ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRONICA

ESCUELA DE INGENIERIA EN ELECTRONICA, TELECOMUNICACIONES Y REDES

"DESARROLLO DE UN PROTOTIPO DE ALARMA MULTIMODAL COMUNITARIA UTILIZANDO EL PROTOCOLO IPV6 Y GPRS PARA SMART CITIES CON MONITOREO EN TIEMPO REAL."

Trabajo de titulación presentado para optar al grado académico de:

INGENIERO EN ELECTRONICA, TELECOMUNICACIONES Y REDES

AUTOR: FREDDY RENÉ AGUILAR VILLALBA

TUTOR: ING. OSWALDO MARTÍNEZ

Riobamba – Ecuador

2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRÓNICA

ESCUELA DE INGENIERIA EN ELECTRONICA TELECOMUNICACIONES Y REDES

El Tribunal del Proyecto de Titulación certifica que el: "**DESARROLLO DE UN PROTOTIPO DE ALARMA MULTIMODAL COMUNITARIA UTILIZANDO EL PROTOCOLO IPV6 Y GPRS PARA SMART CITIES CON MONITORE EN TIEMPO REAL"**, de responsabilidad del Señor Freddy René Aguilar Villalba, ha sido minuciosamente revisado por los Miembros del Tribunal del Proyecto de Titulación, quedando autorizada su presentación.

Ing. Washington Luna	_____	_____
DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA		
Ing. Franklin Moreno	_____	_____
DIRECTOR DE LA ESCUELA DE INGENIERÍA ELECTRÓNICA, TELECOMUNICACIONES Y REDES		
Ing. Oswaldo Martínez	_____	_____
DIRECTOR DEL TRABAJO DE TITULACIÓN		
Ing. Wilson Zúñiga	_____	_____
MIEMBRO DEL TRIBUNAL		

Yo, Freddy René Aguilar Villalba soy responsable de las ideas, doctrinas y resultados expuestos en este trabajo; y, el patrimonio intelectual del Trabajo de Titulación pertenece a la Escuela Superior Politécnica de Chimborazo.

Freddy

AGRADECIMIENTO

Agradezco a la Virgen de Guadalupe, a mi familia por su apoyo incondicional en todo momento de mi formación como profesional, a todas las personas que colaboraron con la realización de este trabajo de titulación y un agradecimiento especial al Ing. Oswaldo Martínez por su invaluable ayuda y guía profesional, a todas muchas gracias por su aporte.

Freddy

DEDICATORIA

Este trabajo está dedicado:

A la Virgen de Guadalupe por haberme dado todas las fuerzas para no rendirme en este difícil camino.

A mi madre Elizabeth por su amor, sacrificio y su incomparable apoyo cuando más lo necesité.

A mi padre Fredy por su ejemplo de perseverancia, por sus consejos y su enorme sacrificio para que no me faltara nada en mi formación académica y humana.

A mis hermanos Jhonny y Karolina por su ayuda incondicional, sus palabras de ánimo en momentos precisos y por ser los mejores hermanos.

A mí enamorada Kassandra que por muchos días y meses fue mi compañera, mi amiga, mi consejera, y mi complemento, te agradezco de la manera más sincera, e infinita por tus ayudas e incontables apoyos para mi vida.

A todos mis familiares que estuvieron pendientes de mi formación académica y personal, en especial a Mamá Laurita, tía Fanny, tío Franklin, tío Milton, tía Anita.

A la memoria de mis abuelitos: Abuelita Elsa y Papá Vicente.

Finalmente a todas las personas que he conocido en esta etapa de mi vida: c4sant, alejos0304, Mogo, Francisco, Fender, @np@, cpmch, Byron, Alexis, Dante, Killer, Harles, Asassin, Fusilero, Yogo, Resurrection, Assault, P@lermo, Latino LordPark, Jefos, Vaca, Jepo, Jagger, Ck, Chava, Legion, Rex.

Freddy Aguilar

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Se desarrollo un prototipo de alarma multimodal comunitaria utilizando el protocolo IPv6 y GPRS para Smart Cities con monitoreo en tiempo real, el prototipo implementado establece la situación real de un sistema de alarma comunitaria para un bloque residencial. Para el diseño e implementación del prototipo se definieron las necesidades a cumplir por el prototipo, como la evaluación de accesos en cada domicilio, central programable para arme & desarme del sistema de alarma, control de acceso por clave, monitoreo centralizado de las casas del conjunto residencial en un punto estratégico, monitoreo remoto individual de las casas del conjunto, sistema de alarma por invación de tipo individual y comunitaria, y un sistema de alarma por activación urgente. Se realizó un estudio de dispositivos disponibles en el mercado que faciliten el direccionamiento IPv6 usando Arduino Mega como centralizador y gestor de los recursos del sistema de evaluación de accesos a las viviendas, Shield SIM900 para montaje sobre Arduino que es un sistema GSM para alerta de violación de acceso. Para el monitoreo se utilizaron RaspBerry Pi3 puesto que permiten la comunicación directa con el microcontrolador además una conectividad inalámbrica wifi. Se seleccionaron sensores discretos, de tipo magnético y ultrasónico-analógico. Para la caracterizacion del prototipo se empleó AutoCAD como herramienta para el modelamiento de las viviendas de un conjunto residencial proyectado a ser implementado en un prototipo a escala que permita la evaluación del sistema. Como resultado se determinó que cada residencia del conjunto contiene su propio sistema de alarma que manejará una señal de sistema en estado normal o violentado, en el caso de leer el estado de violentado esta emite un mensaje de texto al usuario propietario de la vivienda y al guardia del conjunto para la toma de acciones y decisiones sobre el suceso. Se recomienda promocionar el sistema de alarma comunitaria para que pueda ser reproducido a escala real.

Palabras Clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>**,** <TELECOMUNICACIONES>**,** <RASPBERRY Pi3 (HARDWARE – SOFTWARE)>, <IPv6>**,** <6loWPAN>**,** <ESTÁNDAR IEEE802.11>**,** <ARDUINO (HARDWARE – SOFTWARE)>.

ABSTRACT

A prototype community multimodal alarm was developed using the Internet Protocol version 6(IPv6) and General Packet Radio Service (GPRS) protocol for Smart cities with real-time monitoring, the prototype implemented establishes the actual situation of a community alarm system for a residential block. For the design and implementation of the prototype were defined needs to be fulfilled by the prototype, such as: access evaluation in each home, programmable central for arming and disarming the alarm system, access control by key, centralized monitoring of the house of the residential complex at a strategic point, besides individual remote monitoring of the house, alarm system by invasion of individual and community type, and alarm system by urgent activation. A study was carried out of devices available in the market to facilitate the Ipv6 addressing using Arduino Mega as a centralizer and manager of the resources of the system of evaluation of accesses to housing, Shield SIM900 for mounting on Arduino which is a Global System for Mobile (GSM) to alert access violation. For the monitoring was used Rasp-Berry Pi3 since it allows the direct communication with the microcontroller; in addition, wireless connectivity Wi-Fi. It was selected discrete sensors, ultrasonic and magnetic-type anolog. For the characterization of the prototype was used AutoCAD as a tool for the modeling of the houses of a residential complex projected to be implemented in a scale prototype that allows the evaluation of the system. As a result, it was determined that each residence of the set contains its own alarm system that will handle a system signal in normal state or violated, in the case of reading the violated state it sends a text message to the user who owns the house and to the guard of the set for the taking of actions and decisions about the event. It is recommended to provide the community alarm system so that it can be reproduced on a real scale.

Key Words: <TECHNOLOGY AND ENGINEERING SCIENCIES>, <TELECOMMUNICATIONS>**,** <RASPBERRY Pi3 (HARDWARE - SOFTWARE)>**,** <INTERNET PROTOCOL VERSION 6 (IPv6)>, <IPv6 OVER LOW POWER WIRELESS PERSONAL AREA NETWORKS (6loWPAN) >, <STANDAR IEEE802.11>, <ARDUINO (HARDWARE - SOFTWARE)>.

CAPITULO I

1. MARCO REFERENCIAL

1.1. Antecedentes

En los últimos tiempos la falta de seguridad ha pasado a ser uno de los temas centrales de preocupación de la ciudadanía y, por lo tanto, una de las cuestiones a resolver por los responsables de seguridad en el Ecuador. La inseguridad en nuestro país es un tema muy delicado a considerar y gracias al rápido desarrollo de la tecnología, existen varios proyectos que se han realizado con la finalidad de monitorear y poder anticiparse a este fenómeno social que es la delincuencia.

En la actualidad se han desarrollado proyectos de monitoreo y vigilancia a través de la utilización de alarmas comunitarias, cámaras de seguridad, monitoreo personalizado, etc., los cuales desempeñan un rol muy importante con el afán de informar, prevenir y actuar ante la presencia de personas no deseadas en nuestros domicilios, oficinas, laboratorios, etc. En muchos de los casos no basta con tener uno de estos sistemas de seguridad ya que pueden ser buenos pero son limitados es decir que no brindan la intercomunicación que garantice la calidad de servicio en tiempo real al usuario, en donde quiera que este se encuentre.

Los organismos de seguridad, que tienen competencia y/o jurisdicción en la ciudad de Riobamba, no cuentan con los medios necesarios para realizar los controles suficientes, en todos los sectores de la comunidad riobambeña, lo que hace necesaria la colaboración de la comunidad, frente a la posible presencia de delincuentes en las zonas donde existe un bajo respaldo policial.

No se puede desconocer que la comunidad, son los vigilantes constantes y colaboradores inmediatos de los entes de control, y que al igual que los anteriores también requieren de mecanismos y herramientas de apoyo que fortalezca la seguridad en los diferentes barrios y comunas que se encuentran azotados por la inseguridad ya no solo en las calles si no también dentro de sus viviendas.

Frente a esta necesidad se plantea el diseño e implementación un prototipo de alarma comunitaria para sistemas de emergencia en tiempo real basado en una red inalámbrica de sensores a través de 6lowpan para solventar las debilidades e inconvenientes descritos de los sistemas actuales. El trabajo presentado no solo brinda una excelente oportunidad para contribuir al crecimiento de los muchos servicios de alarmas comunitarias, sino que se puede extender a campos en vía de desarrollo, y contribuir en el desarrollo del País.

1.2. Formulación del problema

¿El protocolo de internet IPv6 al ser implementado en las múltiples aplicaciones existentes actualmente en el mercado en remplazo del protocolo IPv4, mejorarán la calidad de servicios (QoS) con respecto a la interacción en tiempo real?

Las aplicaciones que actualmente se encuentran en el mercado ofrecen una capacidad de interacción en tiempo real ya sea mediante una conexión WiFi o redes móviles como son 3G, HSPA+, 4G, 4G-LTE, etc. Pero estas tecnologías de acceso presentan una variedad de problemas ya que la Calidad de Servicio (QoS) no es la esperada además que presenta tiempos de latencia altos y el concepto de interacción en tiempo real no es de lo más óptimo. Esto se debe a que el protocolo de internet IPv4 no permite el mejor desempeño de dichas tecnologías. Lo que hace más interesante y brinda la apertura para que se prioricen los estudios y análisis de la implementación del protocolo IPv6.

1.3. Justificación del trabajo de titulación

1.3.1. Justificación teórica

El desarrollo de este proyecto tiene la finalidad de implementar criterios de monitoreo y control remoto por medio de redes inalámbricas basadas en 6lowpan ya que esto nos plantea una integración de múltiples elementos para el desarrollo e implementación de un sistema de intercomunicación robusto basado en la movilidad para el usuario.

Partiendo como referencia a esta iniciativa, existen varias soluciones prácticas e integrales las cuales ya están siendo comercializadas pero presentan varias limitantes al momento de ofrecer la aplicación final al usuario. Cabe recalcar que el actual "Best-Effort" que ofrece IPv4 no garantiza la calidad de servicio (QoS). Lo cual hace importante el uso de una tecnología que brinde a aplicaciones y a su vez a la red un mejor rendimiento.

Por lo cual, es necesario realizar un análisis del rendimiento de los parámetros de calidad de servicio (QoS) sobre IPv6.

La comunicación en tiempo real es de vital importancia y más aún el garantizar calidad de servicio (QoS) ya sea en el aspecto cuantitativo y cualitativo, para aplicaciones que en la actualidad son herramientas de uso muy común y necesario: monitoreo, control. El protocolo IPv6 brinda prestaciones de gran ayuda para este tipo de aplicaciones que se manejan en tiempo real.

Presentando un alto rendimiento en los parámetros que se ven involucrados en la mejora de la calidad de servicio.

En el proyecto se propone llevar a cabo el desarrollo de un sistema de alarma multimodal comunitaria utilizando el protocolo 6lowpan/IPv6 y GPRS para Smart Cities, el cual facilitará la transmisión-recepción de eventos en tiempo real.

1.3.2. Justificación aplicativa

El uso de IPv6 en la región relativamente es bajo, lo cual motivó a investigar sobre el diseño de una red de nodos sensores basados en dispositivos con soporte para 6lowpan IPv6 (Open hardware de preferencia), módulos inalámbricos programables que proporcionan la conectividad y la potencia de procesamiento necesaria para crear nodos inalámbricos, mismo que estarán instalados en las residencias previamente seleccionadas para el plan piloto de alarma comunitaria en la maqueta de la ciudadela Juan Montalvo de la cuidad de Riobamba.

Las ventajas de 6loWPAN, al ser un estándar abierto, permiten el intercambio de flujos de información end to end e integración de dispositivos de bajo consumo de manera transparente en internet y permite múltiples opciones de topología. 6loWPAN con el fin de eliminar los inconvenientes para transportar los paquetes IPv6 por su MTU en 1280 bytes sobre redes inalámbricas de bajo consumo, posee mecanismos para realizar la compresión y fragmentación de cabeceras a 127 bytes y permitir la comunicación IPv6, específicamente en las redes basadas en IEEE 802.15.4. (Gascón, 2010). La aplicación de este protocolo permite la capacidad de interactuar y comunicarse con una red de objetos, permitiendo la interoperabilidad de las redes LowPan e Internet y así optimizar el uso de los estándares de Internet sobre redes inalámbricas de baja potencia.

1.4. Objetivos

1.4.1. Objetivos generales

- Desarrollo de un prototipo de alarma multimodal comunitaria utilizando el protocolo IPv6 y GPRS para Smart Cities con monitoreo en tiempo real.

1.4.2. Objetivos específicos

- Estudiar hardware y software que den soporte para direccionamiento IPv6 como protocolo base.

- Analizar las diferentes técnicas y características de funcionamiento del protocolo 6lowpan/IPv6.

- Diseñar una red WSN y GPRS usando el estándar 6loWPAN para el monitoreo y control del sistema de alarma comunitaria.

- Implementar y comprobar el adecuado funcionamiento de la red WSN para el control y monitoreo del sistema de alarma comunitaria, efectuando las pruebas necesarias.

CAPITULO II

2. MARCO TEÓRICO

2.1. Redes inalámbricas

El propósito de cualquier sistema de telecomunicaciones es el de transferir información desde un emisor a un receptor por medio de un canal de comunicación. La información es transportada en una señal, que es una cierta cantidad física que cambia en el tiempo. La señal puede ser un voltaje proporcional a la amplitud de la voz, como en un simple teléfono, una secuencia de impulsos de luz en una fibra óptica o una onda radioeléctrica irradiada por una antena. Para señales analógicas estas variaciones son directamente proporcionales a alguna variable física, como el sonido, luz, temperatura, velocidad del viento, etc. La información también puede transmitirse por señales binarias digitales que tendrán sólo dos valores, un uno digital y un cero digital. Cualquier señal analógica puede transformarse en digital por medio de un muestreo apropiado y seguida de una codificación. La frecuencia de muestreo debe ser por lo menos el doble de la máxima frecuencia presente en la señal para preservar toda la información contenida. Las señales aleatorias son aquellas impredecibles que sólo pueden describirse por medios estadísticos. El ruido es una señal aleatoria típica descrita por su potencia promedio y la distribución estadística de la potencia sobre la frecuencia. Una señal se caracteriza por su comportamiento en el tiempo o por sus componentes de frecuencia, lo cual constituye su espectro. (Proyecto WNDW, 2013, p. 28)

El objetivo principal de todo sistema de comunicaciones es intercambiar información entre dos entidades, los elementos claves en estos elementos son:

- **La fuente.** Este dispositivo genera los datos a transmitir

- **El transmisor.** Normalmente los datos generados por la fuente no se transmiten directamente tal y como son generados. Al contrario, el transmisor transforma y codifica la información, generando señales electromagnéticas susceptibles de ser transmitidas a través de algún sistema de transmisión.

- **El sistema de transmisión.** Que puede ser desde una sencilla línea de transmisión hasta una compleja red que conecte a la fuente con el destino.

- **El receptor.** Que acepta la señal proveniente del sistema de transmisión y la transforma de tal manera que pueda ser manejada por el dispositivo destino.

- **El destino.** Que toma los datos del receptor.

A veces no es práctico que dos dispositivos de comunicaciones se conecten directamente mediante un enlace punto a punto. Esto es debido a alguna (o a las dos) de las siguientes circunstancias:

• **Los dispositivos están muy alejados**. En este caso no estaría justificado, por ejemplo, utilizar un enlace dedicado entre cada dos dispositivos, que puedan estar separados por miles de kilómetros.

• **Hay un conjunto de dispositivos que necesitan conectarse entre ellos en instantes de tiempo diferentes.** Un ejemplo de esta necesidad es la red telefónica mundial, o el conjunto de computadores pertenecientes a una compañía. Salvo el caso de que el número de dispositivos sea pequeño, no es práctico utilizar un enlace entre cada dos.

La solución a este problema es conectar cada dispositivo a una red de comunicación y a la vez sugiere dos grandes categorías en las que se clasifican tradicionalmente las redes: redes de área amplia (WAN, Wi- de Área Networks) y redes de área local (LAN, Local Arca Networks). Recientemente, las diferencias entre estas dos categorías son cada vez más difusas, tanto en términos tecnológicos como de posibles aplicaciones; no obstante, es una forma natural y didáctica de organizar su estudio. (Stallings, 2000, p. 4-8)

Una red inalámbrica es un sistema de comunicación de datos inalámbrico, utilizado para la sustitución de una red LAN (Red de área local) cableada o como una extensión de esta, trabaja en base a la tecnología de radiofrecuencia permitiendo a los usuarios amplia movilidad al eliminar en su mayoría la utilización de conexiones cableadas (García, 2016a: p.4).

La tecnología Wireless ofrece conexiones de red sin limitaciones y costos que se requieren en una red cableada, el uso de esta tecnología ha logrado brindar libertad para acceder a internet desde cualquier punto donde se tenga acceso a una red inalámbrica.

Algunos beneficios que ofrecen estás redes son:

Movilidad de los usuarios: La información, internet e incluso los recursos de la red pueden ser de libre acceso para los usuarios, sin importar que estén de manera física conectados a la red cableada, los datos se transmitirán en tiempo real desde cualquier punto de la WLAN a cualquier usuario. (García, 2016b: p.4).

Rápida instalación: Debido a que no es necesaria la utilización de cables su instalación no resulta compleja. (García, 2016c: p.4).

Flexibilidad: Permite tener conexión en lugares donde el cable se torne difícil llegar, atravesando obstáculos sin realizar cambios en la construcción. Permite el acceso instantáneo a usuarios temporales de la red. (García, 2016d: p.4).

2.1.1. Redes Inalámbricas IEEE802.11

El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) forma el mayor consorcio profesional para el fomento en la innovación tecnológica, siendo el principal eje de apoyo para la colectividad de la información en general. La mayor inspiración de la IEEE es buscar un futuro excelente en el campo tecnológico, a través de publicaciones, conferencias, estándares tecnológicos y actividades de índole tanto profesional como educativa (Pérez, 2012a: p.17).

El IEEE es eje de referencia en el mundo de las tecnologías de información, ingeniería y computación por lo cual los equipos que se desarrollan por los fabricantes se basan en las especificaciones de los estándares.

La necesidad de la sociedad actual de comunicarse cada vez más rápido ha ido en aumento y ha contribuido a un crecimiento global y fuerte en las comunicaciones inalámbricas, haciendo que este mundo vaya tendiendo de manera vertiginosa desde diez años atrás aproximadamente a un mundo móvil. (García, 2016e: p.5).

La forma de comunicación mediante cables se ha reducido drásticamente a favor de las conexiones inalámbricas desde la aparición de los estándares IEEE 802.11 o IEEE 802.16.

Las redes inalámbricas, se denominan WLAN (Red de Área Local Inalámbrica). En estas redes las distancias de los equipos suelen situarse en torno a decenas o centenares de metros y se trata de ámbitos generalmente privados que dan servicio a un grupo de usuarios reducido (Pérez, 2012b: p.18).

De la misma manera, cuando los distintos equipos están distribuidos por toda la población representan a redes metropolitanas MAN o WMAN (Red de Área Metropolitana Inalámbrica) en el caso de ser inalámbricas. Las características de estas redes son parecidas a las de las redes WLAN, pero brindan servicio a áreas de una gran extensión. En caso de que la red cubra más allá de los límites de la población, se habla de WAN (Red de Área Extensa) (Pérez, 2012c: p.18).

Este tipo de redes inalámbricas cumplen estándares genéricos aplicados de igual manera a las redes cableadas, con especificaciones extras que precisen el uso del espectro y respalden la comunicación de los diferentes equipos. (García, 2016f: p.5).

En 1997 la IEEE publicó el llamado estándar IEEE 802.11, en la cual define las distintas capas: física, enlace y control del acceso al medio para las redes inalámbricas fundamentadas en SS (espectro ensanchado).

Unos años después, en el año de 1999, un conjunto de emprendedores se juntaron para crear una organización sin motivo de lucro, con la razón de asegurar que exista compatibilidad e interoperabilidad, entre los diferentes dispositivos fabricados por este estándar, llamándose esta organización Wi-fi Alliance. (García, 2016g: p.6).

El programa de la certificación de los equipos que seguían al estándar IEEE 802.11 se designó Wifi (Fidelidad Inalámbrica) iniciándose en marzo del año 2000. Se puede decir que dentro de una red inalámbrica existen varios inconvenientes como el consumo limitado del espectro inalámbrico, y el ancho de banda que nos ofrecen es menor que el de una red cableada principalmente cuando hay una cantidad de usuarios representativo. (García, 2016h: p.5).

Wifi si bien es cierto ha tenido impacto en el mercado y ha ganado campo ante las redes cableadas pero no ha logrado remplazarlas.

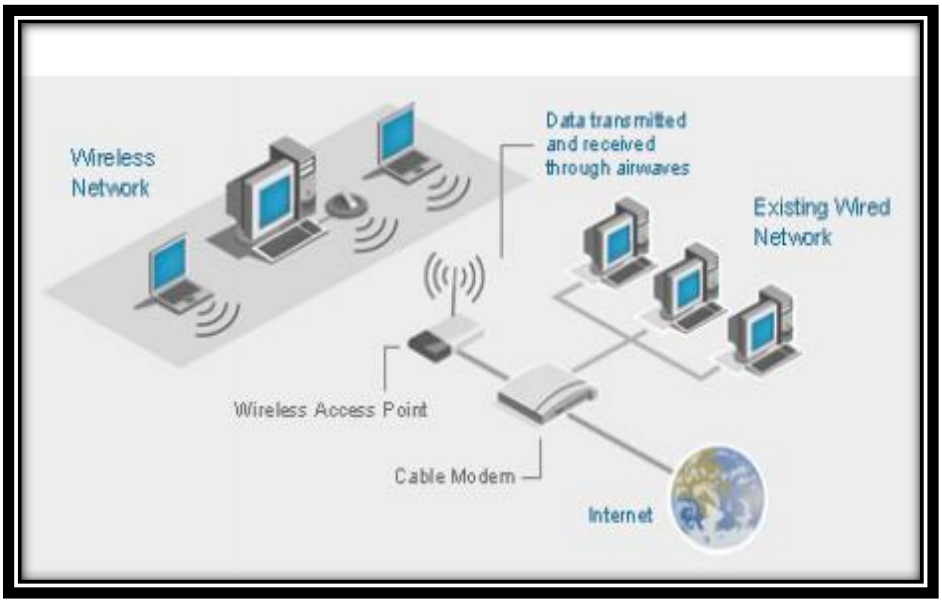


Figura 1 - 2 Esquema gráfico de una 802.11 WLAN

Fuente: Álvarez Y, 2006

2.1.2. Arquitectura 802.11 WLAN

La red inalámbrica 802.11 está compuesta principalmente por cuatro elementos.

- ✓ DS (Sistema de Distribución)
- ✓ AP (Punto de Acceso)
- ✓ STA (Estación)
- ✓ Medio inalámbrico

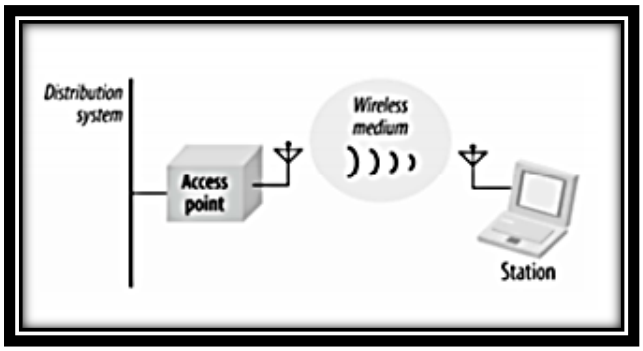


Figura 2 - 1 Arquitectura 802.11

Fuente: Pérez S, Vázquez L 2012

2.1.2.1. *Elementos que componen la arquitectura 802.11*

DS (Sistemas de distribución)

Es un elemento lógico de 802.11 usado para orientar paquetes a cada uno de sus destinatarios, gracias a este se puede relacionar algunos puntos de acceso, y así constituir un área mayor de cobertura. Dentro del estándar ninguna tecnología puntualiza al DS, pero su estructura permite direccionar tramas a través de el al igual que un backbone. (García, 2016i: p.7).

AP (Punto de Acceso)

Los AP, cumplen la función de puente entre una red cableada y una red inalámbrica para tener una comunicación entre las estaciones que se encuentren conectadas al AP. (García, 2016j: p.7).

STA (Estación)

Son los dispositivos que cuentan con la opción de conexión inalámbrica, como un teléfono móvil inalámbrico, asistente digital personal, un ordenador, entre otros. La comunicación para la transferencia de información entre ellos se lo realiza mediante la conexión a una red Wifi. (García, 2016k: p.7).

Medio inalámbrico

Se trata del medio que el estándar utiliza para desplazar los paquetes de una (STA o AP) a otra (STA o AP). (García, 2016l: p.7).

2.1.3. Capas del estándar IEEE802.11

Todos los estándares que conforman la gran familia IEEE 802, como el estándar 802.11 definen primordialmente los protocolos de la capa física PHY (Capa de Señalización Física) y la capa MAC (Control de Acceso al Medio). (García, 2016m: p.8).

PHY es la capa que se ocupa de definir los métodos por los que se difunde la señal; mientras que MAC es la capa que se ocupa del control de acceso al medio físico. En el caso de Wifi el medio físico es el espectro radioeléctrico, la capa MAC es un conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso de este espectro radioeléctrico (Pérez, 2012d: p.25).

Dichas capas concuerdan con los niveles iniciales del modelo OSI (Interconexión de Sistema Abierto), el cual detalla la arquitectura de protocolos de manera ordenada dividiéndola en siete capas o niveles.

Tabla 1 - 2 Capas del Modelo OSI

7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace
1	Física

Realizado por: (Aguilar, 2017)

2.1.3.1. Capa Física

La capa física viene hacer el primer nivel del modelo OSI su función es proveer a las capas superiores servicio de transmisión y recepción de flujo de bits ya que trabaja con señales de radio e impulsos eléctricos. En el estándar 802.11, divide al nivel físico en dos subcapas que son; PLCP (Procedimiento de Convergencia de la Capa Física) encargado de convertir la información en un formato que sea compatible al medio físico, mientras PMD (Capa Dependiente del Medio Físico) es el encargado de difundir la señal. (García, 2016n: p.8).

2.1.3.2. Capa de Enlace

La capa de enlace está ubicada en el segundo nivel del modelo OSI, controla que en el nivel físico exista seguridad, además brinda los medios necesarios para la activación y desactivación del enlace. Una función relevante que provee esta capa es la detección de errores y el control del flujo que es brindado a niveles superiores. (García, 2016o: p.9).

La MAC (Control de Acceso al Medio) y LLC (Control de Enlace Lógico) son subniveles que existen en la capa de enlace para el estándar 802.11. La principal función de MAC es controlar el acceso de los datos que son trasmitidos, mientras que LLC garantiza la sincronización de las tramas al igual que el control del flujo y de errores. (García, 2016p: p.9).

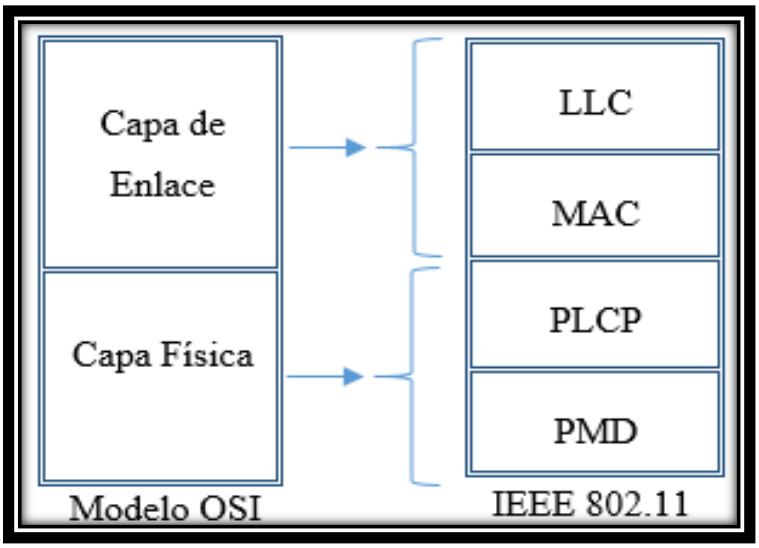


Figura 3 - 2 Comparativa entre la arquitectura de capas de Protocolos de IEEE 802.11 y el modelo OSI

Fuente: García L, Logroño S, 2016

2.2. Ipv6

Desde hace más de una década el crecimiento de la red internet ha venido generando un comportamiento creciente de tipo experimental, causado por la oferta y demanda de nuevos y más sofisticados servicios que incluyen la posibilidad de conectarse y ser controlados mediante este. Esto se traduce en la necesidad de disponer de un gran número de direcciones IP. Sin embargo, el protocolo Ipv4 que contaba con 4.294.967.296 direcciones, hoy solamente dispone de menos del 5% de su totalidad según LACNIC. Por otro lado, el tráfico circulante hoy en día exige garantías de autenticidad, seguridad, confiabilidad y movilidad, elementos del IPv4 no posee núcleo de su estructura sino que podría implementar mediante la inclusión de parches. A nivel de aplicaciones en tiempo real multimediales es fundamental la garantía de calidad de servicio (QoS), aunque IPv4 cuanta con el campo servicios diferenciados dentro de la estructura del protocolo esto no garantiza dicha variabilidad tan importante de las redes de siguiente generación. Todas las falencias han conducido al desarrollo del protocolo IPv6, que es capaz de soportar un innumerable espacio de direcciones, además de mejorar las prestaciones para el transporte de aplicaciones multimediales en tiempo real, incluyendo elementos importantes de QoS y seguridad a los usuarios en internet. Desde este punto de vista es claro que IPv6 será el protocolo que sustituya a IPv4. No obstante, este proceso será gradual ya que muchos ISP (proveedores de servicios de internet) han invertido grandes cantidades de dinero en los backbone IPv4 y hasta que no se recupere la inversión no pensara en la migración al IP de siguiente generación. Esto se traduce en la coexistencia de IPv4 e IPv6 durante los próximos años. (López, García, Nancy, Pedraza, Luis F., 2010)

El protocolo IP(internet Protocol) es en el cual se basa la trasmisión de datos en internet, su definición se encuentra en el RFC 791, su base es la transmisión de datagramas a través de la internet, lo cual hace por medio de un sistema conectionless y unreliable y da servicio best effort, TCP provee las características de confiabilidad y de conexión e IP le delega ese trabajo para no hacer un re trabajo, lo protocolos trabajan en conjunto pero cada uno haciendo lo que es necesario para que los datos lleguen con seguridad a su destino son tener que ser enviados todos los datagramas por el mismo camino. La capacidad de best effort de IP funciona de manera que existe una falla en el enlace por el cual se están transmitiendo los datos, se tengan caminos alternos por los cuales se pueda transmitir la información por medio de un sistema muy sencillo de solución de errores. El mecanismo de control de errores es controlado por el internet control message protocol (ICMP), por ejemplo, si a un ruteador le falla un enlace por el cual estaba transmitiendo los datos, elimina el programa ya manda un mensaje (ICMP) al equipo que está enviando los datos y se olvida del datagrama, no trata de retrasmitirlo, el equipo que estaba transmitiendo, retransmite el datagrama, no teniendo la información de cual enlace está activo o no. Cuando el datagrama

llega al ruteador el vera la manera de hacerlo llegar a su destino por otro enlace, lo que nos refleja ese tipo de servicio es que no implica fiabilidad (unreliable) y no conexión (conectionle) por un camino específico (Ahuatzin Sánchez, G. L, 2005, p. 24-25)

La mayor parte de los sistemas operativos, desde el año 2001 aproximadamente, tienen algún tipo de soporte de IPv6, es cierto, que en algunos casos inicialmente no se trataba de un soporte comercial sino versiones de prueba, aunque se incorporaba a sistemas operativos de producción, cada vez es más frecuente que diversas plataformas o itemas operativos, no solo incorporen Ipv6, sino que además sea activado por defecto por el fabricante, sin requerir intervención alguna por parte del usuario. Lo expuesto es válido para sistemas operativos de computadores de sobremesa y portátiles, sino también para otros dispositivos que utilizan los mismos sistemas operativos, o versiones reducidas de los mismos. Por ejemplo teléfonos celulares, agendas electrónicas, plataformas de juegos, etc. Es cierto, lógicamente, que en algunos casos, dichas versiones reducidas de los sistemas operativos, no incorpora todas las funcionalidades del sistema operativo original, y por lo tanto, se podrá dar el caso de no poder acceder a todos las funciones que se mostraran para la configuración y prueba de IPv6. (Christian O`Flaherty, 2009, p. 21)

2.2.1. Inicio de IPV6

El motivo básico por el que surge en el seno del IETF (Internet Engineering Task Force) la necesidad de crear un nuevo protocolo que en un primer momento se denominó Ipng (Internet Protocol Next Generation o Siguiente Generación del Protocolo de Internet) Fue la evidente falta de direcciones. (Consulintel, 2010).

El Protocolo IPV4 posee un espacio de direcciones de 32 bits es decir 2 *32, en cambio IPV6 ofrece un espacio de 2*128, sin embargo este no es el motivo principal de buscar una mejora ya que IPV4 posee otros problemas que IPV6 los resuelve.

Con esto podemos decir que el camino de IPV4 a IPV6 no es una cuestión de transición ni de migración sino de evolución, de integración, pero se trata de una evolución disruptora, rompedora y al mismo tiempo necesaria. IPV6 permitirá un crecimiento escalable y simple, principales hándicaps actuales de IPV4. (Consulintel, 2010).

2.2.2. Características principales de IPV6

Haciendo un resumen de las principales características de IPV& tenemos las siguientes:

- Mayor espacio de direccionamiento
- Plug & Play Auto configurable
- Seguridad intrínseca en el núcleo del protocolo (Ipsec)
- Calidad de servicio (QoS) y clase de servicio (CoS)
- Multicast
- Anycast
- Paquetes IP eficientes y extensible, sin que haya fragmentación en los encaminadores (Routers), alimentados a 64 bits (Preparados para su procesado optimo con los nuevos procesadores de 64 bits), y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del encaminador (router). (Consulintel, 2010).
- Paquetes con carga útil de más de 65.535 bytes.
- Enrutado más eficiente en el backbone de la red debido a una jerarquía de direccionamiento basada en la agregación.
- Movilidad
- Renumeracion y multi-homing facilitando el proveedor de servicios.

Estas características son las básicas q se puede mencionar, debido a que la propia estructura del protocolo permite que este crezca, o dicho de otro modo, sea más escalable, según las nuevas necesidades y aplicaciones o servicios lo vayan precisando. Cabe recalcar q la escalabilidad es la baza más importante de IPV6 frente a IPV4. (Consulintel, 2010).

2.2.3. Direccionamiento IPV6

Una dirección IPv6 está compuesta por 128 bits de longitud, es decir su número de direcciones son 2 ^ 128.

Un digito hexadecimal está representado por 4 bits (también llamado un " nibble ") Así que 128 bits se reducen hasta 32 dígitos hexadecimales

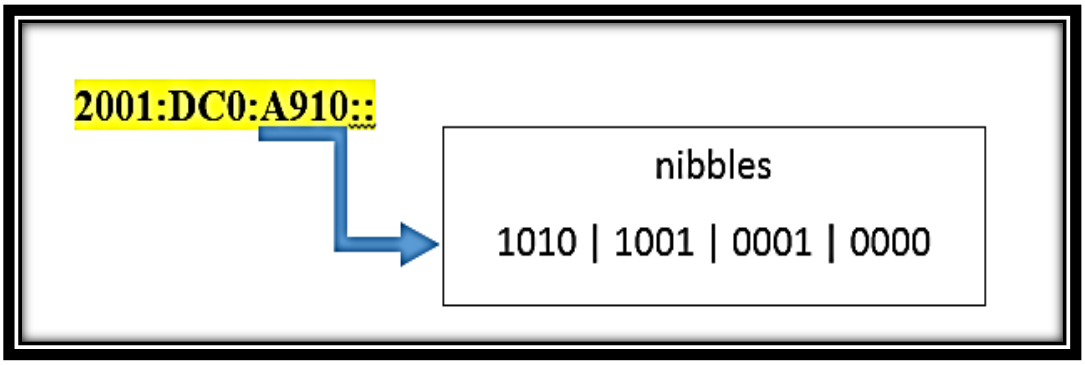


Figura 4 - 2 Representación de un nibble

Realizado por: (Aguilar, 2017)

Los valores hexadecimales se representan en 8 bloques separados por **«:»** Cada bloque contiene 4 dígitos hexadecimales.

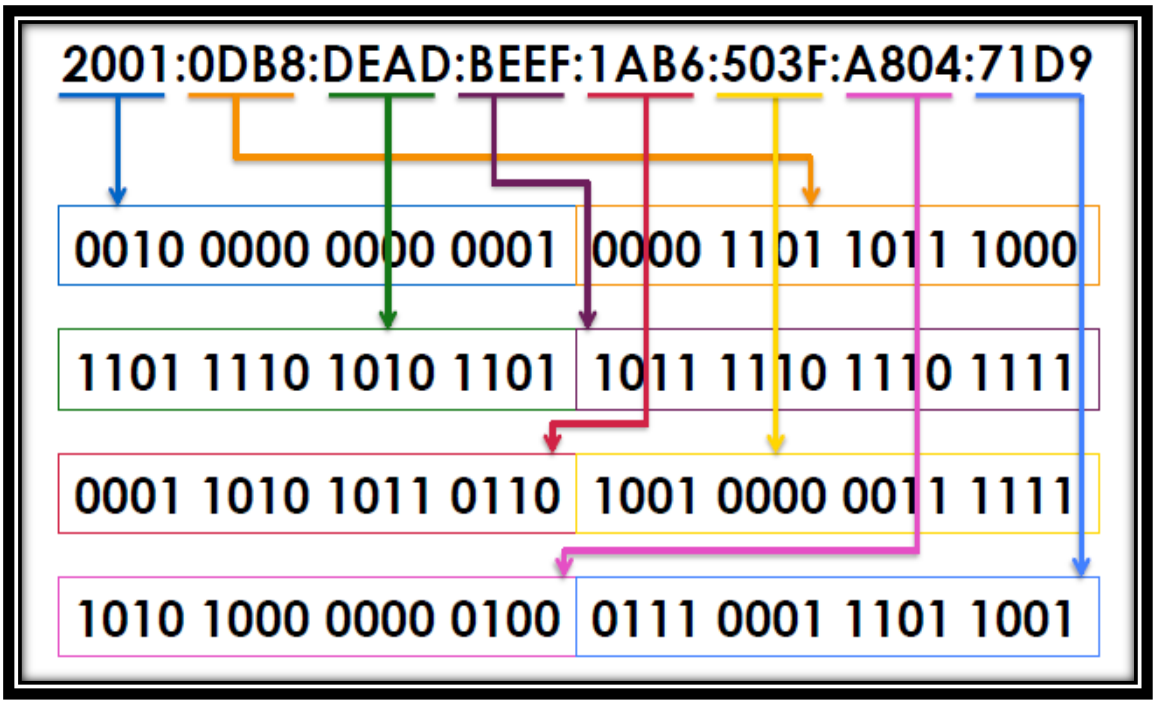


Figura 5 - 2 Representación en bloques de una dirección IPV6

Realizado por: (Aguilar, 2017)

Forma abreviada de la dirección ipv6.

Reglas:

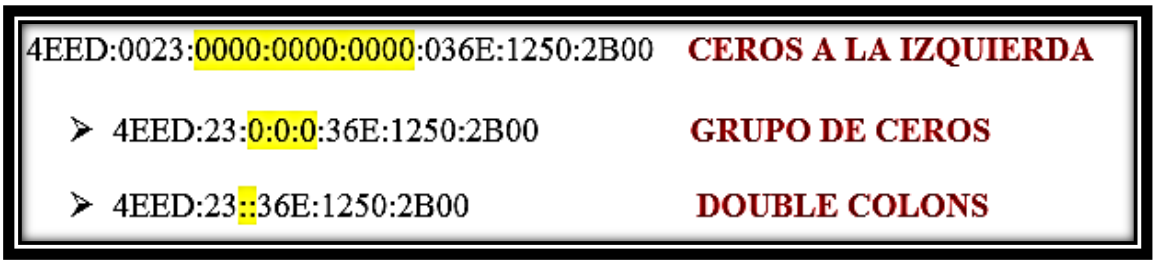


Figura 6 - 2 Reglas para abreviar direcciones IPV6

Realizado por: (Aguilar, 2017)

2.2.4. Estructura de direccionamiento

La dirección IPv6 va a estar compuesta por un prefijo de 64 bits y la otra parte de los 64bits corresponden al identificador de interfaz.

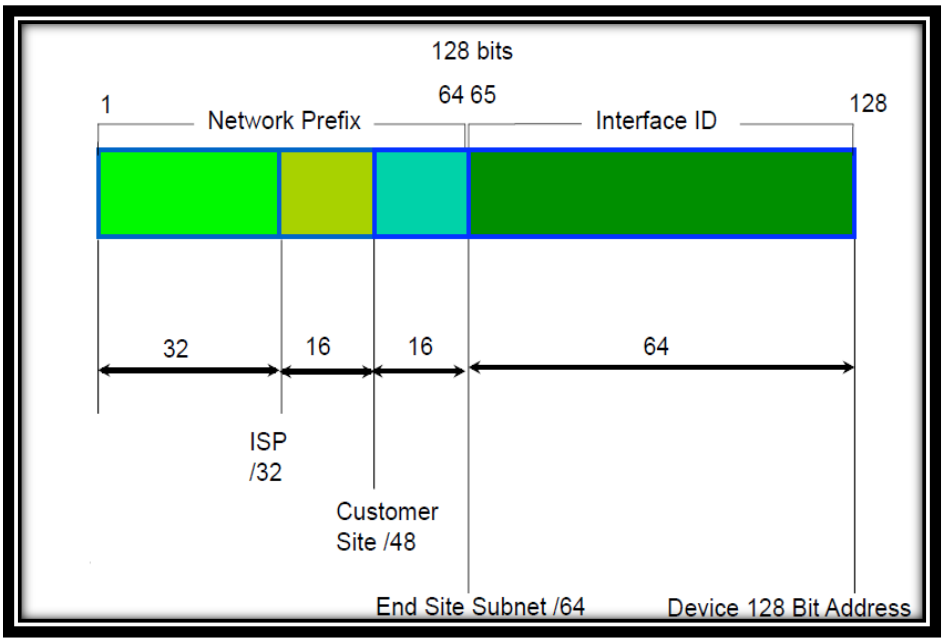


Figura 7 - 2 Estructura de direccionamiento IPV6

Realizado por: (Aguilar, 2017)

Ventajas

- Mejor aprovechamiento del ancho de banda
- Es más flexible, permitiendo añadir nuevas opciones en el futuro
- Mayor capacidad de autentificación y confidencialidad para interconexión de datos
- Hay más seguridad en el núcleo del protocolo, de manera que es muy difícil de manipular por terceros

Desventajas

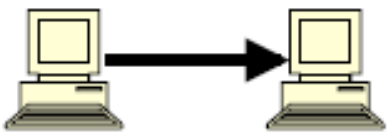
- Difícil implementación de este protocolo en las maquinas por su estructura es inviable un cambio gradual de IPv4 a IPv6 puesto a que maquinas que utilizan distintos protocolos no se pueden comunicar

2.2.5. Modelo de direccionamiento IPV6

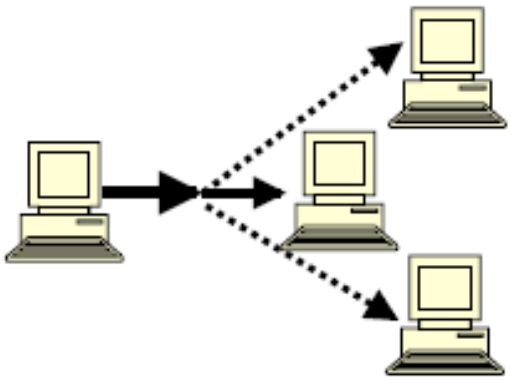
Las direcciones IPV6 son identificadores de 128 bits para interfaces y conjuntos de interfaces. Dichas direcciones se clasifican en tres tipos:

- Direcciones Unicast
- Direcciones Multicast
- Direcciones Anycast

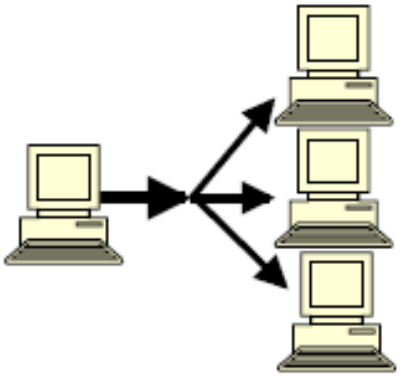
Las direcciones **Unicast**, al igual que en IPv4, son las más comunes y utilizadas. Estas son asignadas a una interface o nodo permitiendo la comunicación directa entre dos nodos de la red. Esta técnica de comunicación es conocida como uno a uno (one-to-one).



Las direcciones **Multicast,** permiten identificar múltiples interfaces o nodos en una red. Mediante este tipo de direcciones podemos comunicarnos con múltiples nodos de manera simultánea. Esta técnica de comunicación es conocida como uno a mucho (one-to-many).



Las direcciones **Anycast,** son un nuevo tipo de dirección en IPv6. Al igual que una dirección Multicast, una dirección Anycast identifica múltiples interfaces, sin embargo, mientras que los paquetes de Multicast son aceptados por varios equipos, los paquetes Anycast sólo se entregan a una interfaz o nodo.



Las direcciones Broadcast

A diferencia de IPv4, el protocolo IPv6 no soporta direcciones Broadcast. Las direcciones broadcast, son las direcciones utilizadas para la comunicación de un nodo con todos los nodos dentro de un segmento de red. Este tipo de dirección fue eliminado en IPv6.

Unicast, Multicast y Anycast son las tres grandes categorías de direcciones IPv6. Sin embargo dentro de las direcciones Unicast podemos mencionar:

- Link-Local
- Site-Local
- Global

Las direcciones Link-Local son el equivalente a las direcciones IP privadas en IPv4. Estas son asignadas a una interface de manera automática a partir del momento que activamos el protocolo IPv6 en un nodo.

El prefijo de estas direcciones es FE80::/10. Estas direcciones no pueden ser encaminadas a través de los Routers fuera del segmento local, de ahí deriva su nombre. El propósito principal es proporcionar direccionamiento IP automático a los nodos en caso que no exista un servidor DHCP.

Una dirección IPv6 Link-Local comienza con el prefijo FE80::/10 (los primeros 10 bits), luego los bits del 11 hasta 64 (los siguientes 54 bits) se configuran con valores de ceros (0000). De esta manera se forma la porción de red representada por los primeros 64bits.

FE80:0000:0000:0000:0000:0000:0000:0000/10

La porción de nodo, que son los últimos 64 bits, se forma con el formato EUI-64. El formato EUI-64 toma los 48 bits de la dirección MAC de la tarjeta Ethernet y le coloca 16 bits adicionales predefinidos por el protocolo IPv6 (FFFE). A continuación tenemos un ejemplo de una dirección Link-Local.

FE80::211:21FF:FE6C:C86B

Las direcciones IPv6 Site-Local son también el equivalente a las direcciones IP privadas en IPv4. A diferencias de las direcciones Link-Local, estas pueden ser encaminadas fuera del segmento local, es decir, podemos enviar paquetes entre diferentes segmentos de la red pero no hacia el Internet.

En las direcciones Site-Local, los primeros 10 bits se establecen con los valores 1111111011, por lo tanto, el prefijo de estás direcciones tendrá un valor en hexadecimal de FEC0 :: /10. Los siguientes 54 bits están compuestos por el ID de red. Los últimos 64 bits son el identificador de la interfaz o nodo, y estos se configuran de la misma forma que las direcciones Link-Local,

tomando 48 bits de la dirección MAC y luego agregando 16 bits con los valores FFFE. A continuación tenemos un ejemplo de una dirección Site-Local.

FEC0::CE00:3BFF:FE85:0

Las direcciones Global en IPv6 son el equivalente de las direcciones IP públicas en IPv4. Estas direcciones pueden ser encaminadas a través de la Internet. Los primeros 3 bits están compuestos por los valores 001 (en notación binaria), por lo tanto, el prefijo de estás direcciones IP tendrá un valor en hexadecimal de 2000 con una máscara /3. Las direcciones Global son el tipo de dirección IPv6 más utilizado.

2.3. Placas Arduino

Arduino es una plataforma de electrónica que puede ser usada por diseñadores, aficionados o cualquier interesado en crear entornos u objetos interactivos, abierta para la creación de prototipos basada en software y hardware flexibles y fáciles de usar. Arduino puede tomar información del entorno a través de sus pines de entrada de toda una gama de sensores y puede afectar aquello que le rodea controlando luces, motores y otros actuadores. (Paredes, 2014).

El microcontrolador en la placa Arduino se programa mediante el lenguaje de programación Arduino (basado en Wiring) y el entorno de desarrollo Arduino (basado en Processing). Los proyectos hechos con Arduino pueden ejecutarse sin necesidad de conectar a un ordenador, si bien tienen la posibilidad de hacerlo y comunicar con diferentes tipos de software (Arduino, 2013).

Las placas pueden ser hechas a mano o compradas montadas de fábrica; el software se descarga de manera gratuita y está disponible para sistemas operativos como Windows, Mac OS X, y Linux (Arduino, 2013).

Como ocurre con las distribuciones Linux, Arduino también cuenta con multitud de ediciones, cada una pensada para un público en particular o para una serie de tareas específicas. Existen gran variedad de modelos oficiales, no oficiales y compatibles que es normal que la gente tenga problemas al momento de elegir la correcta dependiendo para el tipo de aplicación que se la requiera (Paredes, 2014).

2.3.1. Placas Oficiales

Las placas oficiales son aquellas manufacturadas por la compañía italiana Smart Projects y algunas han sido diseñadas por la empresa estadounidense SparkFun Electronics (SFE) o por la también estadounidense Gravitech. Arduino Pro, Pro Mini y LilyPad son las manufacturadas por SFE y Arduino Nano por Gravitech, el resto se fabrican en Italia. Estas placas son las reconocidas oficialmente, incluyen el logo y son las únicas que pueden llevar la marca registrada de Arduino (Paredes, 2014).

2.3.2. Placas no oficiales o compatibles

Son placas compatibles con Arduino pero no pueden estar registradas bajo el nombre de Arduino. Por supuesto son diseñadas y fabricadas por otras compañías ajenas. El desarrollo de estas placas no aporta nada al desarrollo propio de Arduino, sino que son derivados que han salido para cubrir otras necesidades. Estas frecuentemente utilizan un nombre que integra el sufijo "duino" para identificarlas, como por ejemplo Freeduino. (Paredes, 2014).

Existen placas compatibles a nivel del entorno de desarrollo, es decir, solo nivel de software (pudiendo emplear Arduino IDE para programarlas). Otras placas son compatibles a nivel de hardware y eléctricamente para poder emplear los shields y módulos existentes para Arduino sin problema (Paredes, 2014).

2.3.3. Características Generales

- **Cantidad de pines**

Analógicos y digitales (normales y de tipo PWM o modulados por ancho de pulso para simular una salida analógica) (Paredes, 2014).

- **El tamaño del código a generar**

Un programa muy largo, con muchas constantes y variables demandará una cantidad mayor de memoria flash para su almacenamiento, por lo que se debe elegir una placa adecuada (Paredes, 2014).

- **Memoria RAM**

Será la encargada de cargar los datos para su inmediato procesamiento, y afectaría a la velocidad de procesamiento. La RAM va ligada al microcontrolador, puesto que ambos afectan a la agilidad de procesamiento de Arduino (Paredes, 2014).

- **Microcontrolador**

En los Arduinos oficiales se puede diferenciar entre dos tipos fundamentales de microcontroladores, los de 8 y 32 bits basados en ATmega AVR y los SMART basados en ARM de 32 bits y con un rendimiento superior, ambos creados por la compañía Atmel (Paredes, 2014).

- **Voltaje**

En cuanto al voltaje, no importan demasiado a nivel electrónico, excepto en algunos casos, para tener en cuenta la cantidad de tensión que la placa puede manejar para montar el circuito (Paredes, 2014).

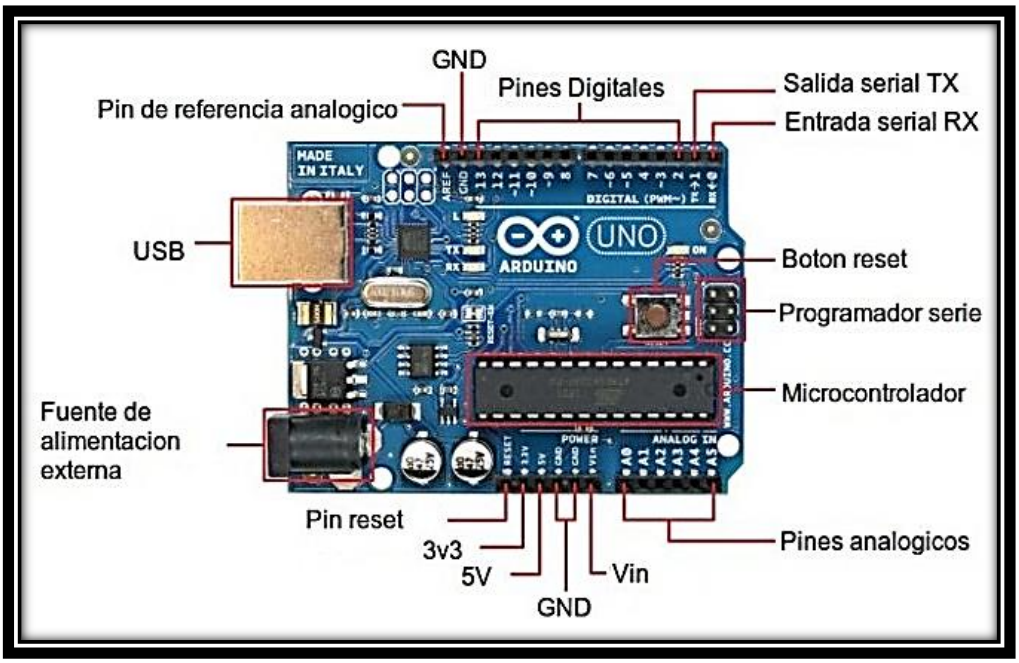


Figura 8 - 2 Partes básicas de una placa Arduino

Fuente: (Paredes I, 2014)

2.4. Raspberry Pi

RaspBerry Pi es un ordenador de placa reducida o SBC de bajo coste, cuyo objetivo es el de Estimular la Enseñanza de las ciencias de la computación.

El gran éxito de esta minicomputadora, radica en la gran comunidad que se ha creado alrededor de esta; gracias a ello se dispone de mucha documentación y ayuda alrededor de esta placa.

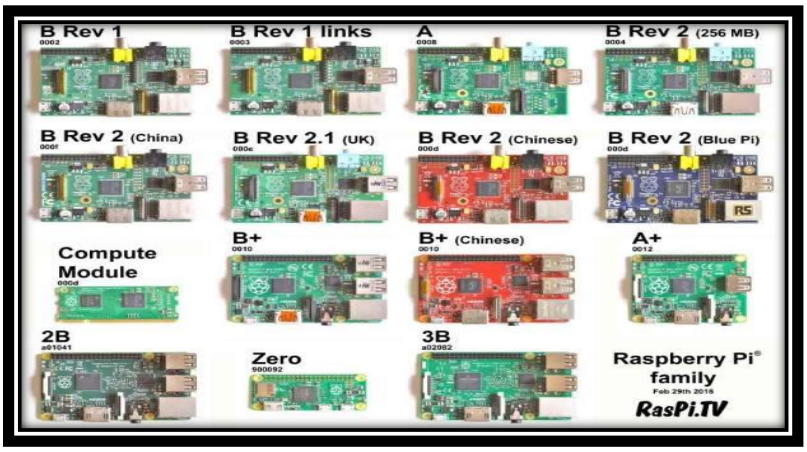


Figura 9 - 2 Módulos RaspBerry

Fuente: https://www.raspberryshop.es/images/modelos-raspberry-pi.jpg

2.4.1. Montaje

Para montar nuestra RaspBerry Pi necesitamos:

● 1 Cargador de 1A (RaspBerry Pi 1) 1,5A+ (RaspBerry Pi 2). Vale cualquier cargador de Android con MIcro-USB.

● 1 Pantalla con HDMI(o adaptador) o una pantalla con RCA.

● Teclado y Ratón

● Cable Ethernet(o adaptador Wifi USB).

● Funda (Opcional) ● Tarjeta SD(o MicroSD) >8Gb (Clase 10 Recomendada)

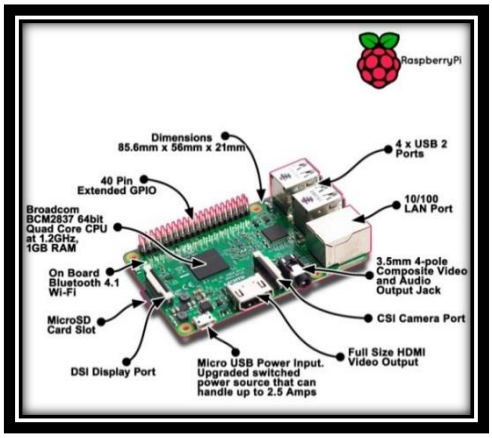


Figura 10 - 2 Raspberry – Puertos de conexión

Fuente: https://www.planetaelectronico.com/images/productos/raspberry-pi-3-modelo-b-1gb-1-18327.jpeg

2.4.2. Sistema Operativo

Una parte importante de la Raspberry Pi, es el Sistema Operativo que utilizaremos; el Sistema Operativo estará instalado en la tarjeta SD y podremos cambiar de este simplemente cambiando de tarjeta.

Uno de los sistemas Operativos más utilizados en este tipo de tarjetas es Raspbian que se trata de un Debian (Linux) optimizado para este ordenador.

Figura 11 - 2 Sistema Operativo Propósito General

Fuente: (Eben Upton, 2017)

Figura 12 - 2 Sistema Operativo Específico

Fuente: (Eben Upton, 2017)

2.4.3. Instalación de Raspbian

Usando NOOBS (New Out Of the Box Software); es un instalador para los distintos sistemas operativos de Raspberry Pi que podemos usar para realizar la instalación de manera sencilla. Para usar NOOBS, simplemente nos lo descargamos desde la web de Raspberry Pi y copiamos los archivos en una Tarjeta SD. Después arrancamos la Raspberry Pi con dicha tarjeta y seguimos las instrucciones de pantalla.

2.4.4. Aplicaciones de la Raspberry Pi

***Ordenador de Oficina*:** Gracias al entorno de Raspbian, tenemos todo lo necesario para utilizar la Raspberry Pi como un ordenador de Oficina.

***Programación*:** Raspberry Pi, tiene como propósito acercar a todo el mundo la ciencia de la computación por lo que trae herramientas para aprender a programar como Scratch o SonicPi.

Internet de las Cosas: El gran Impulso que se le está dando a este concepto hace que podamos usar la Raspberry Pi para comunicarnos con servicios como Bluemix o instalar un Sistema Operativo Windows 10 para realizar aplicaciones con IoT.

Películas/Series: Gracias a distribuciones como OpenElec, podemos tener un centro multimedia de bajo coste y con capacidad de reproducir películas en 1080P en formato MKV.

Juegos: Uno de las aplicaciones que también podemos hacer es convertir nuestra Raspberry Pi en una retro Consola; con las distribuciones como Lakka o RecalBox.

YoctoProject: Si por ejemplo queremos crear nuestra propia distribución para proyectos personalizados, podemos usar YoctoProject para crear distribuciones ligeras con las aplicaciones que necesitemos. **(**Eben Upton, 2017)

2.5. Domótica

2.5.1. Hogar digital

Una denominación que viene ganando posiciones en los últimos años es la de hogar digital, propuesta por Telefónica. Este término encierra un concepto más amplio que el tradicionalmente asociado a la Domótica: por hogar digital entendemos tanto automatización (con el soporte de la electrónica digital) como, sobre todo, comunicación (basada en redes digitales internas y externas) capaz de proporcionar todo un conjunto de tele servicios. El gran progreso tecnológico en los sistemas de telecomunicación de los últimos años, así como el desarrollo y expansión de Internet, han incrementado notablemente nuestra capacidad para crear, transmitir, almacenar y procesar información. Este fenómeno ha venido acompañado de una convergencia indudable en los antiguamente autónomos sectores de las comunicaciones, la informática y el entretenimiento, todo ello gracias a la digitalización. Este escenario se traslada a las viviendas como el marco en el que se materializa la convergencia de entretenimiento, comunicaciones y gestión digital del hogar, gracias al necesario soporte de infraestructuras y mantenimiento y por medio de servicios avanzados o tele servicios. La finalidad del hogar digital consiste en cubrir algunas (no todas, de momento) necesidades domésticas, entre ellas aumentar la seguridad, incrementar el confort, mejorar las comunicaciones, gestionar la energía controlando el gasto y ahorrando dinero, facilitar el control integral de la casa y ofrecer nuevos servicios. En definitiva, hablamos de mejorar la calidad de vida, combinando estas funciones de forma económica y sostenible. (Hugo Martín Domínguez, Fernando Sáez Vacas, 2006, p. 18-19)

2.5.2. Ambiente Inteligente

El hogar es tan sólo uno más de los múltiples escenarios susceptibles de experimentar profundas transformaciones como consecuencia de la innovación tecnológica. Las oficinas, los centros comerciales, los automóviles, los aeropuertos y por supuesto las viviendas son algunos espacios idóneos para el despliegue del Ambiente Inteligente. (Hugo Martín Domínguez, Fernando Sáez Vacas, 2006, p. 18-19)

Este término, introducido por vez primera en 1999 por el equipo investigador europeo de ISTAG, hace referencia a una visión del futuro de la Sociedad de la Información en la cual las personas

estamos inmersas en espacios poblados por multitud de dispositivos, inteligentes, pero invisibles, con los cuales interactuamos de forma sencilla, transparente e intuitiva. Por Ambiente Inteligente aludimos a entornos que incorporan tecnología capaz de detectar la presencia en ellos de individuos y de responder en consecuencia. Estos espacios se caracterizan por su ubicuidad, puesto que el usuario está rodeado por una multitud de sistemas interconectados; su transparencia, dado que estos equipos se integran en objetos cotidianos y tienden a desaparecer ante nuestros ojos; e inteligencia, pues el propio entorno es capaz de reconocer a las personas que lo habitan, adaptarse de forma dinámica a ellas y aprender de su comportamiento y preferencias. (Hugo Martín Domínguez, Fernando Sáez Vacas, 2006, p. 18-19)

Las oportunidades que ofrece el Ambiente Inteligente en el ámbito doméstico son realmente prometedoras. Los escenarios propuestos por ISTAG y las conclusiones que Telefónica expone en su Libro Blanco del Hogar Digital coinciden en que los cambios tecnológicos realmente importantes son aquéllos que dejan de ser visibles y conscientes para formar parte de la vida cotidiana y ser indistinguibles de ella. Si la incorporación de nuevas tecnologías en el hogar permite la integración de facilidades en la vida doméstica y la hace más cómoda, sin que esto suponga un esfuerzo de aprendizaje adicional por parte de sus usuarios, la visión del Ambiente Inteligente constituye un campo de trabajo que no puede pasar desapercibido. (Hugo Martín Domínguez, Fernando Sáez Vacas, 2006, p. 20-22)

Domótica, casas inteligentes, hogar digital, inteligencia ambiental son sólo algunos términos de los muchos que colonizan el intrincado lugar de encuentro entre vivienda, tecnología y ser humano. Esta abundancia de denominaciones dispares y habitualmente fragmentarias constituye el objeto de análisis del presente capítulo. Los diccionarios franceses incorporaron el término domotique a partir de 1998. Esta palabra se introdujo en España por los Pirineos como Domótica, que procede del latín domus (casa, domicilio) y del griego aútóµatoç, automática (aunque existen autores que opinan que deriva de informática, como defiende el Diccionario de la RAE, o incluso de robótica). (Hugo Martín Domínguez, Fernando Sáez Vacas, 2006, p. 20-22)

Huidobro J.M. y Millán R. (2004) recogen que el origen de la Domótica se remonta a los años setenta, cuando en Estados Unidos aparecieron los primeros dispositivos de automatización de edificios basados en la aún hoy exitosa tecnología X-10. Estas incursiones primerizas se alternaron con la llegada de nuevos sistemas de calefacción y climatización orientados al ahorro de energía, en clara sintonía con las crisis del petróleo. Los primeros equipos comerciales se limitaban a la colocación de sensores y termostatos que regulaban la temperatura ambiente. La disponibilidad y proliferación de la electrónica de bajo coste favoreció la expansión de este tipo de sistemas, despertando así el interés de la comunidad internacional por la búsqueda de la casa

ideal. Los ensayos con electrodomésticos avanzados y otros dispositivos automáticos condujeron a comienzos de los años noventa, junto con el desarrollo de los PC y los sistemas de cableado estructurado, al nacimiento de aplicaciones de control, seguridad, comunicaciones que son el germen de la Domótica actual.

La Domótica se aplica a los sistemas y dispositivos que proporcionan algún nivel de automatización dentro de la casa, pudiendo ser desde un simple temporizador para encender y apagar una luz o aparato a una hora determinada, hasta los más complejos sistemas capaces de interactuar con cualquier elemento eléctrico del hogar. La vivienda domótica es por tanto "aquella que integra un conjunto de automatismos en materia de electricidad, electrónica, robótica, informática y telecomunicaciones, con el objetivo de asegurar al usuario un aumento del confort, la seguridad, el ahorro energético, las facilidades de comunicación y las posibilidades de entretenimiento". Se pretende con ello integrar todos los aparatos del hogar a fin de que funcionen de la forma más eficaz posible y con la necesidad de una intervención mínima o inexistente por parte del usuario. (Hugo Martín Domínguez, Fernando Sáez Vacas, 2006, p. 20-22)

Por otra parte, se viene hablando de Inmótica para referirse a la automatización de edificios terciarios o de servicios (hoteles, oficinas, hospitales, plantas industriales, universidades…), como combinación de la voz latina immobilis, aquello que está fijo, de donde deriva el término castellano inmueble, y de la ya vista ´automática´. Este concepto se identifica habitualmente también como building management system, en referencia a la coordinación y gestión de las instalaciones con que se encuentran equipadas las edificaciones, así como a su capacidad de comunicación, regulación y control. El origen del término Inmótica es también francés y, aunque es de uso bastante común en España, todavía no ha sido recogido por el diccionario de la RAE. (Hugo Martín Domínguez, Fernando Sáez Vacas, 2006, p. 13-17)

2.5.3. Funciones de los Sistemas Domóticos

- Gestión de la energía Mejor uso de unos recursos escasos (energía). Diferentes tarifas según la franja horaria, gestionar el consumo de agua para no saltar al siguiente bloque de tarificación, control de iluminación interior y exteriores.

- Automatización de tareas domésticas Riego del jardín, abrir ventanas para ventilación, oscurecer ventanas para reducir la cantidad de luz natural, subir/bajar persianas.

- Seguridad Contra robos, intrusos, detección de fugas de gas e incendio y aviso a los servicios de emergencia.

- Monitorización de la salud Trata de vigilar la salud de una persona con necesidades de vigilancia (avanzada edad, enfermedades crónicas) donde el sistema sea capaz de identificar una situación de riesgo, y llamar a los servicios de emergencia.

- Control remoto desde dentro de la vivienda Desde el salón conectar la calefacción en el dormitorio; o desde el dormitorio, apagar la TV en el salón.

- Control remoto desde fuera de la vivienda. A través de un móvil con WAP, internet o una llamada normal, apagar o encender luces, A/A.

- Control remoto dentro y fuera de la vivienda Programar algunas tareas antes de llegar a la casa, o dentro de la misma, indicar que acondicione la temperatura del baño minutos antes de tomar una ducha.

- Programabilidad Capaz de ser programado por el usuario, de forma fácil, muy fácil.

- Los elementos básicos que conforman un sistema domótica se clasifican en Sensores, Sistema de Control, Actuadores (Valera, 2009, p. 8-10)

2.5.4. Ventajas de la automatización

A la hora de realizar una instalación domótica en una vivienda hay que tener en consideración que los requerimientos de los usuarios residenciales son distintos a los profesionales, ubicados en oficinas o industrias, algo que hay que tener en cuenta al evaluar la tecnología y los sistemas más adecuados para satisfacer sus necesidades que, fundamentalmente, se dirigen, como se ha comentado, a hacer más amigable su relación con el entorno en el que habita una gran parte del tiempo.

La introducción de todos estos sistemas y tecnologías en el hogar aun no es una realidad, salvo en muy pocas contadas ocasiones, pero si existen muchos catalizadores que ayudaran a que ello se realice rápidamente. Por una parte, cada vez existen más dispositivos electrónicos en el hogar y eso provoca una necesidad real de comunicar unos con otros. Por otra, la estandarización de las tecnologías de comunicación privadas, como las redes Ethernet cableadas o las redes inalámbricas WI-FI han reducido los costes a unos niveles que permiten su despliegue masivo. Para las empresas promotoras, dotar a las viviendas que construyen de una instalación domótica supone añadirle valor, lo que les permite venderlas mejor. Y mientras las empresas de telecomunicaciones y los proveedores de contenidos y servicios ven la posibilidad de aumentar los de servicios que

ofrece a sus clientes, generando nuevos ingresos a las compañías de servicios de luz, agua, electricidad, seguridad, etc. se les abre una puerta para racionalizar sus costes, y añadir valor para el usuario final. (Adrian Nogales, 2007, p. 22)

CAPITULO III

3. DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO

El presente trabajo hace uso de tecnología de comunicación inalámbrica para la elaboración de un modelo prototipo de alarma comunitaria. La metodología planteada es propia planteada en el diagrama de flujo de la figura 3.1, en la que se definen los pasos a seguir para el diseño e implementación del sistema.

Figura 1 - 3 Metodología para diseño y construcción del prototipo

Realizado por: (Aguilar, 2017)

3.1. Requerimientos del prototipo

El prototipo a implementarse debe establecer la situación real de un sistema de alarma comunitaria para un bloque residencial dotado de ciertas caracteristicas innovadoras que se plantean en el presente proyecto.

En mira de la innovación tecnólogica el sistema de alarma comunitaria a implementarse deberá cubrir las siguientes condiciones, planteadas como objetivos.

Evaluación de accesos en cada domicilio (Puertas, ventanas).

Central programable para arme & desarme del sistema de alarma.

Control de acceso por clave.

Monitoreo centralizado de las casas del conjunto residencial en un punto estratégico (Garita del conjunto).

Monitoreo remoto individual de las casas del conjunto.

Sistema de alarma por invación de tipo individual y comunitaria (sileciosa por GSM o sonora-sirena).

Sistema de alarma por activación urgente (boton de pánico).

3.2. Caracterización del prototipo

Empleando AutoCAD como herramienta de diseño asistido por computador se modela las viviendas del conjunto residencial proyectado a ser implementado en un prototipo a escala que permita la evaluación del sistema.

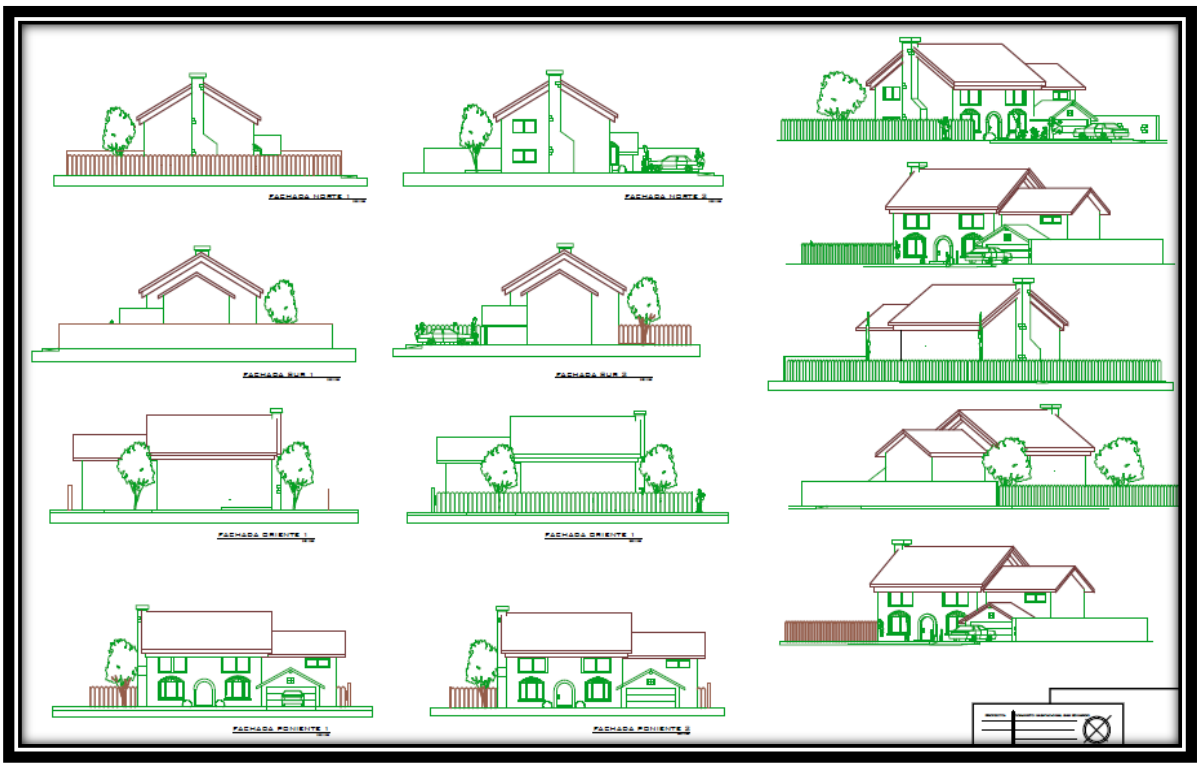


Figura 2 - 3 Metodología para diseño y construcción del prototipo

Realizado por: (Aguilar, 2017)

La figura describe las vistas del modelo de casa diseñado para la implementación del prototipo, se planifica evaluar el sistema para cuatro viviendas.

Los accesos a la vivienda a evaluarse en el prototipo se plantea sean la puerta principal y la ventana de mayor dimensión (ventana trasera), considerando que esto no sería una limitación para el sistema, es decir, la flexibilidad del diseño del sistema permitirá evaluar los accesos que se deseen.

3.3. Estudio de los dispositivos disponibles

3.3.1. Controlador

Como centralizador y gestor de los recursos del sistema de evaluación de accesos a las viviendas se analiza el uso de un controlador Arduino OPEN SOURCE.

Arduino es una herramienta para hacer que los ordenadores puedan sentir y controlar el mundo físico a través de tu ordenador personal. Es una plataforma de desarrollo de computación física (physical computing) de código abierto, basada en una placa con un sencillo microcontrolador y un entorno de desarrollo para crear software (programas) para la placa. Puedes usar Arduino para crear objetos interactivos, leyendo datos de una gran variedad de interruptores y sensores y controlar multitud de tipos de luces, motores y otros actuadores físicos. Los proyectos con Arduino pueden ser autónomos o comunicarse con un programa (software) que se ejecute en tu ordenador. La placa puedes montarla tú mismo o comprarla ya lista para usar, y el software de desarrollo es abierto y lo puedes descargar gratis desde la página www.arduino.cc/en/. El Arduino puede ser alimentado a través de la conexión USB o con una fuente de alimentación externa. La fuente de alimentación se selecciona automáticamente. (Monk, 2012)

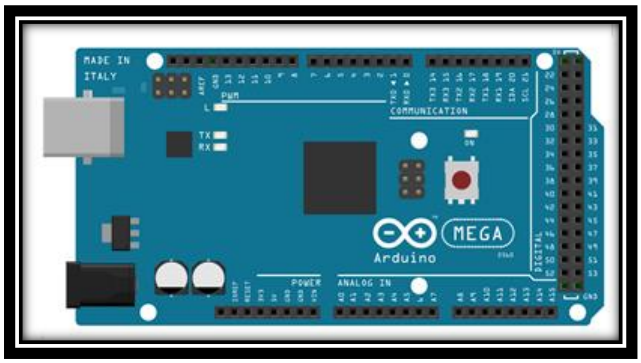


Figura 3 - 1 Arduino Mega

Fuente: http://blascarr.com/wp-content/uploads/2015/05/hc-05-Mega.png

El Arduino Mega es probablemente el microcontrolador más capaz de la familia Arduino. Posee 54 pines digitales que funcionan como entrada/salida; 16 entradas análogas, un cristal oscilador de 16 MHz, una conexión USB, un boton de reset y una entrada para la alimentación de la placa. . (Monk, 2012)

La comunicación entre la computadora y Arduino se produce a través del puerto serie, sin embargo posee un convertidor usb-serie, por lo que sólo se necesita conectar el dispositivo a la computadora utilizando un cable USB como el que utilizan las impresoras. (Monk, 2012)

3.3.1.1. Características

- Microcontrolador: ATmega2560
- Voltaje Operativo: 5V
- Voltaje de Entrada: 7-12V
- Voltaje de Entrada (límites): 6-20V
- Pines digitales de Entrada/Salida: 54 (de los cuales 15 proveen salida PWM)
- Pines análogos de entrada: 16
- Corriente DC por cada Pin Entrada/Salida: 40 mA
- Corriente DC entregada en el Pin 3.3V: 50 mA
- Memoria Flash: 256 KB (8KB usados por el bootloader)
- SRAM: 8KB
- EEPROM: 4KB
- Clock Speed: 16 MHz

Arduino Mega puede ser alimentado mediante el puerto USB o con una fuente externa de poder. La alimentación es seleccionada de manera automática.

Cuando se trabaja con una fuente externa de poder se debe utilizar un convertidor AC/DC y regular dicho voltaje en el rango operativo de la placa. De igual manera se puede alimentar el micro mediante el uso de baterías. Preferiblemente el voltaje debe estar en el rango de los 7V hasta los 12V. (Sabika, 2010)

Arduino Mega posee algunos pines para la alimentación del circuito aparte del adaptador para la alimentación:

- VIN: A través de este pin es posible proporcionar alimentación a la placa.
- 5V: Podemos obtener un voltaje de 5V y una corriente de 40mA desde este pin.
- 3.3V: Podemos obtener un vo
- ltaje de 3.3V y una corriente de 50mA desde este pin.
- GND: El ground (0V) de la placa.

3.3.2. Sensores

El objetivo de la implementación de un sistema de seguridad domiciliaria radica en establecer un sistemas de control de acceso que prevenga robos y atracos, parte fundamental de estos sistemas es la evaluación del estado de apertura y cierre de puertas y ventanas que resultan ser los principales accesos a las residencias, para este fin se utilizan sensores que con el cambio de estado de los accesos proporcionan variación de magnitudes eléctricas que se procesan en el controlador para el control y toma de decisiones sobre los actuadores del sistema.

Considerando el estado de una puerta abierta o cerrada se establece la necesidad de utilizar un sensor del tipo discreto que permita la polarización o no de una entrada del controlador.

De la gran variedad de sensores discretos disponibles en el mercado se selecciona uno del tipo magnético del tipo que se ilustra en la figura 3.6.

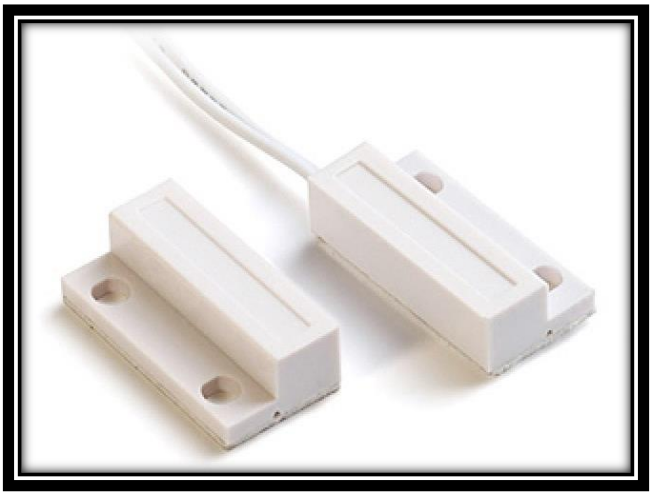


Figura 4 - 3 Sensor Magnético-Discreto.

Fuente: http://www.tanyx.com.ar/media/.cache/01f54832c6251a9ec53e5253273e4a2b.jpg

El principio de funcionamiento del sensor magnético se basa en un contacto normalmente cerrado que al ser sometido a un campo magnético conmuta a su estado de abierto permitiendo que en base a su cambio de estado se lo pueda relacionar con el estado de puerta abierta o cerrada.

Para el caso de una ventana se establece que no es recomendable usar el mismo sensor de la puerta, pues el vidrio es transparente y de poco espesor por lo que el sensor se vuelve vulnerable en el sentido de que el campo magnético que establece el control del contacto de seguridad puede ser violado con un campo externo falso, razón por la cual se plantea usar un sensor de respuesta analógica.

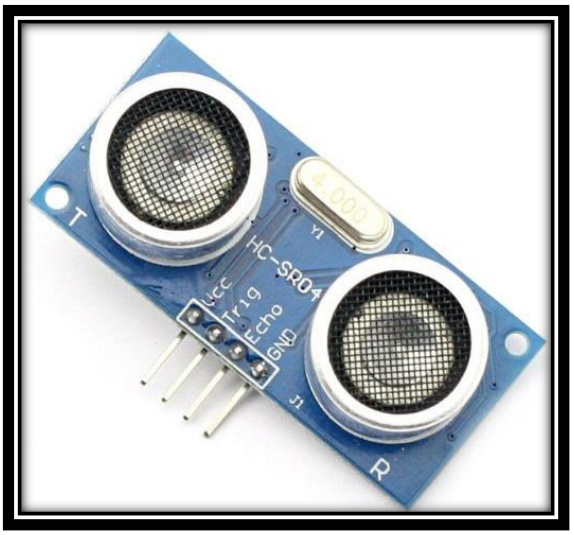


Figura 5 - 3 Sensor Ultrasónico - Analógico

Fuente: https://electronilab.co/wp-content/uploads/2013/07/A1.jpg

El sensor ultrasónico HC-RS04 que es un módulo que incorpora un par de transductores de ultrasonido que se utilizan de manera conjunta para determinar la distancia del sensor con un objeto colocado enfrente de éste.

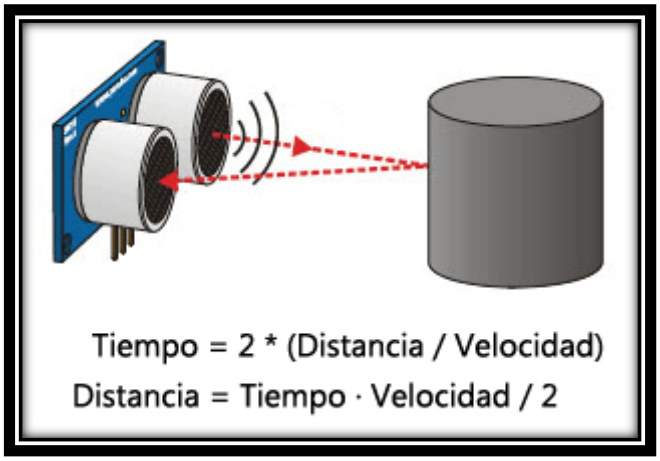


Figura 6 - 3 Principio de funcionamiento HS-RS04

Fuente: https://www.luisllamas.es/wp-content/uploads/2015/06/sensor-ultrasonico-explicacion.png

El sensor funciona por ultrasonidos y contiene toda la electrónica encargada de hacer la medición. Su uso es tan sencillo como enviar el pulso de arranque y medir la anchura del pulso de retorno. De muy pequeño tamaño, el HC-SR04 se destaca por su bajo consumo, gran precisión y bajo precio por lo que está reemplazando a los sensores polaroid en los robots más recientes. (Herrador, 2009). Se destacan las siguientes características:

- De fácil uso y programación con las placas de Arduino y microcontroladores.
- Características
- Dimensiones del circuito: 43 x 20 x 17 mm
- Tensión de alimentación: 5 Vcc
- Frecuencia de trabajo: 40 KHz
- Rango máximo: 4.5 m
- Rango mínimo: 1.7 cm
- Duración mínima del pulso de disparo (nivel TTL): 10 µS.

- Duración del pulso eco de salida (nivel TTL): 100-25000 μS.

- Tiempo mínimo de espera entre una medida y el inicio de otra 20 mS.

Pines de conexión:

- VCC

- Trig (Disparo del ultrasonido)

- Echo (Recepción del ultrasonido)

- GND

Distancia = {(Tiempo entre Trig y el Echo) * (Velocidad del Sonido 340 m/s)}/2

El medir la distancia del sensor al vidrio de la ventana resulta un método de evaluación del acceso eficaz, pues no se puede violar por interacciones de señales externas falsas, al instante de abrir la ventana o romperla la distancia varía, dicha variación es evaluada por el controlador quien procesará la información para el control sobre los actuadores o emisión de señales de alerta.

3.3.3. Interfaz control de acceso a modo de funcionamiento de la alarma

Un sistema de alarma domiciliaria puede estar en estado de armado o desarmado.

- Sistema Armado cuando el usuario no va a estar presente en el domicilio o cuando está en reposo por lo que se requiere que el sistema evalúe en tiempo real todos los accesos, y en caso de violación de los mismos se genere las señales de alarma.

- Sistema Desarmado cuando las acciones por cambio de estado de las señales de sensores son ignoradas por contar con la presencia del usuario en el domicilio.

Se hace mención de los estados del sistema para señalar la necesidad de tener un control de accesos hacia el mismo, pues será un usuario único o usuarios específicos los que puedan determinar el estado del sistema. El control a la configuración del estado del sistema se lo realiza mediante el ingreso de una clave por medio de un teclado matricial que estará conectado hacia el controlador para el procesamiento de sus señales.

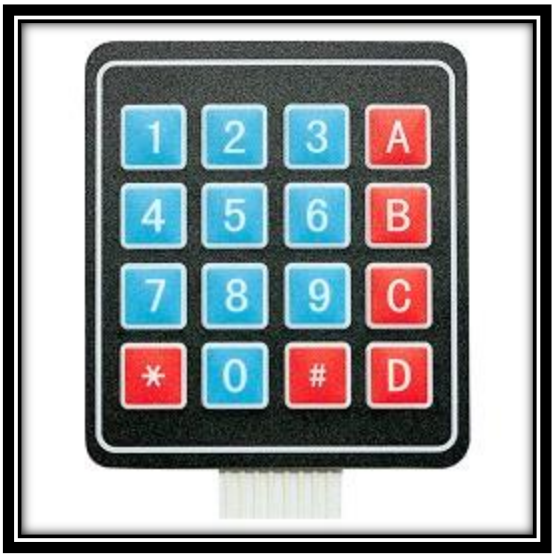


Figura 7 - 3 Teclado matricial

Fuente: http://www.prometec.net/wp-content/uploads/2015/09/keypad4x4_1.jpg

Un teclado no es más que una colección de botones, a cada uno de los cuales le asignamos un símbolo o una función determinada dentro de la programación del controlador.

Los teclados matriciales usan una combinación de filas y columnas para conocer el estado de los botones. Cada tecla es un pulsador conectado a una fila y a una columna. Cuando se pulsa una de las teclas, se cierra una conexión única entre una fila y una columna. (Monk, 2012)

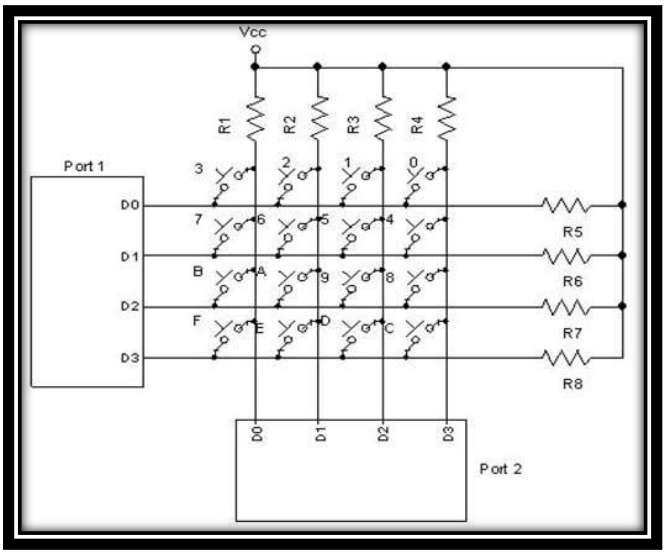


Figura 8 - 3 Constitución interna de un teclado matricial

Fuente: http://www.prometec.net/wp-content/uploads/2014/10/matrix-keypad.jpg

3.3.4. Interfaz de visualización sistema de alarma

Para la visualización del estado de la alarma y verificación de información ingresada, tal como la clave para el arme y desarme de la alarma se selecciona un lcd de 16x2 con conexión I2C.

Figura 9 - 3 LCD con módulo I2C

Fuente: http://lanzarduino.beautifullcode.com/wp-content/uploads/2016/02/lcd1.png

Generalmente las pantallas LCD para Arduino suelen necesitar bastantes pines digitales para funcionar, de 6 a 13 según la pantalla, eso hace que el controlador disminuya sus pines para la conexión de otros sensores o actuadores. Para dar solución al problema de uso de recursos se utiliza un módulo que convierte la conexión en paralelo de la pantalla a conexión en serie mediante alguno de los protocolos de comunicación que soporta Arduino, como conexión ISP, Serial e I2C, siendo este último el más común de todos (Sabika, 2010)

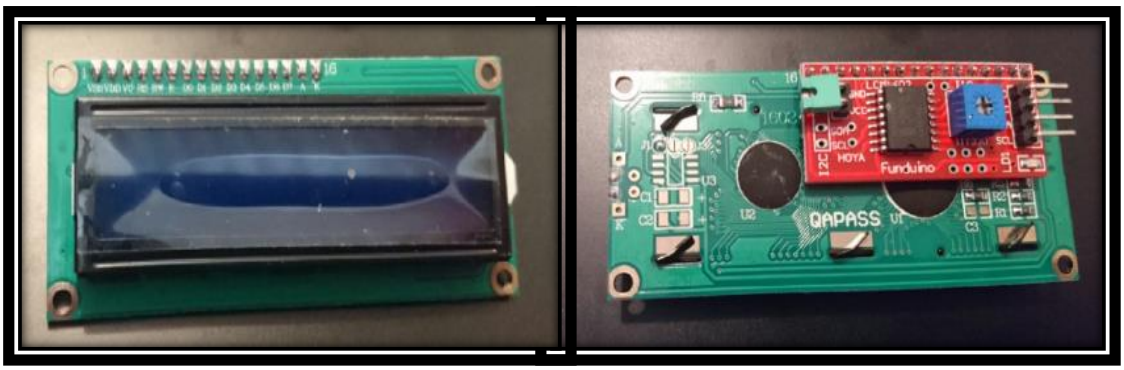


Figura 10 - 3 LCD i2C 16x2

Realizado por: (Aguilar, 2017)

El modulo solo tiene 4 cables que se corresponden a GND, 5V, SDA y SCL. Para conectarlo a la placa Arduino tendremos que enterarnos dónde están los pines SDA y SCL del protocolo I2C ya que varía según la placa y revisión. (Sabika, 2010)

3.3.5. Alerta Urgente

La alerta urgente se la define como alarma de pánico, esta opción implementada en el sistema permite por medio de la conmutación de uno o varios botones instalados en sitios estratégicos de la vivienda puedan enviar señales directas al controlador para la activación de las alertas por invasión informal de los accesos.

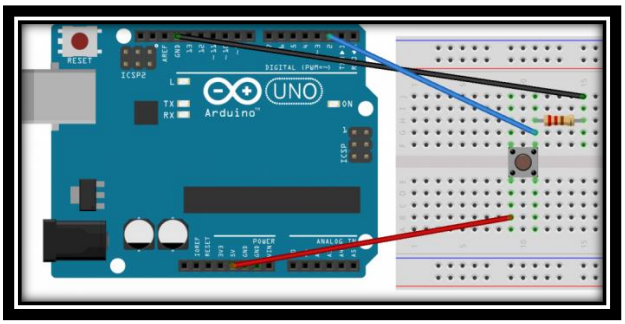


Figura 11 - 3 Entrada digital – botón de pánico

Fuente: http://rufianenlared.com/wp-content/uploads/2016/05/circuitopulsador-1024x489.png

En el microcontrolador Arduino los botones de pánico son interpretados con señales discretas con niveles lógicos alto y bajo, en programación definidos como HIGH o LOW. En la figura 3.13 se señala la forma de polarización de una señal de entrada discreta o digital.

3.3.6. Sistema GSM para alerta de violación de accesos del domicilio

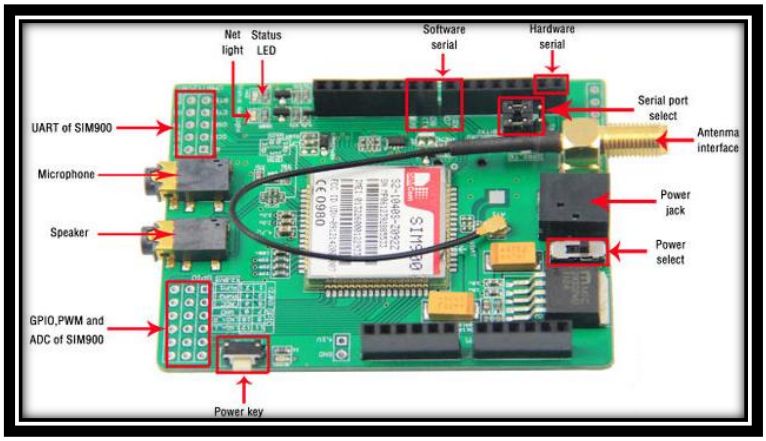


Figura 12 - 3 Shield SIM900 para montaje sobre Arduino

Fuente: https://www.geeetech.com/wiki/images/thumb/c/cf/GPRS001.jpg/700px-GPRS001.jpg

Se estableció como requerimiento del prototipo que posea un sistema de alarma silenciosa que pudiese dar aviso de la violación del o los accesos de un domicilio, se consideró hacer uso de la tecnología GSM para que la alerta que reciba el propietario del domicilio violentado sea mediante un mensaje de texto el mismo que será replicado para todos los usuarios que habitan el conjunto en idea de que se trata de una alarma comunitaria. Para el propósito planteado se utiliza un módulo GSM/GPRS con una tarjeta SIM, de forma que podamos comunicarnos con él como si se tratase de un teléfono móvil. Y es que esta tarjeta basada en el módulo SIM900 permite enviar y recibir llamadas y SMS y conectarnos a Internet, transformando nuestro microcontrolador Arduino en un teléfono móvil.

El Shield SIM900 es una tarjeta GSM/GPRS ultra compacta de comunicación inalámbrica, compatible con todos los modelos de Arduino u otros microcontroladores, está configurada y controlada por vía UART usando comandos AT. Solo conecta la tarjeta al microcontrolador, Arduino, etc, y comienza a comunicarte a través de comandos AT. Ideal para sistemas remotos, comunicación recursiva, puntos de control, mandar mensajes de texto a celulares, etc. (Sabika, 2010)

Este Shield se caracteriza por:

- Totalmente compatible con Arduino Conexión con el puerto serial
- Quad-Band 850/ 900/ 1800/ 1900 Mhz
- GPRS multi-slot clase 10/8GPRS mobile station clase B
- Compatible GSM fase 2/2+Clase 4 (2 W (AT) 850 / 900 MHz)
- Clase 1 (1 W (AT) 1800 / 1900MHz)TCP/UP embebido
- Soporta RTC Consumo de 1.5 mA (susp).

3.3.7. Sistema de monitoreo remoto usando direccionamiento ipv6

Para dar cumplimiento del requerimiento de monitoreo remoto vía Ethernet con ipv6 se plantea la revisión de equipos que soporten el mencionado direccionamiento.

Resultado del estudio de tecnologías y equipos disponibles se determina la existencia de las tarjetas Raspberry Pi3 y módulos de Ethernet de Arduino.

3.3.7.1. Módulo Ethernet Arduino

El ENC28J60 es un controlador de Ethernet diseñado para sistemas embebidos fabricado por Microchip Technology Inc. Se usa el ENC28J60 junto a un microcontrolador Arduino Mega serían útiles para la implementación del prototipo. . (Sabika, 2010)

El ENC28J60 se controla a través de bus SPI, por lo que la conexión con Arduino es muy sencilla. El ENC28J60 opera a 3.3, pero es tolerante a señales de 5V, por lo que su integración es aún más sencilla. Soporta velocidades de 10Mbits/s y los modos Dúplex (Full-Duplex) y Semi-dúplex (Half-Duplex) con detección y corrección automática de la polaridad, es uno de los procesadores más baratos para dotar conectividad. . (Sabika, 2010)

El ENC28J60 cumple con las especificaciones IEEE 802.3 10BASE-T e incorpora filtrado de paquetes para limitar el número de paquetes entrantes, un módulo DMA interno para facilitar el flujo de datos y hardware específico para el cálculo de las sumas de control (IP checksums). Sin embargo, el ENC28J60 carece de una pila de TCP/IP por hardware como sí que incluye el W5100. Por tanto, su uso es más complejo y requiere una mayor carga del procesador. (Sabika, 2010)

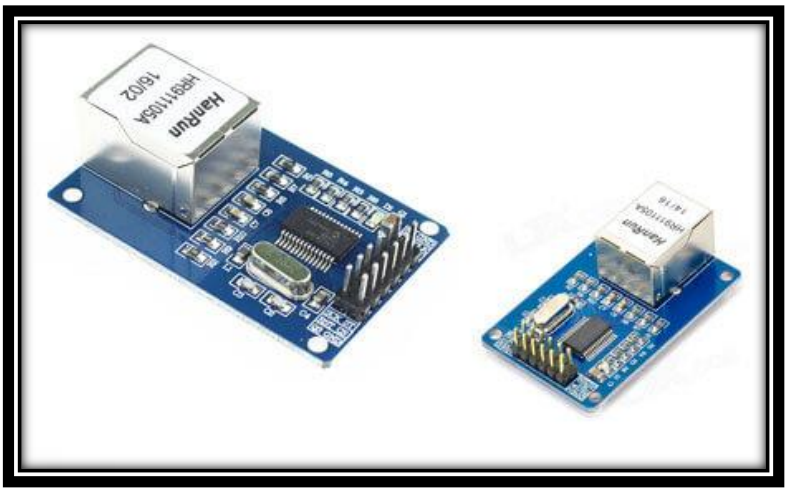


Figura 13 - 3 Shield Ethernet ENC28J60

Fuente: https://www.luisllamas.es/arduino-ethernet-enc28j60/

3.3.7.2. Raspberry PI3

Raspberry Pi es un ordenador de placa reducida (SBC) de bajo coste, que se podría considerar como un ordenador de muy pequeño tamaño, comparable con el de una tarjeta de crédito,

desarrollado en Reino Unido por la fundación Raspberry Pi, con el objetivo principal de incitar tanto a niños en sus colegios como a adultos a que aprendan sobre ordenadores y todo lo relacionado con ellos. (Gonzales 2015)

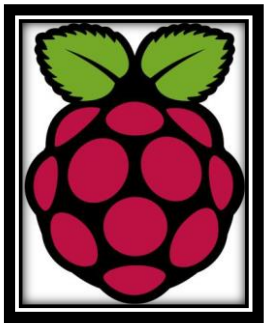


Figura 14 - 3 Logo Raspberry

Fuente: https://www.raspberrypi.org/app/uploads/2011/10/Raspi-PGB001.png

La idea es tener una placa a la que poder conectar monitor, ratón y teclado y ayudar a personas de todas las edades a adentrarse en el mundo de la computación y la programación.

La idea de desarrollar algo así surgió en 2006 cuando Eben Upton, Rob Mullins, Jack Lang and Alan Mycroft del laboratorio de informática de la Universdad de Cambridge empezaron a ver cómo había cambiado los conocimientos de los niños sobre la informática. En la década de 1990 la mayoría de los niños tenían mucha experiencia como programadores aficionados, en cambio en la década del 2000 solo eran capaces de realizar diseño web. (Gonzales 2015)

Los primeros diseños de Raspberry Pi se basaban en el microcontrolador Atmel ATmega644.
En la siguiente figura se puede ver el prototipo basado en ese microcontrolador.

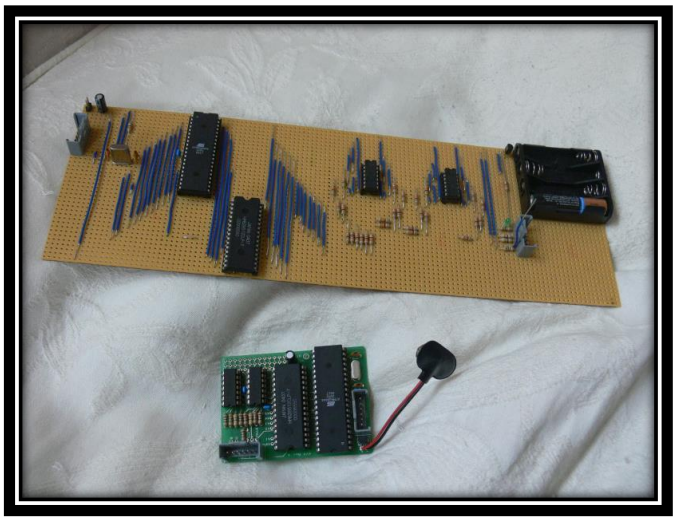


Figura 15 - 3 Primer prototipo Raspberry Pi

Fuente: (Gonzales, 2015)

Hardware

Hoy en día la Raspberry Pi presenta tres modelos, los modelos A+ y B+, que están basados en sus predecesores A y B, y la nueva Raspberry Pi 2 modelo B. Las principales diferencias entre los modelos antiguos A y B y sus versiones más recientes A+ y B+ respectivamente están en el almacenamiento, pasando de ser SD a microSD y en el caso del modelo A una reducción de tamaño y por tanto de peso. Otra diferencia del modelo B es el aumento de 2 a 4 puertos USB. En la siguiente tabla se puede observar la diferencia entre las tres versiones que se comercializan actualmente. (Gonzales, 2015)

Software

La Raspberry Pi está diseñada para ejecutar el sistema operativo GNU/Linux de código abierto. Varias versiones de Linux (conocidas como distribuciones) que soportan la Raspberry Pi son:

Raspbian OS es la distribución por excelencia para la Raspberry Pi. Es la más completa y optimizada de las existentes, por eso cuenta con apoyo oficial. Raspbian OS se basa en la potente distro Debian Wheezy (Debian 7.0) optimizando el código de ésta para la Raspberry Pi. (Gonzales, 2015)

La distribución permite moverse ágilmente en el hardware de la Raspberry Pi, con un entorno de escritorio LXDE y Midori como navegador web predeterminado. Además incluye herramientas de desarrollo muy interesantes, como IDLE para Python, Scratch para programar videojuegos. (Gonzales, 2015)

RISC OS es uno de los pocos sistemas operativos no basados en Linux que existen para la Raspberry Pi. De hecho, RISC OS es un sistema operativo británico desarrollado por Acorn Computers (los creadores de ARM) y que se distribuye bajo licencia Open-Source. Aunque su soporte y catálogo de aplicaciones disponibles no sea tan amplio como el de otras distribuciones, también está considerado como una de los sistemas operativos oficiales de la Raspberry Pi y es especialmente interesante en cuanto a que se ha creado en torno a la plataforma ARM desde cero. (Gonzales, 2015)

Arch Linux es otro de los grandes nombres en cuanto a distribuciones Linux. Se caracteriza por su simplicidad, elegancia, coherencia del código y minimalismo. Pero la simplicidad no quiere decir facilidad de uso, ya que Arch Linux es bastante conocida por ser poco amigable y

recomendable solo para gente con conocimientos más elevados. Ahora Arch Linux soporta ARM y por tanto también puede instalarse en la Raspberry Pi. (Gonzales, 2015)

Pidora es básicamente una distribución Linux Fedora especialmente optimizada para funcionar en ARM. Por el resto de características es similar a Fedora, la hermana pequeña de Red Hat, y mantenida por los mismos desarrolladores de esta comunidad libre. (Gonzales, 2015)

OpenELEC es otro de los sistemas operativos oficiales de la Raspberry Pi y por tanto se incluye en NOOBS. Se trata de una distribución Linux especialmente pensada para crear un centro multimedia barato con la Raspberry Pi. Con él se puede disponer de todo el contenido multimedia y acceso a Internet para transformar una TV en una smartTV. (Gonzales, 2015)

Para ello, OpenELEC incluye paquetes de codecs de audio y vídeo, drivers, y se basa en el famoso Kodi (anteriormente conocido como XBMC, siglas de Xbox Media Center). Kodi es un centro multimedia que fue creado en un inicio para la videoconsola Xbox, pero el desarrollo hizo que se portara a otras plataformas. Se completa con reproductores de audio, vídeo, presentación de diapositivas, visores de imágenes, reportes de clima, y otras funciones implementadas mediante plug-ins. (Gonzales, 2015)

3.3.8. Servidor VNC

Un servidor VNC (acrónimo en inglés de Virtual Network Computing) es un sistema empleado básicamente por administradores de redes para disponer de un acceso remoto a una Raspberry específica dentro del sistema de seguridad de los domicilios del conjunto residencial. Es una aplicación cliente-servidor. Una forma de explicar su funcionamiento es que el servicio de VNC instalado en Raspberry Pi (o cualquier computador host) envía "fotos" del escritorio al computador remoto, varias veces por segundo permitiendo ver el escritorio del computador remoto.

Figura 16 - 3 Administrador de redes VNC para acceso remoto a una RaspBerry.
Fuente:https://lh3.googleusercontent.com/Q23xRNV0bviUBQrQGLfqBmky3pOy0LtUuL78X_H7EBWk9OslEwPYBRC9gUwVW03Zn52=w300

3.4. Pruebas y configuración de dispositivos

3.4.1. Programación controlador

Una vez seleccionado el controlador un Arduino Mega 2560 se procede a programarlo para lo cual se utiliza la plataforma gratuita de la misma empresa Arduino que es de la gama Open Source.

3.4.1.1. IDE (SOFTWARE) DE ARDUINO

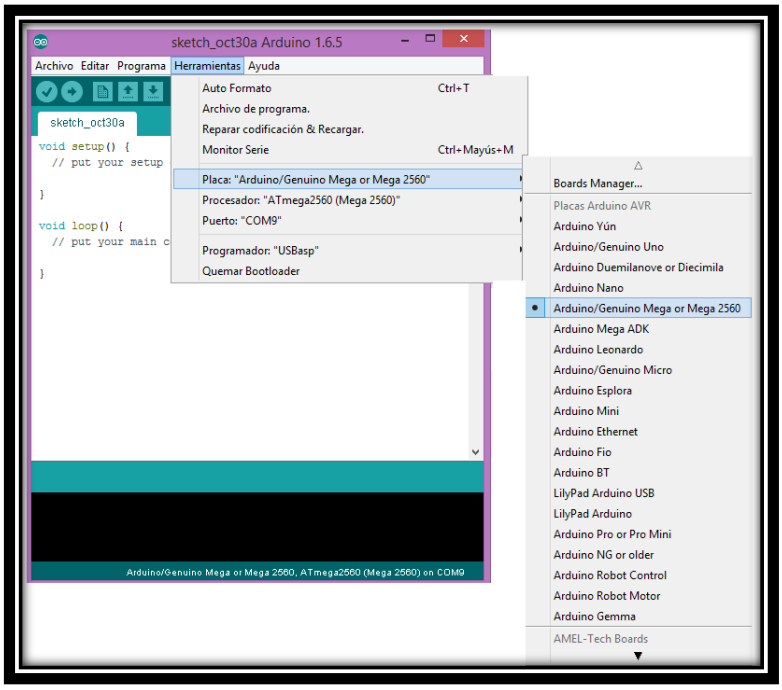


Figura 17 - 3 IDE Arduino, Selección de la Placa Arduino Mega2560

Realizado por: (Aguilar, 2017)

Conocido el microcontrolador a usarse y todos los pines necesarios para el manejo y control del Arduino, se instala el software para poder programarlo mediante el ordenador.

Se cuenta con la placa Arduino se la conecta al ordenador usando el cable USB, una vez conectada el led de la placa PWR (led de alimentación) deberá permanecer encendido.

Instalamos los drivers; al conectar el Arduino, Windows automáticamente deberá de inicializar la instalación de los drivers. Ejecutamos la aplicación Arduino, seleccionamos la placa y el puerto serie. Una vez abierta la aplicación nos vamos a Tools-Board-Arduino Mega 2560

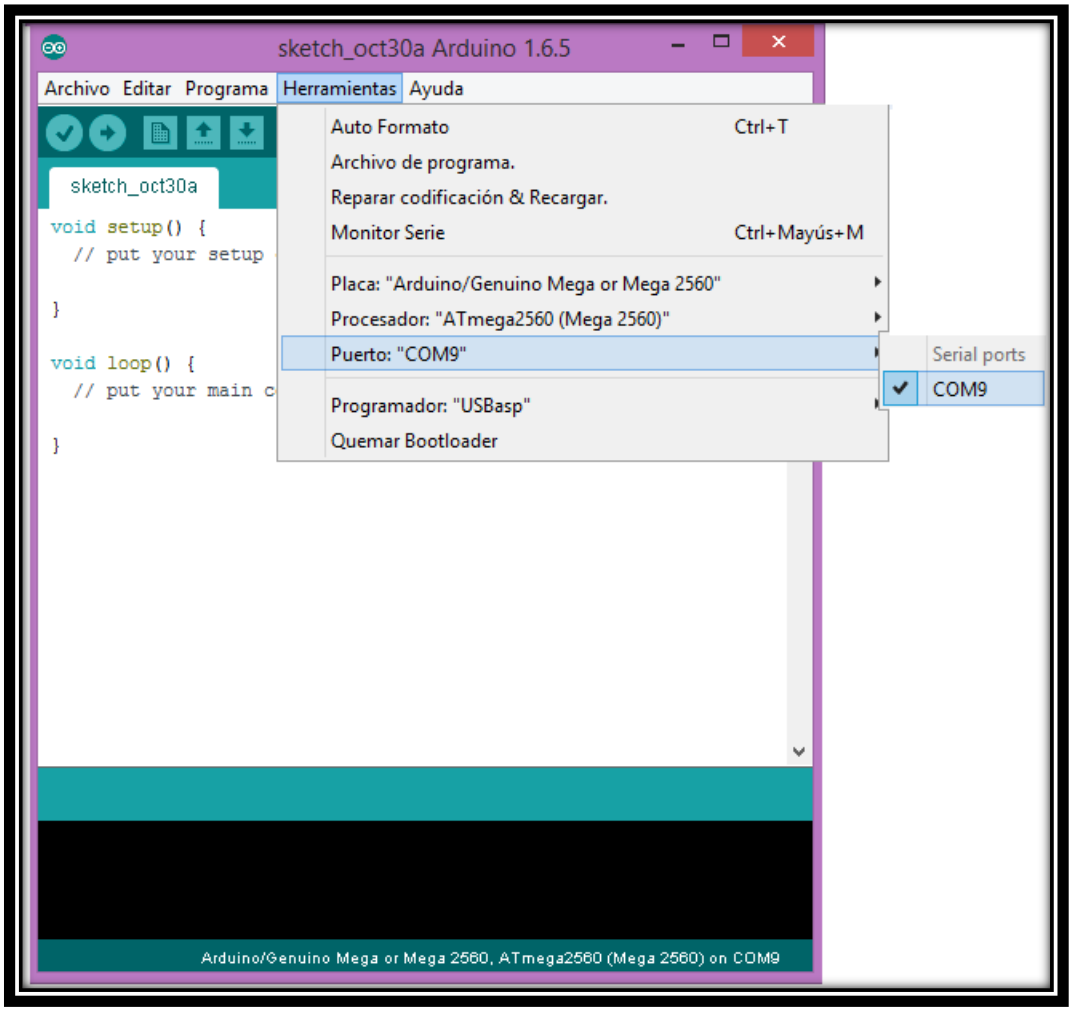


Figura 18 - 3 IDE Arduino, Selección del Puerto.

Realizado por: (Aguilar, 2017)

Una vez seleccionado el modelo de nuestra placa tendremos que seleccionar el puerto COM asignado al dispositivo para la comunicación serial y permitir la carga de instrucciones hacia el microcontrolador.

3.4.1.2. Programa Total del Microcontrolador Arduino

El programa general para el funcionamiento del sistema de alarma domiciliaria parte de la declaración de librerías que se utilizarán para el manejo de recursos de cada elemento o módulo que interviene en el desarrollo del trabajo.

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

#include <Wire.h>

#include <Keypad.h>

#include <SoftwareSerial.h>

Las librerías utilizadas en la programación general del sistema son inicialmente la **LyquidCrystal_I2C.h** y la **Wire.h** citadas para el manejo de funciones que controlan acciones sobre el dispositivo físico LCD con comunicación I2C, **Keypad.h** librería empleada para el manejo de recursos del teclado matricial y la **SotfwareSerial.h** útil para declarar el tipo de comunicación que se empleará entre el microcontrolador y la tarjeta de GSM/GPRS.

Seguido del llamado de librerías se encuentra la declaración de variables definiendo los pines a utilizarse del microcontrolador Arduino y variables globales a usarse dentro del programa.

const int EchoPin = 11;

const int TriggerPin = 12;

La declaración de las constantes EchoPin y TriggerPin se la realiza como recursos necesarios del sensor ultrasónico para la medición de la distancia del sensor hacia el vidrio sensado.

LiquidCrystal_I2C lcd(0x27, 2, 1, 0, 4, 5, 6, 7, 3, POSITIVE);

Se declara una variable del tipo lcd para el control del LCD i2c empleado para la visualización de variables y estados dentro del prototipo. Estableciendo una comunicación Serial.

SoftwareSerial SIM900(7, 8);

Establece que la comunicación UART se va a realizar por los pines 7 y 8 del microcontrolador Arduino.

const byte Filas = 4;

const byte Cols = 4;

Estas constantes definen la dimensión de filas y columnas del teclado matricial en este caso es un teclado de 4 filas y 4 columnas (4X4)

byte Pins_Filas[] = {9,8,7,6};

byte Pins_Cols[] = {5,4,3,2};

Se realiza la declaración de los pines digitales del microcontrolador Arduino que se utilizarán para las conexiones físicas del teclado matricial.

```
char Teclas [ Filas ][ Cols ] =

 {

   {'1','2','3','A'},

   {'4','5','6','B'},

   {'7','8','9','C'},

   {'*','0','#','D'}

 };
```

Teclas es un arreglo matricial que describe todos los caracteres que posee el teclado físicamente la dimensión del arreglo está definida por las constantes previamente definidas como Filas & Columnas.

Keypad Teclado1 = Keypad(makeKeymap(Teclas), Pins_Filas, Pins_Cols, Filas, Cols);

Se define la variable Keypad para asignar al teclado matricial físico.

char codigoSecreto[4] = {'2','2','5','5'};

El arreglo codigoSecreto contiene los caracteres que se desea asignar como elementos de la clave empleada para el arme y desarme del sistema de alarma domiciliaria

int posicion=0;

Esta variable resulta necesaria para el proceso de evaluación del número de caracteres ingresados para el proceso de autenticación que realiza el microcontrolador mediante su programación.

int cursor=5;

int luz=0;

Cursor, variable utilizada para el posicionamiento del cursor en el lcd y **luz** empleada para la habilitación de la luz del lcd.

int clave=0;

Clave, adquiere valores de 0 o 1; 0 en el caso de clave errónea o 1 cuando la clave ingresada es la correcta.

float ventana=A0;

Variable del tipo flotante que albergara el valor de distancia proporcionado por el sensor ultrasónico para el control del acceso ventana. Indica que se conectara a la entrada analógica A0 del microcontrolador Arduino.

int puerta=10;

Esta instrucción señala que la señal del sensor magnético se conectará al pin 10 digital del microcontrolador Arduino.

int alarma=12;

alarma indica que en el pin 12 se obtendrá un nivel de HIGH o LOW lo que se considera como una señal de salida para el control de los actuadores por una interfaz de potencia.

void setup()

{

Serial.begin(9600) ;

pinMode(puerta,INPUT);

```
    pinMode(alarma,OUTPUT);
    lcd.begin(16,2);
    lcd.setBacklight(HIGH);
    lcd.setCursor(0,0);
    lcd.print("Introduzca clave");
    lcd.setCursor(cursor,1);
    pinMode(LedPin, OUTPUT);
    pinMode(TriggerPin, OUTPUT);
    pinMode(EchoPin, INPUT);
   SIM900.begin(19200);
   SIM900power();
  }
```

En el void setup ( ) se inician todos los recursos a utilizarse dentro del programa para la ejecución de sentencias que debe cumplir el sistema. Se fijan las funciones de cada pin declarado en el bloque de variables definiendo si actúan como entradas (INPUT), salidas (OUTPUT) o señales de PWM. Existen también funciones específicas propias de cada módulo conectado al microcontrolador tales como el teclado matricial, el lcd i2C y el Shield SIM900 GSM/GPRS.

```
void SIM900power()
{
  digitalWrite(9, HIGH);
  delay(1000);
```

```
  digitalWrite(9, LOW);

  delay(5000);

  }
```

Esta función sirve para con un pulso desde el pin 9 activar la tarjeta GSM con la SIM900

```
void fsendSMS()

{

  SIM900.print("AT+CMGF=1\r");

  delay(100);

  SIM900.println("AT + CMGS = \"593978689847\"");

  delay(100);

  SIM900.println("VIOLACIÓN DEL SISTEMA DE SEGURIDAD ");

  delay(100);

  SIM900power();

}
```

fsendSMS es la función que contiene los códigos AT necesarios para enviar un mensaje de texto por medio de la tarjeta de GSM. El llamado de ésta función se lo realizará cuando el sistema de seguridad haya sido violentado.

La función void loop ( ) es la función principal del programa, en ésta se establece todas las acciones que deberá estar ejecutando en forma repetida y continua el microcontrolador para establecer el funcionamiento de los modulo que gobierna en base a la lectura de sus entradas.

```
void loop()
```

```
{
  char pulsación = Teclado1.getKey();
```

Asigna a la variable pulsación el valor leído del teclado por medio de la función ***Teclado1.getKey().***

```
  if (pulsación != 0)
   {
    if (pulsación != '#' && pulsación != '*' && clave==0)
     {
```

Pregunta si la variable pulsación es diferente de cero, en el caso de cumplirse esta condición señala que en el teclado físico se ha ejecutado la pulsación de una de sus teclas; en el caso que se cumple la condición, pregunta nuevamente si la pulsación fue diferente a '#', '*' y si la clave aún no ha sido ingresada es decir si sigue asignado un cero a la variable clave.

```
    if (pulsación != '#' && pulsación != '*' && clave==0)
     {
      lcd.print(pulsación);
      cursor++;
      if (pulsación == codigoSecreto[posición])
        posición ++;
```

Por el ciclo de verdadero de la condición se ejecuta la impresión del valor presionado del teclado en el lcd y se recorre el cursor para esperar el siguiente carácter.

El carácter ingresado es evaluado por un proceso de comparación con los elementos del vector patrón que contiene la clave, en el caso de tener correspondencia el carácter ingresado con el carácter del patrón se incrementa la posición.

```
if (posición == 4)
{
  lcd.setCursor(0,0);
  lcd.print(" Clave Correcta  ");
  clave=1;
}
```

Si la variable posición llega al número 4 implica que se ingresó correctamente la clave por lo que la variable del mismo nombre se asigna un 1.

```
  if (cursor>8)
 {
    cursor=5;
    posición=0;
    lcd.setCursor(0,1);
    lcd.print("              ");
    lcd.setCursor(2,1);
    lcd.print(" Alarma OFF ");
```

Al llegar a este bloque de programa significa que se ingresó correctamente la clave por lo que se resetea el mensaje del lcd para especificar el estado de la alarma en desarme **"Alarma OFF"**

```
    if(clave==0){
       lcd.setCursor(0,1);
```

```
                lcd.print("Clave incorrecta");

                Serial.println("Ingreso de Clave Incorrecta");

            }

        }

    }

}
```

La condición indica que cuando la clave no haya sido ingresada correctamente terminado el ingreso del cuarto caracter se mostrará impreso en el lcd el mensaje de “Clave incorrecta”.

```
if (pulsación == '#' && luz==0)

  {

   lcd.backlight();

   luz=1;

   pulsación =0;

  }

if (pulsación == '#' && luz==1)

  {

   lcd.noBacklight();

   luz=0;

  }
```

Utiliza el estado de la tecla ‘#’ para el encendido y apagado de la iluminación del lcd con el llamado paralelo de la función Backlight()

```
if (pulsación == '*')
  {
    posición = 0;
    cursor = 5;
    clave=0;
    posición=0;
    lcd.setCursor(0,0);
    lcd.print("Introduzca Clave");
    lcd.setCursor(0,1);
    lcd.print("                ");
    lcd.setCursor(5,1);
  }
```

Utiliza el estado de la tecla ‘*’ para el armado del sistema de alarma domiciliaria en el caso de salida del usuario o al momento de reposar.

```
if (clave==1)
  {
    Serial.println("Alarma Desarmada");
  }
```

Luego de ingresada la clave correctamente se asigna un valor de 1 a la variable del mismo nombre y envía un mensaje al puerto Serial indicando que el sistema está desactivado, éste mensaje será leído por la Raspberry Pi3 para el monitoreo remoto del sistema.

```
  else
  {
    int a=digitalRead(puerta);
    float b=analogRead(ventana);
    int cm = ping(TriggerPin, EchoPin);
    while ((a==LOW)||((cm>=2)&&(cm<3))){
      Serial.println("Violada seguridad del domicilio");
      delay(1000);
     digitalWrite(alarma, HIGH);
     fsendSMS()
  }
        Serial.println("Alarma Armada");
       digitalWrite(alarma, LOW);
  }
}
```

En el bloque de programación citado se realiza la evaluación del estado de los sensores que controlan los accesos de la puerta y ventana, esto se ejecuta cuando el sistema está armado.

En el caso de violación de los accesos se imprime en el serial "Violada seguridad del domicilio", este mensaje es captado por la Raspberry para el monitoreo remoto del sistema y a su vez se hace el llamado de la función *fsendSMS()*para que se realice e envío de la alerta por medio de un mensaje de texto.

```
. int ping(int TriggerPin, int EchoPin) {

  long duration, distanceCm;

  digitalWrite(TriggerPin, LOW);

  delayMicroseconds(4);

  digitalWrite(TriggerPin, HIGH);

  delayMicroseconds(10);

  digitalWrite(TriggerPin, LOW);

  duration = pulseIn(EchoPin, HIGH);

  distanceCm = duration * 10 / 292/ 2;

  return distanceCm;

}
```

La función **ping** es propia del sensor ultrasónico para determinar la distancia del sensor al vidrio.

3.4.2. Configuración – Raspberry

3.4.2.1. Carga del sistema operativo

Lo primero es dirigirse a la página raspberrypi.org la página oficial de la empresa Raspberry PI seleccionar la sección de descargas y se observa que existe la posibilidad de descargar el software en la versión NOOBS y Raspbian.

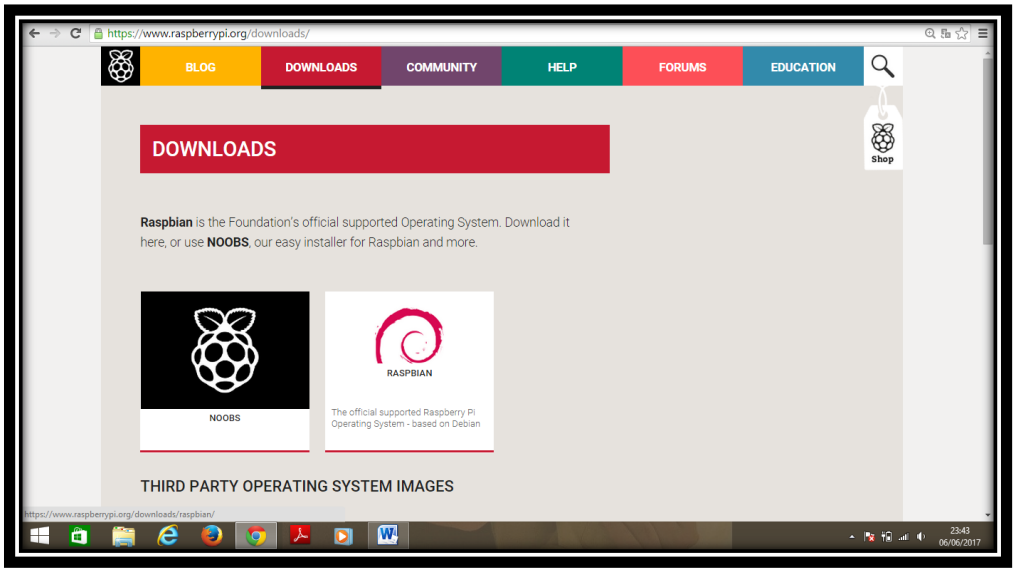


Figura 19 - 3 Página oficial de Raspberry PI.

Elaborado por: (Aguilar, 2017)

Al seleccionar la versión Raspbian que es el sistema operativo seleccionado para el diseño de la aplicación se despliega la opción de descarga de dos versiones actualizadas del sistema operativo de las cuales se descarga la versión Full en formato .zip, el mismo que al descomprimirlo dará una imagen de disco que será la que se instala para la Raspberry.

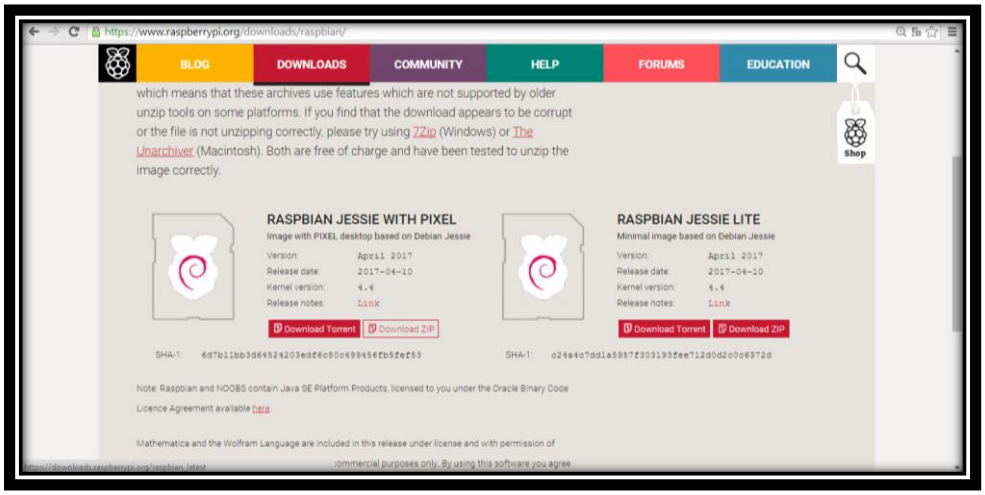


Figura 20 - 3 Página de descarga versiones del Sistema Operativo Raspbian.

Realizado por: (Aguilar, 2017)

Realizada la descarga del sistema operativo se procede a ubicar en el computador una micro SD recomendada sea de clase diez para que pueda correr sin problemas el S.O., se la formatea directamente en un formato básico y en el caso de desearlo se asigna un nombre a la tarjeta.

Una vez preparada la SD card se requiere un programa adicional el WinDiskImage que se lo descarga también de forma gratuita, éste sirve para enrutar la información de la imagen descargada hacia la SD card para de esta manera estar lista para trabajar con la Raspberry Pi3.

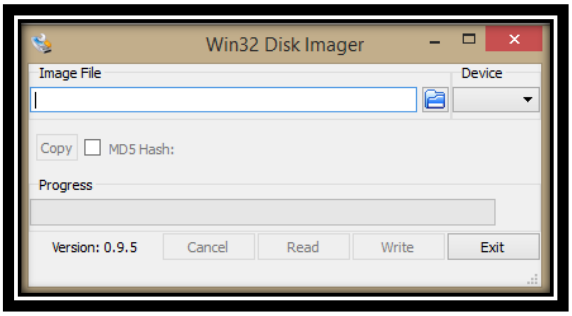


Figura 21 - 3 Interfaz Win32DiskImage

Realizado por: (Aguilar, 2017)

3.4.2.2. Direccionamiento ipv6

Como parte de los objetivos planteados en el presente trabajo se encuentra el uso del direccionamiento ipv6 por lo que en la etapa anterior se estudió dos posibles equipos que daban soporte para éste requerimiento. Se seleccionó el uso de la Raspberry Pi3 que resulta más fácil de configurar, soporte más robusto y permiten la comunicación directa con el microcontrolador que será el que proporcione la información de los sensores del control de accesos a la Raspberry.

Aprovechando las bondades de las Raspberry Pi3 se realiza para el prototipo una red inalámbrica basada en una LAN (Local Area Network) de topología tipo estrella como se puede observar en la figura 3.22. El fin de esta implementación es el centralizar el monitoreo de cada una de las residencias que conforman el conjunto en un punto estratégico, físicamente esto estría ubicado en la garita del conjunto donde personal de seguridad podrá realizar el monitoreo continuo y en tiempo real de las viviendas del conjunto habitacional.

Para el direccionamiento de la red a cada Raspberry que representa una vivienda del conjunto y se le asignará una dirección ip propia.

CONFIGURACIÓN DE LA RED EN LA RASPBERRY

La configuración de la red se realiza desde el archivo de configuración interfaces en /etc/network/interfaces, se da a la Raspberry una dirección IP o se puede usar DHCP, establecer la información de enrutamiento, configurar el enmascaramiento IP, poner las rutas por defecto entre otras acciones.

Para utilizar DHCP se plantea el siguiente código:

auto eth0

allow-hotplug eth0

iface eth0 inet dhcp

Para DHCPv6 (utilizado para IPv6):

iface eth0 inet6 dhcp

Alternativamente, se puede autoconfigurar IPv6 utilizando autoconfiguración de dirección sin estado, o SLAAC (stateless address autoconfiguration), que se especifica utilizando auto en vez de DHCP en la línea de inet6:

iface eth0 inet6 auto

En el caso de poseer direcciones ip estáticas se puede configurar la red manualmente algo como esto pondrá la puerta de enlace por defecto.

auto eth0

iface eth0 inet static

address 192.0.2.7

netmask 255.255.255.0

gateway 192.0.2.254

Para el caso de estudio para añadir una dirección IPV6, se agrega:

iface eth0 inet6 static

address 2001:db8::c0ca:1eaf

[parcial]netmask 255.255.255.0

gateway 2001:db8::1ead:ed:beef

De esta manera están configuradas las Raspberry listas para interrelacionarse con el elemento centralizador.

3.4.2.3. Servidor VNC

Lo primero que se necesita es instalar el servidor VNC en la Raspberry Pi3, para habilitar el acceso remoto al escritorio. Para esto se ingresa al terminal de la Raspberry y se procede a instalar el vncserver.

Se parte de la línea de comando

sudo apt-get update

sudo apt-get install realvnc-vnc-server realvnc-vnc-viewer

Una vez instalado el servidor vnc, es necesario iniciar el servicio. Esto se realiza mediante el comando:

vncserver :1 -geometry 1280x800 -depth 16 -pixelformat rgb565

El comando vncserver permite ciertas variantes, en el comando anterior, ":1" indica el número del escritorio que está monitoreando y será utilizado al momento de realizar el acceso remoto. Para el caso del prototipo se crearon 4 escritorios considerando que el conjunto posee cuatro viviendas. El modificador -geometry indica el tamaño de la pantalla en pixeles. El modificador -depth funciona para la profundidad del color, en este caso 16 bits y por último el modificador -pixelformat indica la presentación del color.

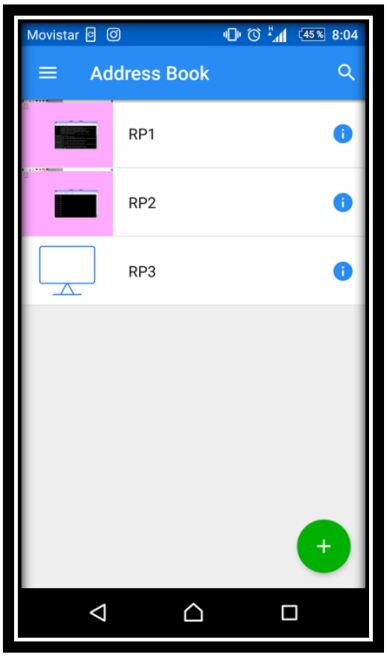


Figura 22 - 3 VNC direcciones agregadas

Realizado por: (Aguilar, 2017)

La figura 3.22 describe la lista de dispositivos que están agregados en el VNC Viewer para conectarse remotamente aquí constarán las viviendas del conjunto.

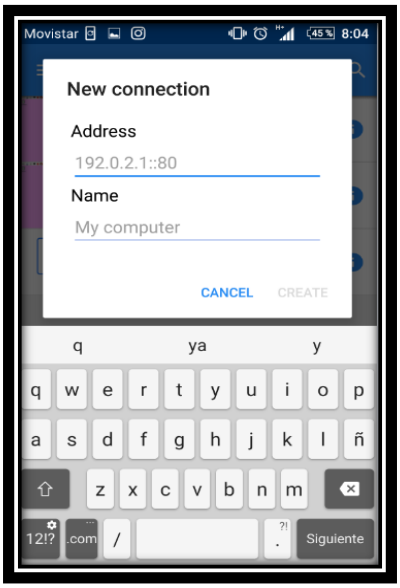


Figura 23 - 3 Pantalla para registrar una nueva entrada en VNC Viewer

Realizado por: (Aguilar, 2017)

Para registrar un dispositivo se lo realiza ingresando la dirección ip seguido del identificador que se le dio en el comando vcnserver de habilitación del servicio, se le puede asignar un nombre específico que defina la Raspberry.

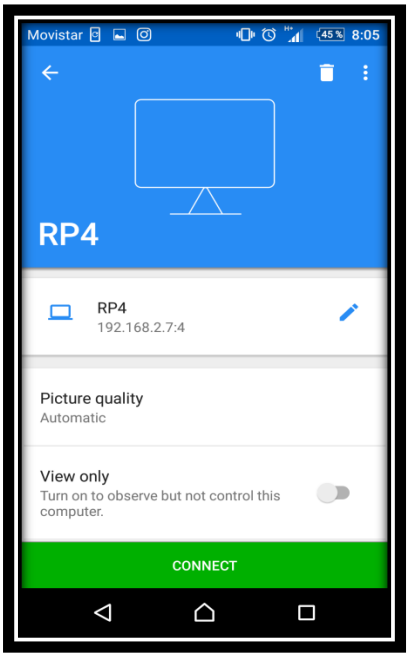


Figura 24 - 3 Pantalla de activación de conexión remota con VNC Viewer

Realizado por: (Aguilar, 2017)

La figura 3.24 describe la interfaz para la conexión remota a una Raspberry específica registrada.

3.4.2.4. Conexión Arduino – Raspberry

La Raspberry y Arduino se conectarán por puerto USB utilizando comunicación Serial gobernada por instrucciones de programación en Arduino para el microcontrolador y en Python para la Raspberry.

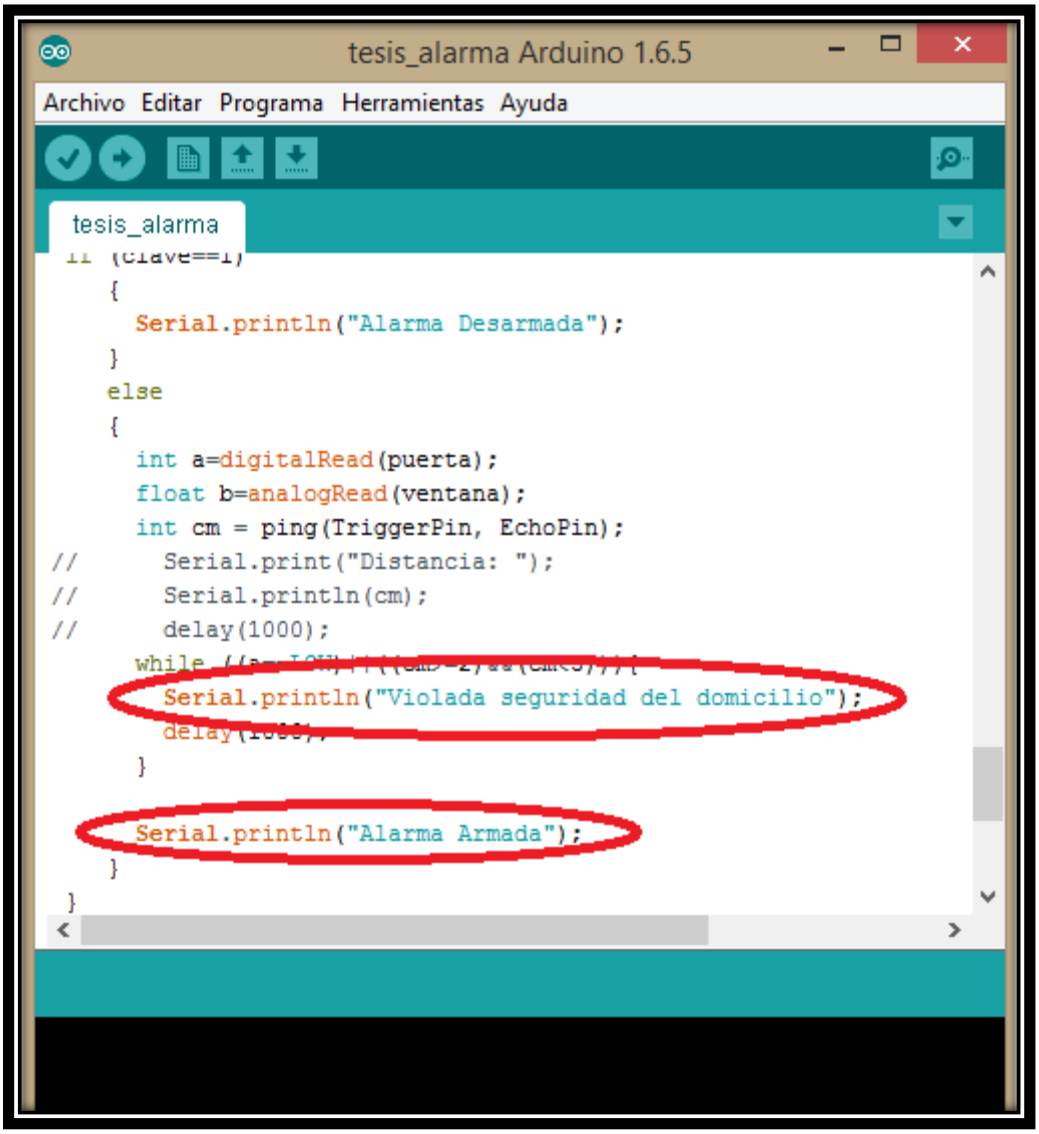


Figura 25 - 3 Programa IDE Arduino.

Realizado por: (Aguilar, 2017)

La función Serial.println del IDE de Arduino permite exportar al puerto Serial mensajes, datos y valores de variables que se evalúan dentro del microcontrolador los mismos que son leidos por la Raspberry mediante instrucciones plasmadas en un bloque de programación en Python.

En la Raspberry para escribir el código de programación se instala inicialmente la 'python-serial' para que no nos de error en la ejecución, se utiliza la siguiente línea de código en el terminal del sistema:

sudo apt-get install python-serial

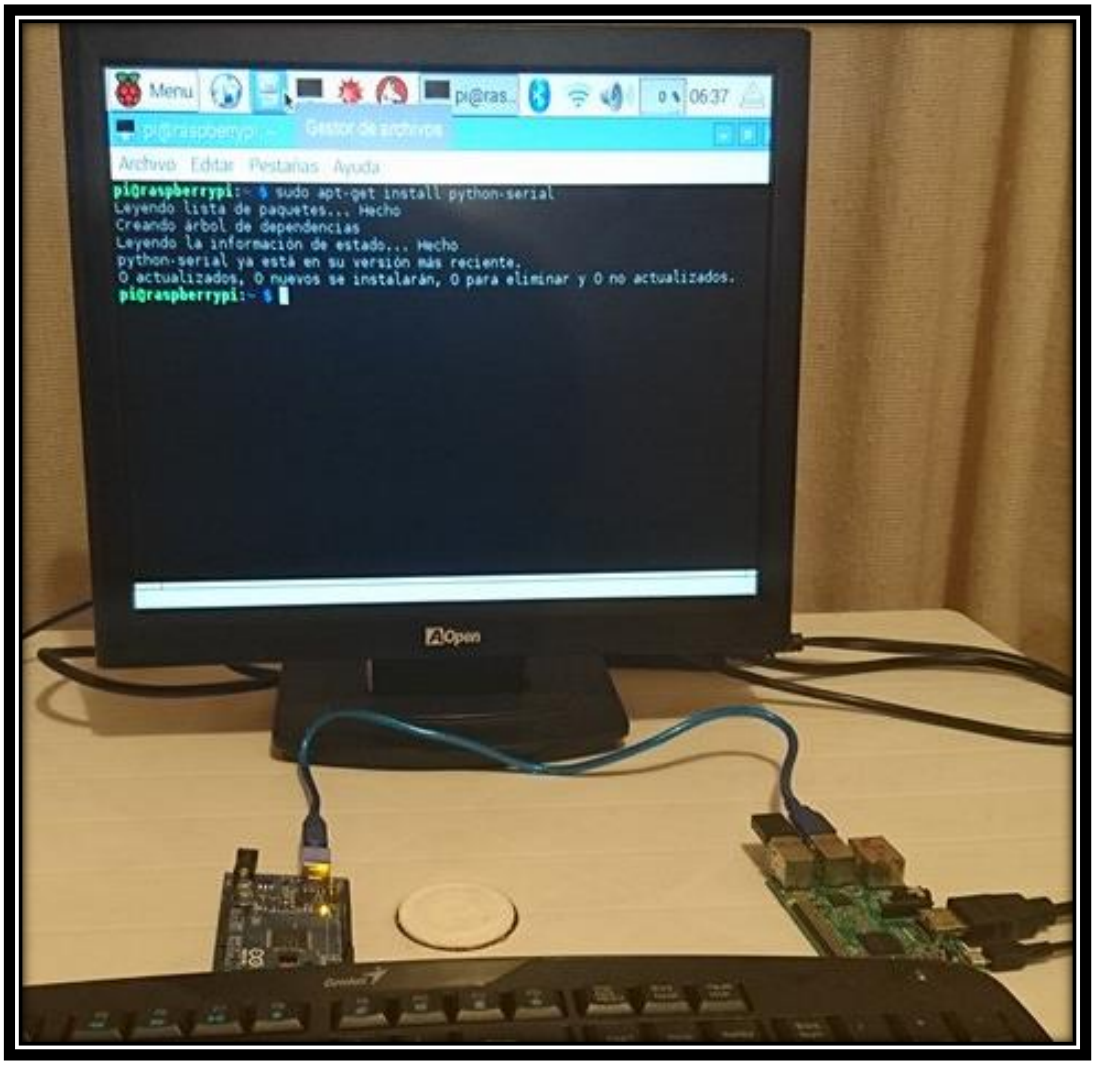


Figura 26 - 3 Levantamiento de la librería python-serial.

Realizado por: (Aguilar, 2017)

Una vez levantada la librería se procede a la creación del archivo de programación de python con extensión .py, para esto utilizamos la instrucción **nano** seguido del nombre del archivo que deseo guardar en este caso para el proyecto se crea Raspduino.py

nano Raspduino.py

Ingresada la línea de código en el terminal esta direcciona al IDE de programación de python donde se carga las instrucciones para realizar la lectura del puerto serial, donde se hallará la información que éste emitiendo el Arduino.

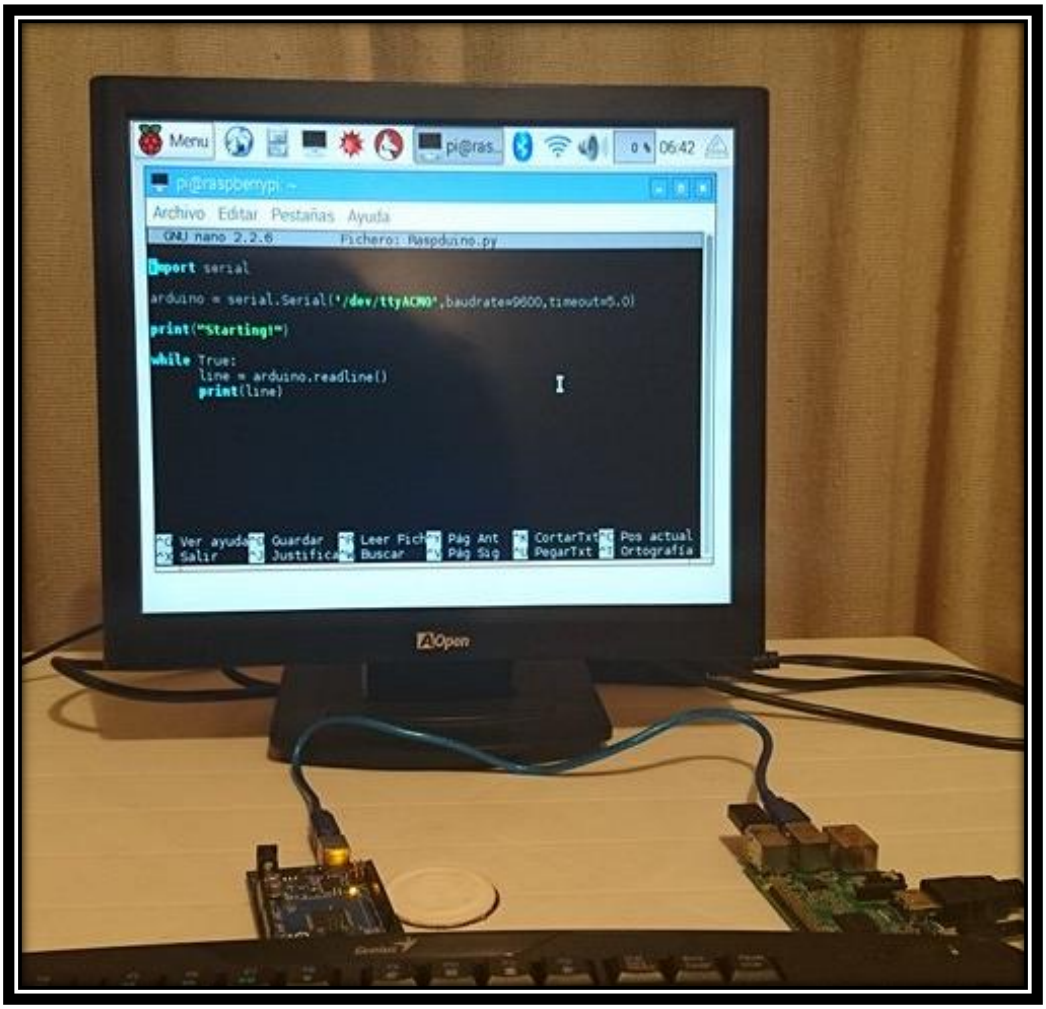


Figura 27 - 3 Programación Raspduino.py.

Realizado por: (Aguilar, 2017)

Las instrucciones manejadas para realizar la comunicación con Arduino se describen a continuación:

import *serial*

Arduino=serial.Serial('dev/ttyACM0, baudrate=9600, timeout=5.0)

Print("Starting")

While *True*

line=Arduino.realine()

print(line)

La programación parte de de importar la librería python-serial, luego se asigna una variable denominada Arduino donde se asigna el valor de la lectura del puerto serial facilitada por el dispositivo conectado al puerto en este caso por defecto al ttyACM0, se esta también la velocidad de comunicación y el tiempo de barrido al puerto.

Se imprime un mensaje de que el sistema arranco y procede a una estructura de repetición donde a una variable denominada line se monta el valor de la lectura de la variable Arduino para luego imprimirla y es lo que se tendrá en el terminal de la Raspberry.

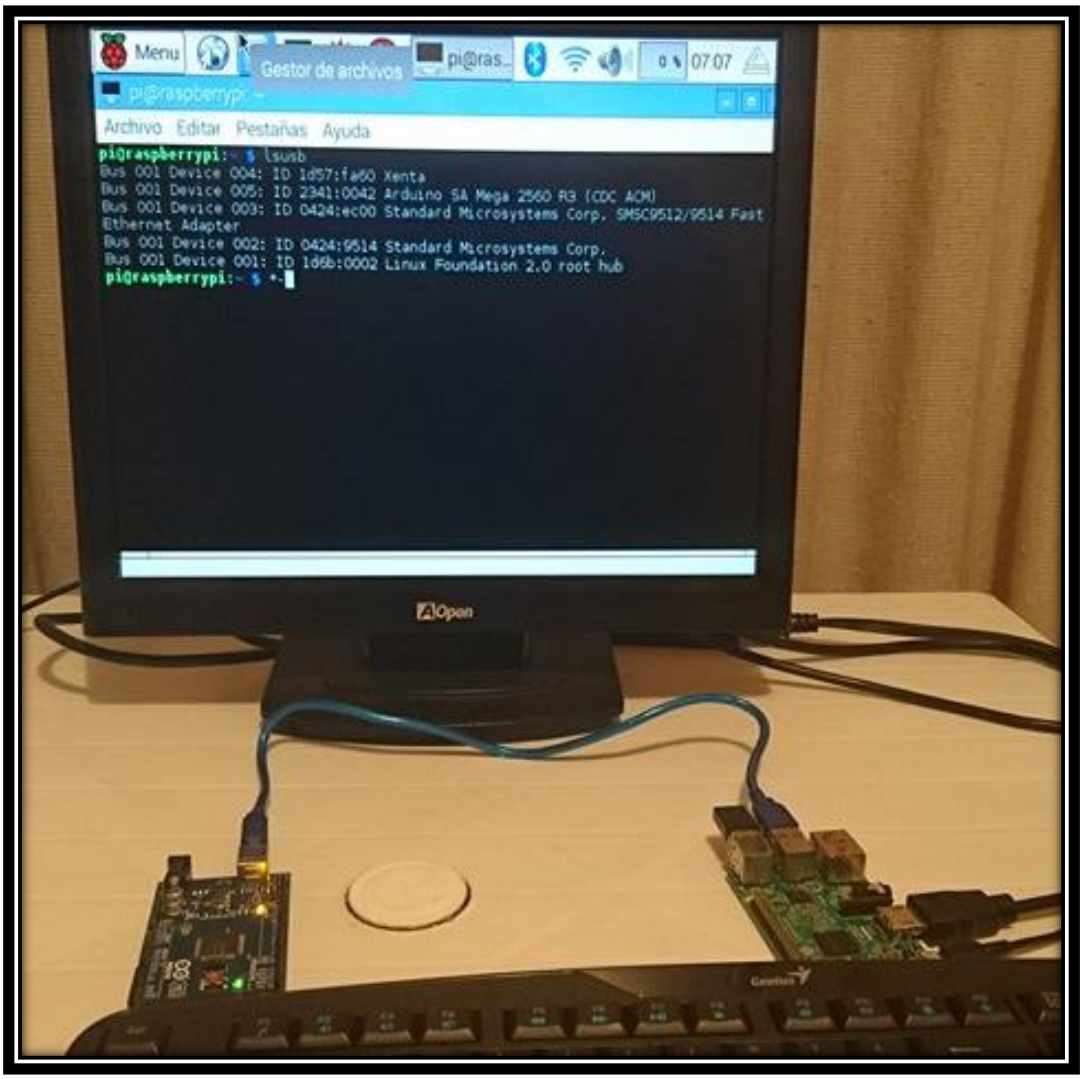


Figura 3 - 2 Lectura de puertos de la Raspberry

Realizado por: (Aguilar, 2017)

Previo a correr el programa de python se verifica que el microcontrolador reconocido por la Raspberry, para ellos utilizamos la sentencia ***lsusb*** y verificamos el COM en el que está conectado como se muestra en la Figura 3.28.

CAPITULO IV

4. IMPLEMENTACIÓN Y PRUEBAS

4.1. Conjunto residencial prototipo

Basados en los planos de la etapa de diseño se realiza la implementación de la maqueta a escala para la prueba del prototipo de alarma comunitaria.

Figura 1 - 4 Maqueta Conjunto residencial.

Realizado por: (Aguilar, 2017)

4.2. Implementación sistema de alarma domiciliaria

En base al diseño se centraliza por medio del microcontrolador Arduino MEGA 2650 los módulos de inserción de información (teclado), visualización (LCD i2C) y sensores de estado de los accesos (sensor de puerta, sensor de ventana) para en conjunto implementar el sistema de alarma propuesto.

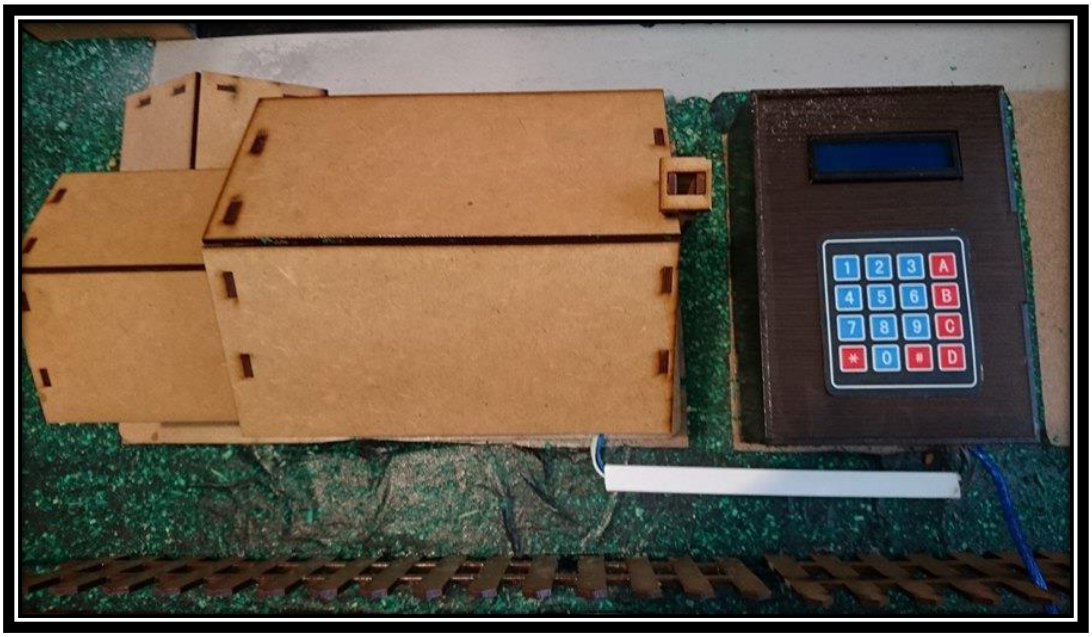


Figura 2 - 4 Sistema Individual de seguridad.

Realizado por: (Aguilar, 2017)

4.2.1. Conexión de sensores

La ubicación de los sensores para el control de una puerta y una ventana definidos como accesos a la vivienda se la realizó como se muestra en la figura 4.3.

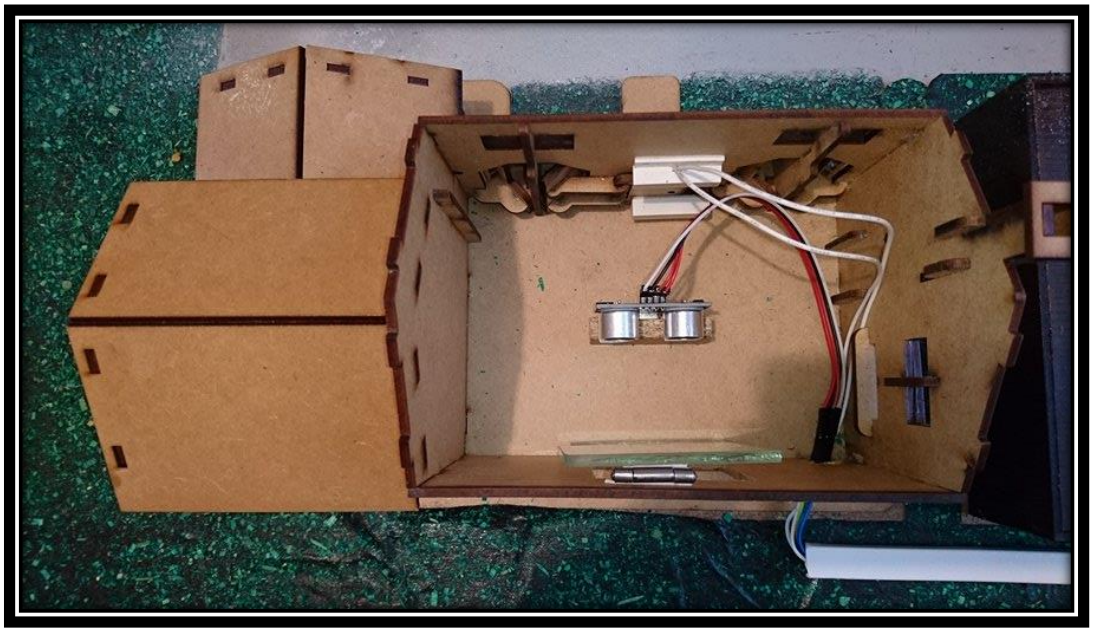


Figura 3 - 4 Instalación de sensores en accesos.

Realizado por: (Aguilar, 2017)

El sensor magnético está conectado a la puerta para que en su acción de apertura y cierre al variar el campo magnético del contacto éste ejecute los cambios de estado, de igual manera el sensor ultrasónico está conectado a cierta distancia de la ventana, distancia que en la programación del microcontrolador se la considera como normal, al variar esta distancia por acercamiento o alejamiento del cristal se considera como acceso violentado.

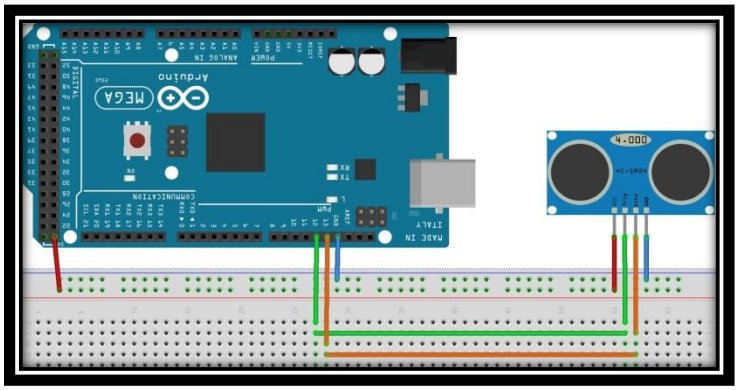


Figura 4 - 1 Conexión sensor ultrasónico al microcontrolador Arduino

Fuente: http://4.bp.blogspot.com/-UWmzFKvAy0g/VgMDhf1i4nI/AAAAAAAADrc/-0bAfYWlU_o/s1600/Untitled%2BSketch_bb.jpg

La figura 4. 4 describe la forma de conexión de los terminales del sensor ultrasónico hacia el microcontrolador.

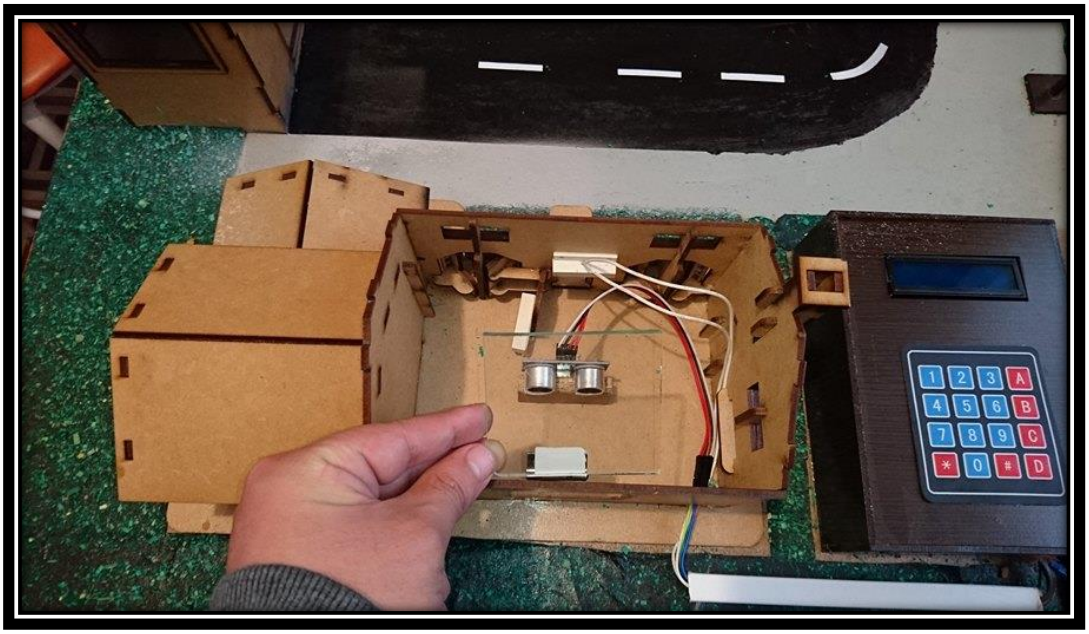


Figura 5 - 4 Accesos violentados

Realizado por: (Aguilar, 2017)

Con la apertura de puerta y ventana se evidencia el cambio de estado de los sensores que son señales que ingresaran al microcontrolador para ser procesadas.

4.2.2. Conexiones sistema de ingreso y visualización de la información al sistema de alarma

La figura 4.6 describe la conexión del teclado para la inserción de información hacia el microcontrolador para el procesamiento de la misma.

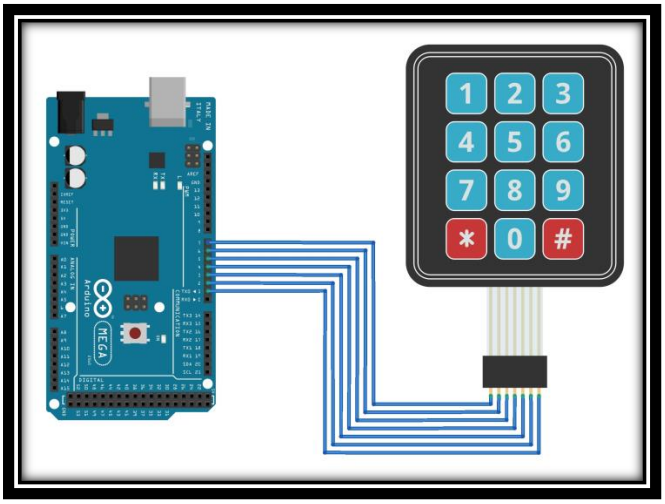


Figura 6 - 4 Conexión Arduino Teclado

Fuente: http://cdn.shopify.com/s/files/1/0557/2945/files/Diagrama_363fdb58-9ad7-4ec6-85a7-2c6c9f0c1b47.png?16039349023821380544

Para verificación de la información y visualización de mensajes de resultado del procesamiento del microcontrolador se añadió a la implementación según el diseño una etapa de visualización, la figura 4.7 evidencia las conexiones del lcd i2c hacia el Arduino.

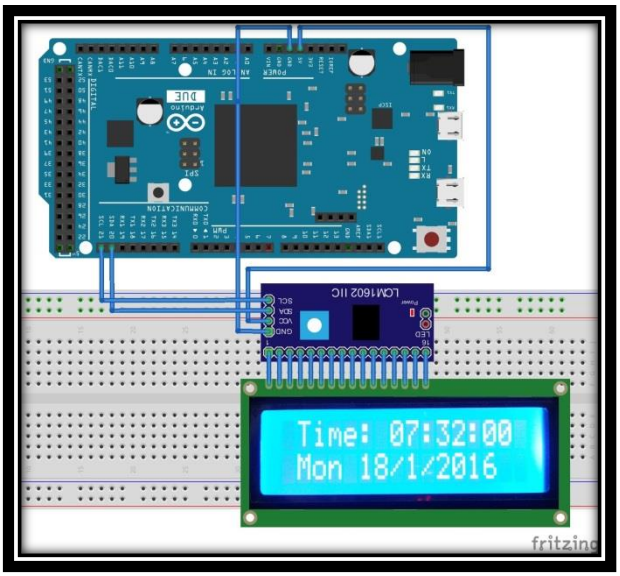


Figura 7 - 4 Conexión Arduino LCD i2C

Fuente: http://2.bp.blogspot.com/-I660lrDJRKw/Vp7ecyCQVkI/AAAAAAAAAHM/x-Zne92-PGI/s1600/Clock%2Band%2BCalendar%2Busing%2BArduino%2BDue%2BRTC_fritzing.jpg

La pantalla de la figura 4.8 describe el sistema armado donde la evaluación del cambio de estado de los accesos está activa, solicita la inserción de la clave de seguridad para desarmar el sistema.

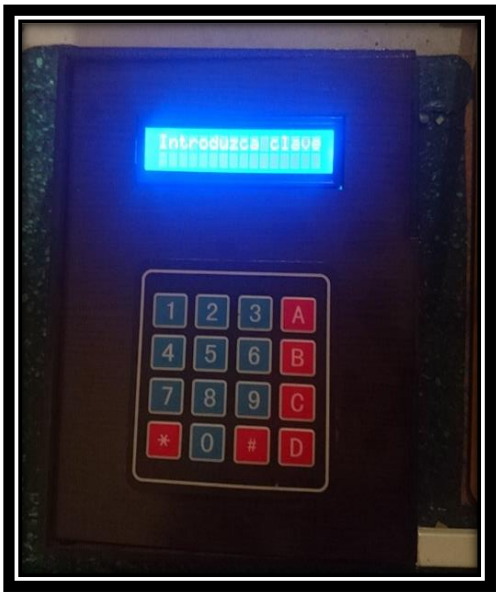


Figura 8 - 4 Pantalla de Autenticación

Realizado por: (Aguilar, 2017)

La figura 4.9 describe la pantalla posterior a haber ingresado correctamente la clave, donde la acción que se ejecuta es la suspensión del sistema de alarma, donde los sensores estarán cumpliendo su función de evaluar los accesos pero sus cambios de estado no serán considerados por el microcontrolador, hasta que el sistema se vuelva a armar.

Figura 9 - 4 Pantalla sistema de alarma desarmada

Realizado por: (Aguilar, 2017)

Al ingresar la clave erróneamente se considera también como una violación al sistema donde en la etapa de monitoreo se fijará un mensaje de alerta y en forma local se fijará el mensaje de clave incorrecta como se muestra en la figura 4.10.

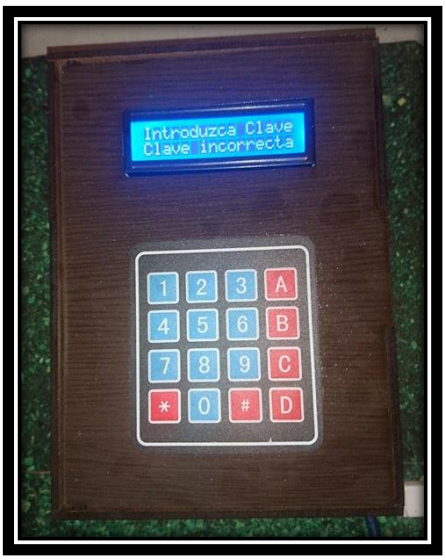


Figura 10 - 4 Pantalla clave mal ingresada.

Realizado por: (Aguilar, 2017)

Cabe mencionar que en el teclado dentro de la programación se puede añadir uno de sus botones como opción para activación de la alerta urgente o pánico.

4.2.3. Sistema de alerta GSM/GPRS

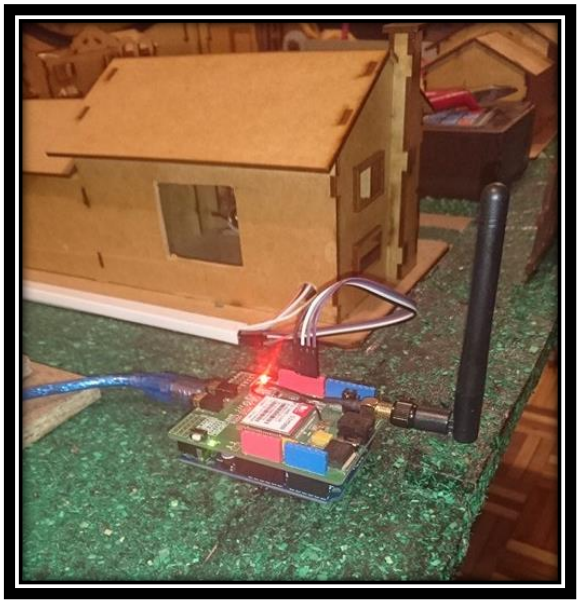


Figura 11 - 4 Modulo GSM/GPRS armados (Microcontrolador Arduino y Shield SIM900).
Realizado por: (Aguilar, 2017)

El sistema de alerta por GSM/GPRS como se fijó en el diseño está formado por un microcontrolador Arduino que interactúa con el Shield SIM900 por la interfaz UART por medio de códigos AT, la conexión que permiten las tarjetas es de montaje como se observa en la figura 4.8.

Cada residencia del conjunto contiene su propio sistema de alarma y de igual manera cada vivienda manejará una señal de sistema en estado normal o violentado, esto dos estados del sistema están también definidos en la programación como una salida digital del microcontrolador la misma que se conecta paralelamente a una entrada del Arduino del sistema de alerta GSM para ser procesada y en el caso de leer el estado de violentada esta emite un mensaje de texto al usuario propietario de la vivienda y al guardia del conjunto para la toma de acciones y decisiones sobre el suceso.

4.2.4. Monitoreo y Alertas

4.2.4.1. Montaje de la Red inalámbrica

Para el monitoreo de las residencias se utilizó un enlace por interfaz WIFI donde a cada Raspberry se le fijó una dirección ip en el formato v6 como aplicación del presente trabajo.

Para el prototipo se activó DHCPv6 al carecer de direcciones estáticas, donde cada residencia tiene su dirección la misma que es considerada como llave para el ingreso mediante acceso remoto.

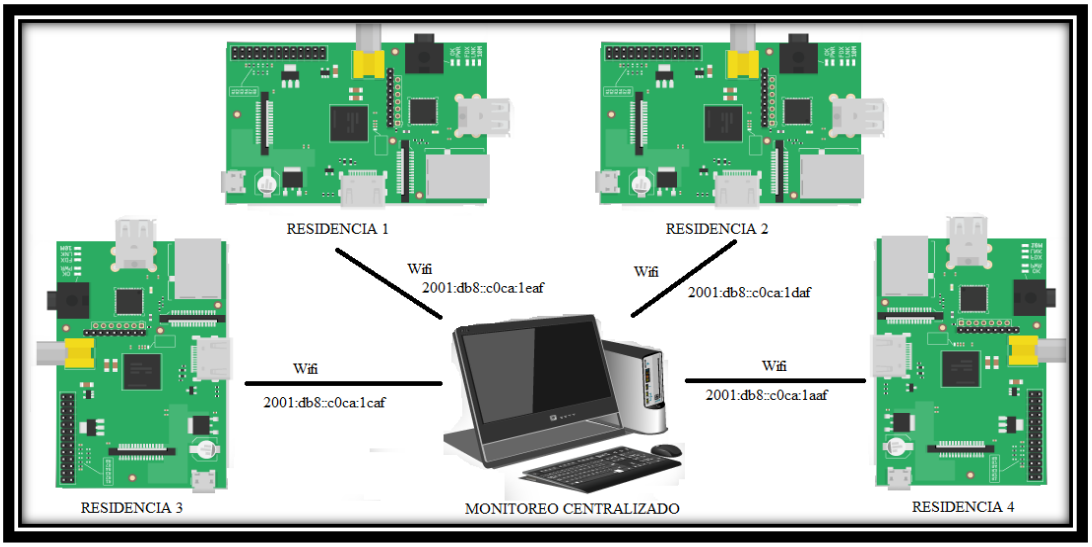


Figura 12 - 4 Red Inalámbrica con direccionamiento ipv6 – topología estrella

Realizado por: (Aguilar, 2017)

Para verificar la dirección ip en v6 se accede al terminal y se setea el comando:

Ifconfig

Donde se podrá acceder a la dirección ip para posteriormente registrarlo en el servidor VNC para el monitoreo remoto.

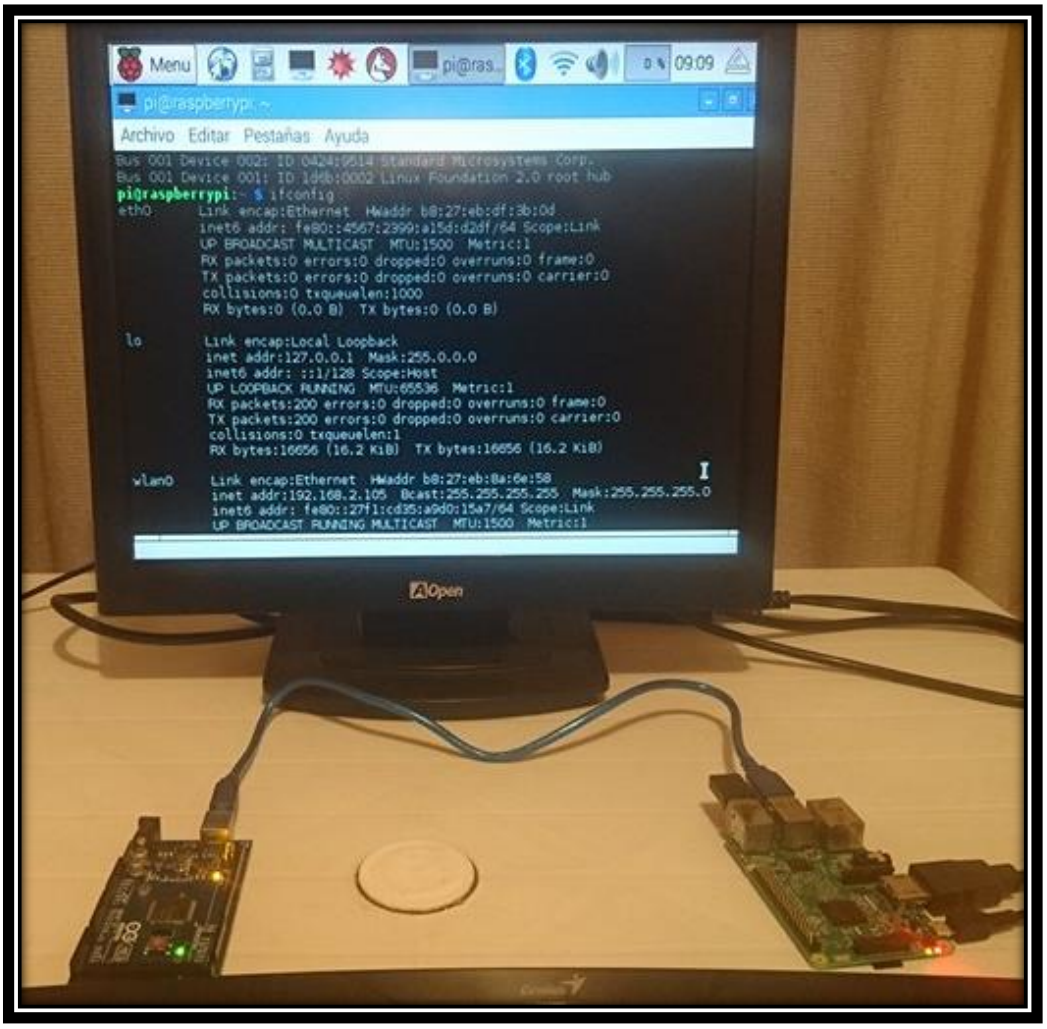


Figura 13 - 4 Terminal ifconfig

Realizado por: (Aguilar, 2017)

4.2.4.2. Comunicación Arduino – Raspberry

El microcontrolador Arduino por medio de la programación cargada previamente procesa las señales de los sensores de control de los accesos a las viviendas, realizando evaluaciones sobre el estado o valor de los mismos, además verifica el ingreso de la clave para activación y desactivación del sistema de alarma.

Los resultados de la evaluación y verificación descrita son impresos con mensajes de texto tanto al LCD como al puerto Serial del microcontrolador.

La comunicación es serial donde la Raspberry por medio del archivo generado Raspduino.py leerá la información que imprime el Arduino a su puerto serial. En la figura 4.10 se diagrama la comunicación entre los dos dispositivos base del prototipo.

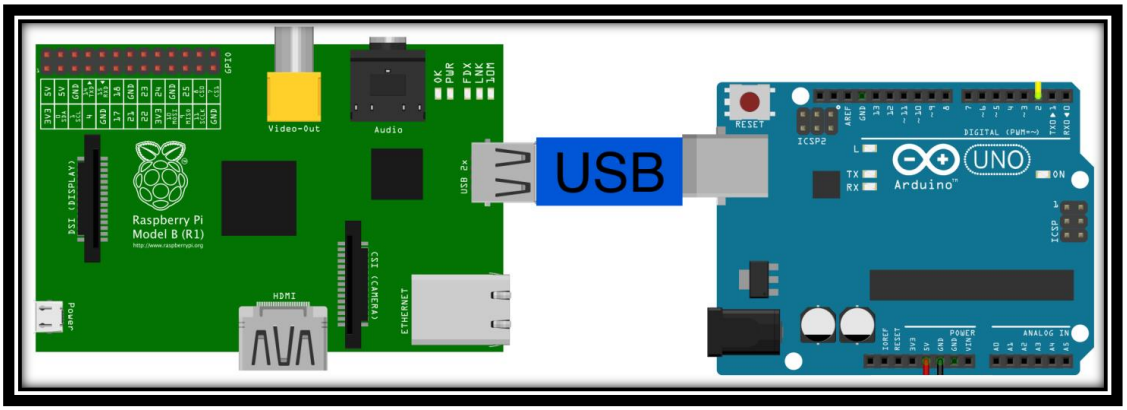


Figura 14 - 2 Comunicación serial Arduino - Raspberry

Fuente: http://booleanbite.com/web/wp-content/uploads/2015/10/iotIII.png

Una vez enlazados Arduino – Raspberry se levanta el servicio VNC para el monitoreo remoto como se lo indico en el apartado 3.4.2.3

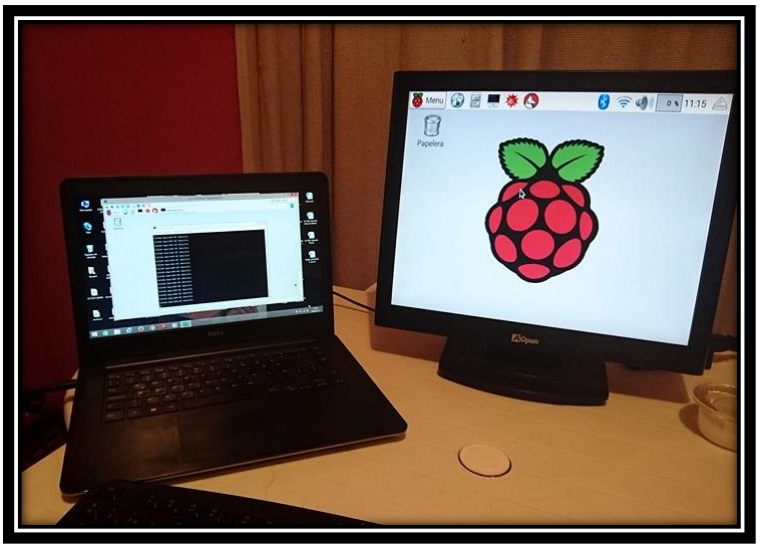


Figura 15 - 4 Acceso remoto al escritorio de la Raspberry

Realizado por: (Aguilar, 2017)

El monitoreo remoto se lo aplicará tanto para el sistema de vigilancia local desde la garita de seguridad del conjunto así como también se dota la posibilidad de realizar un monitoreo remoto por medio de tecnología GSM, es decir desde cualquier teléfono celular.

La figura 4.16 y 4.17 muestran las pantallas de monitoreo remoto en el que la actualización del estado del sistema es dado en tiempo real señalando por ejemplo dos de los estados del sistema, Armado y Violentado ya definidos en apartados anteriores.

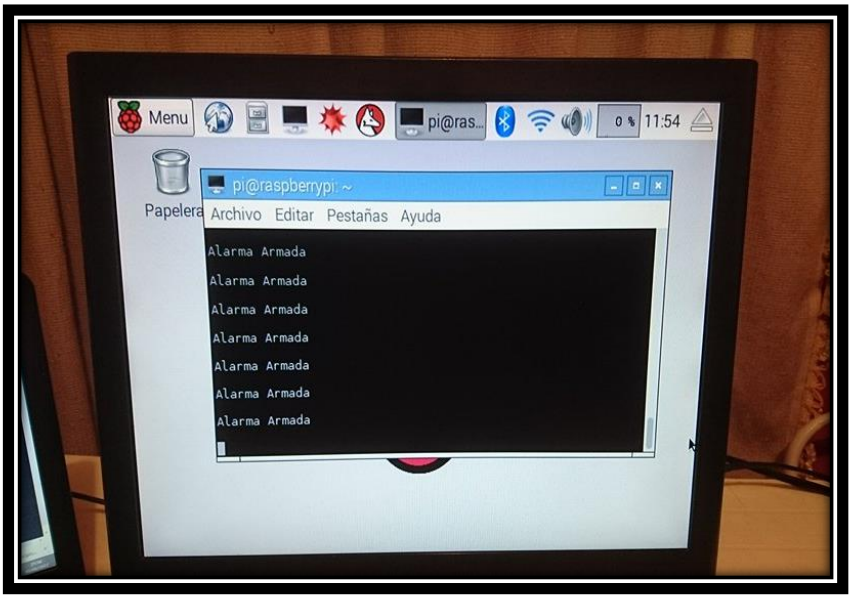


Figura 16 - 4 Monitoreo remoto sistema armado.

Realizado por: (Aguilar, 2017)

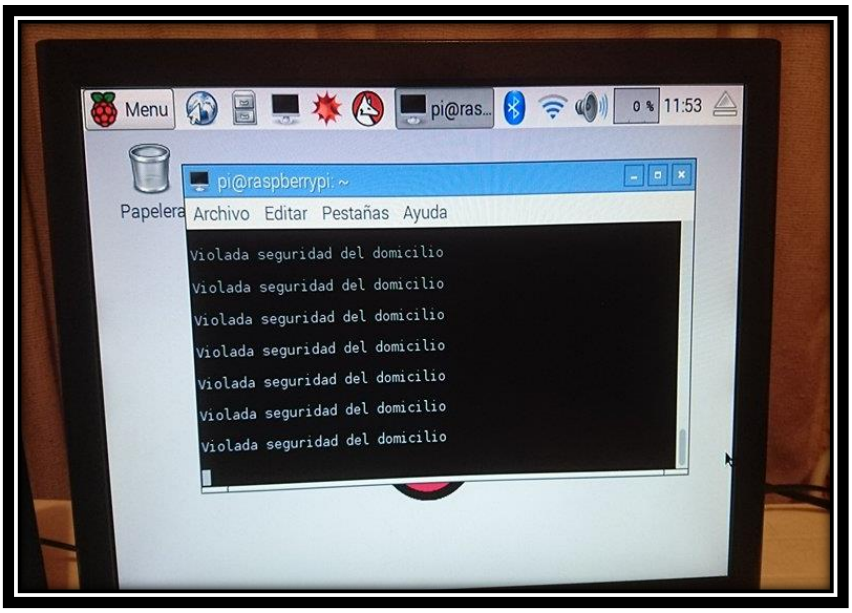


Figura 17 - 4 Acceso remoto alerta sistema violentado.

Realizado por: (Aguilar, 2017)

Dando cumplimiento a los requerimientos planteados en el diseño se implementa el acceso remoto desde un dispositivo de comunicación móvil haciendo uso de la App VNC Viewer como se muestra en la figura 4.18.

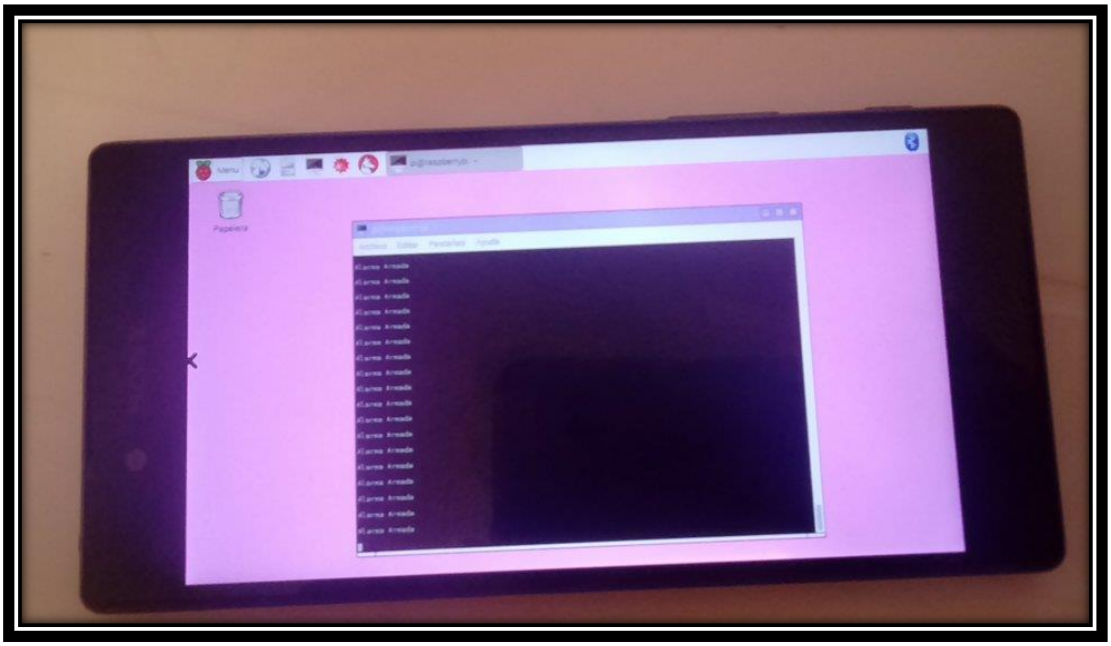


Figura 18 - 4 Monitoreo remoto dispositivo móvil.

Realizado por: (Aguilar, 2017)

CONCLUSIONES

En mira de vencer la frontera tecnológico-científica con la inserción de tecnologías para la mejora de los procesos como menciona el objetivo 10 del plan nacional del buen vivir, se logró implementar con éxito el prototipo de alarma multimodal comunitaria utilizando el protocolo IPv6 y GPRS para Smart Cities con monitoreo en tiempo real.

En mercado dispositivos con soporte de direccionamiento ipv6 para control de procesos de fácil acceso y costo bajo fueron el módulo de Ethernet de Arduino y Raspberry Pi3, siendo la Raspberry la de mayor número de recursos, uno de ellos el poseer interfaz Wi-fi a diferencia del Shield de Arduino que requiere cable.

El uso de direccionamiento ipv6 expande la cantidad de direcciones por su estructura plana, lo que permite cubrir mayor cantidad de puntos, este caso el sistema no tendría inconveniente a la hora de implementarse en grandes conjuntos habitacionales.

El objetivo 3 del Plan Nacional del buen vivir menciona mejorar la calidad de vida de la población, lo que le da valor al prototipo implementado al dar solución al problema de seguridad en los domicilios de un conjunto habitacional.

El uso de tecnología GSM facilita el monitoreo de las residencias desde cualquier lugar con cobertura en el que el usuario se encuentre, a su vez permite el modo de alertas silenciosas que permitirán una acción más oportuna para aprensión de invasores.

RECOMENDACIONES

Para la implementación del sistema con forma de monitoreo expandido se requiere asignación de direcciones ip estáticas, para modelo del prototipo se empleó una LAN lo que limita al prototipo al monitoreo dentro del área.

Promocionar el sistema de alarma comunitaria para que pueda ser reproducido a escala y no se quede en el nivel de prototipo.

BIBLIOGRAFÍA.

1. **ÁLVAREZ, Yelitza.** Seguridad al acceso de información en la implantación de una red inalámbrica. **(TESIS MAESTRÍA).** Universidad Central de Venezuela. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Especialización de Comunicaciones y Redes de Datos. Caracas-Venezuela. 2006, pp. 16. [Consultado el: 2016-11-15]. Disponible en: http://saber.ucv.ve/xmlui/bitstream/123456789/2420/1/Tesis%20yelitza%20Alvarez.pdf

2. **CHAVEZ, Tatiana & TORRES, Ana.** *Desarrollo de una Red de Sensores Inalámbrica Sustentable mediante el Protocolo IEEE 802.15.4 para determinar la calidad de Agua en Pinllo.* **(TESIS PREGRADO).** Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Escuela de Ingeniería Electrónica en Telecomunicaciones y Redes. Riobamba-Ecuador. 2015, pp. 50-53.

3. **CONSULINTEL**. Segunda edición. Madrid -España. Tutorial de IPV6. 2010, pp. 90. [Consultado el: 2016-12-20]. Disponible en: http://www.consulintel.es/html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

4. **DOMÍNGUEZ MARTÍN, Hugo; & SÁEZ VACAS, Fernando.** Domótica: Un enfoque socio técnico. Madrid: Fundación Rogelio Segovia. 2006, pp. 33-50

5. **GONZALES DOMÍNGUEZ, CLAUDIO.** Aplicaciones orientadas a la domótica con Raspberry Pi. Departamento de Ingeniería Electrónica Escuela Técnica Superior de Ingeniería. Universidad de Sevilla. 2005, pp. 20-29

6. **GARCIA, Lenin; & LOGROÑO, Santiago.** *Diseño e Implementación de un Kiosco Tecnológico mediante el uso del Protocolo IEEE 802.11x para los Estudiantes de la Escuela de Ingeniería Electrónica en Telecomunicaciones y Redes de la ESPOCH.* **(TESIS PREGRADO).** Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Escuela de Ingeniería Electrónica en Telecomunicaciones y Redes. Riobamba-Ecuador. 2015, pp. 50-53.

7. **HERRADOR, R. E.** Guía de Usuario Arduino. 2009, pp. 8-10.

8. **LÓPEZ GARCÍA, Nancy; & PEDRAZA, Luis F.** Modelo para la integración de redes IPv4-IPv6 basado en túneles. Tecnura, tecnología y cultura afirmando el conocimiento. 2000, pp. 52-53.

9. **NOGALES, ADRIÁN**. La Domótica como Solución del Futuro. Madrid. 2007, pp. 66-120

10. **O`FLAHERTY, CHRISTIAN.** IPv6 PARA TODOS guía de uso y aplicación para diversos entornos. Buenos Aires, Argentina: ISOC.Ar Asocicion Civil de Argentinos en internet. 2009, pp. 80-90

11. **PROYECTO WNDW.** Redes Inalámbricas en los Países en Desarrollo. Cuarta Edición ed. Gran Bretaña: Hacker Friendly LLC. 2006, pp. 114-150.

12. **PEREZ, Sonia; & LOZADA, Vázquez.** Integración Wi-fi en un proyecto ICT. **(TESIS PREGRADO).** Universidad Politécnica de Madrid. Escuela Universitaria de Ingeniería Técnica de Telecomunicación. Ingeniería de Sistemas de Telecomunicación. Madrid-España. 2012, pp. 17. [Consultado el: 2016-11-15]. Disponible en: http://oa.upm.es/14224/1/TFG_SONIA_PEREZ_VAZQUEZ_LOSADA.pdf

13. **PAREDES, I.** *Análisis comparativo de las placas Arduino (oficiales y compatibles)*. Italia. 2014, pp. 60-80. [Consultado el: 2016-07-15] Disponible en: http://comohacer.eu/analisis-comparativo-placas-arduino-oficiales-compatibles/.

14. **SÁNCHEZ AHUATZIN, G. L**. Teoría y Métodos de Transición IPv4 e IPv6. México. 2005, pp. 75-90

15. **STALLINGS, W.** Comunicaciones y Redes de Computadores. Granada: Prentice Hall. 2000, pp. 49-70.

16. **UPTON EBEN, G. H.** Raspberry Pi Guía de Usuarios. 2017, pp. 55-75

17. **VALERA, A.J**. Introducción a la Domótica. Murcia-España: Germán Villalba. 2009, pp. 65-70.