Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE ALTA CALIDAD A BAJO COSTO

Handy Estuardo Morales Fuentes
Asesorado por la Inga. Ingrid Salomé Rodríguez de Loukota

Guatemala, mayo de 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE ALTA CALIDAD A BAJO COSTO

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

HANDY ESTUARDO MORALES FUENTES
ASESORADO POR LA INGA. INGRID SALOMÉ RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, MAYO DE 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Luis Diego Aguilar Ralón
VOCAL V	Br. Christian Daniel Estrada Santízo
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

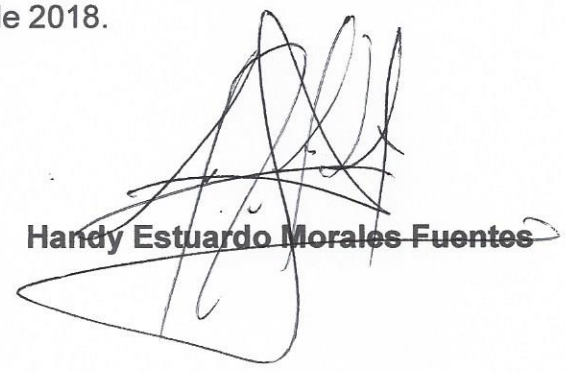
DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Byron Odilio Arrivillaga Méndez
EXAMINADOR	Ing. Helmunt Federico Chicol Cabrera
EXAMINADOR	Ing. Sergio Leonel Gómez Bravo
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE ALTA CALIDAD A BAJO COSTO

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica con fecha 4 de mayo de 2018.



Handy Estuardo Morales Fuentes

Guatemala 7 de febrero de 2019

Ingeniero
Julio Cesar Solares Peñate
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Apreciable Ingeniero Solares.

Me permito dar aprobación al trabajo de graduación titulado "**Diseño e implementación de un sistema de seguridad de alta calidad a bajo costo**", del señor **Handy Estuardo Morales Fuentes**, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesora, nos hacemos responsables por el contenido y conclusiones del mismo.

Sin otro particular, me es grato saludarle.

Atentamente,

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Inga. Ingrid Rodríguez de Loukota
Colegiada 5,356
Asesora

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 21 de febrero de 2019

Señor Director
Ing. Otto Fernando Andrino González
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado **DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE ALTA CALIDAD A BAJO COSTO,** desarrollado por el estudiante **Handy Estuardo Morales Fuentes,** ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Julio César Solares Peñate
Coordinador de Electrónica

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 21. 2019.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto bueno del Coordinador de Área, al trabajo de Graduación de la estudiante: HANDY ESTUARDO MORALES FUENTES titulado: DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE ALTA CALIDAD A BAJO COSTO, procede a la autorización del mismo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Otto Fernando Andrino González

GUATEMALA, 2 DE ABRIL 2019.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.45-2019

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica del trabajo de graduación titulado: **"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE ALTA CALIDAD A BAJO COSTO", p**resentado por el estudiante: **Handy Estuardo Morales Fuentes** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, mayo de 2019

/echm

ACTO QUE DEDICO A:

Dios	Por la oportunidad de cumplir esta meta y ser bueno con todos nosotros.
Mis padres	Aracely Fuentes y Gustavo Morales, por su apoyo y amor invariable.
Mi abuela	Dorothy Morales, por ser la fuente de esperanza de nuestra familia.
Mi hermano	Brian Morales, por sus consejos y ser un ejemplo a seguir profesionalmente.
Mis amigos	Chantelle y Luis Cruz, por compartir tantos momentos inolvidables.
Mi novia	María José Juárez, por ser una persona incondicional en mi vida.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la casa de estudios que me brindó los valores profesionales para afrontar la vida.
Ingeniera Ingrid de Loukota	Por el tiempo y dedicación brindados a mi trabajo de graduación.
Ingeniero David Barrientos	Por compartir sus conocimientos profesionales sin egoísmo y ayudarme con la culminación de mi carrera.
IEEE	Por darme la oportunidad de conocer a personas increíbles y a profesionales interesados en el desarrollo tecnológico de nuestro país.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
A	Amperios
GB	GigaBytes
°c	Grados Celsius
Hz	Hertz
Kbps	Kilobit por segundo
Kb	KiloByte
MB	Megabytes
mA	Miliamperio
%	Porcentaje
Q	Quetzales (moneda guatemalteca)
Rx	Receptor
R	Resistencia
S	Segundos
Tx	Transmisor
VDC	Voltios en corriente directa
V	Voltios nominales

GLOSARIO

3G Abreviación de Tercera Generación de transmitir datos y voz a través de telefonía móvil.

Alarma Señal sonora o visual que notifica de un peligro.

Android Sistema operativo diseñado principalmente para telefonía móvil.

ARM Tecnología de construcción de microprocesadores, la cual utiliza un conjunto de instrucciones de 32 y 64 bits (Advance RISC Machine, en inglés).

Asalto Ataque contra una persona o entrada en una propiedad con intención de robar.

AT Comandos utilizados para configurar y parametrizar dispositivos convertidores de señales digitales en señales analógicas.

Automatización Aplicación de máquinas en la realización de un proceso.

Bit Unidad mínima de información que se puede almacenar en memoria y ser transmitida únicamente en dos estados lógicos, cero o uno.

Byte	Unidad de medida de 8 bits.
CBA	Canasta Básica Alimentaria.
CCTV	Circuito Cerrado de televisión (Closed Circuit Television, en inglés).
CD	Cambio de directorios en consola Linux.
CIEN	Centro de Investigaciones Económicas Nacionales de Guatemala.
CP2012	Adaptador entre comunicación UART.
Dispositivo	Conjunto de piezas para realizar una función determinada.
Domótica	Conjunto de herramientas utilizadas para automatizar una vivienda.
Electrónica	Ciencia derivada de la física que estudia los cambios y movimiento de los electrones libres.
ENCOVI	Encuesta Nacional de Condiciones de Vida.
ENEI	Encuesta Nacional de Empleo e Ingresos.
ETHERNET	Estándar de redes de área local para computadoras. Se utiliza para crear una conexión entre varios

	equipos.
Extorción	Delito que consiste en obligar a una persona a través de intimidación a realizar un acto con ánimo de lucro.
GB	Unidad de almacenamiento de información con capacidad de mil millones de bytes.
Gestión	Llevar a cabo responsabilidades sobre cierto proceso.
GND	Siglas en inglés de Ground, punto cero de todas las tensiones eléctricas presentes en un aparato eléctrico.
GPIO	Pines de entrada/salida de propósito general (General Purpose Input/Output, en inglés).
GPRS	Siglas en inglés de General Packet Radio Service, el servicio general de paquetes vía radio es un servicio de comunicación inalámbrica basado en el uso de paquetes de información.
GPS	Siglas en inglés de Global Positioning System, el sistema de posicionamiento global permite tener la ubicación en todo el mundo de un objeto, persona o vehículo mediante satélites que orbitan alrededor de la tierra

GPU	Siglas en inglés de Graphics Processing Unit (Unidad de Procesamiento Gráfico). Es un coprocesador dedicado únicamente al procesamiento de gráficos u operaciones de punto flotante, permitiendo así el máximo desempeño en otras funciones al procesador central.
GSM	Siglas en inglés de Global System for Mobile Communication. El sistema global para comunicaciones móviles es un protocolo que permite enviar y recibir mensajes por medio de correo electrónico, faxes, navegación a Internet y servicio de mensajes cortos.
Hardware	Componentes eléctricos, electrónicos, electromecánicos y mecánicos de un sistema informático.
HDMI	Siglas en inglés de High-Definition Multimedia Interface. Es la interfaz multimedia de alta definición que permite una mejora de video y audio a cualquier dispositivo que posea esta ranura en su placa madre.
Implementación	Ejecución de una idea programada.
INE	Instituto Nacional de Estadística en Guatemala.
Internet	Red de comunicación que interconecta a millones

	de computadoras.
IOT	El Internet de las Cosas (Internet of Things en inglés) es la acción de interconectar a Internet los objetos cotidianos que rodean a una persona.
IP	Siglas en inglés de Internet Protocol, es una numeración que identifica a una interfaz en red.
Instalación	Establecer o situar algo en algún sitio debido.
LAN	Siglas en inglés de Local Area Network, es una red de área local.
LED	Siglas en inglés de Light Emitting Diode (Diodo Emisor de Luz). Es un dispositivo semiconductor capaz de emitir una longitud de onda visible, dependiendo del dopado del mismo al ser polarizado directamente.
LINUX	Sistema operativo potente y amigable al usuario que permite utilizar programas como editores de texto, navegadores de Internet, etc. Puede utilizarse mediante un interfaz gráfico y mediante líneas de comando por consola.
LS	Comando para mostrar una lista de archivos de un determinado directorio.

Mantenimiento	Conservación de una cosa u objeto en buen estado.
Monitoreo	Proceso en el cual se reúne, observa y estudia información para realizar alguna acción.
NANO	Editor de texto para la terminal de Linux que, generalmente, viene instalado por defecto.
Network	Red física y lógica que contribuye a lograr interconexiones.
Open Source	Término utilizado para denominar cierto software que se distribuye mediante una licencia libre, el cual pueden ser modificado para realizarle mejoras sin tener la aprobación de una institución pública o privada.
Optimizar	Conseguir que algo llegue a los mejores resultados posibles.
OSH	Siglas en inglés de Open Source Hardware, término utilizado para todos aquellos dispositivos cuyas especificaciones, modelos esquemáticos y construcción lógica son puestos en dominio público.
Parámetro	Dato importante desde el que se examina un tema o asunto.
Plataforma	Sistema que sirve como base para hacer funcionar

	determinados módulos de hardware o software.
Protocolo	Conjunto de reglas a seguir para una acción adecuada.
PWM	Modulación por ancho de pulso (Pulse-Width Modulation en inglés).
Python	Puede referirse al lenguaje de programación Python y también a un comando utilizado para compilar un programa.
RAM	Siglas en inglés de Random Access Memory (Memoria de Acceso Aleatorio). Es la memoria donde se cargan las instrucciones que ejecuta el procesador o cualquier unidad de cómputo en el tiempo real.
Raspberry	Dispositivo electrónico u ordenador en placa reducida de bajo costo, desarrollado específicamente para el avance en el estudio tecnológico.
Remoto	Término utilizado para referirse a todo aquello que se encuentra a cierta distancia, retirado o alejado.
RJ45	Interfaz física para conectar redes de computadoras con cableado estructurado.

Roaming	Opción que ofrece un operador de telefonía de utilizar sus servicios en una red móvil distinta de la suya, normalmente fuera del país, que permite conectar al cliente con su red mediante acuerdos entre operadores.
Router	Dispositivo que proporciona conectividad a nivel de red.
Rubro	Cantidad de algo a gastar.
SD	Siglas en inglés de *Secure Digital*, es un dispositivo en formato de tarjeta para almacenar información.
Sensor	Dispositivo capaz de transformar un determinado tipo de energía de entrada a una señal eléctrica de salida.
Servicio web	Tecnología o sistema de software desarrollado para permitir la interacción entre máquinas o aplicaciones a través de una red de Internet, utilizando protocolos y estándares de comunicación.
Sistema	Conjunto ordenado de normas que regulan el funcionamiento de un grupo o dispositivo.
SMS	Siglas en inglés de Short Message Service, el servicio de mensajería corta utilizado para envío y recepción de mensajes cortos en telefonía móvil.

SMTP	El protocolo simple de transferencia de correo (siglas en inglés de Simple Mail Transfer Protocol). Es un protocolo básico que permite el envío de correos electrónicos a través de Internet, es decir, permite enviar *email* de un servidor de origen a un servidor de destino.
Software	Soporte lógico de un sistema informático.
SSH	Protocolo que permite conectar y controlar un equipo de forma remota.
SUDO	Comando que otorga privilegios y permisos a un usuario que tiene restricciones.
Tecnología	Ciencia aplicada a la resolución de problemas concretos.
Thinker A7	Módulo electrónico que integra GSM/GPRS y GPS en un solo dispositivo.
UART	Protocolo de comunicación serial (Universal Asynchronous Reciever-Transmitter por sus siglas en inglés).
USB	Siglas en inglés de Universal Serial Bus (Bus Universal Serial). Está definido como un estándar industrial para especificar los cables, conectores y

	protocolos utilizados en un bus para comunicar y proveer alimentación a otros dispositivos electrónicos.
Variables	Concepto que determina una cualidad de un objeto y atributo que pueda variar en función del tiempo.
WAN	Siglas en inglés de Wide Area Network. Es una red de telecomunicaciones que une equipos de computación a varios kilómetros de distancia y permite brindar conectividad a varias ciudades o a un país entero.
Web	Concepto utilizado en el ámbito tecnológico para nombrar a una red informática.

RESUMEN

Este trabajo de graduación presenta el diseño e implementación de un sistema de seguridad de alta calidad a bajo costo, utilizando componentes electrónicos de bajo consumo de energía eléctrica y de bajo presupuesto.

En el primer capítulo se describe un estudio socioeconómico tomado de estadísticas de plataformas gubernamentales del país, las cuales exponen los índices de pobreza y la inseguridad personal-residencial que padecen las personas de recursos limitados de la población guatemalteca.

En el segundo capítulo se realiza una inducción al tema de sistemas controlados remotamente. Se describe la importancia de los sistemas controlados a distancia, las aplicaciones y ventajas que tienen en la vida cotidiana y las herramientas necesarias para lograr un control óptimo de los mismos.

En el tercer capítulo se describe las bases teóricas para el diseño y gestión de un sistema de seguridad. Contiene las tecnologías utilizadas en dichos servicios, los materiales utilizados para realizar el proyecto y los parámetros básicos de cada uno de ellos.

En el cuarto capítulo se desarrollan las ventajas de un sistema de seguridad de bajo costo, se describen los distintos tipos de sistemas de seguridad actualmente en el mercado, su funcionamiento interno y partes importantes. De igual manera, se incluye un presupuesto de la realización del proyecto y una comparación con los sistemas de seguridad privados en el país.

Por último, se detallan los pasos a seguir para la implementación del sistema de seguridad. Contiene las interconexiones de los dispositivos electrónicos utilizados en la instalación, explicación y manipulación óptima de los comandos utilizados y el material audiovisual para la fácil comprensión e implementación del mismo.

OBJETIVOS

General

Diseñar e implementar un sistema de seguridad de alto nivel y bajo costo controlado remotamente para casa residencial utilizando un procesador ARM Cortex-A53.

Específicos

1. Diseñar un sistema que permita el control a distancia de un sistema de seguridad.

2. Establecer parámetros de hardware y software para la implementación de un sistema de seguridad de bajo costo.

3. Proveer guías de usuario y material didáctico en español, necesarios para la implementación del sistema de seguridad, tanto software como hardware.

4. Realizar un estudio comparativo de costos del sistema de seguridad creado versus las distribuidoras de servicios de seguridad privadas.

INTRODUCCIÓN

Debido al alza de la delincuencia en el país y el incremento de robos especialmente en zonas rojas del mismo, los ciudadanos se ven en la necesidad de tener un sistema de seguridad dentro de su casa que, al mismo tiempo de ejercer su tarea de vigilancia, permita al usuario tener la posibilidad de ser alertado en tiempo real y hacer la toma de decisiones adecuada a la situación.

Dichos sistemas de seguridad están fuera del alcance monetario para muchas familias guatemaltecas, dado que su implementación requiere de costosos sistemas electrónicos y, en muchos casos, las identidades facilitadoras del mantenimiento y servicios requieren de un pago mensual elevado comparado con el ingreso mensual de esa casa.

Es importante considerar que, para aquellas personas que están al tanto de todas las capacidades y beneficios de un sistema de seguridad, el costo de implementación es una preocupación válida. Sin embargo, existen tecnologías que por ser de bajo costo y bajo consumo de potencia, permiten el uso y adecuación de un sistema de seguridad de alto nivel con ciertos dispositivos electrónicos que sí están al alcance de las familias que poseen un presupuesto limitado.

Por lo anterior, este trabajo permitirá a esas personas con limitaciones económicas implementar un sistema de seguridad de alto nivel a bajo costo, con un monto único que cubrirá el pago de los dispositivos a utilizar en el proyecto, sin necesidad de recurrir a una empresa externa o a un pago mensual

por ese servicio, dado que el sistema es OSH (Open Source Hardware) y puede ser modificado con un software de licencia libre.

1. IMPORTANCIA DE UN SISTEMA DE SEGURIDAD

En la actualidad, a medida que los niveles de pobreza crecen y la seguridad ciudadana por parte del Gobierno no se da abasto, es de suma importancia que todas las familias cuenten con un sistema de protección antirrobo o un sistema controlado remotamente con el cual accedan a la seguridad de su vivienda estando a distancia de la misma.

En Guatemala, muchas familias no cuentan con algún tipo de alarma contra cualquier tipo de circunstancias no favorables para un hogar, es por ello que se deben estudiar las posibilidades de implementación de proyectos e ideas factibles a favor de las personas que carecen de dichos servicios. Desde hace años se observa cómo el número de asaltos va incrementándose a medida que crece la pobreza y delincuencia dentro del país.

De manera general, se define a un sistema de seguridad como el conjunto de elementos e instalaciones necesarios para proporcionar a las personas y bienes materiales, en un lugar determinado, la protección frente a agresiones tales como robo, atraco o sabotaje e incendio.

Para suplir esta demanda, existe en el mercado un gran abanico de componentes (centrales, detectores, entre otros) con distintos atributos y distintivos propios (tales como el tamaño, precio, modalidad de trabajo, entre otros), complicando la labor de clasificar dichos materiales a la hora de la realización de diseños de los sistemas de seguridad. Otra dificultad es la obtención de datos acerca de sus topologías, protocolos a utilizar y fuentes de información.

Tomando en cuenta lo anterior, se comprende la importancia de contar con una serie de precauciones en los hogares que permitan tener seguridad y control a sus habitantes cuando los mismos no están en su vivienda.

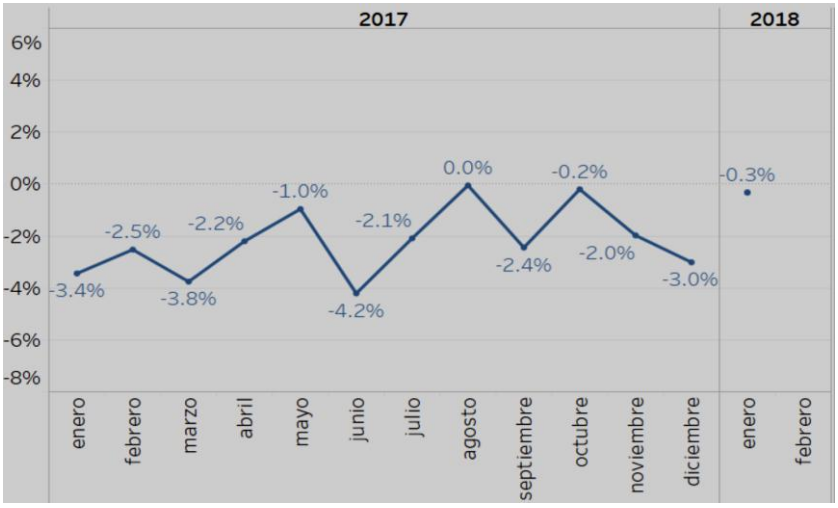
1.1. La inseguridad en la ciudad de Guatemala

La inseguridad y la violencia afectan a una gran parte de los guatemaltecos. Desde asaltos y extorsiones a personas particulares, hogares y negocios, hasta secuestros, violaciones y asesinatos en la vía pública. La integridad física y material de la población está en constante riesgo.

Como consecuencia, se han perdido espacios públicos en donde convivir sin miedo a convertirse en víctima de la violencia y la inseguridad, y la salud psicológica y calidad de vida de los ciudadanos guatemaltecos se ha deteriorado significativamente.

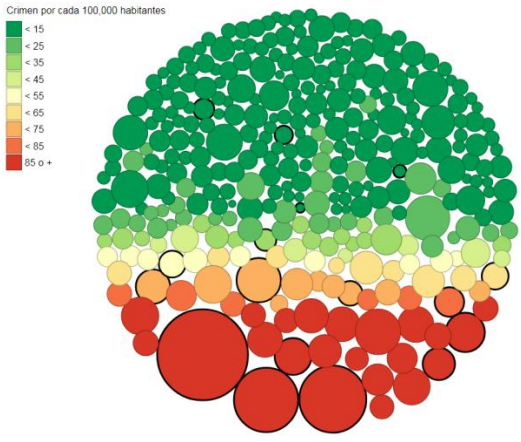
Acorde a la información del Centro de Investigaciones Económicas Nacionales (CIEN), los 17 municipios de la ciudad de Guatemala son los mayores en índices de homicidios, extorsiones, secuestros y robos a mano armada (véase figuras 1 y 2), el Índice de Denuncias de Delitos (IDD) en enero de 2018 se redujo 0,3 % respecto a diciembre de 2017. Esto significa que, en conjunto, hubo una leve reducción en las tasas de los delitos denunciados, aunque el subíndice de delitos contra la propiedad aumentó 1,4 %.

Figura 1. **Índice de denuncias de delitos (IDD) 2017**



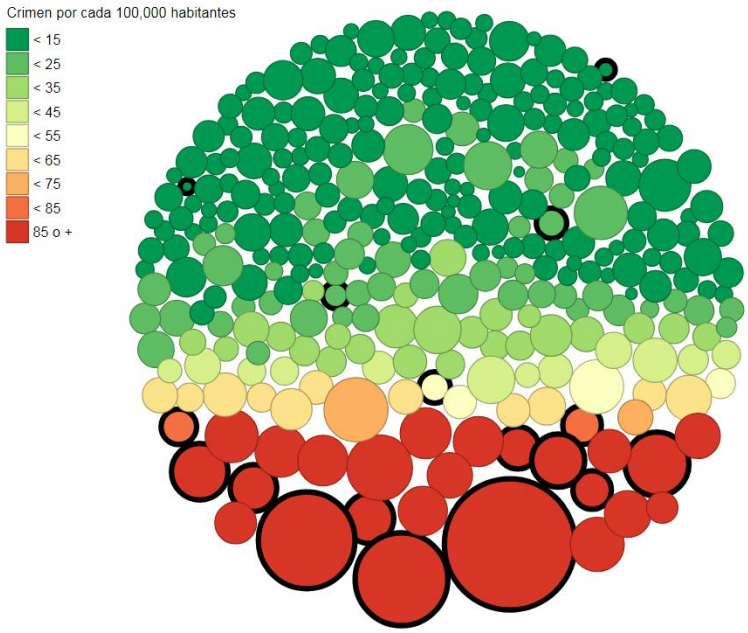
Fuente. Ministerio Público. *Secuestros y extorsiones.* https://public.tableau.com/profile/walter.menchu#!/vizhome/IndicedeDenunciasdeDelitos/CambiosIDD. Consulta: 25 de julio de 2018.

Figura 2. **Homicidios en la ciudad de Guatemala 2012, 2013**



Fuente: Ministerio Público; Policía Nacional Civil. *Robos y homicidios. Secuestros y extorsiones.* Ministerio Público. http://www.cien.org.gt/index.php/indicadores-de-seguridad-3/. Consulta: 25 de julio de 2018.

Figura 3. **Extorsiones en la ciudad de Guatemala 2012-2013**

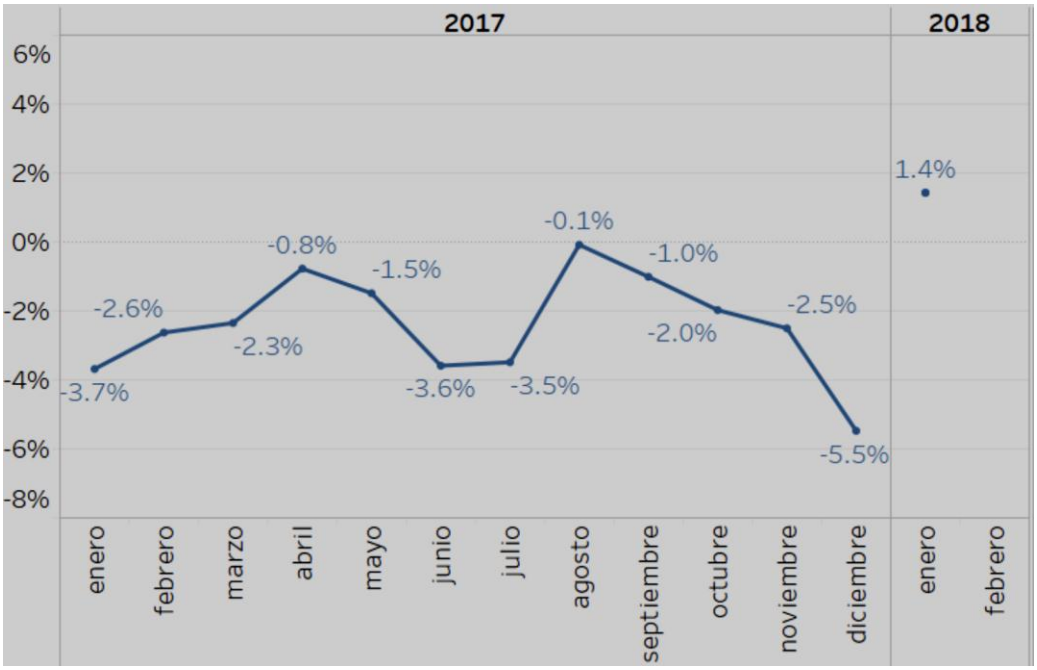


Fuente: Ministerio Público; Policía Nacional Civil. *Robos y homicidios. Secuestros y extorsiones.* http://www.cien.org.gt/index.php/indicadores-de-seguridad-3/. Consulta: 25 de julio de 2018.

1.2. Seguridad personal y residencial en Guatemala

Según el CIEN, el Subíndice de Delitos contra la Propiedad (SDPro) en enero de 2018 aumentó 1,4 % respecto a diciembre de 2017 (ver figura 4), lo cual implica que, en conjunto, aumentaron las tasas que componen este subíndice, principalmente por el incremento en la tasa de robo de vehículos y motocicletas.

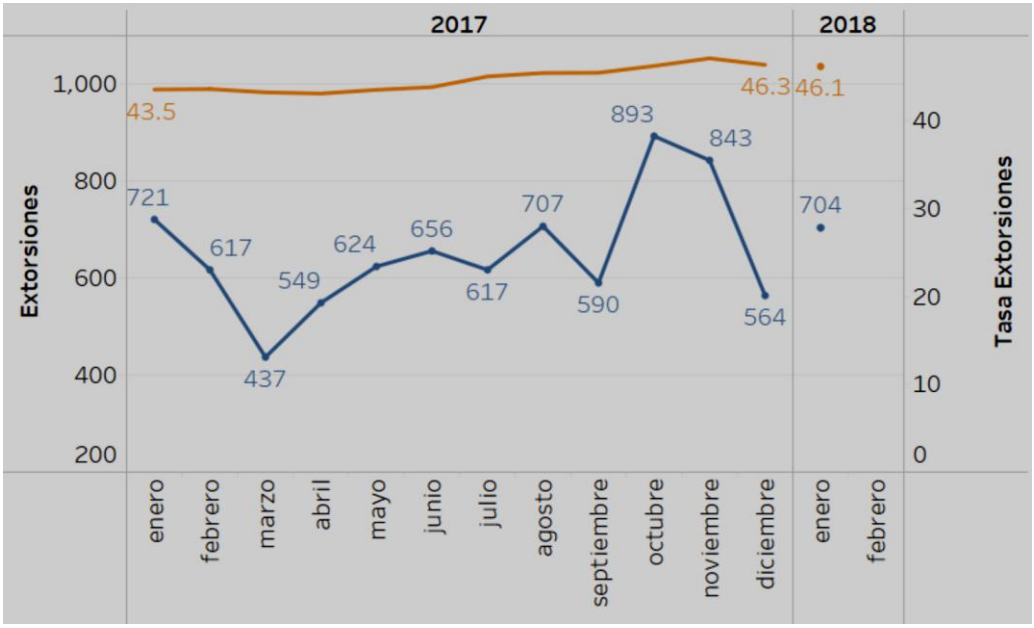
Figura 4. **Subíndice de delitos contra la propiedad**



Fuente: CIEN. *Boletín Estadísticos de Delitos.* http://www.cien.org.gt/wp-content/uploads/2018/02/Boletin-estadistico-delitos-enero-2018.pdf. Consulta: 25 de julio 2018.

En enero, la PNC registró 704 denuncias por extorsión, un promedio de 22,7 denuncias diarias, cifra superior a la registrada en diciembre (18,2 diarias). La cantidad de denuncias por extorsión volvió a incrementar respecto a lo registrado en diciembre. La tasa interanual de denuncias por extorsión en enero de 2018 es de 46,1 por cada 100 mil habitantes.

Figura 5. **Cantidad y tasa de extorsiones**



Fuente: CIEN. *Boletín Estadísticos de Delitos.* http://www.cien.org.gt/wp-content/uploads/2018/02/Boletin-estadistico-delitos-enero-2018.pdf. Consulta: 25 de julio 2018.

1.3. Ingreso *per cápita*, canasta básica y economía familiar en la ciudad de Guatemala

Guatemala cuenta con una de las canastas básicas más costosas de Centroamérica, según el Instituto Nacional de Estadística (INE), a través del documento Canasta Básica Alimentaria (CBA) y Canasta Ampliada (CA), en que presenta la Canasta Básica Alimentaria y su costo de adquisición, tanto por productos como en total.

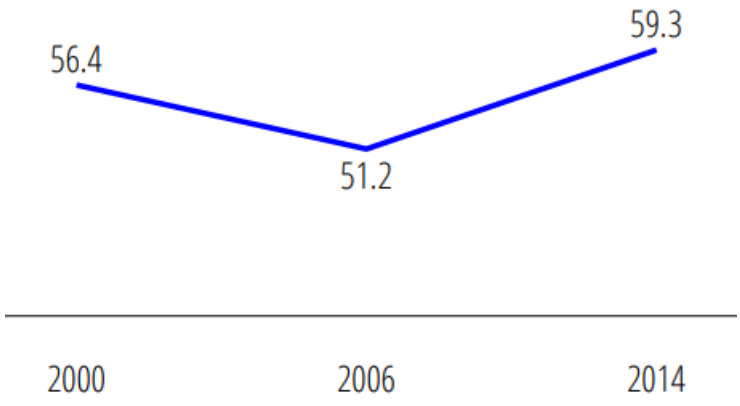
La CBA es un conjunto de alimentos que constituyen un mínimo necesario para satisfacer las necesidades energéticas y proteínicas de una familia y una

referencia para fijar el sueldo mínimo de un país. El costo total de la CBA de Guatemala se ha estimado en Q 3 523,49 al mes de junio de 2018.

La Encuesta Nacional de Condiciones de Vida (Encovi) tiene como principal objetivo conocer y evaluar las condiciones de vida de la población, así como determinar los niveles de pobreza existentes en Guatemala y los factores que los determinan.

Para 2014, el 59,3 % de la población se encontraba en pobreza, es decir, más de la mitad de la población tenía un consumo por debajo de Q 10 218 al año. Se puede observar en la figura 6 que entre 2000 y 2014 la pobreza total aumentó en 2,9 puntos porcentuales, pasando de 56,4 % en 2000 a 59,3 % en 2014.

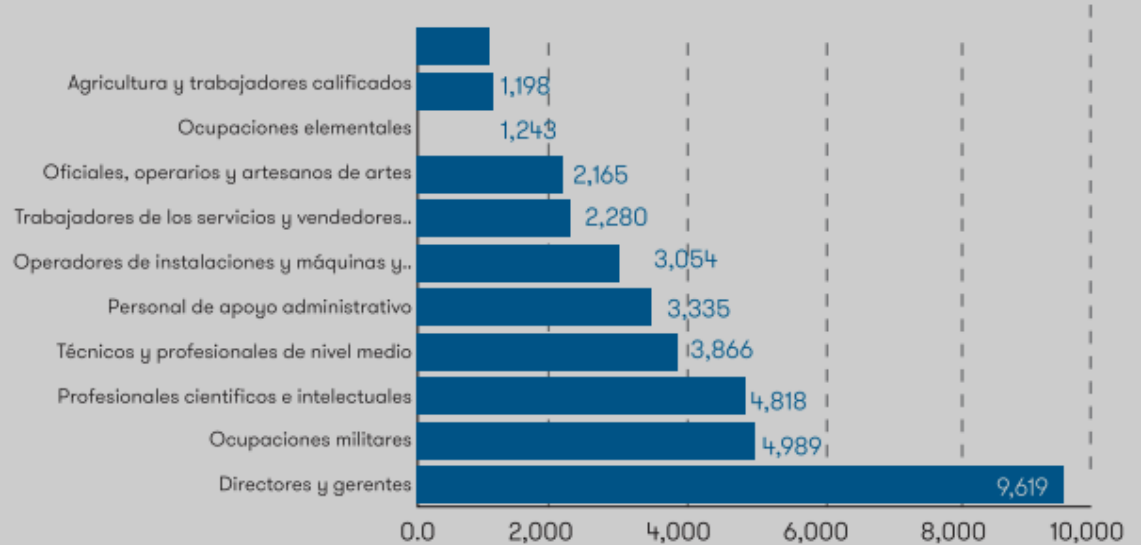
Figura 6. **Incidencia de pobreza total nacional**



Fuente: ENEI. *Encuesta nacional de condiciones de vida 2014*.
https://www.ine.gob.gt/sistema/uploads/2015/12/11/vjNVdb4IZswOj0ZtuivP IcaAXet8LZqZ.pdf
Consulta: 26 de julio 2018.

La Encuesta Nacional de Empleo e Ingreso (ENEI) indica que los ingresos laborales comprenden todos los ingresos provenientes del empleo asalariado, más los ingresos relacionados con el empleo independiente por concepto de beneficio o ganancia en la ocupación principal agrícola y no agrícola. El ingreso promedio a nivel nacional según la encuesta fue de Q 2,150.00. En la figura 7 se observa el promedio de ingreso laboral que obtienen los guatemaltecos por trabajar un promedio de 8 horas al día.

Figura 7. **Promedio de ingreso laboral mensual por ocupación principal**

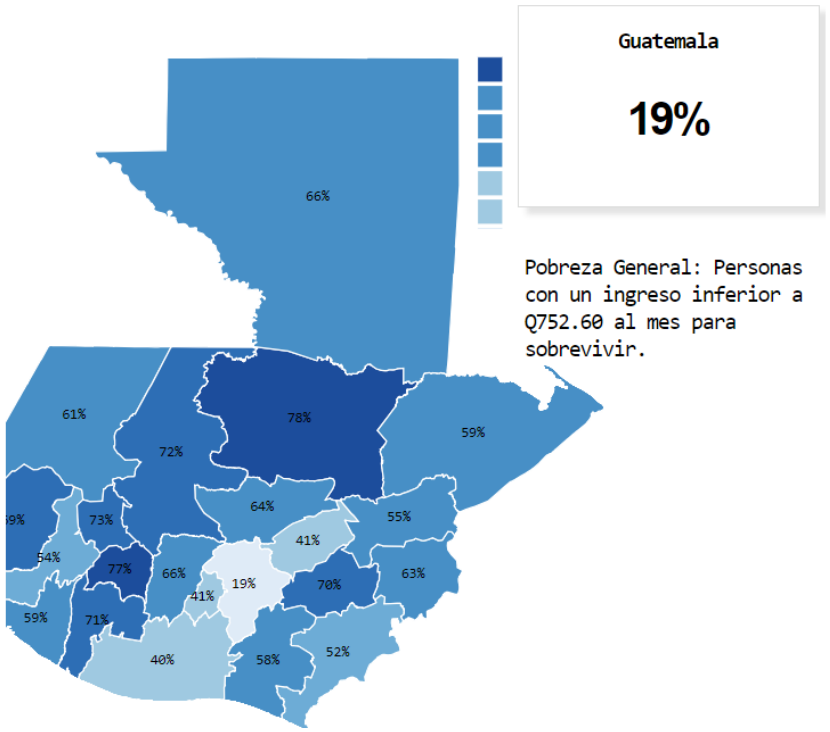


Fuente: ENEI. *Encuesta nacional de empleos e ingresos 3-207*. https://www.ine.gob.gt/sistema/uploads/2018/06/04/20180604154248NvGE8QaDqrUN7CbitcK2fqc8Rt5wIvMj.pdf. Consulta: 26 de julio 2018.

La ciudad de Guatemala cuenta con un 19 % de pobreza en general, esto quiere decir que, por cada 100 habitantes, 19 cumplen con un ingreso inferior a Q 752,60 para sobrevivir.

Tomando en cuenta la investigación del INE a través del documento Canasta Básica Alimentaria (CBA) y Canasta Ampliada (CA), en el cual se menciona que la CBA está en Q 3 523,49 al mes de junio de 2018, y observando la figura 3, 19 personas no tienen suficiente capital para cubrir la Canasta Básica Alimentaria para su familia.

Figura 8. **Porcentajes de pobreza a nivel nacional**



Fuente: elaboración propia, con datos obtenidos en el INE.

1.4. Observaciones de la oferta por parte de empresas distribuidoras de CCTV y de seguridad residencial

A medida que se incrementa el temor ciudadano ante el avance de la delincuencia, se multiplican los intentos de seguridad y ganan espacio los

servicios privados. Conforme avanza el índice de vandalismo y la pobreza dentro del país, la seguridad personal de los guatemaltecos y de sus residencias es cada vez menor y recaen en la necesidad de buscar otras alternativas para salvaguardar sus posesiones y propiedades.

La seguridad electrónica es una opción viable dentro de este sector, la tecnología utilizada por los sectores privados para la seguridad es accesible y, con ciertos conocimientos de electrónica, aplicable a los hogares, pero los servicios prestados por dichas organizaciones no están al alcance del presupuesto de una familia que requiere uno de estos dispositivos para la vigilancia a distancia.

Dentro de la capital guatemalteca hay compañías dedicadas a la distribución de dispositivos electrónicos sofisticados para la vigilancia remota, también se pueden obtener servicios robustos en cuanto al control a distancia de cámaras y alarmas que detectan algún tipo de movimiento dentro de la residencia.

Tabla I. **Costos de algunos servicios de seguridad residencial**

Compañía núm. 1	Equipo desde Q 2 045,00 hasta Q 5 090, aproximadamente. Servicio que incluye, monitoreo y derechos reacción de patrulla Q 250,00 pago mensual. Gastos adicionales dependiendo de la cantidad y tipo de dispositivos.
Compañía núm. 2	Equipo desde Q 3 000,00 hasta Q 5,000, aproximadamente. Únicamente venta de equipo Gastos adicionales dependiendo de la cantidad y mantenimiento

Fuente: elaboración propia.

No obstante, el costo para cubrir dichos servicios con sus respectivas mensualidades es alto y, muchas veces, imposible de cubrir por una familia (véase tabla I). Los pagos a realizar hacia estas empresas privadas varían entre Q 2 000.00 hasta Q 5 000 únicamente en equipo. El monitoreo y soporte es un gasto extra mensual con un intervalo entre Q 200,00 y Q 500,00.

También existen ciertas empresas distribuidoras de equipos electrónicos de vigilancia pero no prestan ningún soporte o mantenimiento a las unidades, únicamente venden el equipo para que el encargado de la familia lo instale y sea su responsabilidad el mantenimiento y soporte del mismo, sin dar alguna capacitación de cómo se debe utilizar y cuáles son los pasos a seguir para realizar una buena instalación.

1.5. La necesidad de sistemas de seguridad de uso doméstico

Conforme los datos proporcionados por el INE, tomando los indicadores de seguridad y justicia dentro de la nación, ha habido un incremento en los robos y hurtos a residencias desde el 2009 (véase tabla II).

De acuerdo con la figura 4, debido al aumento de la inseguridad residencial, hoy en día resulta muy recomendable invertir en la seguridad dentro de las viviendas y así tener un mejor control del patrimonio.

Tabla II. **Incremento de robos reportados por la PNC**

Año	Residencias
2009	964
2010	954
2011	1000
2012	1237

Fuente: elaboración propia.

La mayor cantidad de los allanamientos de morada ocurren cuando los dueños de la propiedad están fuera de casa. Por esto se requiere contar con un buen sistema de alarmas de seguridad que ayudará con el monitoreo de la residencia.

2. INTRODUCCIÓN A SISTEMAS CONTROLADOS REMOTAMENTE

Se recomienda, en la mayoría de los casos, contar con un sistema controlado a distancia y obtener parámetros de variables de entrada y salida en tiempo real. Con la tecnología actual se logra tener acceso a un gran número de dispositivos que logran este propósito de una manera fácil y ordenada, tomando en cuenta que, derivado de su fabricación y protocolos, la gran mayoría de ellos cumple con objetivos similares y aplicaciones a gran escala.

Un sistema controlado a distancia tiene como objetivo automatizar y manipular algún mecanismo para realizar cierta acción estando a una distancia considerable del mismo.

Acceso es el acto de alcanzar o de aproximarse a cierto objeto o mecanismo. Remoto es aquello que se encuentra alejado, apartado en tiempo o en espacio o que es poco probable que suceda.

El acceso remoto se emplea en informática para nombrar a la posibilidad de realizar ciertas tareas en un dispositivo, sin estar físicamente en el espacio donde se encuentra el equipo. Esto es posible gracias a software y dispositivos que cuentan con protocolos de manejo remoto, permitiendo trabajar con la unidad central del proceso a distancia. Escrito de manera sencilla, un acceso remoto consiste en acceder a un dispositivo conectado en una red desde otro dispositivo conectado a otra red diferente. De este modo es posible realizar tareas en un dispositivo, enviando las órdenes desde otro dispositivo a una distancia del mecanismo principal.

2.1. Importancia de un sistema controlado remotamente

El monitoreo mediante accesos remotos a cualquier sistema facilita al usuario visualizar y mantener los parámetros de un proceso, supervisar el comportamiento del sistema y controlar a distancia las variables a utilizar. Contar con acceso remoto a un sistema beneficia directamente a la persona que así lo necesite, ya que no requiere estar físicamente en el lugar donde se encuentra instalado el equipo para brindar soporte, resolver dudas o realizar algún ajuste.

La tecnología de un sistema de gestión a distancia proporciona a los equipos de monitoreo (en este caso cámaras y sensores) datos de manera eficiente y oportuna. Con esta información el usuario puede concentrarse en sus labores diarias sin preocupaciones, dado que será notificado en caso exista algún cambio de las variables en los dispositivos utilizados. El resultado es un procedimiento con mayores niveles de confiabilidad, productividad y confianza.

Un sistema controlado remotamente hace que el manejo de algún proceso o tarea sea más eficiente, permitiendo al usuario manipular variables de entorno de manera inmediata y ordenada mediante hardware y software especializado para dicha labor.

2.2. Herramientas para control de sistemas remotamente

La generalización de Internet como un medio de comunicación global y el surgimiento de nuevas e interactivas plataformas virtuales ha permitido explorar campos de tecnologías a distancia, cuyas ventajas, en cuanto a reducción de recursos económicos y tiempo de operación/reacción, son muchas al momento de hacer una comparación entre implementación-costo.

La comunidad estudiantil es uno de los sectores de la sociedad que más se ha beneficiado con el uso de la red. Cada día crece el número de aplicaciones web y herramientas gratis que brindan alternativas sencillas y fáciles de manejar para el control de algún elemento operado a distancia. Las herramientas para administrar un sistema de control remotamente son creadas para la comodidad del usuario final y, con la expansión del Internet, permiten la manipulación de dos o más elementos simultáneamente.

Dichas herramientas van desde páginas web gratuitas como TeamViewer, que ofrece soporte remoto completo sin necesidad de instalación, JoinMe, que permite a varias personas conectarse a una misma computadora y manipularlo remotamente, hasta aplicaciones móviles para Android e iOs, que interactúan con el usuario final a través de su teléfono celular, permitiendo el acceso en cualquier momento a los elementos conectados a la red.

Es de vital importancia acceder de manera remota a los servidores utilizados en alguna implementación, debido a que no siempre se podrá acceder de manera física a ellos.

Esta capacidad de acceder desde cualquier lugar dota de una gran versatilidad y, por ejemplo, permite en muchos casos poder trabajar a distancia y desempeñar estas funciones desde lugares remotos. Entre las herramientas más utilizadas destacan:

- PuTTY: es una herramienta muy útil, por ejemplo, si se está trabajando en un equipo bajo Windows y tiene que conectarse vía SSH a un servidor con GNU/Linux. Es un cliente muy ligero que ofrece SSH, Telnet y rlogin, es sencillo de manejar, sin necesidad de instalación y muy completo.

- WinSCP: es un cliente SFTP (SSH File transfer Protocol, por sus siglas en inglés) que permite transferir archivos entre un par de hosts en un canal de comunicación seguro.

- UltraVNC: es otra de las herramientas fundamentales ya que, basándose en el protocolo VNC (Virtual Network Computing), ofrece acceso remoto a otros equipos mediante interfaz gráfica o escritorio remoto, por ejemplo, equipos con sistema operativo Windows. La aplicación está basada en un modelo cliente servidor, por tanto, debe ser instalado el módulo servidor en las máquinas que se desean administrar de manera remota y el cliente en aquellas que se utilizarán para el acceso remoto.

- GSM (Global System for Global Communications, por sus siglas en inglés) es el sistema de comunicaciones que más se utiliza en teléfonos móviles y es un estándar en Europa. Permite el manejo remoto a través de la transmisión de datos vía SMS e Internet.

- GPRS (General Packet Radio Service) es una extensión del GSM basada en la transmisión por paquetes que ofrece un servicio más eficiente para las comunicaciones de datos, especialmente en el caso del acceso a Internet. La velocidad máxima del GPRS es de 171kb/s.

2.3. Aplicaciones de un sistema controlado remotamente

Domótica es un sistema capaz de agrupar información proveniente de sensores o entradas de datos en una vivienda, procesarla y ejecutar alguna instrucción de salida. El sistema puede acceder a redes exteriores de comunicación o información mediante dispositivos inteligentes como un teléfono móvil o una computadora portátil, todo esto gracias al manejo de herramientas a

distancia. Este tipo de sistemas aportan ahorro energético, accesibilidad, toma de decisiones y acceso a información instantáneamente.

Mediante la utilización de sistemas domóticos se puede controlar:

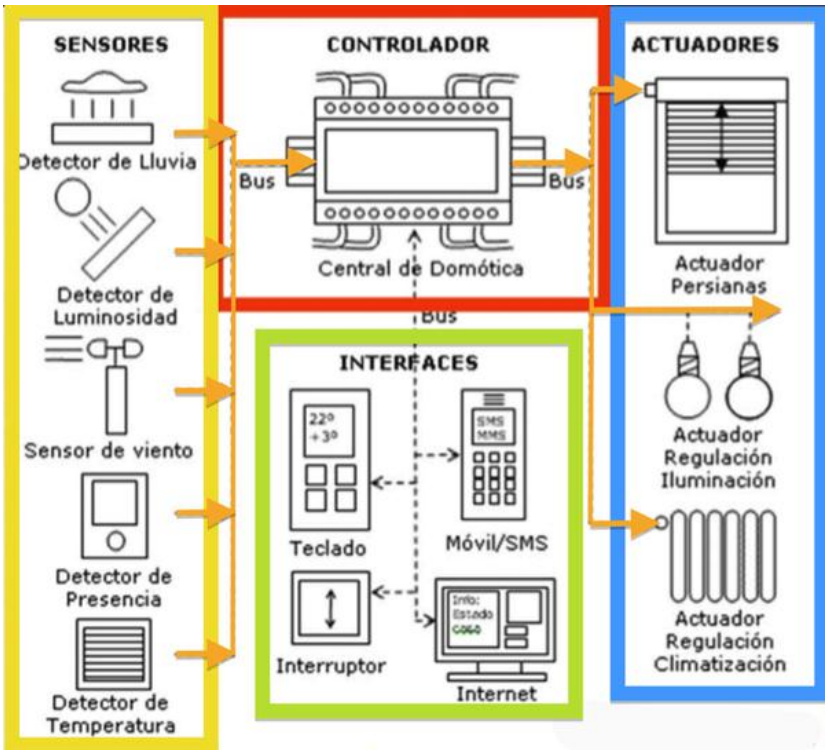
- Iluminación: activar o desactivar, control de presencia, control de intensidad, nivel de luz en diferentes habitaciones simultáneamente.

- Calefacción y refrigeración: aumentar o reducir la calefacción central o detectar variaciones según los diferentes espacios de la edificación, llevando un seguimiento y control de la temperatura.

- Control del riego: mediante sensores de humedad permite controlar este sistema de forma autónoma por medio de temporizadores, este control puede llevarse a cabo con lecturas periódicas de datos arrojados por dichos sensores.

- Electrodomésticos: sctivar o desactivar los electrodomésticos según sea necesario, utilizando por ejemplo un control secuenciado de la puesta en marcha programando su funcionamiento en horarios de menor coste energético.

Figura 9. **Partes de un sistema domótico básico**



Fuente: HERNANDEZ, Pedro. *Partes de un sistema de domótica.* https://pedrojhernandez.com/2014/04/07/domotica/. Consulta: 10 de agosto 2018.

En general, se puede definir un sistema de seguridad como el conjunto de elementos e instalaciones necesarios para proporcionar a las personas y bienes materiales, existentes en un local determinado, protección frente a agresiones, tales como robo, atraco o sabotaje e incendio.

2.4. Sistemas automáticos de seguridad

En este tipo de sistema controlado a distancia se puede monitorear parámetros como apertura de puertas, apertura de ventanas, alarma de intrusos, alarma de humo y control de cámaras conectadas a una misma red.

Los beneficios de implementar un sistema automático de seguridad y controlado a distancia son abundantes, van desde el control de acceso a personas que ingresan a la residencia hasta notificación de las autoridades sobre posibles intrusos.

Figura 10. **Esquema básico de un sistema de seguridad controlado remotamente**

Fuente: Biocomelectronica. *Sistema de seguridad remoto.* http://www.biocomelectronica.com.ar/soluciones/informatica/cctv-product-1.htm. Consulta: 10 de agosto de 2018.

2.4.1. Robótica

Esta rama se ocupa del diseño, construcción, operación y aplicaciones de robots en distintas ramas de ingeniería aplicadas al desarrollo humano y electrónico. El propósito general de los proyectos aplicados en robótica es optimizar el tiempo, realizar trabajos forzosos y, en la mayoría de casos, peligrosos para las personas. Un robot controlado a distancia en la industria o laboratorios que requieran realizar procesos industriales y experimentos/análisis que sean riesgosos para los humanos son un buen ejemplo de aplicación de la robótica.

El sistema de control a distancia puede ser por medio de módulos Bluetooth que permiten realizar trabajos con hasta una distancia de 25 metros a través de paredes normales (concreto) o cristales, con lo que cómodamente un operador puede trabajar en su proceso desde otro cuarto o a una distancia segura, o bien, nanotecnología avanzada para controlar mecanismos complejos a cientos de kilómetros de distancia.

Un ejemplo de esta tecnología es el Rover Curiosity, un astro móvil de exploración marciana dirigido por la NASA. Dicho astro móvil fue lanzado en noviembre de 2011, enviando las primeras imágenes del planeta Marte hacia la Tierra con gran precisión. Utilizando generadores termoeléctricos de radioisótopos como fuente de energía, cámaras MastCam para captar imágenes en múltiples espectros y en color real, espectrómetros y muchas herramientas controladas remotamente. Por ello este astromóvil es una de las aplicaciones destacadas de la robótica controlada a miles de kilómetros de distancia.

3. BASES DEL DISEÑO PARA EL SISTEMA DE SEGURIDAD

Para obtener una mejor gestión en un sistema de seguridad controlado remotamente es necesario contar con ciertos dispositivos electrónicos que permitan la manipulación e implementación sencilla del mismo. Dichos dispositivos, en este caso, deben estar al alcance del presupuesto de los usuarios que deseen adquirirlos y contar con la documentación necesaria para su manejo.

Se realizó una fusión de tecnología digital, soportada por software y hardware libres que brindan propiedades como precisión, confiabilidad y compatibilidad con diferentes componentes, aplicando diferentes conceptos que interactúan entre sí. Todo esto para lograr el control de seguridad en una casa residencial en tiempo real, el cual será apto para enviar parámetros con información esencial a través de una red WAN, con el objetivo de dar al usuario final un manejo remoto en la seguridad de su hogar.

WAN, por sus siglas en inglés Wide Area Network, es una red de telecomunicaciones que une equipos de computación a varios kilómetros de distancia y permite brindar conectividad a varias ciudades o un país entero.

Con base en la tecnología que brindan las telecomunicaciones (red 3G) y los sistemas de hardware integrados, se puede lograr una interconexión entre ambas ciencias aplicadas para desarrollar un sistema embebido de control y monitoreo remoto de parámetros que serán enviados a un servidor central (Raspberry Pi) para el procesamiento de señales digitales, el cual se encarga de los métodos de monitoreo y aviso de alertas hacia el usuario final.

Red 3G es una red móvil de tercera generación que permite la posibilidad de transmisión de voz, descarga de software, intercambio de correos electrónicos y mensajería instantánea

3.1. Raspberry Pi modelo 2B

Es un dispositivo electrónico u ordenador en placa reducida de bajo costo, desarrollado específicamente para el avance en el estudio tecnológico. En la mayoría de casos, utiliza un sistema operativo basado en Debian, específicamente en Raspbian, que está optimizando para este hardware y cuenta además con el conjunto de programas básicos y utilidades, varios paquetes y programas precompilados para una mayor facilidad de instalación y uso de Raspberry Pi. Uno de los modelos más populares de este dispositivo en la actualidad es conocido como Raspberry Pi Modelo 2B, por ser una de las variantes de mayor rendimiento, con 1 GB de RAM, 4 puertos USB, puerto HDMI, velocidad de procesador de 900 Mhz y un puerto Ethernet 100MB.

Figura 11. **Raspberry Pi modelo 2B**

Fuente: Raspberrypi. *Raspberry Pi 2B.* https://www.raspberrypi.org/products/raspberry-pi-2-model-b/ Consulta: 16 de agosto de 2018.

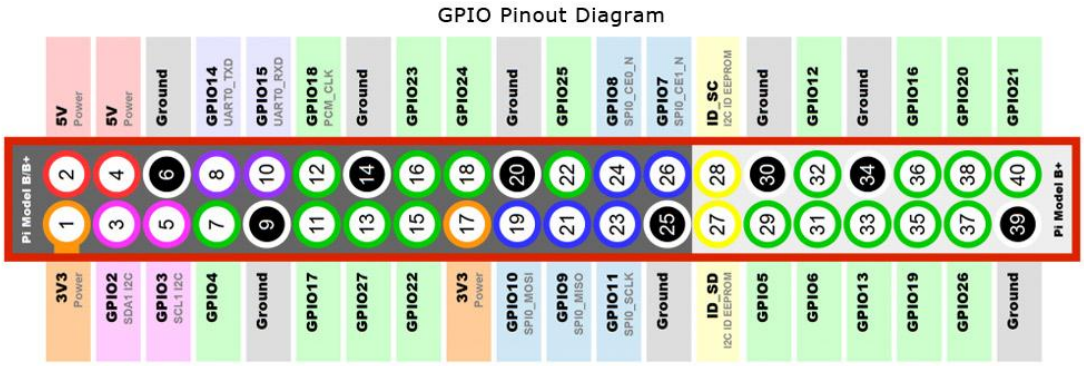
Este modelo de tarjeta, en comparación a modelos anteriores, posee mejoras en procesamiento de señales e instrucciones y memoria de lectura, también dispone de protocolos esenciales como comunicación UART (que será utilizado para la comunicación entre Raspberry Pi y el módulo de conexión a la red), I2C (siglas en inglés de *Inter-Integrated Circuit*), es un bus de datos que permite la comunicación entre diferentes partes de un circuito), SPI (siglas en inglés de Serial Peripheral Interface), es un protocolo de comunicación serial síncrono que permite la transferencia de datos entre dispositivos o una salida digital de modulación de ancho de pulso (PWM), además de 40 pines GPIO.

UART, siglas en inglés de Universal Asynchronous Reciever-Transmitter, significa Recepción-Transmisión Asíncrona Universal, es un protocolo de comunicación serial asíncrono para transferencia de datos entre dispositivos

GPIO, siglas en inglés de General Purpose Input/Output, los pines de Entrada/Salida de Propósito General, son pines en un dispositivo, los cuales pueden comportarse como entrada o salida dependiendo de la configuración hecha por el usuario a nivel software.

Este dispositivo se utilizará como placa base en el proyecto por la capacidad y eficiencia en hardware para interactuar con diferentes dispositivos simultáneamente, además, cumple con los requerimientos expuestos anteriormente para cubrir las necesidades del sistema de seguridad controlado a distancia.

Figura 12. **Configuración de pines de propósito general de Raspberry Pi 2B**



Fuente: RaspberryPi. *Configuración de pines.* https://i.stack.imgur.com/sVvsB.jpg. Consulta: 17 de agosto de 2018.

A continuación se resaltan las características de la Raspberry modelo 2B que se utilizará en el sistema y sus puertos principales, donde se puede observar el rendimiento interno en cuanto a video, audio, memoria y almacenamiento, considerando las siguientes siglas designadas para los nombres en las magnitudes y temas expuestos:

- CHIP: estructura pequeña hecha de material semiconductor sobre la que se fabrican circuitos electrónicos.

- GPU: siglas en inglés de Graphics Processing Unit, Unidad de Procesamiento Gráfico dedicada al procesamiento de gráficos.

- ARM7: es una arquitectura de Ordenador con Conjunto Reducido de Instrucciones o RISC (Reduced Instruction Set Computer, por sus siglas

en inglés), que permite ejecutar tareas con un mínimo consumo de energía.

- GB: unidad de almacenamiento de información con capacidad de mil millones de bytes.

- SDRAM: siglas en inglés de Synchronous Dynamic Random-Access Memory. Memorias de acceso aleatorio síncronas y dinámicas, son utilizadas para el procesamiento de instrucciones desde 1970.

- ETHERNET: estándar de red que permite a las computadoras conectadas a una red local enviar y recibir datos evitando cualquier tipo de superposición de información.

- USB: siglas en inglés de Universal Serial Bus, el Bus Universal de Serie es un dispositivo de almacenamiento de datos.

- HDMI: siglas en inglés de High-Definition Multimedia Interface, es la interfaz multimedia de alta definición que permite una mejora de video y audio a cualquier dispositivo que posea esta ranura en su placa madre.

- SD: siglas en inglés de Security Digital, es una unidad de almacenamiento de datos para dispositivos móviles.

- MMC: siglas en inglés de MultiMedia Card, es igual que la memoria SD con la cualidad de ser más grande de tamaño.

- SDIO: siglas en inglés de Security Digital Input Ourtput, es una de las primeras unidades de almacenamiento de datos para dispositivos móviles, mucho más pequeña en capacidad que una SD.

- LINUX: sistema operativo con licencia libre cuyo código fuente puede ser modificado, programado y redistribuido bajo los términos de Licencia Pública General de Linux.

Tabla III. **Características principales de la Raspberry modelo 2B**

Chip	Broadcom BCM2837 Arm7. Procesador de cuatro núcleos alimentado por una sola computadora que funciona a 900MHz.
Gpu	Doble núcleo con soporte de Open GL ES 2.0, hardware acelerado OpenVG hasta 1080p30 H.264.
Memoria	1GB SDRAM LPDDR2.
Conexión Ethernet	Ethernet RJ45 10/100 BaseT.
USB	4 puertos USB 2.0.
Video	HDMI 1.3 y 1.4 tamaño estándar a 1080p con soporte. CEC para control desde el mando del televisor.
Audio	Audio digital por salida HDMI y salida de audio estéreo compartida con la salida de vídeo compuesto.
Almacenamiento	SD, MMC, SDIO.
Sistema operativo	Linux.
Consumo energético	1A.

Fuente: Element14. *Raspberry 2B.* https://www.element14.com/community/docs/DOC-73827/l/raspberry-pi-2-model-b-1gb-technical-specifications. Consulta: 16 de agosto de 2018

3.2. Tecnologías móviles: módulo de conexión GSM/GPRS

GSM, siglas en inglés de Global System for Mobile Communication, el Sistema Global para Comunicaciones Móviles es un protocolo que permite enviar y recibir mensajes por medio de correo electrónico, faxes, navegación a Internet y servicio de mensajes cortos.

El GSM se ha caracterizado como uno de los más importantes sistemas de comunicaciones móviles a nivel mundial y se desarrolló originalmente para transmisión de voz, pero también es capaz de transmitir paquetes de datos a una velocidad baja.

Con los avances de esta tecnología se obtiene una mejora en la velocidad de transmisión de hasta 43,2 kbit/s que, si bien aún es baja, mejora grandemente el rendimiento de la transmisión de datos por medio de la red.

Dicho sistema global para comunicaciones móviles es utilizado por grandes operadores de redes GSM, ya que tienen acuerdos de *roaming* con operadores extranjeros, con el fin de poder comunicarse sin pagar algún costo adicional (esto ocurre únicamente cuando se tiene cobertura con el mismo distribuidor de servicios). Esta, junto a otras tecnologías como los Servicios de Radio de Paquetes Generales (GPRS), permitió un gran avance en los servicios en telefonías móviles.

La itinerancia, *roaming* en inglés, es la opción que ofrece un operador de telefonía de utilizar sus servicios en una red móvil distinta de la suya, normalmente fuera del país, y permite conectar al cliente con su red mediante acuerdos entre operadores.

GPRS, siglas en inglés de General Packet Radio Service, es el servicio general de paquetes vía radio. También es un servicio de comunicación inalámbrica basado en el uso de paquetes de información, mejorando la versatilidad y velocidad de transmisión de sus predecesores.

Dicho servicio se puede emplear para navegación por Internet, acceso WAP, SMS y MMS. La velocidad máxima de transmisión de datos para este tipo de módulos está en el intervalo de 50 a 100 kilobits por segundo.

WAP, siglas en inglés de Wireless Applications Protocol, es el protocolo de aplicaciones inalámbricas y un estándar utilizado internacionalmente para aplicaciones que requieren conexión a redes inalámbricas, por ejemplo, el servicio de Internet desde algún dispositivo móvil.

SMS, siglas en inglés de Short Message Service, es el servicio de mensajería corta, fue creado en 1985 junto con el GSM y son protocolos utilizados para envío y recepción de mensajes cortos en telefonía móvil.

MMS, siglas en inglés de Multimedia Messaging Service, es la mensajería multimedia móvil y un estándar que permite a los usuarios el envío y recepción de mensajes de texto con formato, sonido, imágenes, animaciones y vídeo *clips.*

3.2.1. Módulo Thinker A7

El módulo A7 integra en un solo dispositivo un modem GSM/GPRS y un receptor GPS. El modem GSM/GPRS permite la recepción y envío de mensajes SMS, también es posible conectarse a Internet mediante GPRS. Dicho módulo, por ser de bajo consumo, trabaja con parámetros de voltaje de alimentación de

5 VDC y una corriente menor a 2mA. El Thinker A7 soporta llamadas de voz, 2 puertos seriales y red celular 2G.

GPS, *s*iglas en inglés de Global Positioning System, el sistema de posicionamiento global permite tener la ubicación en todo el mundo de un objeto, persona o vehículo mediante satélites que orbitan alrededor de la tierra con trayectorias síncronas para cubrir la mayor cantidad superficie terrestre.

A continuación se listan las características principales de dicho módulo, considerando las siguientes siglas designadas para los nombres en las magnitudes y temas expuestos:

- Codificación de voz: proceso de transformar las ondas sonoras en otro tipo de representación con el fin de modificar o alterar su contenido de una manera más adecuada y sin grandes pérdidas.

- GPRS clase 10: referencia a la velocidad de transmisión de datos, en este caso se trata de un GPRS de 5 ranuras activas.

Tabla IV. **Características generales: módulo Thinker A7**

Bandas GSM/GRPS soportadas	850, 900, 1800, 1900 MHZ
Servicios soportados	Llamadas de voz, mensajería de texto SMS, audio digital y soporte de audio analógico para codificación de voz.
GSM / GRPS	GPRS clase 10, sensibilidad menos a -105, tráfico de datos de descarga 85.6 kbps y subida 42.8kbps
Temperatura de funcionamiento	-30 °C a 80 °C.

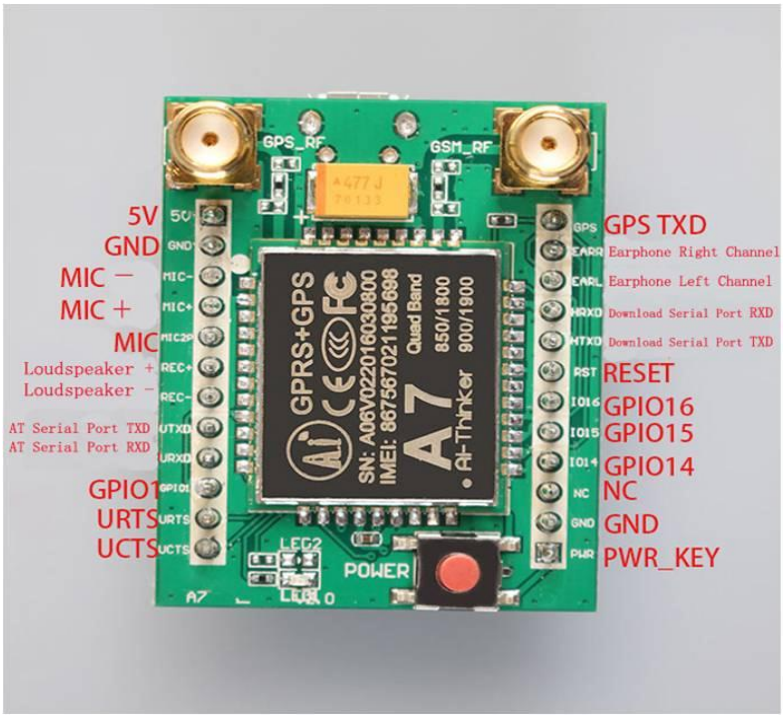
Fuente: Communica Colombia. *Thinker A7.* http://www.communica.co.za/Content/Catalog/Documents/D1266435144.pdf. Consulta: 22 de agosto de 2018.

Tabla V. **Características eléctricas de módulo Thinker A7**

Parámetro	Intervalo	Dimensional
Tensión de funcionamiento	3.3 a 4.2	VDC
Tensión de alimentación	Mayor a 3.4	VDC
Corriente de alimentación	3	mA

Fuente: Communica Colombia. *Características eléctricas de Thinker A7.* http://www.communica.co.za/Content/Catalog/Documents/D1266435144.pdf. Consulta: 22 de agosto de 2018.

Figura 13. **Configuración de pines de propósito general de módulo Thinker A7**



Fuente: Arduino S. A. *Pines de propósito general de Thinker A7.* https://forum.arduino.cc/index.php?topic=455984.0. Consulta: 22 de agosto de 2018.

3.2.2. Aplicaciones de módulo Thinker A7

Por ser un dispositivo económico y de fácil manejo, el módulo Thinker A7 puede ser utilizado en una amplia variedad de proyectos aplicados a la manipulación y control de mecanismos a distancia gracias a su tecnología GSM/GPRS. A continuación se listan algunos ejemplos:

3.2.2.1. El Internet de las Cosas (*Internet Of Things – IoT*)

El Internet de las Cosas o IoT (por sus siglas en inglés), es la acción de interconectar a Internet los objetos cotidianos que rodean a una persona, desde una lámpara sencilla hasta el manejo e interacción de una casa entera. Por medio del módulo se logra tener el control sobre algún dispositivo electrónico, mecánico, electrodoméstico o eléctrico, mediante mensajes de texto y conexión a Internet.

3.2.2.1.1. Control y monitoreo de seguridad vehicular

Mediante la herramienta de GPS y GSM del módulo Thinker A7 se puede implementar un prototipo de control y monitoreo en un sistema de seguridad para vehículos, utilizando las comunicaciones de redes móviles, se puede realizar una llamada al número del vehículo y adquirir controles como activar o desactivar la alarma, abrir o cerrar los seguros de las puertas, encender o apagar el vehículo y aire acondicionado, abrir el baúl o el capó, solicitar información de variables físicas del vehículo como la temperatura, niveles de gasolina o aceite, entre otros.

3.2.2.2. Módulo de comunicación Thinker A7

Para lograr una comunicación fluida y constante entre el usuario final y el mecanismo a manipular, el módulo A7 utiliza una serie de comandos específicos que permiten el manejo de sus funciones generales de una manera amigable y consistente, dichos comandos son conocidos como comandos Hayes o comandos AT. Los comandos AT son un tipo de lenguaje de programación estándar para la configuración y parametrización de dispositivos moduladores y demoduladores de señales (*módems*).

Los comandos AT fueron desarrollados por la empresa Hayes Communications, la cual introdujo el lenguaje AT a las compañías pioneras de *módems* y ayuda a controlar la mayoría de ellos mediante instrucciones enviadas a través del puerto serial de una computadora, estos comandos hacen posible que haya una comunicación entre software y hardware. Este lenguaje es el más conocido y usado para manipulación de *módems*, ya que casi el 100% de ellos debe comenzar con el prefijo AT de Atention, que coloca al *módem* en modo escucha.

A continuación se listan los comandos AT básicos para establecer una comunicación entre *módems* y computadoras:

Tabla VI. **Comandos AT más utilizados**

Nombre	Descripción	Ejemplo
AT	Comando base de los comandos Hayes. Con este se comprueba la disponibilidad del dispositivo.	--
ATA	Para contestar una llamada, también se configura en respuesta automática.	--
ATB	Para elegir el estándar de comunicación a la hora de iniciar la conexión.	ATB0
ATD	Comando para realizar una llamada.	ATD48488259
ATE	Activación/Desactivación del eco del *módem.*	ATE0 desactiva eco ATE1 activa eco
ATH	Permite colgar la llamada actual.	--
ATL	Controla el volumen del altavoz del dispositivo.	--
ATA	Contestar una llamada.	--
AT+CBC	Muestra el estado de la batería del teléfono, valores de estado y los niveles de batería.	AT+CBC=?
AT+CGMM	Para solicitar información sobre el número de modelo del *módem.*	
AT+COPS	Nombre de la compañía telefónica.	
AT+CSCS	Tipo de texto.	
AT+CMGL=ALL	Sirve para ver todos los mensajes que han llegado al SIM.	

Fuente: elaboración propia.

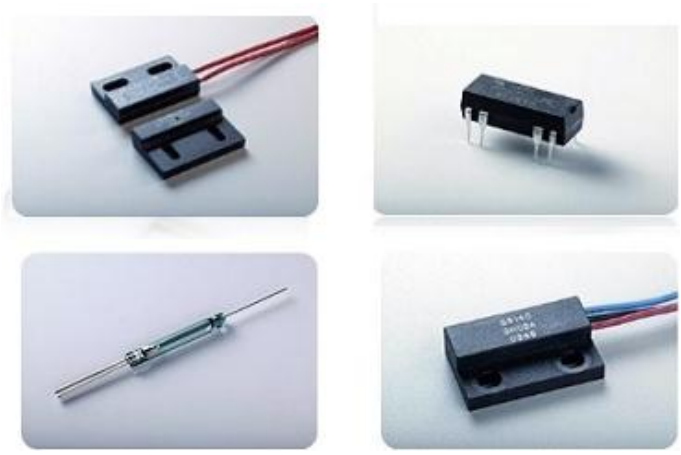
3.3. Interruptor magnético Reed Switch

También llamado interruptor de lengüeta, es un dispositivo que permite o impide el paso de corriente eléctrica con la unión de sus terminales por medio de un campo magnético. Cuando sus terminales están normalmente abiertos, al

someterlos a un campo magnético generado por un imán o electroimán, proceden a cerrarse y dejar pasar el flujo de corriente eléctrica.

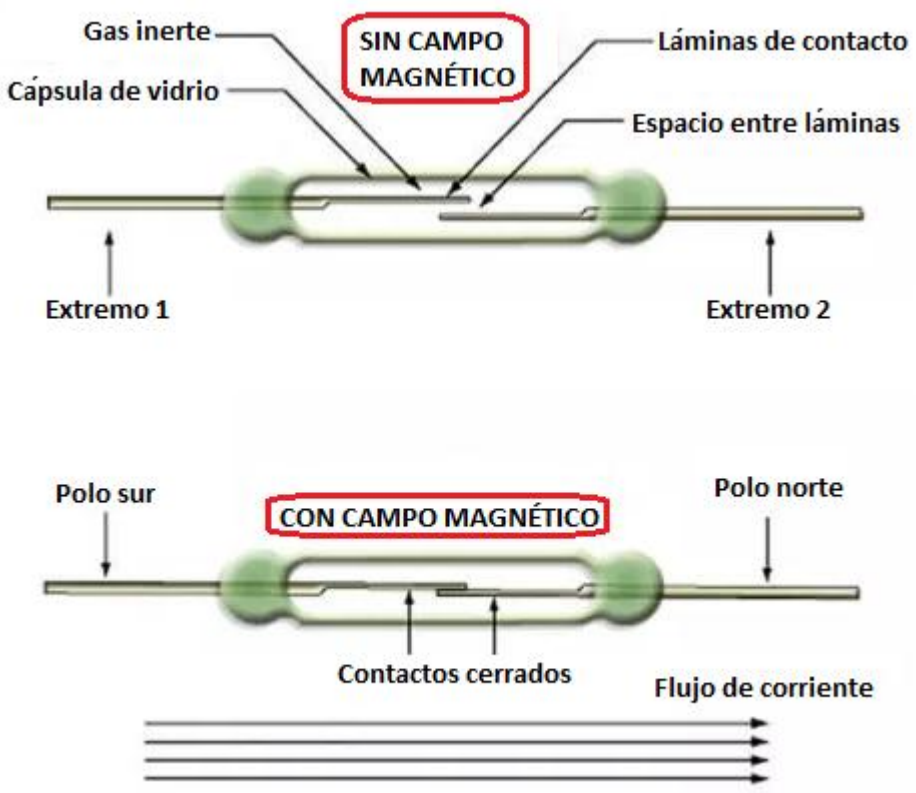
Un interruptor es un dispositivo que permite o interrumpe el paso de la corriente eléctrica mediante accionamientos mecánicos, electrónicos o electromagnéticos. Este interruptor magnético se compone de dos láminas compuestas por hierro y níquel, herméticamente selladas en una cápsula de vidrio. Internamente las dos láminas se intercalan dejando solo un pequeño espacio entre ellas, dicho espacio deja de existir ante la presencia de un campo magnético adecuado. El interruptor es fabricado dependiendo de su aplicación y exposición a las corrientes eléctricas y campos magnéticos que se utilizarán.

Figura 14. **Diferentes tipos de encapsulados Reed Switch**



Fuente: elaboración propia.

Figura 15. **Funcionamiento de interruptor Reed Switch**



Fuente: elaboración propia.

3.3.1. Principales características y aplicaciones

Los interruptores magnéticos tipo Reed se suelen utilizar para la sustitución de los interruptores convencionales (finales de carrera con émbolos, rodillos y palancas giratorias, interruptores de encendido/apagado mediante accionamiento manual). En la industria de los ascensores, los interruptores magnéticos se emplean para el control y el posicionamiento de los mismos.

El uso adecuado para estos interruptores es cuando las condiciones de trabajo, para los interruptores mencionados anteriormente, no son las adecuadas para ciertas labores como velocidades de respuesta altas o bajas, frecuencias de cambio de estados elevadas, condiciones con gran demanda de polvo o suciedad y humedad elevada.

Por tratarse de un dispositivo electrónico mecánico de bajo costo y respuesta inmediata, el interruptor Reed puede aplicarse a diversas situaciones de la vida cotidiana, por ejemplo:

- Lectura de nivel de agua en un tanque cisterna.
- Recuento de objetos de pasaje (cuántas personas u objetos pasan o están dentro de determinada área).
- Indicadores de posición.
- Sistemas básicos de seguridad en cerrojos y ventanas.

4. VENTAJAS DE UN SISTEMAS DE SEGURIDAD DE BAJO COSTO

Los sistemas de seguridad en una residencia, en países del primer mundo, han ganado mucha popularidad en los últimos años debido a que son muy útiles mientras la residencia está vacía, y añaden un valor agregado reduciendo de manera significativa el costo del seguro de hogar. Esto es debido a que las compañías encargadas de asegurar los hogares entienden que, cuando una casa está protegida por un sistema de alarmas inteligentes, el riesgo de demandas en contra de ellos por robo es casi mínimo, así que el costo de equipar una propiedad con alarmas inteligentes normalmente no es visto como un gasto, sino como una inversión.

Un sistema de seguridad puede ayudar con la protección de las personas que residen en dicha vivienda y salvaguardar las posesiones más preciadas cuando la casa está vacía. También es importante contar con un sistema de seguridad residencial, ya que la mayoría de los habitantes de una residencia están gran parte del tiempo en su trabajo o fuera de casa por motivos personales. Los sistemas de seguridad en el hogar se han hecho indispensables para todo aquel que desee tener un control óptimo de su vivienda cuando no está en ella o sobre su integridad física mientras duerme.

Un sistema de seguridad es un conjunto de elementos e instalaciones necesarios para proporcionar, a las personas y bienes materiales existentes en un local determinado, protección frente a agresiones tales como robo, atraco o sabotaje e incendio.

Una red de seguridad debe ser capaz de detectar una problemática dentro del lugar donde está instalada, enviar una notificación a la persona encargada del sistema y realizar alguna acción programada en su memoria. Por ejemplo, en un asalto, en principio detectará el problema, luego lo señalizará, para posteriormente iniciar las acciones y notificar al propietario de la residencia o encargado de dicho sistema para realizar un accionamiento de mecanismos o llamadas a centrales de policía cercanas.

Los sistemas de seguridad pueden ser variables según las necesidades del local a proteger y del presupuesto disponible para ello. En el mercado existe un gran abanico de componentes (centrales, detectores, entre otros) con características técnicas y calidades distintas, haciendo casi imposible de tipificar a la hora de la realización de diseños de los sistemas de seguridad.

La aplicación de los sistemas de seguridad es un hecho en el mundo de la industria automatizada y en los procesos de fabricación, ya sea seguridad por motivos de personal de fábrica o seguridad hacia inmuebles de la compañía. Estos sistemas tienen como finalidad controlar la cadena de funcionamiento, indicar al operario la existencia de un fallo, un mal funcionamiento, un sobrecalentamiento, etcétera. Direccionando de esta manera un sistema de seguridad se puede abrir un campo basto para las aplicaciones y la necesidad de un sistema de control de este tipo.

Estos sistemas no son únicamente para proteger a los bienes e inmuebles de una compañía, además estas aplicaciones se pueden utilizar para otros propósitos como proteger a personas en general (dependiendo la aplicación y motivos para implementar el sistema).

4.1. Necesidad y aplicación de un sistema de seguridad

Cuando se habla de un sistema de seguridad, no se trata únicamente de un sistema antirrobos, a través del tiempo el hombre se ha visto en la necesidad de proteger sus pertenencias, ya sea por motivos de sustracción por parte de otros individuos o por las acciones normales de la naturaleza.

Con la aparición de la electrónica y el avance en los dispositivos controlados a distancia, se ha logrado establecer un rápido progreso en lo que se refiere al concepto de seguridad, ya que proporciona una variedad de posibilidades en los sistemas, transformando antiguos conceptos de vida. Con lo anterior se logra hacer una pequeña lista de las aplicaciones más frecuentes en cuanto a sistemas de seguridad.

4.1.1. Seguridad en la vivienda

Este tipo de sistemas está basado en el control de parámetros como higiene, seguridad antirrobo, seguridad contra accidentes domésticos, etc. El tema de seguridad en la vivienda es ampliamente utilizado en el mundo para tratar problemáticas como las antes expuestas y brindar confianza a los residentes con aplicaciones móviles y avisos periódicos sobre el estado de la vivienda.

4.1.2. Seguridad en establecimientos públicos y privados

Se trata de un sistema con una red cerrada de cámaras y sensores con la finalidad de proteger un área más grande que una vivienda, son aplicados a espacios públicos como centros comerciales o plazas que son visitadas por miles de personas al día.

4.1.3. Seguridad en cárceles, centrales nucleares, entre otros

Este tipo de seguridad es una de las más importantes en aplicación y una de las más robustas y difíciles de implementar, dado que se trata de sensores especializados para la radioactividad (en el caso de un sistema de seguridad para centrales nucleares) y actuadores electromagnéticos y circuitos cerrados de televisión (Closed Circuit Television, CCTV por sus siglas en inglés), en el caso de seguridad en cárceles o centros preventivos.

4.1.4. Seguridad activa contra incendios

Es uno de los sistemas más comunes dentro de un lugar cerrado (casas, locales, centros comerciales, entre otros), se trata de sensores que, con la tecnología en su interior, detectan la presencia de humo en el aire y emiten una señal sonora avisando del peligro de un incendio.

4.1.5. Control de niveles líquidos

Este tipo de control es comúnmente utilizado en la industria para verificar el contenido de un recipiente cerrado y, como proceso automatizado, cerrar válvulas o llaves de paso para detener el caudal de cierto líquido. Se puede ver este tipo de control en bombas de cilindros de gas propano o tanques de líquidos varios (agua, líquidos contaminantes, granos, entre otros).

4.1.6. Seguridad en calefacción y cuartos de máquinas

Al estar en la industria, una de las problemáticas frecuentes es que las maquinarias pesadas están propensas a cambios de temperatura que deben ser controlados mediante procesos automatizados que no pongan en peligro la

vida de las personas a su cargo, este tipo de controles pueden ayudar a prevenir sobrecalentamientos en maquinarias y accidentes por temperaturas elevadas. En la actualidad existe una gran gama de sensores que ayudan a solventar este problema y dar el control apropiado a los operarios, ayudando automáticamente a la toma de decisiones.

4.1.7. Control de gases, presiones, humedad

En los últimos años ha habido un crecimiento exponencial en cuanto a emisiones de gases por parte de empresas y vehículos alrededor de mundo. En la industria, un control de gases y control de presiones es fundamental a la hora de tomar en cuenta la seguridad personal y seguridad industrial, esto se logra con sensores especializados en esta materia que se encargan de extraer los contaminantes generados en un lugar específico, recolectarlos, hacer la conducción de los mismos mediante procesos internos, filtrarlos y hacer una evacuación en algún lugar propio de la empresa, con las mínimas posibilidades de escape o emisión de gases dañinos al ambiente.

4.1.8. Control antirrobos en vehículos automotores

Estos sistemas son los más comunes en el mundo, se trata de la implementación de dispositivos electrónicos como GPS y sensores de apertura, los cuales envían información en tiempo real a un usuario específico, o bien, a una compañía encargada de la distribución de sistemas de seguridad con el fin de proteger los bienes inmuebles de alguna persona que pagó por este servicio.

Los sistemas antirrobos cuentan con una gran serie de elementos que, además de traer un mejor control en una residencia o local comercial, brindan seguridad y tranquilidad hacia los usuarios propietarios de las mismas. Por lo

general cuentan con alarmas sonoras, cámaras con circuito cerrado, sensores de movimiento, sensores de apertura de puertas y ventanas. Ahora bien, los sistemas de vehículos automotores cuentan con una unidad de GPS y aviso en tiempo real de la posición actual del automóvil de algún usuario en específico. También pueden contar con interruptores de apertura para saber si el vehículo fue abierto sin autorización del usuario, todo esto depende de la aplicación que el usuario necesita dentro de su bien inmueble.

4.2. Clasificación de los sistemas de seguridad

En la tabla VII se presenta una serie de las mayores aplicaciones en cuanto a sistemas de seguridad.

Tabla VII. **Campo de aplicación de un sistema de seguridad**

Robo y atraco	Sensores Defensa física Dispositivos de acceso Circuito cerrado de televisión
Incendio	Sensores de incendio Accionamiento de dispositivos de extinción Accionamiento de sistemas de aviso Extinción manual Equipo de bombeo Puertas cortafuego Alumbrado de emergencia
Anti-hurto	Protección de artículos Escáner detector de rayos X Detector de explosivos Detector de metales
Especiales	Detector de humedad Detector de sustancias químicas Detector de presión Detector de gases

Fuente: RaspberryPi. *Campo de aplicación del sistema.* https://sites.google.com/site/seguridadelectronicagcm/capitulo-1/1-2-clasificacion-de-los-sistemas-de-seguridad-electronica. Consulta: 17 de septiembre de 2018.

4.3. Instalación de un sistema de seguridad

La instalación de un sistema de seguridad básico debe contener ciertas partes esenciales como:

4.3.1. Central de alarma

La central de alarmas es la que recibe el impulso eléctrico de los detectores o sensores que por algún motivo son activados. Al recibir esta señal, los circuitos electrónicos que lleva en su interior activan las instrucciones para activar el sistema de aviso e intercomunicador.

Este tipo de centrales son el cerebro de la instalación, dicha central está en continua vigilancia recibiendo información constante de los circuitos detectores que componen el sistema y, dependiendo de los estados en tiempo real de dichos sensores, realizan el accionamiento de algún dispositivo de aviso (sirenas, conexión inmediata al usuario encargado del sistema o alarma visual).

Una central de alarma se subdivide en las siguientes partes:

Tabla VIII. **Subdivisión de central de alarma**

Fuente de alimentación principal	Este tipo de suministro electrónico da la tensión suficiente a los encapsulados electrónicos que están dentro de la central, está constituido de un transformador reductor o fuente regulada de 110VAC (esto dependiendo de la región en donde está instalado el sistema) a un rango entre 6 a 24 voltios continuos, según la necesidad esta fuente también proporcionará voltaje a detectores, bobinas, cámaras etc.

Continuación de la tabla VIII.

Baterías	Este acumulador eléctrico se utiliza para prevenir cualquier falta de fluido eléctrico, puede ser manipulada para dar energía al circuito en ciertos momentos, o bien, desempeñar el papel de fuente de reemplazo del tendido eléctrico del lugar.
Microprocesador	Es la parte más importante dentro de la instalación ya que se encarga de las tomas de decisiones manipulando las diferentes salidas en el caso de incidencia en el sistema, accionamiento de alarmas, luces, sensores, intercomunicador, etcétera. El microprocesador requiere de una programación previa para efectuar dicho funcionamiento, esta programación dependerá exclusivamente de las necesidades a cubrir en el sistema. Dentro de dicha programación, efectuada por la persona encargada del sistema, se almacenan todas las variables a manipular, procedimientos a seguir y señales eléctricas enviadas por lo sensores. Todo lo anteriormente expuesto es guardado en la memoria programable de solo acceso o memoria interna del microprocesador, en ella se guarda cada línea de instrucción emitida por el programador a cargo del sistema.
Conexión con central receptora	Por medio de algún módulo electrónico, la central de alarmas se comunica con una central receptora del mensaje, dicha central puede ser desde el usuario encargado del sistema hasta una sucursal departamental o municipal de policía. La conexión que efectúe la central puede variar desde la comunicación de existencia de alarma, a otras como las de situación de atraco. La central de alarmas comunica a la central receptora toda incidencia en el sistema para que dicha central tome decisiones como activar o desactivar alarmas, zonas de detección, etcétera. La comunicación de esta central con la central de alarmas puede variar desde una llamada, un mensaje de texto o una interacción variada, esto dependerá de la programación de la central de alarmas y las necesidades del usuario en cuanto a la toma de decisiones y adquisición de datos como el estado actual, incidencias producidas, etcétera.

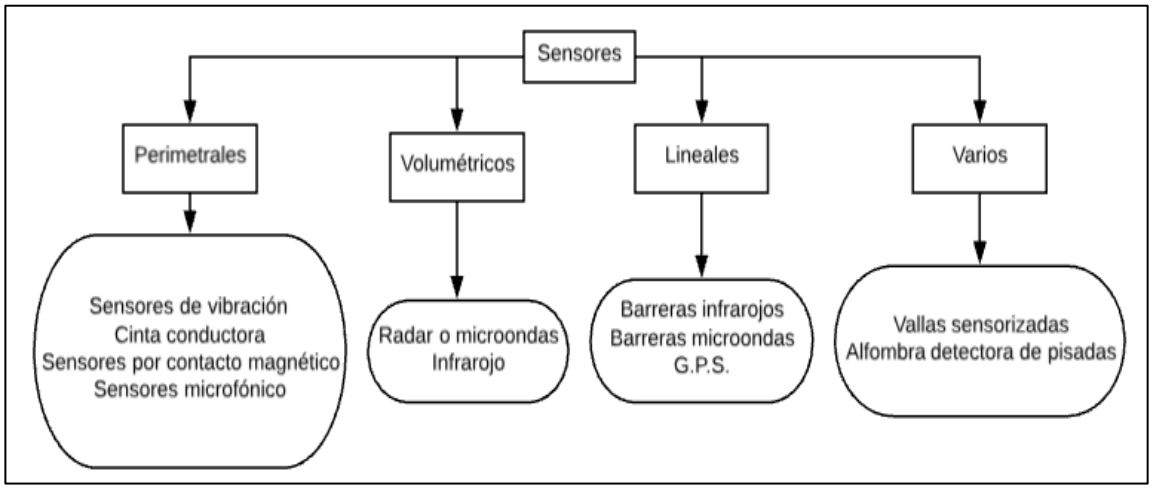
Fuente: elaboración propia.

4.3.2. Sensores

Un sensor es un dispositivo electrónico, eléctrico o mecánico capaz de variar sus propiedades ante alguna magnitud física o química llamadas variables de instrumentación. En un sistema de seguridad, los sensores son elementos capaces de comprobar las variaciones de un entorno determinado y envían información de esa variación a la central de alarmas. Son de reducido tamaño y se alimentan a través de una fuente de alimentación de baja tensión.

A continuación, se muestra una clasificación de los sensores más utilizados en la industria y en la vida cotidiana, su aplicación dependerá exclusivamente de las necesidades que tenga el usuario al momento de implementar un sistema de seguridad.

Figura 16. **Clasificación de los sensores**



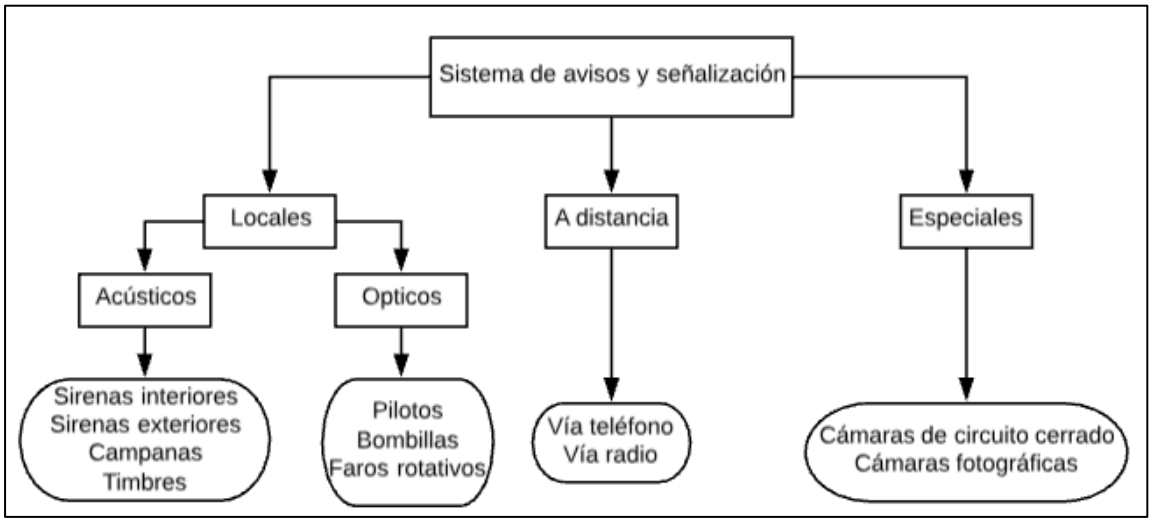
Fuente: elaboración propia.

4.3.3. Sistemas de aviso

Son dispositivos electrónicos simples pero de mucha ayuda, ya que son los encargados de dar indicaciones de las variaciones detectadas por los sensores dentro del sistema de seguridad. Dicho sistema es el que da sentido a los sistemas de seguridad, ya que si no estuvieran configurados dentro de la red, fuera inútil la colocación de detectores y central de alarma. Tales sistemas de aviso pueden ser acústicos (sirenas), ópticos (luces) o por vía Ethernet, dependiendo de la configuración y uso que se quiera darles.

A continuación se muestra una clasificación básica de un sistema de aviso, la aplicación de dicho sistema dependerá exclusivamente de las necesidades que tenga el usuario al momento de implementar un sistema de seguridad.

Figura 17. **Clasificación de los sistemas de aviso y señalización**



Fuente: elaboración propia.

4.3.4. Intercomunicador

Son dispositivos electrónicos de alto nivel de rendimiento encargados de transmitir la información de la central de alarmas al usuario final, este tipo de dispositivo contiene en su interior electrónica avanzada que logra la difícil tarea de intercomunicar a la persona encargada de un sistema de seguridad y todo el mecanismo a utilizar. El bloque del intercomunicador es esencial en la red de seguridad, ya que sin este el usuario no estaría recibiendo la información en tiempo real ni tendría la toma de decisiones final.

4.3.5. Accionamiento de otros dispositivos

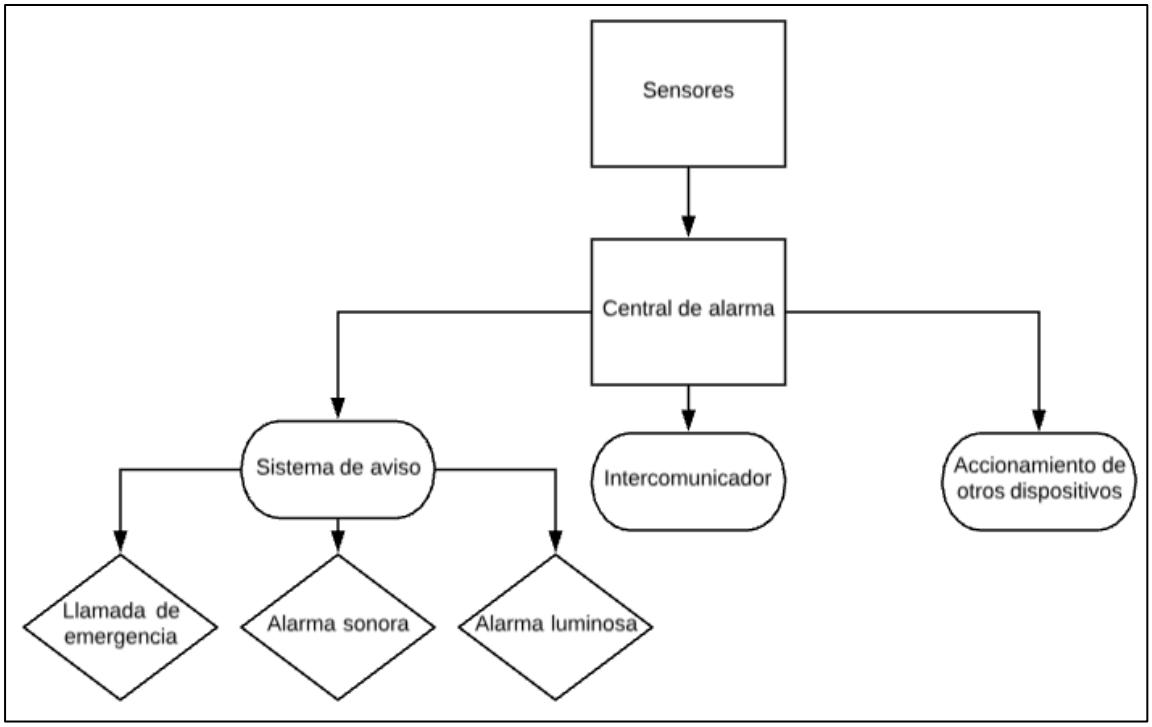
Es el sistema empleado para otorgar otro tipo de beneficios a un sistema de seguridad, puede proporcionar ciertas posibilidades a la hora de la activación de la alarma, algunas de ellas se listan a continuación:

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

La toma de decisiones en cuanto a utilizar un intercomunicador, accionamiento de otros dispositivos o señales de aviso, siempre dependerá de la central de alarmas. El sistema de seguridad será más fiable y seguro mientras más posibilidades externas y variables a manipular se quieran tener.

En la figura 18 se presenta un esquema simple para la conexión de un sistema de seguridad:

Figura 18. **Esquema para la conexión de un sistema de seguridad simple**



Fuente: elaboración propia.

4.3.6. Protección contra robos y atracos

Si bien un sistema de seguridad tiene como beneficio el cuidado de los bienes inmuebles de una persona o familia, también logra el objetivo de salvaguardar la integridad física de los implicados a la hora de implementar dicho sistema. Para tener clara la diferencia entre robo y atraco, atraco se define como aquel acto delictivo encaminado al lucro y que pone en peligro la integridad física de las personas. Por otra parte, robo es un acto delictivo encaminado al lucro pero que no pone en peligro la integridad física de las personas.

Los atracos ocurren cuando el local o establecimiento está funcionando normalmente, esto pone en peligro la integridad física de las personas dentro del área afectada, ya que pueden ser agredidas, golpeadas o, en el caso más grave, asesinadas dentro de dicha área. El robo, por su parte, ocurre en horas en que el establecimiento no tiene actividad y está vacío, o bien, la persona no está consciente de que ha perdido algún objeto personal o está siendo asaltada por alguna persona pero no ocurre ninguna agresión física.

Según las características y necesidades de la zona a proteger, así será la utilización de los tipos de sensores, sistema de aviso y la central de alarma, siempre atendiendo tanto a las características de la zona o zonas a proteger, como a las de los sensores a utilizar (campo de actuación, entre otros).

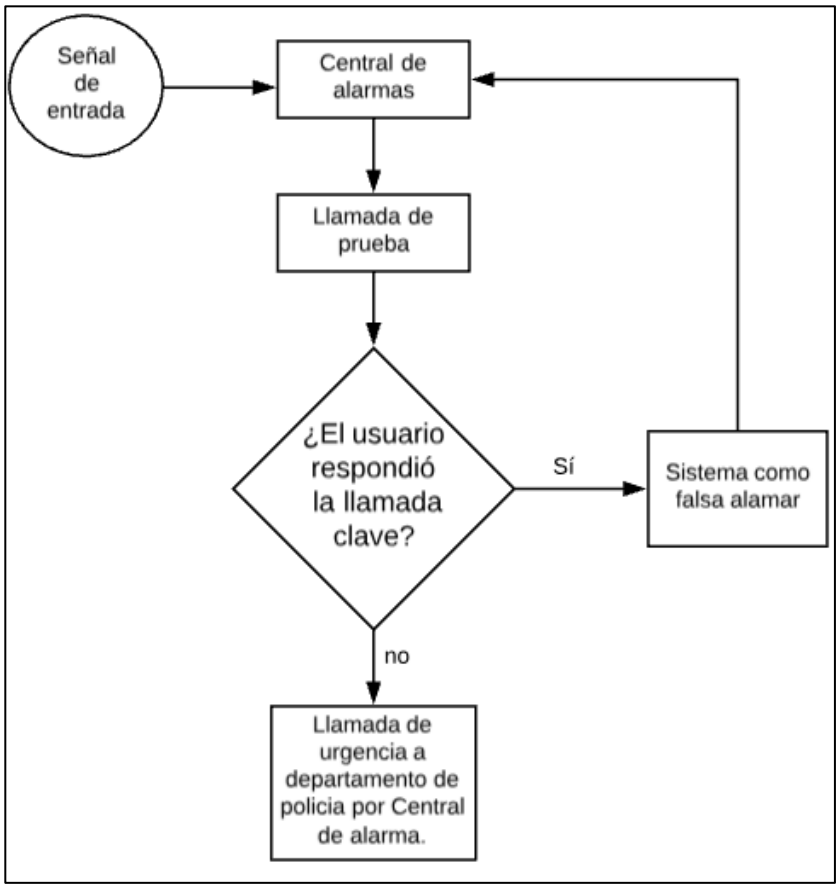
En situaciones como esta se hace necesaria la utilización de sistemas de detección automática que permita a la central de alarmas tomar decisiones de emergencia dado que el usuario no puede hacerlo. El procedimiento de pulsación de robo o atraco sufre un proceso que a continuación se expone. Este tiene como objetivo dar a conocer cuándo es una alarma real o cuándo es una falsa alarma, enviando rápidamente la policía en el primer caso.

El procedimiento utilizado comúnmente en una situación de atraco empieza cuando la central recibe indicación de alarma por medio de un interruptor colocado estratégicamente en el local a asegurar, realiza un envío de texto o una llamada automática de supervisión, que consiste en esperar cierto mensaje programado anteriormente por el encargado del sistema. Cuando se trate de una falsa alarma, el mensaje o llamada será contestada con dicho mensaje programado y el sistema entrará en estado general.

Si el mensaje recibido no es el acordado, o simplemente no se contesta a la llamada de teléfono, la central de alarma da aviso a la policía, que acude inmediatamente o recurre a una señalización óptica o visual para dar a conocer la situación del local afectado.

En la figura 19 se muestra un gráfico que la central de alarma sigue internamente:

Figura 19. **Proceso interno a realizar por central de alarma**



Fuente: elaboración propia.

4.3.7. Alarmas contra intrusos y sensores de movimiento

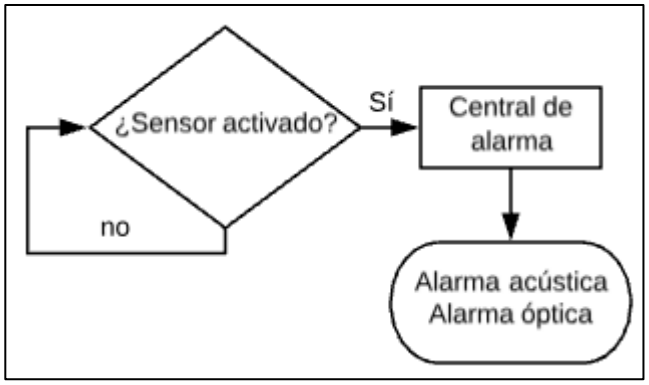
Para muchos expertos y distribuidores de sistemas de seguridad, las alarmas son el complemento de las rejas y cerraduras en un lugar cerrado que necesite algún tipo de protección. Muchos que contaban únicamente con una alarma sencilla, después de pasar cualquier clase de robo, ya sea a ellos o alguna residencia cercana, decidieron agregar rejas y cerraduras para lograr un sistema integral de seguridad. Una alarma, por muy sencilla que sea su fabricación, sirve para disuadir a los ladrones o personas que quieran hacer algún tipo de daño en un inmueble. Al sonar se pretende que dichas personas desistan de realizar lo indebido, por miedo a ser atrapados por algún vecino o que llegue la policía.

Este tipo de sistemas de seguridad se pueden describir como un sistema contra intrusos, su función es simple y se puede lograr una buena gestión de seguridad mediante ciertas instrucciones dadas a una central de alarma modificada por alguna persona capacitada para esa labor.

Por ser un sistema simple de alarma y detección, este sistema únicamente cuenta con un sensor que, por el tipo de trabajo que desempeña, puede ser un sensor magnético o un sensor de movimiento, una central de alarma (puede ser un microcontrolador básico) y una señal de aviso, la cual es local (este trabajo lo puede realizar una alarma o un timbre normal).

En la figura 20 se muestra el proceso interno que realiza la central de alarma:

Figura 20. **Proceso interno básico a realizar por un sistema de alarma contra intrusos**



Fuente: elaboración propia.

4.4. Sistema modificable a necesidades específicas

Al momento de configurar un sistema de seguridad mediante software, se debe tomar en cuenta que no todas las áreas a asegurar tienen las mismas necesidades o tienden a abarcar las mismas disponibilidades que otras. Un sistema de seguridad robusto no se mide únicamente por medio de la cantidad de elementos a utilizar, como por ejemplo cámaras de vigilancia o sensores de movimiento aplicados. Un sistema de seguridad también puede ser robusto por el software utilizado para su implementación.

El sistema puede ser robusto utilizando únicamente una o dos cámaras de seguridad, algunos sensores que detecten movimiento en puertas o ventanas y un intercomunicador para entablar una comunicación directa con el usuario final. Esto dependerá exclusivamente de la habilidad de la persona a cargo de la implementación del programa operativo y las aplicaciones que el usuario final quiera darle al sistema de seguridad.

Dicho software puede tener opciones como personalizar interfaces gráficas para el usuario mediante aplicaciones móviles, integrar posibles dispositivos electrónicos para hacer automatizaciones más grandes dentro del área a asegurar, etcétera.

Entre los objetivos de un sistema modificable se encuentran:

- Eliminar eficientemente los espacios inseguros de un área en específico utilizando pocos recursos y espacio.

- Facilitar el acceso y el cambio de dispositivos electrónicos del sistema en caso de desperfectos por motivo de sobrecalentamiento o utilización continua.

Un sistema modificable a necesidades específicas debe tener como objetivo principal proveer al usuario la facilidad de modificar el sistema de seguridad con pasos sencillos y tener colocados los dispositivos electrónicos con un cómodo acceso, tanto los dispositivos físicos y materiales utilizados como el programa en la central de alarmas. Dicha accesibilidad está a cargo de la persona responsable de la programación del sistema de seguridad, así como del usuario que está implementando el proyecto en el área de trabajo.

4.5. Versatilidad con espacios reducidos

A la hora de realizar una implementación de un sistema de seguridad, el espacio y la adecuada distribución de los dispositivos a utilizar es una de las mayores complicaciones a vencer, es un tema importante a la hora de planear una solución arquitectónica a nivel hardware y software, en la cual el usuario

final y la persona encargada de la central de alarmas deben estar de acuerdo y trabajar en equipo para realizar una implementación adecuada.

Cuando se habla de un sistema versátil se hace referencia a la capacidad del equipo y programación de adaptarse con rapidez y facilidad a distintas funciones y espacios, por lo tanto, la versatilidad es una característica primordial en un sistema gestor de seguridad.

Un sistema es versátil cuando está en condiciones de responder ante distintos desafíos y adaptarse a todo tipo de situaciones. En este caso, se habla de una versatilidad a espacios reducidos, esto quiere decir que los componentes del sistema de seguridad deben ser capaces de tener la propiedad de adaptabilidad a los espacios donde el usuario desee que estén, ya sea un espacio pequeño, grande, húmedo, al aire libre, a pocos centímetros del suelo o a una gran altura.

4.6. Sistema Open Source y aplicaciones

Hoy en día, los avances tecnológicos y las fuertes presiones competitivas han aportado cambios rápidos en las condiciones de trabajo y los procesos para realizar ciertas tareas. En el mundo de la informática hay miles de programas que ayudan con el día a día a millones de personas que desean realizar una labor general o específica. Dichos programas pueden ser de libre distribución y modificación, o bien, pueden tener alguna restricción de distribución.

Se conoce Open Source como un término utilizado para denominar cierto software que se distribuye mediante una licencia libre, que puede ser modificado y recibir mejoras sin tener la aprobación de una institución pública o privada.

Un sistema Open Source es un sistema con cierto tipo de software que se distribuye mediante una licencia que le permite al usuario final, con los conocimientos necesarios, utilizar el código fuente del programa para modificarlo y realizar mejoras. Este tipo de software provee ventajas a las personas interesadas, ya que los programadores, al tener acceso libre al código fuente de una determinada aplicación, pueden modificarlo y hacer mejoras del diseño original, añadiéndole opciones y corrigiendo errores iniciales, con lo que el software modificado estará mejor diseñado y elaborado.

Es de vital importancia saber la diferencia entre un software Open Source, mencionado anteriormente, y un software libre (el cual puede descargarse y redistribuirse de manera gratuita). La diferencia radica en que, a diferencia de un software Open Source, un software libre puede no brindar un acceso al código fuente, por lo que no puede considerarse un software Open Source. De manera similar, existen programas Open Source que se distribuyen de manera comercial o requieren una autorización para ser modificados.

Aunque ambos fundamentos suelen confundirse fácilmente, en muchas ocasiones la aplicación de un software Open Source está vinculada a un pensamiento de trabajo en conjunto sobre programas informáticos. Entre los programas de código abierto más populares se encuentran los siguientes:

- Navegador de Internet Firefox: ofrece herramientas y funciones para una navegación web fluida y completa. Incluye protección contra estafas, robo de identidades y asegura el uso más eficiente de la memoria de la computadora.

- Open Office: ofrece la creación y edición de presentaciones animadas, documentos de texto, hojas de cálculo y bases de datos robustas de uso

gratuito. Es altamente compatible con distintos sistemas operativos y permite la migración de documentos con Microsoft Office y PDF (Portable Documents Format).

- Linux Ubuntu: es un sistema operativo potente y amigable al usuario. Este sistema está basado en Linux e implementa todo el entorno visual similar al de Windows. El usuario puede utilizar todo el entorno de ventanas y conocer el terminal que permite instalar software, correr comandos y aplicaciones de manera más rápida. También viene con un centro de aplicaciones donde se puede buscar y descargar software por temas. Es uno de los sistemas operativos más usados a nivel mundial.

- Android: es el sistema operativo para dispositivos móviles más utilizado del mundo, se ha caracterizado por ser un sistema de código abierto más popular por su versatilidad y disponibilidad, por ende muchos desarrolladores aprovechan para usar sus habilidades y desarrollar aplicaciones para este sistema.

Al igual que un sistema Open Source, existen dispositivos físicos que pueden ser distribuidos y creados desde cero a partir de su diagrama esquemático y otra información libre. Estos dispositivos son llamados OSH.

OSH, por sus siglas en inglés Open Source Hardware, es un término utilizado para todos aquellos dispositivos cuyas especificaciones, modelos esquemáticos y construcción lógica son puestos en dominio público.

Bajo la definición de OSH se logra encontrar diseños para impresión 2D y 3D asistidos por ordenadores, archivos de diseño en PCB (Printed Circuit Board por sus siglas en inglés) y una gran gama de bibliotecas de componentes con

sus diseños esquemáticos (símbolos, huellas, sujetadores, entre otros). Dentro de los dispositivos OSH se encuentran las siguientes clasificaciones:

- Hardware reconfigurable: este tipo de hardware se desarrolla mediante archivos de texto que contienen el código fuente. Un hardware reconfigurable es el que viene descrito mediante lenguajes de descripción hardware (HDL, Hardware Description Language por sus siglas en inglés). En una descripción rápida, un hardware reconfigurable es un código fuente que se puede configurar a las necesidades del usuario.

- Hardware estático: este tipo de hardware es el conjunto de materiales de los sistemas electrónicos, son las piezas físicas que pueden crearse por un diseño PCB, o bien, crear un circuito más grande con la unión de ellos.

4.7. Implementación de bajo presupuesto

Un sistema de seguridad debe ser seleccionado acorde a las necesidades de un usuario, tanto necesidades de protección a inmuebles como necesidades socioeconómicas. Dicho servicio de seguridad es prestado por parte de varias instituciones privadas que, si bien pueden dar un servicio las 24 horas al día, cobran sumas excesivas para dar esa seguridad a los ocupantes de una casa, solo en Guatemala hay más de 200 instituciones privadas con licencia de operación para prestar dicho servicio. El servicio de estas empresas varía según la aplicación, nivel de seguridad, zona de riesgo y estudios que conllevan un gasto para la familia interesada en adquirir un sistema de control para la seguridad de sus bienes inmuebles.

En la tabla X se muestran las comparaciones básicas de un sistema de seguridad ofrecido por 2 de estas empresas privadas y el proyecto redactado en este documento, y el presupuesto para implementarlo:

Tabla IX. **Presupuesto del sistema de seguridad de bajo presupuesto**

Descripción del material	Costo
Raspberry pi 2B + Adaptador	Q 400
Cámara Web	Q 125
Memoria SD Clase 10	Q 85
Módulo Thinker A7	Q 200
Chip de telefonía móvil	Q 5
Adaptador CP2012	Q 60
Total	Q 875

Fuente: elaboración propia.

Tabla X. **Comparación entre sistemas de seguridad proporcionados por instituciones privadas**

Descripción del material	Box Security	Golán Group	Proyecto redactado
CCTV Cámaras	2	2 o más	1
Llamadas a usuario final	NO	SÍ	SÍ
Mensajería de texto	NO	SÍ	SÍ
Central de alarmas	SÍ	SÍ	SÍ
Actualizaciones	NO	SÍ	SÍ
Código abierto	NO	NO	SÍ
Mantenimiento	NO	SÍ	SÍ
Cobros mensuales	SÍ	SÍ	NO
Sistema de aviso (Alarmas visuales o sonoras)	NO	SÍ	SÍ
Costo de implementación	Q 1 899 Pago único	Q 2 045 + Cobros mensuales	Q 875 Pago único

Fuente: elaboración propia.

5. IMPLEMENTACIÓN DE SISTEMA DE SEGURIDAD EN CASA RESIDENCIAL

Se desarrolló un sistema de seguridad controlado a distancia con componentes electrónicos de bajo costo tales como una Raspberry Pi 2B, usada como unidad central de procesamiento del proyecto, encargada de manipular la cámara de vigilancia y la mensajería de texto (trabajando en conjunto con el módulo GSM/GPRS Thinker A7). También se empleó un sensor Reed Swicth, el cual es un interruptor manejado con campo magnético que se utilizó para captar la apertura de la puerta o ventanas de la residencia. Se utilizó el módulo Thinker A7, que permite la recepción y transmisión de mensajería de texto e integrar al proyecto el Internet de las Cosas (IoT) y la activación del sistema de aviso (alarmas sonoras o visuales antirrobos).

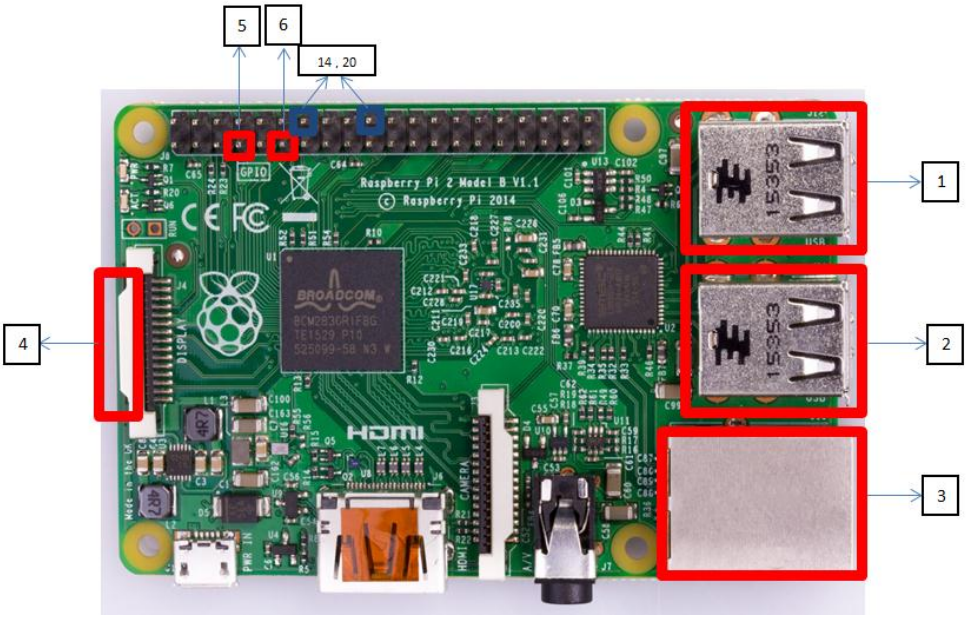
5.1. Principales conexiones de Raspberry Pi 2B

La placa reducida de bajo costo Raspberry Pi 2B cuenta con pines de entrada/salida de propósito general, los cuales, mediante un software diseñado específicamente para la implementación del proyecto, son configurados como transmisor y receptor de datos entre los elementos que controlan las variables externas de la residencia a proteger.

Se realizó y documentó cada parte del proyecto por separado, teniendo en cuenta que, al momento de realizar la implementación del sistema de seguridad, todas las secciones del proyecto deben interactuar en conjunto y trabajar al mismo tiempo para asegurar la eliminación de espacios no cubiertos por el sistema.

Como se observa en la figura 21, se utilizaron 2 pines de propósito general, 2 puertos USB 2.0 (utilizados para conexión de cámara web y adaptador CP2012), ranura SD para la memoria que almacena el sistema operativo a utilizar en el proyecto y la entrada Ethernet RJ45 para la conexión de la placa hacia el *router* residencial.

Figura 21. **Puertos utilizados para interconexión de elementos externos del sistema de seguridad**



Fuente: elaboración propia.

Donde:

- Puerto USB para CP2012 (comunicación con módulo Thinker A7)
- Puerto USB para cámara web
- Puerto Ethernet RJ45 (conexión con *router* residencial)

- Ranura SD para memoria
- Pin 7 de propósito general (entrada de señal del Reed Switch)
- Pin 11 de propósito general (salida de señal para sistema de aviso)
- Pines 14 y 20 para GND del interruptor magnético y alarma sonora

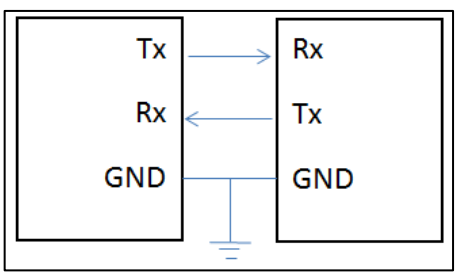
5.1.1. Comunicación Raspberry Pi 2B con elementos externos

A continuación, se muestra la conexión del módulo GSM/GPRS a Raspberry Pi 2B.

5.1.1.1. Conexión del módulo GSM/GPRS a Raspberry Pi 2B

La conexión del módulo GSM/GPRS con la placa reducida Raspberry Pi 2B se realiza a través del protocolo UART mediante un CP2012, el cual es un adaptador que permite la compatibilidad entre el protocolo UART del emisor (en este caso el módulo Thinker A7) y el receptor UART de Raspberry Pi 2B, permitiendo tener una comunicación fluida y confiable por medio del puerto USB. En la figura se muestra una conexión ideal entre emisor y receptor en una comunicación con protocolo UART.

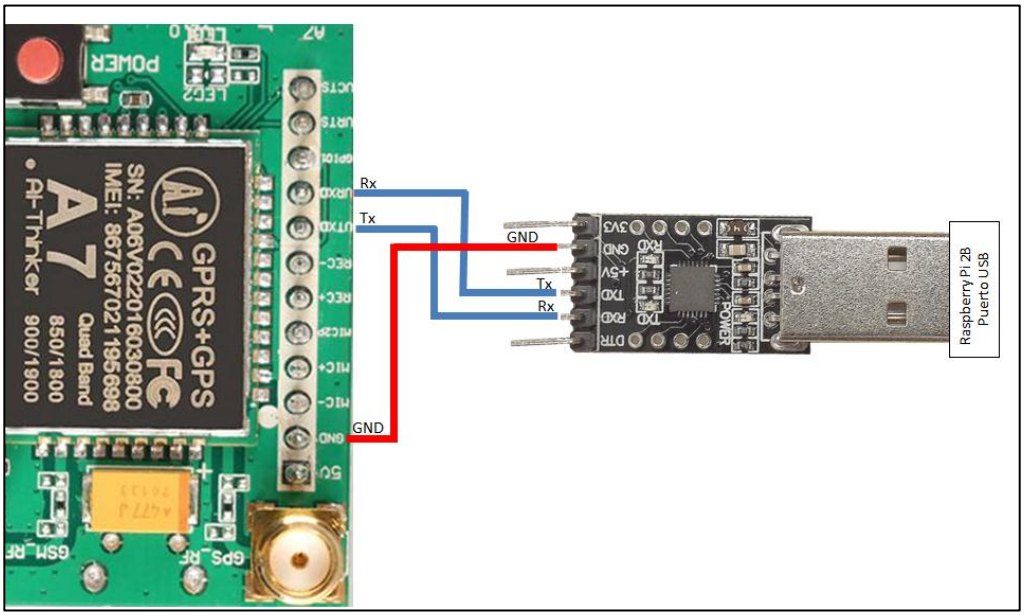
Figura 22. **Esquema básico de UART**



Fuente: elaboración propia.

Observando la figura 22 e interconectando el módulo Thinker A7, el adaptador CP2012 y la tarjeta de desarrollo, el esquema a seguir tomando en cuenta los pines físicos de cada dispositivo es el siguiente:

Figura 23. **Conexión Thinker A7, módulo CP2012 y Raspberry Pi 2B**



Fuente: elaboración propia.

UART (*Universal Asynchronous Reciever-Transmitter*, por sus siglas en inglés) es uno de los protocolos de comunicación serial más popular entre dispositivos y puertos, dicho protocolo posee la facilidad de tener líneas diferentes de comunicación entre transmisión y recepción de información. Para la sincronización entre dispositivos utiliza un bit de inicio y un bit de parada y, comúnmente, 8 bits de información. El transmisor convierte los bytes de información en una secuencia de bits para ser transmitidos hacia el receptor que se encargará de unir la secuencia en bytes de información completos.

Ambos dispositivos, transmisor y receptor, cuentan con un registro de corrimiento, necesario para la conversión entre las formas serial y paralela. La transmisión de datos serial es más eficiente en cuanto a costos y hardware, comparada con la transmisión en paralelo, la cual utiliza una cantidad mayor de conexiones.

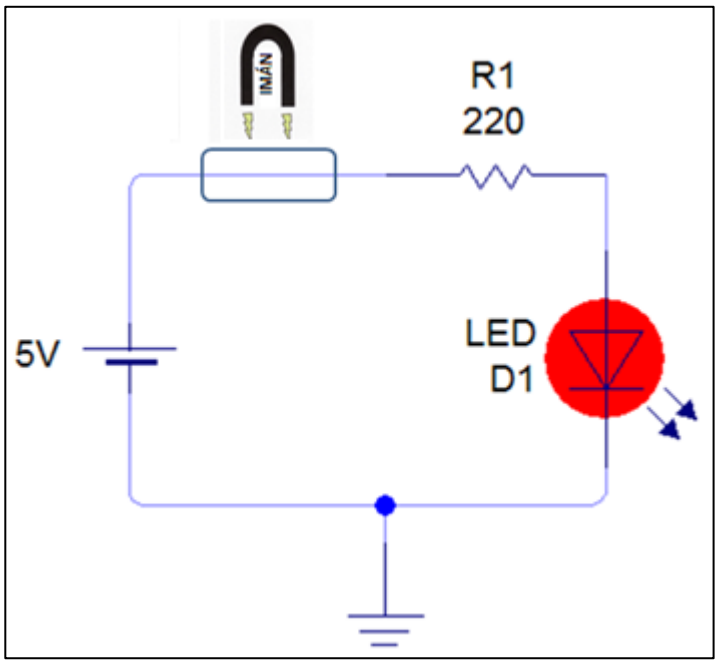
5.1.2. Conexión de interruptor magnético *reed switch*

Este interruptor magnético permite o impide el paso de corriente eléctrica con la unión de sus terminales por medio de un campo magnético generado a partir de un imán. Para este proyecto se utilizó un *reed switch* y no un *switch* convencional, dado que, al momento de cerrar o abrir alguna puerta, un *switch* convencional puede sufrir desperfectos o estropearse de forma grave, ya que estará posicionado en la parte donde la puerta se cierra. Un *reed switch* puede estar fuera de esta parte y únicamente necesita una variación de campo magnético para detectar un movimiento.

En las figuras 24 y 25 se ilustra el método práctico de cómo probar un *reed switch*, ver su correcto uso y comprender cómo es su forma de trabajo.

En la figura 24 el dispositivo está en su estado excitado (en este caso, es un Reed Switch normalmente abierto; esto quiere decir que, mientras exista un campo magnético que lo active, habrá un flujo de corriente en sus terminales). Para la implementación de este proyecto, la figura 24 ilustra el momento en el que la puerta de la residencia está cerrada, quiere decir que el imán está alineado con el *reed switch*, por ende, hay una señal directa hacia la central de alarmas (Raspberry Pi 2b, simbolizada por el diodo emisor de luz, led) y esta se encarga, por medio del software diseñado, de mantener el sistema en equilibrio sin ninguna señal de alarma sonora o visual para el usuario final.

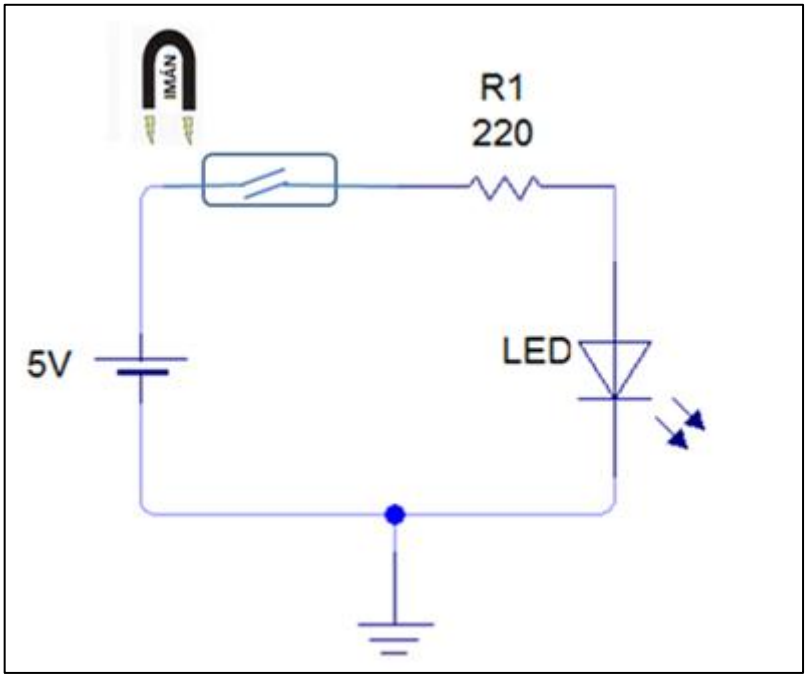
Figura 24. **Diagrama esquemático, prueba de *reed switch* excitado**



Fuente: elaboración propia, empleando Livewire.

Como se aprecia en la figura 25, el dispositivo ha cambiado de estado a normalmente abierto (sus terminales de desalinean y se interrumpe el flujo de corriente), esto es debido a que el imán ha cambiado de posición y su campo magnético ya no es suficiente para mantener al *reed switch* en su estado natural. Aplicado al proyecto, esta situación es cuando la puerta ha sido abierta, el imán fijado en una de las entradas ya no está alineado con el *reed switch* colocado en la puerta de la residencia, debido a esto hay una señal de entrada a la central de alarmas y, trabajando en conjunto con la Raspberry Pi 2B, se da a conocer la situación al usuario final.

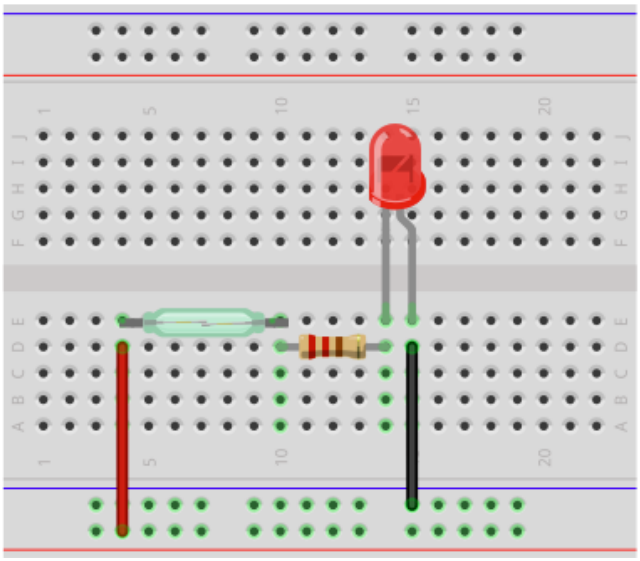
Figura 25. **Diagrama esquemático, prueba de *reed switch* sin excitación**



Fuente: elaboración propia, empleando Livewire.

Para realizar la prueba de funcionamiento del *reed switch*, se debe colocar el circuito mostrado en la figura 26, teniendo en cuenta que, al momento de la implementación en el proyecto, el diodo emisor de luz es cambiado por un pin GPIO de la Raspberry Pi 2B (en este caso, el pin 7).

Figura 26. **Circuito interconectado en galleta de prueba**



Fuente: elaboración propia, empleando Protoboard simulator.

La respuesta de este circuito es la señal de entrada a la central de alarmas del proyecto que, con un software específico para este diseño, notifica al usuario sobre la apertura de la puerta y, mediante el circuito diseñado de la figura 23, la Raspberry Pi 2B recibirá su instrucción por medio de mensaje de texto, o bien, correo electrónico.

5.1.2.1. Conexión de cámaras de vigilancia

Uno de los dispositivos más importantes en la implementación de un sistema de seguridad son las cámaras de vigilancia, ya que, con ellas, se logra una documentación adecuada del lugar al cual se asegurará y, en caso de un asalto, lograr recabar información multimedia, la cual siempre es necesaria para emprender alguna acción legal.

Las cámaras son las encargadas de captar todo lo que ocurre en una vivienda o negocio y ofrecen una calidad de imagen a un precio relativamente bajo. Las cámaras son sin duda alguna una de las mejores opciones en la actualidad para garantizar que una zona o perímetro están siendo vigiladas de forma permanente.

La implementación de una cámara de seguridad es ligeramente sencilla, ya que se debe conectar su puerto USB con el puerto USB de la Raspberry Pi 2B y algunas librerías de programación para lograr tener acceso a imágenes del lugar al cual se requiere vigilar.

5.2. Parámetros necesarios para instalación de sistema de seguridad

En una buena instalación e implementación de un sistema de seguridad, se requieren ciertos parámetros básicos que se deben cubrir para una buena cobertura sin exceder el presupuesto asignado a este. Las consideraciones cubren desde la conexión básica del servicio domiciliar de Internet hasta los parámetros básicos de programación que ayudan a tener el control de sistema de seguridad a distancia. Dichas consideraciones se describen a continuación.

5.2.1. Conexión a internet básica

Es fundamental contar con una conexión a Internet para la implementación de un sistema de seguridad controlado remotamente, ya que, por medio de esta conexión, se logra el acceso a los servidores manejados en el sistema o acceso a las cámaras de vigilancia conectadas a la central de alarmas desde puntos a distancia del mando central.

Cuando se menciona el término conexión se hace referencia a la unión que se establece entre dos o más cosas para que, entre ellas, haya una relación o comunicación. En este sentido, la conexión a Internet realiza un papel fundamental, logrando la comunicación entre la central de alarmas (Raspberry Pi 2B) y el usuario final (por medio de un móvil o una computadora).

Dicha conexión a Internet dependerá de la aplicación que se desea realizar. Para este proyecto, la conexión básica (mínima) para lograr una comunicación viable entre central de alarmas y el usuario final debe ser de 256 kilobit por segundo de subida.

También es necesario contar con un enrutador (*router*) en la residencia o local que se desea asegurar, ya que, por medio de sus puertos Ethernet RJ45 se logra hacer la conexión cableada entre la Raspberry Pi 2B e Internet. Dicha conexión también se puede realizar por medio de Wi-Fi pero se requiere un presupuesto aparte para un módulo de conexión Wi-Fi, el cual se conecta a la Raspberry Pi 2B, para así poder enlazar la placa a Internet. Por motivos de presupuesto, la opción más factible es la conexión vía cable de red.

5.2.2. Conocimiento básico de sentencias de programación

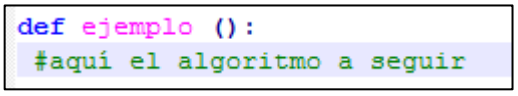
La creación de un software especializado para una tarea asignada debe estar a cargo de una persona que comprenda la necesidad del usuario y sea responsable de dar un seguimiento y mantenimiento correctivo a dicha programación. Para el diseño de cualquier estructura de software es necesario poseer conocimientos de algunas sentencias de programación y algoritmos básicos que permiten el enlace con el exterior.

Para fines de implementación, el software de este proyecto está creado en el lenguaje Python y basta con cambiar el número de teléfono al cual la central de alarmas notificará de algún sucedo inesperado para que el diseño esté funcionando correctamente.

El software creado para este proyecto puede ser utilizado y modificado a conveniencia del usuario. A continuación se da un listado de las sentencias principales, sus definiciones y su modo de programación, tomando en cuenta que únicamente se especifica el concepto de cada sentencia que se utilizó en la implementación del sistema de seguridad, algunas de las instrucciones mencionadas a continuación poseen información robusta en la web pero en este documento se detallará únicamente las instrucciones utilizadas en dicha implementación, tomando en cuenta que un algoritmo es una secuencia de pasos ordenados para llegar a la solución de un problema.

- Definición de funciones: se realiza mediante la instrucción "*def* " más un nombre de función, seguido de paréntesis y finaliza con dos puntos.

Figura 27. **Ejemplo de definición de funciones**



Fuente: elaboración propia, empleando Python.

Una función no se ejecuta si no es invocada o llamada a utilizar, para hacer la invocación de una función simplemente se le llama por su nombre y, para que haga un retorno de datos, pueden asignarse a una variable. En la

siguiente figura se ejemplifica una invocación de función con un retorno utilizando la variable “frase”, la cual se visualizará en la pantalla del ordenador.

Figura 28. **Ejemplo de invocación y retorno de función**

```
def ejemplo():
 return "Sistema seguro"
    frase = ejemplo ()
 print frase
```

Fuente: elaboración propia, empleando Python.

Para el diseño del software utilizado en el sistema de seguridad, algunas definiciones de funciones están ligadas a cierta información que debe recibir, dicha información tiene el nombre de parámetro. Un parámetro es un valor que la función espera recibir cuando sea invocada, a fin de ejecutar acciones con base en ese parámetro recibido. Una función puede esperar uno o más parámetros (que irán separados por una coma) o ninguno.

Figura 29. **Ejemplo de recepción de parámetro**

```
def ejemplo(nombre, apellido):
    nombre_completo = nombre, apellido
 print nombre_completo
```

Fuente: elaboración propia, empleando Python.

- *Try-Except:* sentencias que ayudan a manejar los errores y excepciones del software diseñado, si se encuentra un error o interrupción en el algoritmo, la ejecución del código del bloque de *Try* se detiene y se

transfiere al bloque de *Except*, a continuación se ejemplifica el uso de esta sentencia:

Figura 30. **Estructura de sentencia *Try-Except***

```
try:
    #algoritmo a seguir
except:
    #instrucciones de excepción.
```

Fuente: elaboración propia, empleando Python.

- *If, elif, else:* estas sentencias permiten que un programa ejecute instrucciones cuando se cumple cierta condición y otras instrucciones cuando no se cumple esa condición, pero existen otras condiciones que sí se cumplen. Las tres sentencias, trabajando en conjunto, permiten encadenar varias condiciones a cumplirse para algoritmos que se requieran hacer con esa condición en específico.

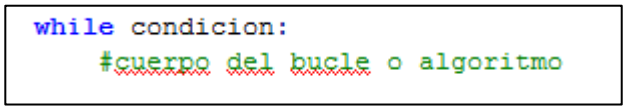
Figura 31. **Estructura de sentencia *if, elif, else***

```
if condición 1:
   #algoritmo 1
elif: condicion 2:
      #algoritmo 2
else:
    #algoritmo 3
```

Fuente: elaboración propia, empleando Python.

- *While:* permite repetir la ejecución de un grupo de instrucciones mientras se cumpla una condición (es decir, mientras la condición tenga el valor *True*). Su estructura se muestra en la figura 32:

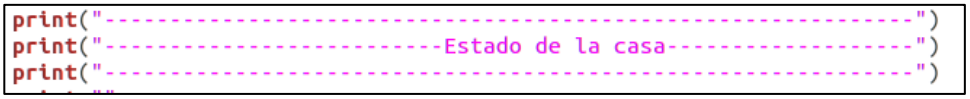
Figura 32. **Estructura de sentencia *while***



Fuente: elaboración propia, empleando Python.

- *Print:* la función *print* permite mostrar texto en pantalla. El texto a mostrar se escribe como argumento y puede ir delimitado tanto en comillas simples como en comillas dobles.

Figura 33. **Estructura de instrucción *print***



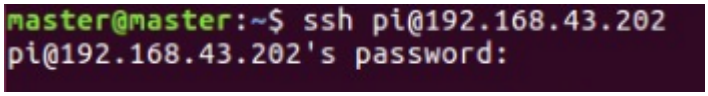
Fuente: elaboración propia.

- Ssh: el protocolo de cubierta segura (Secure Shell, por sus siglas en inglés), permite conectarse, controlar y modificar un equipo de forma remota a través de Internet.

Utilizando el sistema operativo Linux, la conexión ssh se logra a través de la terminal con el código ssh + usuario + @ + host. En este sentido, el usuario puede ser la cuenta a la que se desea acceder y el *host* puede representarse

con una dirección ip asignada. En la figura 34 se ejemplifica una conexión ssh por medio de Linux.

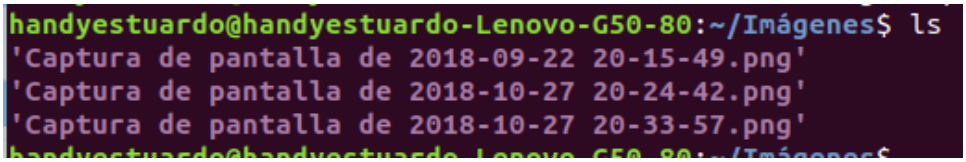
Figura 34. **Conexión ssh por medio de la terminal Linux**



Fuente: elaboración propia.

- Ls: comando de consola que muestra un listado con los archivos y directorios de un determinado directorio. Los resultados se muestran ordenados alfabéticamente.

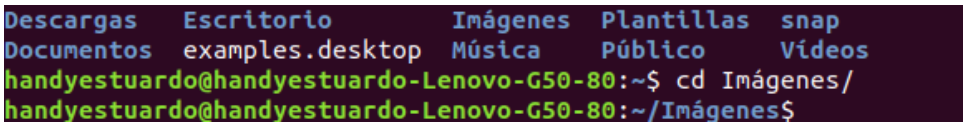
Figura 35. **Comando ls en terminal Linux**



Fuente: elaboración propia.

- Cd: comando de consola básico que permite el cambio entre directorios del sistema. En la siguiente figura se hace el cambio del directorio por defecto que muestra Linux hacia el directorio de “Imágenes” por medio de CD.

Figura 36. **Comando CD en terminal Linux**



Fuente: elaboración propia.

- Sudo: este comando sirve para, con un usuario que posea privilegios y permisos de usuario normal (no administrador), ejecutar ciertos comandos restringidos a otros usuarios, por lo general restringidos al "super usuario" o administrador del sistema, pero sin acceder al sistema con dicha cuenta. Este comando puede ser utilizado de muchas maneras, para este proyecto se utilizó para editar un archivo de texto, o bien, compilar el programa con Python.

Por ejemplo, para instalar un programa desde la terminal Linux utilizando el comando sudo, la estructura del llamado es sudo apt – get install + nombre del programa a instalar.

- Nano: es un editor de texto para la terminal de Linux que, generalmente, viene instalado por defecto. Para editar un archivo con Nano se tiene que ejecutar el comando mostrado en la figura 37:

Figura 37. **Comando nano en terminal Linux**

```
nano nombre_archivo
```

Fuente: elaboración propia.

Donde nombre_archivo será el nombre del archivo que se desee editar. En caso de que el archivo no existiera, se creará un archivo vacío con ese nombre.

- Python: el comando sudo Python se utiliza para compilar un programa escrito en lenguaje Python desde la terminal de Linux. La estructura para hacer el llamado de un programa en Python desde la terminal es sudo Python + nombre del archivo: por ejemplo, en este proyecto se utiliza el llamado sudo Python CódigoC1.py para compilar el programa.

- Apt-get: se utiliza para instalar paquetes desde consola y, en este caso en particular, se utiliza el sufijo *install* para instalar instantáneamente algún paquete por nombre.

5.3. Pasos a seguir para la configuración correcta del sistema de seguridad

A continuación, se muestran los pasos a seguir para configurar de manera correcta el sistema de seguridad.

5.3.1. Ingresar al *router* de la residencia

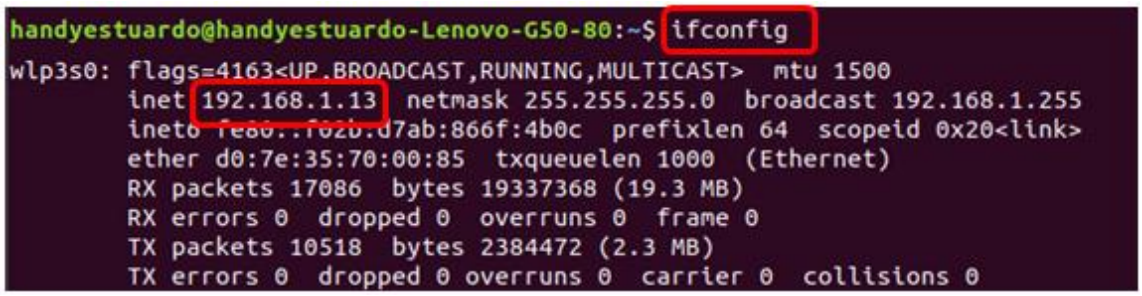
Para empezar a configurar la red donde estará todo el sistema de seguridad, se debe ingresar a las configuraciones del *router* de la residencia y realizar un escaneo de dispositivos para verificar la dirección IP que el enrutador proporcionó a la central de alarmas (Raspberry Pi 2B). Para esto se debe seguir los siguientes pasos:

- Conectar la computadora y la Raspberry Pi 2B a la misma red wifi.

- Ingresar a la terminal de Ubuntu (ctrl+alt+t) e ingresar el comando ifconfig.

- Tomar nota de la dirección IP otorgada a la computadora.

Figura 38. **Verificación de dirección IP de computadora**

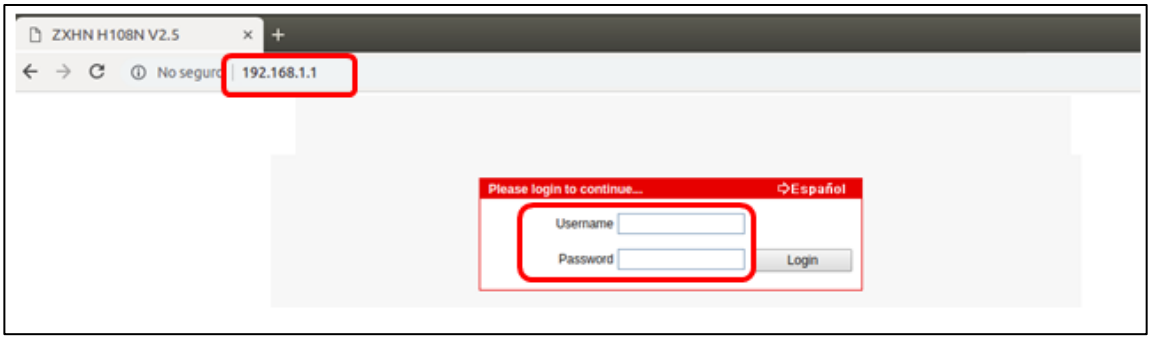


Fuente: elaboración propia.

5.3.2. Ingresar a red de administración

Mediante la información desplegada en la terminal y observando la figura 38, en este caso la dirección IP de la computadora es 192.168.1.13, la red tiene una IP de 192.168.1.1. Con la IP de red se puede acceder al menú de administración del *router* de la residencia desde cualquier navegador web (ver figura 39).

Figura 39. **Ingreso al administrador de la red por medio de navegador web**



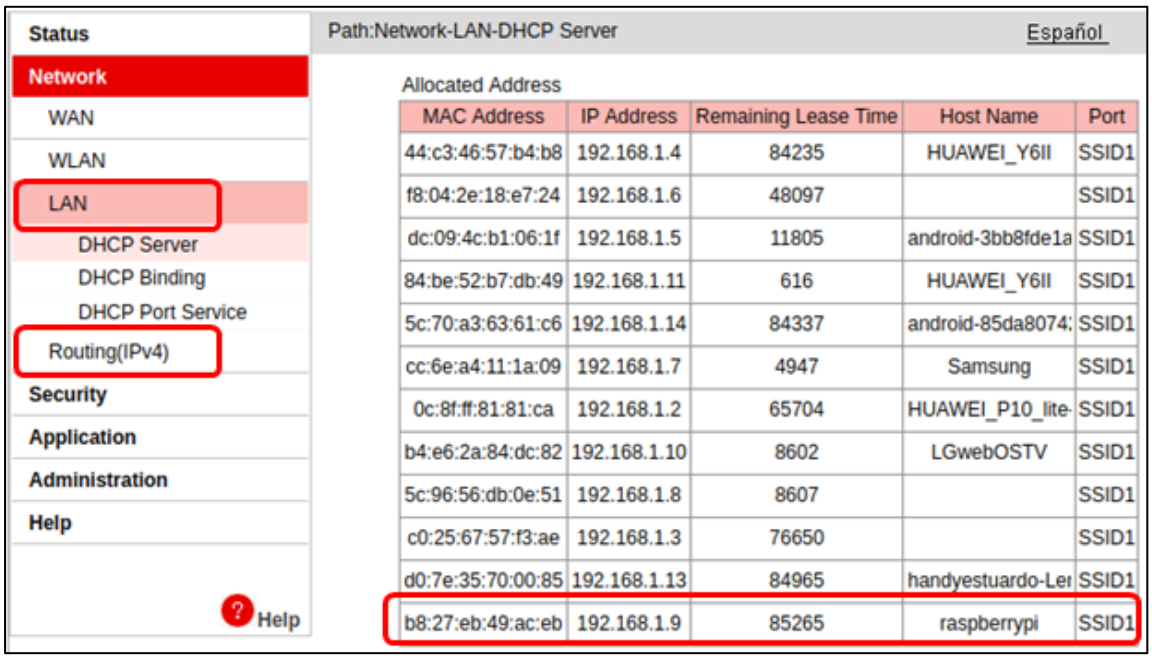
Fuente: elaboración propia.

Ingresando el usuario y contraseña del enrutador se puede tener acceso a toda la información de la red residencial. En este caso se localiza en el menú Network, apartado LAN, la dirección IP que el enrutador asignó a la central de alarmas (Raspberry Pi 2B), en la figura 40 se observa toda la información que el enrutador atribuye a la central de alarmas.

5.3.3. Ingresar al dispostivo Raspberry Pi 2B

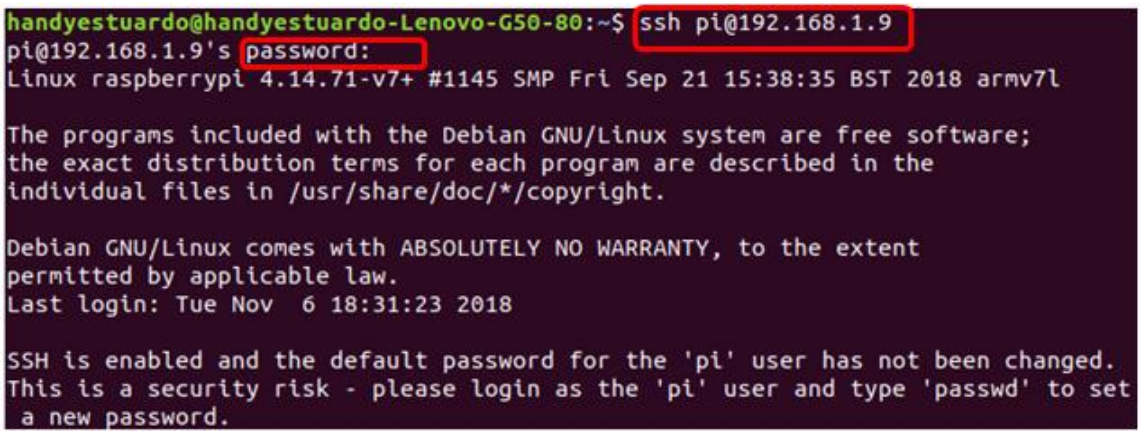
Según la figura 40, la IP de la central de alarmas es 192.168.1.9. Esta dirección IP es volátil y dependerá exclusivamente del servicio automatizado de generación de direcciones IP del *router* para obtenerse la IP asignada a la central de alarmas, esta dirección IP servirá para tener acceso a la Raspberry Pi 2B por medio del protocolo SSH utilizando la configuración propuesta en la FiguraSSH, el comando ssh pi@192.168.1.9 y *password* raspberry como se muestra en la figura 41.

Figura 40. **Obtención de IP dada a Raspberry Pi 2B**



Fuente: elaboración propia.

Figura 41. **Ingreso a memoria de Raspberry Pi 2B por medio de SSH**



Fuente: elaboración propia.

Al acceder al dispositivo, se debe localizar el archivo que tiene el proyecto del sistema de seguridad residencial, para esto se utiliza el comando LS mostrado en la figura 42.

Figura 42. **Lista de archivos guardados en Raspberry Pi 2B**

Fuente: elaboración propia.

El archivo ejecutable del sistema de seguridad se encuentra en la carpeta Proyecto, en la figura 42 se observa dicha carpeta, la cual puede ser abierta mediante el comando CD mostrado en la figura 36. Se logra ver el ejecutable con el comando LS (ver figura 43).

Figura 43. **Apertura de carpeta donde se encuentra el código fuente del proyecto**

Fuente: elaboración propia.

Se debe verificar si la tarjeta Raspberry asignó al adaptador serial CP2012 en el puerto USB0, esto se logra con el comando ls /dev/tty* y observando la figura 44 se confirma que el módulo está en el puerto USB0.

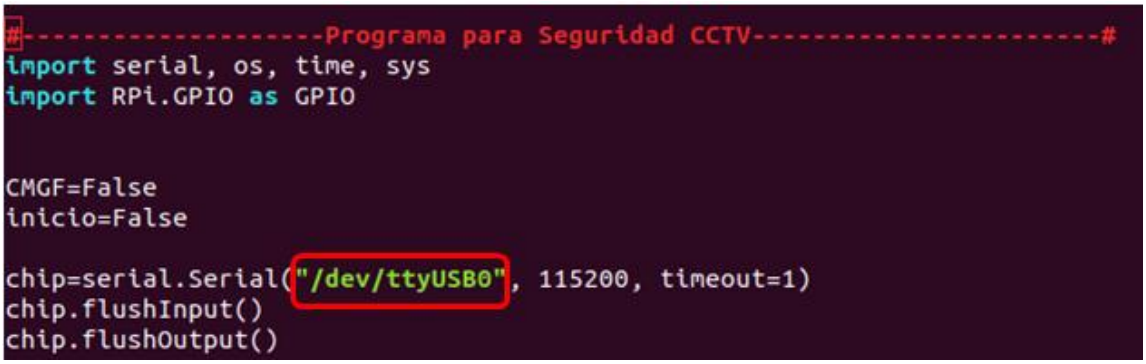
Figura 44. **Verificación de puerto USB para adaptador CP2012**

Fuente: elaboración propia.

Conociendo el archivo que se desea compilar o modificar (el proyecto está en el archivo CodigoC1.py), se hace uso de las instrucciones *sudo nano* o *sudo python* utilizando la estructura de la figura 37, dependiendo de la acción que se quiera realizar.

En caso contrario, si la Raspberry coloca el adaptador serial en algún otro puerto USB, se debe cambiar la sección de la programación mediante el comando en consola sudo nano sms.py y hacer la modificación de USB0 al USB que la Raspberry asignó a dicho módulo, esta modificación se ilustra en la figura 45:

Figura 45. **Verificación o modificación de puerto USB de adaptador CP2012**



Fuente: elaboración propia.

5.3.3.1. Configuración de número telefónico

Para hacer el cambio del número de teléfono al cual la central de alarmas notificará por cualquier incidente, se hace uso de la instrucción SUDO NANO CodigoC1.py y se realiza el cambio en la parte del código designado.

Al estar dentro del archivo CodigoC1.py se desliza el cursor hasta la definición Enviar Alerta, dentro de dicha definición se logra configurar el número de teléfono al cual la central de alarmas enviará el mensaje de alerta, nótese que el número de teléfono debe ir acompañado del prefijo del país donde se encuentra.

Figura 46. **Cambio de número telefónico en código Python**

Fuente: elaboración propia, empleando Python.

Después de hacer el cambio de número de teléfono se presiona ctrl + x para salir y Y (Yes) para guardar los cambios.

5.3.3.2. Configuración de correo electrónico

La configuración del correo electrónico se realiza después de instalar algunos paquetes adicionales con el comando apt-get install dentro de la Raspberry Pi 2B y crear una cuenta en cualquier servidor de correos en Internet (en este caso el correo es seguridadresidencialtesis@gmail.com, es decir, es un correo en el dominio Gmail.com).

SMTP o protocolo simple de transferencia de correo (siglas en inglés de Simple Mail Transfer Protocol), es un protocolo básico que permite el envío de correos electrónicos a través de Internet, es decir, permite enviar *email* de un servidor de origen a un servidor de destino.

Para dicha configuración, se deben seguir los siguientes pasos:

- Ingresar la instrucción sudo apt-get install ssmtp, luego dar *enter.*

- Ingresar la instrucción sudo apt-get install mailutils, luego dar *enter.*

- Ingresar la instrucción sudo nano /etc/ssmtp/ssmtp.conf y a continuación editar el archivo que se abrió con las siguientes sentencias.

  root=Seguridad Residencial Tesis
  mailhub=smtp.gmail.com:587
  hostname=raspberrypi
  AuthUser=seguridadresidencialtesis@gmail.com
  AuthPass=contraseña del correo electrónico creado.
  FromLineOverride=YES
  UseSTARTTLS=YES

- echo 'La puerta ha sido abierta en este momento' | mail -s 'Alerta de Seguridad' (correo electrónico del usuario, omitir los paréntesis).

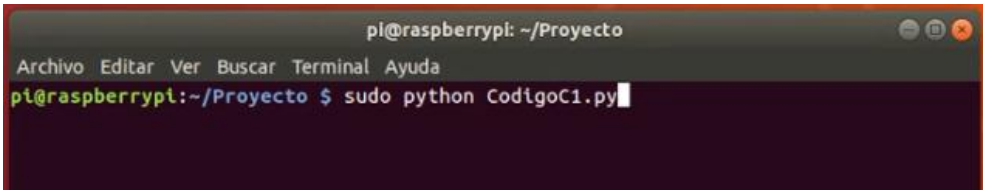
- Salir del documento editado y guardar los cambios.

Con todas las verificaciones exitosas, se hace la compilación del proyecto mediante el comando sudo python CodigoC1.py

5.4. Compilación y manejo de sistema de seguridad

Después de realizar las configuraciones del teléfono, correo y número de puerto USB asignado a la central de alarmas, se procede a la compilación del código fuente del sistema de seguridad. Como se mencionó antes, dicho código está elaborado en lenguaje Python y con la facilidad de funcionamiento óptico únicamente cambiando 3 de los parámetros antes escritos.

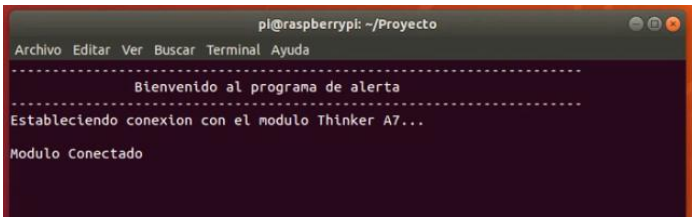
Figura 47. **Instrucción sudo Python para compilación de proyecto**



Fuente: elaboración propia.

Al compilar el proyecto, se realiza automáticamente la conexión de la central de alarmas con el módulo a cargo de avisos al usuario Thinker A7. Si el módulo está configurado y conectado correctamente, el sistema realiza el aviso al usuario con el mensaje módulo conectado.

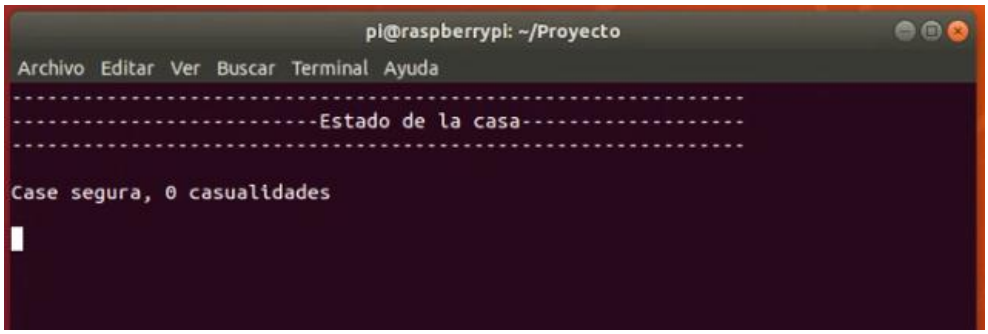
Figura 48. **Estableciendo conexión con módulo GSM/GPRS**



Fuente: elaboración propia.

Si el proyecto ha sido compilado con éxito, el programa despliega un mensaje de 'Case segura, 0 casualidades', el cual significa que la residencia está segura y no se han abierto puertas ni hay alguna alarma activada (estos mensajes pueden ser editados a criterio del usuario desde el código fuente mediante la instrucción sudo nano vista en la figura 43).

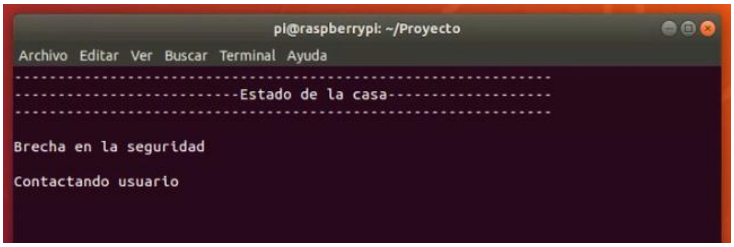
Figura 49. **Estado normal de la residencia**



Fuente: elaboración propia.

Si, por medio del interruptor magnético, la central de alarmas detecta que la puerta ha sido abierta sin autorización, el sistema de seguridad hace contacto con el usuario y espera una respuesta.

Figura 50. **Brecha en la seguridad de la residencia**



Fuente: elaboración propia.

El número telefónico configurado recibirá un mensaje de texto proveniente de la central de alarmas, el cual, en el cuerpo del mensaje, notifica a la persona que su residencia ha sido abierta sin autorización, el código fuente de la central de alarmas tiene 3 opciones configuradas para la toma de decisiones:

- Opción 1: enviar “1” para activar una alarma sonora
- Opción 2: enviar “2” para desactivar la alarma sonora
- Opción 3: enviar “3” para enviar un correo electrónico

Figura 51. **Envío de mensaje de texto al usuario y espera de instrucciones**

Fuente: elaboración propia.

Figura 52. **Mensaje enviado por central de alarmas**

Fuente: elaboración propia.

Si el usuario envía “1” como respuesta, la central de alarmas envía una instrucción que permite encender una alarma sonora para alertar a los vecinos de que la casa ha sido abierta, la alarma debe ser lo más sonora posible para este propósito.

Figura 53. **Activación de alarma sonora**

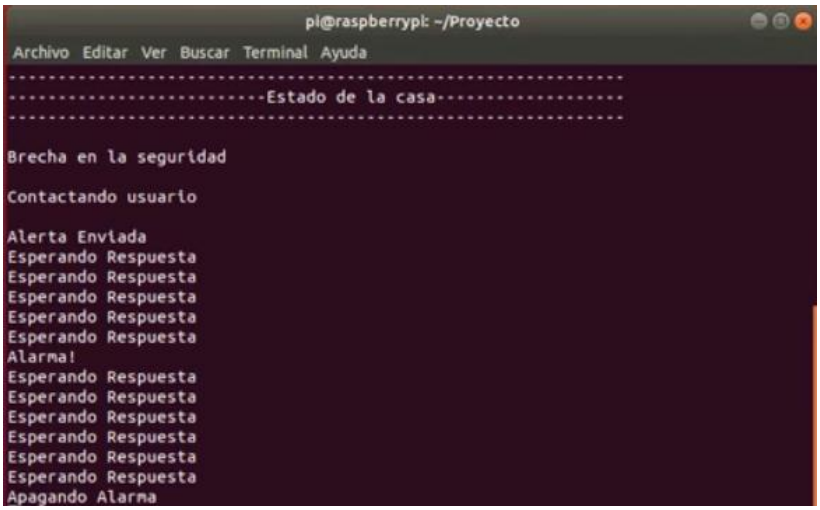
Fuente: elaboración propia.

Para desactivar la alarma, el usuario debe enviar el número “2” en el mismo mensaje que respondió anteriormente.

Figura 54. **Envío de mensaje hacia central de alarmas para desactivar alarma**

Fuente: elaboración propia.

Figura 55. **Desactivación de alarma sonora**



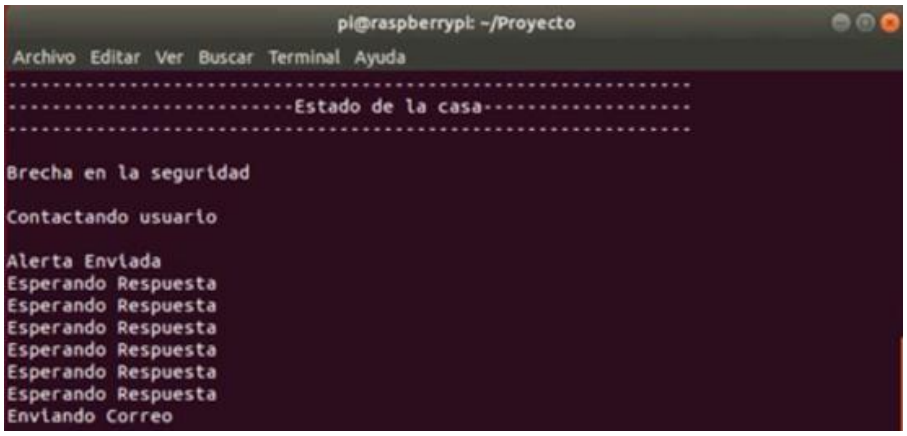
Fuente: elaboración propia.

En caso de que la central de alarma reciba un “3” como instrucción, esta enviará un correo electrónico al correo configurado anteriormente.

Figura 56. **Mensaje hacia central de alarmas para enviar correo electrónico**

Fuente: elaboración propia.

Figura 57. **Envío de correo desde central de alarma**



Fuente: elaboración propia.

Figura 58. **Recepción de correo electrónico de central de alarma a correo configurado**

Fuente: elaboración propia.

Cabe destacar que, por motivos de ejemplo, únicamente se envía 'La puerta ha sido abierta en este momento', pero en este correo puede ir adjunto desde una serie de fotos hasta videos, dependiendo de la programación utilizada. Cabe resaltar que la hora de ingreso del correo ayuda a mantener un registro de incidentes ocurridos y suma pruebas contundentes en caso se requiera una denuncia policial.

5.5. Instalación del sistema de seguridad en la residencia

La ubicación de los dispositivos utilizados en el proyecto está a discreción del usuario y depende de las instalaciones del lugar a proteger, sin embargo, siguiendo el objetivo de establecer parámetros en hardware para la instalación correcta y de bajo costo de un sistema de seguridad, a continuación se realiza el montaje más básico pero funcional de dicho sistema.

5.5.1. Instalación de imán

El imán a utilizar puede ser un imán convencional (utilizado en el proyecto) o un imán de neodimio, ambos cumplen con el funcionamiento necesario para el sistema de seguridad. La única diferencia es que, con el imán de neodimio, se logra una distancia mayor de apertura entre la puerta y el Reed Switch.

La utilización de cinta de doble contacto para adherir el imán a la puerta puede ser opcional, se utilizó en la instalación ya que la puerta es de madera y se necesita un imán fijado en ella.

Figura 59. **Imán utilizado en la instalación**

Fuente: elaboración propia.

5.5.2. Instalación de interruptor magnético Reed Switch

Figura 60. **Imán y Reed Switch en posición adecuada**

Fuente: elaboración propia.

El interruptor magnético puede estar a unos centímetros del imán y funcionar correctamente, entre más fuerte sea el campo magnético generado por el imán, más grande será la distancia en centímetros de separación que se logra obtener entre los 2 dispositivos. En este caso, la distancia debe ser pequeña, esto con el objetivo de detectar un cambio de estado de la puerta con mayor facilidad.

5.5.3. Instalación de cámara de seguridad

Figura 61. **Cámara de seguridad instalada**

Fuente: elaboración propia.

La cámara de seguridad debe estar posicionada en un lugar que permita captar con claridad la apertura de la puerta.

Figura 62. **Capturas de cámara de seguridad**

Fuente: elaboración propia.

5.5.4. Instalación de alarma

Dependiendo de qué alarma se utilice en la instalación así será el punto de localización de la misma. En este caso, la alarma es sonora, puede instalarse en cualquier punto de la residencia en el cual la alarma sea totalmente audible para vecinos o alguna persona alrededor de la casa a proteger.

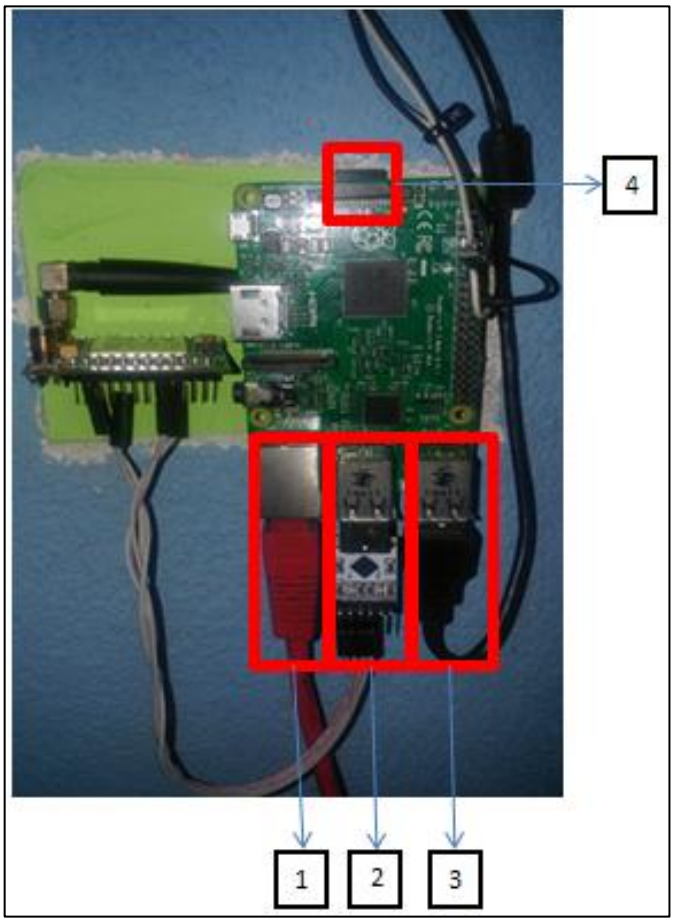
Figura 63. **Instalación de alarma sonora**

Fuente: elaboración propia.

5.5.5. Instalación de central de alarmas y módulo GSM/GPRS

La instalación de la central de alarmas (Raspberry Pi 2B) y el módulo GSM/GPRS debe realizarse con base en el inciso 5.1.1.1, la instalación e interconexión de todos los dispositivos es vital para el funcionamiento adecuado del sistema de seguridad. A continuación se muestra la forma adecuada para la instalación de los mismos.

Figura 64. **Instalación de central de alarmas**

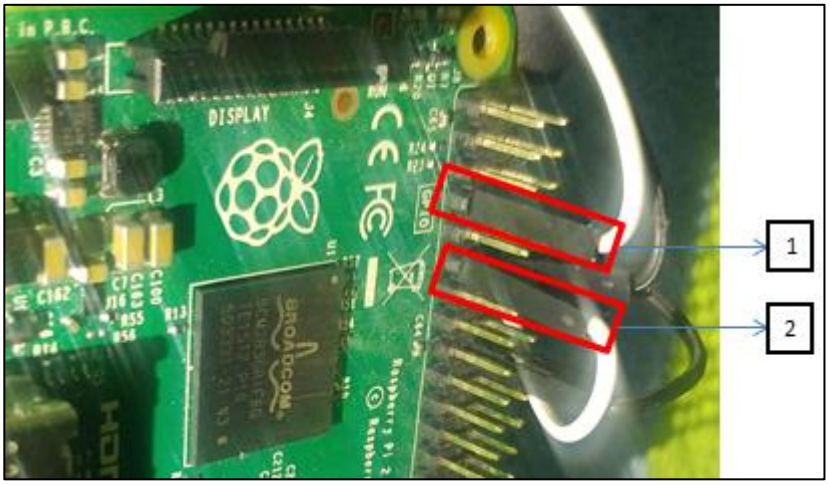


Fuente: elaboración propia.

Donde:

- Puerto Ethernet RJ45 (conexión con *router* residencial)
- Puerto USB para CP2012 (comunicación con módulo Thinker A7)
- Puerto USB para cámara web
- Ranura SD para memoria

Figura 65. **Conexión de señal de entrada de Reed Switch y señal de salida a alarma sonora**

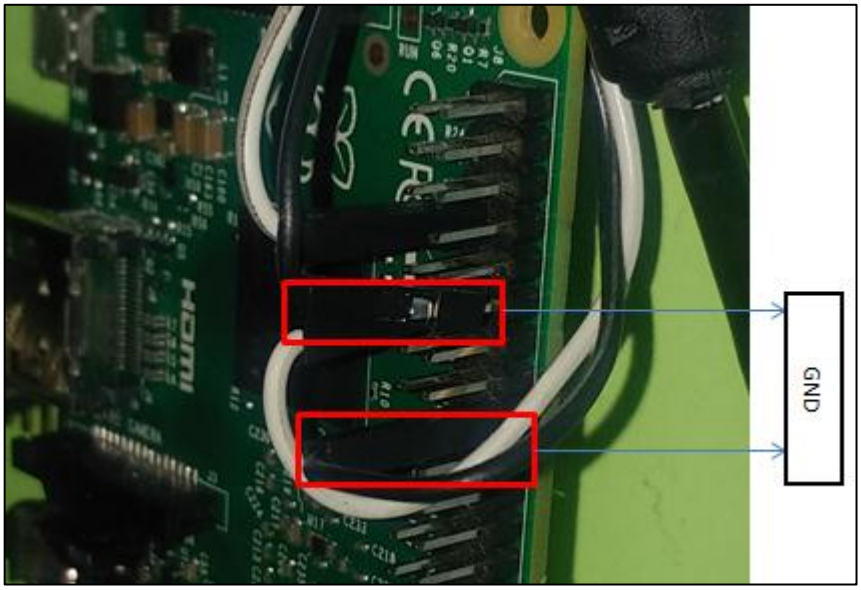


Fuente: elaboración propia.

Donde:

- Pin 7 de propósito general (entrada de señal del Reed Switch)
- Pin 11 de propósito general (salida de señal para sistema de aviso)

Figura 66. **Pines para GND del interruptor magnético y alarma sonora**



Fuente: elaboración propia.

CONCLUSIONES

1. El diseño de un sistema funcional de seguridad controlado a distancia con dispositivos de bajo presupuesto es viable contando con los conocimientos necesarios para la implementación adecuada del mismo.

2. El sistema de seguridad de bajo costo es rentable en la industria debido a sus parámetros básicos de instalación y su bajo costo de implementación (Q 875,00), comparado con sistemas de seguridad empleados por empresas privadas (un mínimo de Q 1 899,00), representando un gran aporte a la seguridad y tranquilidad de una residencia.

3. La tarjeta de desarrollo Raspberry Pi 2B permite la implementación de sistemas de alto desempeño para realizar tareas de optimización y automatización de procesos remotos, apoyada por tecnología de bajo costo por medio de un análisis previo.

4. Se trabajó, en conjunto con la práctica, un documento para la implementación del proyecto, el cual es accesible para todos los interesados en adquirirlo, de modo que personas que tengan conocimientos básicos en electrónica digital, puedan comprender la teoría detrás de la implementación del sistema de seguridad y ejecutar el proyecto sin ningún percance. Tanto el documento escrito en formato portable (PDF) como el video explicativo del proyecto están a disposición de cualquier individuo interesado en la implementación del proyecto y sin costo alguno.

5. Se logró realizar el diseño de un sistema de seguridad contando con un presupuesto bajo comparado con los costos de instituciones privadas que prestan este servicio. Incrementando el intervalo de presupuesto asignado al proyecto se puede lograr mayor cobertura y mayor automatización de procesos de la residencia.

RECOMENDACIONES

1. La persona que desee implementar el sistema de seguridad debe verificar que la red residencial cuente con un *router* con entradas LAN y asegurarse que los adaptadores de voltaje de cada dispositivo entreguen la corriente necesaria para cada uno.

2. Para el correcto funcionamiento y aplicación del Reed Switch, este dispositivo debe estar situado en un lugar con poca humedad y con una distancia de separación no mayor a 2 centímetros del imán que excita sus terminales.

3. Instalar la central de alarmas a una altura accesible para todos.

4. Para una mejor cobertura de la residencia, se deben colocar al menos 2 sensores más en puertas o ventanas y así cubrir la mayor área posible de la casa.

5. El diseño del sistema es básico y de gran funcionamiento, sin embargo, se recomienda el uso de más dispositivos de alto nivel y de bajo costo para mayor control y automatización de la residencia.

6. Para posibles cortes de luz eléctrica, se recomienda colocar una batería independiente a la alimentación del proyecto para que, en ausencia de energía eléctrica, el sistema de seguridad siga funcionando correctamente.

BIBLIOGRAFÍA

1. ARG. *Entrenamiento técnico de módulo GSM.* [en línea]. <https://www.argseguridad.com/admin/archivos/GSM-GPRS%20LightSYS.pdf >. [Consulta: 20 de agosto de 2018].

2. Blogspot. *Área de transparencia GAM de la policía para robos*. [en línea]. <https://areadetransparencia.blogspot.com/2014/02/informe-de-delitos-contra-el-patrimonio.html?q=asaltos>. [Consulta: 20 de julio de 2018].

3. Índex. *Indicadores para la delincuencia de guate (homicios, extorsiones etc)*. [en línea]. <http://www.cien.org.gt/index.php/indicadores-de-seguridad-3/>. [Consulta: 20 de julio de 2018].

4. INE. *Canasta básica guatemalteca*. [en línea]. <https://www.ine.gob.gt/sistema/uploads/2018/07/09/20180709124641T0C5gBHEg4aVBxzX33KukVcyO6shFKlo.pdf>. [Consulta: 26 de julio de 2018].

5. Nobbot. *Herramientas para el control de un sistema remotamente.* [en línea]. <https://www.nobbot.com/redes/las-mejores-8-herramientas-para-conectar-en-remoto-otro-ordenador-y-tomar-el-control/>. [Consulta: 3 de agosto de 2018].

6. Rohde. *Principios básicos de GSM-GPRS.* [en línea]. <https://www.rohde-schwarz.com/es/soluciones/test-and-

measurement/wireless-communication/gsm-gprs-edge-evolution-vamos/fundamentos/ prin cipios-basicos-de-gsm_106328.html>. [Consulta: 17 de agosto de 2018].

7. Prometec. *Módulo GSM/GPRS: llamar y enviar SMS.* [en línea]. <https://www.prometec.net/gprs-llamar-enviar-sms/>. [Consulta: 17 de agosto de 2018].

8. Tecnopro. *Medidas de prevención contra hurtos para comercios y negocios.* [en línea]. <http://www.tecnopro.mx/2017/ 05/14/medi das-de-prevencion-contra-hurtos-para-comercios-y-negocios/>. [Consulta: 27 de julio de 2018].

APÉNDICES

Apéndice 1. **Vídeo de gestión del sistema**

A continuación, se muestra el link de acceso a material audiovisual para la gestión del sistema de seguridad.

Fuente: https://www.youtube.com/watch?v=boZmyh7PN4E&t=

Fuente: elaboración propia.

Apéndice 2. **Programa propuesto**

A continuación, se muestra la programación propuesta para la realización de un sistema de seguridad de bajo costo. Dichos códigos pueden ser modificados, utilizados, mejorados y distribuidos gratuitamente por las personas que deseen hacerlo.

En el código 1 se muestran las configuraciones iniciales para el sistema de seguridad. En este se realiza la configuración del puerto serial, velocidad en baudios y configuraciones de entrada/salida de pines de propósito general.

Continuación del apéndice 2.

Figura A. **Código 1: configuraciones iniciales**

```
#--------------------Programa para Seguridad----------------------#
import serial, os, time, sys
import RPi.GPIO as GPIO


CMGF=False
inicio=False

chip=serial.Serial("/dev/ttyUSB0", 115200, timeout=1)
chip.flushInput()
chip.flushOutput()

GPIO.setmode(GPIO.BOARD)
GPIO.setup(7, GPIO.IN)
GPIO.setup(11, GPIO.OUT)
```

En el código 2 se observa las funciones de control para el módulo Thinker A7. En estas se remueve el ruido proveniente de la comunicación entre la central de alarmas y el usuario.

Figura B. **Código 2: funciones de control del módulo Thinker A7**

```
#-------------Funciones de control del Thinker A7----------------------#
#Envio de comandos#
def EnviarComando(SCommand):
    chip.write((str(SCommand)+ "\r\n").encode())
    CRespuesta = chip.read(128)
    CRespuesta = str(CRespuesta).replace("\\r\\n","\n")
    CRespuesta = CRespuesta.replace("\'", "")
    CRespuesta = CRespuesta.replace("\\x00","")
    CRespuesta = CRespuesta.replace("\n","")
    Resultado = CRespuesta.split("\r")
    Resultado.remove('')
    try:
        Respuesta=Resultado
#       print Respuesta
        return Respuesta
    except IndexError:
        return 0
    except ValueError:
        return 0
```

Continuación del apéndice 2.

En el código 3 se muestra la selección del modo de operación para el módulo Thinker A7. En este caso se utilizó con el modo de mensaje de texto.

Figura C. **Código 3: selección de modo de operación para Thinker A7**

```
#Seleccionar modo de operacion"
#0- SMS PDU
#1- SMS Text
def Operacion(state):
    global CMGF
    if CMGF != state:
        if state==True:
            EnviarComando("AT+CMGF=1")
            CMGF=True
        else:
            EnviarComando("AT+CMGF=0")
            CMGF=False
```

En el código 4 se envía la señal de alerta al usuario. En este se realiza la configuración del número de teléfono al cual la central de alarmas enviará el mensaje de texto escrito en la instrucción “mensaje”. El número de teléfono debe ir acompañado por el prefijo de cada país.

Figura D. **Código 4: envío de mensaje de texto**

```
#Enviar Alerta de brecha en seguridad#
def EnviarAlerta():
    Operacion(True)
    numero="+50241548575"
    mensaje="Alerta: La puerta principal ha sido abierta. "
    RChip=EnviarComando("AT+CMGS=\"{0}\"".format(numero))
    time.sleep(0.5)
    EnviarComando("{}".format(mensaje) + chr(26))
    time.sleep(3)
    print "Alerta Enviada"
```

Continuación del apéndice 2.

En el código 5 se realiza la lectura del mensaje de texto recibido por la central de alarmas. Dependiendo de la opción que el usuario seleccionó al momento de enviar el mensaje, así será la acción a realizar por parte de la central de alarmas.

Figura E. **Código 5: lectura de mensaje de texto**

```
#Lectura de Mensajes SMS Recibidos#
def Accion():
    while True:
        Operacion(True)
        time.sleep(0.5)
        Accion=EnviarComando("AT+CMGR=1")
        time.sleep(2)
        if Accion[2]=="1":
            print "Alarma!"
            Alerta()
        elif Accion[2]=="2":
            print "Apagando Alarma"
            GPIO.output(11, False)
            time.sleep(10)
            EnviarComando("AT+CMGD=1")
            break
        elif Accion[2]=="3":
            print "Enviando Correo"
            j=os.system('sudo echo "La puerta ha sido abierta en este momento" | mail -s "Alerta de Seguridad"
            handymorales2@gmail.com')
            time.sleep(10)
            EnviarComando("AT+CMGD=1")
        else:
            print "Esperando Respuesta"
        #   EnviarComando("AT+CMGD=1")
```

En el código 6 se realiza la activación de la alarma sonora. Se coloca el pin 11 de la Raspberry Pi 2B en alto (en 5V). En este pin puede ir conectada una señal visual o sonora, esto será dependiendo de la necesidad del usuario y se realiza de la misma manera si se requiere colocar 2 o más señales al mismo tiempo, simplemente se cambia el pin a utilizar.

Continuación del apéndice 2.

Figura F. **Código 6: activación de alarma**

```
def Alerta():
    GPIO.output(11, True)
    time.sleep(5)
    EnviarComando("AT+CMGD=1")
    return
```

En el código 7 se muestra la programación para verificar si el módulo Thinker A7 está respondiendo de manera adecuada. Si el módulo tiene una conexión estable y responde al llamado del programa, despliega un mensaje de “módulo conectado”.

Figura G. **Código 7: verificación de conexión a módulo Thinker A7**

```
#Funcion para verificar si el Thinker esta disponible#
def Inicializacion():
    os.system('clear')
    print ("------------------------------------------------------------------------")
    print ("               Bienvenido al programa de alerta                         ")
    print ("------------------------------------------------------------------------")
    print ("Estableciendo conexion con el modulo Thinker A7...")
    print (" ")
    prueba=EnviarComando("AT")
    if prueba[1]=="OK":
        print "Modulo Conectado"
        time.sleep(1)
        print ""
        EnviarComando("ATE1")
        time.sleep(0.5)
        EnviarComando("AT+CNMI=1,1,0,0,0")
        time.sleep(0.5)
        EnviarComando('AT+CPMS="SM"')
        time.sleep(0.5)
        EnviarComando('AT+CPMS="SM","SM","SM"')
        return True
    else:
        print "Error al conectar con el modulo"
        print ""
        print "Intentando de nuevo en 5.0 segundos"
        print ""
        time.sleep(5)
        return False
```

Continuación del apéndice 2.

En el código 8 se realiza la verificación del estado de la puerta en la cual está instalado el sensor Reed Switch y el imán. En este proyecto únicamente se colocó un sensor, sin embargo, se pueden colocar el número de sensores que el usuario requiera para la seguridad necesaria de su residencia. Únicamente se deben colocar más pines como entrada de la central de alarmas.

Figura H. **Código 8: verificación de estado de la puerta**

```
#Funcion para verificar puerta
def EstadoPuerta():
    Estado=GPIO.input(7)
    return Estado
```

En el código 9 se muestra el estado del sistema, el cual dependerá de la lectura del sensor Reed Switch instalado en la puerta de la residencia. Si la puerta ha sido abierta, el sistema ingresa a la acción de “enviar alarma” (código 6) y notifica al usuario del estado actual del sistema.

Figura I. **Código 9: estado actual del sistema**

```
try:
    while inicio==False:
        inicio=Inicializacion()
    os.system('clear')
    while True:
        puerta=EstadoPuerta()
        os.system('clear')
        print("------------------------------------------------------------")
        print("-------------------------Estado de la casa------------------")
        print("------------------------------------------------------------")
        print ""
        if(puerta==1):
            print "Case segura, 0 casualidades"
            print ""
            time.sleep(1)
        else:
            print "Brecha en la seguridad"
            print ""
            print "Contactando usuario"
            print ""
            time.sleep(1)
            EnviarAlerta()
            Accion()
```

Continuación del apéndice 2.

A continuación se detalla una tabla de pines, tanto de la Raspberry Pi modelo 2B como del módulo GSM/GPRS Thinker A7, donde se puede observar a qué número de pin externo equivale cada pin interno y su funcionalidad, considerando las siguientes siglas designadas para los nombres en los pines:

- SDA: Serial Data (datos seriales).
- SCL: Serial Clock I2C (reloj serial).
- SCLK: Serial Clock SPI (reloj serial).
- CE: Chip Enable (habilitación de integrado).
- MISO: Master Input-Slave Output (entrada de datos del maestro y salida de datos del esclavo).
- MOSI: Master Output-Slave Input (salida de datos del maestro y entrada de datos del esclavo).
- TxD: Transmisor UART.
- RxD: Receptor UART.
- GND: Siglas en inglés de Ground, es la tierra común dentro de algún dispositivo electrónico.

Continuación del apéndice 2.

Tabla A. **Pines de Raspberry Pi 2B**

Número de pin	Nombre de pin	Funcionalidad
1	VDC	Pin de alimentación 3.3 voltios.
2	VDC	pin de alimentación de 5v
3	GPIO8/I2C	GPIO8/Pin de datos del bus I2C
4	VDC	pin de alimentación de 5v
5	GPIO9/2C	GPIO9/Pin de reloj del bus I2C
6	GND	GND
7	GPIO7/GPCLK0	GPIO7
8	GPIO15/UART_TXD	GPIO15/ pin de transmisión UART
9	GND	GND
10	GPIO16/UART_RXD	GPIO16/ pin de recepción UART
11	GPIO0	GPIO0
12	GPIO1/PCM_CLK/PWM0	GPIO1/ Salida de PWM0
13	GPIO2	GPIO2/
14	GND	GND
15	GPIO3	GPIO3
16	GPIO4	GPIO4
17	VDC	Pin de alimentación 3.3 voltios
18	GPIO5	GPIO5
19	GPIO12/MOSI_SPI	GPIO12/Pin MOSI de protoclo SPI
20	GND	GND
21	GPIO13/MISO_SPI	GPIO13/Pin MISO de protocolo SPI
22	GPIO6	GPIO6
23	GPIO14/SCLK_SPI	GPIO14/Pin de reloj en protocolo SPI
24	GPIO10/CE0_SPI	GPIO10/Pin de selección 1 en protocolo SPI
25	GND	GND
26	GPIO11/CE1_SPI	GPIO11/Pin de selección 2 de modo en protocolo SPI
27	SDA0/I2C_EEPROM	Pin reservado para la comunicación i2c con EEPROM
28	SLC0_I2C_EEPROM	Pin reservado para la comunicación i2c con EEPROM
29	GPIO21/GPCLK1	GPIO21/Reloj de propósito general.
30	GND	GND
31	GPIO22/GPCLK2	GPIO22/Reloj de propósito general.
32	GPIO26/PWM0	GPIO26/Salida de PWM0
33	GPIO23/PWM1	GPIO23/Salida de PWM1
34	GND	GND
35	GPIO24/PCM_FS/PWM1	GPIO24/Fase de modulación PCM
36	GPIO27	GPIO27
37	GPIO25	GPIO25
38	GPIO28/PCM_DIN	GPIO28/Dato entrante para modulación PCM
39	GND	GND
40	GPIO29/PCM_DOUT	GPIO29/Dato saliente para modulación PCM

Continuación del apéndice 2.

Tabla B. **Pines del módulo A7**

Número de Pin	Nombre de Pin	Funcionalidad
1	No Conectado	No Conectado
2	No Conectado	No Conectado
3	No Conectado	No Conectado hardware para GPIO16
4	No Conectado	No Conectado hardware para GPIO15
5	No Conectado	No Conectado hardware para GPIO14
6	No Conectado	No Conectado hardware para GPIO6
7	No Conectado	No Conectado, hardware para GPIO3
8	PWR_KEY	Botón de encendido, mayor a 1.9V con 2 segundos para arrancar.
9	GPIO1/INT	Usado para controlar el módulo e ingresar a modo de bajo consumo, alto nivel de salida bajo acceder, en este modo. (En este modo, el puerto serial no se puede usar)
10	UART_CTS/GPIO5	Pin UART_CTS
11	UART_RTS/GPIO7	Pin UART_RTS
12	RST	Pin de reseteo para el modulo, este pin usándolo en bajo nivel (menor a 0.05V), la corriente es de 70ma, se recomienda usar el control NMOS.
13	GND	GND
14	SIM_RST	Pin de reset de tarjeta SIM
15	SIM_CLK	Pin del reloj de tarjeta SIM
16	VSIM	Pin de encendido/apagado de tarjeta SIM
17	SIM_DATA	Pin de datos de tarjeta SIM
18	GND	GND
19	MIC-	Pin negativo de micrófono de tarjeta SIM
20	MIC+	Pin positivo de micrófono de tarjeta SIM
21	MIC2_P	Interfaz de micrófono para auriculares
22	GND	GND
23	EAR_L	Pin de auriculares izquierdo
24	EAR_R	Pin de auriculares derecho
25	GND	GND
26	REC+	Pin positivo de bocina
27	REC-	Pin negativo de bocina
28	GND	GND
29	VDD_1V8_OUT	Pin de voltaje externo a 1.8 voltios.
30	UART_TXD	Pin de transmisión UART a 2.8 voltios.
31	UART_RXD	Pin de recepción UART a 2.8 voltios.
32	HST_RXD	Pin de descarga del puerto receptor serial
33	HST_TXD	Pin de descarga del puerto transmisor serial
34	GND	GND
35	GSM_RF	Pin de antena
36	GND	GND
37	No Conectado	No Conectado
38	No Conectado	No Conectado
39	GND	GND
40	GND	GND
41	VBAT	Batería de voltaje externo con rango de 3.5 a 4.2 voltios con corriente de 2 amperios.
42	VBAT	

Fuente: elaboración propia.