi    ZH,high(TramaZigbee*2);inicializo tabla para enviar trama
   ldi    ZL,low(TramaZigbee*2)
        rcall    EnviaTrama          ;envío primera parte de trama

        ldi     XL,low(clave)       ;inicializo la ram para enviar digito
        ldi     XH,high(clave)
        rcall    EnviaClave          ;envía la clave

        rcall EnviaChecksum      ;calcula el checksum  y envía checksum

        rjmp    limpia

;*********************************************************************
;Subrutina LecturaTeclado
;Lee el teclado matricial
;Entradas: Ninguna
;Salidas : r17 es el valor de la tecla presionada
;*********************************************************************

LecturaTeclado:

        clr r18                                 ; Borro el índice de columna
        ldi r16,0b11111110    ;         Selecciono la primera columna
        sts columna, r16      ; Almaceno el valor de columna
        nop

Seleccion:
   out portb,r16        ; Selecciono COLUMNA
   nop
```

```
    nop

Sondeo:
;       rjmp Seleccion
        in   r17,pinb       ;     Lectura de que fila se ha presionado
        andi r17,0b11110000   ;  Enmascaro

ComparaFilas:
        lds  r16,columna     ;  Cargo el valor de COLUMNA
        cpi  r17,0b11100000
        breq Fila1
        cpi  r17,0b11010000
        breq Fila2
        cpi  r17,0b10110000
        breq Fila3
        cpi  r17,0b01110000
        breq Fila4

        inc r18
        sec             ;  Seteo bandera de carry
        rol r16         ;       Pasamos a la siguiente columna
        sts columna,r16     ;  Almaceno la nueva COLUMNA
        cpi r16,0b11101111   ;  Se revisaron las 4 columnas
        breq Fin_Lectura
        rjmp seleccion
Fila1:
        ldi  r17,0          ;       Primer elemento de la fila 1
        add  r17,r18        ;       Le sumo el numero de columna
        sts  indice,r17     ;       INDICE PARA SUMAR A LA TABLA
        rjmp Fin_Lectura

Fila2:
        ldi  r17,4          ;       Primer elemento de la fila 2
        add  r17,r18        ;       Le sumo el numero de columna
        sts  indice,r17     ;       INDICE PARA SUMAR A LA TABLA
        rjmp Fin_Lectura
```

```
Fila3:
        ldi  r17,8          ;       Primer elemento de la fila 3
        add  r17,r18        ;       Le sumo el numero de columna
        sts  indice,r17     ;       INDICE PARA SUMAR A LA TABLA
        rjmp Fin_Lectura

Fila4:
        ldi  r17,12         ;       Primer elemento de la fila 4
        add  r17,r18        ;       Le sumo el numero de columna
        sts  indice,r17     ;       INDICE PARA SUMAR A LA TABLA
        rjmp Fin_Lectura

Fin_Lectura:
        clr r18

        ret
;*********************************************************************
;Subrutina EnviaTrama
;Envía la trama almacenada definida para el coordinador y validar la clave
;Entradas: Tabla Inicializada ZH,ZL
;Salidas : Ninguna
;*********************************************************************
EnviaTrama:

                sbis    UCSRA,UDRE
                rjmp    EnviaTrama
                lpm     dato,Z+
                cpi     dato,$FF
                breq    fin_cadena
                out     UDR,dato
          rjmp  EnviaTrama

fin_cadena:
                ret
        ;               rjmp    ESPERA_RX
;*********************************************************************
;Subrutina EnviaClave
```

```
;Envía la trama almacenada definida para el coordinador y validar la clave
;Entradas: Dígitos de la clave almacenados en "dato"
;Salidas : Ninguna
;*********************************************************************
EnviaClave:

                ld              dato,X+
Continua:
                sbis    UCSRA,UDRE
                rjmp    Continua
                out     UDR,dato
                cpi     dato,$7E
                breq    Salir
                rjmp    EnviaClave
Salir:
                ret
;*********************************************************************
;Subrutina EnviaChecksum
;Calcula y Envia el Checksum
;Entradas: Ninguna
;Salidas : Ninguna
;*********************************************************************
EnviaChecksum:
        ldi     ZH,high(TramaZigbee*2+3);inicializo tabla para calcular checksum
          ldi   ZL,low(TramaZigbee*2+3)
          clr   checksum
          clr   checksum1
Suma: lpm       r16,Z+
                cpi     r16,$FF
                breq    Password
            add checksum,r16
            clr r16
              adc       checksum1,r16
        rjmp    Suma

Password:
                ldi     XL,low(clave)       ;inicializo la ram para enviar digito
```

```
                ldi     XH,high(clave)

LeerPassword:
                ld              r16,X+
                add     checksum,r16
            clr     r18
              adc       checksum1,r18
              cpi r16,$7E
                breq    envia
                rjmp    LeerPassword
Envia:
                sbis    UCSRA,UDRE
                rjmp    Envia
                ldi     dato,$FF
                sub     dato,checksum
                out     UDR,dato
                ret

;*********************************************************************
TablaTeclado:
;.db     0,1,2,3,4,5,6,7,8,9,10,$7E,20,20,20,20
.db      $7E,20,0,10,20,9,8,7,20,6,5,4,20,3,2,1

TramaZigbee:
;.db     1,2,3,4,5,6,7,8,$FF
.db $7E,$00,$13,$10,$0E,$00,$13,$A2,$00,$40,$54,$41,$72,$00,$00,$00,$00,$FF
;*********************************************************************
;Subrutina ConfiguraSerial
;Configura el USART para la comunicación serial asíncrona, 19200 bps, sin paridad,
        1 bit de parada, 8 bits
;Entradas: Ninguna
;Salidas : Ninguna
;*********************************************************************

ConfiguraSerial:
 ;19200 baudios (fosc= 1MHz)
                ldi     r16,high(5)
```

```
                out     UBRRH,r16
                ldi     r16,low(5)
                out     UBRRL,r16


; Velocidad doble, no multiprocesador
                ldi     r16,(0<<RXC | 0<<TXC | 1<<U2X | 0<<MPCM)
                out     UCSRA,r16

; Comunicación asíncrona, sin paridad, 1 bit de parada, 8 bits
                ldi     r16,(1<<URSEL | 0<<UMSEL | 0<<UPM1 | 0<<UPM0 |
        0<<USBS | 1<<UCSZ1 | 1<<UCSZ0)
                out     UCSRC,r16

; Interrupciones de comunicación deshabilitadas, Tx y Rx habilitadas

                ldi     r16,(0<<RXCIE | 0<<TXCIE | 0<<UDRIE | 0<<RXEN |
        1<<TXEN | 0<<UCSZ2 | 0<<TXB8)
                out     UCSRB,r16

        ret
;*********************************************************************
```