UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA INGENIERÍA

CARRERA DE INGENIERÍA EN TELEMÁTICA

Proyecto de Investigación previo a la obtención del título de Ingeniera en Telemática.

Título del Proyecto de Investigación:

"SISTEMA DE SEGURIDAD INTEGRAL DE UNA VIVIENDA CONTROLADA VIA REMOTA"

Autora:

Carmen Amparo Hernández Ordinola

Director de Proyecto:

Ing. Jaime Macías Romero, M.Sc

Quevedo – Los Ríos – Ecuador

2015

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA INGENIERÍA

CARRERA DE INGENIERÍA EN TELEMÁTICA

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

Yo, **Carmen Amparo Hernández Ordinola,** declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Técnica Estatal de Quevedo, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

f. _____
Carmen Amparo Hernández Ordinola

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA INGENIERÍA

CARRERA DE INGENIERÍA EN TELEMÁTICA

CERTIFICACIÓN DE CULMINACIÓN DEL PROYECTO DE INVESTIGACIÓN

El suscrito, **Ing. Jaime Macías Romero, M.Sc,** Docente de la Universidad Técnica Estatal de Quevedo, certifica que la estudiante **Carmen Amparo Hernández Ordinola**, realizó el Proyecto de Investigación de grado titulado **"SISTEMA DE SEGURIDAD INTEGRAL DE UNA VIVIENDA CONTROLADA VIA REMOTA"**, previo a la obtención del título de **INGENIERA EN TELEMÁTICA**, bajo mi dirección, habiendo cumplido con las disposiciones reglamentarias establecidas para el efecto.

……..……..

Ing. Jaime Macías Romero, M.Sc

DIRECTOR DE PROYECTO

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA INGENIERIA

CARRERA INGENIERIA EN TELEMATICA

CERTIFICACIÓN DE REDACCIÓN

Yo, **TEDY DE LA CRUZ** con CC Nº. **0910481522**, Docente de la Facultad Ciencias de la Ingeniería de la Universidad Técnica Estatal de Quevedo, certifico que he revisado el proyecto de investigación de la egresada **Carmen Amparo Hernández Ordinola**, **No. de cédula 171835726-0**, previo a la obtención del título de Ingeniera en Telemática, titulado **"SISTEMA DE SEGURIDAD INTEGRAL DE UNA VIVIENDA CONTROLADA VIA REMOTA",** habiendo cumplido con la redacción y corrección ortográfica.

f. _____

Socióloga. Tedy de la Cruz

DOCENTE DE REDACCIÓN

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA INGENIERÍA

CARRERA DE INGENIERÍA EN TELEMÁTICA

PROYECTO DE INVESTIGACION

Título:

"Sistema de seguridad integral de una vivienda controlada vía remota"

Presentado a la Comisión Académica como requisito previo a la obtención del título de Ingeniera en Telemática.

Aprobado por:

_____

PRESIDENTE DEL TRIBUNAL DE TESIS
ING. JUAN CARLOS PISCO

MIEMBRO DEL TRIBUNAL DE TESIS	**MIEMBRO DEL TRIBUNAL DE TESIS**
ING. EMILIO ZHUMA MERA, M.Sc	ING. VICTOR NASIMBA MEDINA

QUEVEDO – LOS RÍOS – ECUADOR

2015

AGRADECIMIENTO

Gracias infinitas a Dios por permite culminar con éxito otra etapa más de mi vida. A mis Padres Renán y Amparito por brindarme los mejores valores que me han formado como una persona de carácter, apoyándome en los buenos y malos momentos que me ha tocado sobrellevar.

A mi querida hermana Liseth quien siempre a estado a mi lado amiga, hermana y compañera de vida; por sus consejos, apoyo y estimulo recibido desde siempre, a mis dos hermanos Alexandrita y Renancito aunque ellos no están conmigo se que desde el cielo me iluminan. Gracias a mis demás familiares por toda su estima y comprensión.

Gracias a la Universidad Técnica Estatal de Quevedo, por permitir forjar mis conocimientos impartidos dentro de las aulas de clase, a los docentes, y demás autoridades que logran mejorar cada día la calidad de la educación superior.

A todos muchísimas gracias.

Carmen Amparo Hernández Ordinola.

DEDICATORIA

El presente proyecto de tesis se lo dedico a mi hijo Ronny y a mi esposo Ronald, por toda la paciencia, cariño y amor que me demuestran día a día. A mis padres y a mi hermana. A mis queridos amigos y compañeros de clases con quienes compartimos grandes momentos inolvidables, los cuales jamás olvidaré.

Carmen Amparo Hernández Ordinola.

RESUMEN

El empleo de la tecnología como recurso de ayuda en las actividades cotidianas se ha convertido en una pieza fundamental para la sociedad; es así que se la utiliza para enviar/recibir información hasta el uso de aplicaciones avanzadas de todo tipo. En el presente proyecto investigativo se desarrolla un sistema de seguridad integral basado en microprocesadores, un router que deberá ser configurado para que permita la comunicación entre la cámara IP[1] y el dispositivo móvil para lograr observar todo lo que ocurre a través de la misma, además de que se diseñará una aplicación de escritorio remoto que también realizará las funciones de control y monitoreo del sistema de seguridad de la vivienda. El usuario podrá monitorear en tiempo real vía Streaming lo que sucede dentro del inmueble gracias a que se le asigna una dirección IP pública. Todo este sistema está comprendido por: sensores de movimientos, sensores de vibración, cámaras, sensores de humo y alarma de pánico que sirven como recurso de advertencia al propietario de la casa. Además de que le permitirá al dueño de casa estar al tanto mediante la recepción de mensajes de texto como método de aviso siempre y cuando exista movimiento cualquier circunstancia inusual o que cualquier intruso quiera acceder al inmueble.

Palabra claves:

Electrónica, Seguridad, Domótica

[1] Protocol Internet. Protocolo de Internet que permite la conexión a internet

ABSTRACT

The use of technology as a source of assistance in daily activities it has become a fundamental part for the society; it is so that uses from to send or receive information to the use of all kinds advanced applications. In the present research project develops a comprehensive security system based on two microprocessors, a router must be configured to allow the communication between the IP and mobile device to achieve observe everything that goes through the same, plus a remote desktop application that also perform the functions of control and monitoring of the security system of housing design. The user can monitor in real time via Streaming what happens inside the building because it assigns a public IP address. This whole system is comprised of: motion sensors, vibration sensors, cameras, smoke detectors and panic alarm serving as a resource for warning the owner of the house. Plus it will allow the homeowner to be aware by receiving text messages as a method of notice provided there is movement or any unusual circumstances that any intruder wants access to the property.

Key words:

Electronic, Security, Domotic.

ÍNDICE DE CONTENIDO

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS ii
CERTIFICACIÓN DE CULMINACIÓN DEL PROYECTO DE INVESTIGACIÓN iii
CERTIFICACIÓN DE REDACCIÓN iv
APROBACIÓN DEL TRIBUNAL DE TESIS v
DEDICATORIA vii
RESUMEN viii
ABSTRACT ix
ÍNDICE DE FIGURAS xiii
ÍNDICE DE CUADROS xv
ÍNDICE DE TABLAS xvi
CÓDIGO DUBLÍN xvii
INTRODUCCIÓN 1
CAPÍTULO I 3
CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN 3
1.1. Problema de la Investigación. 4
1.1.1. Planteamiento del problema. 4
1.1.1.1. Diagnóstico del problema. 4
1.1.1.2. Pronóstico del problema. 4
1.1.2. Formulación. 4
1.1.3. Sistematización del problema. 5
1.2. Objetivos. 5
1.2.1. Objetivos Generales. 5
1.2.2. Objetivos específicos. 5
1.3. Justificación. 5
CAPÍTULO II 7
FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN 7
2.1.1. Usuarios móviles. 8
2.1.2. Redes de ejemplo. 8
2.1.3. Redes de teléfonos móviles de tercera generación. 9

2.1.4. Transmisión inalámbrica. 10
2.1.5. El sistema de telefonía móvil. 10
2.1.6. GSM – El sistema global para comunicaciones móviles. 11
2.1.7. Protocolos de Internet. 12
2.1.8. Métodos de acceso a redes. 12
2.1.8.1. Módems. 12
2.1.9.1. Soportes limitados. 13
2.1.9.2. Conectores. 15
2.1.10. Arquitectura centralizada. 16
2.1.11. Arquitectura descentralizada. 17
2.1.12. Sistemas de control y monitoreo. 17
2.1.13. Sistemas Inalámbricos. 17
2.1.14. Sistemas con Cableado. 18
2.1.15. Circuito Cerrado. 18
2.1.16. Dispsositivos para los sistemas de seguridad. 18
2.1.16.1. Teclado Matricial. 18
2.1.16.2. El rele. 19
2.1.16.2.1. Reles más utilizados. 20
2.1.16.3. Sensores. 20
2.1.16.4. Sensores de movimiento. 20
2.1.16.5. Sensor de vibración. 21
2.1.16.6. Sensor de humo. 22
2.1.16.7. Sensor magnético. 22
2.1.16.8. Botón de pánico. 23
2.1.17. Equipos de programación. 24
2.1.17.1. Arduino. 24
2.1.17.2. Formas de Conexionado de entradas y salidas. 25
2.1.17.3. Expandir Arduino con los shields. 26
2.1.17.4. Placa Arduino y sus partes. 26
2.1.18. Raspberry PI. 28

2.1.18.1. Noobs para Raspberry. 29
2.2. Marco Referencial. 30
2.2.1. Sistema de Seguridad Domiciliaria. 30
2.2.2. Diseño de sistema electrónico antiintrusos para viviendas individuales. 31
2.2.3. Diseño y Simulación de un Sistema Domótico para una vivienda. 31
CAPÍTULO III 32
METODOLOGÍA DE LA INVESTIGACIÓN. 32
3.1. Localización. 33
3.2. Tipo de investigación. 33
3.3. Métodos de investigación. 34
3.4. Fuentes de recopilación de información. 34
3.4.1. Fuentes primarias. 34
3.4.2. Fuentes secundarias. 34
3.5. Diseño de la investigación. 35
3.6. Instrumentos de investigación. 35
3.7. Recursos humanos y materiales. 36
3.7.1. Recursos humanos. 36
3.7.2. Materiales. 36
CAPÍTULO IV 37
RESULTADOS Y DISCUSIÓN 37
4.1. Resultados. 38
4.2. Discusión. 58
CAPÍTULO V 60
CONCLUSIONES Y RECOMENDACIONES 60
5.1. Conclusiones. 61
5.2. Recomendaciones. 62
CAPÍTULO VI 63
BIBLIOGRAFÍA 64
CAPÍTULO VII 67
ANEXOS 67

ÍNDICE DE FIGURAS

Fig. 1 Diseño Celular de una Red de telefonía Celular 10
Fig. 2 Arquitectura de la red de telefonía GSM. 11
Fig. 3 Router marca Dlink 13
Fig. 4 Cable de pares trenzados 14
Fig. 5 Cable STP 15
Fig. 6 Cable FTP 15
Fig. 7 Conector RJ-45 16
Fig. 8 Arquitectura centralizada 16
Fig. 9 Arquitectura descentralizada 17
Fig. 10 Código de activación teclado 18
Fig. 11 Diagrama de funcionamiento teclado 19
Fig. 12 Simbolo y partes de un relé de armaduras 19
Fig. 13 Tipos de reles 20
Fig. 15 Sensor - detector de movimiento Niessen 21
Fig. 16 Sensor de vibración para viviendas 21
Fig. 17 Sensor de vibración para viviendas 22
Fig. 17 Contacto mágnetico pesado para portones o garaje 22
Fig. 18 Contacto Magnético para portones o garaje 23
Fig. 19 Contacto Magnético Instalado en puerta 23
Fig. 21 Botón de pánico 24
Fig. 22 Placa de Arduino 24
Fig. 23 Interfaz de inicio 25
Fig. 24 Salida digital 25
Fig. 25 Entrada digital 25
Fig. 27 Entrada conectada a resistencia variable (Entrada analógica) 26
Fig. 28 Tipos de adaptaciones para Arduino 26
Fig. 29 Vista frontal de la placa 27
Fig. 30 Vista trasera y superior 27
Fig. 31 Placa Raspberry PI 28

Fig. 32 Partes de la Placa Raspberry PI 28
Fig. 31 Instalacion de Noobs 29
Fig. 32 Instalacion de Raspberry 30
Fig. 33 Instalacion de Raspberry 30
Fig. 34 Mapa de ubicación de la UTEQ. 33
Fig. 35 Plano de ubicación de los elementos del sistema de seguridad integral 40
Fig. 36 Ingreso al modo de configuración para el servidor y asignación de la IP para la cámara 42
Fig. 37 Configuración para el servidor y asignación de la IP 42
Fig. 38 Asignación de la IP para la cámara 43
Fig. 39 Acceso al software para el diseño de la aplicación 43
Fig. 40 Escritorio del Sistema Operativo 44
Fig. 41. Pantalla de carga de la Raspberry 44
Fig. 42 Raspberry iniciada 45
Fig. 43 Interfaz para el diseño de la aplicación de Escritorio 45
Fig. 44 Asignando características para el lenguaje de programación de la Raspberry PI 46
Fig. 45 Código generado al inicio de la aplicación 46
Fig. 46 Asignando botones y funciones para la aplicación 47
Fig. 47 Código generado por cada botón y función para la aplicación 47
Fig. 48 Interfaz preliminar de la aplicación de escritorio 48
Fig. 49 Interfaz ejecutada 48

ÍNDICE DE CUADROS

Cuadro 1. Líneas de código para los sensores de movimiento 49
Cuadro 2. Líneas de código para el sensor de Humo 50
Cuadro 3. Línea de código para el botón de pánico 51
Cuadro 4. Líneas de código para el acceso y autenticación 52
Cuadro 5. Líneas de código para que el usuario pueda cambiar la contraseña de acceso 55
Cuadro 6. Líneas de código para los sensores magnéticos de apertura de puertas 56

ÍNDICE DE TABLAS

Tabla 1. Presupuesto 36
Tabla 2. Comparativa de características de sistemas electrónicos programables 38
Tabla 3. Características de sistemas de seguridad 39
Tabla 4. Costos de sistemas de seguridad 40

CÓDIGO DUBLÍN

Título:	"Sistema de seguridad integral de una vivienda controlada vía remota"		
Autor:	Carmen Amparo Hernández Ordinola		
Palabras clave:	Electrónica	Seguridad	Domótica
Fecha de publicación:	17/12/2015		
Editorial:	Quevedo: UTEQ, 2015.		
Resumen: **(hasta 300 palabras)**	Resumen.-. El empleo de la tecnología como recurso de ayuda en las actividades cotidianas se ha convertido en una pieza fundamental para la sociedad; es así que se la utiliza desde para enviar/recibir información hasta el uso de aplicaciones avanzadas de todo tipo. En el presente proyecto investigativo se desarrolla un sistema de seguridad integral basado dos micoprocesadores, un router que deberá ser configurado para que permita la comunicación entre la cámara IP, y el dispositivo móvil Smartphone mediante una aplicación instalada en el mismo, además de que se diseñará (…). **Abstract. - The use of technology as a source of assistance in daily activities it has become a fundamental part for the society; it is so that uses from to send or receive information to the use of advanced applications of all kinds. In the present research project develops a comprehensive security system based on two microprocessors, a router must be configured to allow the communication between the IP and the camera and Mobile Smartphone device through an installed application on the same, Additionally to a remote desktop application that will also perform the same functions as the smartphone device will be designed. (…).**		
Descripción:	104 hojas : dimensiones, 29 x 21 cm + CD-ROM		
URI:			

INTRODUCCIÓN

En la actualidad el uso de la tecnología es amplio y variado en cuanto a aplicaciones para dispositivos utilizados en el hogar mediante el control de acciones específicas de los aparatos electrónicos, para la vigilancia y seguridad e inclusive realizar operaciones mediante robots maniobrados desde otro lugar del mundo. Ahora bien existen aplicaciones que involucran el uso de dispositivos electrónicos permiten a las personas manipularlos de manera que se adapten a sus actividades cotidianas. Pensando en estas necesidades y haciendo uso de la tecnología que actualmente se encuentra disponible, da hincapié a que se genere la posibilidad de desarrollar sistemas de seguridad que permita a los propietarios tener un control total de su domicilio.

En el mercado existen cientos de dispositivos electrónicos de vigilancia y seguridad los cuales permiten a los propietarios de las viviendas tener un mayor control y mantener la casa totalmente segura; los mismos que a su vez al estar conectados a una central de control (esta puede ser dentro del hogar o mediante algún dispositivo móvil) el dueño de casa pueda monitorear lo que sucede dentro de ella o cuando algún intruso quiera acceder a ella o inclusive cualquier acontecimiento extraño que existiera en algún lugar determinado de la misma.

En el presente trabajo de investigación se pretende diseñar un sistema integral en el cual se instalarán diferentes dispositivos de seguridad (sensor de movimiento, sensores magnéticos, cámaras, sensor de humo, entre otros) en puntos estratégicos, además del desarrollo de una aplicación para smartphone que permita acceder a las cámaras de vigilancia y una aplicacionde escritorio remoto para los dispositivos de la casa mediante la asignación de una dirección IP pública permitiéndole estar al tanto de todo el sistema integral de seguridad vía remota.Este proyecto se ha dividido en siete capítulos, los cuales para su mayor comprensión, se describen a continuación:

En el Capítulo I se realiza una introducción al trabajo investigativo realizado, enmarcándose en el uso de los dispositivos electrónicos y su uso en sistemas de seguridad, además del planteamiento de los objetivos, problematización y la justificación de este proyecto.

En el Capítulo II se describen conceptos básicos y técnicos para la realización de dispositivos de control electrónicos tales como: cámaras IP, sensores de movimiento, relés, router, entre otros conceptos que permitirán describir específicamente cada uno de ellos y su funcionamiento.

En el Capítulo III se desglosa la metodología de la investigación, además de los instrumentos y técnicas que se aplicarán en el proceso investigativo facilitando la elección de cada uno de los recursos que permitirán llevar a cabo con el cumplimiento de los objetivos planteados.

El Capítulo IV está comprendido por los resultados obtenidos en este proyecto de investigación y la comprobación del funcionamiento del sistema de seguridad integral.

En el Capítulo V se describen las conclusiones pertinentes y las recomendaciones de este trabajo para trabajos futuros que se deseen realizar.

En el Capítulo VI se registran todas las citas, bibliografías y referencias de libros, revistas e internet utilizadas en este trabajo.

Y para concluir **el Capítulo VII** se evidencian las fotografías del proyecto desarrollado y las pruebas realizadas al mismo.

CAPÍTULO I

CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

1.1. Problema de la Investigación.

1.1.1. Planteamiento del problema.

1.1.1.1. Diagnóstico del problema.

En la actualidad la falta de seguridad se está volviendo más evidente, sin embargo también existen distintas alternativas de prevención tales como contratar personal de seguridad lo cual resultaría a largo plazo muy costoso y sin dejar de mencionar que este mecanismo no asegura una total confiabilidad, lo que da paso a que se originen y se desarrollen nuevas tecnologías que permitan cubrir la falta de confiabilidad y así obtener un sistema que brinde seguridad en la ausencia y presencia del usuario.

Así mismo, el empleo de sistemas integrales de seguridad resulta inusual debido a que muchos de ellos no son accesibles desde el punto de vista económico y en otro de los casos se necesita de un profesional para la instalación, mantenimiento y monitoreo de dichos dispositivos que conforman el sistema. Lo que se pretende realizar en el siguiente trabajo es utilizar todos los recursos brindados por el uso de herramientas tecnológicas-electrónicas en cuanto a materia de seguridad, y lograr un sistema integral con los dispositivos que se llegasen a instalar en una vivienda para ser controlados de manera remota.

1.1.1.2. Pronóstico del problema.

En el diseño y realización del proyecto de investigación puede ocurrir que la aplicación diseñada para la computadora no se comunique totalmente con el sistema de control y los dispositivos utilizados a causa de algun fallo en el código de programación. Además se puede presentar el caso de que se pierda la conexión entre el router y la cámara IP por la manipulación los cables sufran daños internos afectando así a la visualización de las imágenes que capta la misma.

1.1.2. Formulación.

¿Cómo índice el uso de un sistema de seguridad integral en el control y monitoreo de una vivienda vía remota?

1.1.3. Sistematización del problema.

1) ¿Qué protocolo de comunicación será el más adecuado para establecer conexión remota?

2) ¿Cómo se podrá acceder a un sistema de seguridad para que sea monitoreado desde un ordenador?

3) ¿Qué tipo de método podría garantizar el acceso al sistema de control y monitoreo de la vivienda mediante una conexión remota?

1.2. Objetivos.

1.2.1. Objetivos Generales.

Diseñar un sistema que permita el monitoreo y control de los distintos dispositivos de seguridad instalados dentro de una vivienda para vigilar el estado de la misma mediante una aplicación de escritorio vía remota.

1.2.2. Objetivos específicos.

- Establecer la comunicación entre el sistema integral de seguridad y el servidor mediante una IP Pública.
- Diseñar una aplicación que permita controlar las funciones de un sistema integral de seguridad desde una laptop mediante escritorio remoto.
- Comprobar la accesibilidad al sistema de control de seguridad de la vivienda mediante la identificación y autentificación del usuario.

1.3. Justificación.

La seguridad en el hogar es primordial para toda familia ya sea cuando los miembros se encuentren dentro o fuera de su vivienda, es por ello que la tecnología se acopla

perfectamente en este tipo de circunstancias. Logrando que las personas utilicen además de que aprovechen las oportunidades tecnológicas como herramientas para las actividades del día a día con el único fin de vivir de forma segura y protegida mediante la implementación de los sistemas de seguridad electrónico.

Por lo tanto debido a la problemática generada en cuanto a inseguridad y a circunstancias tales como (incendios, accidentes dentro del hogar, etc.) es necesario adoptar medidas para mitigar los robos y demás calamidades domesticas que se pueden presentar en la vida cotidiana, además otra justificación válida es el aprovechamiento de la tecnología aplicándola a la seguridad mediante un diseño, interconexiones e instalación de manera correcta.

Es por ello que en el presente trabajo se realizará un prototipo en el cual irá implementado un sistema integral de seguridad permitiendo ser manipulado vía remota mediante la asignación de una dirección IP pública, en el que se podrá tener acceso desde cualquier el computador de escritorio o portatil siempre y cuando la aplicación este instalada en el mismo y con la facilidad de hacerlo en tiempo real permitiendo obtener una alerta de manera rápida de los eventos que se estén generando cuando la vivienda este siendo vulnerada por intrusos.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN

2.1. Marco Conceptual.

2.1.1. Usuarios móviles.

Las computadoras móviles como las laptops y las computadoras de bolsillo son uno de los segmentos de más rápido crecimiento en la industria de las computadoras. Sus ventas ya han sobrepasado a las de las computadoras de escritorio. [1] Con frecuencia las personas que pasan mucho tiempo fuera de su oficina u hogar desean usar sus dispositivos móviles para leer y enviar correos electrónicos, usar Twitter, ver películas, descargar música, jugar o simplemente navegar en la Web para buscar información [1]

Los hotspots[2] basados en el estándar 802.11 son otro tipo de red inalámbrica para computadoras móviles. Han emergido por todos los puntos de reunión de la gente, que ahora cuenta con cobertura en cafés, hoteles, aeropuertos, trenes y aviones. Cualquiera con una laptop y un módem inalámbrico sólo necesita encender su computadora para estar conectado a Internet por medio de un hotspot, como si la computadora estuviera conectada a una red alámbrica [1]

2.1.2. Redes de ejemplo.

El tema de las redes de computadoras cubre muchos tipos distintos de redes, grandes y pequeñas, populares y no tanto. Tienen distintos objetivos, escalas y tecnologías. En las siguientes secciones analizaremos algunos ejemplos para tener una idea de la variedad que podemos encontrar en el área de las redes de computadoras. [1]

Empezaremos con Internet, que tal vez sea la red más popular; analizaremos su historia, evolución y tecnología. Después consideraremos la red de teléfonos móviles. Técnicamente es muy distinta de Internet y contrasta muy bien con ella. Más adelante introduciremos el IEEE 802.11, el estándar dominante para las redes LAN inalámbricas. Por último, analizaremos las redes RFID y de sensores, tecnologías que extienden el alcance de la red para incluir al mundo físico y los objetos cotidianos. [1]

[2] Hotspots. Punto que ofrece acceso a internet.

2.1.3. Redes de teléfonos móviles de tercera generación.

A las personas les encanta hablar por teléfono mucho más de lo que les gusta navegar en Internet, y esto ha logrado que la red de teléfonos móviles sea la más exitosa del mundo. Tiene más de cuatro mil millones de suscriptores a nivel mundial. Para poner esta cantidad en perspectiva, digamos que constituye aproximadamente 60% de la población mundial y es mucho más que la cantidad de hosts de Internet y líneas telefónicas fijas combinadas. [2]

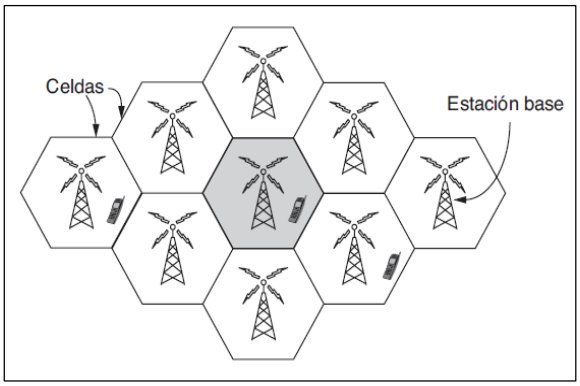
La arquitectura de la red de teléfonos móviles ha cambiado y ha crecido de manera considerable durante los últimos 40 años. Los sistemas de telefonía móvil de primera generación transmitían las llamadas de voz como señales de variación continua (analógicas) en vez de secuencias de bits (digitales). [2]

Los sistemas de teléfonos móviles de segunda generación cambiaron a la transmisión de las llamadas de voz en formato digital para aumentar su capacidad, mejorar la seguridad y ofrecer mensajería de texto. El sistema GSM (Sistema Global para Comunicaciones Móviles, del inglés Global System for Mobile communications), que se implementó a partir de 1991 y se convirtió en el sistema de telefonía móvil más utilizado en el mundo, es un sistema 2G. [2]

Los sistemas de tercera generación (o 3G) comenzaron a implementarse en el año 2001 y ofrecen servicios de datos tanto de voz digital como de datos digitales de banda ancha. También vienen con mucho lenguaje tecnológico y distintos estándares a elegir. La ITU (una organización internacional de estándares de la que hablaremos en la siguiente sección) define al estándar 3G en sentido general como un servicio que ofrece velocidades de por lo menos 2 Mbps para usuarios estacionarios o móviles, y de 384 kbps en un vehículo en movimiento.

El sistema UMTS (Sistema Universal de Telecomunicaciones Móviles, del inglés Universal Mobile Telecommunications System), también conocido como WCDMA (Acceso Múltiple por División de Código de Banda Ancha, del inglés Wideband Code Division Multiple Access), es el principal sistema 3G que se está implementando con rapidez en todo el mundo. [2]

Fig. 1 Diseño Celular de una Red de telefonía Celular



Fuente: (Tanenbaum & Wetherall, 2012 p. 56).

Elaborado por: Carmen A. Hernández O. (2015)

2.1.4. Transmisión inalámbrica.

Nuestra Era ha dado origen a los adictos a la información: personas que necesitan estar todo el tiempo en línea. Para estos usuarios móviles no son de utilidad el par trenzado, el cable coaxial ni la fibra óptica. [1] Necesitan obtener datos para sus computadoras laptop, notebook, de bolsillo, de mano o de reloj de pulsera sin tener que estar atados a la infraestructura de comunicación terrestre. Para estos usuarios, la comunicación inalámbrica es la respuesta. [1]

2.1.5. El sistema de telefonía móvil.

Aun si el sistema de telefonía tradicional llegara algún día a utilizar fibra óptica con capacidad de multigigabit desde un extremo hasta el otro, no podría satisfacer a un grupo creciente de usuarios: las personas en movimiento. [1] Ahora las personas esperan hacer llamadas telefónicas y usar sus teléfonos para revisar su correo electrónico y navegar por la web desde aviones, autos, albercas y mientras trotan en el parque. [2]

Según [1] “En consecuencia, hay mucho interés en la telefonía inalámbrica. En las siguientes secciones estudiaremos este tema con detalle. El sistema de telefonía móvil se utiliza para la comunicación de datos y voz de área amplia. [1] Los teléfonos móviles (también conocidos como teléfonos celulares) han pasado por tres generaciones distintas, conocidas comúnmente como 1G, 2G y 3G”. Las generaciones son [1]:

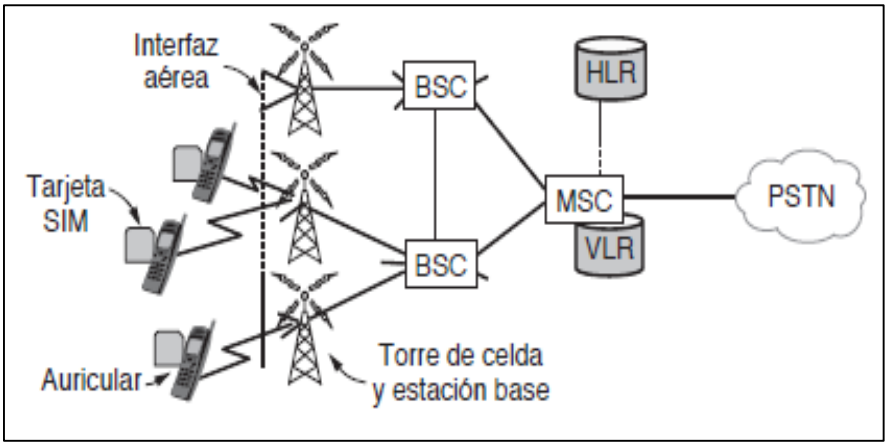
- Voz analógica. [2]
- Voz digital. [2]
- Voz y datos digitales (Internet, correo electrónico, etcétera). [2]

2.1.6. GSM – El sistema global para comunicaciones móviles.

GSM empezó en la década de 1980 como un esfuerzo por producir un solo estándar europeo de 2G. La tarea se asignó a un grupo de telecomunicaciones llamado (en francés) Groupe Specialé Mobile. Los primeros sistemas GSM se implementaron a partir de 1991 y fueron un éxito inmediato. Pronto quedó claro que GSM iba a ser más que un éxito en Europa, puesto que se estaba popularizando en países tan lejanos como Australia, por lo cual se cambió su nombre para que tuviera un atractivo más enfocado al mercado mundial. [1]

La figura 2 muestra que la arquitectura GSM es similar a la arquitectura AMPS, aunque los componentes tienen distintos nombres. Ahora el móvil en sí es dividido en el teléfono y en un chip removible con información del suscriptor y la cuenta, conocido como tarjeta SIM (Módulo de Identidad del Suscriptor, del inglés Subscriber Identity Module). La tarjeta SIM activa el teléfono y contiene los secretos que permiten al móvil y a la red identificarse entre sí y cifrar las conversaciones. Es posible quitar la tarjeta SIM e insertarla en un teléfono distinto para convertirlo en su teléfono móvil en lo que respecta a la red. [2]

Fig. 2 Arquitectura de la red de telefonía GSM.



Fuente: (Tanenbaum & Wetherall, 2012 p. 147).

Elaborado por: Carmen A. Hernández O. (2015)

2.1.7. Protocolos de Internet.

Un equipo de red especial llamado encaminador (router), con una conexión a cada red, se encarga de enviar paquetes entre ellas. El papel de los encaminadores está definido en el RFC 1812 (Request For Comments 1812). Al reducir el papel de la red al mínimo se pudo conectar con cualquier red6, solventando el problema inicial de Kahn para interconectar las redes de satélites y las de radio. [3]

En 1980 David P. Reed diseñó el protocolo UDP (User Datagram Protocol, también llamado Universal Datagram Protocol) para trabajar sobre IP con un esquema de datagramas -no orientado a conexión-.En 1982 el departamento de defensa de los EE.UU. seleccionó TCP/IP como su protocolo estándar y el 1 de enero de 1983 ARPANET mudó sus sistemas al nuevo protocolo. [3]

2.1.8. Métodos de acceso a redes.

Existen métodos diseñados para acceder a las redes de comunicaciones que se caracterizan por comunicar equipos de manera jerárquica: generalmente un equipo "usuario" o "cliente" y un equipo "proveedor", "servidor" o "central" que depende de los llamados "proveedores de acceso" cuyos servicios suponen un coste para el usuario. En algunos textos se les llama "Redes de Acceso", aunque en este se prefiere "Métodos de Acceso a Redes" por coherencia con la definición dada de redes de comunicaciones [3].

2.1.8.1. Módems.

Un módem es un dispositivo que sirve para modular y demodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada portadora mediante otra señal de entrada llamada moduladora. Su uso más común y conocido es para realizar transmisiones de datos por vía telefónica. Estos módems telefónicos existen otros módems como los módems xDSL o módems utilizados para transmisiones radiofónicas y de televisión. Determinan la velocidad de transmisión. Así podemos encontrar desde el V.32. (Transmisión a 9.600 bps) hasta el V.92 (transmisión a 56'6 kbps con compresión de datos y llamada en espera). [3]

Fig. 3 Router marca Dlink

Fuente: www.amazon.com

Elaborado por: Carmen A. Hernández O. (2015)

2.1.9. Soportes de transmisión.

Un soporte de transmisión transporta datos en forma de señales entre las interfaces de red. Hay distintos tipos de soporte en función del precio, de la simplicidad de la instalación, la velocidad, la resistencia a las interferencias, etc. Entre estos, se distinguen los soportes limitados y los no limitados. [4]

2.1.9.1. Soportes limitados.

Son soportes físicos, como los cables que conducen la electricidad. Los principales soportes limitados son el par trenzado, el cable coaxial y la fibra óptica. [1]

a. El par trenzado.

Un par trenzado en su forma más simple está compuesto por dos cables trenzados de cobre, cada uno protegido con una cubierta aislante. Hay varios tipos de pares trenzados: el par trenzado no blindado *Unshielded Twisted Pair* (UTP) y el par blindado *Shielded Twisted Pair* (STP) son los más extendidos. [4]

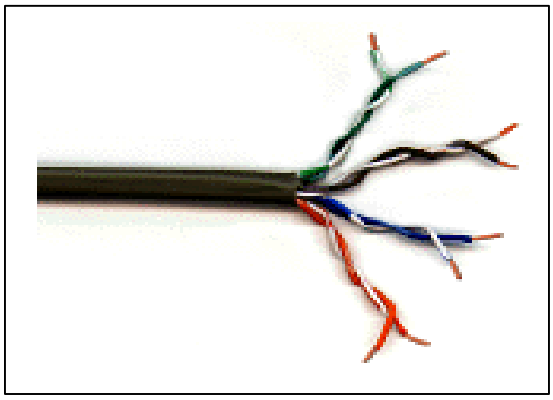
El par trenzado blindado (STP) añade una protección por par. Existe igualmente un tipo de pares FTP (*Foiled Twisted Pair*), que proporciona protección utilizando una tira de aluminio alrededor de los 4 pares. Se puede encontrar también una combinación de los dos anteriores llamada S/FTP o *Shield/Foiled Twisted Pair*. Finalmente, otro tipo de protección consistirá

en una hoja doble por par y en general. Se trata de F/FTP. El número de pares por cable varía. El trenzado de los cables disminuye las interferencias eléctricas procedentes de los pares adyacentes y del entorno exterior. [4]

b. Par trenzado no blindado.

Es el tipo de par trenzado más utilizado en las redes locales. Un segmento de cable UTP puede alcanzar los 100 metros. La mayoría de los sistemas telefónicos utilizan el tipo UTP. La popularidad de este tipo de cable se debe al hecho de que en un gran número de edificios se realiza un cableado previo para los sistemas telefónicos. No obstante, el sistema telefónico debe respetar las características propias de las redes informáticas (como el trenzado) para garantizar una buena calidad de transmisión. [4]

Fig. 4 Cable de pares trenzados



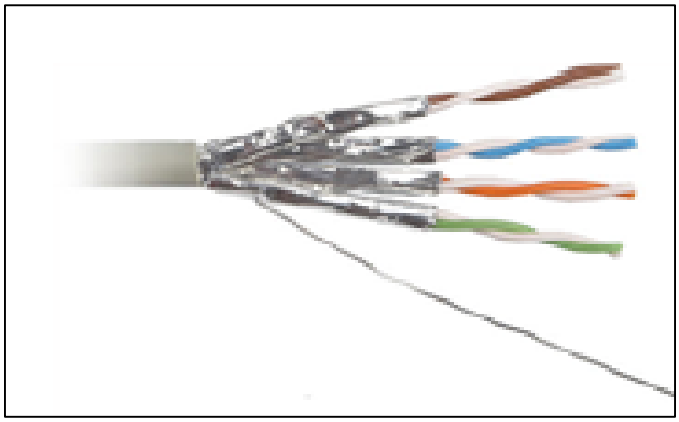
Fuente: José Dorigne Redes Informáticas. Nociones Fundamentales (2010)

Elaborado por: Carmen A. Hernández O. (2015)

c. Par trenzado blindado

El cable UTP es especialmente propenso a las interferencias (mezcla de señales debida a pares vecinos). El cable STP mejora la transmisión utilizando una envoltura trenzada de cobre de mejor calidad y más protectora que la empleada para el cableado UTP. Además, una envoltura dealuminio recubre cada uno de los pares trenzados. Así, a diferencia del cable no blindado, el cable STP alcanza velocidades más elevadas para distancias ligeramente superiores. [4]

Fig. 5 Cable STP



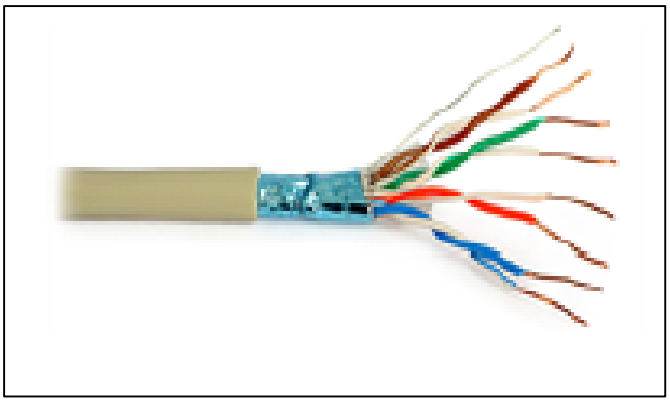
Fuente: José Dorigne Redes Informáticas. Nociones Fundamentales (2010)

Elaborado por: Carmen A. Hernández O. (2015)

d. Cable FTP

El cable FTP es más resistente a interferencias externas.

Fig. 6 Cable FTP



Fuente: José Dorigne Redes Informáticas. Nociones Fundamentales (2010)

Elaborado por: Carmen A. Hernández O. (2015)

2.1.9.2. Conectores.

Existen diferentes tipos de conectores para el par trenzado; veamos los principales a continuación: [4]

- RJ11: cable telefónico de 2 pares trenzados. [4]
- RJ14: cable telefónico de 3 pares trenzados. [4]

- RJ45: cable de red de 4 pares trenzados. [4]

Para redes de gran envergadura, es posible organizar las conexiones a partir de un armario de distribución de cables. El conector RJ45 se utiliza hoy por todas partes, ya sea para conexiones de red o de telecomunicaciones. [4]

Fig. 7 Conector RJ-45

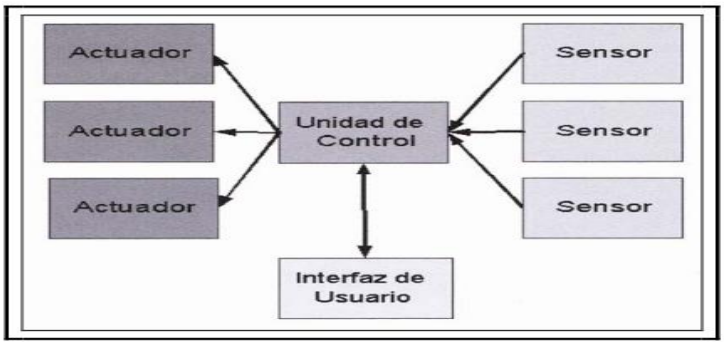
Fuente: José Dorigne Redes Informáticas. Nociones Fundamentales (2010)

Elaborado por: Carmen A. Hernández O. (2015)

2.1.10. Arquitectura centralizada.

Es aquella en la que los elementos a controlar y supervisar (sensores, luces, válvulas, etc.) han de cablearse hasta el sistema de control de la vivienda (PC o similar). El sistema de control es el corazón de la vivienda, en cuya falta todo deja de funcionar, y su instalación no es compatible con la instalación eléctrica convencional en cuanto que en la fase de construcción hay que elegir esta topología de cableado [5].

Fig. 8 Arquitectura centralizada



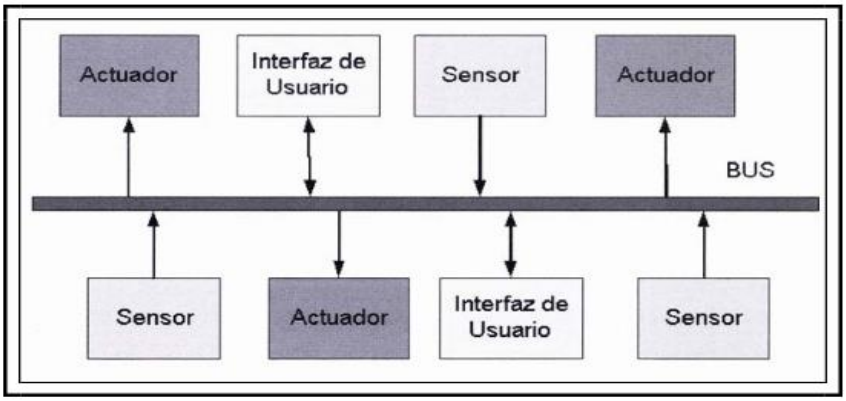
Fuente: Carlos Álvarez, Danilo Holguín, Ernesto Serrano. Instalación de casa inteligente (2007)

Elaborado por: Carmen A. Hernández O. (2015)

2.1.11. Arquitectura descentralizada.

Es aquella en la que el elemento de control se sitúa próximo al elemento a controlar. Cada elemento del sistema tiene su propia capacidad de proceso y puede ser ubicado en cualquier parte de la vivienda. Esta característica proporciona al instalador domótico una libertad de diseño que le posibilita adaptarse a las características físicas de cada vivienda en particular [5].

Fig. 9 Arquitectura descentralizada



Fuente: Carlos Álvarez, Danilo Holguín, Ernesto Serrano. Esquema de bloque de la casa inteligente (2007)
Elaborado por: Carmen A. Hernández O. (2015)

2.1.12. Sistemas de control y monitoreo.

Los sistemas de monitoreo para casas habitación tienen ya una larga historia, pues no es en los últimos años que surge la necesidad del ser humano de hacer más segura su casa tanto cuando está como cuando no está en ella. Actualmente existen diversos sistemas de monitoreo tanto para empresas como para casas habitación. Existen sistemas que tienen cableado y sistemas inalámbricos. [6] [7]

2.1.13. Sistemas Inalámbricos.

Estos sistemas se comunican mediante radio transmisión y como su nombre lo indica no es necesario tener un cableado especial para lograr una comunicación con una centro o con un usuario determinado. [8] [7]

2.1.14. Sistemas con Cableado.

Estos sistemas son el opuesto a los sistemas inalámbricos, como su nombre lo indica necesitan de ciertas conexiones que permitan establecer la comunicación entre ciertos componentes del mismo sistema o a otros usuarios. [8] [7]

2.1.15. Circuito Cerrado.

El circuito cerrado es aquel que tiene cámaras y que nos permite vigilar en su totalidad zonas de un lugar, estas cámaras pueden grabar de forma continua o en determinados periodos de tiempo. Además de las cámaras se deben de colocar monitores para observar lo que están grabando las cámaras previamente instaladas. [7] [9]

2.1.16. Dispsositivos para los sistemas de seguridad.

2.1.16.1. Teclado Matricial.

Es un dispositivo que se utiliza para el ingreso de códigos de seguridad para los accesos automatizados, estos poseen un sistema de programación que puede ser configurados de la manera que el usuario desee.

Fig. 10 Código de activación teclado

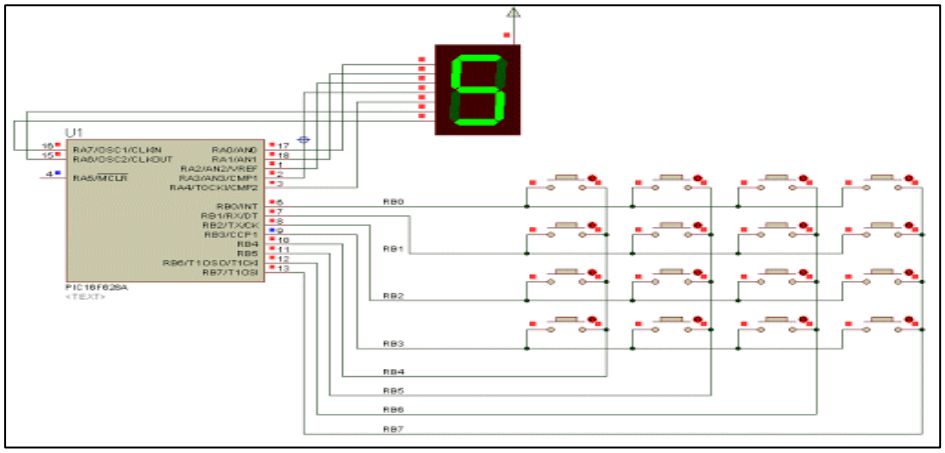
```
INICIO  movlw   0x07                ; Deshabilitar comparadores
        movwf   CMCON               ; analogicos
        bsf     STATUS,RP0          ; Cambio a banco 1
        movlw   0xF0                ; Nibble alto del puerto B como
        movwf   TRISB               ; entrada y bajo como salida
        clrf    TRISA               ; Puerto A como salida
        bcf     OPTION_REG,NOT_RBPU ; Resistencias de pull-up
                                    ; habilitadas
        bcf     STATUS,RP0          ; Cambio a banco 0

        movlw   NUM.0               ; Iniciar Puerto A para que
        movwf   PORTA               ; despliegue un "0"

PRINCIPAL
        call    TECLADO             ; Llamar a rutina de teclado
        movwf   PORTA               ; Desplegar numero en puerto A
        goto    PRINCIPAL           ; Ejecucuon ciclica del programa
```

Fuente: Martinez, Lopez. Circuitos electrónicos (2011)

Elaborado por: Carmen A. Hernández O. (2015)

Estos sistemas funcionan basicamente con códigos binarios representados por unos y ceros, además de que estos pueden ser complemento de pantallas LCD.

Fig. 11 Diagrama de funcionamiento teclado



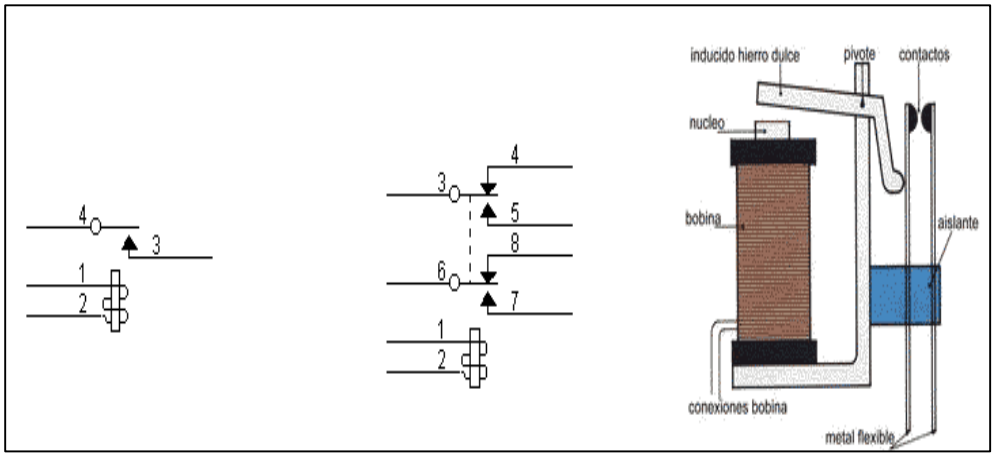
Fuente: Martinez, Lopez. Circuitos electrónicos (2011)

Elaborado por: Carmen A. Hernández O. (2015)

2.1.16.2. El rele.

Es un circuito electromagnético (electroimán) y un circuito de contactos que permite controlar la tensión.

Fig. 12 Simbolo y partes de un relé de armaduras

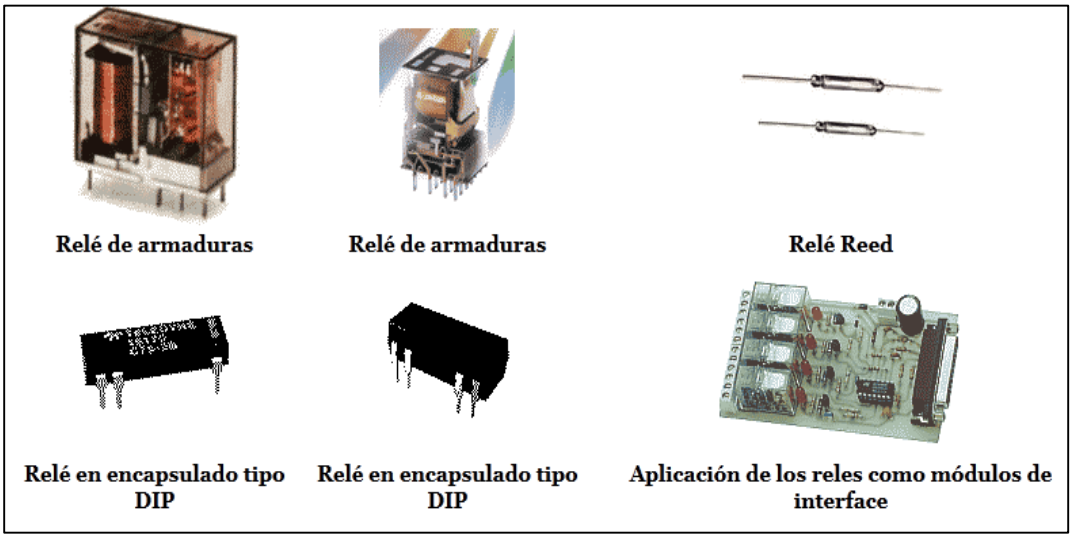


Fuente: http://www.electronicafacil.net/tutoriales/El-rele.php

Elaborado por: Carmen A. Hernández O. (2015)

2.1.16.2.1. Reles más utilizados.

Fig. 13 Tipos de reles



Fuente: http://www.electronicafacil.net/tutoriales/El-rele.php

Elaborado por: Carmen A. Hernández O. (2015)

2.1.16.3. Sensores.

Según [7] "Un sensor es un dispositivo que detecta manifestaciones de fenómenos físicos, como la energía, velocidad, aceleración, tamaño, cantidad, etc."

Un sensor es un tipo de transductor que transforma la magnitud que se quiere medir a otra para facilitar su medida. Algunos sensores electrónicos son Termopar, termistor, galga extensiométrica, fotodiodo, micrófono, etc. [7] Los tipos de sensores que requerimos para el desarrollo del presente trabajo son [7]:

- Sensores de movimiento. [7]
- Sensores de humo. [7]
- Sensores magnéticos. [7]

2.1.16.4. Sensores de movimiento.

Estos sensores estan elaborados para la detección de intrusos y para su correcto funcionamiento deben ser colocados en lugares estratégicos. [10]

Fig. 14 Sensor - detector de movimiento Niessen

Fuente: Voltium, (2014)

Elaborado por: Carmen A. Hernández O. (2015)

2.1.16.5. Sensor de vibración.

Los sensores de vibración son acelerómetros que permiten trabajar en frecuencias altas, que es donde se produce principalmente la vibración. [11] Estas frecuencias y en consecuencia estos acelerómetros se utilizan para diferentes aplicaciones, pero hay una que destaca sobre el resto, y es el control preventivo o mantenimiento preventivo en maquinaria. [12]

Estos sensores de vibración en combinación con el acondicionador o equipo de adquisición pertinente, nos permiten llevar a cabo una instalación de sensores para el registro y posterior análisis de las vibraciones, ver tendencias de desgaste o problemas de funcionamiento de la maquinaria, debido a un mayor nivel de vibración en ciertas frecuencias. [12]

Fig. 15 Sensor de vibración para viviendas

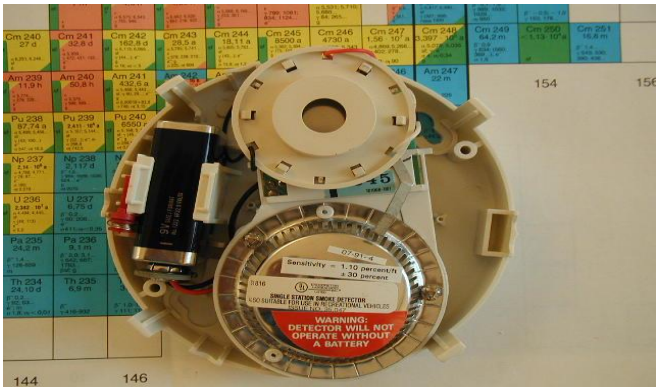
Fuente: http://www.ehowenespanol.com/tipos-sensores-vibracion-lista_317332/

Elaborado por: Carmen A. Hernández O. (2015)

2.1.16.6. Sensor de humo.

Sistema que permite la detección de agentes contaminantes en el ambiente y puede ser calibrado a conveniencia del usuario. [13]

Fig. 16 Sensor de vibración para viviendas



Fuente: www.profisica.cl

Elaborado por: Carmen A. Hernández O. (2015)

2.1.16.7. Sensor magnético.

Estos sensores estan diseñados para detectar aperturas inusuales de ventanas o puertas, estó dependerá de donde sean instalados. [14]

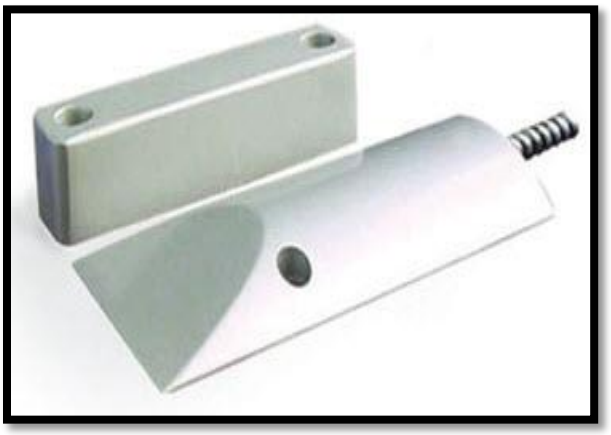
Fig. 17 Contacto mágnetico pesado para portones o garaje

Fuente: TecnoSeguro, Sensor Mágnetico, (2011)

Elaborado por: Carmen A. Hernández O. (2015)

Existen diferentes tipos de detectores: de aplicación en las ventas, puertas y garajes, etc. [14] [15]

Fig. 18 Contacto Magnético para portones o garaje



Fuente: TecnoSeguro, Sensor Mágnetico, (2011)

Elaborado por: Carmen A. Hernández O. (2015)

Otro tipo conocido es el que se presenta a continuación:

Fig. 19 Contacto Magnético Instalado en puerta

Fuente: TecnoSeguro, Sensor Mágnetico, (2011)

Elaborado por: Carmen A. Hernández O. (2015)

2.1.16.8. Botón de pánico.

Los botones de pánico no son más que pulsadores conectados a un sistema de alarma, generalmente ubicado en una locación remota. Su primera aplicación comercial fue en los bancos y todavía perdura en estas empresas y comercios [16] .

Fig. 20 Botón de pánico

Fuente: TecnoSeguro, Sensor Mágnetico, (2011)
Elaborado por: Carmen A. Hernández O. (2015)

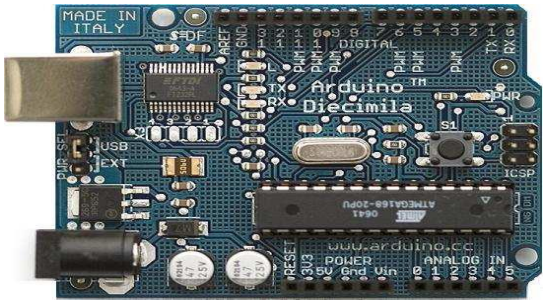
El botón es colocado en un lugar al que no pueden llegar los clientes sino empleados con autorización especial. Cuando se presenta una emergencia, generalmente un robo, es presionado y emite una señal hacia el tablero de control al que está conectado mediante un cable o por frecuencia de radio y que envía una señal a nuestra Central Nacional de Monitoreo [16].Los puedes encontrar del tipo alámbrico o inalámbrico, es decir, puede estar fijo en alguna oficina o área del inmueble o llevarlo consigo como un dispositivo de seguridad portátil.

2.1.17. Equipos de programación.

2.1.17.1. Arduino.

Al igual que la raspberry arduino propone un diseño versátil para la programación utilizando lenguaje C contando con licencia libre y fácil de emplear. [15]

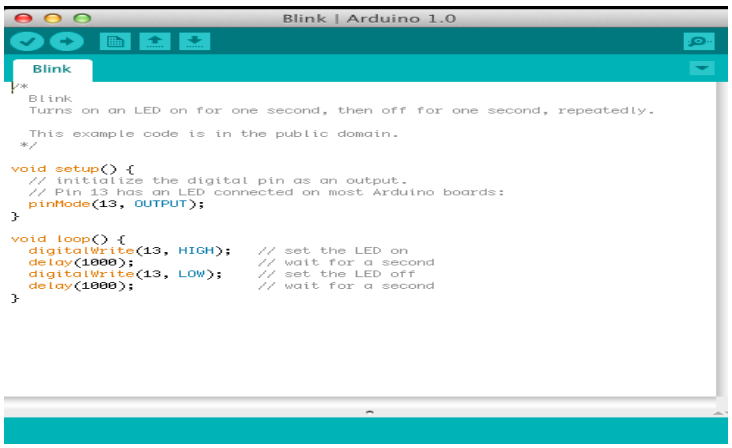
Fig. 21 Placa de Arduino



Fuente: (Beginner's & Evans, 2007)
Elaborado por: Carmen A. Hernández O. (2015)

En el se presentan algoritmos fáciles de emplear con el fin de que el que realice los proyectos se familiarice con esta herramienta [17]:

Fig. 22 Interfaz de inicio



Fuente: Guía Básica de Arduino- Robótica (2008)

Elaborado por: Carmen A. Hernández O. (2015)

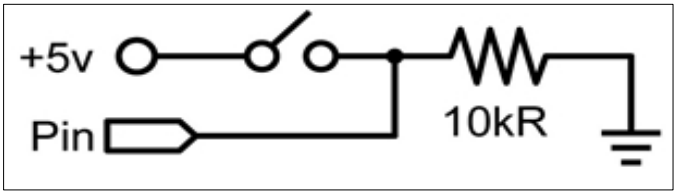
2.1.17.2. Formas de Conexionado de entradas y salidas.

Fig. 23 Salida digital

Fuente: (Beginner's & Evans, 2007 Manual de Programación de Arduino p. 29)

Elaborado por: Carmen A. Hernández O. (2015)

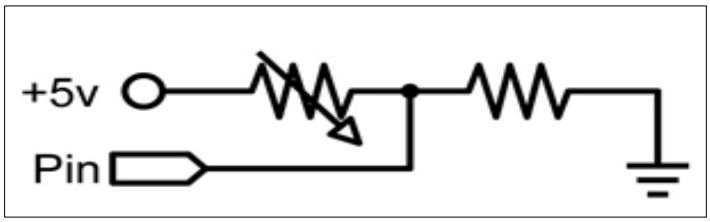
Fig. 24 Entrada digital



Fuente: (Beginner's & Evans, 2007 Manual de Programación de Arduino p. 30)

Elaborado por: Carmen A. Hernández O. (2015)

Fig. 25 Entrada conectada a resistencia variable (Entrada analógica)



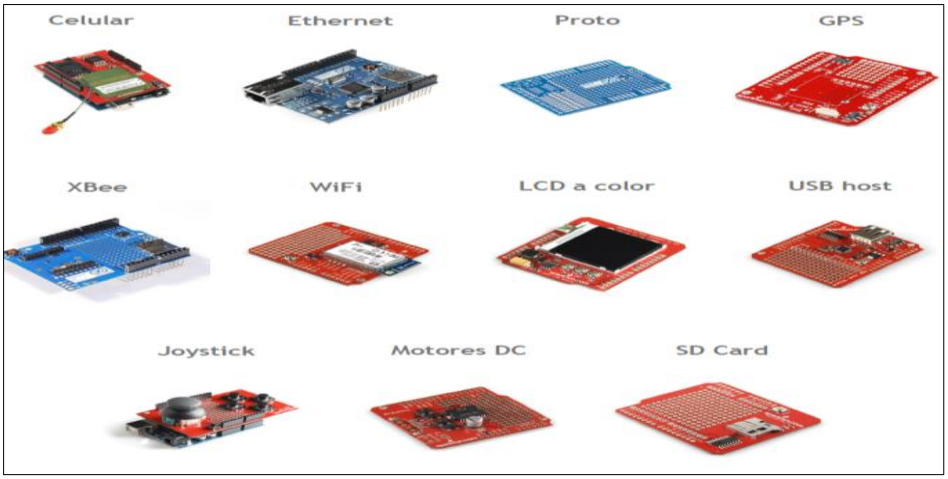
Fuente: (Beginner's & Evans, 2007 Manual de Programación de Arduino p. 34)

Elaborado por: Carmen A. Hernández O. (2015)

2.1.17.3. Expandir Arduino con los shields.

Un Shield o escudo es una placa que permite expandir funcionalidades a tu Arduino, con lo cual puedes conectar motores, o a la red celular, a una red WiFi, a una red Ethernet o tener un MP3 en el Arduino. [17]

Fig. 26 Tipos de adaptaciones para Arduino



Fuente: (Robótica, 2010 Guía Básica de Arduino p.45).

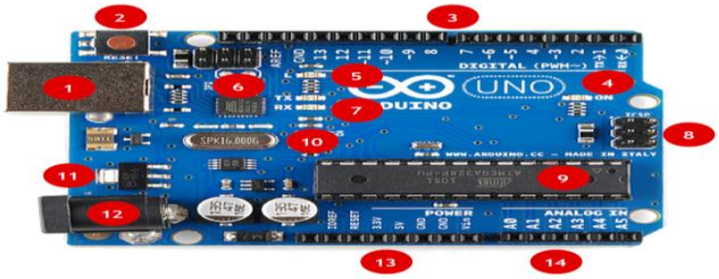
Elaborado por: Carmen A. Hernández O. (2015)

2.1.17.4. Placa Arduino y sus partes.

1. Conector USB para el cable Tipo AB. [17]
2. Pulsador de Reset. [17]
3. Pines de E/S digitales y PWM [17]
4. LED verde de placa encendida [17]

5. LED naranja conectado al pin13 [17]
6. ATmega 16U2 encargado de la comunicación con el PC [17]
7. LED TX (Transmisor) y RX (Receptor) de la comunicación serial [17]
8. Puerto ICSP para programación serial [17]
9. Microcontrolador ATmega 328, cerebro del Arduino [17]
10. Cristal de cuarzo de 16Mhz [17]
11. Regulador de voltaje [17]
12. Conector hembra 2.1mm con centro positivo [17]
13. Pines de voltaje y tierra [17]
14. Entradas análogas [17]

Fig. 27 Vista frontal de la placa



Fuente: (Robótica, 2010 Guía Básica de Arduino p.45).

Elaborado por: Carmen A. Hernández O. (2015)

Fig. 28 Vista trasera y superior

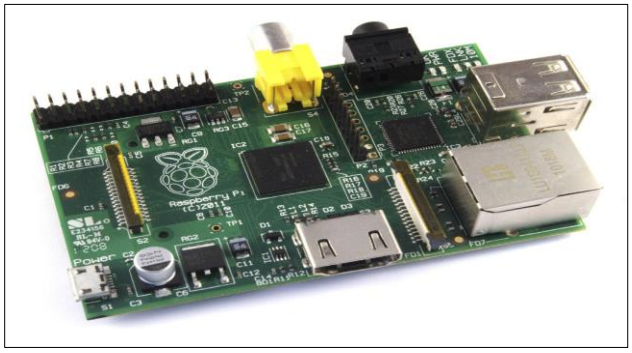
Fuente: (Robótica, 2010 Guía Básica de Arduino p.45).

Elaborado por: Carmen A. Hernández O. (2015)

2.1.18. Raspberry PI.

Es un dispositivo utilizado para diversos proyectos comprendidos en materia de electrónica, telecomunicaciones, robótica y demás requerimientos de la tecnología. Existen muchas versiones de este dispositivo, dado a la acogida que este ha tenido durante su aparición en el mercado. Estos dispositivos se los encuentra en el mercado por su bajo costo y requieren poca energía. [18]

Fig. 29 Placa Raspberry PI

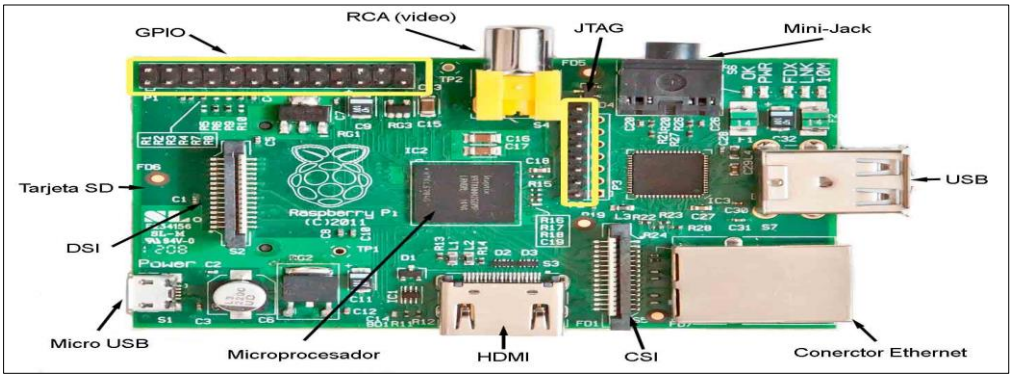


Fuente: Raspberry, (2010)

Elaborado por: Carmen A. Hernández O. (2015)

Esta comprendida por un microcontrolador que permite la programación de las funciones y procesos que pueden realizarse.

Fig. 30 Partes de la Placa Raspberry PI



Fuente: Raspberry, (2010)

Elaborado por: Carmen A. Hernández O. (2015)

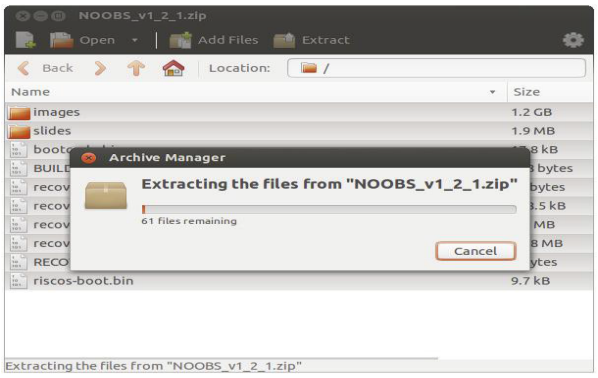
Los pines en la parte superior izquierda de la RasPi componen el header o conector con entradas-salidas de propósito general (GPIO) que puede utilizarse para conectar la RasPi a otros hardwares. El uso más frecuente de este puerto es para conectar una placa de expansión (Add-On). El puerto GPIO es extremadamente poderoso, pero también frágil; cuando manipule la RasPi, siempre evite tocar estos pines, así como también nunca conectar nada en ellos mientras la RasPi se encuentra encendida [18].

El conector de plástico y metal debajo del puerto GPIO es el puerto DSI (Display Serial Interface), que sirve para conectar sistemas de pantalla plana controlada digitalmente. Estas pantallas rara vez son utilizadas excepto por los desarrolladores profesionales en sistemas embebidos, ya que el puerto HDMI es más flexible. Un segundo conector de plástico y metal, se encuentra a la derecha del puerto HDMI, es el puerto CSI (Camera Serial Interface), que proporciona una conexión de alta velocidad para el módulo de cámara de la Raspberry Pi u otros sistemas de cámaras con conexión CSI compatibles con la RasPi. [18].

2.1.18.1. Noobs para Raspberry.

Esta herramienta, ha sido diseñada para hacer lo más fácil posible el comenzar a utilizar la RasPi, y se encuentra precargada en algunas tarjetas SD incluidas con la placa Raspberry Pi, así como por separado, en forma de descarga gratuita.

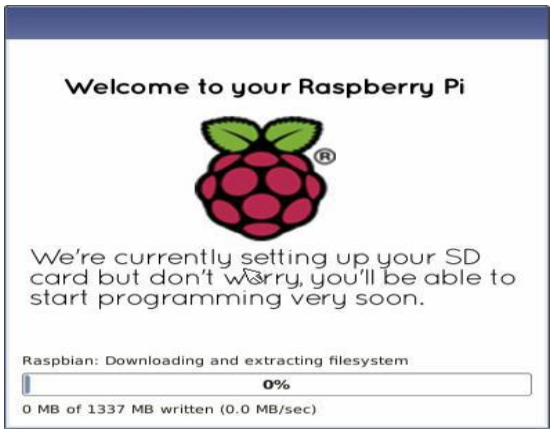
Fig. 31 Instalacion de Noobs



Fuente: Raspberry, (2010)

Elaborado por: Carmen A. Hernández O. (2015)

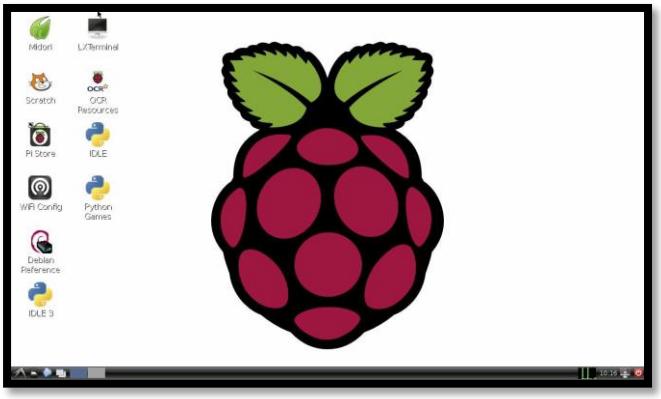
Fig. 32 Instalacion de Raspberry



Fuente: Upton, Eben; Halfacree, Gareth-Raspberry PI Guia de Usuario 2010

Elaborado por: Carmen A. Hernández O. (2015)

Fig. 33 Instalacion de Raspberry



Fuente: Upton, Eben; Halfacree, Gareth-Raspberry PI Guia de Usuario 2010

Elaborado por: Carmen A. Hernández O. (2015)

2.2. Marco Referencial.

2.2.1. Sistema de Seguridad Domiciliaria.

El proyecto implementa un sistema de seguridad domiciliaria de bajo costo que cumpla con las necesidades básicas de los usuarios. Este sistema opera como herramienta de monitoreo y prevención que incorpore criterios tales como: la planeación estratégica y el costo–

efectividad basados en los dispositivos de seguridad existentes. Uno de los puntos importantes del sistema de seguridad domiciliaria a implementarse, esto se logra a través de cualquier equipo remoto que disponga de un acceso a internet que permita al usuario acceder a un sistema de cámaras ubicadas en su domicilio [19].

2.2.2. Diseño de sistema electrónico antiintrusos para viviendas individuales.

Este sistema está constituido con una energía de alimentación que representa el elemento de activación del sistema, por lo que se debe disponer de una fuente de alimentación, que automatice el sistema ante posibles faltas de suministro casuales o intencionadas. Esto se logra por medio de acumuladores de energía y baterías (SAI, sistema de alimentación independiente). La unidad de control es el cerebro de todo el sistema. Recibe los impulsos de los detectores y, tras analizarlos, los transforma oportunamente en señales que envía a los señalizadores o avisadores locales y/o remotos [20].

2.2.3. Diseño y Simulación de un Sistema Domótico para una vivienda.

El objetivo principal del proyecto es la simulación funcional de una vivienda domótica unifamiliar. La programación de la aplicación y la simulación de la implantación de la tecnología, así como del funcionamiento de los sensores serán llevados a cabo mediante el uso del software LabView [21].

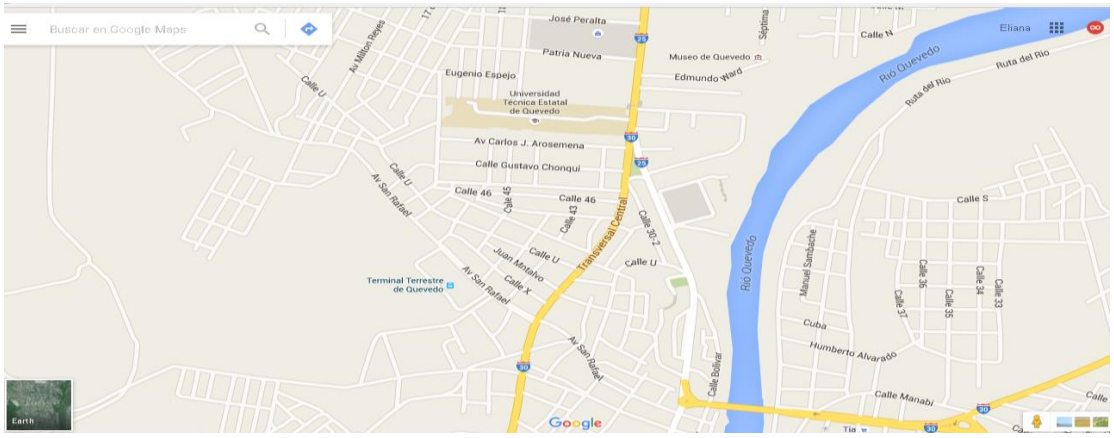
CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN.

3.1. Localización.

El siguiente proyecto se demostrará en el Campus Universitario "Ingeniero Manuel Haz Álvarez", Av. Quito km. 1 ½ vía a Santo Domingo de los Tsáchilas en la ciudad de Quevedo Provincia de Los Ríos.

Fig. 34 Mapa de ubicación de la UTEQ.



Fuente: Google Map (2015)

Elaborado por: Carmen A. Hernández O. (2015)

3.2. Tipo de investigación.

Bibliográfica.- Porque se recurre a bibliografías de libros programación web de aplicaciones Android, entre otros logrando así; ampliar los conocimientos acerca de los problemas que se presentarían al programar la aplicación para el proyecto del sistema integral de seguridad.

Exploratoria.- La investigación exploratoria se pudo realizar un búsqueda exhaustiva de la información y selección de temas concernientes a la creación de un sistema integral de seguridad, proceso que se lo llevo a cabo mediante la recolección de datos técnicos con la finalidad de tener conocimientos teóricos para el diseño previo del sistema, implementación de dispositivos de control, elementos electrónicos y mecanismo de comunicación remota.

Acción.- Mediante la investigación de acción lo que se buscó fue vincular la investigación exploratoria junto con la práctica, buscando poner en marcha cada una de las diferentes etapas de implementación para su creación tales como: Sistema de conexión remoto, Sistema

Electrónico, Diagramas Eléctricos. Aspectos sumamente importantes para un correcto funcionamiento en un sistema de seguridad integral.

Aplicada.- La investigación aplicada ayudó a observar proyectos previamente realizados, despertando interés para generar nuevos conocimientos.

3.3. Métodos de investigación.

- **Método de observación**

El uso de esta técnica permitirá el análisis y lograr determinar los problemas de sincronización de la aplicación instalada en el computador mediante el escritorio remoto con el sistema integral de seguridad a fin de que permita monitorear en línea cualquier imprevisto que se presente en el hogar.

- **Método analítico**

Permite conocer los problemas que se pueden presentar en el diseño y programación del sistema de seguridad con el módulo de la Raspberry junto con el módulo Arduino. Además de la instalación de los dispositivos (sensores, alarma, cámara, entre otros) con el objetivo de que cumplan sus funciones.

- **Método síntesis**

La realización de este proyecto de automatización de procesos permite conocer y comprender los aspectos que se involucran en el desarrollo de sistemas de seguridad mediante la utilización de dispositivos electrónicos, comprender la esencia del mismo, conocer sus aspectos y relaciones básicas en una perspectiva de totalidad.

3.4. Fuentes de recopilación de información.

3.4.1. Fuentes primarias.

- Libros
- Revistas y Manuales

3.4.2. Fuentes secundarias.

- Internet

- Diccionarios
- Enciclopedias

3.5. Diseño de la investigación.

La investigación de este proyecto esta orientada a la investigación ***no experimental***, dado que no existen variables definidas pero si existe un objeto de investigación el cual será observado en su entorno natural. Además esta es una investigación ***no experimental longitudinal*** permitiendo recolectar datos o información en una o varias circunstancias. En el diseño de este sistema de seguridad se pueden observar las distintas circunstancias por las que el sistema podría presetar los mensajes de alerta, para conocer un poco más las funciones son descritas a continuación:

- **Avisos telefónicos** a un número específico es decir a los propietarios y a quien se designe en la programación del módulo Raspberry en caso de presentarse la presencia de algún intruso.

- **Puertas** en lo que respecta a las puertas en este prototipo se utilizaran servomotores para simular la apertura y cierre de las mismas.

- **La detección de intrusos** mediante la utilización de sensores magnéticos en el caso de que fueran forzadas las puertas o ventanas. Además del acceso a la puerta de la vivienda con un código de acceso.

- **Alarmas:** este sistema está constituido por el sensor de humos, de movimiento y la cámara de video vigilancia que permitirá grabar o monitorear los diferentes puntos de la vivienda en los que se hayan colocado las cámaras. Además de que los sensores de movimiento se encargarían de detectar cualquier intruso.

3.6. Instrumentos de investigación.

Planeación.- Lo primero que se hizo fue programar la aplicación para el teléfono celular, seguidamente la programación del sistema de control que llevara el prototipo, que sería la

pieza clave en este proyecto, ya que por medio del dispositivo móvil se sincronizarían estos dos dispositivos, logrando así la comunicación perfecta logrando cumplirse los objetivos planteados.

Recopilación.- Para determinar el problema de sincronización de la aplicación se investigó en foros y páginas web en donde se pudo obtener algunos datos para la solución y como poner en marcha cada objetivo planteado en el proyecto.

Internet.- Varias de las informaciones fueron recopiladas de páginas web y foros de electrónica específicamente, que tienen una información de gran confiabilidad.

3.7. Recursos humanos y materiales.

3.7.1. Recursos humanos.

Autora del proyecto de investigación

- Carmen Amparo Hernandez Ordinola

Director de tesis

- Ing. Jaime Macías Romero, M.Sc.

3.7.2. Materiales.

Tabla 1. Presupuesto

Cantidad	Detalle	Valor Unitario	Valor Total
1	Cámara IP dlink	144,48	144,48
2	Sensor de movimiento	7,28	14,56
3	Sensor de vibración	11,20	33,60
3	Sensores magnéticos	10,63	31,89
1	Raspberry	90,00	90,00
1	Arduino mega	37,50	37,50
1	sim900	90,00	90,00
1	paro de emergencia (botón de pánico)	8,00	8,00
2	sensor de humo	22,4	44,80
1	router wireless dlink	39,29	39,29
	Subtotal	700,69	
	Iva	84,08	
	Total	784,77	

Elaboración: Carmen A. Hernández O.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1. Resultados.

Antes de iniciar con el proceso de construcción del prototipo del sistema de seguridad se realizó una tabla comparativa de los sistemas que existen en el mercado para la construcción de sistemas electrónicos mostrada a continuación:

Tabla 2. Comparativa de características de sistemas electrónicos programables

Raspberry PI	• Chip integrado Broadcom BCM2835, que contiene un procesador ARM11Posibilidad de (overclocking) • Un procesador gráfico videocore IV • Posibilidad de reproducir vídeo en 1080p. • Salida de vídeo y audio a través de un conector HDMI • Posee una conexión Ethernet 10/100 Wi-Fi, dos puertos USB incluidos, Wi-Fi USB, hub USB con alimentación. • Procesamiento 3 GHz • Cuenta con un lector de tarjetas SD • Da la posibilidad de instalar un sistema operativo en una tarjeta de memoria de 16 GB • Cuenta con una serie de conexiones o puertos de entrada y salida de propósito general o GPIO, permiten hacer todo tipo de interfaces como el control de otros dispositivos, proyectos de domótica, etc. • Cuenta con la distribución Raspbian derivada de Debian, Wheezy, Arch Linux y RISC OS. Existe la posibilidad de utilizar Android como sistema operativo.
PcDuino	• La CPU es una AllWinner A20 1Ghz ARM Cortex A7, • GPU Mali 400 dualcore, • 1GB de RAM, 4GB de memoria flash en placa • Contiene GPIO, ADC, I2C, UART, PWM, HDMI, USB, Ethernet, WiFi, IR, SATA
CIAA	• Sirve para crear un SBC, aplicaciones industriales como: maquinaria agrícola, maquinas industriales, robots, automatismos, vehículos • 8MB de SDRAM, 4MB de memoria Flash y una memoria EEPROM. • Se puede programar en lenguaje C • Su conectividad viene de conexiones como la RS485, RS232 serie, Ethernet, por bus CAN
DreamPlug	• No es un SBC. • Puede correr sistemas basados en Debian Linux • Contiene una CPU Marvell Kirkwood 88F6281 a 1.2Ghz, • 512MB de DDR2, • 1GB de flash • Integra puertos Ethernet, eSATA

Fuente: http://www.xataka.com/tag/raspberry-pi

Elaborado por: Carmen A. Hernández O. (2015)

De acuerdo a la tabla comparativa se ha establecido que el dispositivo electrónico programable (RASPBERRY PI) empleado en el desarrollo de este sistema poseía las características idóneas para la implementación de varios dispositivos de seguridad, debido a la capacidad de procesamiento que es de 3 GHz, además de que posee almacenamiento externo mediante el uso de una memoria SD, puertos USB, software libre y demás accesorios que la hacen versátil en comparación con los demás dispositivos.

Tabla 3. Características de sistemas de seguridad

SISTEMA DE SEGURIDAD INTEGRAL	SISTEMAS BOSCH	SISTEMAS D-LINK	SISTEMAS VIVOTEK
• Control de acceso a puerta principal • Sensores de movimiento • Sensores de vibración (ventanas) • Sensor de humo • Cámaras de vigilancia • Botón de pánico • Mensajes de alertas ante un intruso • Llamadas de emergencia • Control del sistema de cámaras desde dispositivo android • Control y monitoreo del sistema desde un ordenador	• Control de Acceso • Detección de Incendio • Detección de Intrusión • Megafonía y música ambiental	• Cámaras IP • Cloud IP (Cámara Inalámbrica mediante el internet WIFI)	• Cámaras de red • Cámaras PTZ • Detección de incendio

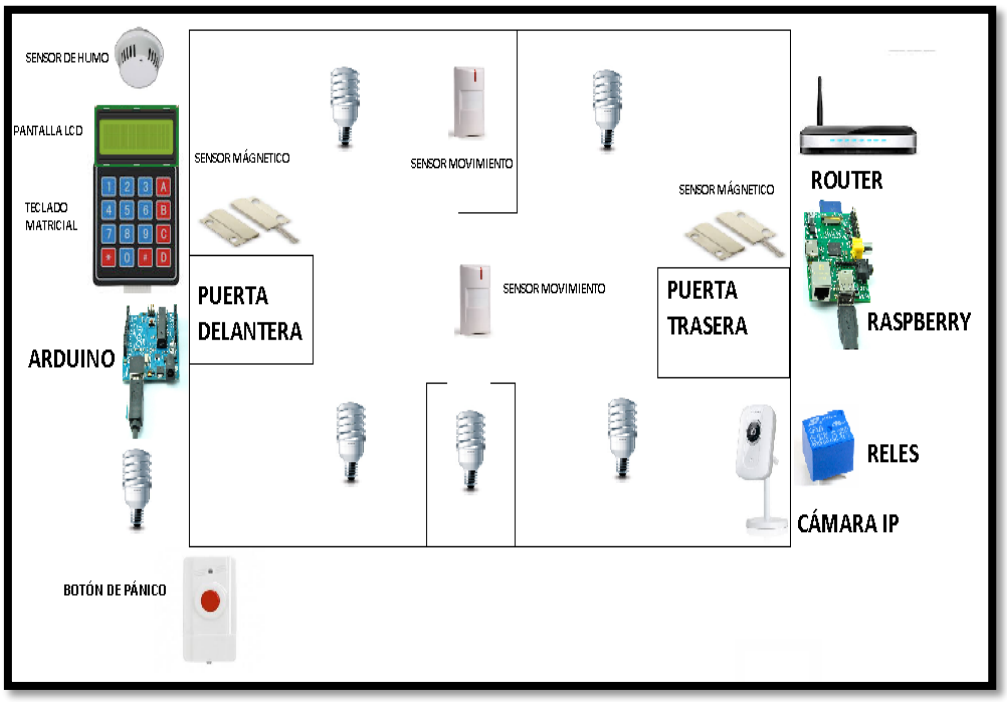
Elaborado por: Carmen A. Hernández Ordinola (2015)

Tabla 4. Costos de sistemas de seguridad

SISTEMA DE SEGURIDAD INTEGRAL	SISTEMAS BOSCH	SISTEMAS D-LINK	SISTEMAS VIVOTEK
$ 784,77 (Sistema) $100,00 (Instalación)	$1800,00	$500,00	$600,00
$884,77	**$1800,00**	**$500,00**	**$600,00**

Elaborado por: Carmen A. Hernández Ordinola (2015)

Fig. 35 Plano de ubicación de los elementos del sistema de seguridad integral



Elaborado por: Carmen A. Hernández O. (2015)

4.1.1. Establecimiento de la comunicación.

Como se ha mencionado en capítulos anteriores, el prototipo del sistema integral de control para la seguridad de vivienda consta con los siguientes dispositivos con sus funcionalidades:

- **Control de acceso al sistema:** Este sistema cuenta con un código de acceso que se basa en un cifrado de 4 números comprendidos del 0 al 9 y las letras de la A hasta la D. La misma

que el usuario define a su conveniencia, por defecto viene en la programación 1234 dado que en el arduino se programa este control y por ende viene predefinida. El cambio de clave podrá hacerlo desde el teclado ingresando como modo administrador presionando la letra C, en este menú se le pedirá al usuario que ingrese dos veces la nueva clave además presionando la tecla # y para aceptar los cambios deberá presionar D.

- **Sensor de movimiento:** Los sensores ubicados en el sistema poseen sensibilidad capaz de detectar movimientos a 3 metros de distancia. Estos sensores no necesitan ser calibrados, porque el nivel de sensibilidad dependerá solamente de la persona que los quiera utilizar. En el mercado existen sensores con alcance desde 3 a 9 metros de distancia.

- **Sensores magnéticos:** Estos sensores fueron ubicados en las puertas y ventanas de la casa, estos tampoco necesitan calibración, pues su configuración ya viene predefinida de fábrica. Su funcionamiento será activado siempre que las puertas y ventanas sean violentadas.

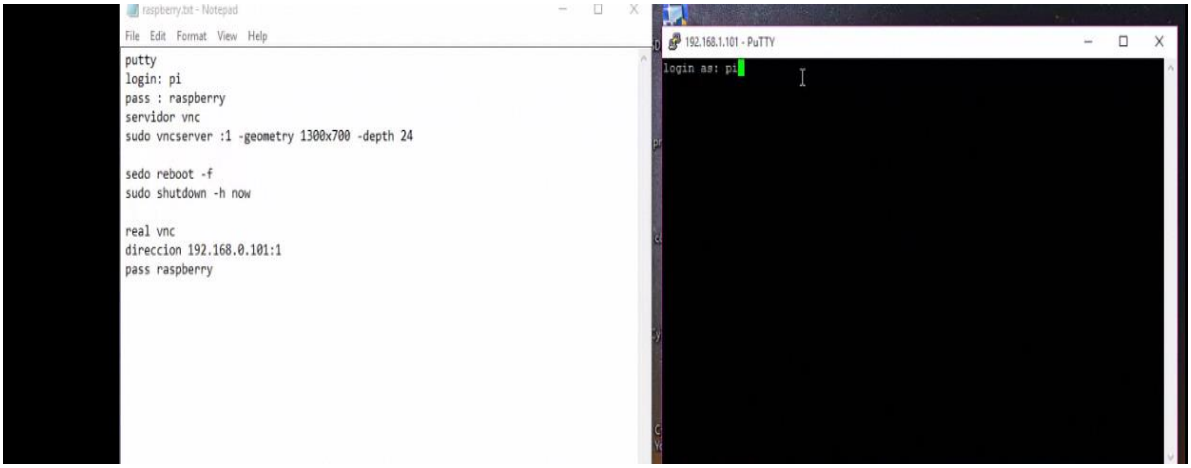
- **Sensor de humo:** Su funcionamiento básicamente detectando el nivel de Co2 que se encuentre dentro de la vivienda. Este nivel debe ser calibrado de acuerdo a las necesidades del usuario del sistema, los mismos que se realizan colocando un destornillador en medio del sensor, adaptándolo a los requerimientos. Los niveles que pueden ser detectados por este sensor van desde el humo emitido por una vela que ha sido apagada, así como el aliento humano hasta el humo más espeso.

- **Cámaras de video:** Estan ubicadas en las esquinas de las casas para cubrir las áreas de visualización, este dispositivo es instalado y configurado en la raspberry mediante el código que se especifíca más adelante además de la asignación de una dirección IP para que sea visualizada desde el internet. Lo que se necesita para su funcionamiento es, conectar la cámara al módulo raspberry y colocar las líneas de código.

- **Sensor de vibración:** Este dispositivo tambien debe ser calibrado para su correcto funcionamiento, al igual que el sensor del humo posee un lugar en medio del mismo que permite ser manipulado y configurado desde fuera del mismo. El sensor de este prototipo ha sido calibrado para que se active cuando la vibración sea fuerte, dado que si no se calibra, este puede funcionar con la mínima vibración.

- **Botón de pánico:** El botón sólo debe ser configurado mediante el módulo raspberry. Este dispositivo permite al usuario realizar una llamada de emergencia al 911 directamente al este botón ser presionado. Ahora bien se procede a la configuración del servidor y la comunicación con la cámara IP. Se ingresa al modo de configuración, en el cual se debe loguear con el usuario y contraseña predeterminada.

Fig. 36 Ingreso al modo de configuración para el servidor y asignación de la IP para la cámara

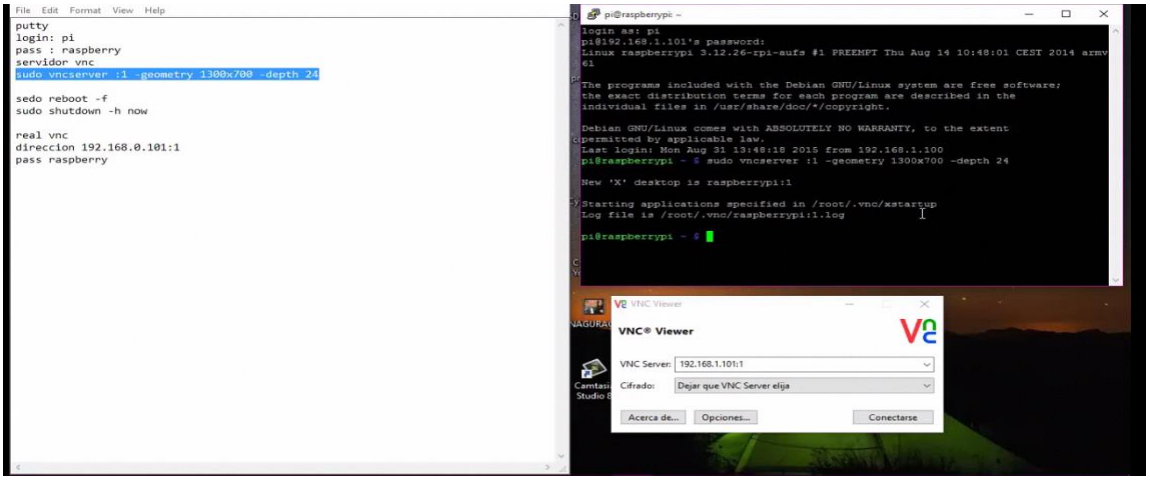


Elaborado por: Carmen A. Hernández O. (2015)

Una vez ingresado al sistema root se procede a configurar los parámetros para el servidor con el código siguiente:

sudo vncserver :1 –geometry 1300x700 –deght 24

Fig. 37 Configuración para el servidor y asignación de la IP

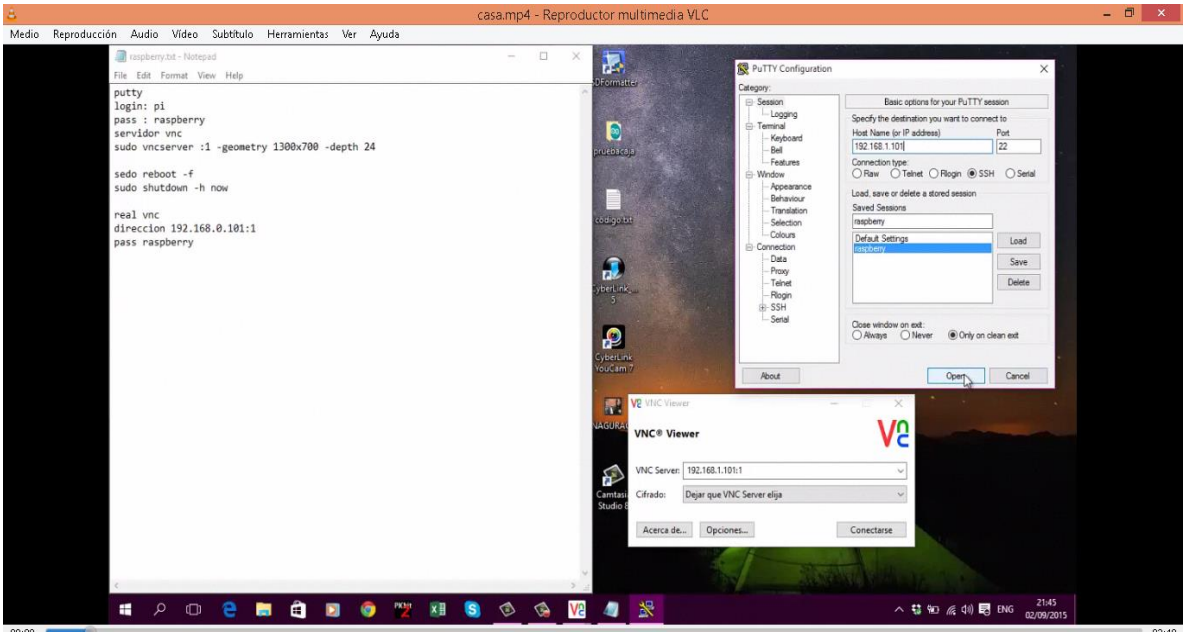


Elaborado por: Carmen A. Hernández O. (2015)

Después de ingresar se accederá al escritorio del sistema operativo

Luego a continuación se abrirá la pantalla de configuración de la IP que se asignará a la IP para que sea vista desde la web.

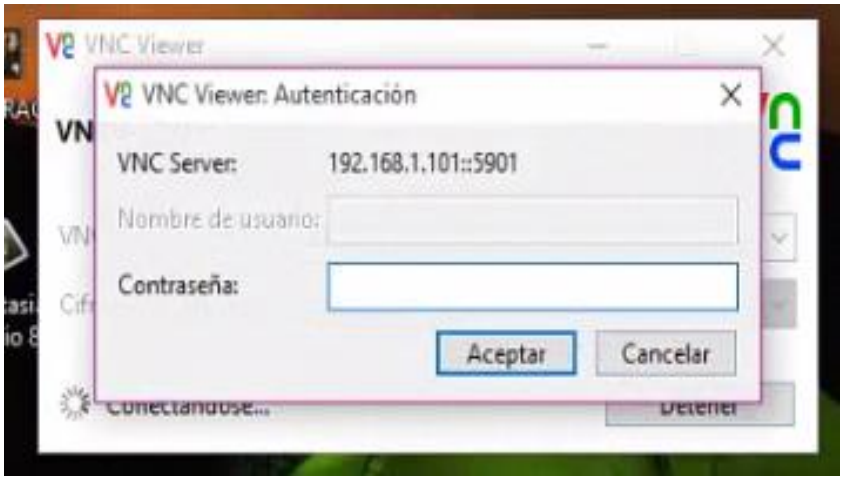
Fig. 38 Asignación de la IP para la cámara



Elaborado por: Carmen A. Hernández O. (2015)

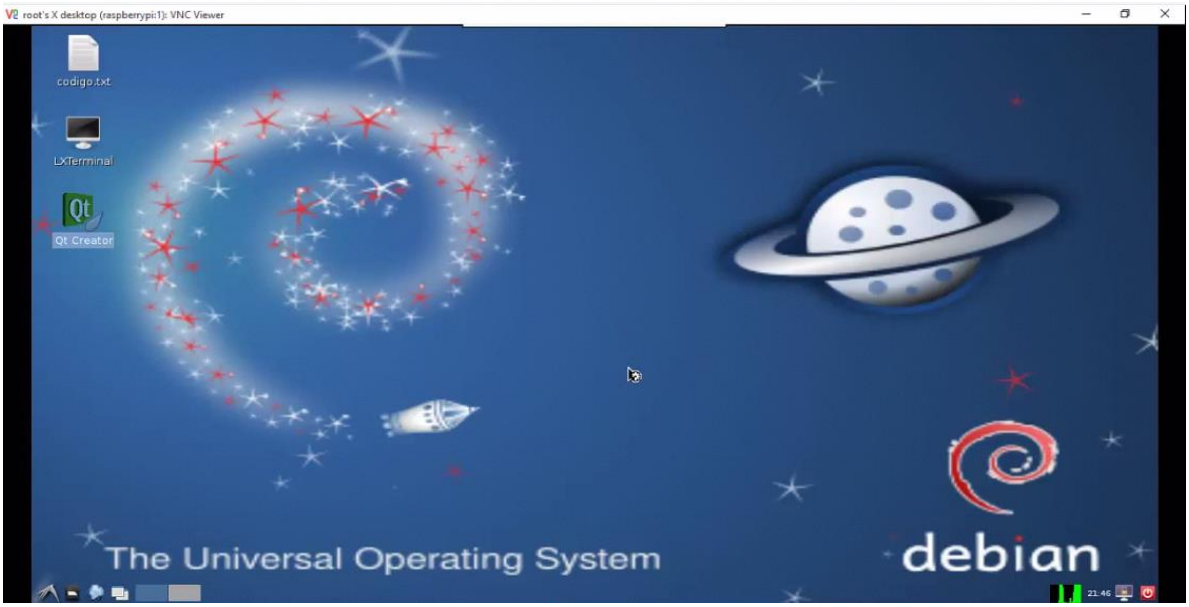
A continuación se reiniciará el sistema y se podrá acceder al escritorio para el siguiente proceso de programación de la aplicación que controlará los dispositivos instalados.

Fig. 39 Acceso al software para el diseño de la aplicación



Elaborado por: Carmen A. Hernández O. (2015)

Fig. 40 Escritorio del Sistema Operativo



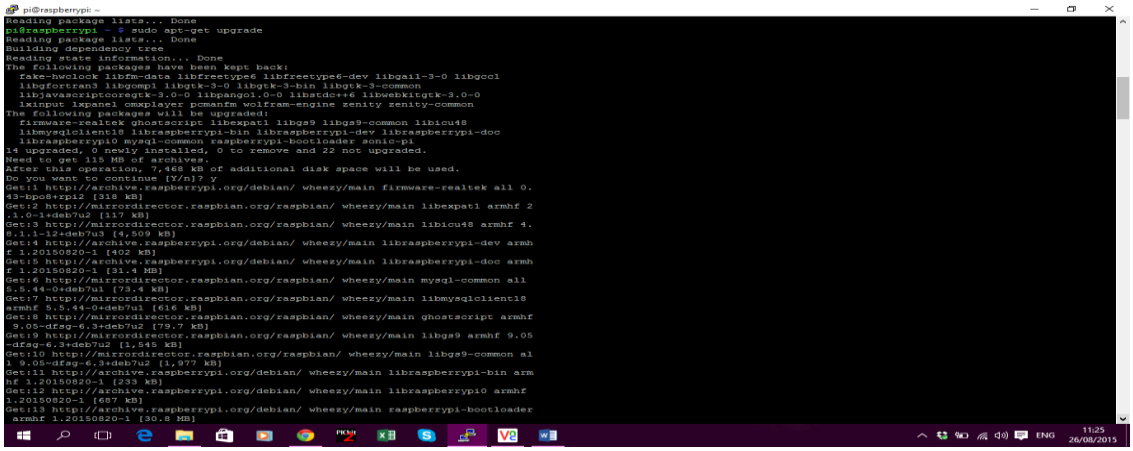
Elaborado por: Carmen A. Hernández O. (2015)

4.1.2. Diseño de la aplicación para el sistema de seguridad.

Para el control desde la aplicación instalada en el computador se diseño la misma mediante la utilización del software libre que permita diseñar todo tipo de aplicaciones.los siguientes procesos que se llevaron a cabo para la programación fueron los siguientes:

Una vez en la pantalla de inicio del sistema operativo se deberá iniciar la Raspberry

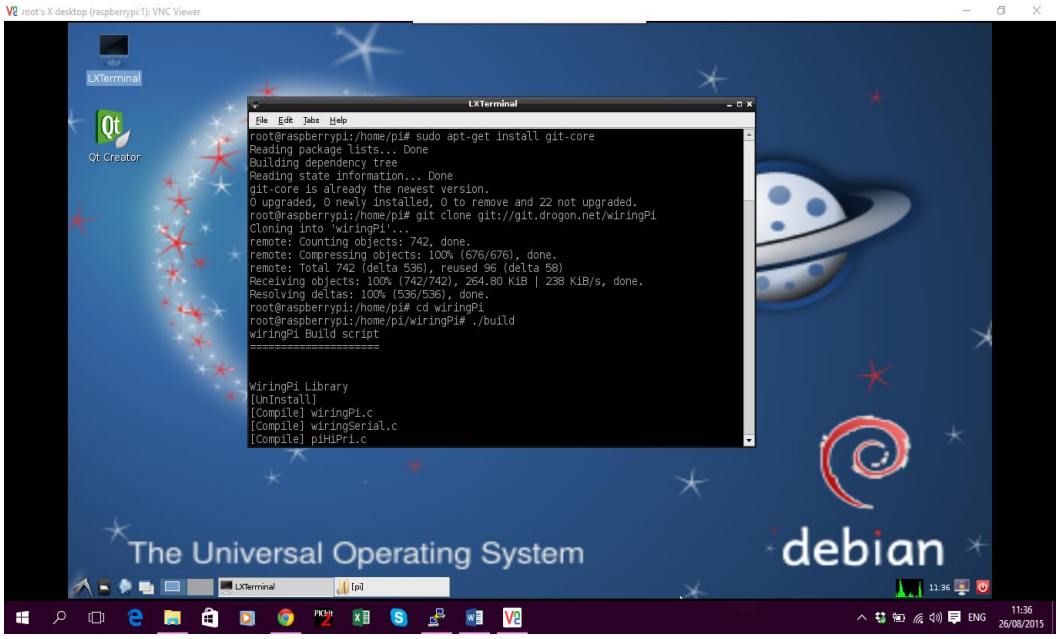
Fig. 41. Pantalla de carga de la Raspberry



Elaborado por: Carmen A. Hernández O. (2015)

Luego de esperar un tiempo prudencial se cargará la pantalla de root de la raspberry

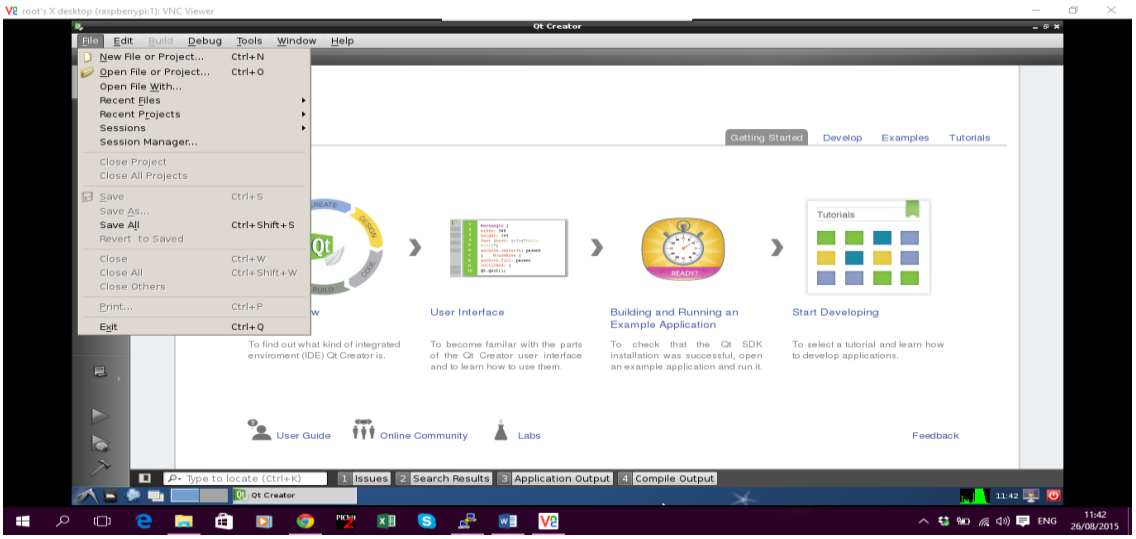
Fig. 42 Raspberry iniciada



Elaborado por: Carmen A. Hernández O. (2015)

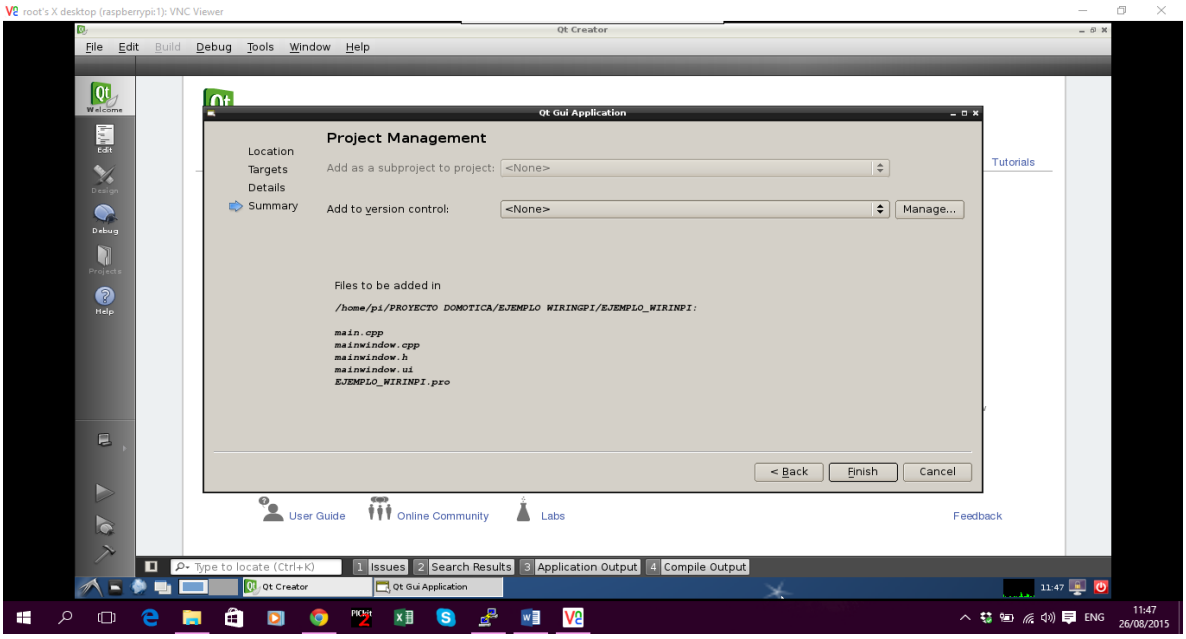
A continuación se accedera al software predeterminado de la Raspberry para el diseño de la aplicación QtCreator que estará ubicado en el escritorio y se creará un nuevo proyecto

Fig. 43 Interfaz para el diseño de la aplicación de Escritorio



Elaborado por: Carmen A. Hernández O. (2015)

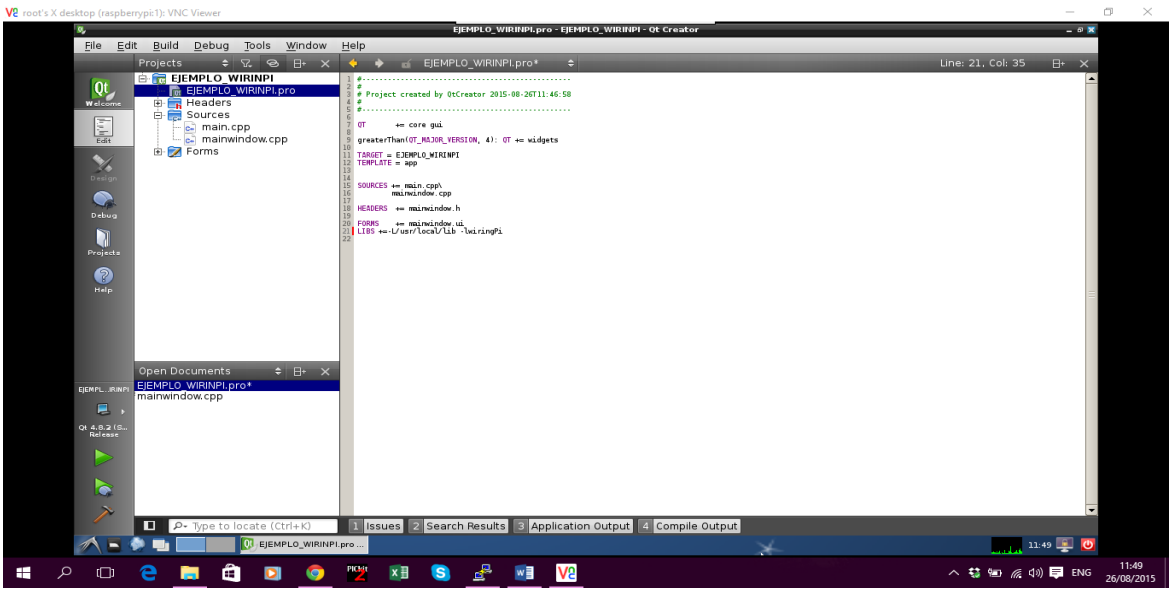
Fig. 44 Asignando características para el lenguaje de programación de la Raspberry PI



Elaborado por: Carmen A. Hernández O. (2015)

Una vez especificado los parámetros se procedió al diseño de la interfaz de escritorio, para lo cual el programa generó un código automático como el mostrado a continuación:

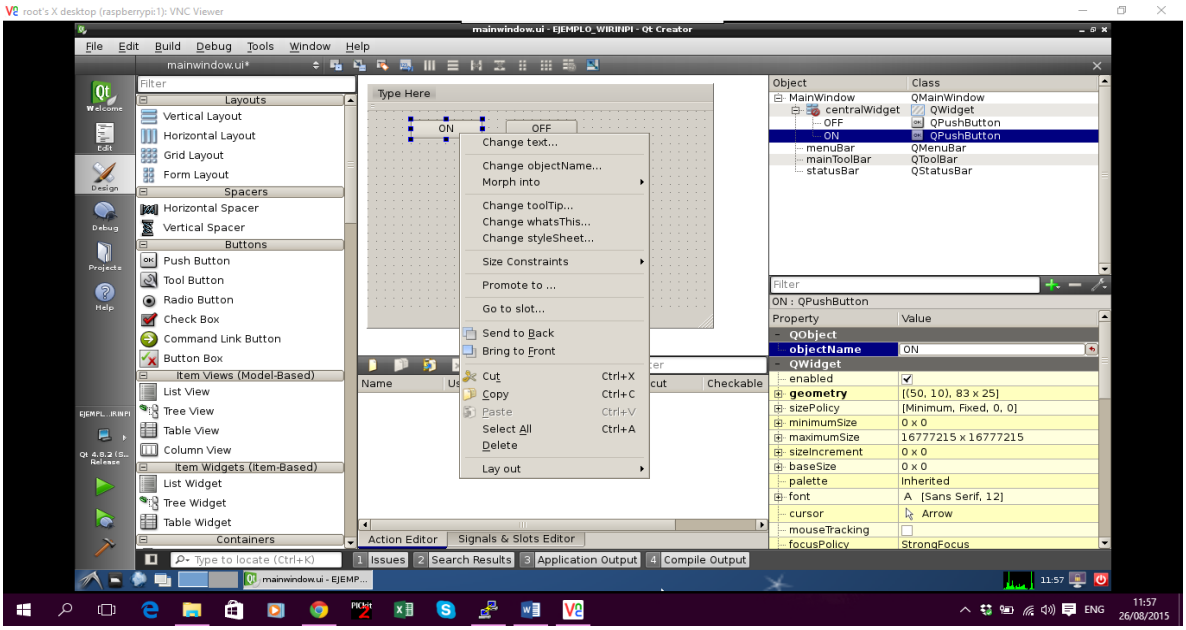
Fig. 45 Código generado al inicio de la aplicación



Elaborado por: Carmen A. Hernández O. (2015)

Luego se procederá al diseño de los botones y demás opciones de la aplicación.

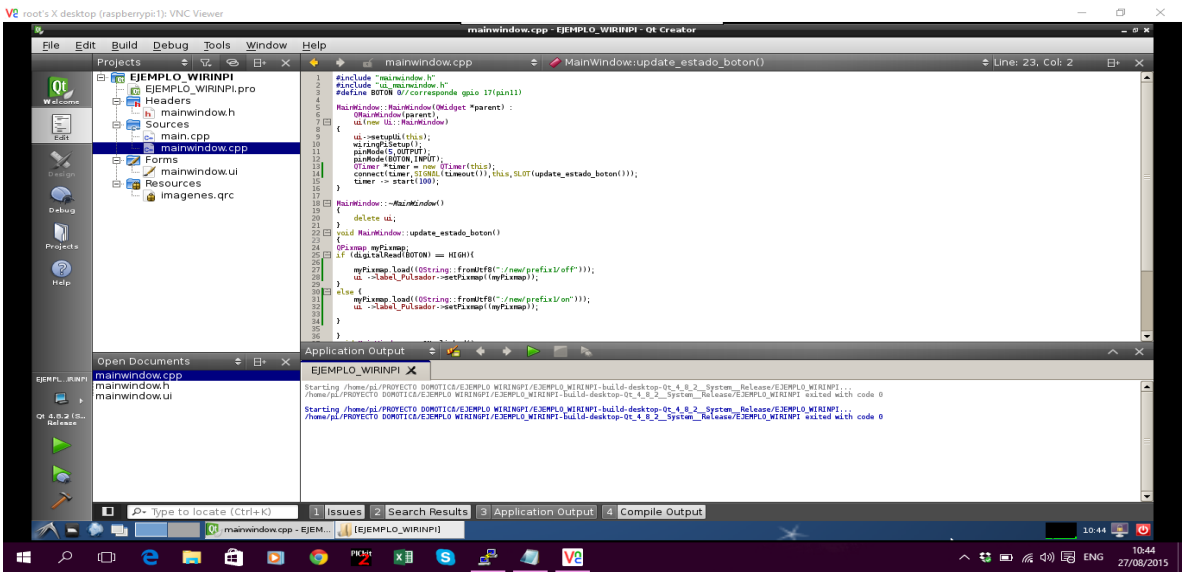
Fig. 46 Asignando botones y funciones para la aplicación



Elaborado por: Carmen A. Hernández O. (2015)

Una ve que se le asigne los botones el software creará las líneas de código y las funciones para que en el momento de sincronizar las líneas de código de los dispositivos electrónicos, estos funcionen correctamente.

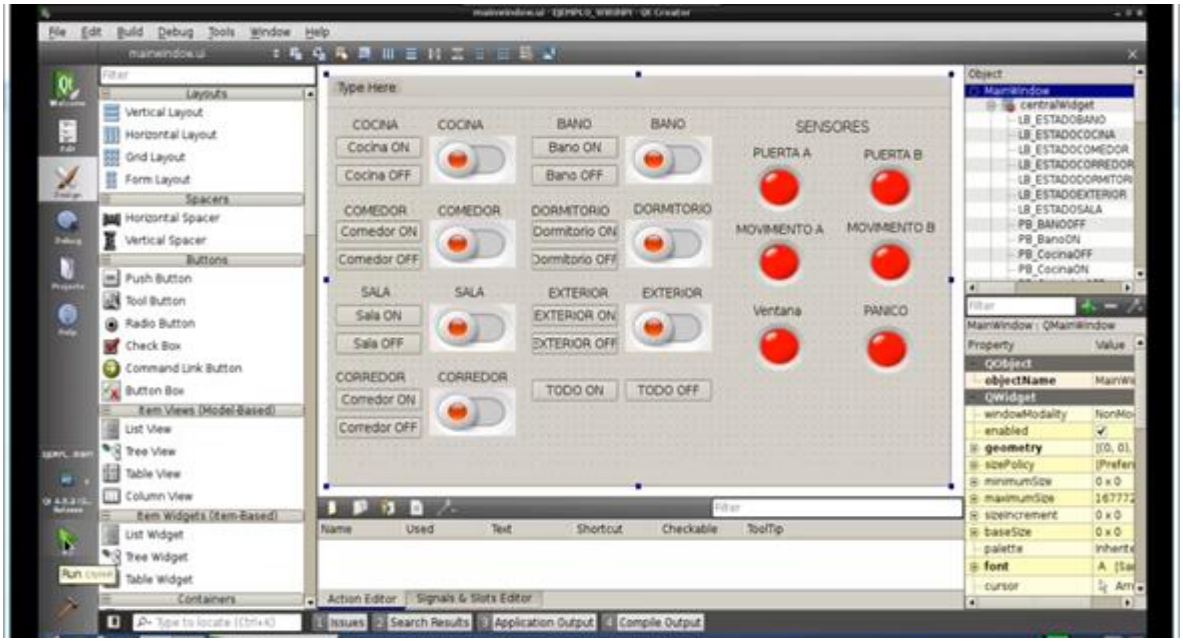
Fig. 47 Código generado por cada botón y función para la aplicación



Elaborado por: Carmen A. Hernández O. (2015)

Una vez diseñado colocados los botones la aplicación quedará de la siguiente manera:

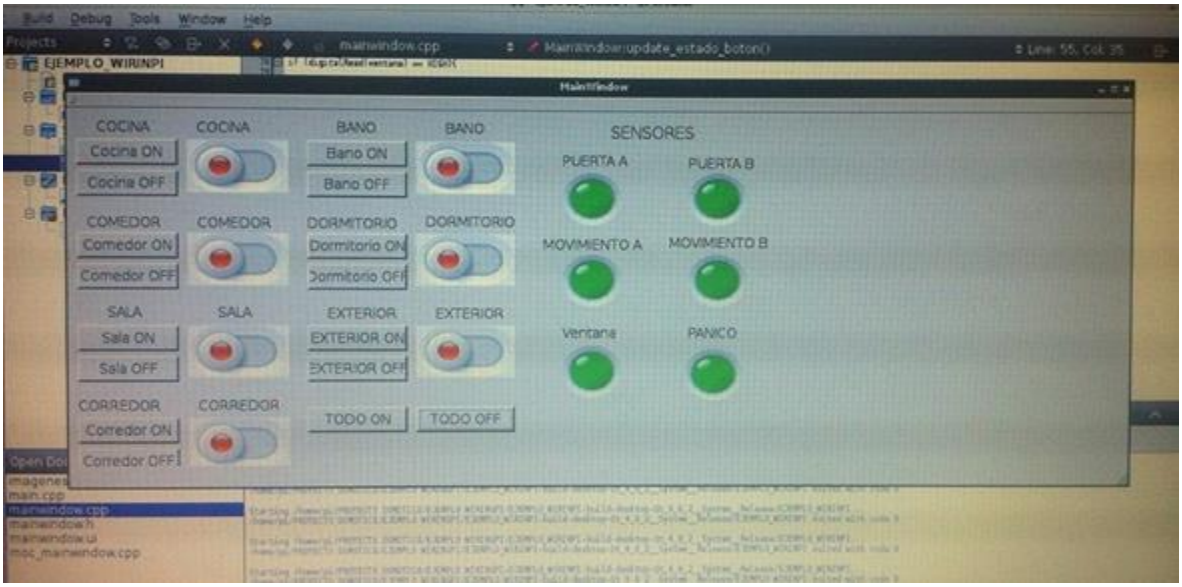
Fig. 48 Interfaz preliminar de la aplicación de escritorio



Elaborado por: Carmen A. Hernández O. (2015)

A continuación se ejecuta la aplicación

Fig. 49 Interfaz ejecutada



Elaborado por: Carmen A. Hernández O. (2015)

Luego de los pasos de diseño de la aplicación de escritorio se procede a la configuración de las líneas de código para los sensores del sistema integral de seguridad, cabe destacar que este sistema cuenta con un aviso o alerta que se enviará mediante un mensaje de texto al número de celular que se establezca en el código, para las funciones descritas a continuación.

- **Programación de los sensores de movimiento**

Cuadro 1. Líneas de código para los sensores de movimiento

```
void sendsms2()//enviar mensajes a un numero de telefono
{
Serial.println("enviando mensaje s2");
SIM900.print("AT+CMGF=1\r"); // comando AT para realizar mensajes
delay(100);
SIM900.println("AT + CMGS = \"+593998749007\"");
delay(100);
SIM900.println("se ha detectado movimiento en la venta sin desactivar la alarma"); // mensaje a enviar
delay(100);
SIM900.println((char)26);// finalizar los comandos AT
delay(100);
SIM900.println();
delay(5500); // tiempo para que el modulo envie el mensaje
SIM900power();
}
void sendsms3()//enviar mensajes a un numero de telefono
{
Serial.println("enviando mensaje s3");
SIM900.print("AT+CMGF=1\r"); // comando AT para realizar mensajes
delay(100);
SIM900.println("AT + CMGS = \"+593998749007\"");// enviar mensajes con formato internacional(+593<numero de telefono>)
delay(100);
SIM900.println("se ha detectado moviemiento en la sala frontal sin desactivar la alarma"); // mensaje a enviar
delay(100);
SIM900.println((char)26);  // finalizar los comandos AT
delay(100);
SIM900.println();
delay(5500);  // tiempo para que el modulo envie el mensaje
SIM900power();
}
void sendsms4()//enviar mensajes a un numero de telefono
{
Serial.println("enviando mensaje s4");
SIM900.print("AT+CMGF=1\r"); // comando AT para realizar mensajes
delay(100);
SIM900.println("AT + CMGS = \"+593998749007\"");// enviar mensajes con formato internacional(+593<numero de telefono>)
delay(100);
SIM900.println("se ha detectado moviemiento en la sala posterior sin desactivar la alarma"); // mensaje a enviar
```

```
delay(100);
SIM900.println((char)26);// finalizar los comandos AT
delay(100);
SIM900.println();
delay(5500); // tiempo para que el modulo envie el mensaje
SIM900power();
}
void sendsms5()//enviar mensajes a un numero de telefono
{
```

Elaborado por: Carmen A. Hernández O. (2015)

- **Programación del sensor de humo**

Cuadro 2. Líneas de código para el sensor de Humo

```
void sensor135()
{
int valor = analogRead(A8); //Serial.print("lectura sensor:");
//Serial.println(valor);
if (valor >= 200)
{
 humo = true;

if (humo == true)
{
 puerta.write (90);
digitalWrite(39,HIGH);
sendsms5();
Serial.print('a');
digitalWrite(39,LOW);
humo == false;
}
if(humo == false);
digitalWrite(39,LOW);
}
delay(10);
}
void SIM900power()
{
  digitalWrite(9, HIGH)
delay(1000);
digitalWrite(9, LOW);
  delay(5000);
}
void LlamadaEmergencia()
{ //llamada a un numero de telefono
  Serial.println("LLAMADA EMERGENCIAS");
SIM900.println("ATD + +593998749007;"); // llamada con formato internacional(+593<numero de telefono>)
delay(100);
SIM900.println();
delay(30000);
SIM900.println("ATH");   // colgar despues de 30 segundos
digitalWrite(aviso,LOW);
}
void sendSMS()//enviar mensajes a un numero de telefono
{
void sendsms5()//enviar mensajes a un numero de telefono
```

```
{
Serial.println("enviando mensaje s5");
SIM900.print("AT+CMGF=1\r"); // comando AT para realizar mensa
delay(100);

SIM900.println("AT + CMGS = \"+593998749007\"");
delay(100);
SIM900.println("ALERTA!! ALTAS CONCENTRACIONES DE HUMO"); // mensaje a enviar
delay(100);
SIM900.println((char)26); // finalizar los comandos AT
delay(100);
SIM900.println();
delay(5500);  // tiempo para que el modulo envie el mensaje
SIM900power();
}
```

Elaborado por: Carmen A. Hernández O. (2015)

- **Botón de pánico**

Cuadro 3. Línea de código para el botón de pánico

```
void LlamadaEmergencia()
{
//llamada a un numero de telefono
Serial.println("LLAMADA EMERGENCIAS");
SIM900.println("ATD + +593998749007;"); // llamada con formato internacional(+593<numero de telefono>)
delay(100);
SIM900.println();
delay(30000);
//
  SIM900.println("ATH");
// colgar despues de 30 segundos
digitalWrite(aviso,LOW);
}
```

Elaborado por: Carmen A. Hernández O. (2015)

4.1.3. Identificación y Autentificación para el usuario.

Para esta etapa se considera como identificación y autentificación al sensor magnético junto con el uso del código de acceso a las puertas de ingreso a la vivienda. Cabe mencionar que este dispositivo también cuenta con aviso al propietario de la vivienda en el caso de que exista alguna persona que quiera ingresar a la misma aunque haya burlado el código de acceso. A continuación se presenta las líneas de código para el código de acceso y nueva clave:

Cuadro 4. Líneas de código para el acceso y autenticación

```
void setup()
{
puerta.attach(12);
char co[5] = {'1','2','3','4'};
lcd.begin(16, 2);
delay(500);
puerta.write(90);
delay(20);
  puerta.write(10);
for(int i =0;i<=3;i++)
{  //LEER CONTRASEÑA DE LA EEPROM
co[i]= EEPROM.read(i);
lcd.print(co[i],DEC);
delay(500);
}
lcd.setCursor(0, 0);
lcd.print("BIENVENIDO");
lcd.setCursor(0, 1);
lcd.print("ESTA INICIANDO");
pinMode(13,OUTPUT);
pinMode(9,OUTPUT);
pinMode(39,OUTPUT);
  pinMode(53,OUTPUT);
//SALIDA VENTANA MAGNETICA
 pinMode(aviso,OUTPUT);
 pinMode(s0, INPUT);
// SENSOR PUERTA A
  pinMode(s1, INPUT);
// SENSOR PUERTA B
  pinMode(s2, INPUT);
// SENSOR VENTANA
  pinMode(s3, INPUT);
// SENSOR PUERTA B
  pinMode(s4, INPUT);
// SENSOR VENTANA
  digitalWrite(13, HIGH); // mantiene la cerradura cerrada
bloqueo = true;
delay(2000);
lcd.clear();
lcd.setCursor(5, 0);
lcd.print("PUERTOS");
lcd.setCursor(2, 1);
lcd.print("CONFIGURADOS");
 Serial.begin(9600);
lcd.clear();
lcd.setCursor(4, 0);
lcd.print("INGRESAR");
lcd.setCursor(0, 1);
lcd.print("PASS: ____");
digitalWrite(13, LOW); // mantiene la cerradura cerrada
}
void loop()
```

```
{
  //programa principal
estados5 = digitalRead(s5);
if (estados5 == HIGH )
{
digitalWrite(41,HIGH);
LlamadaEmergencia();
}
else{
digitalWrite(41,LOW);
}
sensor135();
cl[contador] = teclado.getKey(); // lectura de datos del teclado matricial y almacenamiento en un array
if (cl[contador] != NO_KEY)
{// verificacion de que el teclado sea presionado
  switch (cl[contador])
{
//switch para verificar los diferentes estados del teclado matricial
case 'A'://en caso de que la tecla A se haya presionado
comp = comprobacion(cl,co)+1;
// comp almacena si los 4 numeros son iguales
if (comp==4 && error < 3)
{
//si los 4 digitos son los mismos y no ha sido ingresado mas de 4 veces mal el password
digitalWrite(13, LOW); //abrir la cerradura
error = 0;
//marcar el error en cero para reiniciar el sistema
lcdtextoizq("PASS: CORRECTO");
delay(1000);
lcd.clear();
lcd.setCursor(4, 0);
lcd.print("ALARMA");
lcd.setCursor(2, 1);
lcd.print("DESARMADA");
bloqueo = false;
puerta.write(90);
//lcdnumero();
} //fin del if de comp >=4
else{
 //si al pulsar 'A' no son iguales // emitir luces de advertencia de codigo erroneo
digitalWrite(13, LOW);
delay(250);
digitalWrite(13, HIGH);
delay(250);
digitalWrite(13, LOW);
delay(250);
digitalWrite(13, HIGH);
delay(250);
digitalWrite(13, LOW);
delay(250);
digitalWrite(13, HIGH);
lcdtextoizq("PASS: INCORRECTO");
bloqueo = true;
puerta.write(10);
```

```
delay(1000);
error = error + 1; // incrementar en uno el error cada vez que sea ingresado de manera incorrecta
lcdnumero();
}
// fin del else al if comp>=4
break;
//break al caso 'a'
 case 'B':
 lcd.clear();
lcd.setCursor(4, 0);
lcd.print("ALARMA");
lcd.setCursor(4, 1);
lcd.print("ARMADA");
puerta.write(10);
delay(2000) ;
for(int i = 0 ; i<4;i++)
{ // borra el codigo temporal guardado
 cl[i]='0';
//bloqueo = true;
}//fin del for
lcdnumero();
bloqueo = true;
digitalWrite(13, HIGH); // mantiene la cerradura cerrada
break;  //break al caso 'a'
 case 'C':
 repetirpass();
if (comp>=4){  //si la contraseña concide entonces
lcd.clear();
delay(10);
lcdtextoizq("Pass correcta");
delay(500);
nuevapass();
vuelve();
//volver a introducir
} //funcion cambio de password
else{
lcd.clear();
delay(10);
lcdtextoizq("No pudo cambiar");
delay(2000);
lcd.clear();
delay(10);
lcd.setCursor(0,0);
lcd.print("C CONFIGURAR");
lcd.setCursor(0,1);
delay(10);
lcd.print("B SALIR");
}
comp = comprobacion(cn,cl);
if (comp>=4){
lcd.clear();
delay(10);
lcdtextoizq("Correcto");
delay(500);
```

```
lcd.clear();
delay(10);
lcdtextoizq("Nueva pass");
delay(500);
lcd.clear();
delay(10);
lcdtextoizq("guardada");
delay(500);
}
```

Elaborado por: Carmen A. Hernández O. (2015)

Cuadro 5. Líneas de código para que el usuario pueda cambiar la contraseña de acceso

```
}
void lcdnumero()
{
lcd.clear();
lcd.setCursor(4, 0);
lcd.print("INGRESAR");
lcd.setCursor(0,1);
lcd.print("PASS: ");
lcd.setCursor(6,1);
lcd.print("____");
cursorr=6;
contador=0;
} //fin de lcdresetparatexto
void
repetirpass()
{
lcd.clear();
delay(10);
int i =0;
lcdtitulo("Introduzca");
delay(800);
lcd.clear();
delay(10);
lcdtitulo("pass anterior");
delay(1000);
lcd.clear();
delay(10);
lcdtextoizq("Finalice con #");
delay(1000);
lcdnumero();
while (i<=4)
{            //hará esto 4 vces
cl[contador] = teclado.getKey();  //obtiene valor
if (cl[contador]!=NO_KEY)
{  //si detecta una tecla entonces
switch (cl[contador])
{
case '#':  //comprueba si la pass escrita es igual a la anterior
comp=0;
comp = comprobacion(cl,co);
if (comp>=4){ //si es igual
```

```
lcd.clear();
delay(10);
lcdtextocentrado("Correcto");
  i=5;} //fin
if comp<=4
else
}//fin del switch
}//fin del if no key
}//fin del if contador==4
 //fin del while
}//fin de la funcion repetirpass
void
nuevapass()
{
lcd.clear();
delay(10);
lcdtitulo("Intro nueva pass");
delay(1000);
lcd.clear();
delay(10);
lcdtitulo("Finalice con '#'");
delay(1500);
lcd.clear();
delay(10);
lcdtextoizq("SOLO NUMEROS");
delay(1500);
lcdnumero();
while(contador<=4)
{ //cuatro veces el ciclo
cl[contador] = teclado.getKey();
if (cl[contador]!=NO_KEY)
{ //si escribi algo
switch (cl[contador])
{
case '#':
  if (contador>=4)
{ // si ya escribio 4 numeros
lcd.clear();
delay(10);
lcdtextoizq("Vuelve a ingresarla");
delay(1000);
contador=5;
}//fin del if contador==$
```

Elaborado por: Carmen A. Hernández O. (2015)

Cuadro 6. Líneas de código para los sensores magnéticos de apertura de puertas

```
void sendSMS()//enviar mensajes a un numero de telefono
{
Serial.println("enviando mensaje");
SIM900.print("AT+CMGF=1\r"); // comando AT para realizar mensajes
```

```
delay(100);
SIM900.println("AT + CMGS = \"+593998749007\"");
delay(100);
SIM900.println("Error en codigo de acceso a puerta principal"); // mensaje a enviar
delay(100);
SIM900.println((char)26);// finalizar los comandos AT
delay(100);
SIM900.println();
delay(5500); // tiempo para que el modulo envie el mensaje
SIM900power();
}
void sendsms0()//enviar mensajes a un numero de telefono
{
Serial.println("enviando mensaje s0");
SIM900.print("AT+CMGF=1\r"); // comando AT para realizar mensajes
delay(100);
SIM900.println("AT + CMGS = \"+593998749007\"");
delay(100);
SIM900.println("se ha abierto la puerta principal sin desactivar la alarma"); // mensaje a enviar
delay(100);
SIM900.println((char)26);  // finalizar los comandos AT
delay(100);
SIM900.println();
delay(5500); // tiempo para que el modulo envie el mensaje
SIM900power();
}
void sendsms1() //enviar mensajes a un numero de telefono
{
Serial.println("enviando mensaje s1");
SIM900.print("AT+CMGF=1\r"); // comando AT para realizar mensajes
  delay(100);
SIM900.println("AT + CMGS = \"+593998749007\"");
delay(100);
SIM900.println("se ha abierto la puerta posterior sin desactivar la alarma"); // mensaje a enviar
delay(100);
SIM900.println((char)26); // finalizar los comandos AT
```

```
delay(100);
SIM900.println();
delay(5500);   // tiempo para que el modulo envie el mensaje
SIM900power();
}
```

Elaborado por: Carmen A. Hernández O. (2015)

4.2. Discusión.

Los autores que han realizado sus tesis se basan tambien en sistemas de seguridad para las viviendas, con la única diferencia de que estos, solo utilizan un dispositivo para llevar el control, una de ellas utiliza solo cámaras de vigilancia, otros utilizan solo sensores de movimiento y finalmente la última tesis qué tambien usa sensores a diferencia de que utiliza LabView.

Los proyectos que se han tomado como referencia para el desarrollo de este proyecto, han permitido que se desarrolle un prototipo de seguridad integral con gran parte de sensores, dispositivos de vigilancia, de acceso y de emergencia, con el objetivo de ofrecer satisfacción a quien utilice este sistema.

En este caso para el correcto desarrollo de la conexión remota se decidió emplear una tecnología que se orienta a la electrónica, asi como el uso del internet para la manipulación de una aplicación de escritorio que sería la encargada de controlar los diferentes dispositivos de seguridad, convirtiendo a este prototipo como un mecanismo indispensable para un desempeño eficiente e innovador de acuerdo al mundo tecnológico.

Este sistema integral de seguridad se basó en la programación del módulo Raspberry y Arduino permitiendo la obtención de buenos resultados en comparación con los demás sistemas. Las funciones realizadas por este prototipo fueron:

- La cámara IP implementada logró ser manipulada y pudieron ser visualizadas las imágenes que ha captado mediante la aplicación diseñada.

- Este sistema funciona como un ordenador además de que posee las herramientas necesarias para que funcione debidamente.

- Tanto sensores como botón de pánico son los mecanismos que pueden ser controlados por el módulo de la Raspberry, además de que se debe contar con el servicio de internet para el monitoreo de este sistema.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones.

- Dado a los objetivos planteados y dando mención a que se debía establecer la comunicación entre el sistema integral y el servidor; se concluye que todo esto fue posible mediante los dispositivos conectados a la Raspberry y una dirección IP asignada y dedicada para uso exclusivo del sistema. La utilización del puerto GPIO permitió la comunicación entre los dispositivos extrernos e interno para que fluyera sin inconvenientes; el esquema de ubicación de los dispositivos logró que cada uno cumpla con las funciones para que así no existiera algún inconveniente cuando se inicie la comunicación entre el sistema y el ordenador.

- Dado que en el diseño de la aplicación se realizó la comunicación de manera inalámbrica y mediante un escritorio remoto esta permitió el correspondiente acceso correcto a cada una de las funciones programadas en la Raspberry PI y en el módulo Arduino. Como se trata de un sistema de seguridad este logró ser manipulado solo por el propietario de la casa y por quien el designe como usuarios secundarios, mediante el acceso a una página web con protocolo HTTPS de manera segura.

- Una vez terminadas las aplicaciones se procedió a la comprobación del sistema mediante la identificación y autenticación utilizando la aplicación de escritorio remoto para la administración del sistema de seguridad, y a través de la cámara poder visualizar las imágenes emitidas a tiempo real. El sistema logró obtener imágenes en tiempo real demostrando su correcto funcionamiento comprobando todos los sensores instalados concluyendo que este sistema es funcional y le permitirá al dueño del inmueble sentirse más seguro cuando no se encuentre en casa.

5.2. Recomendaciones.

En base a las conclusiones de este proyecto de investigación se procede a las siguientes recomendaciones:

- Cuando se realicen trabajos con muchos dispositivos es necesario establecer correctamente el funcionamiento individual de cada uno de ellos, para que así cuando los mismos vayan a ser implementados no presenten inconvenientes dado que estos poseen características, estructuras y lenguajes de programación distintos por ello es necesario seleccionar de manera concreta y correcta como, para qué y porque se utilizarán, una herramienta útil sería utilizar los diagramas de bloques que de una u otra manera permiten establecer los parámetros de funcionamiento que tendrá el sistema a diseñar o desarrollar.

- Cuando se trate de diseño de aplicaciones que serán acopladas a sistemas ya sea de seguridad, control o demás se deberán utilizar softwares que sean de fácil utilización para el usuario, además cuando se trata de aplicaciones basados en lenguajes de programación se recomienda revisar minuciosamente la sintaxis e instalación de las librerías para que durante el desarrollo de la misma no surjan inconvenientes cuando se necesite compilar el código.

- Al trabajar con módulos tales como: Raspberry PI y Arduino, se debe tomar en consideración manipular con sumo cuidado estos dispositivos, dado que los mismos trabajan con señales eléctricas y puede existir algún fallo si no se realiza una conexión adecuada, afectando directamente al sistema y repercutiendo en el fallo parcial o total, además no olvidar que los demás dispositivos tampoco deberán ser manipulados por terceras personas, si se debería realizar un mantenimiento de los equipos deberá ser por una persona autorizada.

CAPÍTULO VI

BIBLIOGRAFÍA

[1] J. Restrepo, «Wordpress,» 28 Octubre 2015. [En línea]. Available: http://juliorestrepo.files.wordpress.com/2010/08/redes-de-computadoras-tanenbaum-4ta-edicion-espanol.pdf. [Último acceso: 28 Octubre 2015].

[2] A. S. Tanenbaum y D. J. Wetherall, Redes de Computadoras, Quinta ed., L. M. Cruz, Ed., México: Pearson, 2012.

[3] monografias.com, «monografias.com,» 28 Octubre 2015. [En línea]. Available: http://www.monografias.com/trabajos-pdf2/redes-comunicaciones/redes-comunicaciones.pdf. [Último acceso: 28 Octubre 2015].

[4] J. Dordoigne, Redes Informáticas. Nociones Fundamentales (Protocolos, Arquitecturas, Redes Inalámbricas, Virtualización, Seguridad, IPV6, ...)), Quinta ed., España: Eni, 2008.

[5] D. H. E. S. Carlos Alvarez, «Repositorio Espol,» 15 Mayo 2007. [En línea]. Available: http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-35940.pdf . [Último acceso: 11 Junio 2015].

[6] J. F. Talamanes, «Sistema de Monitoreo para casa habitacion,» *Revista Digital Universitaria,* vol. VII, nº 1, p. 19, 2006.

[7] DocPlayer, «DocPlayer,» 28 Octubre 2015. [En línea]. Available: http://docplayer.es/8812587-Sistema-de-monitoreo-integral-para-casa-habitacion.html. [Último acceso: 28 Octubre 2015].

[8] J. M. Angulo U., Microcontroladores PIC, Segunda ed., Madrid: McGraw Hill, 2006, p. 295.

[9] P. A. Ramón, Sensores y Acondicionadores de la señal, Marcombo: Alfaomega, 2004, p. 480.

[10] Voltium, «Voltium,» 16 Marzo 2010. [En línea]. Available: http://www.voltimum.es/articulos-tecnicos/sensores-movimiento. [Último acceso: 27 Agosto 2015].

[11] eHow, «eHow en Español,» 29 Agosto 2015. [En línea]. Available: http://www.ehowenespanol.com/tipos-sensores-vibracion-lista_317332/. [Último acceso: 29 Agosto 2015].

[12] Anónimo, «Sensing,» Agosto 2015. [En línea]. Available: http://www.sensores-de-medida.es/sensing_sl/MEDIDA-DE-VIBRACIONES_151/Sensores-de-vibraci%C3%B3n_290/. [Último acceso: 2015 Agosto 2015].

[13] J. L. Giordano, «Profísica,» 06 Abril 2006. [En línea]. Available: http://www.profisica.cl/comofuncionan/como.php?id=11. [Último acceso: 29 Agosto 2015].

[14] M. Miguez, «TecnoSeguro,» 29 Agosto 2015. [En línea]. Available: http://www.tecnoseguro.com/faqs/alarma/%C2%BFque-es-un-detector-magnetico-de-apertura.html. [Último acceso: 29 Agosto 2015].

[15] R. O. Abata Castro, «TESIS PARA REVISION S.P.docx,» U.T.C, Latacunga.

[16] G. Luis, «Tip GMSI: ¿Qué son los botones de pánico?,» 15 Abril 2013. [En línea]. Available: http://www.luisgyg.com/blog/2013/04/15/que-son-los-botones-de-panico/. [Último acceso: 29 Agosto 2015].

[17] T. d. Robótica, Guía Básica de Arduino, Bogotá, 2010.

[18] E. Upton y G. Halfacree, Raspberry PI Guia de Usuario, Segunda ed., Estados Unidos, 2010.

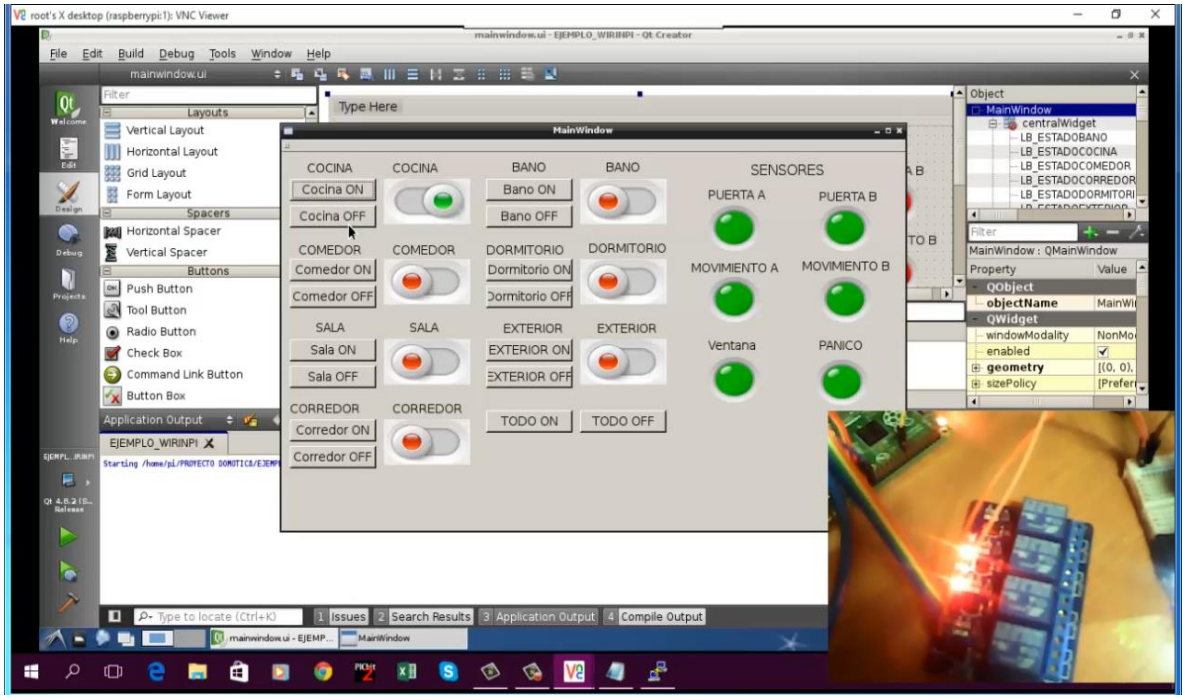
[19] A. C. Jose Luis, T. B. Erik Augusto y V. Carlos, «Sistema de Seguridad Domiciliaria,» Guayaquil, ESPOL, 2005, pp. 2-3.

[20] J. A. R. Pérez, «Diseño de sistema electronico de alarma antiintrusos para viviendas individuales,» Cartagena, UNIVERSIDAD POLITÉCNICA DE CARTAGENA, 2010, pp. 6-7.

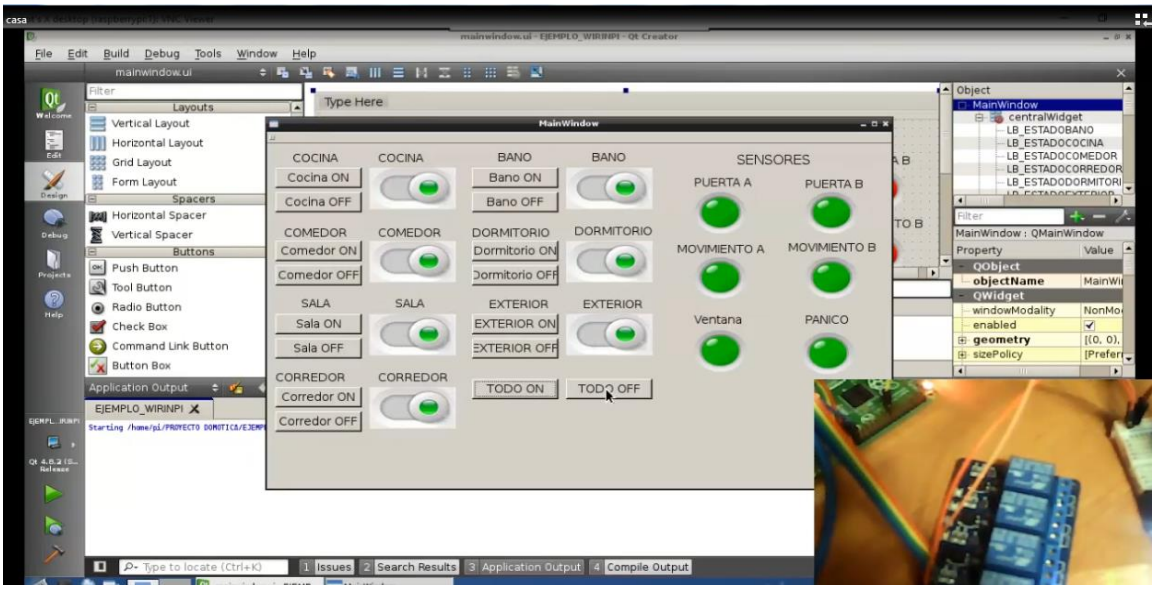
[21] E. P. Rocamora, «Diseño y Simulación de un Sistema Domótico para una vivienda,» Cartagena, Universidad de Cartagena, 2008 , pp. 8-9.

CAPÍTULO VII
ANEXOS

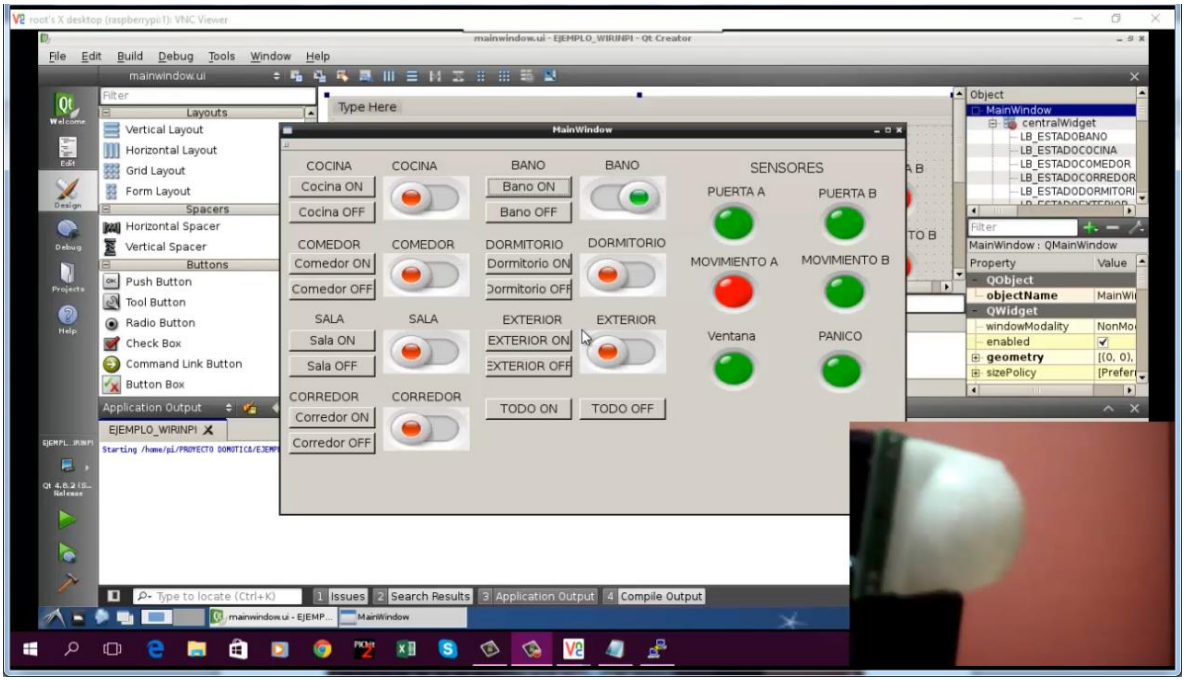
Sistema de las puertas funcionando



Alarma activada y desactivada



Sistema de los sensores de movimiento funcionando

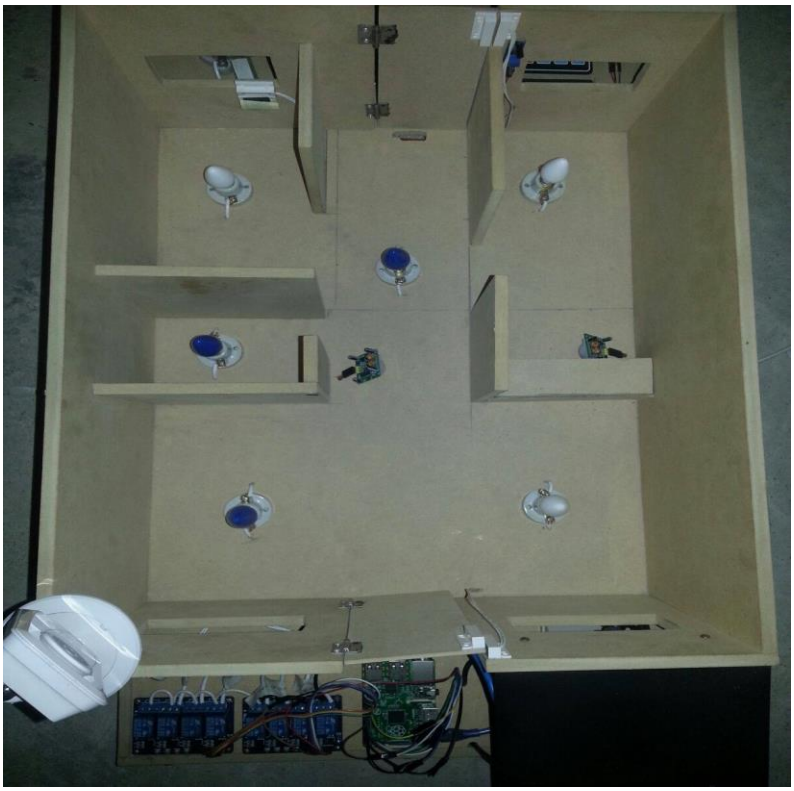


Vista superior de la maqueta

Vista delantera

Botón de pánico instalado

Maqueta terminada



SISTEMA INTEGRAL PARA LA SEGURIDAD DE UNA VIVIENDA
MANUAL DE USUARIO

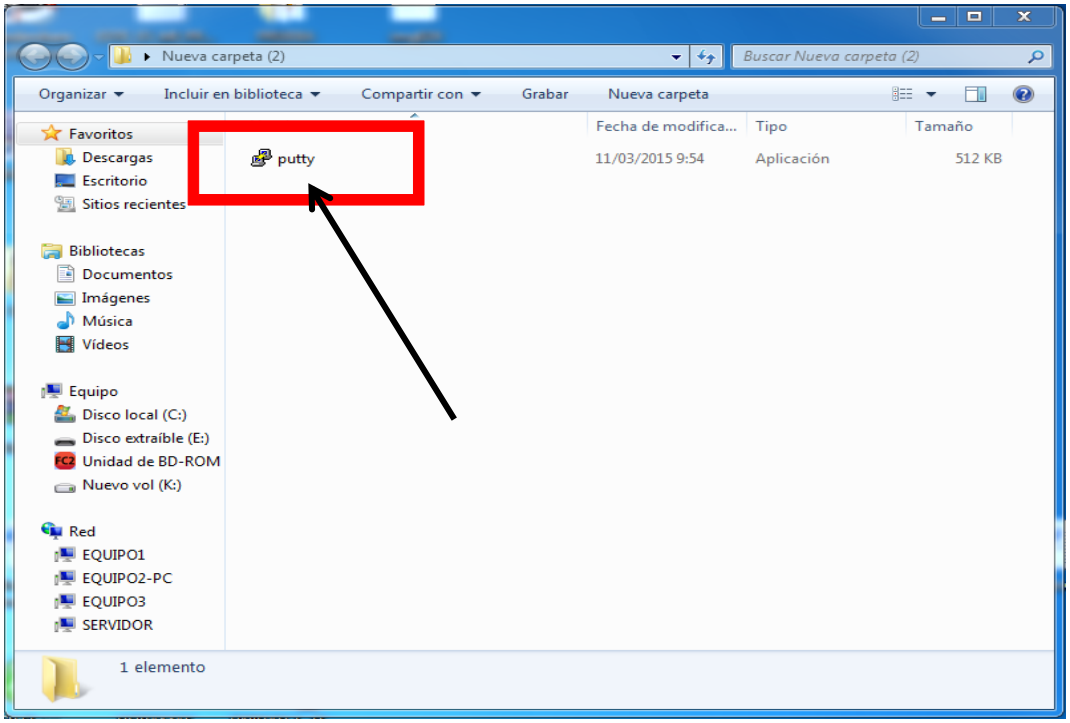
El sistema de seguridad puede controlar los siguientes dispositivos:

- Sensor de humo
- Sensor de vibración
- Sensores magnéticos en puertas y ventanas
- Sensores de movimientos
- Botón de pánico
- Control de acceso para la puerta principal
- Control de encendido y apagado de luces
- Cámara

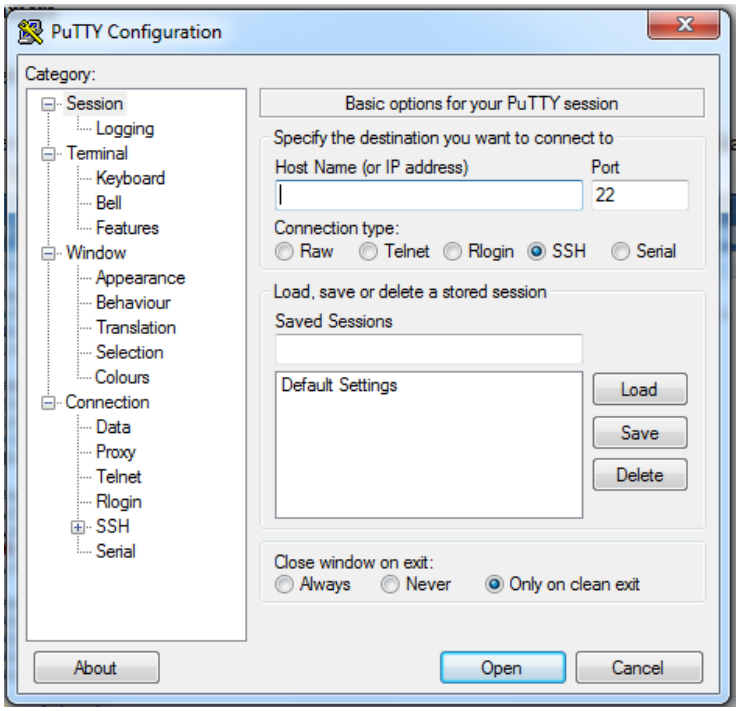
Para que el sistema este activado el usuario debe realizar los siguientes pasos:

INSTALACIÓN DE LA APLICACIÓN PUTTY (COMUNICACIÓN CON LA RASPBERRY)

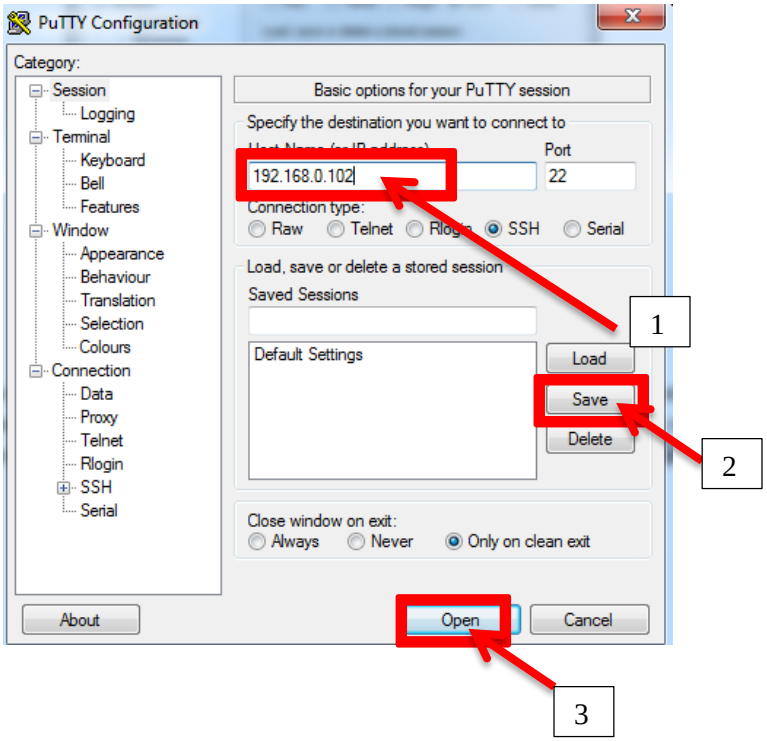
Luego se debe instalar el archivo “putty”, el cual permitirá acceder a la raspberry mediante una dirección IP asignada.



Se procede a dar doble clic y aparecerá la siguiente ventana en la que se configurará los parámetros de la dirección IP

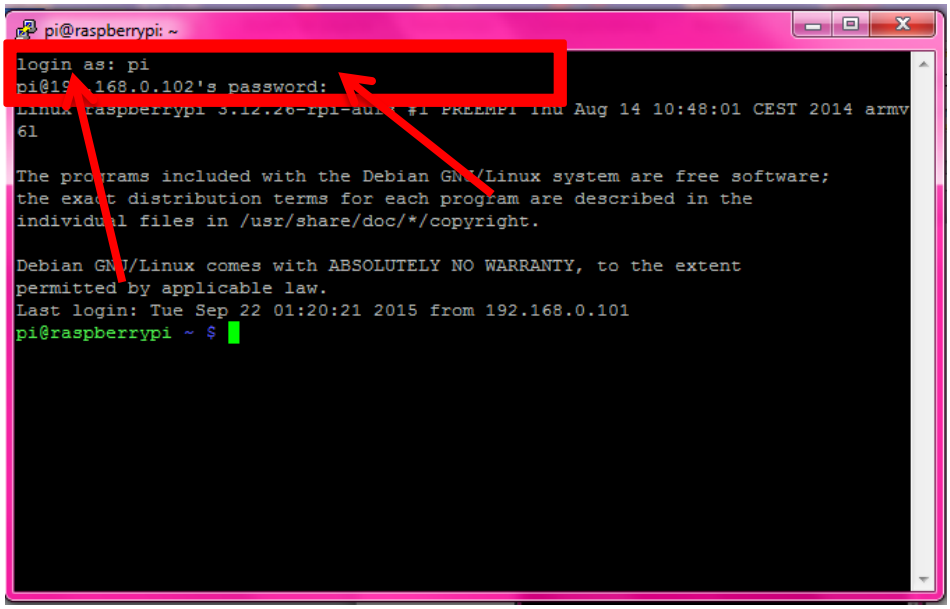


Luego se procede asignar la dirección IP por defecto que trae el módulo raspberry en el campo **Host Name (or IP address)**, en este caso es la **192.168.0.102** (nota: cada raspberry trae una dirección IP). Damos clic en **"Save"** y procedemos a dar clic en **"Open"**



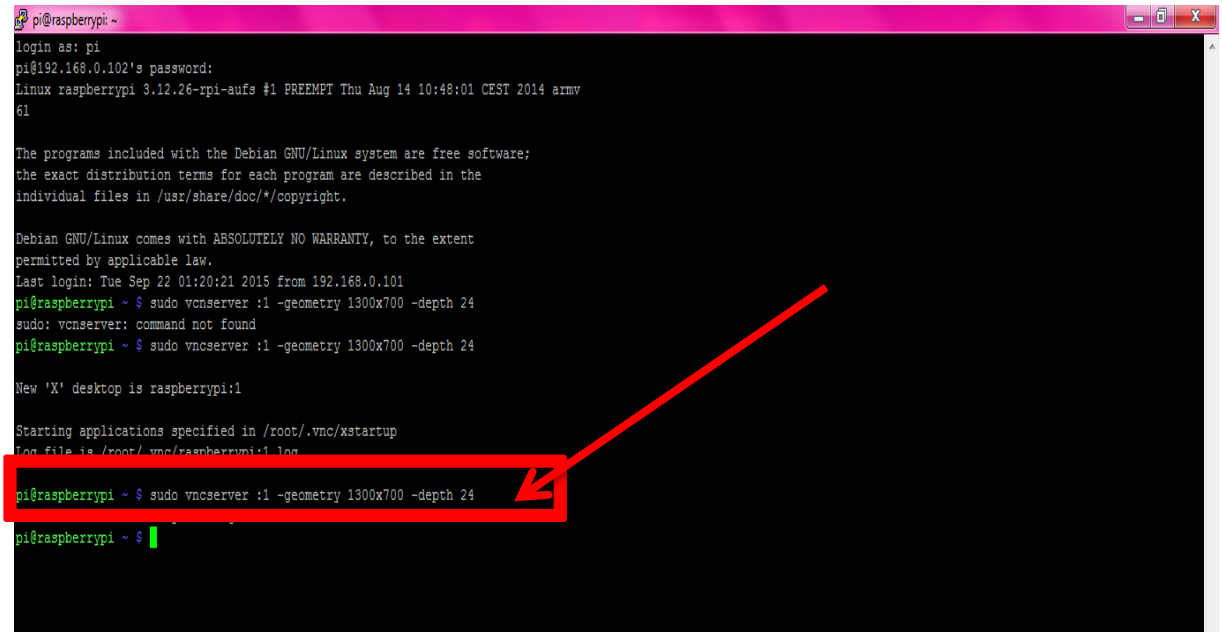
Luego de configurado se abrirá una pantalla que permitirá el acceso a la raspberry en la cual se deberá registrar el usuario y contraseña ya especificada en el sistema en este caso **"Login**

as: pi" "contraseña: raspberry", como se muestra a continuación, en la que el sistema carga.



Para poder ingresar y dimensionar el tamaño de la ventana del escritorio remoto VNC (su instalación será explicada más abajo), digitamos lo siguiente:

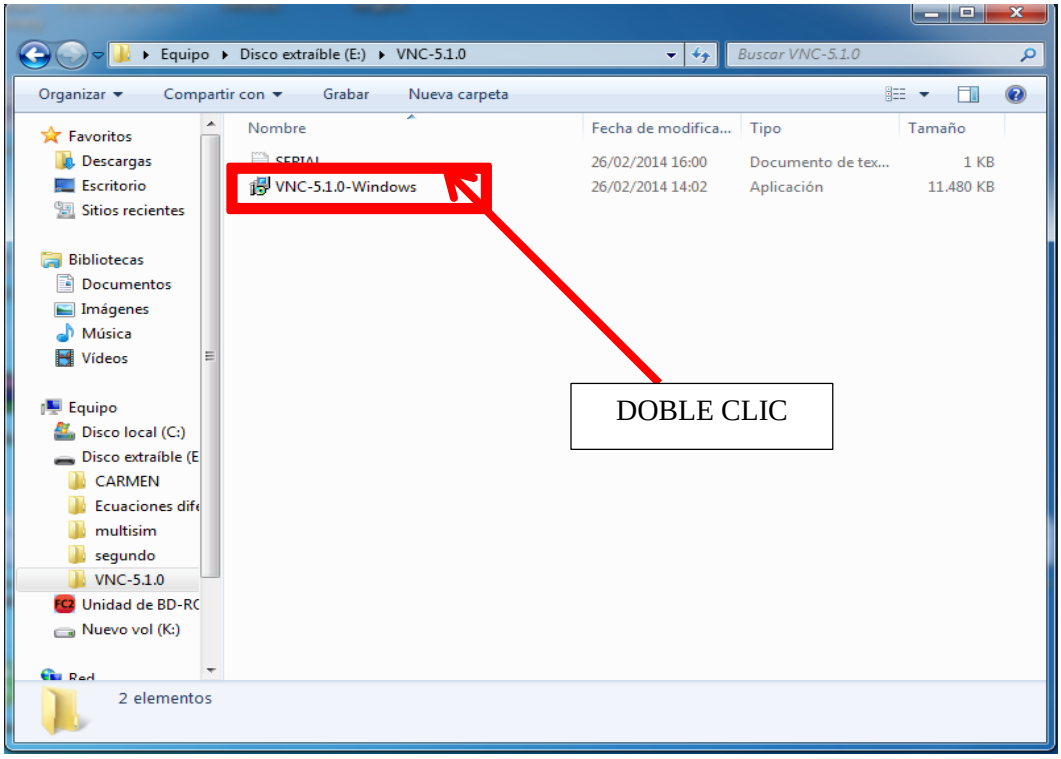
sudo vncserver :1 –geometry 1300*700 –depth 24



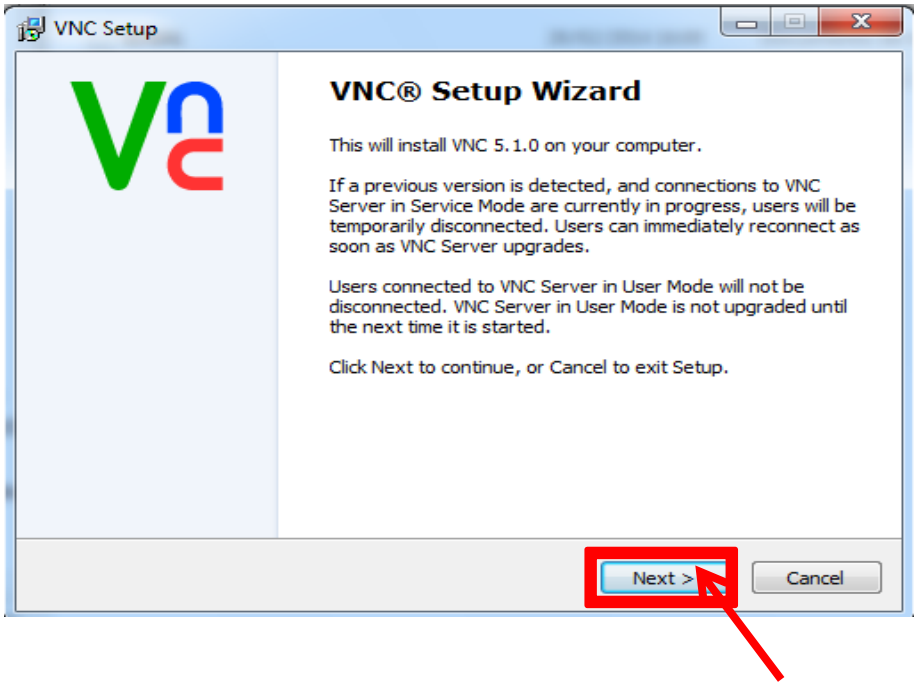
Y luego de esta configuración se podrá ingresar sin complicación a la aplicación de escritorio remoto

INSTALACIÓN DE VNC (ESCRITORIO REMOTO)

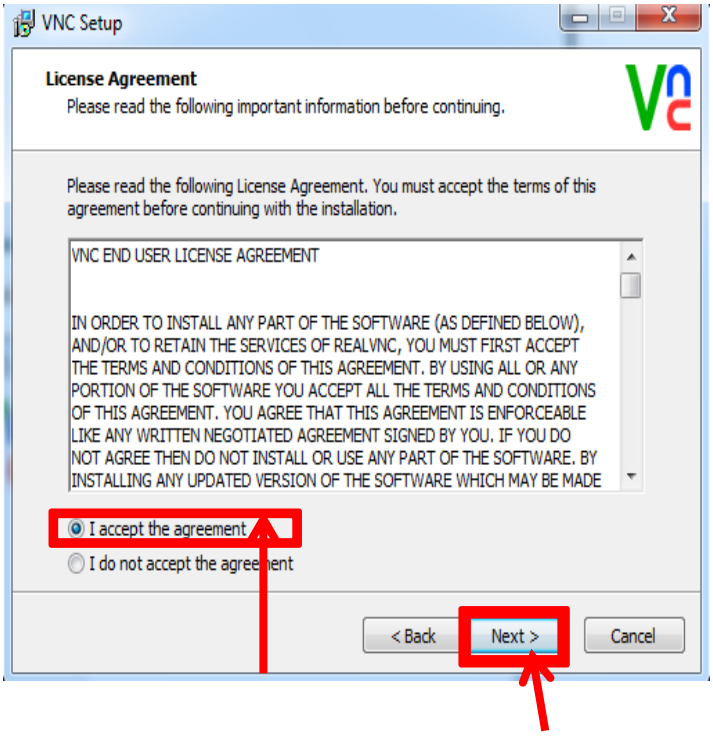
Se procede a instalar la aplicación para escritorio remoto, este puede ser instalado en el disco local C: o D:



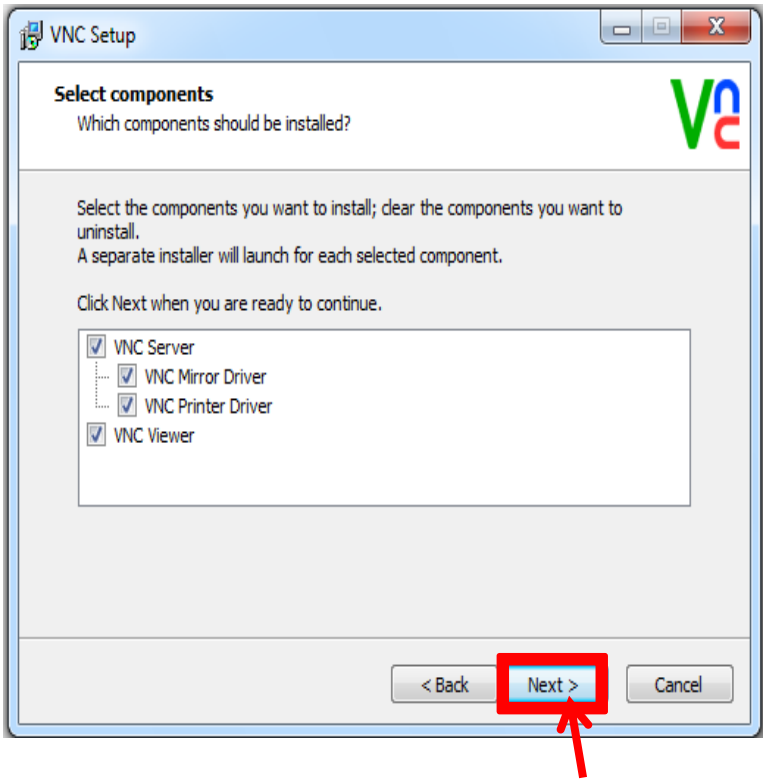
A continuación aparecerá la siguiente pantalla, damos clic en **"Next"**



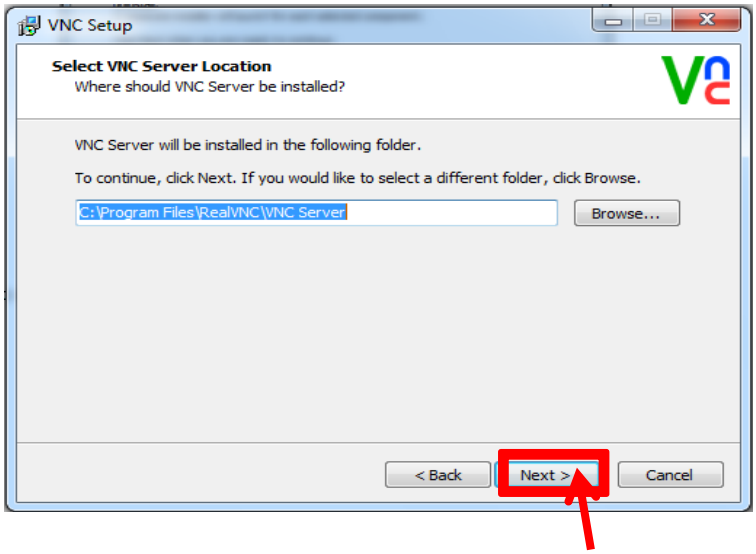
Luego aceptamos los términos y condiciones **“I accept the agreement”** y clic en **“Next”**



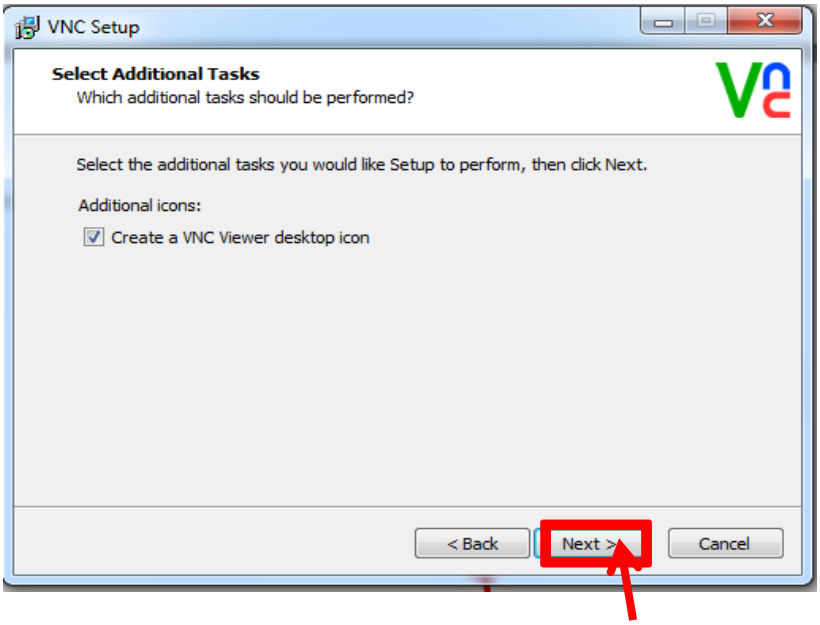
Damos clic en **“Next”**



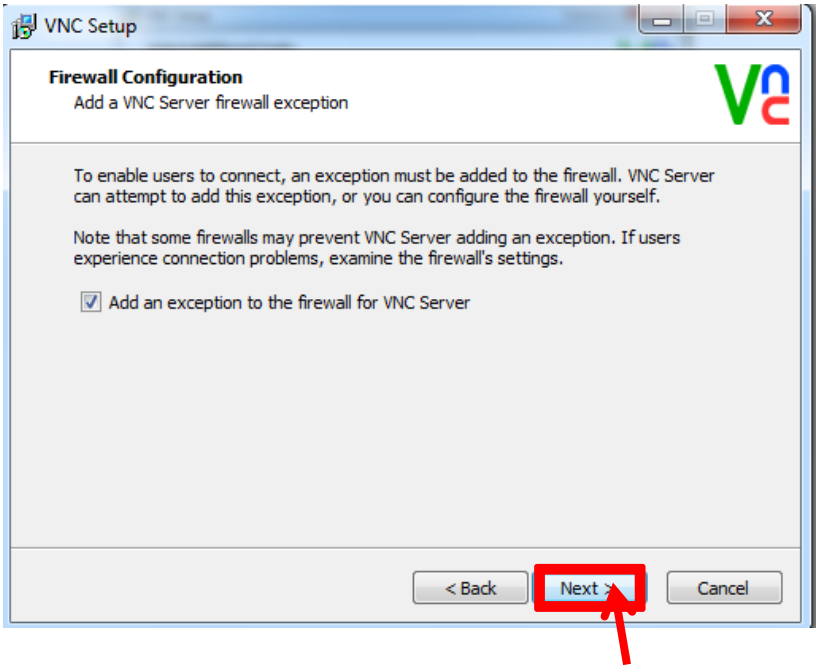
Damos clic en **“Next”**



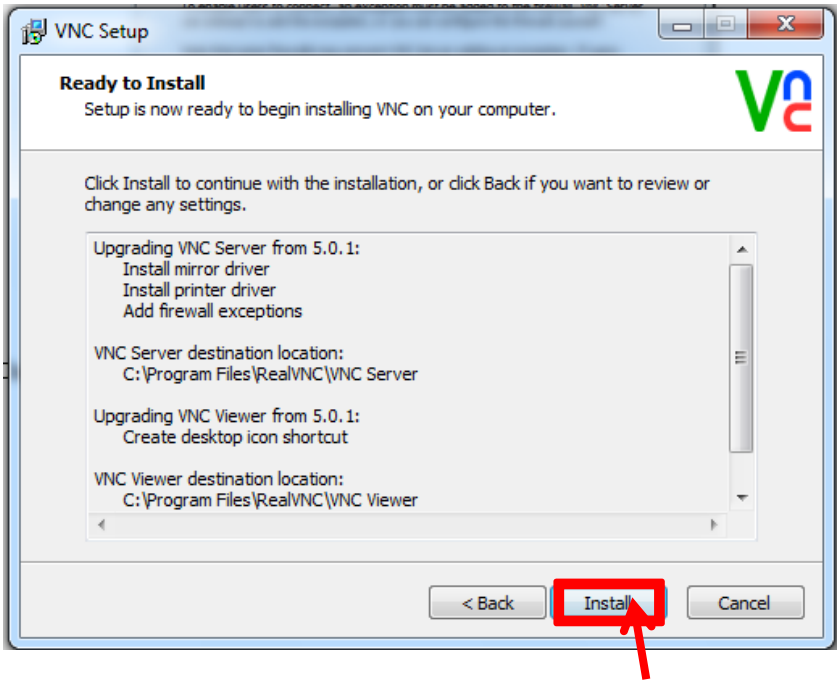
Damos clic en **“Next”**



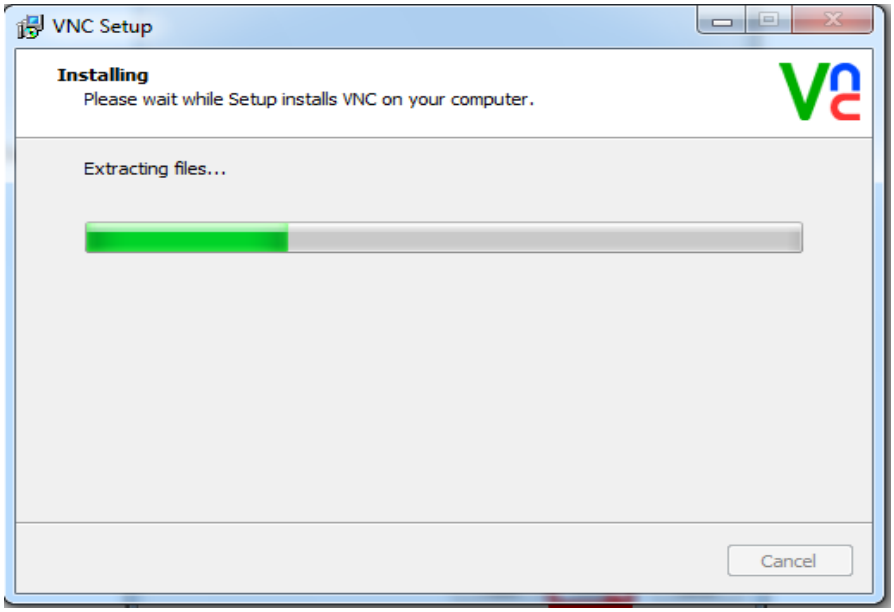
Damos clic en **“Next”**



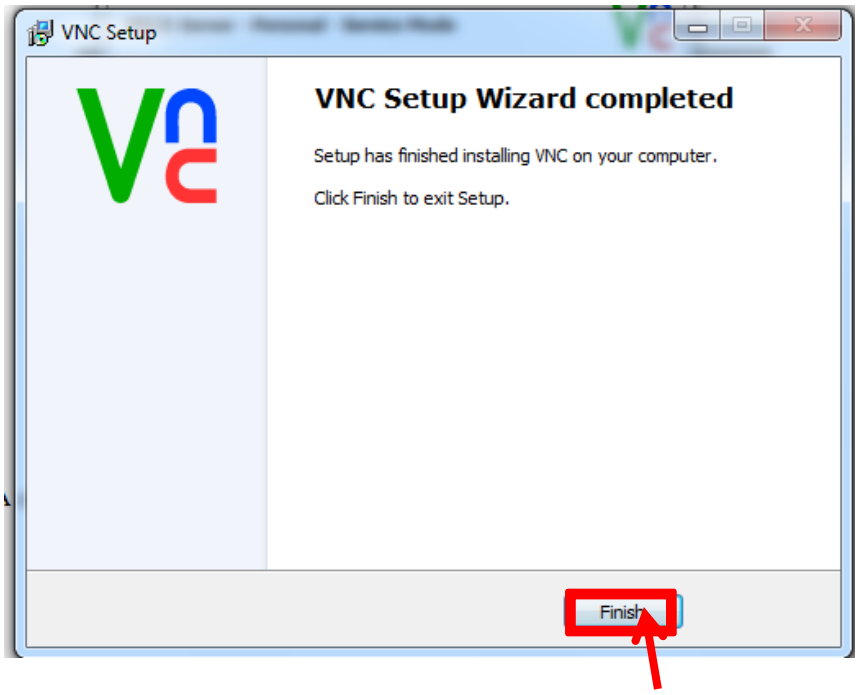
Damos clic en **“Install”**



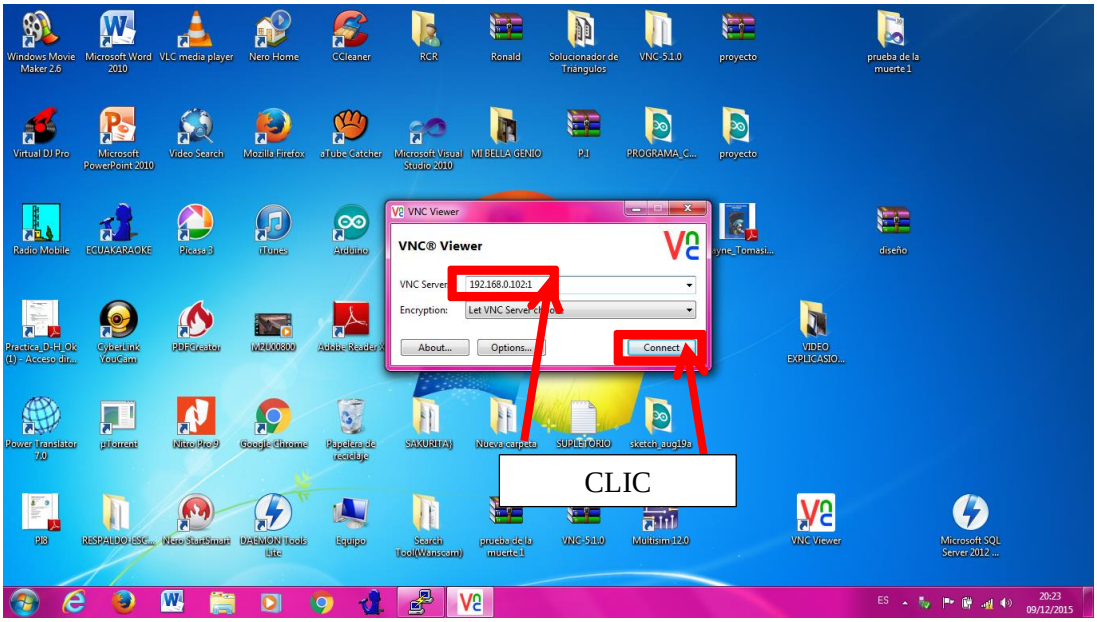
Y luego se espera hasta que cargue



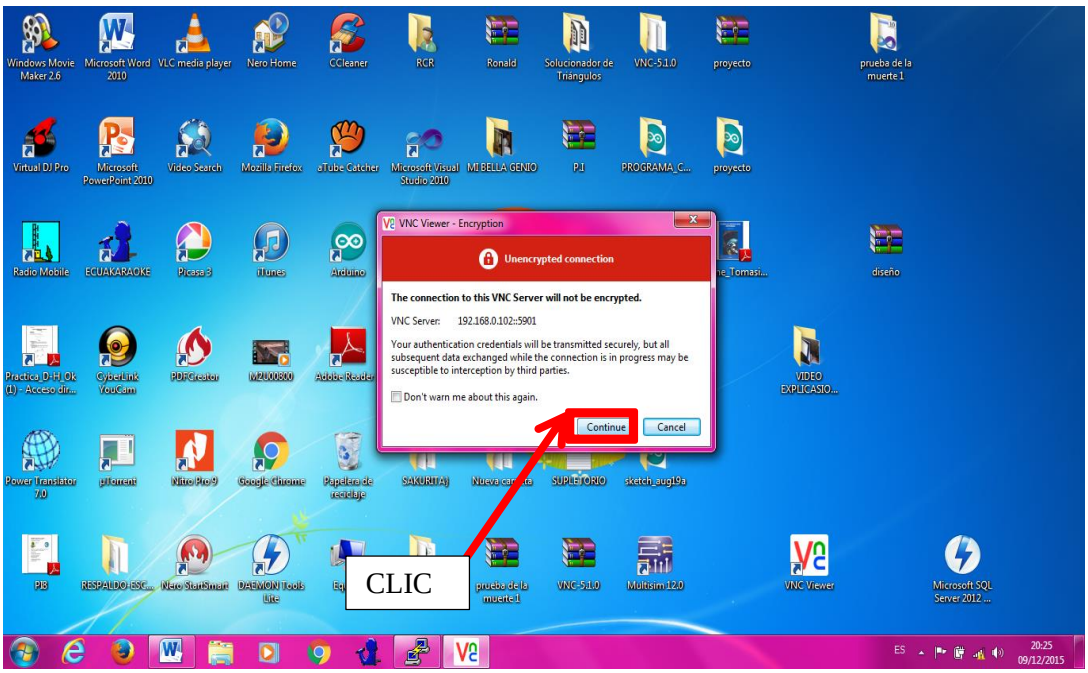
Luego aparecerá la pantalla en la que se dará clic en Finalizar “Finish”.



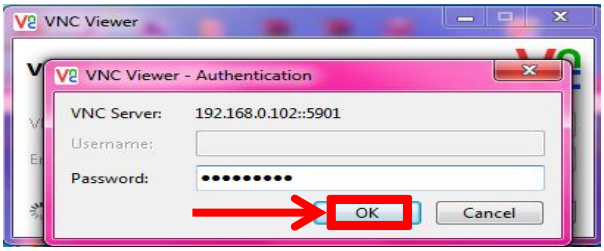
A continuación se procede a abrir la aplicación, en la cual debemos ingresar la dirección IP que asignamos en la aplicación PuTTY, luego damos clic en “Connect” para conectar:



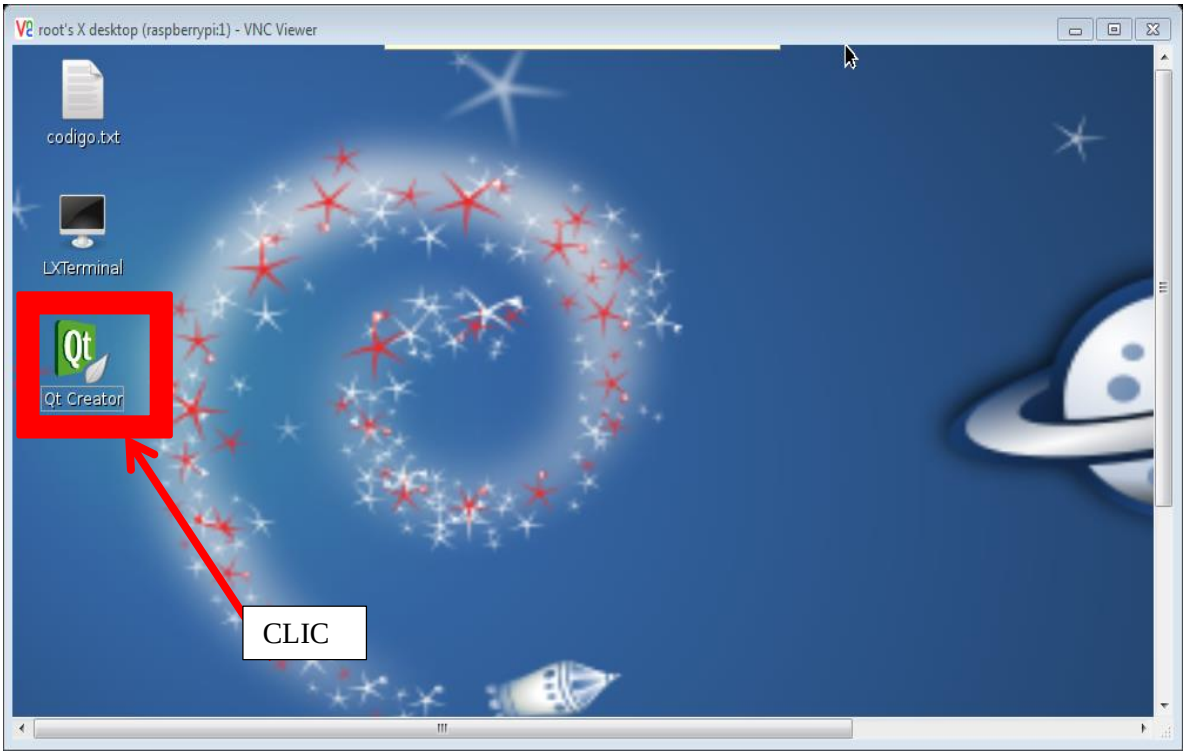
Luego aparecerá la siguiente pantalla y le damos clic en “Continue”



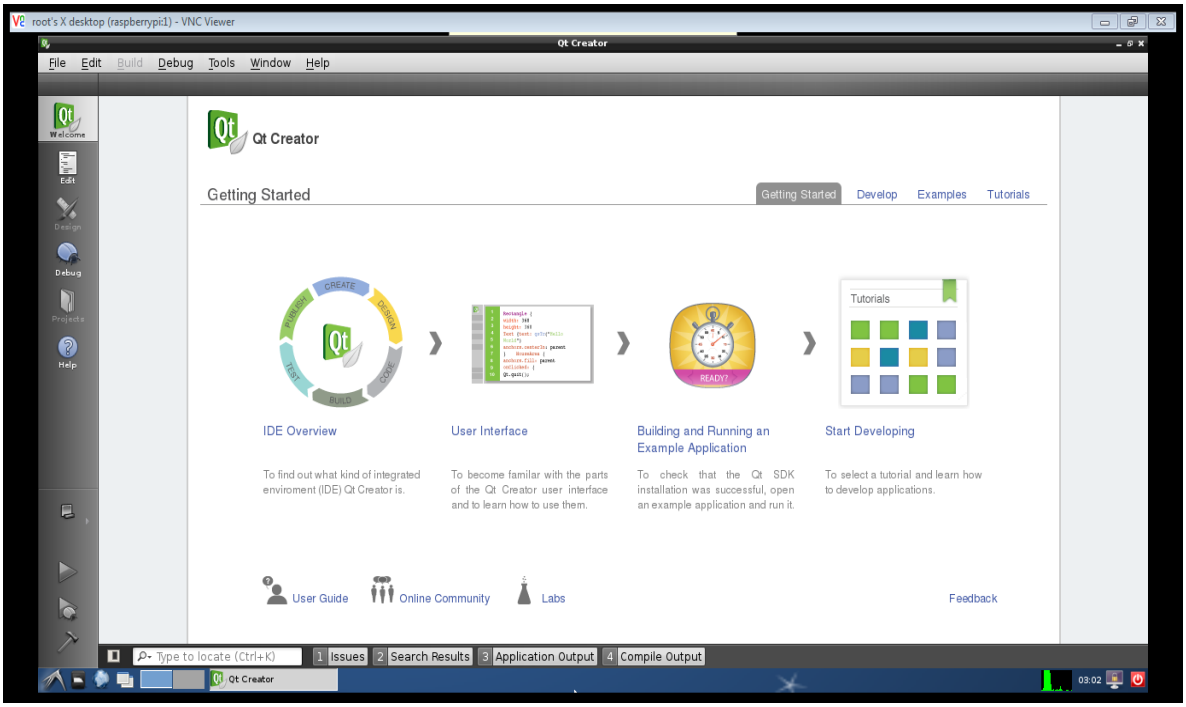
Luego volvemos a escribir el usuario y contraseña, a continuación damos clic en “Ok”



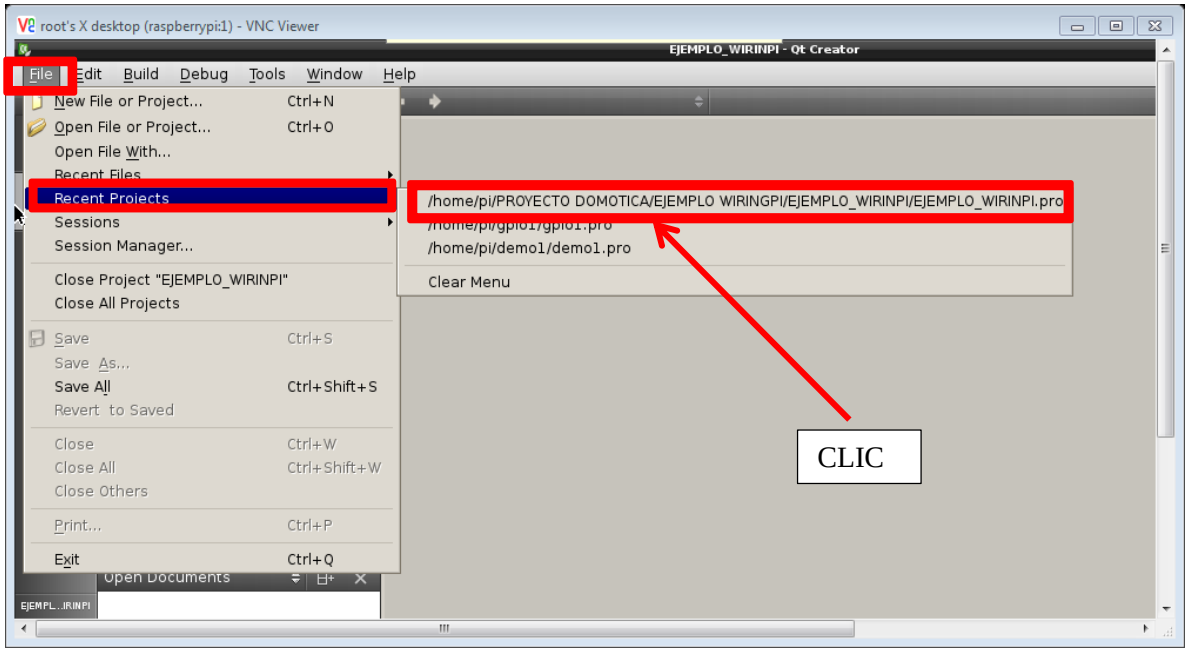
A continuación se abrirá el sistema operativo de la raspberry y damos clic en “Qt Creator”



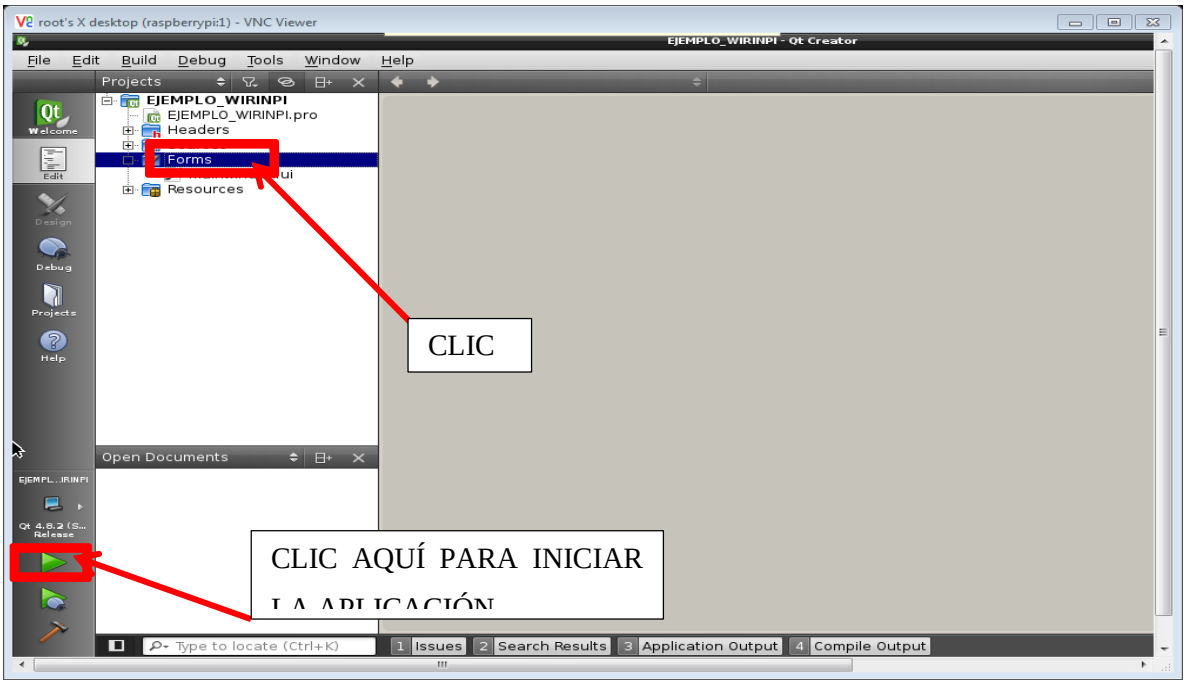
Se abrirá la siguiente ventana



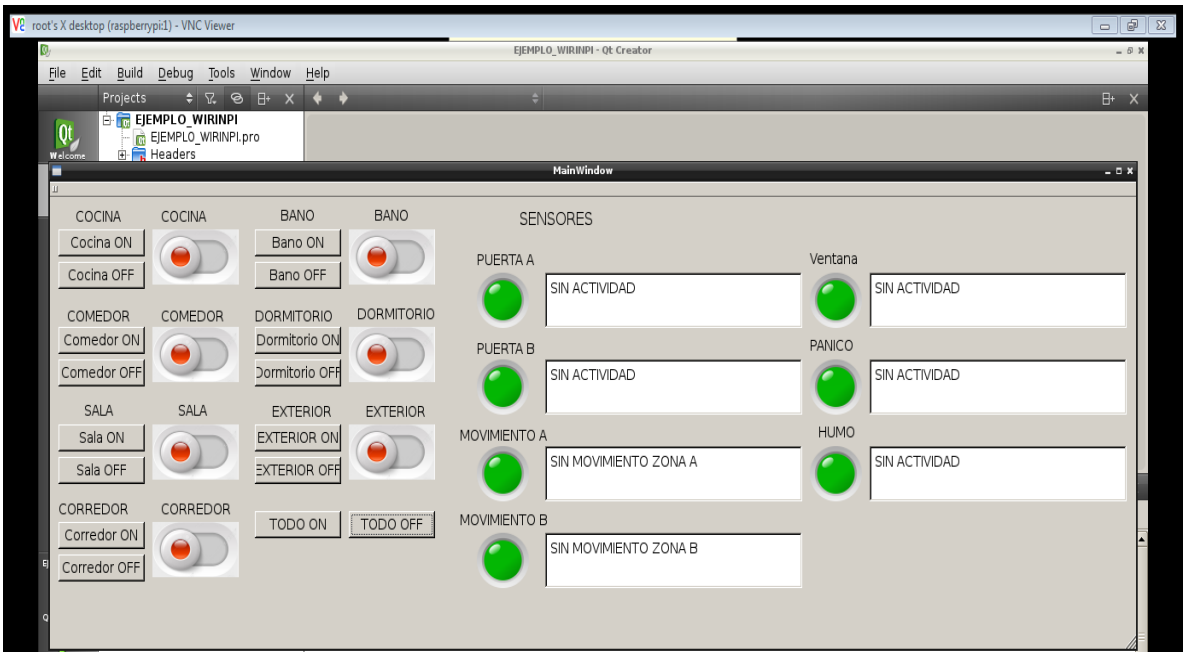
Luego ubicaremos la opción “File> Projects>Nombre de la aplicación”. En nuestro caso, como ya la hemos utilizado nos ubicamos en File>Recent Projects > /home/pi/PROYECTO DOMOTICA/EJEMPLO WIRINGPI/EJEMPLO_WIRINPI/EJEMPLO_WIRINPI.pro



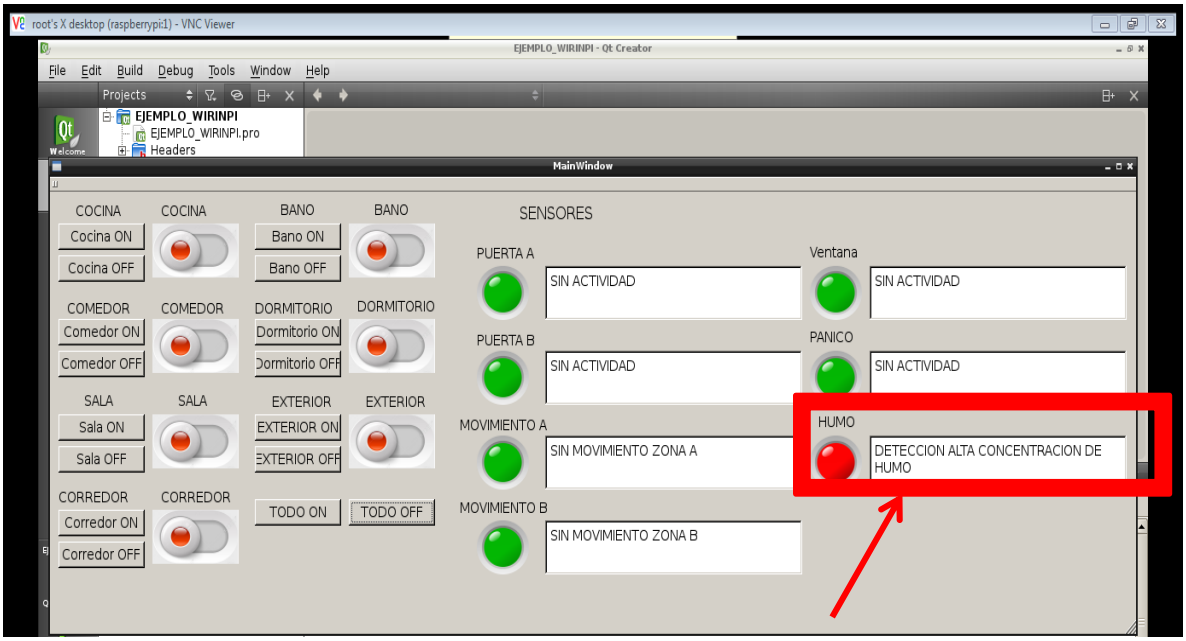
A continuación se abrirá el proyecto, en la cual daremos clic en “Forms” y luego damos clic en iniciar en el icono como se muestra en la siguiente figura.



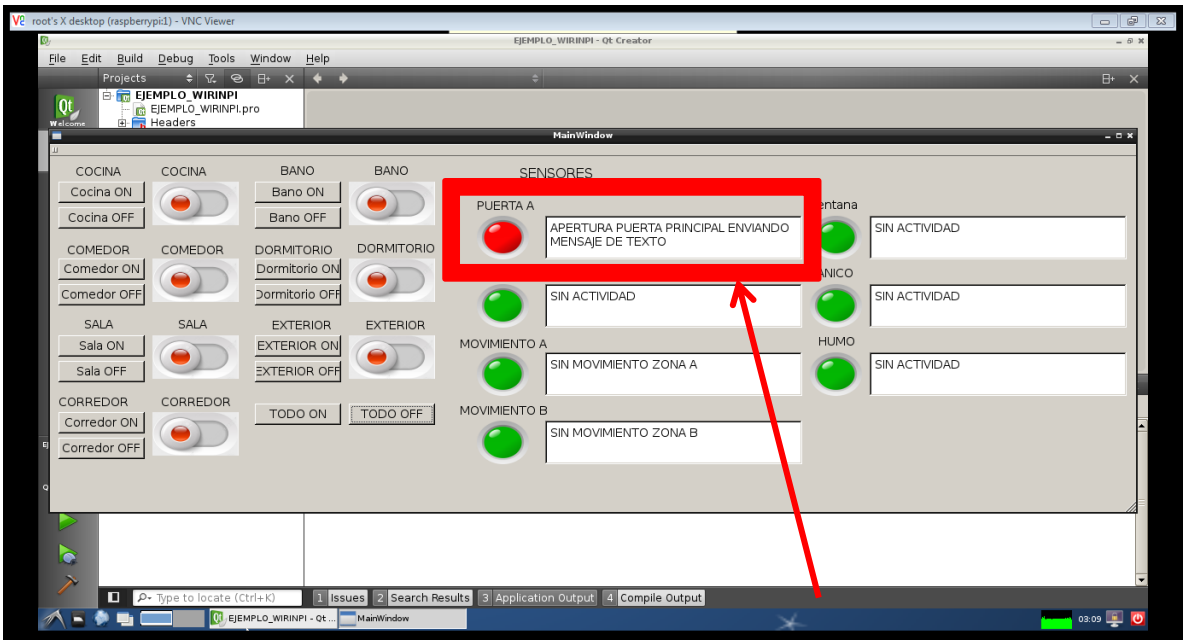
A continuación se abrirá la aplicación, en esta etapa el sistema está activado, es decir que todos los dispositivos están funcionando.



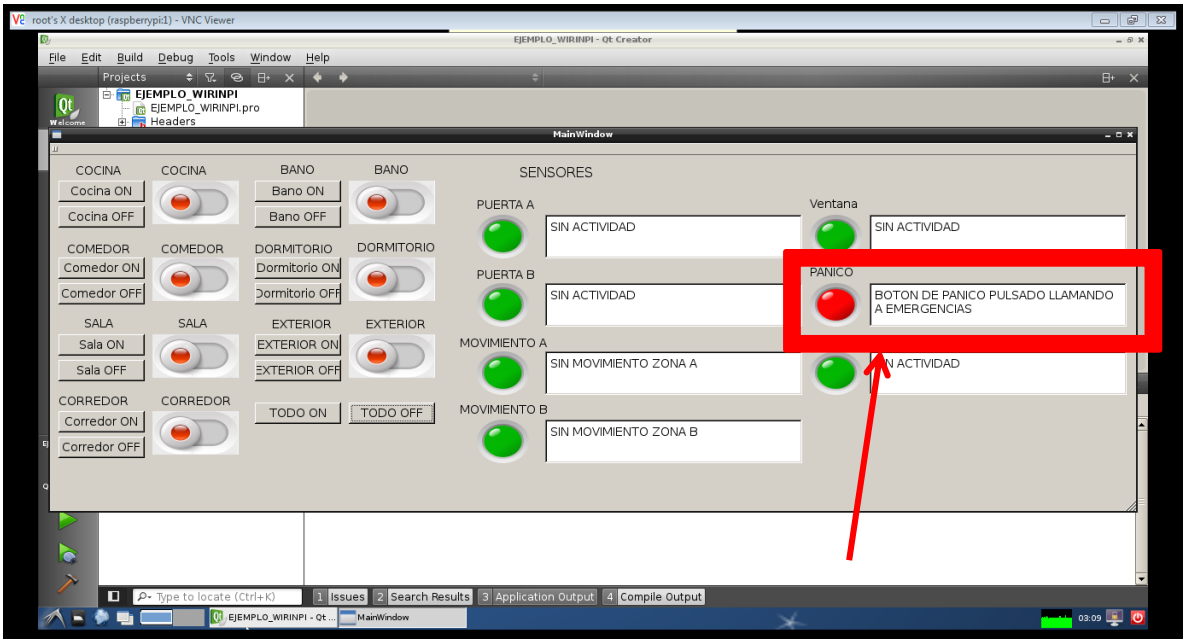
Se procede a realizar una prueba, en la que se demuestra una alerta cuando se detectan anomalías.



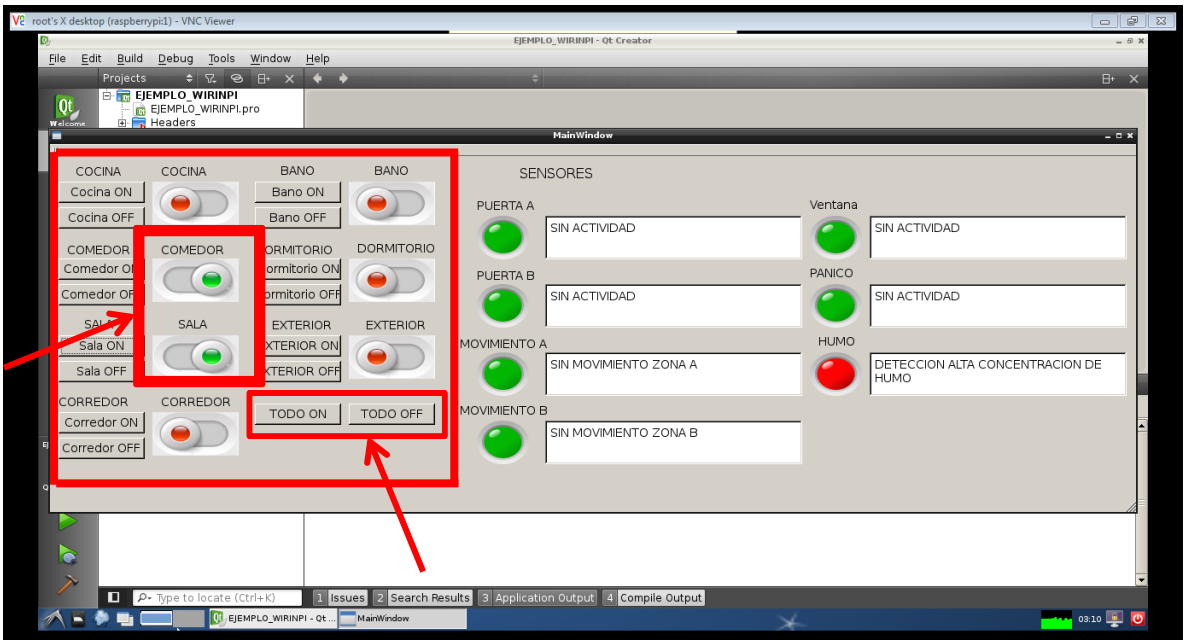
En la siguiente figura se procede a simular la apertura de la puerta, y en este caso el sistema enviará un mensaje de texto al propietario.



En el caso de esta imagen, al presionar el botón de pánico, este realizará una llamada al 911 desde el celular.



En la parte izquierda se encuentran los controles de las luces de la vivienda y como se demuestra en la siguiente imagen, las luces del comedor y la sala están encendidas.



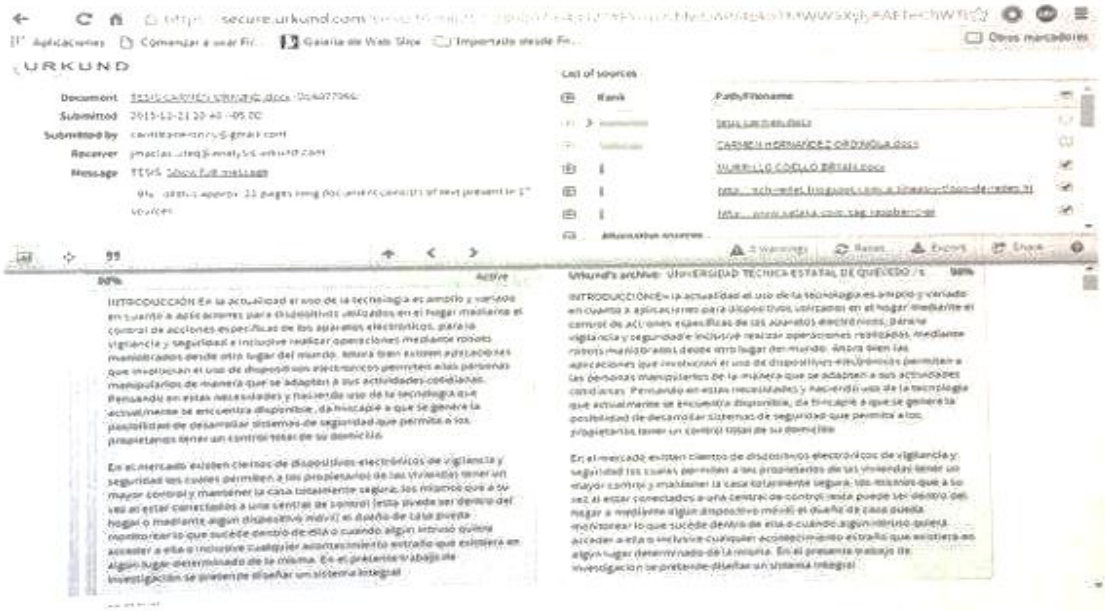
Finalmente dando clic en “Todo ON” o “Todo OFF” puede activar o desactivar el sistema.

Universidad Técnica Estatal de Quevedo
Facultad de Ciencias de la Ingeniería

Memorando 003-2015

Fecha: 22 de diciembre del 2015
De: Ing. Jaime Macías Romero.
Para: Ing. Jorge Murillo Oviedo, Decano FCI
Asunto: Informe del Urkund

Mediante la presente cumplo en presentar a usted el informe de tesis de la Srta. Carmen Amparo Hernández Ordinola cuyo tema: **'SISTEMA DE SEGURIDAD INTEGRAL DE UNA VIVIENDA CONTROLADA VÍA REMOTA"**, revisado bajo mi dirección, toda vez que se ha desarrollado de acuerdo al reglamento general de graduación de pregrado de la Universidad Técnica Estatal de Quevedo y cumple con el requerimiento de análisis de URKUND el cual avala los niveles de originalidad en un 91%, y de similitud 9%.



Particular que informo para trámites pertinentes, de acuerdo a lo que establece el reglamento de grados y títulos de la Universidad Técnica Estatal de Quevedo.

Por la atención a la presente reitero mis agradecimientos.

Atentamente,

Ing. Jaime Macías Romero, MSc.
TUTOR DE PROYECTO DE INVESTIGACIÓN