
# ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

## FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

### ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

# "IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA DE SEGURIDAD DOMÉSTICO BASADO EN WPAN PARA UNA RED IoT"

**TRABAJO DE TITULACIÓN**

**Tipo:** PROYECTO TÉCNICO

Presentado para optar al Grado Académico de:

**INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES**

**AUTOR:** DANIEL ALEXANDER VILAÑEZ UVIDIA

**TUTOR:** ING. MARCO VINICIO RAMOS

Riobamba-Ecuador

2019

Yo, Daniel Alexander Vilañez Uvidia, declaro que el presente Trabajo de Titulación es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos que constan en el documento y provienen de otra fuente están debidamente referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación.

Riobamba, xx de xx del 2019

DANIEL ALEXANDER VILAÑEZ UVIDIA
C.I. 100376187-9

**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES**

El Tribunal del Trabajo de Titulación certifica que: la investigación: "IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA DE SEGURIDAD DOMÉSTICO BASADO EN WPAN PARA UNA RED IoT", de responsabilidad del señor Daniel Alexander Vilañez Uvidia, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

| **NOMBRE** | **FIRMA** | **FECHA** |
|---|---|---|
| Ing. Washington Luna<br>**DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA** | _____ | _____ |
| Ing. Patricio Romero<br>**DIRECTOR DE ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES** | _____ | _____ |
| Ing. Vinicio Ramos<br>**DIRECTOR DEL TRABAJO DE TITULACIÓN** | _____ | _____ |
| Ing. Diego Veloz<br>**MIEMBRO DEL TRIBUNAL** | _____ | _____ |

**TABLA DE CONTENIDO**

**ÍNDICE DE TABLAS**

**ÍNDICE DE FIGURAS**

**ÍNDICE DE ANEXOS**

**RESUMEN**

En el presente proyecto se realizó la detección de intrusiones y niveles de gas mediante una red de sensores y el Internet de las Cosas. La selección de los elementos que conforman la red se desarrolló en base a las características más importantes de acuerdo a los requerimientos planteados. El prototipo cuenta con 5 nodos: el nodo sensor para obtener la información de cada sensor, el nodo actuador, el cual, a través del usuario realiza una acción determinada. El nodo coordinador encargado de recibir la información tanto de conexión a internet como de los nodos sensores, interconectando unos a otros, estableciéndose como el punto central de la red. Finalmente, el nodo de conexión a internet el cual está conformado por un Arduino y un computador, encargado de enviar o recibir los datos de la base datos. Para la visualización de los datos, se desarrolló en Microsoft Visual Studio una aplicación móvil multiplataforma y una aplicación de escritorio. El prototipo funciona basado en la visualización y guardado de la información en la base de datos en tiempo real, mediante las aplicaciones. Con la ayuda del software de captura de paquetes Wireshark, se pudo definir que el prototipo posee una pérdida de paquetes de alrededor de 71% a una distancia máxima de 9 metros con la presencia de obstáculos. Un porcentaje de detección del sensor de movimiento de 74.71% y una imprecisión del sensor de gas de ±0.027 voltios. La utilización de la red de sensores inalámbricos en conjunto con el Internet de las Cosas provee una amplia aplicabilidad. Se recomienda tomar en cuenta que el sistema requiere tener una conexión estable de internet para un funcionamiento adecuado.

**PALABRAS CLAVE:** <DOMÓTICA>, <COMUNICACIÓN INALÁMBRICA>, < INTERNET DE LAS COSAS>, <IEEE 802.15>, <RED DE SENSORES INALÁMBRICOS>, <ENTORNO DE DESARROLLO>, <TRANSMISIÓN DE DATOS>.

**ABSTRACT**

In this project, the detection of intrusions and gas levels was carried out through a network of sensors and the Internet of Things. The selection of the elements that make up the net was developed based on the essential features according to the requirements. The prototype has five nodes: the sensor node to obtain the information of each sensor, the actuator node, which, through the user, performs a specific action; the coordinating node in charge of receiving information both from the internet connection and from the sensor nodes, interconnecting each other, establishing itself as the central point of the network. Finally, the internet connection node, which is made up of an Arduino and a computer, is responsible for sending or receiving data from the database. For the visualization of the data, a mobile platform application and a desktop application were developed in Microsoft Visual Studio. The prototype works based on the visualization and saving of the information in the database in real time, through the forms.With the help of Wireshark packet capture software, it was possible to define that the prototype has a packet loss of around 71% at a maximum distance of 9 meters with the presence of obstacles. A detection percentage of the motion sensor of 74.71% and imprecision of the gas sensor of 0.027 volts. The use of the wireless sensor network in conjunction with the Internet of Things provides broad applicability. It is recommended to take into account that the system requires a stable internet connection for proper operation.

**Keywords:** <DOMOTIC>, <WIRELESS COMMUNICATION>, <INTERNET OF THINGS>, <IEEE 802.15>, <WIRELESS SENSORS NETWORK>, <DEVELOPMENTAL ENVIRONMENT>, <DATA TRANSMISSION>.

## INTRODUCCION

## ANTECEDENTES

Para los sistemas de video vigilancia con almacenamiento en físico el usuario debe estar en el mismo lugar en el que se encuentran los equipos de almacenamiento y en el momento exacto en el que son capturados los datos, para transformarlos en información La automatización de los hogares en nuestro país no se ha explotado en su totalidad, los servicios que se ofrecen a nivel local están centrados en las ciudades grandes como Quito, Guayaquil o Cuenca.

En 2014 en Colombia se desarrolló un artículo para la revista EAN en el cual se muestra la importancia de la gestión eléctrica domiciliaria por medio del diseño, desarrollo e implementación de un prototipo de sistema domótico, que permite utilizar de manera remota una bombilla LED a través de las acciones de prender y apagar. Para lo cual emplearon elementos de Hardware como el Arduino y de Software como los servicios en la nube de Windows Azure; con esta aplicación, se pretendió observar la interoperabilidad entre un dispositivo ubicado en el hogar y un servidor ubicado en el mundo virtual del Internet. Estos sistemas fueron implementados en otros países debido a la gran aceptación de los mismos (Internet de los objetos empleando arduino para la gestión eléctrica domiciliaria, 2014)

En Ecuador en el 2016 Escuela Politécnica Nacional se presenta el proyecto de Investigación denominado "Estudio del modelo de referencia del internet de las cosas (IoT), con la implementación de un prototipo domótico", el prototipo utilizado en ésta es bastante similar a la investigación realizada en Colombia, utilizando un Arduino, un microcontrolador y una aplicación web utilizando los lenguajes de programación PHP, HTML y CSS (Peña, y otros, 2016)

En el 2009 en la ciudad de Riobamba en la Escuela Superior Politécnica de Chimborazo se presenta un trabajo de Investigación denominado "Estudio de los sistemas Web embebidos y su aplicación en un sistema de control domótico con microcontroladores" (Robalino, 2010)

Los sistemas presentados presentan limitaciones debido a que solamente tienen un control domótico reducido y/o no presentan un sistema de alerta en tiempo real para los usuarios.

## FORMULACIÓN DEL PROBLEMA

¿Cómo implementar un prototipo de sistema de seguridad doméstico basado en WPAN para una red IoT?

## SISTEMATIZACIÓN DEL PROBLEMA

¿Cuáles son las características, generalidades y tecnologías presentes en redes WPAN para su interacción con el internet de las cosas?

¿Cuáles son los principales requerimientos que debe cumplir el prototipo de sistema de seguridad, la tecnología, los elementos electrónicos y el diseño?

¿Cómo implementar el prototipo de red con el diseño, elementos y requerimientos propuestos?

¿Cómo desarrollar una interfaz para que el usuario pueda acceder al control y los datos de la red?

¿Cómo evaluar el rendimiento del prototipo de sistema de seguridad doméstico?

## JUSTIFICACIÓN TEORICA

Los países de Sudamérica aun no cuentan al 100% con las nuevas tecnologías, debido a muchos factores entre ellos: un bajo presupuesto, pobre investigación, pocos laboratorios equipados. La automatización de los hogares en nuestro país no se ha explotado en su totalidad, existen varias instituciones que han optado por brindar una mejora a sus sistemas, sin embargo, los servicios que se ofrecen a nivel local están centrados en las ciudades grandes como Quito, Guayaquil o Cuenca (Jurado, y otros, 2011)

Se puede observar que en nuestro medio no hay una gran oferta si se habla de manera masiva como otros productos o servicios, pero al momento de realizar una búsqueda más minuciosa se pueden encontrar varias empresas que ofrecen servicios como los denominan, de automatización de casas y edificios, con la premisa de que esto ayudará a que estos sean inteligentes y auto sostenibles (Viteri, 2013)

Los sistemas de video vigilancia con almacenamiento en físico cuentan con procesos de evaluación de los datos dependientes de la disponibilidad de tiempo y localización del usuario dado que éste debe estar en el mismo lugar en el que se encuentran los equipos de almacenamiento y en el momento exacto en el que son capturados los datos, para transformarlos en información (Betancourt, y otros, 2015)

Las estadísticas correspondientes a robos de domicilios según la Fiscalía General del Estado muestran que, entre enero y octubre de 2014 y el mismo periodo de 2015, los robos a personas y domicilios aumentaron. La variación fue de 7,4 % en el caso de personas y 7,9 % en robo a domicilios. En Manta este delito tiene alta incidencia, al punto que desde enero hasta el 26 de abril de 2018 se han denunciado en la Fiscalía 308 casos, es decir 77 asaltos por mes, y en el mismo período en el 2017 sumaron 349 robos a casas, es decir más de 87 por mes. Mientras que en Guayaquil entre el 1 de enero y el 1 de julio de 2017 se dieron 25 robos, y en 2018 en el mismo periodo la cifra ascendió a 28 casos.

Por esta razón se propone la realización de un prototipo para el diseño de un sistema de seguridad doméstico utilizando el internet de las cosas para el control y monitoreo, así como protocolos de comunicación inalámbrica para la interacción de los sensores y actuadores del sistema, buscando así generar una solución con buenas características de eficiencia y flexibilidad.

**JUSTIFICACIÓN PRACTICA**

El estado actual de la electrónica y la informática ha alcanzado una gran capacidad en cuanto a la recepción y análisis de datos gracias a la conectividad de Internet y el uso masivo de redes inalámbricas, así como la aparición de dispositivos móviles inteligentes capaces de efectuar procesos computacionales complejos. (Prieto, 2011)

La automatización y la electrónica ayudan a optimizar recursos y manejar sistemas inteligentes ya sea en el campo industrial, comercial o doméstico. Es necesaria la exploración y desarrollo de la internet de las cosas dentro del entorno nacional, teniendo en cuenta que es una corriente nueva en el mundo, ofrece grandes oportunidades para mejorar las condiciones en el entorno social de cualquier persona. (Betancourt, y otros, 2015)

En la Figura 1-0 se presenta el sistema que consta de un detector de intrusos, que detecta la presencia por diferentes métodos combinados para no producir falsas alarmas, como pueden ser el movimiento, la vibración de ventanas y puertas producida por golpear o abrir estas. También dispone de sistemas de detección de humo y gases tóxicos, producidos por la mala combustión de chimeneas, calderas, calentadores de agua, calefactores y estufas.

Como sistema disuasorio, dispone de un simulador de presencia automático, que consta del encendido y apagado selectivo de determinadas luces y control de persianas.

Para controlar todo el sistema se dispone de una interfaz móvil, que puede ser accedida desde un teléfono móvil. Desde la interfaz el usuario puede activar o desactivar la alarma, activar la simulación de presencia y activar un botón de pánico, entre otras cosas.

Además, se puede configurar los medios por los que comunicarse en caso de que se produzca una alarma. En el caso de producirse una alerta, se activa una señal acústica y se genera una alerta en la aplicación.

Para que todo el sistema funcione, se ha diseñado e implementado una arquitectura, hardware, software y de comunicaciones, desde la programación de los sensores, pasando por el servidor y hasta la interfaz.

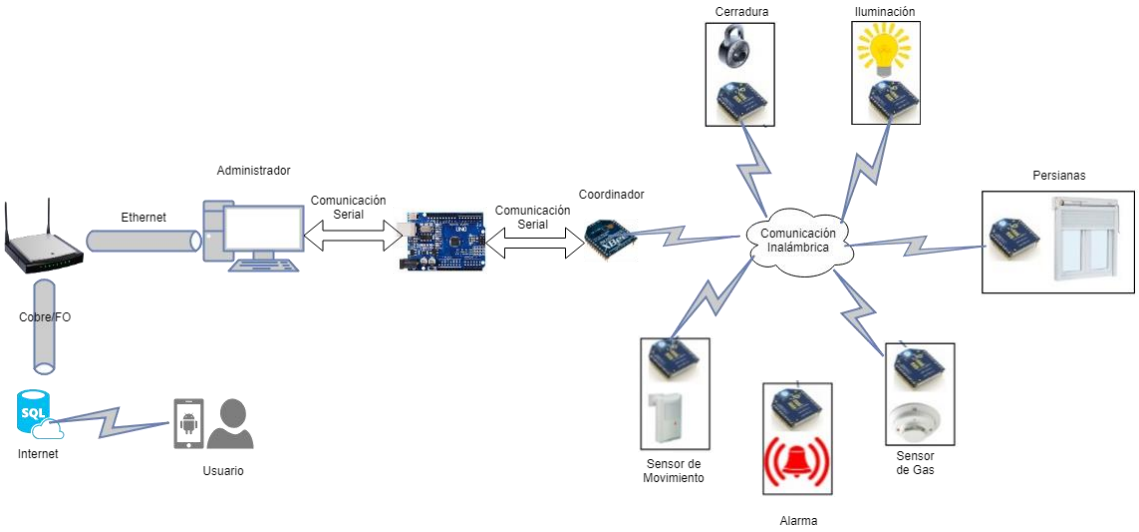


**Figura 1-0** Concepción del sistema

**Realizado por:** Daniel Vilañez,2018

## OBJETIVOS

### OBJETIVO GENERAL

Implementar un prototipo de sistema de seguridad doméstico basado en WPAN para una red IoT

### OBJETIVOS ESPECIFICOS

Estudiar las características, generalidades y tecnologías presentes en redes WPAN para su interacción con el internet de las cosas.

Establecer los principales requerimientos que debe cumplir el prototipo de sistema de seguridad, la tecnología, los elementos electrónicos y el diseño.

Implementar el prototipo de red con el diseño, elementos y requerimientos propuestos.

Desarrollar una interfaz para dispositivos móviles mediante la cual el usuario pueda acceder al control y los datos de la red.

Evaluar el rendimiento del prototipo de sistema de seguridad doméstico.

# 1. CAPITULO I: MARCO TEÓRICO

En el presente capítulo se realizará una investigación documental acerca de los principales componentes que estructuraran el tema del trabajo de titulación.

Los 3 principales componentes son: las tecnologías que están basadas en el protocolo de comunicación WPAN, para lo cual se estudiaran: sus grupos de trabajo, su estructura fundamental, sus características, etc. Las redes IoT, como están conformadas y su utilidad actualmente. Y finalmente los sistemas de seguridad domésticos, su evolución, características e importancia en la actualidad.

## 1.1. Estado del Arte de IoT

IoT puede dividirse en algunas capas de abstracción; la capa física relacionada a sensores y actuadores, la capa de red, constituida por protocolos y tipos de comunicación y la infraestructura de red, la capa de servicios, y, finalmente, la capa de aplicaciones. (Brea, 2018)

La capa física o de percepción encargada de obtener los datos del entorno, persona, proceso o sistema sobre el que se actúa. Los principales elementos de la capa son los sensores, qué, muchas veces se integran en nodos de procesamiento IoT los cuales son encargados de subir a la nube los datos mediante servicios de almacenamiento en la nube. (Vermesan, y otros, 2018)

Los servicios web habitualmente se establecen bajo pedido, de forma flexible y con baja latencia mediante computación en la nube. La computación en la nube también suministra infraestructura como servicios de almacenamiento de datos remoto o aplicaciones. La necesidad de respuestas rápidas en cualquier instante de tiempo y en cualquier lugar hará que parte de la computación se desplace o se distribuya a los nodos de red de comunicaciones, creando lo que se denomina computación en la niebla (fog computing), o incluso en el nodo sensor IoT (edge computing). (Vermesan, y otros, 2017)

En términos de aplicaciones, en la actualidad, la Unión Europea financia 5 grandes proyectos piloto de IoT con 100 millones de euros. Estos cinco grandes proyectos son:

- Activage- centrado en IoT para crear ambientes inteligentes para personas mayores.
- IoF2020- centrando en IoT para el procesamiento de comida y agricultura.
- Monica- centrado en dispositivos vestibles IoT.
- Synchronicitymercado único mediante IoT-

- Autopilot- coche autonómo potenciado por IoT. Todos estos proyectos están desligados unos de otros, pero el hecho de que existan y dispongan de buena financiación da idea de la apuesta por IoT de las instituciones.

Además, existe un proyecto de IoT como prueba de concepto de ciudades inteligentes denominado Smart City Padova, donde se ejecutan acciones como aparcamiento inteligente, avisando a los conductores a través de GPS donde hay plazas de aparcamiento libres, alumbrado inteligente, con farolas o luces que se encienden sólo con transeúntes, etc. Así pues, la apuesta de la Unión Europea por IoT en la actualidad y de cara a futuro es clara. (Zanella, y otros, 2014)

**Salud, bienestar y envejecimiento activo**

La salud, bienestar y envejecimiento constituyen una parte de IoT claramente centrada en el individuo. Los denominados dispositivos vestibles constituyen la tecnología que permite IoT de la salud y el bienestar. Se prevé la incorporación de muchos elementos externos, como integrados en la vestimenta. Dispositivos para medir características del cuerpo humano como sudor, calorías quemadas, aliento, ritmo cardíaco, cantidad de flúor de dientes, análisis de excrementos, composición de mocos o saliva, o prendas que estimulen y que ayuden a la rehabilitación de un músculo o hueso dañado. Todos estos datos podrían analizarse por un médico o experto en colaboración con técnicas de inteligencia distribuida entre el nodo sensor IoT, o en la nube. (Brea, 2018) (Zanella, y otros, 2014)

**Edificios Inteligentes**

Transformación de edificios en elementos activos integrando dispositivos de generación de energía, que interaccionarían con la red de energía intercambiando paquetes de energía con el distribuidor. Los edificios también podrían interaccionar con otros elementos externos, formando parte de la ciudad inteligente. Además, facilitarán la vida de sus ocupantes y su interacción mediante aplicaciones y servicios como la localización e identificación de personas en edificios, o la interacción táctil o gestual para ejecutar determinadas acciones mediante dispositivos vestibles, o mediante cámaras que reconozcan acciones, o mediante entornos de realidad aumentada o virtual. (Brea, 2018) (Zanella, y otros, 2014)

**Energía Inteligente**

Un aspecto importante de la red de energía en el futuro es la proliferación de mecanismos de recolección y almacenamiento de energía en el propio hogar. Esto cambiará tanto el papel de los

consumidores, que se convertirán en prosumidores, como el de los distribuidores de energía, ya que habrá flujo de energía bidireccional; del hogar hacia la fuente de generación de energía, y viceversa. Se prevé que la energía fotovoltaica sea la dominante en el futuro, y que la red de energía se convierta en la denominada energía en la nube, en donde se analizarán el consumo y distribución de energía de forma similar a cómo se analiza el flujo de información en Internet. En este sentido, las técnicas de inteligencia artificial jugarán un papel determinante para toma de decisiones en procesos de optimización energética. (Brea, 2018) (Zanella, y otros, 2014)

**Transporte Inteligente**

Se prevé que el uso del automóvil sea completamente diferente al actual, de manera que no se dispondrá de un vehículo para todo, trabajo, ocio, etc., sino que se dispondrá del vehículo como un servicio gestionado bajo demanda a través del móvil integrado en la red global IoT, sobre todo en entornos cada vez menos amigables para el vehículo, como las ciudades superpobladas. Otro elemento disruptivo será la llegada masiva del vehículo autónomo, sin conductor, lo que supondrá un reto en términos de toma de decisiones en ms mediante técnicas de inteligencia artificial, y en términos de la interacción del vehículo con la infraestructura del entorno y con otros vehículos, obligando a mapas actualizados en tiempo real, y a una red global IoT de bajo tiempo de respuesta, gracias, entre otros elementos a la computación distribuida entre nodo sensor IoT y la computación en la nube. Finalmente, también se hará un cambio total de vehículo alimentado por combustibles fósiles al vehículo eléctrico o de energía menos contaminante. (Brea, 2018) (Zanella, y otros, 2014)

**Agricultura Inteligente, Medio Ambiente**

La agricultura de precisión es y será cada vez más frecuente, de manera que se extenderán aplicaciones como la previsión de plagas en cualquier plantación mediante la integración de modelos de inteligencia artificial con sensores sobre el terreno, avisando o recomendando el momento y la cantidad de insecticida necesarios. Así mismo, la trazabilidad de la comida desde su recogida hasta su consumo será un común denominador en la industria agroalimentaria. Este mismo modelo se aplicará al ganado. En medio ambiente y en la actividad pesquera, será muy importante evaluar la calidad del agua, o la previsión de riesgos naturales. El despliegue desde drones de sensores de bajo tamaño, robustos a las inclemencias meteorológicas, y que recogen energía del ambiente será clave para abrir nuevas aplicaciones. (Brea, 2018) (Zanella, y otros, 2014)

**Ciudades Inteligentes**

Las denominadas ciudades inteligentes son y serán la suma de interacciones entre las aplicaciones citadas con anterioridad, es decir, salud y bienestar, transporte inteligente, edificios inteligentes, energía inteligente, y medio ambiente. (Brea, 2018) (Zanella, y otros, 2014)

## 1.2. Protocolo IEEE 802.15 PAN

Los dispositivos electrónicos personales día a día se vuelven más inteligentes e interactivos. Muchos de estos han mejorado sus capacidades de datos. Estas capacidades permiten retener, usar, procesar y comunicarse con distintos tipos de información. (Archundia, 2003)

Comúnmente se utilizaban cables con propósitos específicos para conectar aparatos personales. Sin embargo, los usuarios encuentran que la utilización de cables resulta una tarea un tanto reprimente e ineficaz. Además, los cables presentan problemas como: se pierden, dañan y aumentan innecesariamente el peso y volumen de los dispositivos. Por lo que se vuelve necesario el desarrollo de soluciones para la conexión de dispositivos de forma inalámbrica. Es significativo que esta medida inalámbrica no presente un impacto sustancial en cuanto a la forma original, peso, requerimientos de energía, costos, facilidad de uso, etc. (Archundia, 2003)

De aquí nace la necesidad de crear una forma eficiente, rápida y confiable de hacer transiciones de información de forma inalámbrica. Dicha solución se conoce como redes inalámbricas de área personal o WPAN por sus siglas en inglés (Wireless Personal Area Network). (Archundia, 2003) (LAN/MAN Standards Committee of the IEEE Computer Society, 2002)

Una WPAN puede tomarse como una burbuja de comunicación en torno a una persona. Dentro de esta burbuja, que se moviliza al unísono con la persona, los dispositivos personales se pueden conectar entre ellos. (Archundia, 2003)

### 1.2.1. *Características IEEE 802.15*

La característica principal de este tipo de redes es que enfocan sus sistemas de comunicaciones a un área típica de 10 metros a la redonda que envuelve a una persona o a algún dispositivo, ya sea que esté en movimiento o no. (Camargo Olivares, 2009 pág. 31)

WPAN involucra a muy poca o nula infraestructura o conexiones directas hacia el mundo exterior. También procura hacer un uso eficiente de recursos, por lo que se han diseñado protocolos simples y lo más óptimos para cada necesidad de comunicación y aplicación. (Camargo Olivares, 2009 pág. 31)

El usuario es relacionado con los dispositivos electrónicos de su posesión, o en su proximidad en lugar de una zona geométrica en particular o sitio de la red. El término PAN (red de área personal), se concibió para describir estos diferentes tipos de conexión en red. La versión inalámbrica o desconectada de dicho concepto es el concepto de WPAN. (Camargo Olivares, 2009 pág. 31)

Para satisfacer las diferentes necesidades de comunicación dentro de un área personal la IEEE se dividen los grupos de estudio en 4 grupos de trabajo, que se encargan del desarrollo de estándares. (Camargo Olivares, 2009 pág. 31)

### 1.2.2. *Aplicaciones*

El IEEE 802.15 se desarrolla para ser utilizado en gran cantidad de aplicaciones, incluyendo el control y monitoreo industrial, seguridad pública, medición en automóviles, tarjetas o placas inteligentes, agricultura de precisión, periféricos para PC, aparatos electrónicos, monitoreo de salud, juguetes y juegos interactivos entre personas o grupos. Sin embargo, existen grandes oportunidades de desarrollo en la automatización del hogar. (Archundia, 2003)

Se espera que los requerimientos máximos de transmisión de datos para aplicaciones con periféricos de PC estén en el rango de los 115.2 kb/s, a menos de 10kb/s para automatización del hogar y para algunos dispositivos electrónicos. De la misma manera se espera que los periféricos de PC acepten rangos de aproximadamente 15 m y de más de 100 m para aplicaciones de automatización del hogar. (Archundia, 2003)

### 1.2.3. *Modelo*

El proyecto IEEE 802 divide al DLL en dos subcapas, la subcapa de enlace de acceso a medios (Medium Access Control, MAC) y la de control de enlaces lógicos (Logical link control, LLC). El LLC es común a todos estándares 802. La subcapa MAC depende del hardware y cambia respecto a la implementación física de esta capa, como se muestra en la figura 1-1. (Archundia, 2003 pág. 13)

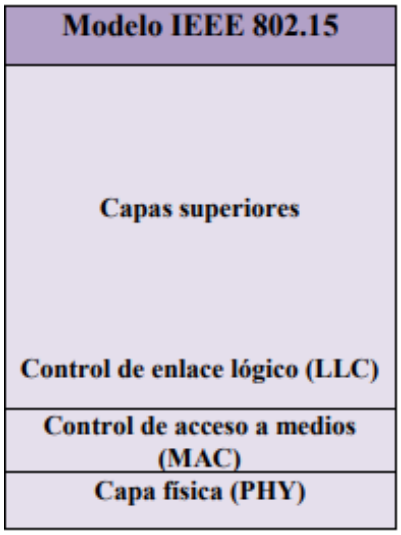


**Figura 1-1** Modelo de Capas IEEE 802.15

**Realizado por:** Daniel Vilañez,2018

### 1.2.4. *Grupos de trabajo*

Existen cuatro grupos básicos de trabajo dentro de la tecnología WPAN, cada uno de ellos con características e intereses específicos los cuales elaboran estándares que satisfacen necesidades específicas en cada comunicación. (Camargo Olivares, 2009 pág. 32) (Archundia, 2003 pág. 4)

1. El grupo de trabajo 802.15.1 realiza el estándar basado en las especificaciones del SIG de Bluetooth. Este grupo de trabajo publicó el estándar IEEE 802.15.1 el 14 junio de 2002. (Camargo Olivares, 2009 pág. 32) (Archundia, 2003 pág. 4)
2. El grupo de trabajo 802.15.2 desarrolló un modelo de coexistencia entre las WLAN y WPAN, así como de los aparatos que las envuelven. (Camargo Olivares, 2009 pág. 32) (Archundia, 2003 pág. 4)
3. El grupo de trabajo 802.15.3. Trabaja para establecer los estatus y publicar un estándar nuevo de alta velocidad (20 Mbits/s o mayores) para WPANs. Además de ofrecer una alta velocidad de transmisión, este estándar se está diseñando para consumir poca energía y ofrecer soluciones a bajos costos, así como aplicaciones multimedia. (Camargo Olivares, 2009 pág. 32) (Archundia, 2003 pág. 4)
4. El grupo de trabajo IEEE 802.15.4, investiga y desarrolla soluciones que requieren una baja transmisión de datos y con ello una duración en las baterías de meses e incluso de años, así como una complejidad relativamente baja. (Camargo Olivares, 2009 pág. 32) (Archundia, 2003 pág. 4)

#### *1.2.4.1. IEEE 802.15.1 Bluetooth*

Tecnología utilizada para la conectividad inalámbrica de corto alcance entre dispositivos como PDAs, teléfonos celulares, teclados, máquinas de fax, computadoras de escritorio y portátiles, módems, proyectores, impresoras, etc. (Camargo Olivares, 2009 pág. 35)

El principal mercado es la transferencia de datos y voz entre dispositivos y computadoras personales; es una tecnología de radiofrecuencia (RF) que trabaja en la banda de 2.4 GHz y utiliza salto de frecuencia para expansión del espectro. (Camargo Olivares, 2009 pág. 35)

La distancia de conexión puede ser de hasta 10 metros o más, dependiendo del incremento de la potencia del transmisor, pero los dispositivos no necesitan estar en línea de vista ya que las señales de RF pueden atravesar paredes y otros objetos no metálicos sin problema. (Camargo Olivares, 2009 pág. 35)

*Características*

Según Camargo (2009 págs. 36-37) las características que presenta el protocolo, son las siguientes:

- Opera en la banda de 2,4 GHz con una tasa binaria máxima de 720 Kbps.
- Utiliza expansión del espectro con saltos en frecuencia (Frequency Hopping), lo cual especifica 1600 saltos por segundo entre 79 frecuencias.
- Utiliza modulación GFSK (modulación FSK con un filtrado gaussiano).
- Usa duplexación en el tiempo TDD.
- Soporta hasta ocho dispositivos en una piconet (un maestro y siete esclavos).
- Tiene dos tipos de transferencia de datos entre dispositivos: los orientados a conexión de tipo síncrono y los no orientados a conexión de tipo asíncrono.
- Las piconets pueden combinarse para formar lo que se denominan scatternets.
- La potencia de transmisión está comprendida entre 0 dBm y 20 dBm.
- El control de potencia es obligatorio para ciertos dispositivos y opcional para el otros.
- Presenta un canal asíncrono, fundamentalmente utilizado para transmisión de datos.
- Canales síncronos, fundamentalmente utilizados para servicios que requieran calidad.

*Arquitectura*

La arquitectura de Software que presenta posee 2 partes:

- Núcleo

Se utiliza la interfaz HCI (Host Controller Interface, por sus siglas en inglés), para extender la relación entre los distintos dispositivos Bluetooth y sus anfitriones, ya sean estos, laptops, teléfonos móviles, etc. (Rodríguez Saucedo, 2012 pág. 38)

- Perfiles y protocolos de las capas superiores

Los protocolos de alto nivel como:

- SDP: utilizado para encontrar otros dispositivos Bluetooth dentro del rango de comunicación, encargado, también, de detectar la función de los dispositivos en rango. (Rodríguez Saucedo, 2012 pág. 39)
- RFCOMM: utilizado para emular conexiones de puerto serial. (Rodríguez Saucedo, 2012 pág. 39)
- TCS: control de telefonía. (Rodríguez Saucedo, 2012 pág. 39)
- L2CAP: ayuda a la interacción de los otros protocolos con el controlador de banda base. Además, se encarga de la segmentación y re ensamblaje de los paquetes para poder enviar paquetes de mayor tamaño a través de la conexión Bluetooth. (Rodríguez Saucedo, 2012 pág. 39)

El hardware que compone el dispositivo Bluetooth está compuesto por dos partes:

- Un dispositivo de radio, encargado de modular y transmitir la señal. (Rodríguez Saucedo, 2012 pág. 39)
- Un controlador digital compuesto por un CPU, un procesador de señales digitales (DSP - Digital Signal Processor, por sus siglas en inglés) llamado LC (Link Controller, por sus siglas en inglés) y de los interfaces con el dispositivo anfitrión. (Rodríguez Saucedo, 2012 pág. 39)

*Parámetros de Modulación*

La modulación es del tipo GFSK (Gaussian frequency shift keying, por sus siglas en inglés) con un BT (tiempo de ancho de banda) = 0.5. El índice de modulación debe ser de entre 0.28 y 0.35. Un 1 binario se representa con una desviación positiva de frecuencia, y un 0 binario se representa con una desviación negativa de frecuencia. La sincronización de símbolo deber mejor que ±20 ppm. (Archundia, 2003 pág. 27)

Para cada canal de transmisión, la desviación mínima de frecuencia (Fmin = la menor de {Fmin+,Fmin-}) que corresponde a la secuencia 1010 debe de ser menor a ±80% de la desviación de frecuencia (fd) que corresponde a la secuencia 00001111. Adicionalmente, la desviación mínima nunca debe de ser menor a 115 kHz. La transmisión de datos tiene una tasa de 1 Msímbolos/s. (Archundia, 2003 págs. 27-28)

El error de cruce por cero es la diferencia de tiempo entre el periodo ideal del símbolo y el tiempo de cruce real. Este debe de ser menor a ± 0.125 del periodo de un símbolo. La desviación máxima de frecuencia debe de ser entre 140 kHz y 175 kHz. (Archundia, 2003 pág. 28)

*Establecimiento de Conexión*

Como los dispositivos Bluetooth operan en 2 modos (como maestro y como esclavo), sólo es posible la comunicación entre el maestro y los esclavos, nunca entre varios esclavos. (Camargo Olivares, 2009 pág. 43)

- Establecimiento del enlace: se lleva a cabo mediante el Link Manager Protocol (LMP). El enlace físico es una secuencia de trasmisión sobre un canal físico de timeslots alternados entre el maestro y el esclavo. (Camargo Olivares, 2009 pág. 43)
- Establecimiento del canal: después del establecimiento del enlace físico, se debe establecer un canal Bluetooth (enlace lógico) entre ambos dispositivos mediante el protocolo L2CAP. (Camargo Olivares, 2009 pág. 43)
- Establecimiento de la conexión: Finalmente, se establece la conexión entre las aplicaciones de los dos dispositivos. Por ejemplo, la conexión entre el ordenador y el móvil (una aplicación basada en el puerto serie) RFCOMM se inicializa y establece la conexión entre los dispositivos. Una vez que la conexión ya ha sido establecida, el maestro envía el primer paquete de tráfico, mientras que el esclavo responde con cualquier tipo de paquete. (Camargo Olivares, 2009 pág. 43)

*Seguridad*

Hay tres modos primarios de seguridad:

- Modo 1. Sin seguridad. Todos los mecanismos de seguridad (autenticación y cifrado) están deshabilitados. Además, el dispositivo se sitúa en modo “promiscuo”, permitiendo que todos los dispositivos Bluetooth se conecten a él. (Rodríguez Saucedo, 2012 pág. 49)

- Modo 2. En la capa L2CAP, nivel de servicios. Los procedimientos de seguridad son inicializados después de establecerse un canal entre el nivel LM y el de L2CAP. Un gestor de seguridad controla el acceso a servicios y dispositivos. Variando las políticas de seguridad y los niveles de confianza se pueden gestionar los accesos de aplicaciones con diferentes requerimientos de seguridad que operen en paralelo. Su interface es muy simple y no hay ninguna codificación adicional de PIN o claves. (Rodríguez Saucedo, 2012 pág. 49)
- Modo 3. En el nivel de Link. Todas las rutinas están dentro del chip Bluetooth y nada es transmitido en plano. Los procedimientos de seguridad son iniciados antes de establecer algún canal. Aparte del cifrado, tiene autenticación PIN y seguridad MAC. Su metodología consiste en compartir una clave de enlace secreta entre un par de dispositivos. Para generar esta clave, se usa un procedimiento de "pairing" (emparejamiento) cuando los dos dispositivos se comunican por primera vez. (Rodríguez Saucedo, 2012 pág. 49)

#### *1.2.4.2. Zigbee IEEE 802.15.4*

El término ZigBee describe un protocolo inalámbrico normalizado para la conexión de una Red de Área Personal Inalámbrico o WPAN. (Acosta, 2006 pág. 23)

ZigBee es diferente de los otros estándares inalámbricos, ha sido diseñado para soportar un diverso mercado de aplicaciones con una conectividad más sofisticada que los anteriores sistemas inalámbricos. El estándar enfoca un segmento del mercado no atendido por los estándares existentes, con baja tasa de transmisión de datos, bajo ciclo de servicio de conectividad y bajo costo. (Acosta, 2006 pág. 23)

La razón de promover un nuevo estándar, es para permitir la interoperabilidad entre dispositivos fabricados por compañías diferentes. ZigBee es un estándar donde el estándar IEEE 802.15.4 solo contempla las capas PHY (Physical Layer) y MAC (Médium Access Control); las capa NWK (Network Layer) y APS (Application Layer) han sido establecidas por la Alianza ZigBee. (Acosta, 2006 pág. 23)

*Características*

Según Acosta (2006 págs. 23-24) las características que presenta el protocolo, son las siguientes:

- Bajo consumo de energía.

- Los dispositivos que conforman la red deben estar conscientes de la cantidad de energía existente. Considere una casa del futuro con 100 dispositivos de control o censado inalámbrico.
- Los dispositivos de ZigBee serán más ecológicos que sus predecesores, ahorrando megavatios de energía a despliegue total.
- Bajo costo en los dispositivos, la instalación y el mantenimiento.
- Los dispositivos ZigBee extenderán la vida de las baterías, las mismas que no necesitarán recarga sino hasta varios años después. La simplicidad de ZigBee permite la creación de redes que requieren poco mantenimiento.
- Redes de alta densidad de nodos. ZigBee permite que las redes manejen hasta 216 dispositivos. Este atributo es fundamental para la creación de series masivas de sensores y redes de mando.
- Presenta un stack de protocolos simple. Se estima que el stack de ZigBee es aproximadamente 1/4 del stack de protocolos de Bluetooth u 802.11. Siendo esta simplicidad esencial para el costo, interoperatibilidad, y mantenimiento.
- Implementación global. La capa física del IEEE 802.15.4 adoptada por ZigBee se ha diseñado para la banda de 868 MHz en Europa, la banda de 915 MHz en Norte América, Australia, etc.; y la banda de 2.4 GHz que es reconocida como una banda global aceptada en casi todos los países.

*Arquitectura*

La arquitectura definida para este protocolo se puede observar en la fig. 2-1.

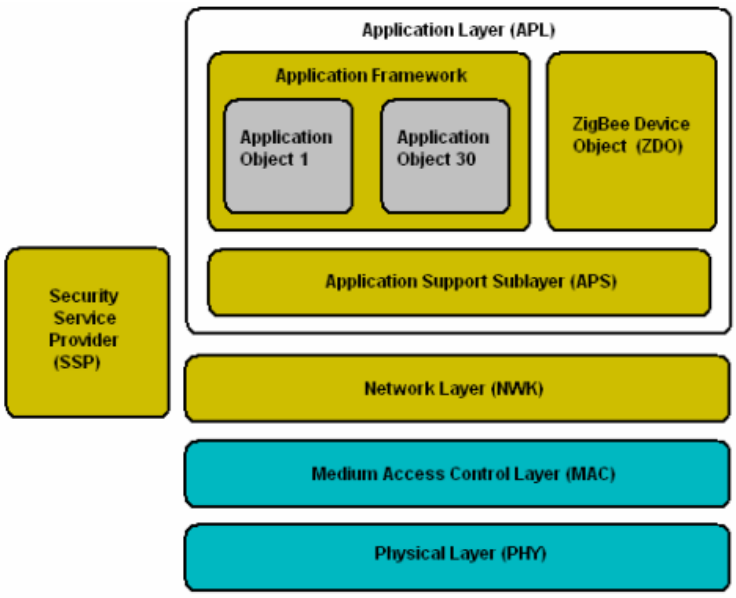


**Figura 2-1** Stack de protocolos ZigBee

**Fuente:** Acosta María, 2006.

- **Application Layer (APL)**

La capa aplicación ZigBee consiste de la subcapa Applications Supports (APS), ZigBee Device Object (ZDO) y la Application Object (objeto aplicación) definidos por el fabricante. (Acosta, 2006 pág. 30)

- **Network Layer (NWK)**

La capa red se construye sobre las características de la capa MAC del estándar IEEE 802.15.4, para permitir una mayor cobertura de la red con lo que nuevas redes podrán ser adicionadas para consolidarse o dividirse según la aplicación que se requiera. Debido a que el stack de protocolos de ZigBee es relativamente simple comparado con otros stacks de protocolos de comunicaciones. (Acosta, 2006 pág. 31)

- **Medium Access Control Layer (MAC)**

La subcapa MAC del protocolo IEEE 802.15.4 provee un interfaz entre la capa física y las capas superiores de los LR-WPANs. Presenta las siguientes características:

- Asociación/disociación
- Acuse de recibo (ACK)
- Mecanismos de acceso al canal
- Validación de trama
- Control de garantía de ranuras de tiempo (Slot Time)
- Control de guías (Beacon) • Sondeo del canal (Scan)

MAC proporciona dos tipos de servicios hacia las capas superiores, a través de dos Puntos de Acceso a Servicios (Service Access Points, SAPs):

- A los servicios de datos MAC se acceden por medio de la parte común de la subcapa MCPS-SAP (MAC Common Part Sublayer-Service Access Point).
- Al manejo de servicios MAC se accede por medio de la capa MAC de manejo de identidades MLME-SAP (MAC Layer Management Entity-Service Access Point).

- **Physical Layer (PHY)**

La capa física es la responsable de la transmisión y la recepción de datos en un canal de radio y acorde con las técnicas de modulación y spreading. La IEEE 802.15.4 ofrece tres bandas de frecuencia en las cuales operar: 2.4 GHz, 915MHz y 868 MHz. El estándar IEEE 802.15.4 utiliza la técnica DSSS (Direct Secuence Spread Spectrum) para transmitir la información a través del medio. Además, las velocidades de transmisión son de 250 Kbps en la banda de 2.4 GHz, 40 Kbps en la banda de 915 MHz y 20 Kbps en la banda de 868 MHz. (Acosta, 2006 pág. 53)

*Parámetros de Modulación*

Si se emplean las frecuencias de 915 MHz y 868 MHz la señal es modulada con BPSK (Binary Phase Shift Keying). Mientras que a la frecuencia 2.4 GHz se emplea una técnica de modulación O-QPSK. (Acosta, 2006 pág. 58)

En términos de eficiencia (energía requerida por bit), la modulación ortogonal mejora su funcionamiento en 2 dB que BPSK. Sin embargo, en términos de sensibilidad de recepción, a las frecuencias 868MHz y 915 MHz se tiene una ventaja de 6-8 dB debido a que tiene velocidades de transmisión más bajas. (Acosta, 2006 pág. 58)

*Establecimiento de Conexión*

Sólo es posible la comunicación entre el maestro y los esclavos, nunca entre varios esclavos.

- **Establecimiento del enlace**

El establecimiento del enlace se lleva a cabo mediante el Link Manager Protocol (LMP). El enlace físico es una secuencia de trasmisión sobre un canal físico de time-slots alternados entre el maestro y el esclavo. (Acosta, 2006 pág. 108)

- **Establecimiento del canal**

Después del establecimiento del enlace físico, se debe establecer un canal Bluetooth (enlace lógico) entre ambos dispositivos mediante el protocolo L2CAP. (Acosta, 2006 pág. 108)

- **Establecimiento de la conexión**

Finalmente, se establece la conexión entre las aplicaciones de los dos dispositivos. Por ejemplo, la conexión entre el ordenador y el móvil (una aplicación basada en el puerto serie) RFCOMM se inicializa y establece la conexión entre los dispositivos. (Acosta, 2006 pág. 108)

Una vez que la conexión ya ha sido establecida, el maestro envía el primer paquete de tráfico, mientras que el esclavo responde con cualquier tipo de paquete. (Acosta, 2006 pág. 109)

*Seguridad*

En cuanto a seguridad, ZigBee puede utilizar la encriptación AES de 128bits, que permite la autentificación y encriptación en las comunicaciones. Además, existe un elemento en la red llamado Trust Center (Centro de validación) que proporciona un mecanismo de seguridad en el que se utilizan dos tipos de claves de seguridad, la clave de enlace y la clave de red. (Moreno, y otros, 2007 pág. 8)

- **Seguridad MAC**

Cuando una trama en la capa MAC tiene que ser asegurada, ZigBee tiene que usar la capa de seguridad que se indica en la especificación 802.15.4. La capa MAC se encarga de su propio proceso de seguridad, aunque sean las capas superiores las encargadas de determinar el nivel de seguridad a usar. (Moreno, y otros, 2007 pág. 25)

- **Seguridad NWK (Red)**

Cuando una trama en la capa de red necesita ser asegurada, ZigBee debe usar ciertos mecanismos de protección de los datos. Al igual que la capa MAC, el mecanismo de protección de trama en la capa de red NWK la encriptación AES (Advanced Encription Standard). Sin embargo, son las capas superiores las que deben indicar el nivel de seguridad que se tiene que aplicar. (Moreno, y otros, 2007 pág. 25)

La capa de red tiene que enviar como broadcast sus peticiones de enrutado y recibir las respuestas. Si la clave es adecuada, la capa de red usa esta clave de enlace para asegurar sus tramas de red. Si por el contrario no lo es, para poder asegurar los mensajes de la capa de red usa su propia clave de red para asegurar las tramas de red. (Moreno, y otros, 2007 pág. 26)

- **Seguridad en APL**

Cuando una trama en la capa APL necesita ser asegurada, la subcapa APS es la encargada de gestionar dicha seguridad. La capa APS permite que la seguridad de trama se base en las claves de enlace y de red (Link y Network Keys) como se ha visto en apartados anteriores. (Moreno, y otros, 2007 pág. 26)

### *1.2.4.3. UWB IEEE 802.15.3*

El estándar IEEE 802.15.3 se desarrolló debido a la necesidad de crear WPANs que fueran capaces de transmitir datos de manera rápida, y eficiente. Para esto fue necesario integrar un grupo de trabajo que se encargara de elaborar las bases para realizar este estándar. Con esto en diciembre de 1999 la IEEE autoriza la creación del grupo de trabajo IEEE 802.15.3 quien en agosto de 2003 fue el encargado de publicar el primer borrador de dicho estándar, en el que se especifican los requerimientos en la capa física y para el control de acceso a medios. (Archundia, 2003 pág. 112)

A principios del año 2003, con la aprobación de la FCC, para la utilización y delimitación de un gran ancho de banda para las señales de RF denominadas UWB (ultra wide band por sus siglas en inglés), la IEEE escoge otro grupo de trabajo que poseen los mismos objetivos que el grupo de trabajo IEEE 802.15.3, con la variante de que este grupo es el encargado de estandarizar la utilización de las UWB. Este nuevo grupo es conocido como el IEEE 802.15.3a, los cuales estudian las propuestas de las principales empresas interesadas en desarrollar y vender productos basados en este nuevo estándar. (Archundia, 2003 pág. 113)

*Características*

Según Camargo (2009 págs. 36-37) las características que presenta el protocolo, son las siguientes:

- El grupo de trabajo IEEE 802.15.3 se preocupó en desarrollar un estándar que fuera barato en su implementación y en sus costos de operación, por lo que este estándar es poco complejo. Otra razón para que sea sencillo es que mientras más simple sean los protocolos, el formato de las tramas, la modulación, etc., de un estándar la transmisión de datos es más eficiente y por lo tanto más rápido.
- La red formada con este estándar tiene características que la hacen segura ya que cuenta con encriptación compartida de información basada en el estándar Advanced Encryption Standard (AES 128).

- Es fácil de utilizarse e implementarse. Tiene un coordinador dinámico de selección y de handover. No depende de una red con backbone. Además, está diseñado para trabajar en un ambiente multirutas.
- El IEEE 802.15.3 trabaja en la banda libre ISM (industrial, scientific, medical) de los 2.4 GHz.
- El grupo de trabajo definió cinco rangos de velocidad de transmisión. 11, 22, 33, 44 y 55 Mb/s.
- Los canales tienen un ancho de banda de 15 MHz. Con 3 o 4 canales libres de traslape (3 canales alineados con el IEEE 802.11b, para su coexistencia).
- La potencia de transmisión de datos es aproximadamente de 8 dBm. Para un rango de aproximadamente de 30 – 50 metros.

*Arquitectura*

Las estructuras de superframe consisten en 3 secciones de tiempo como se muestra en la figura 3-1.

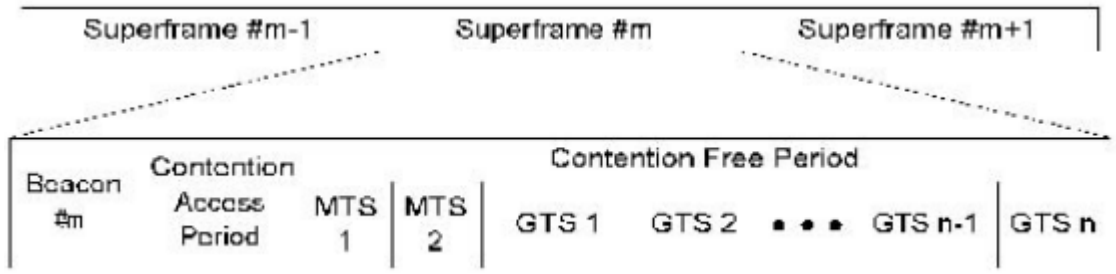


**Figura 3-1** Estructura en el tiempo de las Superframes

**Fuente:** John Barr, 2002.

- Beacon; transmite información de control a toda la picored, localización de recursos (GTS) por trama y proporciona sincronización en tiempo.
- Periodo opcional de acceso a contención (CAP) (CSMA/CA); utilizado en la autentificación, solicitud y respuesta de asociación, parámetros de flujo, negociación y demás comandos del frame.
- Periodo libre de contención (CFP); formado por ranuras de tiempo unidireccionales (GTS) que son asignadas por el dispositivo maestro, para transmisión datos de forma asíncrona o sincronizada; de manera opcional se encuentra el Management Time Slots (MTS) en lugar del CAP para frames de comandos.

*Parámetros de Modulación*

Cada banda utilizaria frequency hopping con multiplexado ortogonal y multiplexado de división de frecuencia (TFI – OFDM), lo que permitiria a cada banda en el UWB ser dividido en un conjunto de canales ortogonales (con una mayor duración en el periodo de los símbolos). Debido al incremento en la longitud del periodo en los símbolos OFDM, esta modulación puede reducir exitosamente los efectos de ISI. Sin embargo, su robusta tolerancia a las múltiples trayectorias, afecta la complejidad del transceptor, incrementa la necesidad la combatir la interferencia entre portadoras y restringe los elementos lineales de los circuitos amplificadores.

*Establecimiento de Conexión*

Este estándar tiene una topología centralizada en una conexión orientada tipo adhoc. El dispositivo coordinador conserva la sincronía y el tiempo en la red, vigila el ingreso de nuevos dispositivos a la red, concede los tiempos para conexiones entre los dispositivos 802.15.3, etc. (Archundia, 2003 págs. 114-115)

El tipo de comunicación entre dispositivos es peer to peer y soporta QoS multimedia; con una arquitectura TDMA de super-tramas con GTS (Guaranteed Time Slots), además tiene técnicas de autentificación y encriptación. (Archundia, 2003 pág. 115)

El estándar se caracteriza por ser robusto. La selección de canales es dinámica y existe un control de energía de transmisión por link. Otra característica que le da fuerza al estándar es el protocolo de handover. (Archundia, 2003)

*Seguridad*

Una característica importante en este estándar es que los niveles de seguridad pueden variar, de acuerdo a las necesidades del usuario.

- El modo 0 significa que no existe seguridad.
- El modo 1 permite al usuario restringir el acceso a la picored. El usuario puede especificar, de forma externa, que dispositivos pueden formar parte de la conexión asíncrona.
- El modo 2 proporciona autentificación por criptografía, protección de la información del usuario e integración de comandos.
- El modo 3 ofrece protección de la información del usuario, integridad de los datos y los comandos, así como autentificación por criptografía.

#### *1.2.4.4. Z-Wave*

*Características*

Los dispositivos de Z-Wave pueden comunicarse de punto a punto hasta 30 metros por sí solos, pero alcanzan fácilmente rangos efectivos de hasta 100 metros. Cada red Z-Wave puede admitir hasta 232 dispositivos, lo que le permite la flexibilidad de agregar tantos dispositivos como desee. Trabaja en la banda de los 868MHz evitando la gran cantidad de emisoras en la banda de los 2,4GHZ y puede llegar a trabajar a 40 kbit/s pudiendo operar en rangos de hasta 30 metros en condiciones ideales. Usan tecnología de encriptación AES-128.

*Arquitectura*

Z-Wave se basa en una red tipo mesh. Esto significa que cada dispositivo instalado en la red se convierte en un repetidor de señal. Como resultado, cuantos más dispositivos tenga en su hogar, más fuerte se volverá la red.

El sistema define dos tipos básicos de dispositivos:

- Los controladores siempre son conocedores de la organización de toda la red con el objeto de poderse comunicar con cualquier nodo. El primer controlador que instalemos tomará el papel de controlador primario y será el encargado de crear la red. Solo puede existir un controlador primario por red Z-Wave y él solo tendrá suficiente potestad para añadir y eliminar nodos de la red.
- Los esclavos son los dispositivos que reciben comandos, los ejecutan y responden. Un esclavo no puede intercambiar información directamente con otro esclavo.

*Parámetros de Modulación*

- Ancho de banda: 9.6 ó 100 Kbps, ambas velocidades son totalmente interoperables
- Modulación: codificación de canal GFSK Manchester
- Banda de frecuencia: Z-Wave Radio utiliza el 868.42 MHz Banda SRD (Europa, banda ISM de 900 MHz: 908.42 MHz (Estados Unidos); 916 MHz (Israel); 919.82 MHz (Hong Kong); 921.42 MHz (Australia / Nueva Zelanda).

### 1.2.5. *Comparativa Bluetooth vs Zigbee vs Z-Wave*

Para la realización de la tabla comparativa se utilizará el método denominado "Escala de Likert", para obtener resultados que permiten una selección sustentada la calificación de cada uno de los indicadores se basa en la escala presentada en la tabla 1-1.

**Tabla 1-1** Escala de valoración para el procesamiento de información

| ESCALAS DE VALORACIÓN CUALITATIVA | | | |
|---|---|---|---|
| **1** | **2** | **3** | **4** |
| Malo | Regular | Bueno | Muy Bueno |
| Avanzado | Intermedio | Básico | Principiante |
| No | | | Si |

**Fuente:** (QuestionPro, 2015)

**Realizado por:** Vilañez, Daniel, 2018

En la tabla 2-1 se muestran las características más relevantes para el desarrollo de la red de las tecnologías WPAN conjuntamente con un protocolo adicional que comparte características similares y es considerado una red de área personal.

**Tabla 2-1** Características Tecnologías WPAN

| Tecnologías Inalámbricas | | | |
|---|---|---|---|
| **Variable** | **Bluetooth** | **Zigbee** | **Z-Wave** |
| **Topología** | Punto a Punto, Multipunto Piconet | Punto a Punto, Multipunto Subred | Punto a Punto, Multipunto |
| **Tasa de Transferencia** | Hasta 3000 Kbps | Hasta 250 Kbps | Hasta 100 Kbps |
| **Cobertura** | Optimo: hasta 10 m, hasta 60m | Entre 10 y 75 m | Hasta 40 m |
| **Tamaño de la red** | Hasta 8 nodos | Hasta 65.000 nodos | Hasta 232 nodos |
| **Seguridad** | Autenticación PIN y seguridad MAC | 128-bit AES | 128-bit AES |

**Fuente:** (Archundia, 2003) (Acosta, 2006) (Ventajas de la tecnología Near Field Communication (NFC) como sistema de pago electrónico, 2016)

**Realizado por:** Vilañez, Daniel, 2018

En la tabla 3-1 se muestra la evaluación de las características de las tecnologías.

**Tabla 3-1** Evaluación de Indicadores de la Tecnología

| TECNOLOGÍAS INALÁMBRICAS | | | |
|---|---|---|---|
| **VARIABLE** | **BLUETOOTH** | **ZIGBEE** | **Z-Wave** |
| **Topología** | | | |
| Punto a Punto | Si | Si | Si |
| Punto Multipunto | Si | Si | Si |
| **Tasa de Transferencia** | | | |
| Entre 0 y 1 Mbps | Si | Si | Si |
| Mayor que 1 Mbps | Si | No | No |
| **Cobertura** | | | |
| Entre 0 y 30 m | Muy bueno | Muy Bueno | Muy Bueno |
| Entre 30 y 100 m | Regular | Bueno | Bueno |
| **Tamaño de la Red** | | | |
| Entre 1 y 32 nodos | Bueno | Muy Bueno | Muy Bueno |
| Entre 33 y 65 000 nodos | Malo | Muy Bueno | Regular |
| **Seguridad** | | | |
| Datos Encriptados | Muy Bueno | Bueno | Muy Bueno |
| Soporta transmisiones seguras | Muy Bueno | Muy Bueno | Muy Bueno |

**Realizado por:** Vilañez, Daniel, 2018

La calificación definitiva de la solución en base a cada parámetro de comparación, se obtiene sumando los puntajes obtenidos del análisis, utilizando las siguientes fórmulas:

$$Cc_{Bluetooth} = \left(\frac{P_{Bluetooth}}{Pt}\right) x\ 100\%$$

$$Cc_{Zigbee} = \left(\frac{P_{Zigbee}}{Pt}\right) x\ 100\%$$

$$Cc_{Z-Wave} = \left(\frac{P_{Z-Wave}}{Pt}\right) x\ 100\%$$

En donde:

$Pt$: Representa la base del puntaje sobre la cual se está calificando

$P_{Bluetooth}$: Puntaje acumulado por la tecnología Bluetooth.

$P_{Zigbee}$: Puntaje acumulado por la tecnología Zigbee.

$P_{Z-Wave}$: Puntaje acumulado por la tecnología Z-Wave.

$Cc_{Bluetooth}$: Porcentaje de la calificación total que obtuvo Bluetooth.

$Cc_{Zigbee}$: Porcentaje de la calificación total que obtuvo Zigbee.

$Cc_{Z-Wave}$: Porcentaje de la calificación total que obtuvo Z-Wave.

Para aplicar las fórmulas primero obtenemos los puntajes de cada una de las tecnologías, para lo cual aplicamos la conversión a valores presentadas en la Tabla 1-1, dando como resultado:

$$P_{Bluetooth} = 4 + 4 + 4 + 4 + 4 + 3 + 2 + 1 + 4 + 4 = 34$$
$$P_{Zigbee} = 4 + 4 + 4 + 1 + 4 + 3 + 4 + 4 + 3 + 4 = 35$$
$$P_{Z-Wave} = 4 + 4 + 4 + 1 + 4 + 3 + 4 + 2 + 4 + 4 = 34$$

La base del puntaje sobre la cual se está calificando es:

$$Pt = 40$$

Con lo cual la calificación de cada una de las tecnologías queda de la siguiente manera:

$$Cc_{Bluetooth} = \left(\frac{34}{40}\right)\ x\ 100\% = 85\%$$

$$Cc_{Zigbee} = \left(\frac{35}{40}\right)\ x\ 100\% = 87{,}5\%$$

$$Cc_{Z-Wave} = \left(\frac{22}{40}\right)\ x\ 100\% = 85\%$$

Luego de haber realizado el análisis comparativo de las tecnologías inalámbricas Bluetooth, Zigbee y Z-Wave, el puntaje obtenido para cada uno de los indicadores nos muestra como resultado que la tecnología basada en Zigbee ha obtenido el puntaje más alto con un porcentaje del 87,5% que equivale a 35 frente al 85% alcanzado por las tecnologías Bluetooth y Z-Wave equivalente a 34, los índices más importantes para esta aplicación son topología, tamaño de la red y seguridad que hacen de Zigbee una tecnología óptima para el prototipo.

## 1.3. **Sistemas de Seguridad**

Conjunto de componentes e infraestructura requeridos para brindar a las personas y bienes materiales presentes en una localidad determinada, protección frente a percances, tales como robo, atraco o sabotaje e incendio. (CEi1, 2016 pág. 1)

Así, en un percance, en principio lo detectará, luego lo señalizará, para posteriormente iniciar las acciones encaminadas a disminuir o extinguir los efectos. Los sistemas de seguridad pueden ser variables según las necesidades de la localidad a proteger y del presupuesto disponible pare ello. (Gormaz, 2007 pág. 50)

En el mercado existe un gran abanico de componentes con características técnicas y calidades distintas, que hacen que no se pueda tipificar a la hora de la realización de diseños de los sistemas de seguridad. (CEi1, 2016 pág. 2)

### 1.3.1. *Clasificación de los sistemas de seguridad*

El CEi1 (2016 págs. 3-4) expone cuatro grandes bloques de aplicación de los sistemas de seguridad:

- **Robo y atraco**

- Sensores y centrales de alarma.
- Defensa física.
- Aviso central receptora de alarma.
- Señalización de robo.
- Dispositivos de acceso.

- **Incendio**

- Sensores y centrales de incendio.
- Aviso central receptora de alarma.
- Accionamiento de dispositivos de extinción.
- Accionamiento de sistemas de aviso y señalización.
- Extinción manual.
- Bocas de incendios equipadas.
- Equipo de bombeo.
- Puertas cortafuegos.
- Alumbrado de emergencia.

- **Anti-hurto**

- Protección de artículos.
- Scanner detector de rayos X.
- Detector de explosivos.
- Arco detector de metales.

- **Especiales**

- Detector de metales.
- Sonda detectora de niveles.
- Sonda detectora de humedad.
- Detector de sustancias químicas.
- Detector de presión.
- Detector de drogas.
- Detector de gases.
- Etc.

### 1.3.2. *Composición de un sistema de seguridad*

Una instalación se compone de ciertas partes básicas: central de alarma, sensores y sistemas de aviso y señalización, ver figura 4-1. A estos se les puede sumar un cuarto elemento que sería el intercomunicador con la Central Receptora de Alarmas y que siempre es opcional su colocación en la instalación, aunque es absolutamente aconsejable su utilización. (CEi1, 2016 pág. 4)

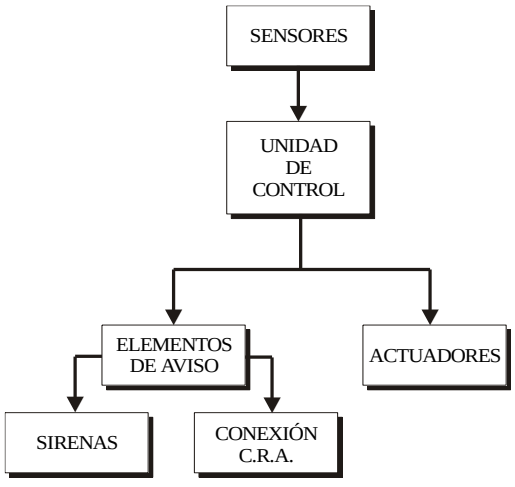


**Figura 4-1** Esquema de composición de un sistema de seguridad.

**Fuente:** CEi1, 2016.

#### *1.3.2.1. Central de alarmas o unidad de control.*

La central de alarmas es la que recibe la señal eléctrica de los detectores o sensores que por algún motivo son activados. Al recibir esta señal, los circuitos electrónicos que lleva en su interior, hacen que se pongan en marcha el sistema de alarma y aviso. (Gormaz, 2007 pág. 53)

Los sensores son elementos capaces de comprobar las variaciones de una condición de reposo en un lugar determinado y envían información de esa variación a la Central de Alarmas. Son de reducido tamaño y se alimentan a través de una fuente de alimentación de baja tensión. (CEi1, 2016 pág. 5)

#### *1.3.2.2. Sistemas de aviso y señalización.*

Son los dispositivos encargados de avisar de las variaciones detectadas por los sensores dentro del sistema de seguridad. Son los que dan sentido a los sistemas de seguridad, pueden ser acústicos, ópticos y mensajeros para la Central Receptora de Alarmas. (Gormaz, 2007 pág. 54)

#### *1.3.2.3. Central Receptora de Alarmas.*

Su cometido consiste en recibir la señal de activaci6n de alarma y comunicar al usuario la existencia de la misma, para que se ponga en marcha los mecanismos establecidos en cada instalación en particular, que pueden variar según el tipo de alarma activado. (CEi1, 2016 pág. 6)

A la central de alarmas están conectados todos los sistemas de seguridad vigilados a distancia. En el momento de la activación de cualquiera de ellas, nos proporciona la información exacta de la alarma activada. (CEi1, 2016 pág. 6)

Si dado el volumen de instalaciones diferentes en puntos geográficos distintos conectados a ella, se producen varias a la vez, esta efectúa una selección de las alarmas más importantes y las posiciones en pantalla, mostrándosela al vigilante, pare posteriormente ir pasando el resto de los avisos de alarma. (Gormaz, 2007 pág. 56)

La central receptora de alarmas está conectada a un ordenador central que se encarga de almacenar toda la información que le va llegando de las instalaciones, conexión, desconexión, aviso de alarma, avisos de pre alarma, avisos de avería. etc. (Gormaz, 2007 pág. 57)

#### *1.3.2.4. Dispositivos de conexión / desconexión.*

Mecanismos que permiten la conexión y desconexión de los sistemas de seguridad. Pueden ser de tipo mecánico, como las llaves, o de tipo electrónico, como el teclado. (CEi1, 2016 pág. 6)

La llave de seguridad consiste en conectar o desconectar un circuito eléctrico mediante una llave metálica con una forma especial, que al introducirla acciona un mecanismo que abre o cierra un circuito eléctrico. (CEi1, 2016 pág. 7)

Mediante el teclado se eliminan las posibilidades de sustracción, con lo que sólo puede desactivar la central de alarma aquella o aquellas personas que conozcan la clave. Esta clave está formada por la pulsaci6n de 3 o 4 números del teclado. (Gormaz, 2007 pág. 59)

#### *1.3.2.5. Accionamiento de otros dispositivos.*

El sistema empleado puede proporcionarnos ciertas posibilidades a la hora de la activación de la alarma:

- Activación de luces de emergencia.
- Activación de electroimanes de puertas cortafuegos para cerrar puertas.
- Señal de alarma a central, sin activar sirenas y elementos ópticos.

En todo caso, siempre dependerá de las centrales de alarma utilizadas, que cuanto más sofisticadas y completas sean, más posibilidades externas nos darán, posibilitando así la realización de un sistema de seguridad fiable y seguro. (CEi1, 2016 pág. 7)

### 1.3.3. ***Sistema de Seguridad Anti hurto***

Uno de los métodos más seguros y comunes para proteger los hogares se basa en la instalación de sistemas de alarma adaptados a las características de la residencia. Aunque la instalación de una alarma no la hace completamente segura, sí proporciona mayor tranquilidad a los propietarios. (Martínez, 2012 pág. 1)

Si al sistema de alarma se le suman sensores mejorará la protección y seguridad. Los sensores de movimientos solos tal vez no conseguirán proveer de una seguridad apta, debido a que trabajarán solamente cuando alguien ingrese a la residencia. También pueden dar falsos positivos al detectar

mascotas. Sin embargo, algunos de los sistemas permiten ajustar algunas opciones cuando estés dentro de la casa, para evitar falsos positivos. (Martínez, 2012 pág. 1)

#### *1.3.3.1. Complementos para un Sistema de Alarma*

Los sensores básicos que componen un sistema de alarma, se listan a continuación:

- Sensores de apertura en puertas y ventanas: detectan la invasión en el hogar. Cuando esto sucede, el sensor envía una señal.

- Sensores de movimiento: Actúan ante la detección de movimientos. Su principal ventaja es la facilidad de instalación.

- Sensores de sonido: Este dispositivo se activa mediante la captación de sonidos como puede ser la ruptura de cristales.

- Protección contra fugas e inundaciones: Algunas de estas instalaciones pueden cortar el suministro eléctrico. Los detectores de gas se activan en el momento que registran una concentración determinada en el área.

#### *1.3.3.2. Simuladores de Presencia*

Otro medio de seguridad para la residencia son los sistemas domésticos que encienden y apagan las luces del hogar, además de levantar y bajar persianas o encender la televisión o la radio. Con esto se busca mantener alejados a los delincuentes. (Martínez, 2012 pág. 1)

### 1.3.4. ***Instalaciones de Gas***

Las viviendas actualmente cuentan con instalaciones que permiten la circulación de GLP (gas licuado de petróleo), las cuales representan un riesgo para la integridad de las personas y de la vivienda.

#### *1.3.4.1. Composición del GLP*

El GLP tiene dos orígenes: el 60% de la producción se obtiene durante la extracción de gas natural y petróleo del suelo. El 40% restante se produce durante el refinado de crudo de petróleo. El GLP es, por tanto, un producto secundario que existe de forma natural. Los principales elementos que

constituyen el GLP son: propano y butano, y en menor proporción se pueden encontrar: isobutanos, propilenos y butenos. (Venegas, y otros, 2017 págs. 17-18)

#### *1.3.4.2. Toxicidad del GLP*

El GLP no es tóxico, sin embargo, la acción fisiológica que se produce en el organismo cuando se lo inhala produce un efecto anestésico. (Venegas, y otros, 2017 pág. 34)

#### *1.3.4.3. Olor y Color del GLP*

En estado natural, el GLP no tiene olor ni color, y al ser un combustible, en caso de una fuga para poder detectarlo, se le añade pequeñas cantidades de sustancias que le dan un olor característico, fuerte y no tan agradable, llamadas mercaptanos. (Venegas, y otros, 2017 pág. 34)

#### *1.3.4.4. Riesgos del GLP*

El manejo de GLP genera riesgos por su utilización al ser un combustible. NFPA ha establecido un sistema para la identificación de los peligros de un material en términos de tres categorías principales: salud, inflamabilidad e inestabilidad. (Venegas, y otros, 2017 págs. 35-36)

Para el caso del GLP se tienen las siguientes calificaciones para la clasificación de riesgos:

- Peligro de salud: leve = 1.
- Peligro de inflamación: es un gas inflamable = 4.
- Peligro de inestabilidad = 0.
- Peligros especiales = ninguno.

## 1.4. **Redes IoT**

El Internet de las cosas (IoT) percibe un mundo donde los dispositivos que lo conforman pueden ser identificados en el Internet y está creciendo a un ritmo acelerado con nuevos dispositivos que se van conectando. En este sentido, las redes de sensores inalámbricos juegan un papel importante para incrementar la ubicuidad de las redes con dispositivos inteligentes de bajo costo y fácil implementación, que se integran en el concepto de IoT para traer nuevas experiencias en las actividades de la vida diaria, como por ejemplo en aplicaciones para hogares y oficinas confortables, salud, vigilancia del medio ambiente y ciudades inteligentes. En el presente artículo

se relacionará a la red de sensores inalámbricos con el Internet de las cosas a través de estándares y protocolos. (Las redes de sensores inalámbricos y el Internet de las cosas, 2012)

### 1.4.1. *Aplicaciones*

Existen variedad de aplicaciones para este tipo de redes, según Tarrio (2008) podemos citar algunas aplicaciones de WSN entre las que se destacan:

- Aplicaciones militares:
  - Monitorización de fuerzas y equipos enemigos
  - Vigilancia en el campo de batalla
- Reconocimiento del terreno
  - Detección de ataques biológicos químicos o nucleares, etc.
- Aplicaciones medioambientales:
  - Seguimiento de animales
  - monitorización de las condiciones ambientales en cultivos
  - Riego
  - Agricultura de precisión
  - Detección de incendios forestales
  - Detección de inundaciones
  - Estudios de contaminación
  - Prevención de desastres
  - Monitorización de áreas afectadas por desastres, etc.
  - Estudios sísmicos
  - Seguridad de estructuras
- Aplicaciones médicas:
  - Telemonitorización de datos fisiológicos en pacientes
  - Diagnóstico
  - Administración de medicamentos
  - seguimiento de médicos y pacientes en hospitales, etc.
  - Aplicaciones en el hogar/edificios
  - Domótica
  - Control de electrodomésticos
  - Entornos inteligentes
  - Control ambiental
  - Aplicaciones industriales

– Seguimiento de vehículos
– Control de flota
– Control de inventarios

• Aplicaciones turísticas

– Interactividad en museos y espacios turísticos, control de acceso

### 1.4.2. *Constitución de la red IoT*

En la figura 5-1 se muestra una categorización de elementos internos y elementos externos que conforman Internet de las cosas.

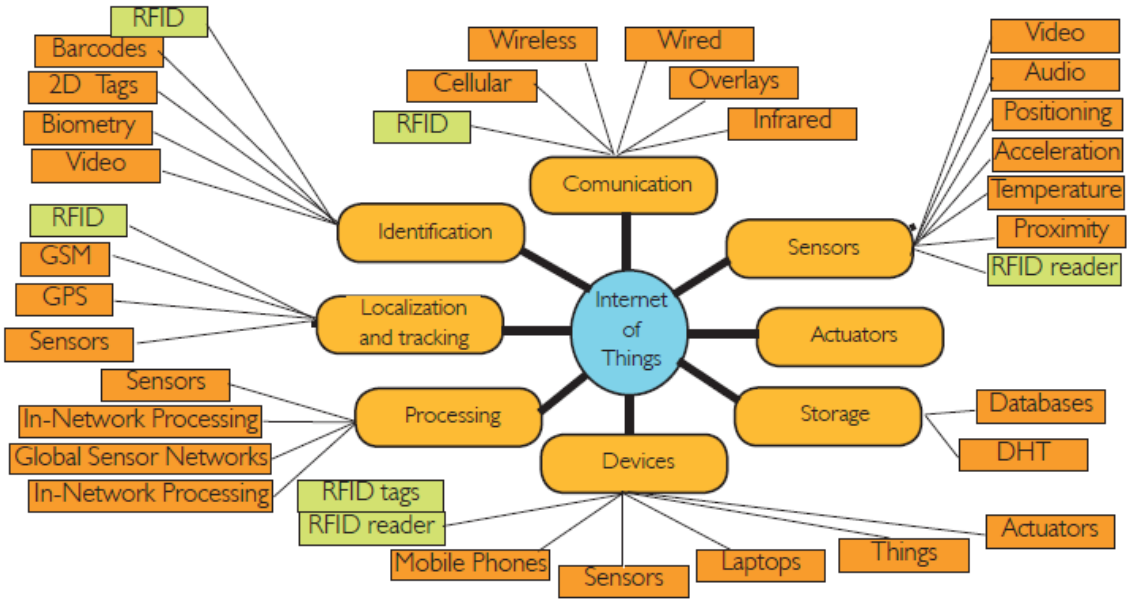


**Figura 5-1** Constitución de la red IoT

**Fuente:** L. Joyanes, J. Delgado, P. García. 2015.

- Comunicación, para permitir el intercambio de información entre dispositivos.
- Sensores, para capturar y representar el mundo físico en el digital.
- Almacenamiento, para los datos recogidos de los sensores y de los sistemas de seguimiento e identificación.
- Actuadores, para llevar a cabo las acciones dirigidas desde el mundo digital al físico.
- Dispositivos de interacción con humanos en el mundo físico.
- Procesamiento, para proporcionar datos a los sistemas de minería de datos y a los servicios.
- Localización y seguimiento, para la determinación de la ubicación física y el seguimiento.
- Identificación, para proporcionar la identificación única de un objeto físico en el mundo
- digital.

### 1.4.3. *Ventajas*

La comunicación inalámbrica en aplicaciones industriales tiene muchas ventajas las cuales enlistaremos a continuación: (Redes de sensores inalámbricos, 2006 pág. 2)

- Mayor fiabilidad.
- Bajo coste de instalación: prescindir de los cables significa que las instalaciones son más baratas.
- La naturaleza ad hoc de WSN permite un sencillo ajuste y configuración: para apoyar la cobertura de sensores inalámbricos a nivel de planta se ha de minimizar el trabajo manual de configuración de la red.
- Configuración de tipo 'plug and produce' (enchufar y producir) de la red permite desplegar redes temporales de sensores para garantizar el mantenimiento o la localización y corrección de fallos

A nivel de hogar a continuación se presentan algunas de las principales ventajas de IoT: (Casco, 2015)

- Interacción entre objetos: los dispositivos en el hogar pueden intercambiar información y actualizar datos entre sí.
- Interpretación del entorno y manipulación: los dispositivos podrán manejar el entorno al recibir información de otros dispositivos o por la interpretación del contexto.
- Capacidad de localización: es más fácil localizar objetos.
- Identificación y personalización: los objetos dejarán de ser impersonales y existirá la posibilidad de identificar su procedencia y propietario mediante distintas tecnologías.

### 1.4.4. *IoT (internet de las cosas por sus siglas en inglés)*

Internet de las cosas lo cambiará todo debido al impacto que Internet ha tenido sobre muchos aspectos como lo son: la educación, la comunicación, las empresas, la ciencia, el gobierno y la humanidad. (Evans, 2011 pág. 2)

Se debe tener en cuenta que IoT representa la próxima evolución de Internet, que será un enorme salto en su capacidad para reunir, analizar y distribuir datos que podemos convertir en información, conocimiento y en última instancia, sabiduría. En este contexto, IdC se vuelve inmensamente importante. (Evans, 2011 pág. 2)

Son varios los aspectos que amenazan con rezagar el avance de IoT, como el cambio a IPv6, el desarrollo de un conjunto de estándares en común y la realización de fuentes de energía para millones de sensores diminutos. (Evans, 2011 pág. 2)

#### *1.4.4.1. Arquitectura*

Los pilares sobre los cuales reposa todo lo relacionado con IoT hoy en día se muestra en la figura 6-1, la cual consta de los siguientes componentes: (Londoño, 2016 pág. 6)

- Objetos Conectados
- Tecnologías de red.
- Protocolos de comunicación.
- Plataforma IoT, para el tratamiento inteligente de datos.
- Aplicaciones de usuario.

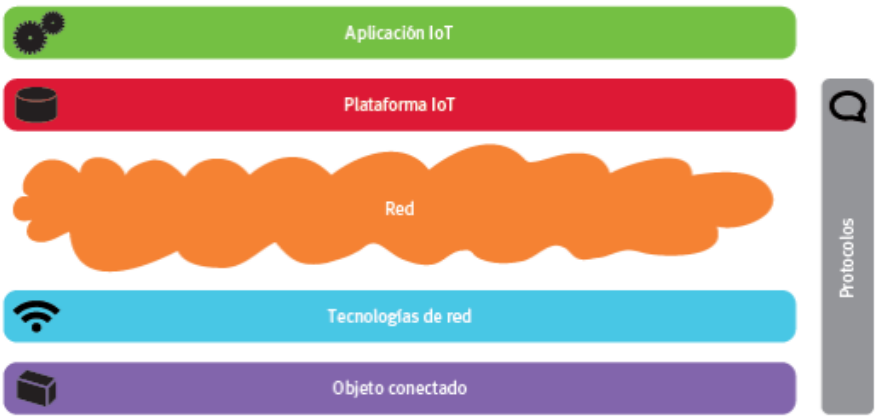


**Figura 6-1** Arquitectura IoT

**Fuente:** Roby Londoño, 2016.

#### *1.4.4.2. Aplicaciones*

El número de aplicaciones y servicios que pueden proporcionar es prácticamente ilimitado y se puede adaptar a muchos campos de la actividad humana, facilitando y mejorando su calidad de vida en múltiples formas. A continuación, enlistamos un número reducido de las aplicaciones que se pueden realizar aplicando IoT.

- Edificios inteligentes conectados
- Aplicaciones domóticas incluyendo sensores y actuadores inteligentes

- Los servicios de salud y educación en el hogar.
- Control remoto de los tratamientos para los pacientes.
- Servicios de cable / satélite.
- Sistemas de almacenamiento / generación de energía. A
- Ciudades inteligentes y transporte
- Integración de los servicios de seguridad.
- Optimización del transporte público y privado.
- Gestión inteligente de los servicios de estacionamiento y el tráfico en tiempo real.
- Gestión inteligente de semáforos en función de las colas de tráfico.
- Localización de los coches que han sobrepasado el tiempo de estacionamiento.
- Administración del Agua. Riego de parques y jardines.
- Contenedores de basura inteligentes.
- Controles de contaminación y movilidad.
- Obtener una respuesta inmediata y conocer las opiniones de los ciudadanos.
- Sistemas de Votación.
- Monitoreo de accidentes
- Coordinación acciones de emergencia.
- Conectividad inteligente
- Gestión de datos y prestación de servicios.
- El uso de medios de comunicación social y las redes sociales.
- La comunicación de grupo interactiva.
- En streaming en tiempo real.
- Juegos interactivos.
- Realidad aumentada.
- Métodos de autenticación biométrica.
- Servicios de computación en nube.
- Visión por computador.
- Antenas inteligentes.

Estas son algunas del sinfín de aplicaciones a las cuales pueden ser sometido el internet de las cosas, las aplicaciones solo están limitadas por la imaginación del ser humano.

#### *1.4.4.3. Seguridad*

El término seguridad se refiere a la provisión de servicios que incluyen confidencialidad, autenticación, integridad, autorización, no repudio y disponibilidad, así como algunos servicios excepcionales de detección de duplicados y paquetes obsoletos. Estos servicios de seguridad se

pueden implementar mediante una combinación de mecanismos criptográficos y no criptográficos. (Seguridad en Internet de las Cosas, 2017 pág. 4)

Con este fin se puede distinguir y analizar distintos aspectos de seguridad en IoT:

1. La arquitectura de seguridad describe a las relaciones físicas entre los componentes del sistema y a la forma en que estas relaciones son administradas durante su ciclo de vida.
2. El modelo de seguridad de un nodo describe cómo se gestionan en los componentes los procesos de seguridad, aplicaciones y parámetros de seguridad.
3. El arranque de seguridad enfatiza el procedimiento para que los objetos establezcan una conexión segura tomando en cuenta la localización y autorización del dispositivo.
4. La seguridad de red detalla los parámetros aplicados en una red para asegurar una operación confiable de IoT.
5. La seguridad de aplicación garantiza la comunicación entre elementos autorizados.

**Comunicación**

La investigación en protocolos de comunicación ha alcanzado medidas que proporcionan autenticidad y confidencialidad como TLS o IPSec. A pesar de que existe fuerte investigación, la alteración de Disponibilidad por ataques distribuidos de denegación de servicio es un tema difícil de tratar. (Seguridad en Internet de las Cosas, 2017 pág. 5)

**Sensores**

La confidencialidad de los datos de los sensores es un requisito débil, ya que un atacante puede colocar su sensor físicamente cerca y recibir los mismos valores. La privacidad se dirige principalmente al mundo físico que está detectando. La disponibilidad de los sensores depende, sobre todo, de la infraestructura de comunicación. (Seguridad en Internet de las Cosas, 2017 pág. 5)

**Actuadores**

La Integridad, Autenticidad y Confidencialidad de los datos enviados a un actuador dependen, en su mayoría, en la seguridad de la comunicación. Lo que sí debe asegurarse es que un atacante no pueda controlar el actuador. Tanto la privacidad como la disponibilidad de los actuadores dependerá del escenario y tipo de actuador, por lo tanto, no se puede dar una valoración general de sensibilidad. (Seguridad en Internet de las Cosas, 2017 pág. 6)

**Almacenamiento**

El empleo de los mecanismos de seguridad para los dispositivos de almacenamiento es muy reducido. Debido a que los ataques con respecto a datos son frecuentes, las regulaciones deben

extenderse para proporcionar la protección adecuada a la Privacidad del usuario. La disponibilidad del almacenamiento depende de la disponibilidad de la infraestructura de comunicaciones y de los mecanismos bien establecidos para la redundancia del almacenamiento. (Seguridad en Internet de las Cosas, 2017 pág. 6)

**Dispositivos**

La integridad dispone que un dispositivo está libre de malware. La confidencialidad tiene estrecha relación con la integridad asegurando que no exista acceso de terceros a los datos del dispositivo. La privacidad de un dispositivo depende de la seguridad física y de comunicaciones. (Seguridad en Internet de las Cosas, 2017 pág. 6)

**Procesamiento**

La integridad en el procesamiento de datos para servicios se basa en la integridad del dispositivo, su comunicación, correcto diseño e implementación de algoritmos de procesado. La autenticidad del procesamiento depende exclusivamente de la autenticidad del dispositivo y de la comunicación, por lo tanto, no es en sí mismo sensible al procesamiento. La disponibilidad del Procesamiento depende de la disponibilidad del dispositivo y de las comunicaciones exclusivamente. (Seguridad en Internet de las Cosas, 2017 pág. 6)

**La localización y el seguimiento**

La confidencialidad y la privacidad de los datos de localización y seguimiento son de gran importancia para asegurar la privacidad del usuario y, por lo tanto, muy sensibles. La privacidad en los datos de localización significa que no hay manera para un atacante el revelar la identidad de la persona u objeto, que los datos de localización están adjuntos a él y que la localización y seguimiento no es posible sin el acuerdo explícito o el conocimiento. La disponibilidad de la localización es importante para asegurar que las señales de referencia para la localización son robustas y no pueden ser manipuladas por un atacante. (Seguridad en Internet de las Cosas, 2017 pág. 6)

**Identificación**

Para la identificación se ven las mismas sensibilidades que para localización y seguimiento. La única diferencia es la mayor sensibilidad respecto a la integridad. Es más fácil, para un atacante, manipular el proceso de identificación que el de localización. Este resultado es debido principalmente a que la tecnología utilizada es más factible de manipular que las tecnologías de localización. (Seguridad en Internet de las Cosas, 2017 pág. 7)

# 2. CAPITULO II: MARCO METODOLÓGICO

En el presente capítulo se analizarán los principales componentes para la realización de la implementación de un prototipo de sistema de seguridad doméstico, el cual estará basado en una red IoT. Para ello se pretende establecer los principales requerimientos que deberá cumplir el sistema de seguridad, la tecnología, los elementos electrónicos y el diseño; según las normativas EN50131, NFPA 730 y NFPA 731 para el sistema de seguridad y los elementos electrónicos, el protocolo IEEE 802.15.4 para la tecnología y el diseño, para así poder implementar el prototipo de sistema de seguridad.

## 2.1. Metodología

### 2.1.1. *Metodología de Investigación*

En el presente documento se utilizan y utilizarán los siguientes tipos de investigación:

- Método Deductivo: En este proceso el razonamiento parte de una o más declaraciones para llegar a una conclusión. La deducción conecta las premisas con las conclusiones; si todas las premisas son ciertas, los términos son claros y las reglas de deducción son usadas, la conclusión debe ser cierta.
- Investigación Aplicada: en este tipo de investigación el énfasis del estudio está en la resolución práctica de problemas. Se centra específicamente en cómo se pueden llevar a la práctica las teorías generales.
- Investigación Documental: es una técnica que consiste en la selección y compilación de información a través de la lectura y crítica de documentos y materiales bibliográficos, bibliotecas, bibliotecas de periódicos, centros de documentación e información.
- Investigación Experimental: es la alteración de una variable experimental o varias al mismo tiempo, en un ambiente estrictamente vigilado por la persona que realiza el experimento. De esta manera el investigador puede evaluar de qué forma o por qué razón sucede algo en particular.
- Investigación Descriptiva: su objetivo es describir la naturaleza de un objeto o segmento demográfico, sin centrarse en las razones por las que se produce un determinado fenómeno.

### 2.1.2. *Metodología de Desarrollo del Prototipo*

La metodología a ser utilizada es una combinación de dos metodologías presentadas a continuación: la primera metodología que es aplicada para elaboración de redes de sensores

inalámbricos la cual consta de 7 pasos, publicada en la revista Universidad, Ciencia y Tecnología de la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" desarrollada por Pérez Juan, Urdaneta Elizabeth, Custodio Ángel. La segunda metodología que es aplicada a la implementación de la tecnología identificación por radiofrecuencia la cual consta de 7 pasos, publicada en Revista de Investigaciones de la Universidad del Quindío. (Metodología para la implementación de la tecnología identificación por radiofrecuencia en entornos industriales y sanitarios en Colombia., 2014 pág. 50) (Pérez, y otros, 2014 págs. 16-17)

1. Definición de indicadores: se establecen los parámetros de evaluación de la red para poder determinar que funciona adecuadamente, basándonos en la metodología propuesta y en los requerimientos que se establecerán a posteriori.
2. Diseño del prototipo: se establecen los requerimientos, la concepción del sistema, se describe cada uno de los nodos, su comunicación y tanto el software como el hardware que se utilizarán para el diseño del prototipo.
3. Implementación del prototipo: una vez establecido el diseño del prototipo se procede a realizar la implementación para posteriormente realizar las pruebas.
4. Pruebas en el prototipo: una vez implementado el prototipo se procede a realizar las pruebas de funcionamiento, las cuales se establecen en el primer punto de esta metodología.
5. Ajustes y monitoreo: una vez realizadas las pruebas en el prototipo se establecerán los puntos en los cuales el sistema esté fallando para posteriormente corregirlos y poder obtener un funcionamiento adecuado de la red

## 2.2. Definición de indicadores

Para la realización del prototipo se utilizará la tecnología Xbee debido a que presenta mejores características para la realización de redes inalámbricas de sensores y por lo cual es ampliamente recomendada por el grupo de trabajo IEEE 802.15 y la alianza Zigbee, en adición a esto en el apartado 1.1.5, en el primer capítulo del presente documento, se expone una comparación entre las dos principales tecnologías de WPAN dando como mejor resultado a la tecnología Xbee. (Zigbee Alliance, 2002)

La definición de indicadores se ha realizado en base a indicadores presentes en la metodología aplicada en la elaboración de redes de sensores inalámbricos citada anteriormente, y además de esto tomando en cuenta los requerimientos definidos para este proyecto.

- Precisión de los sensores: se requiere realizar una prueba con la cual se pueda realizar una calibración adecuada de los sensores, ya que de estos dependerán las condiciones mediante las cuales el sistema alertará al usuario.
- Latencia: es necesario realizar pruebas de latencia debido a que al ser un sistema en tiempo real es indispensable que el sistema posea un tiempo de respuesta corto.
- Pruebas de Conexión: es importante verificar que los datos obtenidos de los sensores y las acciones realizadas por el usuario lleguen a su destino adecuadamente, para así no tener inconvenientes.
- Pruebas de Alerta: es indispensable realizar las pruebas de alerta del sistema para conocer si las alertas llegan adecuadamente al usuario.

## 2.3. Parámetros para Elaboración de Pruebas del Sistema

Para que los nodos puedan conectarse entre sí se debe configurar cada uno de los dispositivos con los parámetros listados en la tabla 1-2. La configuración se realizará en el IDE XCTU que provee la empresa Digi principal fabricante de los dispositivos conocidos como Xbee.

**Tabla 1-2** Configuración de Dispositivos Xbee

| Parámetro | Coordinador | Sensor | Actuador |
|---|---|---|---|
| **Channel** | C | C | C |
| **PAN ID** | 3332 | 3332 | 3332 |
| **Destination Address Low** | FFFF | FFFF | 0 |
| **Source Address** | CXXX | BXXX | AXXX |
| **Coordinator Enable** | Coordinator | End Device | End Device |
| **Input Address** | FFFFFFFFFFFFFFFF | FFFFFFFFFFFFFFFF | CXXX |

**Realizado por:** Vilañez, Daniel, 2018

En la tabla se puede observar que algunas direcciones posen una X en su estructura, esto indica que se reemplazará con un número en hexadecimal entre 0 y F, teniendo en cuenta que el nodo actuador habrá de tener en su Input Address la misma dirección que el Source Address del nodo coordinador.

Para realizar las pruebas de alerta del sistema, se define los tipos de alerta y las condiciones de activación. Existen 2 tipos de alerta del sistema, estas son:

- Cuando los sensores con el mismo objetivo se activan a la vez se emite un aviso de alerta.
- Cuando solamente se activa uno de los sensores se emite un aviso de precaución.

A continuación, se detallan las condiciones de activación, las cuales nos indican los valores que nos sirven como disparadores de los sensores:

- Cuando el GLP supere el 20% del límite inferior de explosividad. (Ortrat, 2014 pág. 4)
- Cuando se detecte movimiento al interior del hogar.
- Cuando se detecte movimiento en puertas o ventanas.

### 2.3.1. *Tamaño de la Muestra*

Para el cálculo del tamaño de la muestra se utiliza el método de cálculo de la muestra desconociendo el tamaño de la población, debido a que se desconoce el tamaño de la población debido a que son medidas obtenidas en intervalos de tiempo distintos, dependiendo de la configuración de cada dispositivo. (Pickers, 2015 pág. 1)

La fórmula para calcular el tamaño de muestra cuando se desconoce el tamaño de la población es la siguiente:

$$n = \frac{Z_a^2 * p * q}{d^2}$$

En donde
Z = nivel de confianza, (correspondiente con tabla de valores de Z)
P = probabilidad de éxito, o proporción esperada
Q = probabilidad de fracaso
D = precisión (error máximo admisible en términos de proporción)

Para el cálculo se toma valores de precisión de 5% y un nivel de confianza del 95% equivalente a 1.96, además se pretende tener un nivel alto de mediciones exactas en el sistema por lo cual se utilizará una probabilidad de éxito p=95%.
Reemplazando los valores definidos, el cálculo del tamaño muestral se muestra a continuación:

$$n = \frac{1.96^2 * 95\% * 5\%}{4.6\%^2} = 86.23$$

Por lo tanto, se debe tomar 86 muestras para poder mantener niveles de error dentro de los rangos definidos.

## 2.4. Diseño y Concepción del Sistema

### 2.4.1. *Requerimientos*

Los requerimientos de la red basándonos en el primer capítulo se presentan a continuación:

- Ser de bajo costo, sencillo de instalar e intuitivo para el usuario.
- Supervisar por zonas los parámetros previamente definidos.
- Presentar información referente a los niveles de gases permitidos.
- Supervisar y emitir avisos.
- Los módulos deben tener comunicación en tiempo real.
- Almacenar los datos constantemente en una base de datos.
- Operar independientemente del país en el cual se implemente.

Para la realización de la red IoT los dispositivos tanto eléctricos como electrónicos de los cuáles se deberá disponer son los siguientes:

- Dispositivos WPAN
- Tarjeta de desarrollo
- Sensores
- Actuadores
- Dispositivos Electrónicos
- Implementos de Oficina
- Router

Por otra parte, para la programación y realización de la conexión de la red con el usuario mediante cualquier dispositivo y desde cualquier lugar en el cual exista presencia de una conexión a internet, se requerirá de los siguientes softwares:

- Almacenamiento en la nube
- Software de programación
- IDE de desarrollo

### 2.4.2. *Concepción del sistema*

En la figura 1-2 se puede observar el diseño que se realizara en los prototipos para la realización de las pruebas:

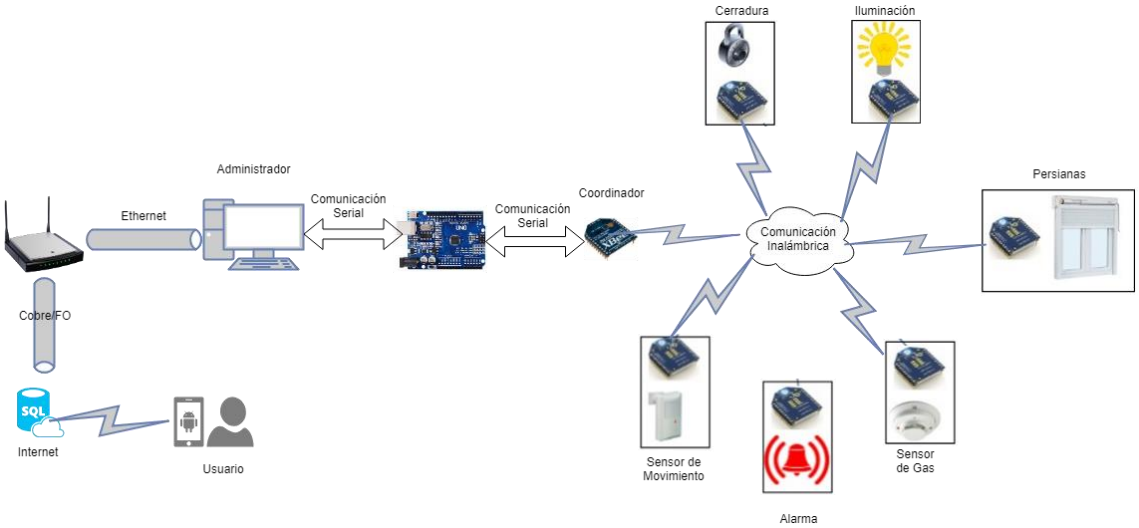


**Figura 1-2** Diseño del prototipo del sistema

**Realizado por:** Daniel Vilañez,2018

## 2.5. Descripción de los Nodos

### 2.5.1. *Nodo Sensor/Actuador*

Se encarga de adquirir y enviar las lecturas de los sensores al nodo coordinador. El número de nodos depende de la cantidad de elementos que se quiera supervisar y controlar. Para la alimentación del nodo se utiliza una fuente que brinde 3.3V y 50mA. El funcionamiento del nodo sensor/actuador se puede observar gráficamente en la figura 2-2.

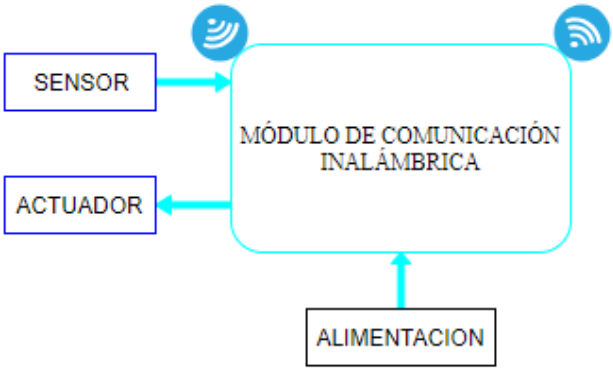


**Figura 2-2** Diagrama de Bloques de Nodo Sensor/Actuador

**Realizado por:** Daniel Vilañez,2018

### 2.5.2. *Nodo Coordinador*

Encargado de receptar las lecturas que proveen cada uno de los sensores de la red, para asignar los procesos que deben cumplir en caso de requerirlo. Además, se irá actualizando la base de datos para que la información de los sensores esté disponible para los usuarios. El funcionamiento del nodo coordinador se puede observar gráficamente en la figura 3-2.

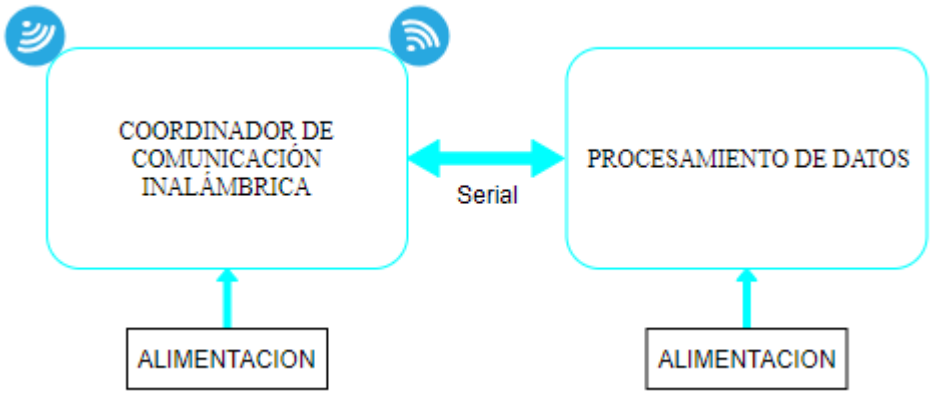


**Figura 3-2** Diagrama de Bloques de Nodo Coordinador

**Realizado por:** Daniel Vilañez, 2018

### 2.5.3. *Nodo de Procesamiento de Datos*

Es una tarjeta de desarrollo encargada de receptar la información del nodo coordinador mediante comunicación serial, la cual se comunica con un ordenador. Además, esta tarjeta se encarga de recibir la información acerca de las acciones que el usuario requiere. El funcionamiento del nodo de procesamiento de datos se puede observar gráficamente en la figura 4-2.

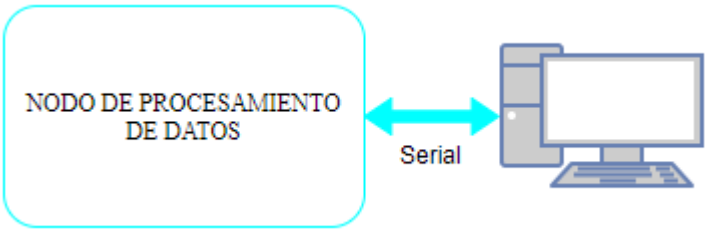


**Figura 4-2** Diagrama de Bloques de Nodo de Procesamiento de Datos

**Realizado por:** Daniel Vilañez, 2018

### 2.5.4. *Nodo de Conexión a Internet*

Es un ordenador con conexión a Internet, mediante una aplicación, el cual está encargado de recibir la información del nodo de procesamiento de datos y almacenar la información en la nube para que el usuario pueda acceder a ella en todo momento siempre y cuando este posea una conexión a internet y recibir las acciones que el usuario requiera, las cuales serán ejecutadas desde una aplicación móvil. El funcionamiento del nodo de conexión a internet se puede observar gráficamente en la figura 5-2.

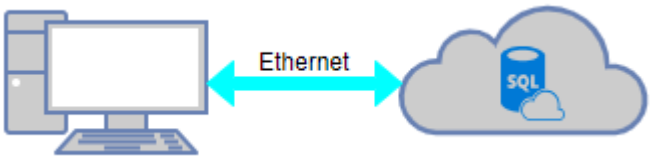


**Figura 5-2** Diagrama de Bloques de Nodo de Conexión a Internet

**Realizado por:** Daniel Vilañez, 2018

## 2.6. Selección de los Protocolos de Comunicación

### 2.6.1. *Protocolo de la Red Actuador – Sensor*

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

### 2.6.2. *Protocolo de la Red de Soporte*

La red de soporte será implementada bajo el protocolo LAN, puesto que actualmente existe un gran número de viviendas con redes locales. De esta manera, se podrá aprovechar este recurso para el control y monitoreo de los dispositivos que conforman el sistema de seguridad. Finalmente, el uso de la LAN permitirá el acceso a la red desde cualquier dispositivo que tenga instalada la aplicación móvil.

### 2.6.3. *Protocolo de Interconexión de Redes*

La interconexión entre el nodo coordinador y el nodo de acceso a Internet 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.

## 2.7. **Selección de los Dispositivos del Sistema de Seguridad**

Para la selección de los dispositivos de seguridad se utilizará el método denominado "Escala de Likert", utilizando indicadores para realizar una puntuación a las cualidades de los mismos.

Para obtener resultados que permiten una selección sustentada la calificación de cada uno de los indicadores se basa en la escala presentada en la tabla 2-2.

**Tabla 2-2** Escala de valoración para el procesamiento de información

| **ESCALAS DE VALORACIÓN CUALITATIVA** | | | |
|---|---|---|---|
| **1** | **2** | **3** | **4** |
| Malo | Regular | Bueno | Muy Bueno |
| Avanzado | Intermedio | Básico | Principiante |
| No | | | Si |

**Fuente:** (QuestionPro, 2015)

**Realizado por:** Vilañez, Daniel, 2018

### 2.7.1. *Módulos Zigbee*

La red actuador - sensor requerirá que los módulos Zigbee sean de alta flexibilidad, bajo consumo y deberán proporcionar una amplia cobertura para la comunicación eficiente dentro del área, 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 de procesamiento de datos, proporcionando la interconexión desde la

red actuador - sensor hacia la LAN de soporte. En la tabla 3-2 se presentan las especificaciones técnicas de algunos módulos Zigbee.

**Tabla 3-2** Comparación de dispositivos Zigbee

| Especificación | Xbee S1 | ZigBit Amp | MRF24J40MB |
|---|---|---|---|
| **Fabricante** | Digi | ATmel | Microchip |
| **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 Rx** | 40mA | 23mA | 25mA |
| **Corriente Tx** | 40mA | 50mA | 130mA |
| **Puerto Serial** | UART | USART, SPI | SPI |
| **DI/O** | 10 | 9 | 6 |
| **Precio (USD)** | 24.15 | 48.36 | 26.58 |

**Fuente:** (Digi, 2018) (ATmel, 2009) (Microchip, 2006)

**Realizado por:** Vilañez, Daniel, 2018

De esta manera, se seleccionarán los módulos Xbee S1, 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 S1 es reducido, otorgando ventajas sobre la disponibilidad de los mismos para el desarrollo de la solución.


**Figura 6-2** Módulo Xbee S1

**Realizado por:** Daniel Vilañez, 2018

### 2.7.2. *Tarjeta de Desarrollo*

La tarjeta de desarrollo es un punto fundamental en la red, esto debido a que será el núcleo en la recepción de información del nodo coordinador mediante comunicación serial, la cual se

comunicará con un ordenador. Además, esta tarjeta se encarga de recibir la información acerca de las acciones que el usuario requiere. En la tabla 4-2 se presentan las especificaciones técnicas de algunas tarjetas de desarrollo, y la calificación de cada una de estas especificaciones se presentan en la tabla 5-2.

**Tabla 4-2** Características Tarjetas de Desarrollo

| **Tarjetas de desarrollo** | | | |
|---|---|---|---|
| **Variable** | **Arduino** | **Beaglebone Black** | **Raspberry Pi** |
| **Alimentación** | 3.3V, 5V, | 5V | 5V |
| **Puertos** | 54 DI/O, 12 AI, 2 AO | 69 GPIO, LCD, GPMC, MMC1, MMC2, 7 AIN, 4 temporizadores, 4 puertos seriales, CAN0 | GPIO de 40 pines |
| **Costo** | Desde $22 hasta $80 | Desde $95 hasta $149 | Desde $60 hasta $150 |
| **Programación** | Basado en C++ | Varios lenguajes | Varios lenguajes |

**Fuente:** (Arduino, 2015) (Coley, y otros, 2013) (Raspberry Pi Foundation, 2017)

**Realizado por:** Vilañez, Daniel, 2018

**Tabla 5-2** Evaluación de Indicadores de la Tarjeta de Desarrollo

| **TARJETAS DE DESARROLLO** | | | |
|---|---|---|---|
| **VARIABLE** | **ARDUINO** | **BEAGLEBONE BLACK** | **RASPBERRY PI** |
| **Alimentación** | | | |
| < 5V | Si | No | No |
| = 5V | Si | Si | Si |
| > 5V | Si | No | No |
| **Puertos** | | | |
| GPIO | Muy Buena | Muy Buena | Muy Buena |
| Serial UART | Muy Buena | Buena | Muy Buena |
| Salida de 3V | Si | Si | Si |
| **Programación** | | | |
| IDE | Si | No | No |
| Dificultad | Intermedio | Avanzado | Avanzado |
| | | | |
| **Costo** | Muy Bueno | Regular | Regular |

**Realizado por:** Vilañez, Daniel, 2018

La calificación definitiva de la solución en base a cada parámetro de comparación, se obtiene sumando los puntajes obtenidos del análisis, utilizando las siguientes fórmulas:

$$Cc_{Arduino} = \left(\frac{P_{Arduino}}{Pt}\right) x\ 100\%$$

$$Cc_{Beaglebone} = \left(\frac{P_{Beaglebone}}{Pt}\right) x\ 100\%$$

$$Cc_{Raspberry} = \left(\frac{P_{Raspberry}}{Pt}\right) x\ 100\%$$

En donde:

$Pt$: Representa la base del puntaje sobre la cual se está calificando

$P_{Arduino}$: Puntaje acumulado por Arduino.

$P_{Beaglebone}$: Puntaje acumulado por la tecnología Beaglebone Black.

$P_{Raspberry}$: Puntaje acumulado por la tecnología Raspberry Pi.

$Cc_{Arduino}$: Porcentaje de la calificación total que obtuvo Arduino.

$Cc_{Beaglebone}$: Porcentaje de la calificación total que obtuvo Beaglebone Black.

$Cc_{Raspberry}$: Porcentaje de la calificación total que obtuvo Raspberry Pi.

Para aplicar las fórmulas primero obtenemos los puntajes de cada una de las tarjetas, para lo cual aplicamos la conversión a valores presentadas en la Tabla 2-2, dando como resultado:

$$P_{Arduino} = 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 2 = 38$$
$$P_{Beaglebone} = 1 + 4 + 1 + 4 + 4 + 4 + 1 + 4 + 1 + 1 = 25$$
$$P_{Raspberry} = 1 + 4 + 1 + 4 + 4 + 4 + 1 + 4 + 1 + 1 = 25$$

La base del puntaje sobre la cual se está calificando es:

$$Pt = 40$$

Con lo cual la calificación de cada una de las tecnologías queda de la siguiente manera:

$$Cc_{Arduino} = \left(\frac{38}{40}\right) x\ 100\% = 95\%$$

$$Cc_{Beaglebone} = \left(\frac{25}{40}\right) x\ 100\% = 62{,}5\%$$

$$Cc_{Raspberry} = \left(\frac{25}{40}\right) x\ 100\% = 62{,}5\%$$

Luego de haber realizado el análisis comparativo de las tarjetas de desarrollo Arduino, Beaglebone Black y Raspberry Pi, el puntaje obtenido para cada uno de los indicadores nos muestra como resultado que la tarjeta Arduino ha obtenido el puntaje más alto con un porcentaje del 95% que equivale a 38 frente al 62,5% alcanzado por las otras tarjetas, que equivale a 25, los índices más importantes son puertos, costo y programación que hacen de Arduino una tarjeta óptima para el prototipo.

#### *2.7.2.1. Tarjetas Arduino*

La red actuador - sensor requerirá que los módulos Zigbee sean de alta flexibilidad, bajo consumo y deberán proporcionar una amplia cobertura para la comunicación eficiente dentro del área, 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 de procesamiento de datos, proporcionando la interconexión desde la red actuador - sensor hacia la LAN de soporte. En la tabla 6-2, se presentan las especificaciones técnicas de algunos módulos Zigbee.

**Tabla 6-2** Comparación Arduino

| Especificación | Mega | Uno | Nano |
|---|---|---|---|
| **Microcontrolador** | ATmega2560 | ATmega328 | ATmega328 |
| **Voltaje de Operación** | 5V | 5V | 5V |
| **Voltaje de Entrada (Recomendado)** | 7-9V | 7-9V | 7-9V |
| **Voltaje de Entrada (Límite)** | 6-20V | 6-20V | 7-12V |
| **Digital I/O Pines** | 54 | 14 | 22 |
| **Pines Entrada Analógicos** | 16 | 6 | 8 |
| **Corriente en Pines I/O** | 40mA | 40mA | 40mA |
| **Corriente en Pin 3.3V** | 50mA | 50mA | 50mA |
| **Memoria Flash** | 256KB | 32KB | 32KB |
| **SRAM** | 8KB | 2KB | 2KB |
| **EEPROM** | 4KB | 1KB | 1KB |
| **Velocidad de Reloj** | 16MHz | 16MHz | 16MHz |
| **Precio (USD)** | 12 | 28 | 7 |

**Fuente:** (Arduino, 2015)

**Realizado por:** Vilañez, Daniel, 2018

De esta manera, se seleccionará el Arduino UNO, figura 7-2, es así que poseen catorce pines digitales y un puerto UART para la comunicación con otros dispositivos seriales. Asimismo, el costo del Arduino UNO es reducido, otorgando ventajas sobre la disponibilidad de los mismos para el desarrollo de la solución.

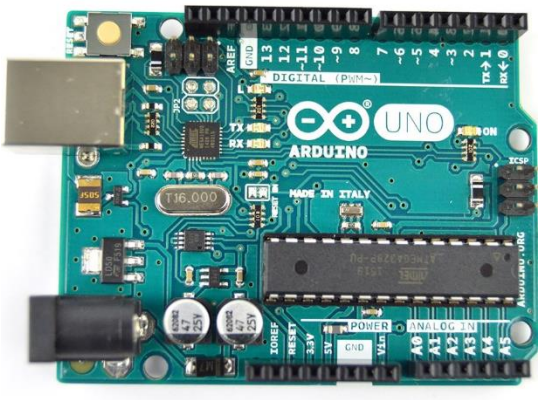


**Figura 7-2** Arduino UNO

**Realizado por:** Daniel Vilañez, 2018

### 2.7.3. ***Sensores***

#### *2.7.3.1. Sensor de Humo*

Para el monitoreo de humo y gases peligrosos presentes en los hogares se utilizará los sensores MQ4, figura 8-2, los cuales son adecuados para detectar GLP, propano, metano, alcohol, hidrógeno, humo.


**Figura 8-2** Sensor de Humo/Gases MQ4

**Realizado por:** Daniel Vilañez, 2018

#### *2.7.3.2. Sensor de Movimiento*

Para el monitoreo de las posibles intrusiones que existan en el hogar se utilizará un sensor infrarrojo pasivo, figura 9-2, que utiliza una medición de radiación infrarroja para la detección de

movimiento. Son baratos, pequeños, de baja potencia, y fáciles de usar. Por esta razón son frecuentemente usados en juguetes, aplicaciones domóticas o sistemas de seguridad.

**Figura 9-2** Sensor de Movimiento PIR

**Realizado por:** Daniel Vilañez, 2018

*2.7.3.3. Sensor de Vibración*

Para la detección de intrusión conjuntamente con el sensor de movimiento, y así evitar posibles falsas alarmas, se utilizará un módulo sensor de vibración 801S, figura 10-2, que se puede utilizar en dispositivos antirrobo, cerraduras electrónicas, detección de vibración de equipos mecánicos, contando el alcance de tiro de tiro en blanco de las pruebas de vibración.

**Figura 10-2** Sensor de Vibración Módulo 801S

**Realizado por:** Daniel Vilañez, 2018

### 2.7.4. *Actuadores*

Para la realización de los actuadores es necesario buscar un medio para lograr controlar circuitos de potencia (corriente alterna) con circuitos de corriente continua, ya que la red compuesta por Xbee solo es suministrada con corriente continua de bajo voltaje.

Para realizar esto se ha optado por utilizar un opto acoplador TRIAC MOC 3021, es un dispositivo de emisión y recepción que funciona como un interruptor activado mediante la luz emitida por un diodo LED que satura un componente opto electrónico, normalmente en forma de fototransistor o fototriac. Estos elementos se encuentran dentro de un encapsulado que por lo general es del tipo DIP. Se suelen utilizar para aislar eléctricamente a dispositivos muy sensibles. En la figura 11-2 se puede observar el circuito que será utilizado para implementar los actuadores. (Texas Instruments, 1995)

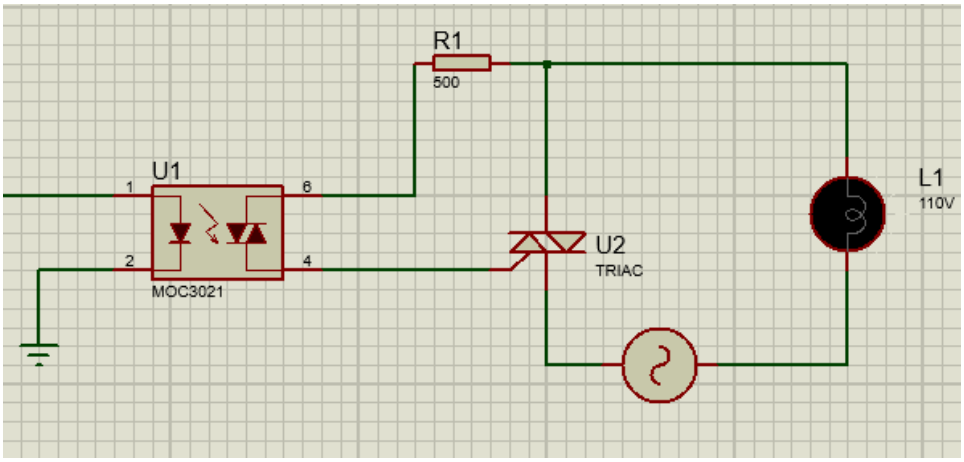


**Figura 11-2** Circuito Actuador

**Realizado por:** Daniel Vilañez, 2018

### 2.7.5. *Otros Dispositivos*

Debido a que los pines del Xbee son mucho más pequeños de lo que comúnmente suelen ser, no es posible manipularlo para configurarlo o colocarlo en una protoboard, por eso para ocuparlo se utilizara un adaptador para colocarlo en la protoboard, el cual se muestra en la figura 12-2, y para configurarlo se hace uso de un Xbee explorer USB mostrado en la figura 13-2, que se encarga de comunicarse directamente con los pines seriales del Xbee.

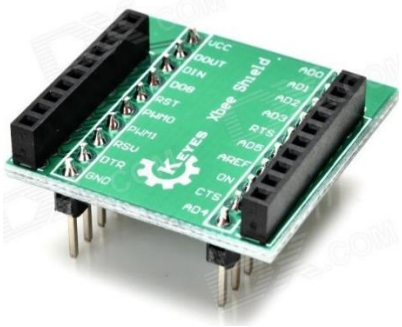


**Figura 12-2** Adaptador de Protoboard para Xbee

**Realizado por:** Daniel Vilañez, 2018

**Figura 13-2** Xbee Explorer USB

**Realizado por:** Daniel Vilañez, 2018

## 2.8. Selección del Software para realizar el Sistema de Seguridad

La selección del software de desarrollo de las aplicaciones se realizará de forma similar a la de los dispositivos de seguridad utilizando el método denominado "Escala de Likert", utilizando indicadores para realizar una puntuación a las cualidades de los mismos.

Para obtener resultados que permiten una selección sustentada la calificación de cada uno de los indicadores se presenta la escala basada en la tabla 7-2.

**Tabla 7-2** Escala de valoración para el procesamiento de información

| ESCALAS DE VALORACIÓN CUALITATIVA | | | |
|---|---|---|---|
| **1** | **2** | **3** | **4** |
| Muy Bajo | Bajo | Medio | Alto |
| Deficiente | Poco eficiente | Eficiente | Muy Eficiente |
| Malo | Regular | Bueno | Muy Bueno |
| Avanzado | Intermedio | Básico | Principiante |
| No | | | Si |

**Fuente:** (QuestionPro, 2015)

**Realizado por:** Vilañez, Daniel, 2018

### 2.8.1. *Servicio de Almacenamiento en la Nube*

El servicio de almacenamiento en la nube es un punto importante, debido a que de esto dependerá que la red sea considerada como una red IoT. Para esta selección se han tomado tres de los servicios más utilizados en la actualidad, estos son Amazon Web Service, Windows Azure y Google Cloud Plataform. Los indicadores que se utilizarán para la selección del servicio de almacenamiento se listan a continuación:

- Bases de Datos
- Seguridad
- IoT
- Almacenamiento
- Lenguajes de Programación Soportados
- Escalabilidad y disponibilidad
- Número de Servicios
- Infraestructura
- Almacenamiento de Aplicaciones
- Precios

En la tabla 8-2 se presentan las características referentes a los indicadores de los principales servicios de almacenamiento en la nube, y la calificación de cada una de estas especificaciones se presentan en la tabla 9-2.

**Tabla 8-2** Características de Servicios de Almacenamiento en la Nube

| Variable | AWS | Azure | GCP |
|---|---|---|---|
| **Bases de Datos** | Bases de datos relacionales, no sql, de documentos y clave-valor, almacenamiento en caché, migración, warehouse, basada en grafos. | Bases de datos relacionales, no sql, de documentos y clave-valor, almacenamiento en caché, migración, warehouse, basada en grafos. | Bases de datos relacionales, no sql, de documentos y clave-valor, almacenamiento en caché, warehouse. |
| **Seguridad** | Autenticación y autorización, cifrado, firewall, evaluación de seguridad, administración de certificados e identidades, servicios de directorio, protección DDOS, detección | Autenticación y autorización, protección de la información, cifrado, firewall, evaluación de seguridad, administración de certificados e identidades, servicios de directorio, protección DDOS, detección | Autenticación y autorización, cifrado, protección DDOS, detección de amenazas y actividades anómalas. |

| | | | |
|---|---|---|---|
| | de amenazas y actividades anómalas. | de amenazas y actividades anómalas. | |
| **IoT** | Conexión y supervisión, edge computing, administración remota, detección de eventos y respuesta, Marketplace para consumir productos/servicios de terceros. | Conexión y supervisión, edge computing, administración remota, detección de eventos y respuesta, Marketplace para consumir productos/servicios de terceros. | Conexión y supervisión, Marketplace para consumir productos/servicios de terceros. |
| **Tipos de Almacenamiento** | Objetos, para archivado, disco para instancias, transferencia de datos a la nube, backup, híbrido. | Objetos, para archivado, disco para instancias, transferencia de datos a la nube, backup, híbrido, recuperación de desastres. | Objetos, para archivado, disco para instancias, transferencia de datos a la nube, backup. |
| **Lenguajes Soportados** | Tiene soporte de aplicaciones con .NET Framework en lenguajes como C# y Visual Basic o sin .NET en C++, Java y otros lenguajes. | Tiene soporte de aplicaciones con .NET Framework en lenguajes como C# y Visual Basic o sin .NET en C++, Java y otros lenguajes. | Tiene soporte, con algunas limitaciones, de aplicaciones con .NET Framework en lenguajes como C# y Visual Basic o sin .NET en C++, Java y otros lenguajes. |
| **Infraestructura** | 11 centros de datos, 37 puntos de distribución contenidos | 20 centros de datos, 32 puntos de distribución contenidos | 4 centros de datos, 160 puntos de distribución contenidos |
| **Almacenamiento de Aplicaciones** | Elastic Beanstalk | App Service, Service Fabric, Cloud Services | App Engine |
| **Precio** | Pago por hora o fracción, distinto tamaño de servidor, descuentos en contratación de 1 a 3 años | Pago por distintas fracciones de tiempo, distinto tamaño de servidor | Pago por minuto, descuentos por horas de consumo, distintos tamaños de servidor. |

**Fuente:** (Microsoft, 2018) (Amazon, 2018) (Google, 2018)

**Realizado por:** Vilañez, Daniel, 2019

**Tabla 9-2** Evaluación de Indicadores de Servicio de Almacenamiento en la Nube

| **ALMACENAMIENTO EN LA NUBE** | | | |
|---|---|---|---|
| **VARIABLE** | **AWS** | **AZURE** | **GCP** |
| **Bases de Datos** | | | |
| SQL | Si | Si | Si |
| No SQL | Si | Si | Si |
| Bases en Memoria | Si | Si | No |
| **Seguridad** | | | |
| Respaldos | Muy Buena | Muy Buena | Regular |
| Recuperación de | Muy Buena | Muy Buena | Regular |

| | | | |
|---|---|---|---|
| desastres | | | |
| Autenticación y gestión de acceso. | Muy Buena | Muy Buena | Muy Buena |
| **IoT** | | | |
| Monitoreo | Muy Eficiente | Muy Eficiente | Eficiente |
| Administración | Eficiente | Muy Eficiente | Eficiente |
| | | | |
| **Tipos de Almacenamiento** | Muy Buena | Muy Buena | Regular |
| **Lenguajes de Programación Soportados** | Alto | Alto | Medio |
| **Escalabilidad y disponibilidad** | Medio | Alto | Medio |
| **Número de Servicios** | Alto | Alto | Alto |
| **Infraestructura** | Alto | Medio | Medio |
| **Almacenamiento de Aplicaciones** | Si | Si | Si |
| **Precios** | Bueno | Bueno | Bueno |

**Realizado por:** Vilañez, Daniel, 2019

La calificación definitiva de la solución en base a cada parámetro de comparación, se obtiene sumando los puntajes obtenidos del análisis, utilizando las siguientes fórmulas:

$$Cc_{AWS} = \left(\frac{P_{AWS}}{Pt}\right) x\ 100\%$$

$$Cc_{Azure} = \left(\frac{P_{Azure}}{Pt}\right) x\ 100\%$$

$$Cc_{GCP} = \left(\frac{P_{GCP}}{Pt}\right) x\ 100\%$$

En donde:

$Pt$: Representa la base del puntaje sobre la cual se está calificando

$P_{AWS}$: Puntaje acumulado por AWS.

$P_{Azure}$: Puntaje acumulado por Azure.

$P_{GCP}$: Puntaje acumulado por GCP.

$Cc_{AWS}$: Porcentaje de la calificación total que obtuvo AWS.

$Cc_{Azure}$: Porcentaje de la calificación total que obtuvo Azure.
$Cc_{GCP}$: Porcentaje de la calificación total que obtuvo GCP.

Para aplicar las fórmulas primero obtenemos los puntajes de cada uno de los servicios, para lo cual aplicamos la conversión a valores presentadas en la Tabla 7-2, dando como resultado:

$$P_{AWS} = 4+4+4+4+1+4+4+3+4+4+4+4+3+4+4+4+3 = 62$$
$$P_{Azure} = 4+4+4+4+4+4+4+4+4+4+4+4+4+4+4+3+4+3 = 66$$
$$P_{GCP} = 4+4+1+1+1+4+3+3+4+1+1+3+3+4+3+4+3 = 47$$

La base del puntaje sobre la cual se está calificando es:

$$Pt = 68$$

Con lo cual la calificación de cada una de las tecnologías queda de la siguiente manera:

$$Cc_{AWS} = \left(\frac{62}{68}\right) x\ 100\% = 91{,}18\%$$

$$Cc_{Azure} = \left(\frac{66}{68}\right) x\ 100\% = 97{,}06\%$$

$$Cc_{GCP} = \left(\frac{47}{68}\right) x\ 100\% = 69{,}12\%$$

Luego de haber realizado el análisis comparativo de los servicios de almacenamiento: Amazon Web Service, Microsoft Azure y Google Cloud Platform, el puntaje obtenido para cada uno de los indicadores nos muestra como resultado que Microsoft Azure ha obtenido el puntaje más alto con un porcentaje del 97,06% que equivale a 66 frente al 91,18% y 69,12% que equivalen a 62 y 47 alcanzado por Amazon y Google, respectivamente, el índice más importante es el de IoT que hacen de Azure un servicio óptimo para el prototipo.

### 2.8.2. *Software de Desarrollo de Aplicaciones*

El desarrollo de las aplicaciones, tanto la móvil como la de escritorio, son un punto sustancial para el monitoreo y administración de la red. Para esta selección se han tomado los softwares: Visual Studio, Netbeans IDE y Eclipse.

Los indicadores que se utilizarán para la selección del software de desarrollo de aplicaciones se listan a continuación:

- Desarrollo de Aplicación Móvil
- Desarrollo de Aplicación de Escritorio
- Enlace a Base de Datos SQL
- Soporte de Windows Azure
- Lenguajes de Programación Soportados
- Guías de Usuario

Estos indicadores son clasificados según el nivel de conocimiento requerido para su programación, así como el nivel de complementos necesario para el desarrollo.

En la tabla 10-2 se presenta la calificación de cada una de los indicadores.

**Tabla 10-2** Evaluación de Indicadores del Software de Desarrollo

| **SOFTWARE DE DESARROLLO** | | | |
|---|---|---|---|
| **VARIABLE** | **Visual Studio** | **Netbeans IDE** | **Eclipse** |
| **Aplicación Móvil** | | | |
| Android | Intermedio | Avanzado | Avanzado |
| IOS | Intermedio | Avanzado | Avanzado |
| Windows Phone | Intermedio | Avanzado | Avanzado |
| | | | |
| **Aplicación de Escritorio** | Básico | Básico | Intermedio |
| **Base de Datos SQL** | Básico | Básico | Intermedio |
| **Windows Azure** | Fácil | Intermedio | Intermedio |
| **Lenguajes de Programación** | Alto | Medio | Medio |
| **Guías de Usuario** | Si | Si | Si |

**Realizado por:** Vilañez, Daniel, 2019

La calificación definitiva de la solución en base a cada parámetro de comparación, se obtiene sumando los puntajes obtenidos del análisis, utilizando las siguientes fórmulas:

$$Cc_{VS} = \left(\frac{P_{VS}}{Pt}\right) x\ 100\%$$

$$Cc_N = \left(\frac{P_N}{Pt}\right) x\ 100\%$$

$$Cc_E = \left(\frac{P_E}{Pt}\right) x\ 100\%$$

En donde:

$Pt$: Representa la base del puntaje sobre la cual se está calificando
$P_{VS}$: Puntaje acumulado por Visual Studio.
$P_N$: Puntaje acumulado por Netbeans IDE.
$P_E$: Puntaje acumulado por Eclipse.
$Cc_{VS}$: Porcentaje de la calificación total que obtuvo Visual Studio.
$Cc_N$: Porcentaje de la calificación total que obtuvo Netbeans IDE.
$Cc_E$: Porcentaje de la calificación total que obtuvo Eclipse.

Para aplicar las fórmulas primero obtenemos los puntajes de cada una de las tecnologías para lo cual aplicamos la conversión a valores presentadas en la Tabla 7-2, dando como resultado:

$$P_{VS} = 2 + 2 + 2 + 3 + 3 + 4 + 4 + 4 = 24$$
$$P_N = 1 + 1 + 1 + 3 + 3 + 2 + 3 + 4 = 18$$
$$P_E = 1 + 1 + 1 + 2 + 2 + 2 + 3 + 4 = 16$$

La base del puntaje sobre la cual se está calificando es:

$$Pt = 32$$

Con lo cual la calificación de cada una de las tecnologías queda de la siguiente manera:

$$Cc_{VS} = \left(\frac{24}{32}\right) x\ 100\% = 75\%$$

$$Cc_N = \left(\frac{18}{32}\right) x\ 100\% = 56{,}25\%$$

$$Cc_E = \left(\frac{16}{32}\right) x\ 100\% = 50\%$$

Luego de haber realizado el análisis comparativo de los Software de Desarrollo: Visual Studio, Netbeans IDE y Eclipse, el puntaje obtenido para cada uno de los indicadores nos muestra como resultado que Visual Studio ha obtenido el puntaje más alto con un porcentaje del 75% que equivale a 24 frente al 56,25% y 50% que equivalen a 18 y 16 alcanzado por Netbeans IDE y Eclipse, respectivamente, el índice más importante es el de Soporte de Windows Azure.

### 2.8.3. *XCTU*

XCTU es una aplicación gratuita multiplataforma diseñada para permitir a los desarrolladores interactuar con los módulos Digi RF a través de una interfaz gráfica fácil de usar. Incluye nuevas herramientas que facilitan el montaje, configuración y prueba de los módulos de RF XBee. Las características únicas como la vista de red gráfica, que representa gráficamente la red XBee junto con la potencia de la señal de cada conexión, y el generador de marcos de API XBee, que intuitivamente ayuda a crear e interpretar marcos API para XBees que se utilizan en el modo API, se combinan para hacer el desarrollo de XBee más fácil que nunca. (Digi International Inc., 2017)

### 2.8.4. *Arduino IDE*

Arduino IDE es un entorno de desarrollo que tiene como base el entorno de Processing. Por su parte, también tiene como base un lenguaje de programación fundamentado en Wiring. Además, tiene instalado como base el cargador de arranque (bootloader), el cual se ejecuta en el microcontrolador. (Arduino, 2015)

## 2.9. Esquema de conexión de la Red

Una vez realizada la selección de los dispositivos electrónicos que integran los diferentes nodos y el software para el desarrollo de la configuración, las conexiones de cada no se realizaron en Proteus 8 Profesional. En Isis se realizó las conexiones de cada nodo de la red, se instaló librerías para la compatibilidad con Arduino Uno, sensores, entre otros permitiendo realizar modificaciones rápidas para la implementación.

### 2.9.1. *Esquema de conexión de Nodo Sensor*

El esquema de conexión del nodo sensor se aprecia en la figura 14-2, tiene como elemento central un Xbee S1 que se comunica con cada uno de los sensores:

- Se ubica el Xbee sobre el adaptador para ubicarlo sobre la protoboard.

- Debido a que la distancia entre sensores es amplia cada uno de los sensores se conectara a un Xbee independiente, las señales de los sensores se ubican en los puertos DI/O del Xbee S1.
- Se establece la comunicación inalámbrica entre el sensor y el coordinador para enviar las lecturas por RF.

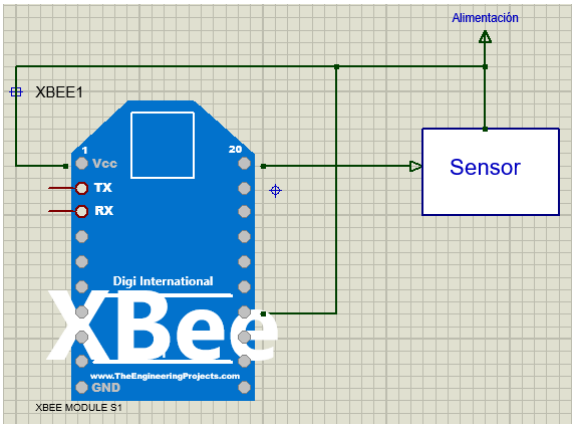


**Figura 14-2** Conexión del nodo sensor

**Realizado por:** Daniel Vilañez, 2018

### 2.9.2. *Esquema de conexión de Nodo Actuador*

El esquema de conexión del nodo actuador se aprecia en la figura 15-2, tiene como elemento central un Xbee S1 que se comunica con el circuito actuador:

- Se ubica el Xbee sobre el adaptador para ubicarlo sobre la protoboard.
- La conexión de los puertos DI/O del Xbee hacia los actuadores debe ser específica y se debe realizar dependiendo a la configuración realizada en el Nodo de Supervisión y Control.
- Se establece la comunicación inalámbrica entre el sensor y el coordinador para leer las acciones enviadas por RF.

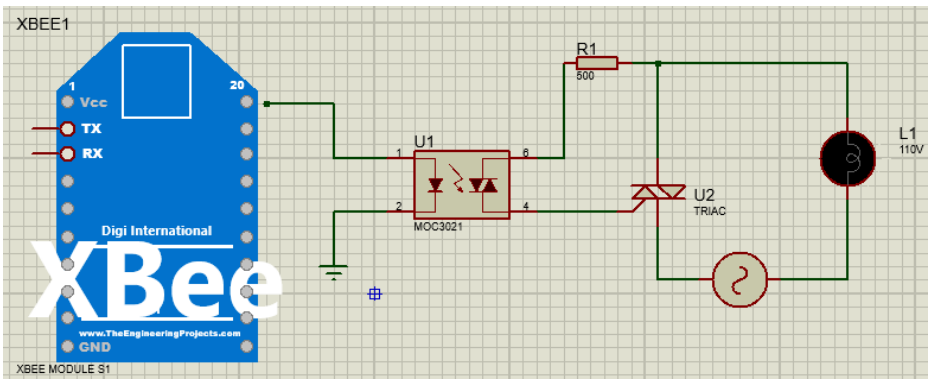


**Figura 15-2** Conexión del nodo actuador

**Realizado por:** Daniel Vilañez, 2018

### 2.9.3. *Esquema de conexión de Nodo de Supervisión y Control*

Tiene como elemento central el Arduino UNO, como se puede apreciar en la figura 16-2, conectado a el nodo Coordinador para la recepción y emisión de información.

- Al Coordinador llegan la información por RF, esta información se envía al Arduino UNO mediante comunicación serial conectando los puertos 2 y 3 del Xbee, que representan los puertos de comunicación serial, con los puertos de transmisión y recepción del Arduino ubicados en los puertos A0 y A1.
- El Arduino UNO procesa la información recibida, realiza la calibración respectiva y permite visualizar los valores obtenidos tanto en el computador como en la aplicación móvil.
- El procesador comprueba si el usuario requiere de alguna acción, si el usuario así lo requiere realizará las siguientes acciones:
  - Si el usuario requiere de abrir la cerradura se coloca en alto el terminal D2 el cual se conecta al DI/O 0 del coordinador y se envía la señal al actuador correspondiente.
  - Si el usuario requiere de activar la luminaria se coloca en alto el terminal D3 el cual se conecta al DI/O 1 del coordinador y se envía la señal al actuador correspondiente.
  - Si el usuario requiere de activar el rociador se coloca en alto el terminal D4 el cual se conecta al DI/O 2 del coordinador y se envía la señal al actuador correspondiente.
  - Si el usuario requiere de activar las persianas se coloca en alto el terminal D5 el cual se conecta al DI/O 3 del coordinador y se envía la señal al actuador correspondiente.
  - Si el usuario requiere de activar la alarma se coloca en alto el terminal D6 el cual se conecta al DI/O 4 del coordinador y se envía la señal al actuador correspondiente.

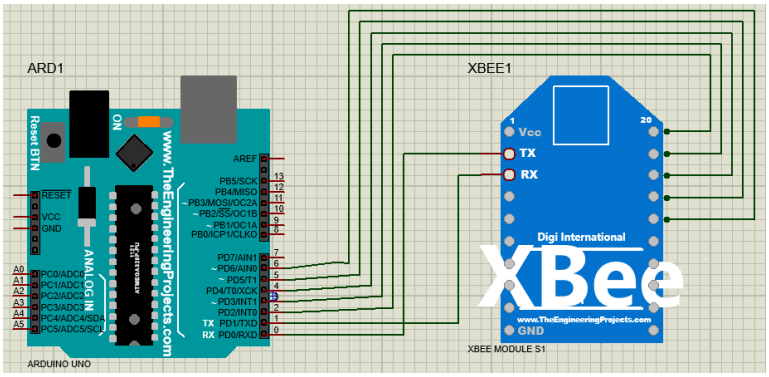


**Figura 16-2** Conexión del Módulo Supervisión-Control

**Realizado por:** Daniel Vilañez, 2018

## 2.10. Diseño del Software la Red

El diseño del Software se realiza en IDE de Arduino, Visual Studio y Microsoft Azure, se empieza puntualizando los requerimientos que se debe realizar, se despliega los diagramas de flujo, las funciones y librerías utilizadas que en complemento con el hardware cumplirán los requerimientos globales del prototipo.

### 2.10.1. *Requerimientos del Software de la Red*

- Obtener los datos de los sensores de movimiento, vibración, humo y temperatura.
- Determinar los valores máximos y mínimos de temperatura y humo medidos por el sistema.
- Transmisión de datos en tiempo real entre el procesador y la aplicación de escritorio.
- Interfaz amigable e intuitiva para el usuario que muestre los datos recibidos.
- Las alertas deben ser emitidas en tiempo real con rapidez y efectividad.
- Permitir un control para el encendido y apagado de los actuadores.

### 2.10.2. *Diagrama de Flujo del Programa del Nodo de Supervisión y Control*

Para el desarrollo del programa del Nodo de Supervision y Control se utiliza el IDE de Arduino, en la figura 17-2 se muestra el diagrama de flujo del programa detallando su proceso.

Para la inicialización:

- Se realiza la inclusión de librería puerto serie virtual para inicializar la comunicación con el dispositivo Xbee.
- Declaración e inicialización de las variables globales que se utilizará.
- Se inicializa la comunicación serial.

Para el ciclo de repetición:

- Se verifica si existe información disponible en la comunicación con el Coordinador, mediante el uso del comando Serial.available ().
- Se busca el inicio de la trama Xbee, la cual se conoce como el numero en hexadecimal 0x7E.
- Si la trama es detectada se descartan los bytes hasta la lectura de la dirección de los Nodos sensores.

- Una vez detectada la dirección de origen se pregunta si proviene de un nodo analógico o digital.
- Si la información proviene de un nodo analógico toma 2 bytes de información, con el método de descarte.
- Si la información proviene de un nodo digital toma 1 bytes de información, con el método de descarte.
- Luego se establece la conexión vía serial al computador.
- Si se envía información el bucle regresa a su estado inicial.
- Si se recibe información establece conexión con el Coordinador mediante la salida correspondiente a la acción requerida.

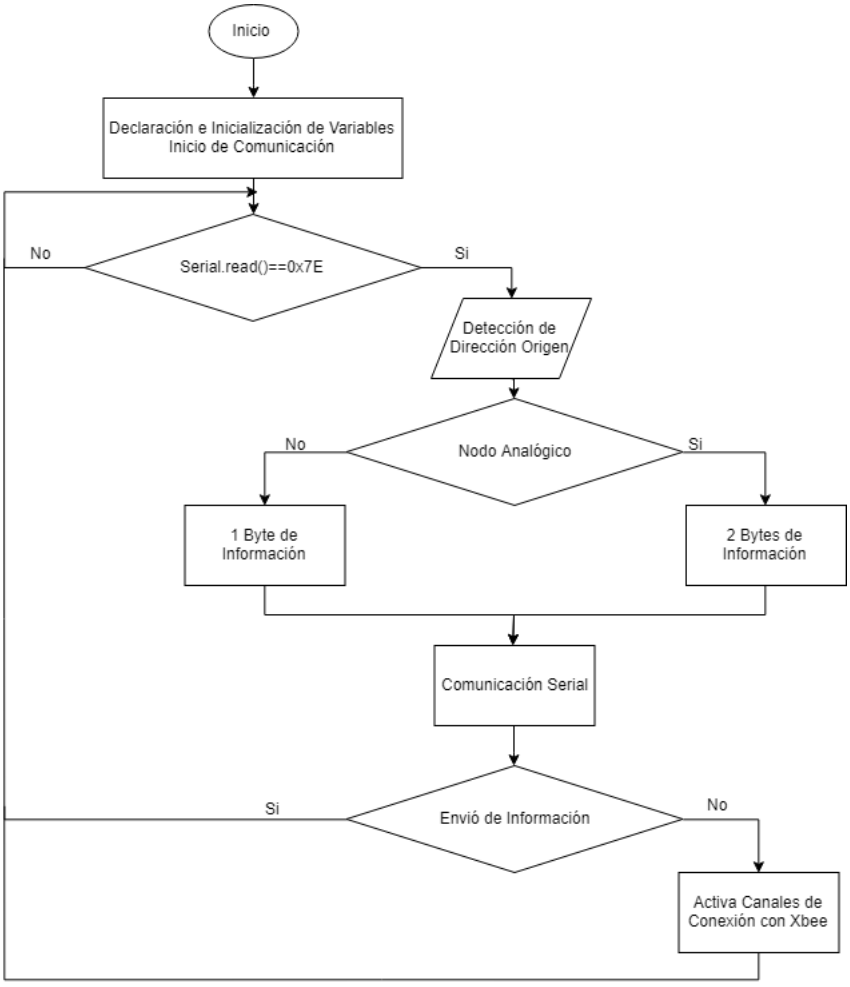


**Figura 17-2** Diagrama de Flujo del Programa del Nodo de Supervisión y Control

**Realizado por:** Daniel Vilañez, 2018

### 2.10.3. *Diagrama de Flujo de Aplicación de Escritorio*

Para el desarrollo de la aplicación de escritorio se utiliza Visual Studio, en la figura 18-2 se muestra el diagrama de flujo del programa detallando su proceso.

- Se realiza la inclusión de librería Data y Data.SqlClient.
- Declaración e inicialización de las variables globales que se utilizará.
- Se inicializa la comunicación tanto la comunicación serial como con la base de datos.
- Se verifica si existe información disponible en las comunicaciones.
- Si la información leída es procedente de la comunicación serial se toma los datos y se realiza el procedimiento para su respectivo almacenamiento en la base de datos.
- Si los datos son procedentes de la base de datos se los procesa y se los envía al Arduino para que realice las acciones correspondientes, si es necesario que se envíe una notificación a la aplicación móvil se lo realizará.
- Si la comunicación no procede de las fuentes antes descritas se volverá a realizar la lectura.
- Si el usuario requiere de realizar en alguna habitación, primero debe seleccionar la habitación.
- Una vez seleccionada la habitación se visualizarán los datos y podrá seleccionar una acción a realizar, la cuál será almacenada en la base de datos.

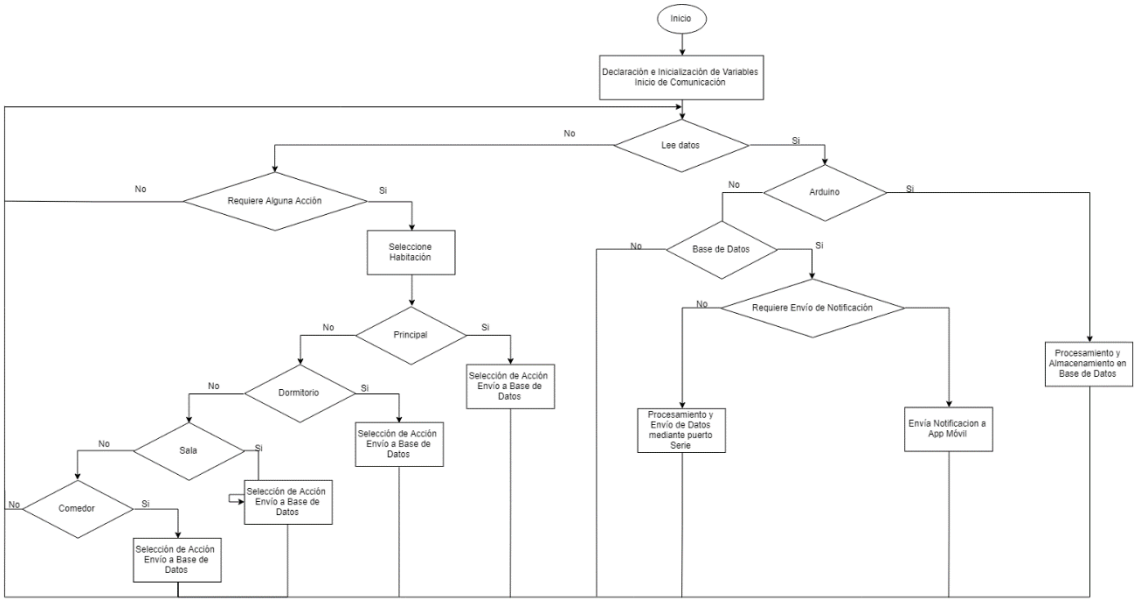


**Figura 18-2** Diagrama de Flujo de Aplicación de Escritorio

**Realizado por:** Daniel Vilañez, 2018

### 2.10.4. *Diagrama de Flujo de Aplicación Móvil*

Para el desarrollo de la aplicación móvil se utiliza Visual Studio, en la figura 19-2 se muestra el diagrama de flujo del programa detallando su proceso.

- Se realiza la inclusión de librería Data y Data.SqlClient.
- Declaración e inicialización de las variables globales que se utilizará.
- Se inicializa la comunicación con la base de datos.
- Se pide al usuario confirmación de ingreso a la aplicación.
- Si el usuario ingresa a la aplicación se le pedirá que seleccione una habitación para realizar las acciones o visualizar los datos.
- Una vez seleccionada la habitación se visualizarán los datos y podrá seleccionar una acción a realizar, la cuál será almacenada en la base de datos.

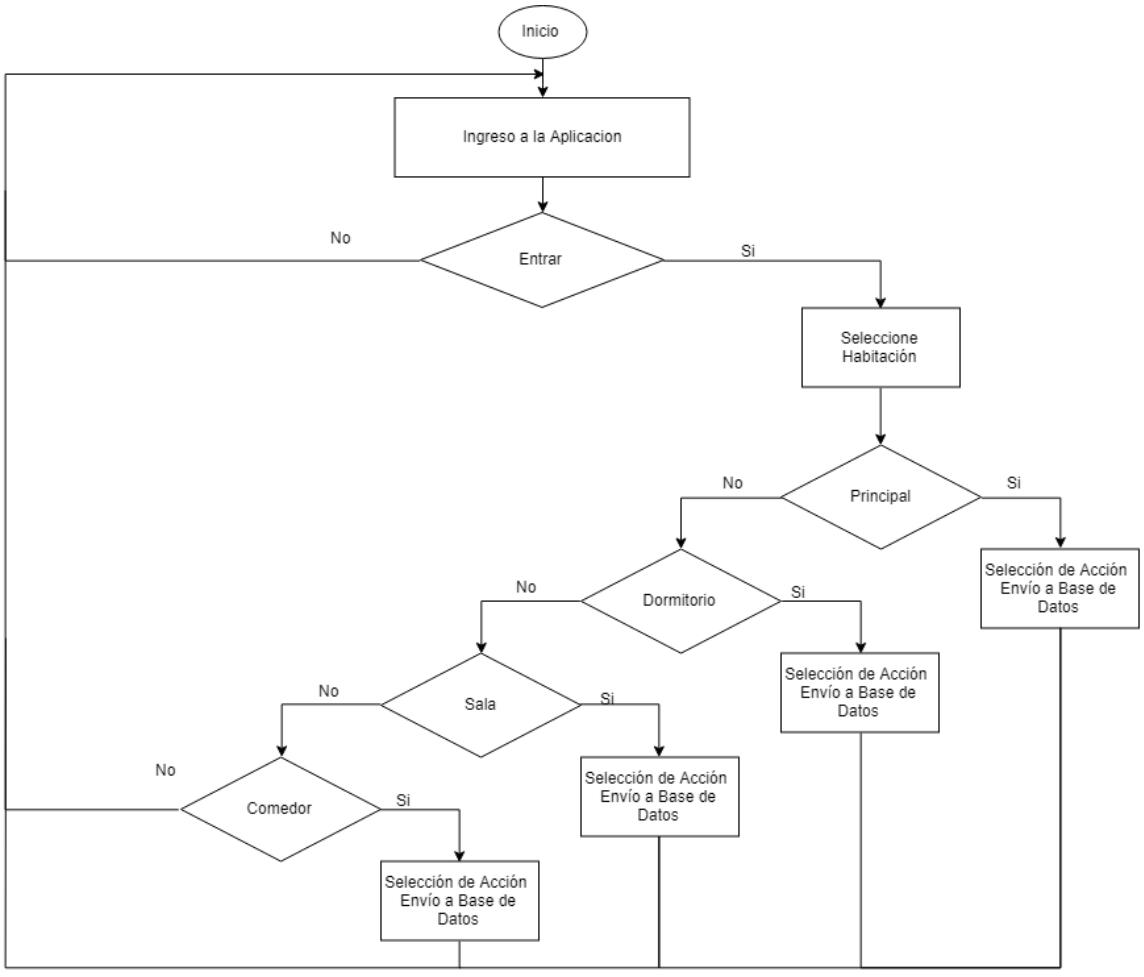


**Figura 19-2** Diagrama de Flujo de Aplicación Móvil

**Realizado por:** Daniel Vilañez, 2018

# 3. CAPITULO III: MARCO DE PRUEBAS Y RESULTADOS

En el presente capítulo se detalla las pruebas realizadas para la implementación de los nodos del sistema las cuales fueron: prueba en el nodo sensor, prueba en el nodo actuador, prueba en el nodo coordinador, prueba de alerta del sistema y evaluación del sistema para determinar la estabilidad.

## 3.1. Pruebas de Funcionamiento

Esta fase se centra en presentar el funcionamiento de los diferentes nodos bajo distintas circunstancias, para lo cual se activa intencionalmente los sensores, se estudia si los actuadores funcionan adecuadamente y se verifica si las notificaciones llegan apropiadamente a los usuarios.

### 3.1.1. *Pruebas en Nodo Sensor*

La red cuenta con 3 sensores de los cuales 2 sirven para la detección de intrusiones y el restante se ocupa para la detección de gases. Los dos primeros son: sensor de movimiento mediante detección infrarroja colocado en lugares cerca de puertas y ventanas, y sensor de vibración que se coloca en puertas y ventanas, estos dos sensores conjuntamente brindaran la detección de intrusiones no deseadas. El siguientes es un sensor gas que emitirá una alerta cuando los valores de gas superen cierto rango.

Para el correcto funcionamiento de estos sensores se realizó las pruebas de calibración, las mismas que son detalladas a continuación.

#### *3.1.1.1. Precisión de Sensores*

Debido a que la información se envía en bruto se requiere realizar pruebas de precisión y calibración, para esto se sometió a los sensores a distintos escenarios controlados y se obtuvo una forma de procesar la información para que fuese lo más exacta posible.

Las pruebas con el sensor de gases se realizaron con mediciones de activación de las alarmas, debido a que no se cuenta con los equipos necesarios para obtener datos exactos de estas mediciones.

Para calcular la imprecisión de los sensores se utilizó las fórmulas de error absoluto, las cuales se presentan en las ecuaciones siguientes:

- Media:

$$X = \sum_{i=1}^{n} \frac{X_i * f_i}{n}$$

Donde X: media de las medidas, Xi: mediciones realizadas, fi: frecuencia de las mediciones, n: total de la muestra.

- Error Absoluto:

$$E_a = \frac{\sum_{i=1}^{n} |X - X_i|}{n}$$

*Sensor de Movimiento*

Las pruebas en el sensor de movimiento se basaron en la modificación de los valores de sensibilidad del sensor, los cuales se modifican mediante un potenciómetro presente en la placa del sensor.

Estas pruebas fueron realizadas mediante el software Arduino, figura 1-3, y con los valores mínimo, medio y máximo del potenciómetro con lo cual se obtuvo, los siguientes resultados.

En la tabla 1-3, se puede observar que la distancia de detección que tiene el sensor de movimiento cuando su potenciómetro está en el valor mínimo.

**Tabla 1-3** Prueba Sensor de Movimiento-Valor mínimo

| Distancia (m) | Muestras | Detección | Porcentaje de Detección(%) |
|---|---|---|---|
| **1** | 87 | 87 | 100 |
| **3** | 87 | 80 | 91.95 |
| **5** | 87 | 30 | 34.48 |
| **7** | 87 | 10 | 11.49 |
| **9** | 87 | 0 | 0 |

**Realizado por:** Vilañez, Daniel, 2019

En la tabla 2-3, se puede observar que la distancia de detección que tiene el sensor de movimiento cuando su potenciómetro está a la mitad del valor.

**Tabla 2-3** Prueba Sensor de Movimiento-Valor medio

| Distancia (m) | Muestras | Detección | Porcentaje de Detección(%) |
|---|---|---|---|
| **1** | 87 | 87 | 100 |
| **3** | 87 | 85 | 97.70 |
| **5** | 87 | 65 | 74.71 |
| **7** | 87 | 44 | 50.57 |
| **9** | 87 | 0 | 0 |

**Realizado por:** Vilañez, Daniel, 2019

En la tabla 3-3, se puede observar que la distancia de detección que tiene el sensor de movimiento cuando su potenciómetro está en el valor máximo.

**Tabla 3-3** Prueba Sensor de Movimiento-Valor máximo

| Distancia (m) | Muestras | Detección | Porcentaje de Detección(%) |
|---|---|---|---|
| **1** | 87 | 87 | 100 |
| **3** | 87 | 87 | 100 |
| **5** | 87 | 83 | 95.4 |
| **7** | 87 | 75 | 86.21 |
| **9** | 87 | 65 | 74.71 |

**Realizado por:** Vilañez, Daniel, 2019

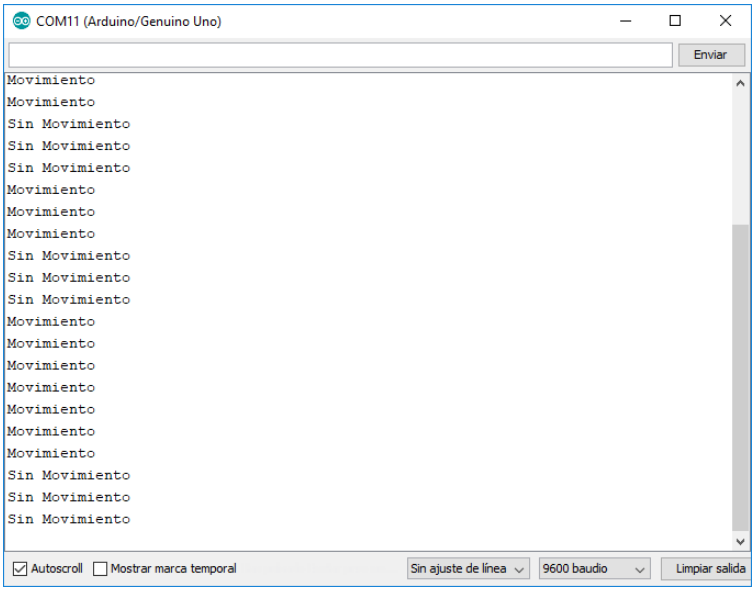


**Figura 1-3** Mediciones de Sensor de Movimiento

**Realizado por:** Daniel Vilañez, 2018

*Sensor de Gases*

Para el sensor de gas se utilizó, además del sensor MQ4, un sensor MQ2 el cual nos sirvió como referencia para el nivel a medir, para esto se realizó 3 pruebas con valores de voltaje de 119, 195 y 255. Se recogieron un total de 87 muestras, mediante el software Arduino, Fig. 2-3, para los cálculos respectivos.

En la tabla 4-3, se puede observar que el sensor de gas presenta una imprecisión de ±0.02312 a un valor de 119.

**Tabla 4-3** Prueba sensor de Gas valor de 119

| Media Xi | Frecuencia fi | Xifi | X-Xi |
|---|---|---|---|
| 118 | 5 | 590 | 1.01 |
| 119 | 76 | 9044 | 0.01 |
| 120 | 6 | 720 | -0.99 |
| | | 10354 | |
| **Media *X*** | 119.01 | | |
| **Error Absoluto** | 0.02312 | | |

**Realizado por:** Vilañez, Daniel, 2019

En la tabla 5-3, se puede observar que el sensor de gas presenta una imprecisión de ±0.02550 a un valor de 195.

**Tabla 5-3** Prueba sensor de Gas valor de 195

| Media Xi | Frecuencia fi | Xifi | X-Xi |
|---|---|---|---|
| 194 | 32 | 6208 | 0.78 |
| 195 | 42 | 8190 | -0.22 |
| 196 | 13 | 2548 | -1.22 |
| | | 16946 | |
| **Media X** | 194.78 | | |
| **Error Absoluto** | 0.02550 | | |

**Realizado por:** Vilañez, Daniel, 2019

En la tabla 6-3, se puede observar que el sensor de gas presenta una imprecisión de ±0.027 a un valor de 255.

**Tabla 6-3** Prueba sensor de Gas valor de 255

| Media Xi | Frecuencia fi | Xifi | X-Xi |
|---|---|---|---|
| 253 | 11 | 2783 | 1.38 |
| 254 | 32 | 8128 | 0.38 |
| 255 | 44 | 11220 | -0.62 |
| | | 22131 | |
| **Media X** | 254.38 | | |
| **Error Absoluto** | 0.027 | | |

**Realizado por:** Vilañez, Daniel, 2019

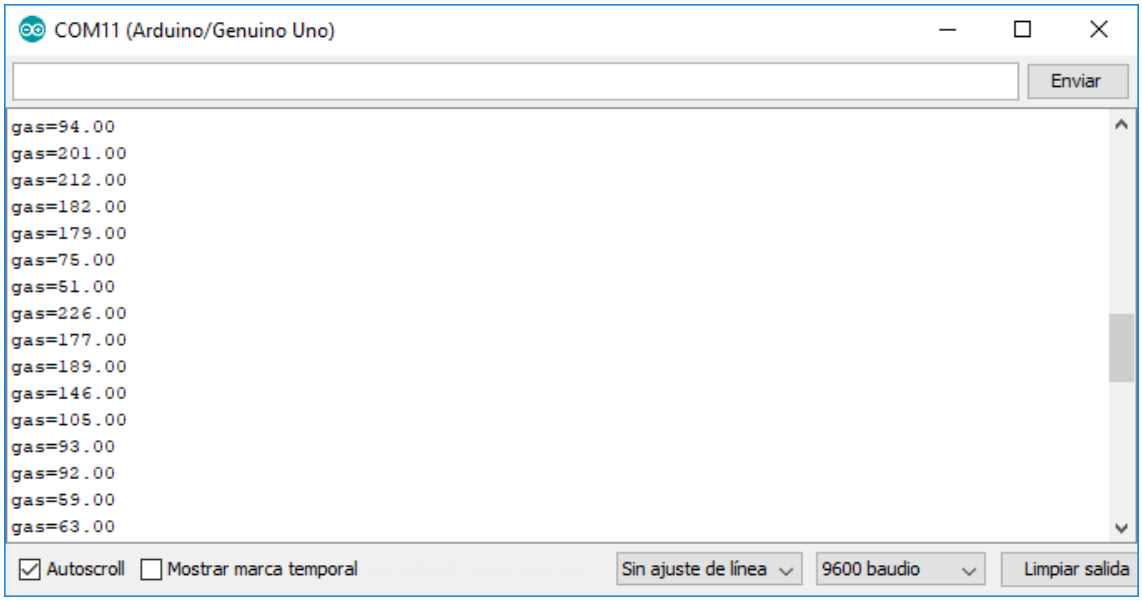


**Figura 2-3** Mediciones de Sensor de Gas

**Realizado por:** Daniel Vilañez, 2018

### *3.1.1.2. Tiempo de Subida de Datos a Azure*

Los resultados del tiempo de subida fueron realizados con una conexión a internet estable, esto influye en gran medida debido a que si se tiene una mala conexión el tiempo de respuesta aumentara en gran medida tanto en la parte del usuario como en la del nodo coordinador.

En la tabla 7-3 se realiza un análisis de los tiempos de subida de los nodos sensores de la red, de los cuales se calcula un tiempo medio y se lo toma como el tiempo de subida de los datos a la base de datos. Entendiéndose como Coordinador el tiempo que toma a los datos llegar hasta el nodo coordinador, Computador el tiempo de la conexión serial del computador con el nodo

coordinador y el tiempo que le toma acondicionar la información, Base de Datos el tiempo que le toma subir la información a la base de datos.

**Tabla 7-3** Tiempo de Subida de Nodo Sensor

| N° Muestra | Coordinador | Base de Datos | Base de Datos | Total |
|---|---|---|---|---|
| **1** | 0.08 | 0.00404 | 0.45593 | 0.53997 |
| **2** | 0.08 | 0.00419 | 0.345144 | 0.429334 |
| **3** | 0.08 | 0.004095 | 0.512728 | 0.596823 |
| **4** | 0.08 | 0.004102 | 0.480312 | 0.564414 |
| **5** | 0.08 | 0.004044 | 0.444733 | 0.528777 |
| **6** | 0.08 | 0.004071 | 0.349612 | 0.433683 |
| **7** | 0.08 | 0.004098 | 0.354492 | 0.43859 |
| **8** | 0.08 | 0.004026 | 0.459371 | 0.543397 |
| **9** | 0.08 | 0.004053 | 0.364251 | 0.448304 |
| **10** | 0.08 | 0.00408 | 0.469131 | 0.553211 |
| **11** | 0.08 | 0.004007 | 0.47401 | 0.558017 |
| **12** | 0.08 | 0.004034 | 0.37889 | 0.084034 |
| **13** | 0.08 | 0.004062 | 0.453769 | 0.537831 |
| **14** | 0.08 | 0.004089 | 0.388649 | 0.472738 |
| **15** | 0.08 | 0.004016 | 0.493529 | 0.577545 |
| **16** | 0.08 | 0.004043 | 0.398408 | 0.482451 |
| **17** | 0.08 | 0.00407 | 0.503288 | 0.587358 |
| **18** | 0.08 | 0.004098 | 0.408167 | 0.492265 |
| **19** | 0.08 | 0.004025 | 0.513047 | 0.597072 |
| **20** | 0.08 | 0.004052 | 0.417927 | 0.501979 |
| **21** | 0.08 | 0.004079 | 0.322806 | 0.406885 |
| **22** | 0.08 | 0.004006 | 0.427686 | 0.511692 |
| **23** | 0.08 | 0.004034 | 0.332565 | 0.416599 |
| **24** | 0.08 | 0.004061 | 0.537445 | 0.621506 |
| **25** | 0.08 | 0.004088 | 0.442325 | 0.526413 |
| **26** | 0.08 | 0.004015 | 0.447204 | 0.531219 |
| **27** | 0.08 | 0.004042 | 0.452084 | 0.536126 |
| **28** | 0.08 | 0.00407 | 0.356963 | 0.441033 |
| **29** | 0.08 | 0.004097 | 0.461843 | 0.54594 |
| **30** | 0.08 | 0.004024 | 0.366723 | 0.450747 |
| **31** | 0.08 | 0.004051 | 0.371602 | 0.455653 |
| **32** | 0.08 | 0.004078 | 0.476482 | 0.56056 |
| **33** | 0.08 | 0.004006 | 0.511361 | 0.595367 |
| **34** | 0.08 | 0.004033 | 0.506241 | 0.590274 |
| **35** | 0.08 | 0.004005 | 0.491121 | 0.575126 |
| **36** | 0.08 | 0.004077 | 0.37596 | 0.460037 |

| | | | | |
|---|---|---|---|---|
| **37** | 0.08 | 0.004014 | 0.40088 | 0.484894 |
| **38** | 0.08 | 0.004042 | 0.505759 | 0.589801 |
| **39** | 0.08 | 0.004069 | 0.510639 | 0.594708 |
| **40** | 0.08 | 0.004096 | 0.415519 | 0.499615 |
| **41** | 0.08 | 0.004123 | 0.320398 | 0.404521 |
| **42** | 0.08 | 0.004151 | 0.325278 | 0.409429 |
| **43** | 0.08 | 0.004078 | 0.430157 | 0.514235 |
| **44** | 0.08 | 0.00402 | 0.435037 | 0.519057 |
| **45** | 0.08 | 0.004132 | 0.539917 | 0.624049 |
| **46** | 0.08 | 0.004059 | 0.444796 | 0.528855 |
| **47** | 0.08 | 0.004086 | 0.549676 | 0.633762 |
| **48** | 0.08 | 0.004014 | 0.454555 | 0.538569 |
| **49** | 0.08 | 0.004041 | 0.359435 | 0.443476 |
| **50** | 0.08 | 0.004168 | 0.464314 | 0.548482 |
| **51** | 0.08 | 0.004195 | 0.519194 | 0.603389 |
| **52** | 0.08 | 0.004122 | 0.484074 | 0.568196 |
| **53** | 0.08 | 0.00415 | 0.378953 | 0.463103 |
| **54** | 0.08 | 0.004077 | 0.483833 | 0.56791 |
| **55** | 0.08 | 0.004104 | 0.358712 | 0.442816 |
| **56** | 0.08 | 0.004031 | 0.463592 | 0.547623 |
| **57** | 0.08 | 0.004058 | 0.518472 | 0.60253 |
| **58** | 0.08 | 0.004186 | 0.523351 | 0.607537 |
| **59** | 0.08 | 0.004113 | 0.538231 | 0.622344 |
| **60** | 0.08 | 0.00414 | 0.52311 | 0.60725 |
| **61** | 0.08 | 0.004067 | 0.41799 | 0.502057 |
| **62** | 0.08 | 0.004094 | 0.37287 | 0.456964 |
| **63** | 0.08 | 0.004022 | 0.357749 | 0.441771 |
| **64** | 0.08 | 0.004049 | 0.422629 | 0.506678 |
| **65** | 0.08 | 0.004176 | 0.437508 | 0.521684 |
| **66** | 0.08 | 0.004103 | 0.512388 | 0.596491 |
| **67** | 0.08 | 0.00403 | 0.517268 | 0.601298 |
| **68** | 0.08 | 0.004158 | 0.542147 | 0.626305 |
| **69** | 0.08 | 0.004085 | 0.537027 | 0.621112 |
| **70** | 0.08 | 0.004112 | 0.461906 | 0.546018 |
| **71** | 0.08 | 0.004139 | 0.366786 | 0.450925 |
| **72** | 0.08 | 0.004066 | 0.371666 | 0.455732 |
| **73** | 0.08 | 0.004094 | 0.376545 | 0.460639 |
| **74** | 0.08 | 0.004021 | 0.371425 | 0.455446 |
| **75** | 0.08 | 0.004048 | 0.386304 | 0.470352 |
| **76** | 0.08 | 0.004075 | 0.491184 | 0.575259 |
| **77** | 0.08 | 0.004102 | 0.496064 | 0.580166 |
| **78** | 0.08 | 0.00413 | 0.500943 | 0.585073 |
| **79** | 0.08 | 0.004057 | 0.505823 | 0.58988 |

| | | | | |
|---|---|---|---|---|
| **80** | 0.08 | 0.004084 | 0.510702 | 0.594786 |
| **81** | 0.08 | 0.004011 | 0.515582 | 0.599593 |
| **82** | 0.08 | 0.004138 | 0.420462 | 0.5046 |
| **83** | 0.08 | 0.004066 | 0.425341 | 0.509407 |
| **84** | 0.08 | 0.004093 | 0.330221 | 0.414314 |
| **85** | 0.08 | 0.00412 | 0.48351 | 0.56763 |
| **86** | 0.08 | 0.004147 | 0.43998 | 0.524127 |
| **87** | 0.08 | 0.004074 | 0.44486 | 0.528934 |
| **Media** | **0.08** | **0.004076908** | **0.438295069** | **0.522372** |

**Realizado por:** Vilañez, Daniel, 2019

Tiempo medio de conexión con coordinador: 0.08s
Tiempo medio de conexión con el computador: 0.004076908s
Tiempo medio de conexión con nodo base de datos: 0.438295069

**Tiempo medio total de subida de datos a Azure: 0.522372s**

El tiempo de subida total medio es de aproximadamente 0.522372 segundos, en condiciones ideales, esto quiere decir con una conexión de internet estable y comunicación con línea de vista directa.

### 3.1.2. ***Pruebas en Nodo Actuador***

Para realizar las pruebas en el nodo actuador se utilizó la aplicación de escritorio, mediante la que se solicita la ejecución de una acción, y la visualización de los resultados se obtuvo mediante el uso del software Wireshark.

#### *3.1.2.1. Prueba de Activación*

El software Whireshark ayuda en la visualización de la conexión de la red de con la base de datos y muestra las consultas realizadas hacia la base de datos, y en adición a esto también posee una extensión que permite observar el comportamiento de los puertos USB que nos sirve para obtener los datos que se envían y reciben en el nodo coordinador.

En la figura 3-3 se puede observar la ejecución de la aplicación que solicita se encienda la iluminación. Acción que genera los paquetes mostrados en la figura 4-3, en la que observamos la captura de paquetes enviados y recibidos a la base de datos, y en la figura 5-3 se puede observar la comunicación con el nodo coordinador que envía la comunicación con el nodo coordinador.

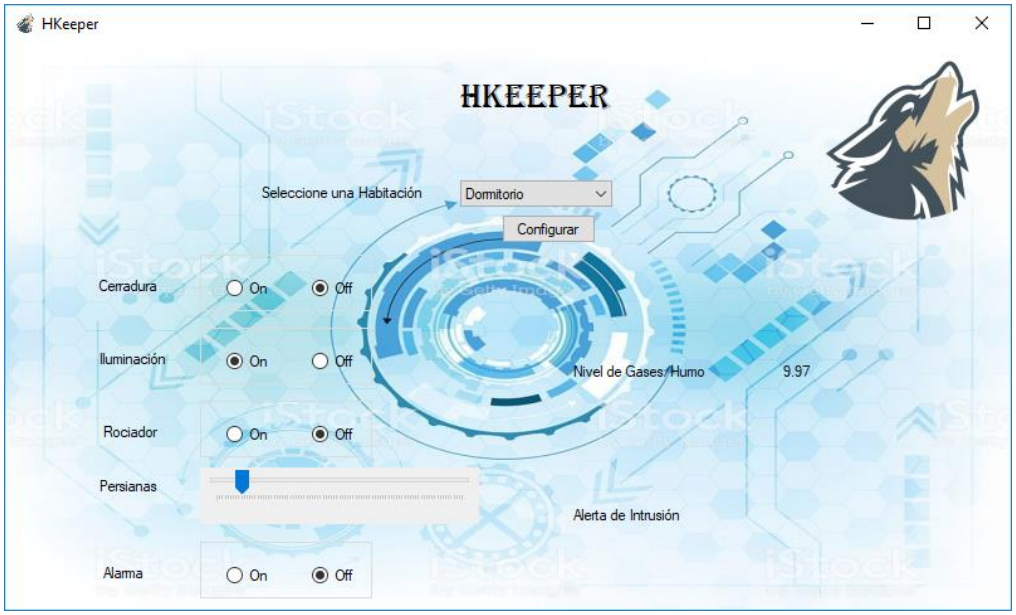


**Figura 3-3** Aplicación de Escritorio

**Realizado por:** Daniel Vilañez, 2018

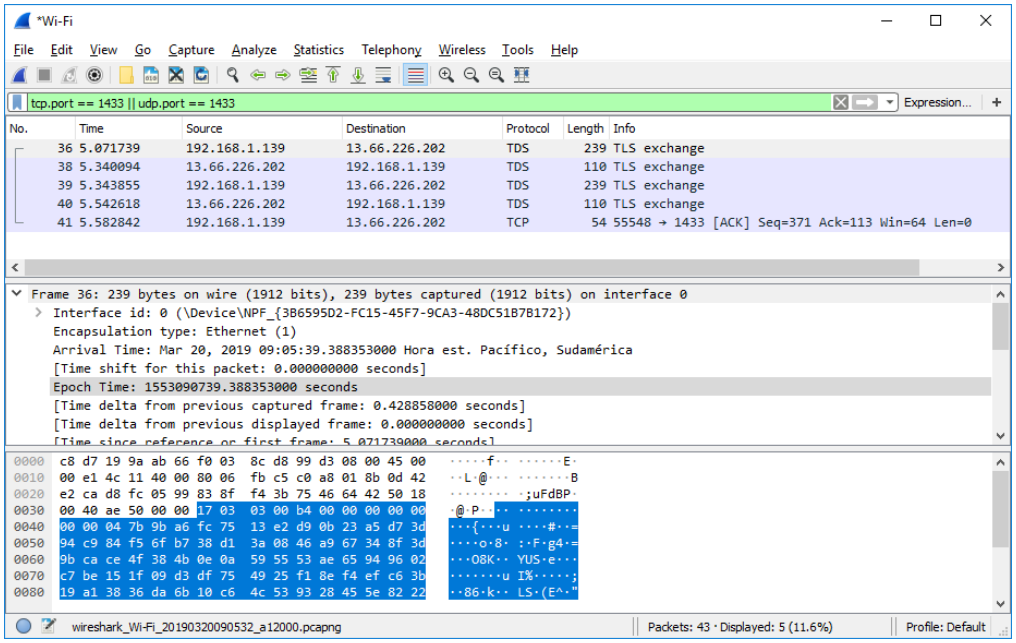


**Figura 4-3** Conexión a Base de Datos

**Realizado por:** Daniel Vilañez, 2018

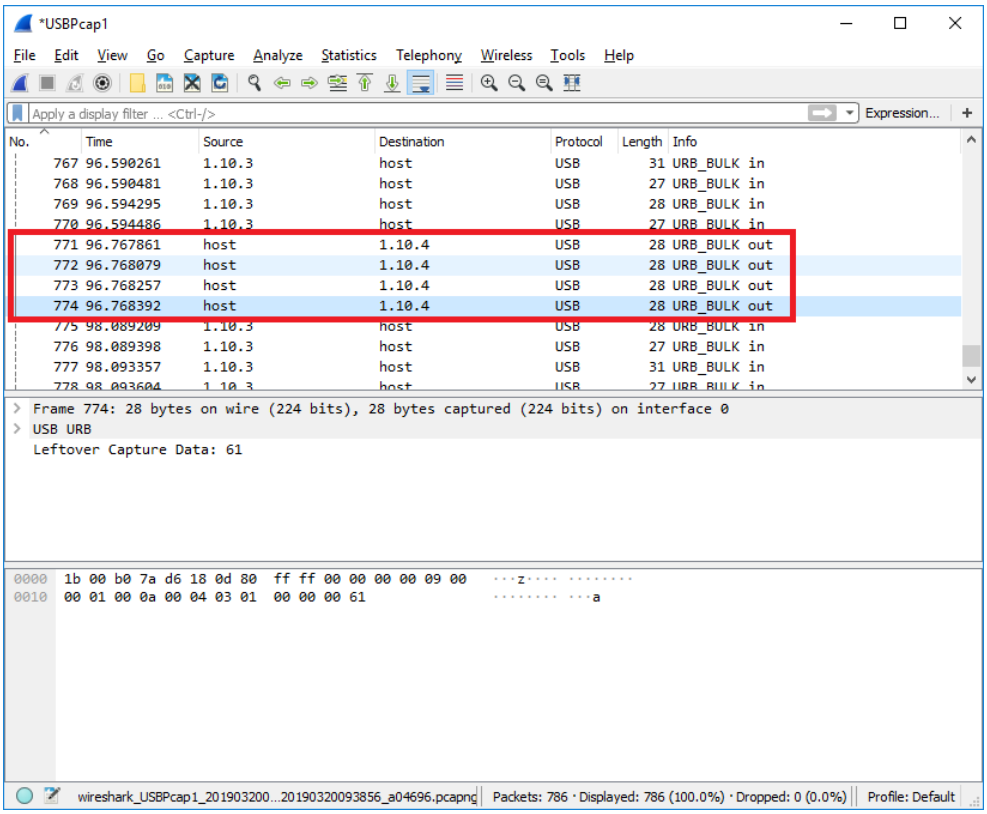


**Figura 5-3** Conexión con tarjeta de desarrollo

**Realizado por:** Daniel Vilañez, 2018

### *3.1.2.2. Prueba de Tiempos de Respuesta*

Para la obtención del tiempo de respuesta de una acción se utilizará de igual manera el software Wireshark, mediante el cual se puede obtener los tiempos de ejecución de los comandos programados tanto en la aplicación como en la tarjeta de desarrollo.

Los resultados del tiempo de respuesta fueron realizados con una conexión a internet estable, esto influye en gran medida debido a que si se tiene una mala conexión el tiempo de respuesta aumentara en gran medida tanto en la parte del usuario como en la del nodo coordinador.

En la tabla 8-3 se realiza un análisis de los tiempos de respuesta de los nodos actuadores de la red, de los cuales se calcula un tiempo medio y se lo toma como el tiempo que se demora el sistema en reaccionar a una acción. Entendiéndose como Base de Datos el tiempo que le toma a una orden quedar almacenada en la base de datos, Computador el tiempo de conexión entre la base de datos al computador, Coordinador el tiempo que toma a los datos llegar hasta el nodo coordinador, Actuador el tiempo que le toma a la información llegar desde el nodo coordinador al nodo actuador para que ejecute la acción necesaria.

**Tabla 8-3** Tiempo de Respuesta del Nodo Actuador

| N° Muestra | Base de Datos | Computador | Coordinador | Actuador | Total |
|---|---|---|---|---|---|
| **1** | 0.507761 | 0.45593 | 0.004012 | 0.08 | 1.047703 |
| **2** | 0.473595 | 0.345144 | 0.004095 | 0.08 | 0.902834 |
| **3** | 0.540549 | 0.512728 | 0.004097 | 0.08 | 1.137374 |
| **4** | 0.525951 | 0.416334 | 0.004102 | 0.08 | 1.026387 |
| **5** | 0.542345 | 0.444733 | 0.004044 | 0.08 | 1.071122 |
| **6** | 0.454497 | 0.349612 | 0.004071 | 0.08 | 0.88818 |
| **7** | 0.466649 | 0.354492 | 0.004098 | 0.08 | 0.905239 |
| **8** | 0.478802 | 0.459371 | 0.004026 | 0.08 | 1.022199 |
| **9** | 0.500954 | 0.364251 | 0.004053 | 0.08 | 0.949258 |
| **10** | 0.503107 | 0.469131 | 0.00408 | 0.08 | 1.056318 |
| **11** | 0.515259 | 0.47401 | 0.004007 | 0.08 | 1.073276 |
| **12** | 0.517411 | 0.37889\| | 0.004034 | 0.08 | 0.601445 |
| **13** | 0.539564 | 0.453769 | 0.004062 | 0.08 | 1.077395 |
| **14** | 0.451716 | 0.388649 | 0.004089 | 0.08 | 0.924454 |
| **15** | 0.463869 | 0.493529 | 0.004016 | 0.08 | 1.041414 |
| **16** | 0.546021 | 0.398408 | 0.004043 | 0.08 | 1.028472 |
| **17** | 0.508173 | 0.503288 | 0.00407 | 0.08 | 1.095531 |
| **18** | 0.460326 | 0.408167 | 0.004098 | 0.08 | 0.952591 |
| **19** | 0.472478 | 0.513047 | 0.004025 | 0.08 | 1.06955 |
| **20** | 0.524631 | 0.417927 | 0.004052 | 0.08 | 1.02661 |
| **21** | 0.526783 | 0.322806 | 0.004079 | 0.08 | 0.933668 |
| **22** | 0.548935 | 0.427686 | 0.004006 | 0.08 | 1.060627 |
| **23** | 0.541088 | 0.332565 | 0.004034 | 0.08 | 0.957687 |
| **24** | 0.47324 | 0.537445 | 0.004061 | 0.08 | 1.094746 |
| **25** | 0.478539 | 0.442325 | 0.004088 | 0.08 | 1.004952 |
| **26** | 0.479754 | 0.447204 | 0.004015 | 0.08 | 1.010973 |
| **27** | 0.509697 | 0.452084 | 0.004042 | 0.08 | 1.045823 |
| **28** | 0.52185 | 0.356963 | 0.00407 | 0.08 | 0.962883 |
| **29** | 0.543402 | 0.461843 | 0.004097 | 0.08 | 1.089342 |
| **30** | 0.546154 | 0.366723 | 0.004024 | 0.08 | 0.996901 |
| **31** | 0.458307 | 0.371602 | 0.004051 | 0.08 | 0.91396 |
| **32** | 0.530459 | 0.476482 | 0.004078 | 0.08 | 1.091019 |
| **33** | 0.502612 | 0.511361 | 0.004006 | 0.08 | 1.097979 |
| **34** | 0.494764 | 0.506241 | 0.004033 | 0.08 | 1.085038 |
| **35** | 0.496916 | 0.491121 | 0.004005 | 0.08 | 1.072042 |
| **36** | 0.491906 | 0.37596 | 0.004077 | 0.08 | 0.951943 |
| **37** | 0.493122 | 0.40088 | 0.004014 | 0.08 | 0.978016 |
| **38** | 0.543374 | 0.505759 | 0.004042 | 0.08 | 1.133175 |
| **39** | 0.555526 | 0.510639 | 0.004069 | 0.08 | 1.150234 |
| **40** | 0.467678 | 0.415519 | 0.004096 | 0.08 | 0.967293 |
| **41** | 0.539831 | 0.320398 | 0.004123 | 0.08 | 0.944352 |

| | | | | | |
|---|---|---|---|---|---|
| **42** | 0.531983 | 0.325278 | 0.004151 | 0.08 | 0.941412 |
| **43** | 0.534136 | 0.430157 | 0.004078 | 0.08 | 1.048371 |
| **44** | 0.516288 | 0.435037 | 0.00402 | 0.08 | 1.035345 |
| **45** | 0.518441 | 0.539917 | 0.004132 | 0.08 | 1.14249 |
| **46** | 0.490593 | 0.444796 | 0.004059 | 0.08 | 1.019448 |
| **47** | 0.452745 | 0.549676 | 0.004086 | 0.08 | 1.086507 |
| **48** | 0.454898 | 0.454555 | 0.004014 | 0.08 | 0.993467 |
| **49** | 0.54705 | 0.359435 | 0.004041 | 0.08 | 0.990526 |
| **50** | 0.489203 | 0.464314 | 0.004168 | 0.08 | 1.037685 |
| **51** | 0.511355 | 0.519194 | 0.004195 | 0.08 | 1.114744 |
| **52** | 0.513507 | 0.484074 | 0.004122 | 0.08 | 1.081703 |
| **53** | 0.52566 | 0.378953 | 0.00415 | 0.08 | 0.988763 |
| **54** | 0.513781 | 0.483833 | 0.004077 | 0.08 | 1.081691 |
| **55** | 0.549965 | 0.358712 | 0.004104 | 0.08 | 0.992781 |
| **56** | 0.462117 | 0.463592 | 0.004031 | 0.08 | 1.00974 |
| **57** | 0.464269 | 0.518472 | 0.004058 | 0.08 | 1.066799 |
| **58** | 0.486422 | 0.523351 | 0.004186 | 0.08 | 1.093959 |
| **59** | 0.498574 | 0.538231 | 0.004113 | 0.08 | 1.120918 |
| **60** | 0.521072 | 0.52311 | 0.00414 | 0.08 | 1.128322 |
| **61** | 0.522879 | 0.41799 | 0.004067 | 0.08 | 1.024936 |
| **62** | 0.443503 | 0.37287 | 0.004094 | 0.08 | 0.900467 |
| **63** | 0.524718 | 0.357749 | 0.004022 | 0.08 | 0.966489 |
| **64** | 0.525933 | 0.422629 | 0.004049 | 0.08 | 1.032611 |
| **65** | 0.471489 | 0.437508 | 0.004176 | 0.08 | 0.993173 |
| **66** | 0.483641 | 0.512388 | 0.004103 | 0.08 | 1.080132 |
| **67** | 0.479579 | 0.517268 | 0.00403 | 0.08 | 1.080877 |
| **68** | 0.507946 | 0.542147 | 0.004158 | 0.08 | 1.134251 |
| **69** | 0.520098 | 0.537027 | 0.004085 | 0.08 | 1.14121 |
| **70** | 0.532251 | 0.461906 | 0.004112 | 0.08 | 1.078269 |
| **71** | 0.53444 | 0.366786 | 0.004139 | 0.08 | 0.985365 |
| **72** | 0.556555 | 0.371666 | 0.004066 | 0.08 | 1.012287 |
| **73** | 0.468708 | 0.376545 | 0.004094 | 0.08 | 0.929347 |
| **74** | 0.48086 | 0.371425 | 0.004021 | 0.08 | 0.936306 |
| **75** | 0.493013 | 0.386304 | 0.004048 | 0.08 | 0.963365 |
| **76** | 0.425165 | 0.491184 | 0.004075 | 0.08 | 1.000424 |
| **77** | 0.437317 | 0.496064 | 0.004102 | 0.08 | 1.017483 |
| **78** | 0.41947 | 0.500943 | 0.00413 | 0.08 | 1.004543 |
| **79** | 0.441622 | 0.505823 | 0.004057 | 0.08 | 1.031502 |
| **80** | 0.453775 | 0.510702 | 0.004084 | 0.08 | 1.048561 |
| **81** | 0.465927 | 0.515582 | 0.004011 | 0.08 | 1.06552 |
| **82** | 0.478079 | 0.420462 | 0.004138 | 0.08 | 0.982679 |
| **83** | 0.490232 | 0.425341 | 0.004066 | 0.08 | 0.999639 |
| **84** | 0.502384 | 0.330221 | 0.004093 | 0.08 | 0.916698 |

| | | | | | |
|---|---|---|---|---|---|
| **85** | 0.514537 | 0.48351 | 0.00412 | 0.08 | 1.082167 |
| **86** | 0.526689 | 0.43998 | 0.004147 | 0.08 | 1.050816 |
| **87** | 0.538841 | 0.44486 | 0.004074 | 0.08 | 1.067775 |
| **Media** | **0.500681667** | **0.43755969** | **0.00407552** | **0.08** | **1.0223169** |

**Realizado por:** Vilañez, Daniel, 2019

Tiempo medio de conexión con la base de datos: 0.500681667s

Tiempo medio de conexión con el computador: 0. 43755969s

Tiempo medio de conexión con nodo coordinador: 0. 00407552s

Tiempo medio de conexión con nodo actuador: 0.08 s

**Tiempo medio total de conexión con nodo actuador: 1.0223169s**

El tiempo de respuesta total medio es de aproximadamente 1.0223169 segundos, en condiciones ideales, esto quiere decir con una conexión de internet estable y comunicación con línea de vista directa.

### 3.1.3. *Pruebas en Nodo Coordinador*

Con la configuración de cada uno de los nodos como se explicó en la tabla 2-1, figura 6-3, se realizaron las pruebas en el nodo coordinador.

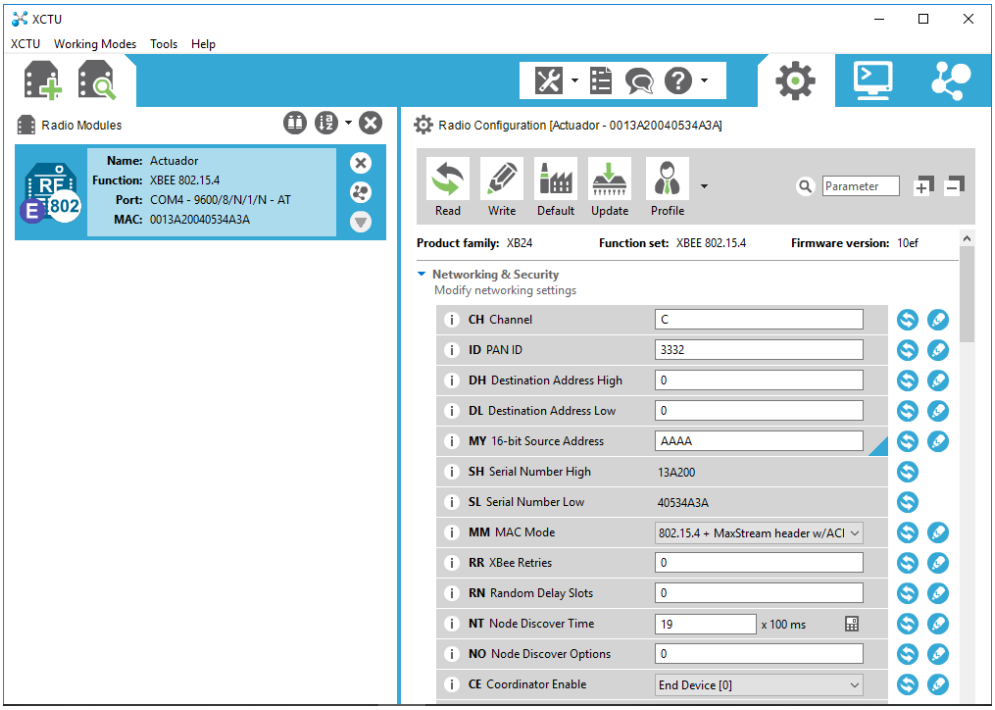


**Figura 6-3** IDE XCTU de Digi

**Realizado por:** Daniel Vilañez, 2018

### *3.1.3.1. Prueba de Conexión con los Nodos*

El sortware XCTU nos permite realizar un escaneo para detectar todos los posibles dispositivos que se encuentran alrededor, siempre y cuando tengan la misma configuración de canal y PAN ID, como se muestra en la figura 7-3.

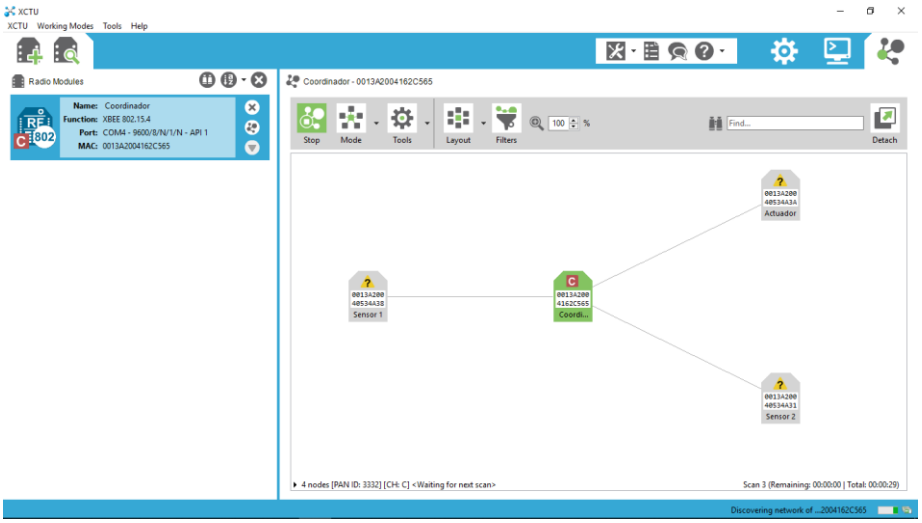


**Figura 7-3** Detección de Nodos

**Realizado por:** Daniel Vilañez, 2018

En la figura 8-3 se puede observar las tramas que recibe y envía el nodo coordinador, el cual nos indica los dispositivos activos actualmente y el tipo de información que recibe de cada uno de los nodos, además de enviar la información necesaria hacia los nodos actuadores.

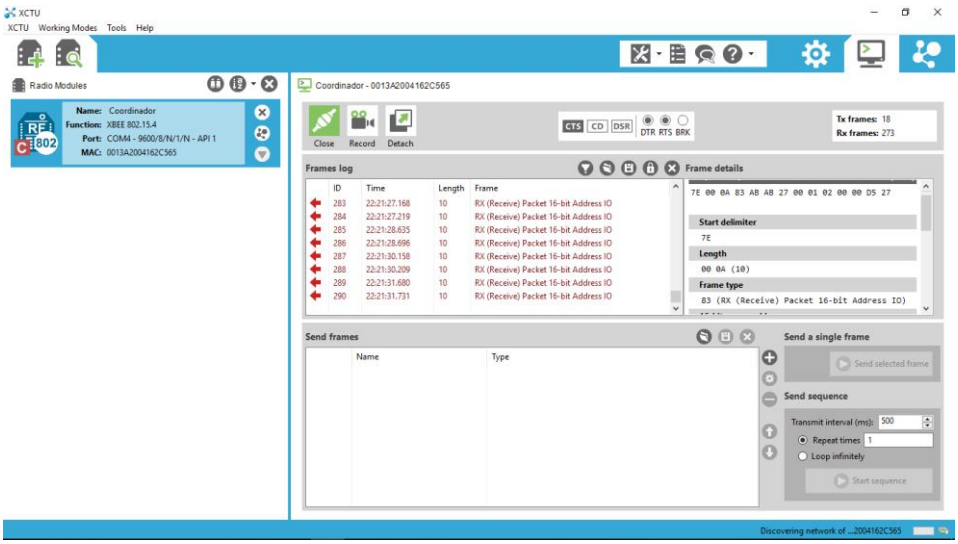


**Figura 8-3** Captura de Paquetes Recibidos en el Nodo Coordinador

**Realizado por:** Daniel Vilañez, 2018

### *3.1.3.2. Prueba de Conexión con Tarjeta de Desarrollo*

Para la conexión del Nodo Coordinador con la tarjeta de desarrollo se establece una conexión de tipo serial entre estas. El resultado de la comunicación serial es información en forma de tramas Zigbee, como se muestra en la figura 9-3, por lo cual fue necesario buscar una forma de obtener la información.

Para esto se realizó un algoritmo basado en el lenguaje de programación C++ con el cual trabaja el IDE Arduino, con el cual se pudo obtener los datos de cada uno de los sensores, como se muestra en la figura 10-3, para posteriormente poderlos enviar a la base de datos.

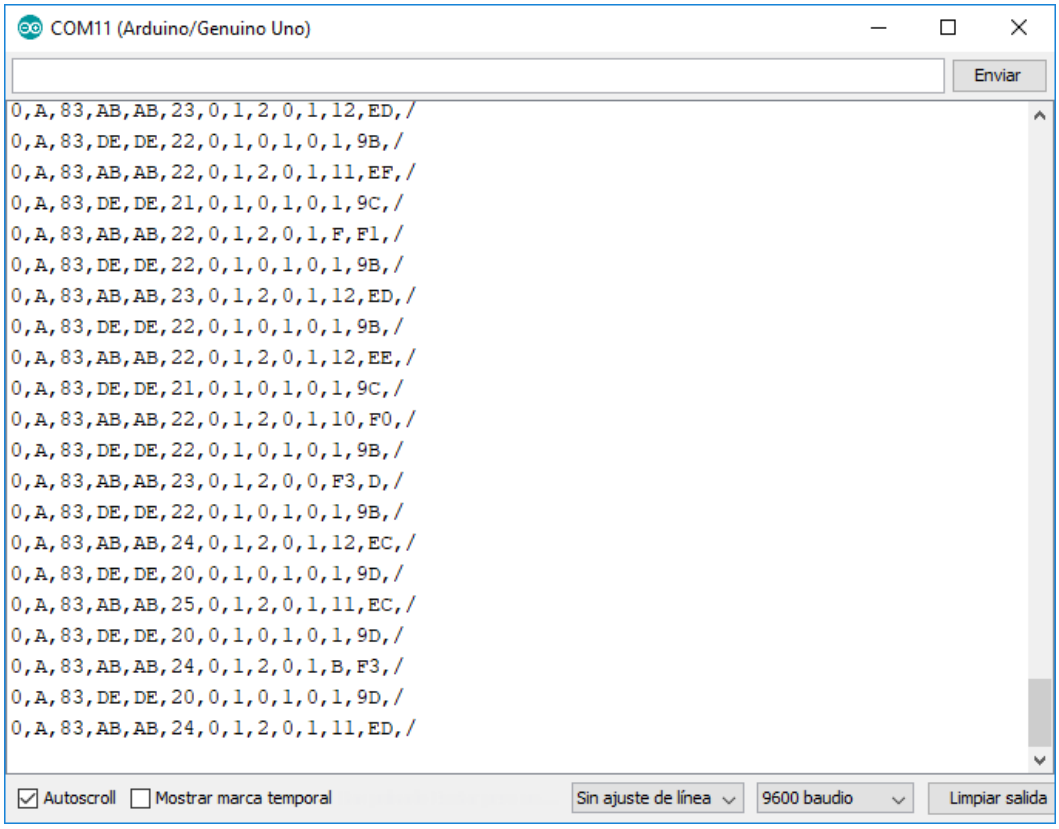


**Figura 9-3** Obtención de Tramas Zigbee con Arduino

**Realizado por:** Daniel Vilañez, 2018

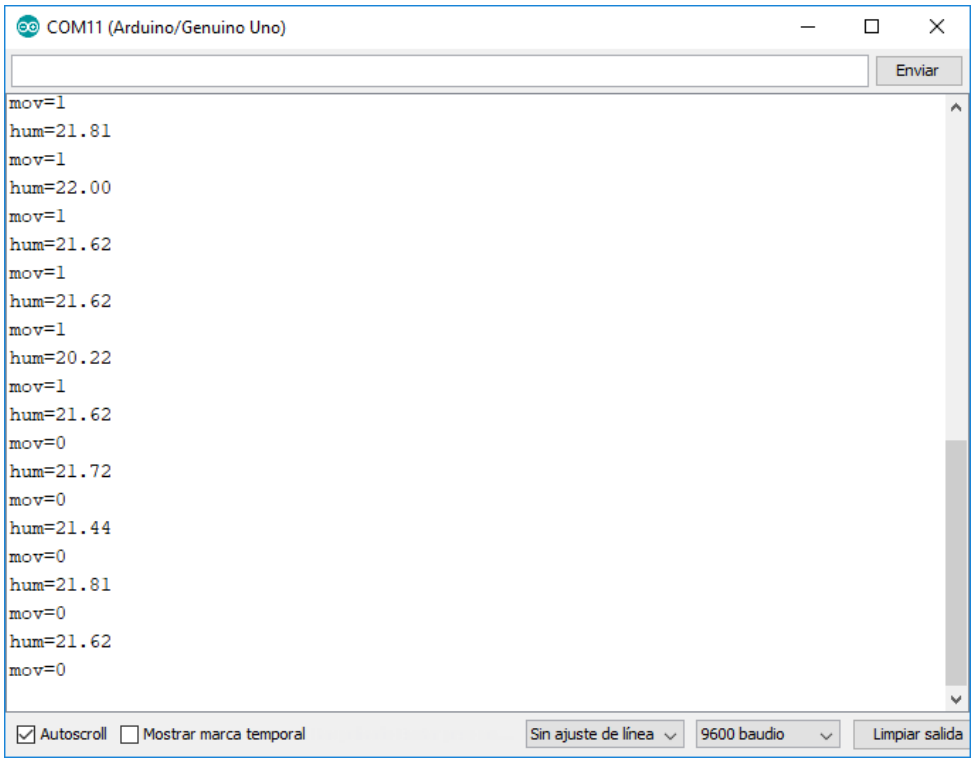


**Figura 10-3** Obtención de la Información presente en las Tramas

**Realizado por:** Daniel Vilañez, 2018

### *3.1.3.3. Prueba de Conexión con Windows Azure*

Para realizar la prueba de conexión con la base de datos es necesario analizar la red LAN, para lo cual se procede a utilizar el software Wireshark, filtrando la información del puerto 1433 que es el encargado de hacer consultas de bases basadas en SQL Server que es el lenguaje que se utiliza en Windows Azure para la base de datos.

Tanto la información enviada como la recibida a través de las aplicaciones se puede observar en la figura 11-3.

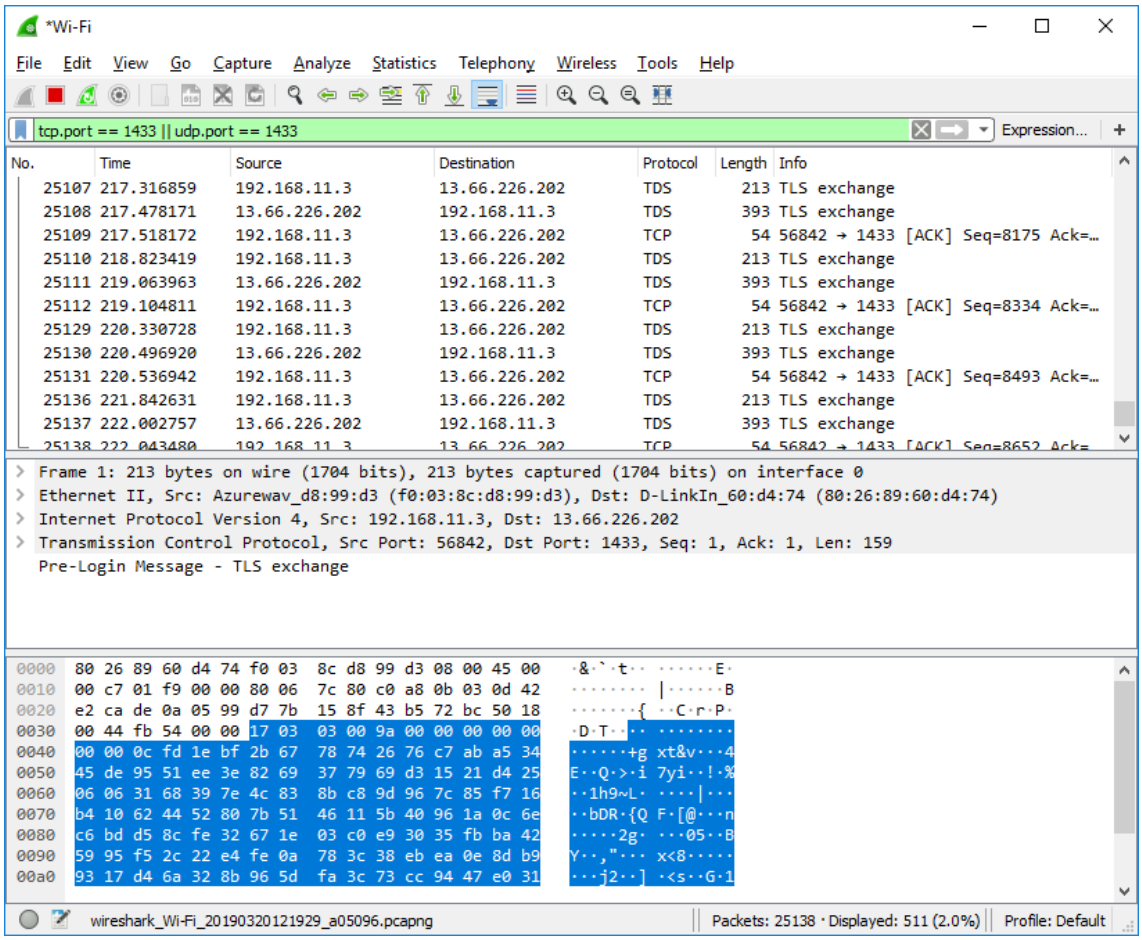


**Figura 11-3** Análisis de WLAN para deteccion de Conexion a Base de Datos

**Realizado por:** Daniel Vilañez, 2018

## 3.2. **Prueba de Alerta del Sistema**

Con los parámetros definidos en el apartado 2.3 del capítulo 2 se procede a realizar las pruebas, interactuando directamente en la base de datos y modificando los valores de cada uno de los sensores para obtener los resultados deseados.

Para poder visualizar la alerta de intrusión en el hogar se procede a modificar los valores de los sensores de movimiento y vibración, por lo cual el sistema emite una alerta la cual podemos observar en la figura 12-3.

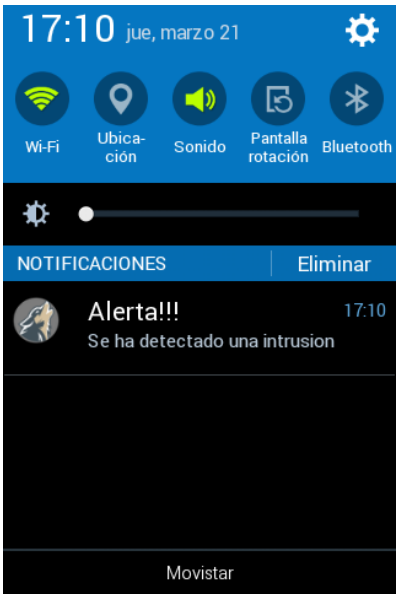


**Figura 12-3** Alerta de Intrusión

**Realizado por:** Daniel Vilañez, 2018

De igual manera para la activacion de la alerta de fuga de gas se procede a modificar el valor del sensor de gases, obteniendo asi la alerta que se puede visualizar en la figura 13-3.

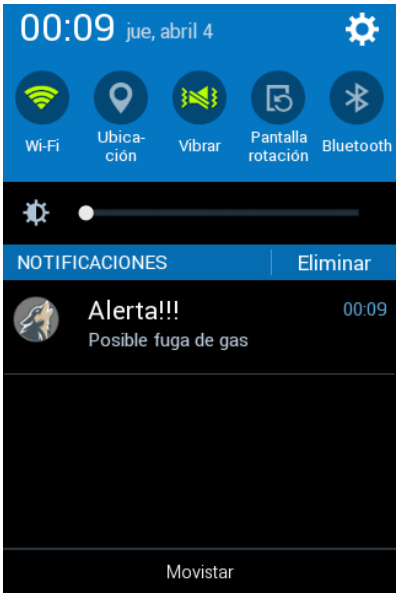


**Figura 13-3** Alerta de Fuga de Gas

**Realizado por:** Daniel Vilañez, 2018

De igual manera se alteran los valores para obtener las alertas de precaución para cada uno de los casos antes mencionados, el resultado lo podemos observar en la figura 14-3.

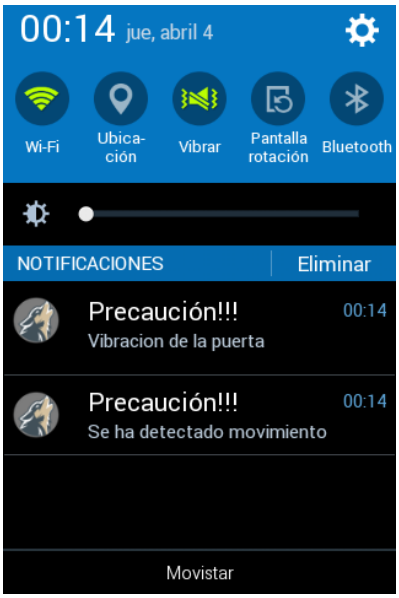


**Figura 14-3** Precauciones del Sistema

**Realizado por:** Daniel Vilañez, 2018

## 3.3. **Pérdida de Paquetes**

Para definir la tasa de entrega de paquetes, se realiza la relación existente entre paquetes enviados y paquetes recibidos obteniendo el porcentaje de fiabilidad en la entrega de paquetes que tiene. El número de paquetes que serán enviados en cada uno de los casos respeta el número de muestras definido en el apartado 2.3.1.

$$Tasa\ de\ Entrega = \frac{Paquetes\ Recibidos}{Paquetes\ Entregados} * 100\%$$

Para la realización de las pruebas se colocó los sensores/actuadores a diferentes distancias del nodo coordinador, así mismo con línea de vista directa y con obstáculos. Las distancias con las cuales se trabajó tanto en línea de vista directa como con obstáculos son de 1m, 3m, 5m, 7m, 9m.

### 3.3.1. ***Línea de Vista Directa***

Los resultados para la tasa de entrega de paquetes de los diferentes nodos de la red a las diferentes distancias con línea de vista directa se pueden observar a continuación.

La primera distancia con la cual se realizó la prueba fue de 1m, obteniendo los resultados de la tabla 9-3.

**Tabla 9-3** Tasa de Entrega de Red a 1m en Línea de Vista Directa

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 87 | 100 |
| **Vibración** | 87 | 87 | 100 |
| **Gases** | 87 | 87 | 100 |
| **Cerradura** | 87 | 87 | 100 |
| **Iluminación** | 87 | 87 | 100 |
| **Persiana** | 87 | 87 | 100 |
| **Alarma** | 87 | 87 | 100 |
| **Total** | **609** | **609** | **100** |

Vilañez, Daniel, 2019

Como se puede observar en la tabla 9-3 ninguno de los nodos presenta pérdida de paquetes debido a que la prueba fue realizada a una distancia corta y con línea de vista directa.

La siguiente distancia con la cual se realizó la prueba fue de 3m, obteniendo los resultados de la tabla 10-3.

**Tabla 10-3** Tasa de Entrega de Red a 3m en Línea de Vista Directa

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 83 | 95.40 |
| **Vibración** | 87 | 85 | 97.70 |
| **Gases** | 87 | 84 | 96.55 |
| **Cerradura** | 87 | 86 | 98.85 |
| **Iluminación** | 87 | 85 | 97.70 |
| **Persiana** | 87 | 85 | 97.70 |
| **Alarma** | 87 | 86 | 98.85 |
| **Total** | **609** | **594** | **97.54** |

**Realizado por:** Vilañez, Daniel, 2019

Como se puede observar en la tabla 10-3 los nodos presentan una pérdida de paquetes que no supera el 5% de paquetes perdidos esto debido a que los nodos están separados del nodo coordinador, pero no es una distancia demasiado grande, teniendo como porcentaje de pérdida del total de paquetes enviados alrededor de un 3% de pérdida de paquetes.

La siguiente distancia con la cual se realizó la prueba fue de 5m, obteniendo los resultados de la tabla 11-3.

**Tabla 11-3** Tasa de Entrega de Red a 5m en Línea de Vista Directa

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 80 | 91.95 |
| **Vibración** | 87 | 82 | 94.25 |
| **Gases** | 87 | 80 | 91.95 |
| **Cerradura** | 87 | 83 | 95.40 |
| **Iluminación** | 87 | 81 | 93.10 |
| **Persiana** | 87 | 82 | 94.25 |
| **Alarma** | 87 | 80 | 91.95 |
| **Total** | **609** | **568** | **93.27** |

**Realizado por:** Vilañez, Daniel, 2019

Como se puede observar en la tabla 11-3 los nodos presentan una pérdida de paquetes que no supera el 9% de paquetes perdidos esto debido a que los nodos están separados del nodo coordinador, empezando a ser una distancia media, teniendo como porcentaje de pérdida del total de paquetes enviados alrededor de un 7% de pérdida de paquetes, y con respecto al resultado anterior se tiene una diferencia de porcentaje de alrededor de 4%.

La siguiente distancia con la cual se realizó la prueba fue de 7m, obteniendo los resultados de la tabla 12-3.

**Tabla 12-3** Tasa de Entrega de Red a 7m en Línea de Vista Directa

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 77 | 88.51 |
| **Vibración** | 87 | 76 | 87.36 |
| **Gases** | 87 | 79 | 90.80 |
| **Cerradura** | 87 | 76 | 87.36 |
| **Iluminación** | 87 | 78 | 89.66 |
| **Persiana** | 87 | 77 | 88.51 |
| **Alarma** | 87 | 79 | 90.80 |
| **Total** | **609** | **542** | **89.00** |

**Realizado por:** Vilañez, Daniel, 2019

Como se puede observar en la tabla 12-3 los nodos presentan una pérdida de paquetes que no supera el 13% de paquetes perdidos esto debido a que los nodos están separados del nodo coordinador a una distancia media, teniendo como porcentaje de pérdida del total de paquetes

enviados un 11% de pérdida de paquetes, y con respecto al resultado anterior se tiene una diferencia de porcentaje de alrededor de 4%.

La última distancia con la cual se realizó la prueba fue de 9m, obteniendo los resultados de la tabla 13-3.

**Tabla 13-3** Tasa de Entrega de Red a 9m en Línea de Vista Directa

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 70 | 80.46 |
| **Vibración** | 87 | 72 | 82.76 |
| **Gases** | 87 | 73 | 83.91 |
| **Cerradura** | 87 | 72 | 82.76 |
| **Iluminación** | 87 | 71 | 81.61 |
| **Persiana** | 87 | 70 | 80.46 |
| **Alarma** | 87 | 71 | 81.61 |
| **Total** | **609** | **499** | **81.94** |

**Realizado por:** Vilañez, Daniel, 2019

Como se puede observar en la tabla 13-3 los nodos presentan una pérdida de paquetes que no supera el 20% de paquetes perdidos esto debido a que los nodos están separados del nodo coordinador a una distancia considerable, teniendo como porcentaje de pérdida del total de paquetes enviados alrededor de un 11% de pérdida de paquetes, y con respecto al resultado anterior se tiene una diferencia de porcentaje de alrededor de 8%, empezando a presentar una pérdida considerable con respecto a las otras pruebas realizadas.

### 3.3.2. *Con Obstáculos*

Los resultados para la tasa de entrega de paquetes de los diferentes nodos de la red a las diferentes distancias con obstáculos, entendiéndose obstáculos como la separación de los nodos por paredes, se pueden observar a continuación.

La primera distancia con la cual se realizó la prueba fue de 1m, obteniendo los resultados de la tabla 14-3.

**Tabla 14-3** Tasa de Entrega de Red a 1m con Obstáculos

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 84 | 96.55 |
| **Vibración** | 87 | 83 | 95.40 |
| **Gases** | 87 | 84 | 96.55 |
| **Cerradura** | 87 | 86 | 98.85 |
| **Iluminación** | 87 | 85 | 97.70 |
| **Persiana** | 87 | 86 | 98.85 |
| **Alarma** | 87 | 85 | 97.70 |
| **Total** | **609** | **593** | **97.37** |

**Realizado por:** Vilañez, Daniel, 2019

Como se puede observar en la tabla 14-3 los nodos presentan una pérdida de paquetes que no supera el 5% de paquetes perdidos esto debido a que los nodos están separados del nodo coordinador por una pared, teniendo como porcentaje de pérdida del total de paquetes enviados alrededor de un 3% de pérdida de paquetes.

La siguiente distancia con la cual se realizó la prueba fue de 3m, obteniendo los resultados de la tabla 15-3.

**Tabla 15-3** Tasa de Entrega de Red a 3m con Obstáculos

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 82 | 94.25 |
| **Vibración** | 87 | 80 | 91.95 |
| **Gases** | 87 | 81 | 93.10 |
| **Cerradura** | 87 | 83 | 95.40 |
| **Iluminación** | 87 | 81 | 93.10 |
| **Persiana** | 87 | 80 | 91.95 |
| **Alarma** | 87 | 82 | 94.25 |
| **Total** | **609** | **569** | **93.43** |

**Realizado por:** Vilañez, Daniel, 2019

Como se puede observar en la tabla 15-3 los nodos presentan una pérdida de paquetes que no supera el 9% de paquetes perdidos esto debido a que los nodos están separados del nodo coordinador por una pared a una distancia no tan grande, teniendo como porcentaje de pérdida del total de paquetes enviados alrededor de un 7% de pérdida de paquetes, y con respecto al resultado anterior se tiene una diferencia de porcentaje de alrededor de 4%.

La siguiente distancia con la cual se realizó la prueba fue de 5m, obteniendo los resultados de la tabla 16-3.

**Tabla 16-3** Tasa de Entrega de Red a 5m con Obstáculos

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 76 | 87.36 |
| **Vibración** | 87 | 77 | 88.51 |
| **Gases** | 87 | 79 | 90.80 |
| **Cerradura** | 87 | 76 | 87.36 |
| **Iluminación** | 87 | 78 | 89.66 |
| **Persiana** | 87 | 79 | 90.80 |
| **Alarma** | 87 | 78 | 89.66 |
| **Total** | **609** | **543** | **89.16** |

**Realizado por:** Vilañez, Daniel, 2019

Como se puede observar en la tabla 16-3 los nodos presentan una pérdida de paquetes que no supera el 13% de paquetes perdidos esto debido a que los nodos están separados del nodo coordinador por una pared a una distancia media, teniendo como porcentaje de pérdida del total de paquetes enviados alrededor de un 11% de pérdida de paquetes, y con respecto al resultado anterior se tiene una diferencia de porcentaje de alrededor de 4%.

La siguiente distancia con la cual se realizó la prueba fue de 7m, obteniendo los resultados de la tabla 17-3.

**Tabla 17-3** Tasa de Entrega de Red a 7m con Obstáculos

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 71 | 81.61 |
| **Vibración** | 87 | 70 | 80.46 |
| **Gases** | 87 | 73 | 83.91 |
| **Cerradura** | 87 | 72 | 82.76 |
| **Iluminación** | 87 | 71 | 81.61 |
| **Persiana** | 87 | 71 | 81.61 |
| **Alarma** | 87 | 70 | 80.46 |
| **Total** | **609** | **498** | **81.77** |

**Realizado por:** Vilañez, Daniel, 2019

Como se puede observar en la tabla 17-3 los nodos presentan una pérdida de paquetes que no supera el 20% de paquetes perdidos esto debido a que los nodos están separados del nodo

coordinador por una pared a una distancia medianamente considerable, teniendo como porcentaje de pérdida del total de paquetes enviados alrededor de un 19% de pérdida de paquetes, y con respecto al resultado anterior se tiene una diferencia de porcentaje de alrededor de 8%, empezando a presentar una pérdida considerable con respecto a las pruebas realizadas anteriores.

La última distancia con la cual se realizó la prueba fue de 9m, obteniendo los resultados de la tabla 18-3.

**Tabla 18-3** Tasa de Entrega de Red a 9m con Obstáculos

| Nodo | Paquetes Enviados | Paquetes Recibidos | Tasa de Entrega(%) |
|---|---|---|---|
| **Movimiento** | 87 | 64 | 73.56 |
| **Vibración** | 87 | 63 | 72.41 |
| **Gases** | 87 | 62 | 71.26 |
| **Cerradura** | 87 | 63 | 72.41 |
| **Iluminación** | 87 | 60 | 68.97 |
| **Persiana** | 87 | 61 | 70.11 |
| **Alarma** | 87 | 61 | 70.11 |
| **Total** | **609** | **434** | **71.26** |

**Realizado por:** Vilañez, Daniel, 2019

Como se puede observar en la tabla 18-3 los nodos presentan una pérdida de paquetes que no supera el 32% de paquetes perdidos esto debido a que los nodos están separados del nodo coordinador por una pared a una distancia considerable, teniendo como porcentaje de pérdida del total de paquetes enviados alrededor de un 29% de pérdida de paquetes, y con respecto al resultado anterior se tiene una diferencia de porcentaje de alrededor de 10%, siendo una pérdida considerable con respecto a las pruebas realizadas anteriores.

## 3.4. **Análisis Económico del Prototipo**

En la tabla 19-3 se presenta el análisis económico de la implementación de los nodos, con elementos adquiridos en nuestro país.

**Tabla 19-3** Costo del prototipo

| Componentes | Cantidad | Costo Unitario(USD) | Costo Total(USD) |
|---|---|---|---|
| Xbee S1 | 8 | 30 | 240 |
| Sensor de Movimiento PIR | 1 | 2.5 | 2.5 |
| Sensor de Gas MQ-4 | 1 | 5.5 | 5.5 |

| | | | |
|---|---|---|---|
| Sensor de Vibracion 801S | 1 | 2.5 | 2.5 |
| Cerradura Eléctrica | 1 | 90 | 90 |
| Foco | 1 | 1.25 | 1.25 |
| Cortina Enrollable | 1 | 17 | 17 |
| Alarma 110V | 1 | 20 | 20 |
| Contenedores | 8 | 5 | 40 |
| Regulador de Volatje LM2596 | 7 | 4 | 28 |
| Baquelita Perforada 9x15 | 8 | 2 | 16 |
| Arduino UNO | 1 | 10.5 | 10.5 |
| Adaptador para Xbee | 8 | 5 | 40 |
| Varios | - | - | 30 |
| Costo de Desarrollo | - | - | 100 |
| **Costo Total del Prototipo** | | | 643.25 |

**Fuente:** Mercado Libre Ecuador, 2019

**Realizado por:** Vilañez, Daniel, 2019

La empresa Domintell ofrece un servicio básico para un apartamento de 2 habitaciones con equipamiento estándar es cotizado en aproximadamente en $2460 sin incluir los costes de instalación ni el IVA. Por otro lado, la empresa Laarcom ofrece un kit básico de alarma el cual incluye: control de alarma, teclado, detector de movimiento, contacto magnético, sirena, instalación, mano de obra. El cual posee un precio de $236.00 sin incluir el IVA. La empresa Wattio ofrece un kit de seguridad que incluye: una centralita domótica de pantalla táctil, un sensor de movimiento y temperatura, sensor de apertura de puertas y ventanas y una sirena inteligente que podrás comandar desde el móvil, a un precio de $297. La empresa ISDE ofrece un servicio de sistema de seguridad, más el control de accesos y control remoto desde el celular, puede costar alrededor de $1500.

**Tabla 20-3** Comparativa Prototipo con Soluciones Comerciales

| **Comparativa Prototipo con Soluciones Comerciales** | | | | | |
|---|---|---|---|---|---|
| | **Domintell** | **Laarcom** | **Wattio** | **ISDE** | **Hkeeper** |
| **Unidades (Habitaciones)** | 2 | 2 | 2 | 2 | 2 |
| **Precio (USD)** | 2460 | 472 | 594 | 1500 | 1186.5 |

**Realizado por:** Vilañez, Daniel, 2019

Los resultados indican que construyendo un prototipo de sistema de seguridad doméstica basado en WPAN para una red IoT, un software que sirva para administrar la red y un servidor para el almacenamiento de la información, presenta un costo considerable. Pero al comparar con

soluciones comerciales que se ofertan actualmente se puede observar que el prototipo posee un precio estándar.

## CONCLUSIONES

- Al realizar el estudio de las características de las tecnologías más representativas del protocolo WPAN se determinó que la más adecuada para redes que se centren en domótica está ampliamente recomendada por la alianza Zigbee es la tecnología Xbee debido a que posee características como: bajo consumo de energía, bajo costo de los dispositivos, instalación y mantenimiento, alta densidad de nodos y trabaja sobre bandas ISM.

- El sistema se diseñó con los requerimientos establecidos: sencillo de instalar, intuitivo para el usuario, configurable, se supervisa por habitación, la comunicación se realiza en tiempo real, estable y los datos se almacenan constantemente en la base de datos. Construyendo una aplicación móvil y de escritorio para el monitoreo y administración de la red.

- El desarrollo de la aplicación móvil presenta una mejora en la interacción del usuario con la red, haciendo que pueda estar constantemente informado de las irregularidades que se presenten en su vivienda. Además, cuenta con el control de algunos dispositivos los cuales pueden ser accionados desde cualquier lugar en el que se encuentre.

- Se realizó la prueba de precisión de los sensores definiendo así que el sensor de movimiento trabaja de manera fluida cuando el valor de su potenciómetro se encuentra en el valor más alto, obteniendo porcentajes de detección de 74.71% a una distancia máxima de 9 metros. Así mismo, la prueba realizada al sensor de gas muestra que posee una imprecisión máxima de ±0.027 voltios al momento de detectar la presencia de GLP en el aire de una habitación.

- El tiempo de retardo en la transmisión, según el nodo, determinó un tiempo de 1.0223169 segundos en hacer que las acciones de los actuadores sucedan, y un retardo de comunicación entre nodos de 0.522372 segundos y la información sea almacenada, mientras que al momento de notificar al usuario con las alertas no se generó ningún retardo y de igual manera al momento de la actualización de las aplicaciones.

- La prueba de alerta del sistema muestra que la aplicación móvil en conjunto con la red trabaja de forma adecuada, de forma tal que cuando la información es subida a la base de datos el usuario es inmediatamente notificado, y de esta manera el usuario pueda tomar las medidas que crea necesarias.

## RECOMENDACIONES

- Incorporar otro tipo de sensores, como lo son sensores de consumo eléctrico o medidores de caudal para tener un completo control sobre las actividades de la vivienda y de esta manera reducir costos tanto en electricidad como en agua.

- Puesto que el sistema solo provee de una detección de intrusiones, se recomienda complementarlo con un sistema de video vigilancia para una mayor funcionalidad.

- Al tener alojada la base de datos en un servidor en la nube se recomienda que el sistema siempre debe tener una conexión a internet estable para así evitar una denegación de acceso a la información.

- Utilizar dispositivos Xbee de serie 2 debido a que posee un sistema de conexión con Arduino y entre sí mucho más fácil de implementar que los dispositivos de serie 1, además de presentar un mayor número de funcionalidades.

**BIBLIOGRAFÍA**


**ACOSTA, María.** Estudio Del Estándar IEEE 802.15.4 “ZIGBEE” Para Comunicaciones Inalambricas De Area Personal De Bajo Consumo De Energía Y Su Comparacion En El Estandar IEEE 802.15 "BLUETOOTH". Quito, Pichincha, Ecuador : Escuela Politécnica Nacional, 2006.

**AMAZON.** Amazon Web Services. *Amazon.* [En Línea] Amazon, 2018. [Citado El: 20 De Enero De 2019.] Https://Aws.Amazon.Com/Es/.

**ANTONY, Suica.** Redes WPAN. *Prezi.* [En Línea] 2013. [Citado El: 7 De Mayo De 2018.] Https://Prezi.Com/Kn2amgq26ney/Redes-Wpan/.

**ARCHUNDIA PAPACETZI, Martín Francisco.** Wireless Personal Area Network (WPAN) & Home Networking. *Udlap.* [En Línea] 16 De Diciembre De 2003. [Citado El: 25 De 08 De 2018.] Http://Catarina.Udlap.Mx/U_Dl_A/Tales/Documentos/Lem/Archundia_P_Fm/.

**ARDUINO.** Overview Arduino. *Tutorialspoint.* [En Línea] 2015. [Citado El: 13 De 2 De 2019.] Https://Www.Tutorialspoint.Com/Arduino/Arduino_Overview.Htm.

**ATMEL.** Zigbit™ 2.4 Ghz Amplified Wireless Modules. *Transfer Multisort Elektronik.* [En Línea] 2009. [Citado El: 21 De 11 De 2018.] Https://Www.Tme.Eu/Document/68df29044596c92b9afbeabc7dd07781/Atzb-A24-Ufl_U0.Pdf.

**BARR, John.** IEEE 802.15.3 Overview. *Ieee802.* [En Línea] 2002. [Citado El: 28 De 9 De 2018.] Http://Www.Wimedia.Org/Events/Docs/02006r0wm_PUB-GEN05_802.15.3_Overview_Wimedia_Oct_2002.Pdf.

**BETANCOURT, Diana Y GÓMEZ, Germán.** Prototipo De Sistema De Vigilancia Basado En La Internet De Las Cosas Con Aplicativo Para Dispositivos Móviles. *Udistrital.* [En Línea] 2015. [Citado El: 15 De 8 De 2018.] Http://Repository.Udistrital.Edu.Co/Bitstream/11349/2918/1/PROTOTIPO%20DE%20SISTEMA%20DE%20VIGILANCIA%20BASADO%20EN%20LA%20INTERNET%20DE%20LAS%20COSAS%20CON%20APLICATIVO%20PARA%20DISPOSI.Pdf.

**BREA, Victor.** Internet De Las Cosas. Horizonte 2050. *IEEE.* [En Línea] 2018. [Citado El: 10 De Junio De 2019.] Http://Www.Ieee.Es/Galerias/Fichero/Docs_Investig/2018/DIEEEINV17-2018_Internet_De_Las_Cosas_Horizonte_2050.Pdf.

**CAMARGO OLIVARES, José Luis.** Modelo De Cobertura Para Redes Inalámbricas De Interiores. Sevilla, España : Universidad De Sevilla, Mayo De 2009.

**CASCO, Nico.** Beneficios De Iot En La Práctica. *Mundocontact.* [En Línea] 18 De 06 De 2015. [Citado El: 15 De 3 De 2019.] Https://Mundocontact.Com/Beneficios-De-Iot-En-La-Practica/.

**Cei1.** Técnicas Y Procesos De Instalaciones Singulares - Sistemas De Seguridad. *Scribd.* [En Línea] 2016. [Citado El: 12 De 10 De 2018.] Https://Es.Scribd.Com/Document/247405489/SISTEMAS-DE-SEGURIDAD1.

**CENDÓN, Bruno.** El Origen Del Iot. [En Línea] 2017. [Citado El: 30 De Mayo De 2019.] Http://Www.Bcendon.Com/El-Origen-Del-Iot/.

**CENDON, Bruno.** Los 5 Grandes Retos Del Iot. [En Línea] 2017. [Citado El: 30 De Mayo De 2019.] Http://Www.Bcendon.Com/Los-5-Retos-Del-Iot/.

**COLEY, Gerald Y DAY, Robert.** Beaglebone Black System Reference Manual. *Adafruit.* [En Línea] 11 De Abril De 2013. [Citado El: 12 De 04 De 2019.] Https://Cdn-Shop.Adafruit.Com/Datasheets/BBB_SRM.Pdf.

**DIGI.** DIGI XBEE S1 802.15.4 RF Modules. *Digi.* [En Línea] 2018. [Citado El: 12 De 10 De 2018.] Https://Www.Digi.Com/Pdf/Ds_Xbeemultipointmodules.Pdf.

**DIGI INTERNATIONAL Inc.** Overview XCTU. *Digi.* [En Línea] Digi, 2017. [Citado El: 24 De 11 De 2018.] Https://Www.Digi.Com/Resources/Documentation/Digidocs/90001496/Concepts/C_Xbee_Application_Structure.Htm?Tocpath=Additional%20resources%7CXCTU%20walkthrough%7C_____1.

**EVANS, Dave.** Internet De Las Cosas Cómo La Próxima Evolución De Internet Lo Cambia Todo. *Cisco.* [En Línea] 4 De 2011. [Citado El: 23 De 02 De 2019.] Https://S3.Amazonaws.Com/Academia.Edu.Documents/34766160/Internet-Of-Things-Iot-Ibsg.Pdf?Awsaccesskeyid=AKIAIWOWYYGZ2Y53UL3A&Expires=1533313447&Signature=

E%2blhnfvmbciykv%2fzcsvay6oxz3y%3D&Response-Content-Disposition=Inline%3B%20filename%3dinternet-Of-Th.

**GOOGLE.** Google Cloud Platform. *Google.* [En Línea] 2018. [Citado El: 20 De Enero De 2019.] Https://Cloud.Google.Com.

**GORMAZ, Isidoro.** *Técnicas Y Procesos En Las Instalaciones Singulares En Los Edificios.* 2. Madrid : S.A. Ediciones Paraninfo, 2007. Pág. 424. 8497320522, 9788497320528.

**VEGA, Adriana, SANTAMARIA, Francisco Y RIVAS, Edwin.** *Internet De Los Objetos Empleando Arduino Para La Gestión Eléctrica Domiciliaria.* 77, S.L. : Revista EAN, 2014, Revista EAN, Vol. 1, Págs. 22-41. ISSN 0120-8160.

**IOT MÁSTER.** Origen E Historia Del Internet Of Things. *Master-Internet-Of-Things.* [En Línea] 2017. [Citado El: 13 De 5 De 2019.] Https://Www.Master-Internet-Of-Things.Com/Historia-Iot/.

**JURADO, Marco Y CÁCERES, Wagner.** Sistema De Automatización De Luces Y Persianas En Casas Residenciales Utilizando Módulos Infrarrojos Para Mejorar El Estilo De Vida De Personas Con Discapacidad Física En Extremidades Inferiores. Ambato, Ecuador : Universidad Técnica De Ambato, 2011.

**LAN/MAN STANDARDS COMMITTEE OF THE IEEE COMPUTER SOCIETY.** IEEE. *IEEE.* [En Línea] 2002. [Citado El: 22 De 11 De 2018.] Http://Www.Ieee802.Org/.

**CAMA, Alejandro, HOZ, Emiro De La Y CAMA, Dora.** *Las Redes De Sensores Inalámbricos Y El Internet De Las Cosas.* 1, Bogotá-Colombia : Revista INGE CUC, 2012, Vol. 8.

**LONDOÑO, Roby.** INTERNET DE LAS COSAS. *Umanizales.* [En Línea] 2016. [Citado El: 29 De 1 De 2019.] Http://Ridum.Umanizales.Edu.Co:8080/Xmlui/Bitstream/Handle/6789/2916/Informe%20final%20monografia.Pdf?Sequence=1&Isallowed=Y.

**LOUBET, Gaël, TAKACS, Alexandru Y DRAGOMIRESCU, Daniela.** Towards The Design Of Wireless Communicating Reinforced Concrete. *IEEE.* [En Línea] 27 De 11 De 2018. [Citado El: 9 De 2 De 2019.] Https://Ieeexplore.Ieee.Org/Document/8546738.

**MARTÍNEZ, César.** Protege Tu Casa Con Un Sistema De Seguridad. [En Línea] 5 De 7 De 2012. [Citado El: 10 De 9 De 2018.] Http://Www.Metroscubicos.Com/Articulo/Decoracion-Y-Hogar/2012/06/14/Protege-Tu-Casa-Con-Un-Sistema-De-Seguridad.

**TRUJILLO, Diana Y CALDERÓN, Oscar.** *Metodología Para La Implementación De La Tecnología Identificación Por Radiofrecuencia En Entornos Industriales Y Sanitarios En Colombia.* 1, Popayán-Colombia : Universidad Del Quindío, 2014, Revista De Investigaciones, Vol. 25, Págs. 46-52.

**MICROCHIP.** MRF24J40 Datasheet. *Alldatasheet.* [En Línea] 2006. [Citado El: 15 De 10 De 2018.] Http://Www.Alldatasheet.Com/Datasheet-Pdf/Pdf/199133/MICROCHIP/MRF24J40.Html.

**MICROSOFT.** Microsoft Azure. *Microsoft.* [En Línea] Microsoft, 2018. [Citado El: 20 De Enero De 2019.] Https://Azure.Microsoft.Com/Es-Es/.

**MORENO, Javier Y RUIZ, Daniel.** Informe Técnico: Protocolo Zigbee (IEEE 802.15.4). *UA.* [En Línea] 6 De 2007. [Citado El: 4 De Mayo De 2018.] Https://Rua.Ua.Es/Dspace/Bitstream/10045/1109/7/Informe_Zigbee.Pdf.

**ORTRAT.** Detección De Gases-Grandes Cocinas. *Ortrat.* [En Línea] 2014. [Citado El: 23 De 02 De 2019.] Http://Www.Ortrat.Es/Documentos/Productos/(DETECCI%C3%93N%20DE%20GASES).Pdf.

**PEÑA, Janneth Y SUQUILLO, Geovanna.** Estudio Del Modelo De Referencia Del Internet De Las Cosas (Iot), Con La Implementación De Un Prototipo Domótico. Quito : EPN, 2016.

**PÉREZ, Juan, URDANETA, Elizabeth Y CUSTODIO, Ángel.** Metodología Para El Diseño De Una Red De Sensores Inalámbricos. *Scielo.* [En Línea] 3 De 2014. [Citado El: 19 De 6 De 2018.] Http://Www.Scielo.Org.Ve/Pdf/Uct/V18n70/Art02.Pdf.

**PICKERS, Simeon.** ¿Cómo Determinar El Tamaño De Una Muestra? *Psyma.* [En Línea] 11 De 04 De 2015. [Citado El: 29 De 3 De 2019.] Https://Www..Com/Company/News/Message/Como-Determinar-El-Tamano-De-Una-Muestra.

**PRIETO, Josep.** Introduccion A Los Sistemas De Comunicacion Inalambricos. *Exabyteinformatica.* [En Línea] 9 De 2011. [Citado El: 20 De 8 De 2018.]

Https://Www.Exabyteinformatica.Com/Uoc/Informatica/Tecnologia_Y_Desarrollo_En_Dispositivos_Moviles/Tecnologia_Y_Desarrollo_En_Dispositivos_Moviles_(Modulo_1).Pdf.

**QUESTIONPRO.** Questionpro. [En Línea] 2015. [Citado El: 10 De Diciembre De 2018.] Https://Www.Questionpro.Com/Blog/Es/Que-Es-La-Escala-De-Likert-Y-Como-Utilizarla/.

**RASPBERRY PI FOUNDATION.** Raspberry Pi 3 Model B+. *Hardzone.* [En Línea] Hardzone, 2017. [Citado El: 24 De 1 De 2019.] Https://Hardzone.Es/Reviews/Perifericos/Analisis-Raspberry-Pi-3-Modelo-B/.

**AAKVAAG, Niels Y FREY, Jan-Erik.** *Redes De Sensores Inalámbricos.* 2, Madrid : Revista ABB 2, 2006, Vol. 1, Págs. 39-42. ISSN 1013-3135.

**ROBALINO, Irma.** Estudio De Los Sistemas WEB Embebidos Y Su Aplicación En Un Sistema De Control Domótico Con Microcontroladores. Riobamba, Ecuador : Escuela Superior Politécnica De Chimborazo, 2010.

**RODRÍGUEZ SAUCEDO, César Iván.** Eficiencia Y Seguridad En Bluetooth Y Zigbee. [En Línea] 29 De 2 De 2012. [Citado El: 28 De 6 De 2018.] Http://132.248.52.100:8080/Xmlui/Handle/132.248.52.100/229.

**AGUILAR, Luis, DELGADO, John Y GARCÍA, Pablo.** *Seguridad En Internet De Las Cosas.* 10, S.L. : Perspectiv@S, 2017, Perspectiv@S, Vol. 10, Págs. 3-10. ISSN 1996-1952.

**SUICA, Antony.** Redes WPAN. *Prezi.* [En Línea] 2013. [Citado El: 7 De Mayo De 2018.] Https://Prezi.Com/Kn2amgq26ney/Redes-Wpan/.

**TARRÍO, Alonso.** Redes De Sensores. *Upm.* [En Línea] 2008. [Citado El: 13 De 10 De 2018.] Http://Oa.Upm.Es/7342/1/Paula__Tarrio_Alonso.Pdf.

**TEXAS INSTRUMENTS.** 6-Pin DIP Random-Phase Optoisolators Triac Driver Output. *Texas Instruments.* [En Línea] Texas Instruments, 1995. [Citado El: 26 De 1 De 2019.] Https://Www.Alldatasheet.Com/Datasheet-Pdf/Pdf/27236/TI/MOC3021.Html.

**VENEGAS, Diego Y AYABACA, César.** Instalaciones De Gas Licuado De Petróleo Para Sistemas Residenciales, Comerciales E Industriales. *Researchgate.* [En Línea] 2017. [Citado El: 13 De 3 De 2019.]

Https://Www.Researchgate.Net/Publication/318776409_Instalaciones_De_Gas_Licuado_De_Petroleo.

**ROGELIO, Avilés.** *Ventajas De La Tecnología Near Field Communication (NFC) Como Sistema De Pago Electrónico.* 10, S.L. : Reci Revista Iberoaméricana De Las Ciencias Computacionales E Informáticas, 2016, Reci Revista Iberoaméricana De Las Ciencias Computacionales E Informáticas, Vol. 5, Págs. 135-146. ISSN: 2007-9915.

**VERMESAN, Ovidiu Y BACKQUET., Joël.** Cognitive Hyperconnected Digital Transformation: Internet Of Things Intelligence Evolution. *Internet-Of-Things-Research.* [En Línea] 2017. [Citado El: 10 De Junio De 2019.] Http://Www.Internet-Of-Things-Research.Eu/Pdf/Cognitive_Hyperconnected_Digital_Transformation_IERC_2017_Cluster_Ebook_978-87-93609-10-5_P_Web.Pdf.

**VERMESAN, Ovidiu, Y Otros.** The Next Generation Internet Of Things-Hyperconectivity And Embedded Intelligence Of The Edge. *Internet-Of-Things-Research.* [En Línea] 2018. [Citado El: 10 De Junio De 2019.] Http://Www.Internet-Of-Things-Research.Eu/Pdf/The_Next_Generation_Iot_Hyperconnectivity_And_Embedded_Intelligence_At_The_Edge_Research_Trends_IERC_2018_Cluster_Ebook_978-87-7022-007-1_P_Web.Pdf.

**VITERI, Fernando.** Diseño De Un Modelo Estándar De Domótica Para Hogares Digitales Basado En La Tecnología INSTEON. Quito : PUCE, 2013.

**ZANELLA, Andrea, Y Otros.** Internet Of Things For Smart Cities. *IEEE.* [En Línea] 2 De 2014. [Citado El: 9 De Junio De 2019.] Https://Ieeexplore.Ieee.Org/Document/6740844.

**ZENNARO, Marco.** Introducción A Las Redes. *Academia.* [En Línea] 10 De 2010. [Citado El: 23 De 7 De 2018.] Https://Www.Academia.Edu/2236615/Introduction_To_Wireless_Sensor_Networks.

**ZIGBEE Alliance.** Zigbee Alliance. *Zigbee* . [En Línea] 2002. [Citado El: 26 De 03 De 2019.] Https://Www.Zigbee.Org/.

**ANEXOS**

**ANEXO A.** CODIGO DE PROGRAMACION APLICACION DE ESCRITORIO

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Text;
using System.Windows.Forms;
using System.IO.Ports;
using comunicacion_arduino.Properties;
using System.Data.SqlClient;

namespace comunicacion_arduino
{
   public partial class Form1 : Form

   {
      public string con = @"data
source=dbtesisdv.database.windows.net;initial
catalog=TesisDV;user
id=d4lk13lD;password=n4m3l3ssD;Connect
Timeout=60";

      public Form1()
      {
         InitializeComponent();

Control.CheckForIllegalCrossThreadCalls =
false;
      }

      private void puertosDisponibles()
      {
         foreach (string puertoDis in
System.IO.Ports.SerialPort.GetPortNames())
         {
            cmbPuertos.Items.Add(puertoDis);
         }
      }


      private void LecturaDatos(string hab)
      {

         var listView = new ListView();
         DataTable dt = new DataTable();
         string con = Conexion.cadenaConexion;
         string sql = "SELECT cerradura,
iluminacion, rociador, persiana, humo, movim,
alarma, vibrac, temp FROM Datos WHERE
habitacion ='"+hab+"'";
         SqlConnection sqlConn = new
SqlConnection(con);
         SqlCommand comando = new
SqlCommand(sql, sqlConn);
         SqlDataAdapter adap = new
SqlDataAdapter(comando);
         adap.Fill(dt);

         DataRow row = dt.Rows[0];

         c = Convert.ToString(row["cerradura"]);
         i =
Convert.ToString(row["iluminacion"]);
         r = Convert.ToString(row["rociador"]);
         p = Convert.ToString(row["persiana"]);
         h = Convert.ToString(row["humo"]);
         m = Convert.ToString(row["movim"]);
         a = Convert.ToString(row["alarma"]);
         v = Convert.ToString(row["vibrac"]);
         t = Convert.ToString(row["temp"]);

      }
```

```
      private void
serialPort1_DataReceived(object sender,
SerialDataReceivedEventArgs e)
      {
         string datorx = serialPort1.ReadLine();
         string dato;

         if (datorx=="mov=1\r")
         {
            string sql = "UPDATE Datos SET
Movim = 1 WHERE habitacion = 'Dormitorio'";

            SqlConnection sqlConn = new
SqlConnection(Conexion.cadenaConexion);
            sqlConn.Open();
            SqlCommand comando = new
SqlCommand(sql, sqlConn);
            comando.CommandType =
System.Data.CommandType.Text;
            comando.ExecuteNonQuery();
            sqlConn.Close();

         }
         else if (datorx == "mov=0\r")
         {
            string sql = "UPDATE Datos SET
Movim = 0 WHERE habitacion = 'Dormitorio'";

            SqlConnection sqlConn = new
SqlConnection(Conexion.cadenaConexion);
            sqlConn.Open();
            SqlCommand comando = new
SqlCommand(sql, sqlConn);
            comando.CommandType =
System.Data.CommandType.Text;
            comando.ExecuteNonQuery();
            sqlConn.Close();

         }
         dato = datorx.Substring(0,3);

         if (dato == "hum")
         {

            string sql = "UPDATE Datos SET
temp = '"+ datorx.Substring(4) + "' WHERE
habitacion = 'Dormitorio'";

            SqlConnection sqlConn = new
SqlConnection(Conexion.cadenaConexion);
            sqlConn.Open();
            SqlCommand comando = new
SqlCommand(sql, sqlConn);
            comando.CommandType =
System.Data.CommandType.Text;
            comando.ExecuteNonQuery();
            sqlConn.Close();

         }

         var listView = new ListView();
         DataTable dt = new DataTable();
         string con = Conexion.cadenaConexion;
         string sqlb = "SELECT * FROM Datos
WHERE Habitacion ='Dormitorio'";
         SqlConnection sqlConnb = new
SqlConnection(con);
         SqlCommand comandob = new
SqlCommand(sqlb, sqlConnb);
         SqlDataAdapter adap = new
SqlDataAdapter(comandob);
         adap.Fill(dt);
         if (dt.Rows.Count > 0)
         {
            DataRow row = dt.Rows[0];

      cerr = Convert.ToString(row["Cerradura"]);
      ilu = Convert.ToString(row["Iluminacion"]);
      roc = Convert.ToString(row["Rociador"]);
```

```
    per = Convert.ToString(row["Persiana"]);
    alar = Convert.ToString(row["Alarma"]);
        }
    }

    private void button1_Click(object sender,
EventArgs e)
    {
        hab = comboBox1.Text;
        LecturaDatos(hab);
        int length = h.Length-2;
    }

    private void NC_CheckedChanged(object
sender, EventArgs e)
    {
        string sql = "UPDATE Datos SET
cerradura = 1 WHERE habitacion = '"+hab+"';";
        SqlConnection sqlConn = new
SqlConnection(con);
        sqlConn.Open();
        SqlCommand comando = new
SqlCommand(sql, sqlConn);
        comando.CommandType =
CommandType.Text;
        comando.ExecuteNonQuery();
        sqlConn.Close();
    }

    private void FC_CheckedChanged(object
sender, EventArgs e)
    {
        string sql = "UPDATE Datos SET
cerradura = 0 WHERE habitacion = '"+hab+"';";
        SqlConnection sqlConn = new
SqlConnection(con);
        sqlConn.Open();
        SqlCommand comando = new
SqlCommand(sql, sqlConn);
        comando.CommandType =
CommandType.Text;
        comando.ExecuteNonQuery();
        sqlConn.Close();
    }

    private void NI_CheckedChanged(object
sender, EventArgs e)
    {
        string sql = "UPDATE Datos SET
iluminacion = 1 WHERE habitacion = '" + hab
+ "';";
        SqlConnection sqlConn = new
SqlConnection(con);
        sqlConn.Open();
        SqlCommand comando = new
SqlCommand(sql, sqlConn);
        comando.CommandType =
CommandType.Text;
        comando.ExecuteNonQuery();
        sqlConn.Close();
    }

    private void FI_CheckedChanged(object
sender, EventArgs e)
    {
        string sql = "UPDATE Datos SET
iluminacion = 0 WHERE habitacion = '" + hab
+ "';";
        SqlConnection sqlConn = new
SqlConnection(con);
        sqlConn.Open();
        SqlCommand comando = new
SqlCommand(sql, sqlConn);
        comando.CommandType =
CommandType.Text;
        comando.ExecuteNonQuery();
        sqlConn.Close();
    }
```

```
        private void NR_CheckedChanged(object
sender, EventArgs e)
        {
            string sql = "UPDATE Datos SET
rociador = 1 WHERE habitacion = '" + hab +
"';";
            SqlConnection sqlConn = new
SqlConnection(con);
            sqlConn.Open();
            SqlCommand comando = new
SqlCommand(sql, sqlConn);
            comando.CommandType =
CommandType.Text;
            comando.ExecuteNonQuery();
            sqlConn.Close();
        }

        private void FR_CheckedChanged(object
sender, EventArgs e)
        {
            string sql = "UPDATE Datos SET
rociador = 0 WHERE habitacion = '" + hab +
"';";
            SqlConnection sqlConn = new
SqlConnection(con);
            sqlConn.Open();
            SqlCommand comando = new
SqlCommand(sql, sqlConn);
            comando.CommandType =
CommandType.Text;
            comando.ExecuteNonQuery();
            sqlConn.Close();
        }

        private void NA_CheckedChanged(object
sender, EventArgs e)
        {
            string sql = "UPDATE Datos SET
alarma = 1 WHERE habitacion = '" + hab + "';";
            SqlConnection sqlConn = new
SqlConnection(con);
            sqlConn.Open();
            SqlCommand comando = new
SqlCommand(sql, sqlConn);
            comando.CommandType =
CommandType.Text;
            comando.ExecuteNonQuery();
            sqlConn.Close();
        }

        private void FA_CheckedChanged(object
sender, EventArgs e)
        {
            string sql = "UPDATE Datos SET
alarma = 0 WHERE habitacion = '" + hab + "';";
            SqlConnection sqlConn = new
SqlConnection(con);
            sqlConn.Open();
            SqlCommand comando = new
SqlCommand(sql, sqlConn);
            comando.CommandType =
CommandType.Text;
            comando.ExecuteNonQuery();
            sqlConn.Close();
        }

        private void tbp_Scroll(object sender,
EventArgs e)
        {
            int value = tbp.Value;
            string sql = "UPDATE Datos SET
persiana = " + value + " WHERE habitacion =
'"+hab+"';";
            SqlConnection sqlConn = new
SqlConnection(con);
            sqlConn.Open();
            SqlCommand comando = new
SqlCommand(sql, sqlConn);
```

```
            comando.CommandType =
CommandType.Text;
            comando.ExecuteNonQuery();
            sqlConn.Close();
        }

        private void
comboBox2_SelectedIndexChanged(object
sender, EventArgs e)
        {
            serialPort1.PortName =
cmbPuertos.Text;
            cmbPuertos.Enabled = false;
            try
            {
                serialPort1.Open();
            }
            catch (Exception ex)
            {
                MessageBox.Show("Selecciones otro
puerto", "Puerto no disponible");
                cmbPuertos.Enabled = true;
            }
        }

        private void Form1_Load(object sender,
EventArgs e)
        {
            puertosDisponibles();
        }

        private void Form1_FormClosing(object
sender, FormClosingEventArgs e)
        {
            serialPort1.Close();
        }
    }
}
```

**ANEXO B.** CODIGO DE PROGRAMACION APLICACION MÓVIL

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using Xamarin.Forms;
using Xamarin.Forms.Xaml;
using System.Data;
using System.Data.SqlClient;
namespace Hkeeper
{
[XamlCompilation(XamlCompilationOptions.C
ompile)]
public partial class Habitacion : ContentPage
        {
    public Habitacion ()
        {
      InitializeComponent ();
      LecturaDatos();
    }
    private void LecturaDatos()
    {
var listView = new ListView();
DataTable dt = new DataTable();
string con = Conexion.cadenaConexion;
string sql = "SELECT cerradura, iluminacion,
rociador, persiana, humo, movim, alarma,
vibrac, temp FROM Datos WHERE habitacion
='dormitorio'";
SqlConnection sqlConn = new
SqlConnection(con);
SqlCommand comando = new
SqlCommand(sql, sqlConn);
SqlDataAdapter adap = new
SqlDataAdapter(comando);
adap.Fill(dt);
DataRow row = dt.Rows[0];
c = Convert.ToString(row["cerradura"]);
i = Convert.ToString(row["iluminacion"]);
r = Convert.ToString(row["rociador"]);
p = Convert.ToString(row["persiana"]);
h = Convert.ToString(row["humo"]);
m = Convert.ToString(row["movim"]);
a = Convert.ToString(row["alarma"]);
v = Convert.ToString(row["vibrac"]);
t = Convert.ToString(row["temp"]);
    }
private void SWroc_Toggled(object sender,
ToggledEventArgs e)
    {
int on = 1;
int off = 0;
LecturaDatos();
string con = @"data
source=dbtesisdv.database.windows.net;initial
catalog=TesisDV;user
id=d4lk13lD;password=n4m3l3ssD;Connect
Timeout=60";

if (r == "1")
        {
string sql = "UPDATE Datos SET rociador = "
+ off + " WHERE habitacion = 'dormitorio';";
SqlConnection sqlConn = new
SqlConnection(con);
sqlConn.Open();
SqlCommand comando = new
SqlCommand(sql, sqlConn);
comando.CommandType =
CommandType.Text;
comando.ExecuteNonQuery();
sqlConn.Close();
        }
        else
        {
```

```
string sql = "UPDATE Datos SET rociador = "
+ on + " WHERE habitacion = 'dormitorio';";
SqlConnection sqlConn = new
SqlConnection(con);
sqlConn.Open();
SqlCommand comando = new
SqlCommand(sql, sqlConn);
comando.CommandType =
CommandType.Text;
comando.ExecuteNonQuery();
            sqlConn.Close();
        }
    }

private void SWalar_Toggled(object sender,
ToggledEventArgs e)
    {
int on = 1;
int off = 0;
LecturaDatos();
string con = @"data
source=dbtesisdv.database.windows.net;initial
catalog=TesisDV;user
id=d4lk13lD;password=n4m3l3ssD;Connect
Timeout=60";

if (a == "1")
        {
string sql = "UPDATE Datos SET alarma = " +
off + " WHERE habitacion = 'dormitorio';";
SqlConnection sqlConn = new
SqlConnection(con);
sqlConn.Open();
SqlCommand comando = new
SqlCommand(sql, sqlConn);
comando.CommandType =
CommandType.Text;
comando.ExecuteNonQuery();
sqlConn.Close();
        }
        else
        {
string sql = "UPDATE Datos SET alarma = " +
on + " WHERE habitacion = 'dormitorio';";
SqlConnection sqlConn = new
SqlConnection(con);
sqlConn.Open();
SqlCommand comando = new
SqlCommand(sql, sqlConn);
comando.CommandType =
CommandType.Text;
comando.ExecuteNonQuery();
sqlConn.Close();
        }
    }
private void SWcerr_Toggled(object sender,
ToggledEventArgs e)
    {
int on = 1;
int off = 0;
LecturaDatos();
string con = @"data
source=dbtesisdv.database.windows.net;initial
catalog=TesisDV;user
id=d4lk13lD;password=n4m3l3ssD;Connect
Timeout=60";
if (c == "1")
        {
string sql = "UPDATE Datos SET cerradura = "
+ off + " WHERE habitacion = 'dormitorio';";
SqlConnection sqlConn = new
SqlConnection(con);
sqlConn.Open();
SqlCommand comando = new
SqlCommand(sql, sqlConn);
comando.CommandType =
CommandType.Text;
comando.ExecuteNonQuery();
sqlConn.Close();
        }
```

```
            else
            {
string sql = "UPDATE Datos SET cerradura = "
+ on + " WHERE habitacion = 'dormitorio';";
                SqlConnection sqlConn = new
SqlConnection(con);
sqlConn.Open();
SqlCommand comando = new
SqlCommand(sql, sqlConn);
comando.CommandType =
CommandType.Text;
comando.ExecuteNonQuery();
sqlConn.Close();
            }
        }
private void SWluz_Toggled(object sender,
ToggledEventArgs e)
        {
            int on = 1;
            int off = 0;
            LecturaDatos();
string con = @"data
source=dbtesisdv.database.windows.net;initial
catalog=TesisDV;user
id=d4lk13lD;password=n4m3l3ssD;Connect
Timeout=60";
            if (i == "1")
            {
string sql = "UPDATE Datos SET iluminacion
= " + off + " WHERE habitacion =
'dormitorio';";
SqlConnection sqlConn = new
SqlConnection(con);
sqlConn.Open();
SqlCommand comando = new
SqlCommand(sql, sqlConn);
comando.CommandType =
CommandType.Text;
comando.ExecuteNonQuery();
sqlConn.Close();
            }
            else
            {
string sql = "UPDATE Datos SET iluminacion
= " + on + " WHERE habitacion =
'dormitorio';";
SqlConnection sqlConn = new
SqlConnection(con);
sqlConn.Open();
SqlCommand comando = new
SqlCommand(sql, sqlConn);
comando.CommandType =
CommandType.Text;
comando.ExecuteNonQuery();
sqlConn.Close();
            }
        }
void OnSliderValueChanged(object sender,
ValueChangedEventArgs args)
        {
double value = args.NewValue;
string con = @"data
source=dbtesisdv.database.windows.net;initial
catalog=TesisDV;user
id=d4lk13lD;password=n4m3l3ssD;Connect
Timeout=60";
string sql = "UPDATE Datos SET persiana = "
+ value + " WHERE habitacion = 'dormitorio';";
SqlConnection sqlConn = new
SqlConnection(con);
sqlConn.Open();
SqlCommand comando = new
SqlCommand(sql, sqlConn);
comando.CommandType =
CommandType.Text;
comando.ExecuteNonQuery();
sqlConn.Close();
        }
    }
}
```

**ANEXO C.** CODIGO DE PROGRAMACION ARDUINO

```
#include <SoftwareSerial.h>
const int act1 = 6;
const int act2 = 7;
const int act3 = 8;
const int act4 = 9;
const int act5 = 10;
int r;

int MSBdig;
int LSBdig;
int MSBana;
int LSBana;
int p;
int i;
int m;
int h;
byte discardByte;
SoftwareSerial Xbee(4,5);
void setup ()
{
  Serial.begin(9600);
  Xbee.begin(9600);
  pinMode(act1 , OUTPUT);
  pinMode(act2 , OUTPUT);
  pinMode(act3 , OUTPUT);
  pinMode(act4 , OUTPUT);
  pinMode(act5 , OUTPUT);
}
void loop()
{
  if(Xbee.available()>=21)
  {
    if(Xbee.read()==0x7E)
    {
    for (i = 1; i<4; i++)
    {
    discardByte = Xbee.read();
    }
    p = Xbee.read();
    if(p==0xDE)
    {
    for (i = 1; i<7; i++)
    {
    discardByte = Xbee.read();
    }
     MSBdig = Xbee.read(); //
     LSBdig = Xbee.read(); //
     if (LSBdig==0){
      Serial.println("mov=0") ;
      delay(500);
     }
     else{
      Serial.println("mov=1") ;
      delay(500);
     }
     }
     else if(p==0xAB)
    {
    for (int i = 1; i<7; i++)
    {
    discardByte = Xbee.read();
    }
     MSBana = Xbee.read(); //
     LSBana = Xbee.read(); //
     float suma = (MSBana+LSBana);
      Serial.print("gas=") ;
      Serial.println(suma) ;
      delay(500);
    }
}
}
r=Serial.read();
  if (r == 'C')
  {
 digitalWrite(act1 , HIGH);
  }
```

```
 if (r == 'I')
 {
digitalWrite(act2 , HIGH);
 }
 if (r == 'R')
 {
digitalWrite(act3 , HIGH);
 }
 if (r == 'P')
 {
digitalWrite(act4 , HIGH);
 }
 if (r == 'A')
 {
digitalWrite(act5 , HIGH);
 }
 if (r == 'c')
 {
digitalWrite(act1 , LOW);
 }
 if (r == 'i')
 {
digitalWrite(act2 , LOW);
 }
 if (r == 'r')
 {
digitalWrite(act3 , LOW);
 }
 if (r == 'p')
 {
digitalWrite(act4 , LOW);
 }
 if (r == 'a')
 {
 digitalWrite(act5 , LOW);
 }
}
```