UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

CARRERA DE INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo
a la obtención del título
de Ingeniero Electrónico

PROYECTO TÉCNICO CON ENFOQUE SOCIAL

DESARROLLO E IMPLEMENTACIÓN DE UN PROTOTIPO-INTERFAZ PARA COMUNICACIÓN DE PROTOCOLO CONTACT-ID CON UN SISTEMA DE GESTIÓN IP, APLICADO A DISPOSITIVOS DE SEGURIDAD RESIDENCIAL

AUTORES:

ALEX FABIAN YUNGA MUYULEMA

ELVIS GEOVANNY ZARUMA QUITUIZACA

TUTOR:

ING. JUAN DIEGO JARA, MgT.

CUENCA – ECUADOR

2019

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Alex Fabian Yunga Muyulema con documento de identificación N° 060367099 y Elvis Geovanny Zaruma Quituizaca con documento de identificación N° 0105803720, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación: **DESARROLLO E IMPLEMENTACIÓN DE UN PROTOTIPO-INTERFAZ PARA COMUNICACIÓN DE PROTOCOLO CONTACT-ID CON UN SISTEMA DE GESTIÓN IP, APLICADO A DISPOSITIVOS DE SEGURIDAD RESIDENCIAL**, mismo que ha sido desarrollado para optar por el título de: *Ingeniero Electrónico*, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Cuenca, marzo del 2019

Alex Fabian Yunga Muyulema
CI: 0603676099

Elvis Geovanny Zaruma Quituizaca
CI: 0105803720

CERTIFICACIÓN

Yo declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: **DESARROLLO E IMPLEMENTACIÓN DE UN PROTOTIPO-INTERFAZ PARA COMUNICACIÓN DE PROTOCOLO CONTACT-ID CON UN SISTEMA DE GESTIÓN IP, APLICADO A DISPOSITIVOS DE SEGURIDAD RESIDENCIAL**, realizado por Alex Fabian Yunga Muyulema y Elvis Geovanny Zaruma Quituizaca, obteniendo el *Proyecto Técnico con enfoque social* que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana.

Cuenca, marzo del 2019

Ing. Juan Diego Jara. Mgt.

CI: 0103543658

DECLARATORIA DE RESPONSABILIDAD

Nosotros, Alex Fabian Yunga Muyulema con número de cédula 0603676099 y Elvis Geovanny Zaruma Quituizaca con número de cédula 0105803720, autores del trabajo de titulación: **DESARROLLO E IMPLEMENTACIÓN DE UN PROTOTIPO-INTERFAZ PARA COMUNICACIÓN DE PROTOCOLO CONTACT-ID CON UN SISTEMA DE GESTIÓN IP, APLICADO A DISPOSITIVOS DE SEGURIDAD RESIDENCIAL,** certificamos que el total contenido del *Proyecto Técnico con enfoque social***,** es de nuestra exclusiva responsabilidad y autoría

Cuenca, marzo del 2019

Alex Fabian Yunga Muyulema
CI: 0603676099

Elvis Geovanny Zaruma Quituizaca
CI: 0105803720

AGRADECIMIENTOS

Agradezco a Dios quien ha sido el motor principal en mi camino para culminar satisfactoriamente mis estudios, por guiarme en todo mi camino por ser el apoyo y fortaleza en todos los momentos difíciles que se me han presentado en toda mi carrera. A mis padres Carlos Yunga y Ana Muyulema por confiar en mí, por los valores y principios que me han inculcado, por haber estado conmigo apoyándome en los momentos difíciles.

Por sus conocimientos compartidos y apoyo para la elaboración de la presente tesis, a nuestro director Ing. Juan Diego Jara Saltos, Mgt.

Alex Fabia Yunga Muyulema

Agradezco en primer lugar a Dios por brindarme la vida y la salud para poder terminar mis estudios superiores. A mis padres Segundo Zaruma y Grima Quituizaca por haber sido mi principal apoyo durante todo este trayecto. A mis hermanos Jaime, Jonnathan y Jessica gracias por el apoyo incondicional que siempre he recibido. A mis abuelitos Leopoldo y Rosario por inspirarme a seguir adelante cuando la meta parecía imposible. También quiero dedicar un agradecimiento especial a mis tíos Luis German Zaruma y Ana Lucia Borja por ayudarme y aconsejarme en todo momento.

A nuestro director Ing. Juan Diego Jara Saltos, Mgt, quien con su apoyo incondicional ha sabido guiarnos durante todo este trabajo.

Elvis Geovanny Zaruma Quituizaca

DEDICATORIAS

A Dios por permitirme culminar una meta más en mi vida. A mis padres por todo el apoyo que me han brindado a lo largo de toda mi carrera, quienes han velado por mi bienestar y depositar su confianza en mí para llevarme a culminar una meta más en mi vida.

Alex Fabian Yunga Muyulema

Este proyecto está sin duda dedicado a mis padres ya que sin ellos nunca hubiera podido llegar hasta aquí, a ustedes les debo todo y luchare hasta lograr recompensar todo el esfuerzo invertido en mí.

También dedico este trabajo a mis hermanos, y a mis abuelitos. Gracias a todos ustedes por siempre confiar en mí y ser mi apoyo incondicional.

Elvis Geovanny Zaruma Quituizaca

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Los paneles de alarma residencial en la actualidad requieren estar conectados a una línea telefónica local para permitir el servicio de monitoreo, sin embargo en zonas alejadas esto es casi imposible. En el presente artículo se detalla el desarrollo de un prototipo-interfaz para la comunicación con un panel de alarma DSC-585 básico que trabaje con el protocolo Contact ID, este prototipo se conecta directamente a una red de internet domiciliara, con el objetivo de enviar las emergencias o avisos mediante una trama a un Sistema de Gestión a través de una red privada virtual (VPN). La ventaja de este prototipo es el tiempo de respuesta ante un evento pues está en el rango de un minuto, además es de bajo costo lo que hace que sea un producto accesible para la comunidad.

INTRODUCCIÓN

En la actualidad los sistemas de seguridad domiciliara con monitoreo representan un esquema de tranquilidad en el cuidado de los bienes para los usuarios, pues la inseguridad crece con el pasar de los días. En Ecuador los índices se han incrementado notablemente en los últimos años.

Los paneles de alarma básicos DSC-585 utilizan el medio de comunicación urbano más común; la línea telefónica, pues a través de la misma las empresas de seguridad ofrecen servicio de monitoreo. Las empresas privadas encargadas de monitorear cuentan con una central de operaciones donde tienen una centralita telefónica a la espera de la notificación de violación de zonas. Las zonas son las borneras en donde se conectan los distintos sensores.

El inconveniente que presenta el sistema de monitoreo a través de la línea telefónica es el reducido campo de cobertura ya que no se puede llegar a zonas urbanas alejadas o zonas rurales, limitando las posibilidades de asegurar el domicilio o local comercial, adicionalmente la alarma produce interferencia con los teléfonos y el internet en el caso de XDSL.

Al ver limitada las posibilidades de brindar servicio de monitoreo a ciertos lugares en donde no se cuenta con línea telefónica alámbrica, las empresas de seguridad cuentan con un dispositivo capaz de lograr la misma comunicación a través de la nube de internet, sin embargo el inconveniente principal es el costo de implementación de este equipo, además de eso protocolos propietarios de comunicación.

Las alarmas básicas DSC-585 para comunicarse con la central telefónica utilizan el Protocolo Contact ID a través de tonos DTMF. Los datos obtenidos de la alarma mediante el prototipo implementado en este trabajo, son enviados a un Sistema de Gestión mediante un túnel Open VPN, que se encarga de encriptar la información y desencriptar en el servidor remoto, para luego ser mostrada en el gestor.

En el trabajo presentado en este proyecto de titulación se crea un dispositivo con las funciones de una mini central telefónica para la recepción de los eventos enviados por la alarma. El dispositivo es capaz de comunicar una alarma básica con el sistema de gestión, pero en este caso ya no se necesita la línea telefónica fija sino más bien es

necesario contar con servicio de internet domiciliario, a través de cualquier acceso alámbrico o inalámbrico, por donde viajaran los eventos generados hacia el Sistema de Gestión IP.

ANTECEDENTES DEL PROBLEMA DE ESTUDIO

La alarma residencial, es un dispositivo que debe garantizar una respuesta inmediata ante una emergencia, como por ejemplo el ingreso de personas no autorizadas en hogares, departamentos, locales comerciales, entidades financieras, instituciones educativas, etc.

Las primeras alarmas creadas constaban de un conjunto bien elaborado de campanillas que estaban vinculadas de manera mecánica a las puertas, el inventor fue el Ingles Tildesley. Se mejoró el sistema tiempo después con la utilización imanes para las alarmas electromagnéticas. El inventor que presento por primera vez una alarma electromagnética y una empresa de instalaciones eléctricas fue Edwin Holmes [1][2].

Uno de los principales componentes de un sistema de alarma residencial es el sensor de movimiento, este dispositivo sale al mercado por primera vez en la década de 1950 [3]. En la actualidad existe gran variedad de sensores; tales como: Detectores de movimiento interior, Detectores de movimiento para interiores, mascotas, magnéticos, de humo, etc. [4].

En la actualidad los hogares tienen en su interior un sistema de alarma conectados a un proveedor de monitoreo que ofrece diferentes tipos de servicios ante cualquier emergencia, por un costo mensual, no obstante se ve limitado a la red de conexión PSTN [5], pues las empresas no pueden ofrecer monitoreo constante en los lugares en donde no se cuente con una línea telefónica o esté demasiado distante de su centro de despacho de vehículos de seguridad privada. Se pretende entonces la opción de implementar este dispositivo en los Hogares, y que sea monitoreado por un ente de seguridad Estatal, considerando que algunos hogares no cuentan con el suficiente capital económico para pagar el servicio privado y optan por adquirir alarmas de bajo costo. También existen hogares que tienen un sistema de alarma con mayor costo que comunica directamente al propietario del hogar cualquier tipo de evento que se presente vía mensajes de texto, sin embargo, el tiempo de respuesta ante dicho evento es prolongado, corriendo el riesgo de no comunicar la emergencia a las respectivas autoridades, y en el peor de los casos perder los enseres del hogar.

JUSTIFICACIÓN (IMPORTANCIA Y ALCANCES)

Según datos tomados del portal web del Ministerio del Interior, a finales del año 2017 en el Ecuador se reportaron: 14.842 robos a domicilios, siendo el mes de mayo el más crítico. En el primer trimestre del 2018 se reportan alrededor de 2.151 robos a domicilios, cifra desfavorable, ya que en el primer trimestre del 2017 tan solo fueron 1.204 casos. En la provincia del Azuay, en donde se plantea implementar nuestro dispositivo, al finalizar el año 2017 el número de robos fue de 813 que representa un incremento del 0,49% con respecto al año 2016. En el primer trimestre del 2018 se registran 132 casos, número que también presenta un incremento con respecto al año 2017 donde se produjo 124 robos a domicilios [6].

Ante esta problemática lo que se plantea es diseñar un dispositivo inteligente que estará conectado con la memoria de la alarma residencial respectivamente instalada en los hogares. Este dispositivo estará conectado mediante la red de internet con un Sistema de Gestión, por lo que es necesario que los hogares cuenten con un proveedor de servicio internet. El dispositivo enviará todos los eventos que ocurran en el hogar, almacenes, oficinas, microempresas, instituciones educativas, etc.

OBJETIVOS

OBJETIVO GENERAL

Desarrollar un prototipo-Interfaz para comunicación de protocolo Contact ID con un sistema de gestión IP, aplicado a un dispositivo de seguridad residencial.

OBJETIVOS ESPECÍFICO

- Investigar las características, protocolos de comunicación y funcionamiento de una memoria de alarma residencial (DSC-585).
- Diseñar un prototipo Interfaz para la comunicación entre una alarma residencial y el sistema de gestión IP.
- Realizar un Sistema de Gestión en software libre para visualizar los eventos ocurridos en la alarma residencial a través de la red IP.
- Validar mediante pruebas de funcionamiento en campo el correcto funcionamiento del dispositivo interfaz y los mensajes de alerta notificados en el Sistema de Gestión.

CAPÍTULO 1: INTRODUCCIÓN Y REVISIÓN DEL ESTADO DEL ARTE

1.1 INDICE DE ROBO A DOMICILIOS EN ECUADOR

En Ecuador, los índices de robos a domicilios varía según la región, en la parte costanera del país las estadísticas de atracos a bienes privados son más frecuentes, debido al alto índice de población, seguido a esto la segunda región afectada es la sierra y le siguen la región oriental y la insular. En la Figura 1.1 se puede ver las estadísticas del año 2017.

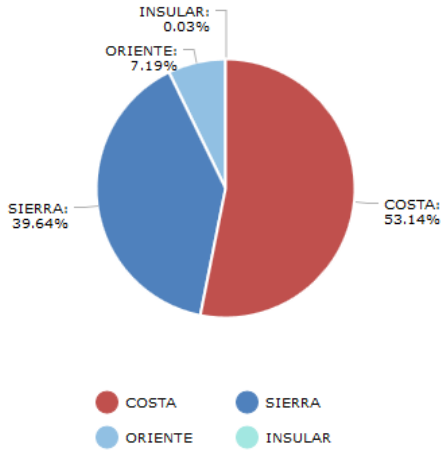


Figura 1.1: Estadísticas de robo a domicilios en Ecuador por región, año 2017 [6]

1.1.1 OCURRENCIA

Las familias ecuatorianas por lo general tienen la tendencia de abandonar sus hogares los fines de semana, por lo general para salir en busca de lugares de entretenimiento familiar, esta situación es aprovechada por personas ajenas que buscan ingresar a los hogares valiéndose de la falta de vigilancia. Los días con mayor índice son: el viernes, sábado y domingo, como se muestra en la Figura 1.2.

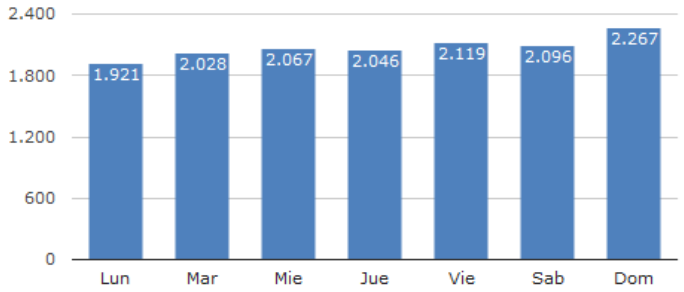


Figura 1.2: Estadística de días con mayor índice de robos, año 2017 [6]

1.2 SERVICIO DE MONITOREO EN LA CIUDAD DE CUENCA

Existen varias empresas que ofrecen servicio de monitoreo de domicilios, y locales comerciales con alarmas de seguridad básicas como las del fabricante DSC, o con paneles de otras marcas con un costo más elevado.

1.2.1 EMPRESAS CON SERVICIO DE MONITOREO

Según datos tomados en la ciudad de Cuenca se puede distinguir cinco empresas que brindan servicio de seguridad, sin embargo para este trabajo se tomó en cuenta a tres empresas que son las más reconocidas y que acaparan el mercado en la ciudad como se muestra en la Tabla 1.1 Los valores presentados incluyen el precio de una alarma residencial básica DSC-585.

Servicio de monitoreo ofrecido por las principales empresas de Cuenca		
EMPRESA	Costo de Instalación servicio	Costo de monitoreo mensual
Crimestop S.A	550	25
Omnitron	500	20
ATS	620	29,9

Tabla 1.1 Empresas que ofrecen monitoreo en la ciudad de Cuenca. Fuente: Web empresas

1.3 PROBLEMÁTICA DE ENVIÓ DE MENSAJES DE ALERTA POR INTERNET

Los mensajes de aviso a través de internet en la mayoría de los casos se ve limitado debido al uso de software propietario impidiendo a los usuarios enviar mensajes de alerta de manera directa.

1.3.1 EQUIPOS CON SOFTWARE PROPIETARIO

Software propietario es un término inglés “propetary software” que hace referencia a la posesión o control privado. También en la lengua anglosajona se le conoce como “proprietary”. En general software propietario hace referencia a que la empresa creadora tiene el poder total sobre todos los derechos del software allí creado [7][8].

Al término software propietario también se menciona como privado, no libre, privativo, con propiedad o de propiedad. Estos términos hacen referencia a que el usuario se encuentra con limitaciones para modificar y distribuirlo, pues el código fuente del software está restringido por un contrato de licencia [9].

En términos generales si se impide el uso libre de un software para estudio, realizar posibles mejoras y publicarlas pierde el sentido de libertad y más bien recae en el grupo de software con propietario.

1.3.2 EQUIPOS CON SOFTWARE LIBRE.

El software libre es aquel que respeta la libertad de los usuarios sobre un producto que adquiere, este puede ser copiado, estudiado, modificado y distribuido libremente [10].

En los años 60 el software no era considerado un producto sino más bien un aporte de los creadores a los usuarios de manera libre y voluntaria, sin embargo a partir de los años finales de la década de los 70 las compañías empezaron a poner restricciones a los usuarios para el libre uso de sus software creando el termino con software propietario o con propietario.

El proyecto GNU es un trabajo realizado por Richard Stallman en el año1984, se trata de un proyecto para la creación de la Free Software Foundation (FSF). Este proyecto permitió a los usuarios poder ejecutar, modificar, mejorar y distribuir el software.

Otros términos propios de confusión son: software libre y software gratuito, pues el software gratuito no cuesta nada y esto no lo convierte en software libre [10].

Han existido confusiones con respecto a la palabra Free, traducido al español también puede significar tanto libre como gratis.

1.3.3 SOFTWARE DE ALARMA DSC-585

Los paneles de alarma DSC por lo general utiliza el protocolo SIA Contact ID, el mismo que es un protocolo dominante y ha sido estandarizado para su aplicación en sistemas de seguridad [11], el usuario puede tomar su información y utilizarla según la aplicación que se esté realizando.

1.4 PENETRACIÓN DEL INTERNET EN LAS ZONAS RURALES

En la ciudad de Cuenca el servicio de internet cubre prácticamente toda el área urbana, por lo que la comercialización de los servicios de monitoreo es accesible [12]. En el ecuador la penetración del internet fijo en los hogares ha tenido un crecimiento significativo, pues la demanda se ha incrementado considerablemente en todo el territorio nacional [13].

El plan nacional del gobierno planteado en al año 2016 y que se prevé obtener beneficios en el 2021 pretende llevar la cobertura de banda ancha a la mayoría de rincones del país, pues todas personas en forma individual o colectiva, tienen derecho al acceso universal a las tecnologías de información y comunicación [14][15].

En la actualidad en la mayoría de los hogares ecuatorianos existe por lo menos una conexión a la red de internet fija, las provincias que mayor índice de crecimiento presentan son: Pichincha, Guayas y la provincia del Azuay, esto contrasta con el servicio de telefonía que ha decrecido de manera considerable [13].

1.5 PANEL DE ALARMA DSC

Un panel de alarmas es un dispositivo programable que consta de entre 4 y 64 zonas, lo que lo hace ser un dispositivo escalable diseñado para usos residencial y comercial ligero. El panel de alarma de la marca DSC-585 (Digital Security Control) es compatible con dispositivos cableados e inalámbricos existentes o futuros, en caso de actualización estos productos tienen la capacidad de permitir al usuario expandir y mejorar sus sistemas de seguridad sin necesidad de reemplazarlo [16].

El panel consta de una batería de respaldo en caso de falla eléctrica, además cuenta con la memoria que controla todos los eventos ocurridos en las diferentes zonas, para el caso de estudio en este trabajo se utilizó una alarma con cuatro zonas con la posibilidad de expandirlas a ocho.

1.5.1 ZONAS

La zona es un conjunto de sensores de tipo normalmente cerrado (como contactos de puerta) conectado a serie o normalmente abierto (como detectores de humo) conectados en paralelo, la idea principal de una zona es la de generar un estado lógico de abierto o cerrado al momento de ser violentado [17].

1.5.2 CONEXIÓN A LA LÍNEA TELEFÓNICA

Los cables de línea telefónica externa se conectan a las entradas TIP y RING de la central, y los cables T-1 y R-1 al sistema telefónico como se puede apreciar en la Figura 1.3.

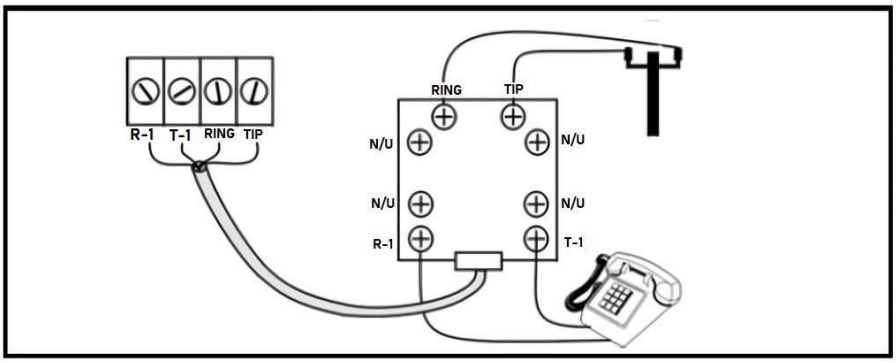


Figura 1.3: Conexión a la línea telefónica [18]

1.5.3 CONEXIÓN DEL TECLADO

El panel de alarma DSC-585 es conectado a un teclado básico para poder programar de forma manual los parámetros necesarios para el funcionamiento del mismo. Las borneras del panel están marcadas con las mismas iniciales que las que posee el teclado, de esta manera se puede realizar conexión de manera sencilla. En la Figura 1.4 se visualiza una representación de la conexión.

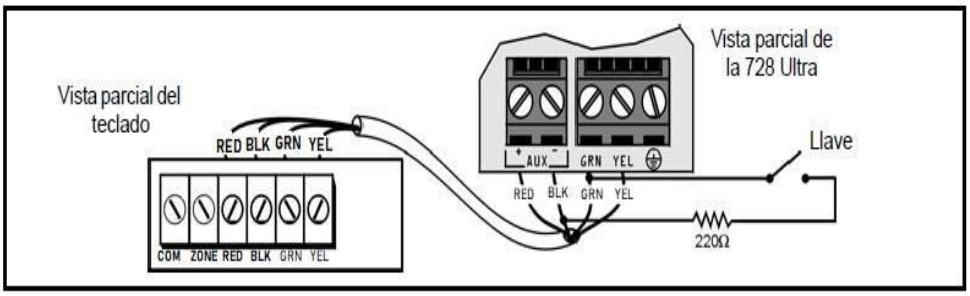


Figura 1.4: Conexión del teclado [18]

1.6 PROTOCOLO CONTACT ID

El formato Contact ID es la composición de una serie de dígitos con información de los eventos ocurridos en el panel de alarmas. Fue desarrollado por la compañía Ademco para comunicar sus diferentes equipos, es un formato reconocido por la Asociación de Industrias de Seguridad (SIA) [11] como un estándar que puede ser adoptado por muchos fabricantes con la finalidad de aumentar la compatibilidad entre paneles de alarma.

Los objetivos del formato Contact ID son:

- Proveer información de los eventos ocurridos en un panel de alarmas. La información debe ser de fácil interpretación para la central de operación.
- Minimizar el tiempo utilizado en la línea de transacción con el objetivo de minimizar la cantidad de receptores.
- Minimizar la tasa de error.
- Minimizar el costo de hardware asociado con la transmisión de la información.

1.6.1 HANDSHAKE

El intercambio de información que se da entre un usuario y un servidor se le conoce como Handshake. El Handshake está presente en todas las redes móviles y fijas [19], pues con la extensión del internet de las cosas (IoT) es importante el intercambio de información constante entre los nodos de una misma red LAN o de diferentes redes WAN con el fin de encontrar la ruta más corta cuando se suscite un evento [20][21].

Cuando en un domicilio ocurre un evento inmediatamente la transmisión ocurre detectando un tono de marca y posterior llamada del panel de alarma hacia el numero asignado en la central de monitoreo, cuando la central recibe la llamada esta responde con una secuencia de tonos que se detallan a continuación.

La secuencia comienza con un tono de 1400Hz que tiene una duración de 100ms, luego de esto se da una pausa de 100ms y por último la central envía un tono de 2300 Hz de igual manera con un tiempo de duración de 100ms. Todo lo anterior puede tener un error de $\pm 5\%$, además para poder recibir la información generada por el panel de alarma se puede generar un Hansdhake simplemente presionando la tecla 1.

1.6.2 KISSOFF

Cuando la secuencia de tonos Handshake finalice, el panel de alarma envía el bloque de datos Contact ID con un retardo de entre 250 a 300ms. Cada mensaje es hexadecimal, es decir consta de 16 dígitos separados con espacios y con tiempo de separación de 1,25 segundos previo un tono de reconocimiento emitido por el receptor llamado Kissoff. [22]

El bloque de mansajes se divide de la siguiente manera.

NNNN	Cuatro dígitos de numero de abonado (0-9, B-F) asignado durante la programación
BB	Dos dígitos de identificación para el Contact ID, estos pueden ser el 18(preferiblemente) y el 98 (opcional).
C	Calificador de evento, si es uno será un evento de apertura, si es tres será de restablecimiento o cierre y por ultimo si es seis será un evento ya reportado que sigue vigente
EEE	Código de eventos (3 dígitos hexadecimales0-9. B-F)
PP	Número de partición que ocupa en el panel (2 dígitos hexadecimales 0-9. B-F).
CCC	Ubicación física de la zona en los terminales del panel de alarma
D	Un digito hexadecimal checksum calculado de tal manera que: (Suma de todos los dígitos +D) MOD 15=0

Tabla 1.2: Detalle de las partes del Contact ID [18]

El suceso ocurrido en el panel de la alarma genera una alarma de aviso, según el evento ocurrido se puede determinar el grado de la emergencia.

En la Tabla 1.3 se presenta algunos de los códigos de eventos tomados del manual de instalación de la alarma DSC-585 [18]. En los códigos de contacto la letra A representa un cero.

Sección #	Código de reporte	Código Enviado Cuando…	Dirección del Marcado*	Códigos del Contact ID
[320]	Alarmas de zona	La zona de entra en alarma	A/R	(1)3ª
[324]	Restablecimiento de zona	La condición de zona ha sido restaurada	A/R	(1)3ª
[330] [334]	Sabotaje/Rest. de zona	La zona presenta una condición de sabotaje/la condición de sabotaje es restablecida	T/R	(1)44
[328]	Alarma de coacción	Código de coacción entrado en el teclado	A/R	(1)21
[328]	Apertura después de una alarma	Sistema es desarrollado con alarma en memoria	A/R	(4)A6
[328]	Cierre reciente	Alarma ocurre dentro de dos minutos de armar el sistema	A/R	(4)59
[329]	Alarma/Rest. de supervisor de expansor de zona	Supervisión sobre el Keybus del módulo enlistado PC5 132 o teclados con entradas de zona	A/R	(1)43
[329]	Alarma de zonas cruzadas (Código de la Policía)	Dos zonas en la misma partición entran en alarma durante cualquier periodo dado de armado a armado (incl. Zona 24 horas)	A/R	(1)4ª
[329]	Alarma/Rest. de Tecla [F].	Alarma de incendio en el teclado (cod. de rep. de alarma/restablecimiento son enviados juntos)	A/R	(1)15
[329]	Alarma/Rest. de tecla [A].	Alarma de auxiliar en el teclado (cod. de rep. de alarma/restablecimiento son enviados juntos)	A/R	(1)AA
[329]	Alarma/Rest. de tecla [P].	Alarma de pánico en el teclado (cod. de rep. de alarma/restablecimiento son enviados juntos)	A/R	(1)2ª

Tabla 1.3: Código de evento [18]

1.7 TONOS DTMF

Los tonos DTMF (Dual Tone Multi-frequency) fueron desarrollados por los laboratorios Bell y es el estándar utilizado para las señalizaciones de la comunicación telefónica [23].

Los tonos de las señales DTMF están compuestas por la suma de dos señales sinusoidales, una de alta frecuencia y otra de baja frecuencia [22], lo más común para la utilización de los tonos DTMF es en la telefonía fija, sin embargo también existen otras aplicaciones como las comunicaciones móviles y servicio de radio para pequeños aficionados, como por ejemplo la aplicación y control de un pequeño robot móvil [25][26]. En la Figura 1.5 se puede ver las frecuencias de los tonos DTMF.

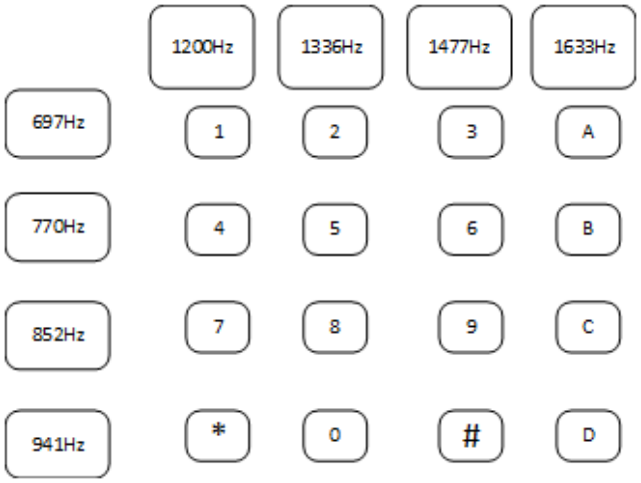


Figura 1.5: Codificación DTMF [24]

1.7.1 NORMAS PARA LAS SEÑALES DTMF

Los tonos expuestos en la Figura 1.5 representan la distribución de frecuencias para los tonos audibles que se genera al pulsar cada valor ahí especificado, sin embargo la UIT demanda el cumplimiento de diferentes parámetros en cuanto a los tonos DTMF.

La UIT especifica que una frecuencia es válida si esta se encuentra en el rango de $\pm 1.5\%$ de las frecuencias consideradas como nominales, de la misma manera se especifica que una frecuencia es invalida si la misma está en el rango $\pm 3.5\%$ de dichas frecuencias.

También otra de las normas expuestas por la UIT es la duración de la señal DTMF, pues el tiempo mínimo requerido será de 40ms, lo cual corresponde al tiempo típico de una tecla de un teléfono [27].

En la Tabla 1.4 se presenta las recomendaciones de la UIT para los tonos DTMF, en donde se detalla las diferentes características para el correcto uso de los tonos como por ejemplo las frecuencias para los dos tipos de tono: alto y bajo.

Frecuencia de las señales bajas	Grupo alto Grupo bajo	1209, 1336, 1477, 1633 897, 770, 852, 941
Tolerancia de frecuencias	Operación No operación	<=1.5% >=3.5%
Excepciones de la señal	Operación No operación	40 ms mínimo 23 ms máximo
Duración de la señal	Duración de pausa Interrupción de señal	41 ms mínimo 10 ms máximo
Twist	Directa Inversa	8dB 4dB
Potencia de la señal	SNR Potencia	15 dB mínimo -25 dBm máximo
Talk-Off		>30 dB

Tabla 1.4: Recomendaciones de la UIT para los tonos DTMF [27]

1.7.2 CODIFICACIÓN DE TONOS DTMF

La codificación de tonos DTMF se puede realizar de diferentes maneras y consiste en generar las ondas sinusoidales correspondientes a las frecuencias presentadas en la Figura 1.5, la codificación es una combinación de tonos altos y bajos [30] y se pueden conseguir de manera análoga mediante un integrado o de manera digital mediante el procesamiento digital de señales [28].

1.7.3 DECODIFICACIÓN DE TONOS DTMF

Los tonos DTMF que están presentes en las comunicaciones mediante teléfono por lo general son simples tonos audibles que representan una frecuencia, sin embargo cuando se necesita determinar el valor de la tecla marcada se requiere otras técnicas de decodificación para poder visualizar el valor del tono [28].

La decodificación digital se puede realizar mediante algoritmos como el de Goertzel [22][26], la FFT o una tarjeta FPGA, utilizando la herramienta Matlab para la visualización de los tonos recibidos.

1.7.3.1 DECODIFICADOR MT88L70

El decodificador MT88L70 de la empresa MITEL, es un receptor de tonos DTMF que tiene en su configuración dos filtros separadores de las frecuencias altas y de las bajas [30][31].

Este integrado con tecnología CMOS tiene bajo consumo de potencia (35 mW como máximo) y un control preciso de los datos. Este decodificador detecta y decodifica los 16 tonos DTMF y los transforma en un numero binario de 4 bits [30].

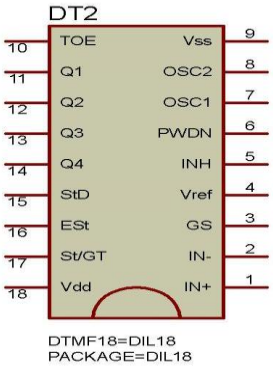


Figura 1.6: Integrado decodificador DTMF, MT88L70 [24]

El decodificador presentado en la Figura 1.6 recibe los tonos provenientes de la línea telefónica, luego devuelve por medio de las salidas Q1 a Q4 un número binario que corresponde a la tecla marcada en el instante.

1.8 COMUNICACIÓN SERIAL PIC 16F877A

La mayoría de los Microcontroladores PIC en la actualidad utilizan un módulo de comunicación serie denominado USART/SCI, con el mismo pueden cumplir la función de transmitir datos o a su vez recibirlos en serie.

Existen dos categorías para realizar la operación de envió o recepción de datos, síncrona y asíncrona. En la categoría de transmisión síncrona es necesario enviar la señal de reloj y a su vez una línea de datos, generalmente se utiliza cuando la distancia es corta entre el transmisor y el receptor. Por otra parte en la transmisión asíncrona no es necesario la señal de reloj, lo que conlleva a que el transmisor y receptor deben tener señal de reloj sincronizado a la misma frecuencia y fase, esta categoría de transmisión es utilizada cuando la distancia entre emisor y receptor es considerable [32].

1.8.1 MÓDULO USART EN “C”

Para realizar la comunicación entre el microcontrolador PIC y el software libre “PIC C Compiler” se debe realizar una configuración genérica al módulo de comunicación USART (#USE RS232), para poder modificar las líneas de comando

con simplemente anteponer la directiva #USE DELAY que a su vez habilita el uso de múltiples funciones secundarias [32].

1.9 RASPBERRY PI

La Raspberry Pi 2 B es una versión más actualizada de la versión anterior (Raspberry Pi), presenta una mejora considerable en su procesador multinúcleo ARMv7 y la memoria RAM es de 1 gigabyte. El rendimiento de este mini ordenador es mucho mejor en comparación de las versiones anteriores, pues tiene un aumento de velocidad de hasta 7.5x! [33]. En la Figura 1.7 se muestra un dispositivo Raspberry Pi 2B.

Figura 1.7: Raspberry Pi 2B [33]

1.10 VPN

La Red Privada Virtual (VPN) es la tecnología de crecimiento más rápido en los últimos tiempos debido a los beneficios de proporcionar seguridad a la hora de trasmisión de datos. Una VPN es una red de carácter privada que utiliza la red pública para permitir la conexión de sitios o usuarios ubicados en lugares remotos [34].

En la actualidad existe el protocolo VPN SSL (Secure Socket Layer VPN) que reemplaza al tradicional protocolo IPSec VPN que es complejo y en muchos casos redundante. Con VPN SSL no es necesario que el usuario final cuente o mantenga instalado alguna clase de software de carácter especial en su dispositivo de recepción del cliente final [35].

Existen dos tipos importantes de VPN que se describen a continuación.

1.10.1 VPN DE SITIO A SITIO

Este tipo de VPN permite que varios locales en lugares específicos puedan establecer comunicación entre ellas a través de una red de carácter público como el internet, esto se puede observar en la siguiente Figura 1.8.

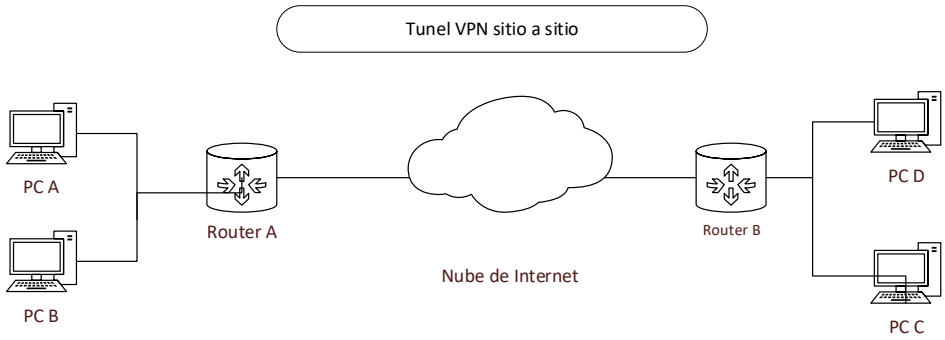


Figura 1.8: Esquema VPN de Sitio a Sitio

1.10.2 VPN DE ACCESO REMOTO

Este tipo de VPN permite a uno o varios usuarios establecer un tipo de conexión a una red remota, pudiendo estos acceder a la información de dicha red de manera segura como si lo estuvieran haciendo directamente con los servidores, como se observa en la Figura 1.9.

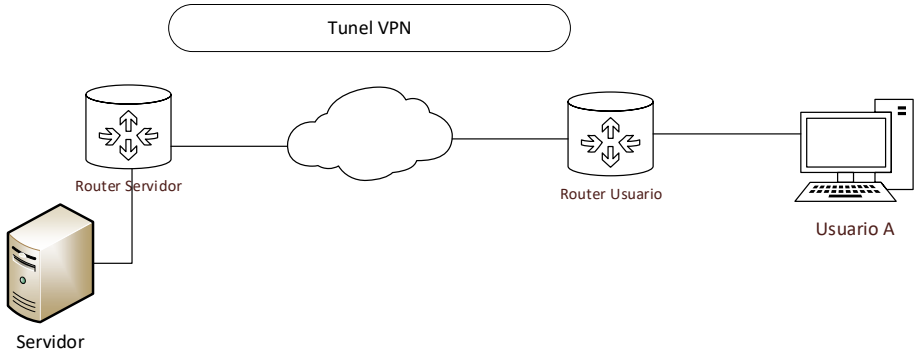


Figura 1.9: Esquema VPN de Acceso Remoto

1.11 SOCKETS

El socket es un medio de comunicación entre un programa de tipo cliente y un programa de servidor en una red. Su definición está dada por un par de direcciones IP local y remota, un protocolo de transporte y un par de números de puerto local y remoto. Un socket es un proceso de comunicación entre la máquina del cliente y la del servidor, esto con la finalidad que el usuario cliente y el servidor tengan la

factibilidad de leer y escribir información sin inconveniente alguno. Esta información será transmitida posteriormente por las diferentes capas de red [36]. En la Figura 1.10 se observa el esquema de la comunicación por sockets.

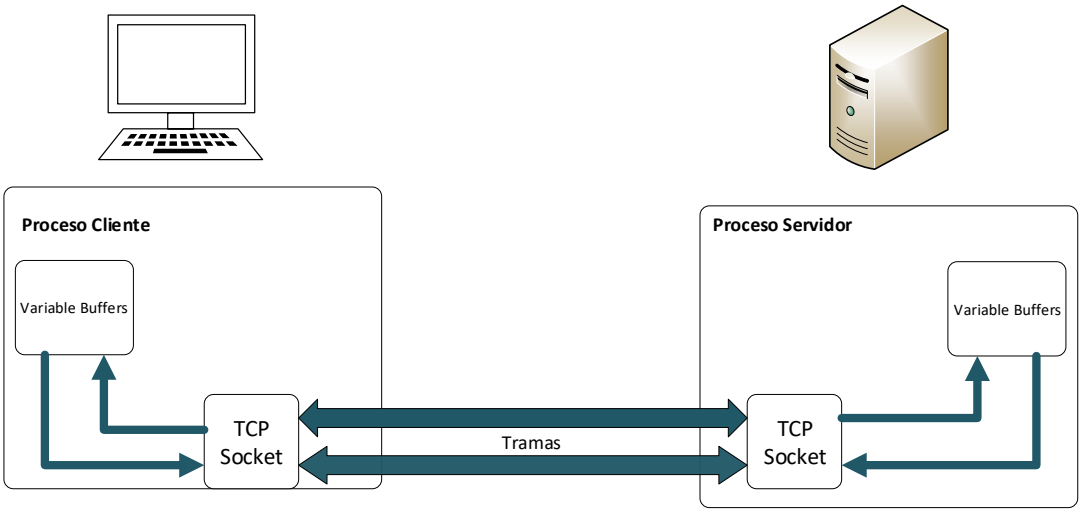


Figura 1.10: Comunicación por socket, cliente-servidor [37]

CAPÍTULO 2: MARCO METODOLÓGICO.

2.1 ESQUEMA DEL CIRCUITO A IMPLEMENTAR

El prototipo planteado consta de 5 etapas: Tono de Marcación, Circuito de recepción de dígitos, Circuito de control, Circuito de conmutación y circuito de recepción del protocolo Contact ID. En la Figura 2.1 se presenta el esquema de funcionamiento del prototipo diseñado.

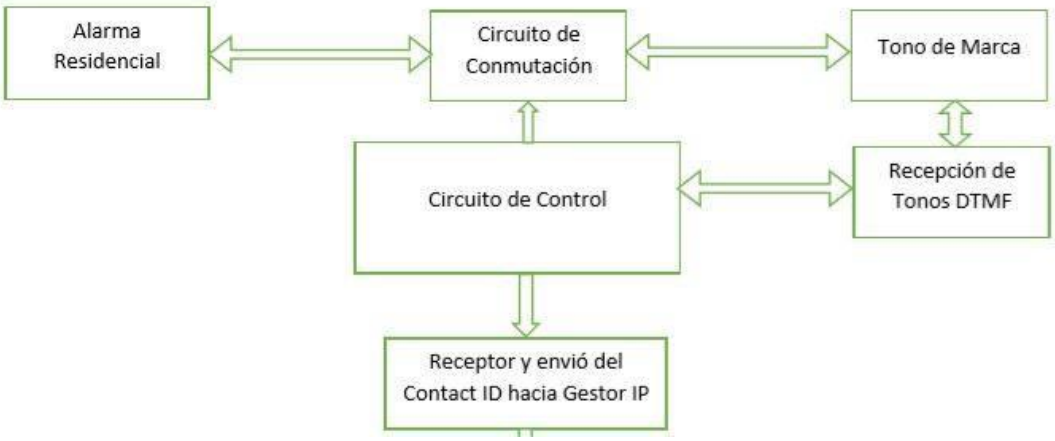


Figura 2.1: Esquema del prototipo diseñado

2.1.1 TONO DE MARCA

Como se mencionó anteriormente, para nuestro diseño del prototipo-interfaz se ha utilizado la alarma residencial DSC-585. Este equipo se comunicará con el prototipo mediante un circuito generador de tonos, denominado: tono de marca cuyo objetico es producir señales en un rango de frecuencia entre 1KHz y 3KHz.

Los eventos ocurridos en la alarma son notificados mediante una llamada a un número telefónico previamente programado, la marcación sucede al momento que en el panel se presente un evento, dicha marcación se da mediante tonos DTMF. Para el diseño de este circuito se utilizó un temporizador Integrado IC555. En la Figura 2.2 se presenta el esquema del integrado.

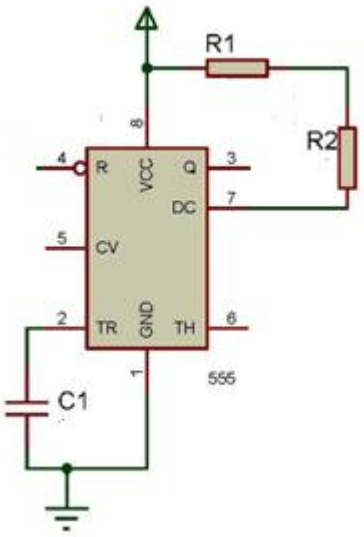


Figura 2.2: Temporizador 555

Para calcular los valores de las resistencias R1 y R2 se tomó el valor de un capacitor (C) de 10nF, además se considera los tiempos de bajada de 4 seg T1 y 5 seg T2 para las frecuencias. En la Figura 2.3 se presentan los valores calculados para obtener el tono de marca.

$$T1 = 0.693 * R2 * C$$ Ecuación (1)

$$T2 = 0.693 * (R2 + R1) * C$$ Ecuación (2)

Entonces para obtener los valores de las resistencias despejamos de las Ecuaciones (1) y (2).

$$R2 = T1/(0.693 * C)$$
$$R2 = 9.2K\Omega \approx 10k\Omega$$
$$R1 = T2/((0.693 * C) - R2)$$
$$R1 = 2.28K\Omega \approx 2.2k\Omega$$

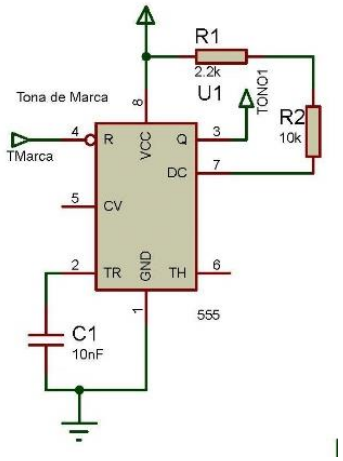


Figura 2.3: Circuito de tono de marca

Como la corriente de salida del integrado IC555 es pequeña se procedió a utilizar un transistor configurado como interruptor.

2.1.1.1 CIRCUITO AMPLIFICADOR

Para el diseño del circuito amplificador se utilizó un transistor BJT en polarización emisor común, se escogió esta configuración debido a que permite obtener mayor ganancia, ya que la salida del IC555 es baja y el elemento que decodifica los tonos DTMF necesita una entrada amplificada.

La señal de entrada es $9v$, como se desea amplificar la parte positiva y negativa necesitamos que el voltaje en el colector sea v/2, en este caso seria 4.5v. Mediante la ley de Ohm se calcula la resistencia en el colector.

$$Rc = \frac{V_{cc} - V_c}{I_c} \qquad \text{Ecuación (3)}$$

La corriente Ic se toma de la hoja de datos del transistor, para los cálculos se utilizó el valor de 1mA.

Entonces el valor de la resistencia de colector es: $Rc = 4.5KOhms$. El valor de resistencias comerciales es de $4.7K\Omega$

El transistor se activa si se aplica un voltaje mínimo en el límite inferior ($0.6v$ para silicio), para ello se aplica resistencias de polarización R1 y R2 como se observa en la Figura 2.4.

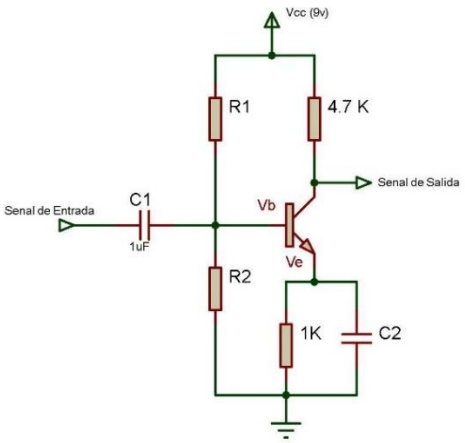


Figura 2.4: Circuito amplificador

Donde Ve es de $1v$ por la caída de voltaje entonces $Vb = 1 + 0.6v = 1.6v$, con este valor se realiza un divisor de voltaje.

$$V1 = \frac{R2}{R1+R2} * Vin$$ Ecuación (4)

Donde:

$Vin = 9v$

$V1 = 1.6v$

Entonces.

$$\frac{R_1}{R_2} = \frac{V_{in} - V_{out}}{V_{out}}$$

$$\frac{R_1}{R_2} = \frac{9 - 1.6}{1.6} = 4.6$$

La ecuación anterior nos indica que R1 tiene que ser 4.6 veces más grande que R2. Para ello se usó para R2 una resistencia de $1K$ y para R1 una resistencia de 4.7KΩ. En la Figura 2.5 se puede observar los valores calculados para el circuito.

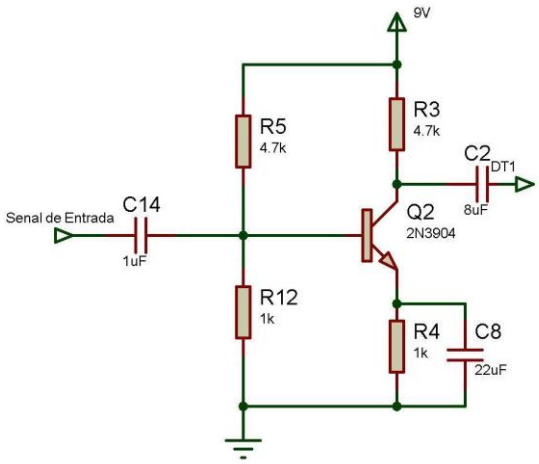


Figura 2.5: Circuito amplificador diseñado

2.1.2 CIRCUITO PARA LA RECEPCIÓN DE DÍGITOS

El número digitado por el panel de alarma llega en forma de tonos DTMF (Dual Tono Multi Frequency), por lo cual se necesita un decodificador. Se utilizó el

decodificador MT88L70 presentado en la Figura 2.6 que tiene la capacidad de convertir las señales DTMF de entrada en señales digitales.

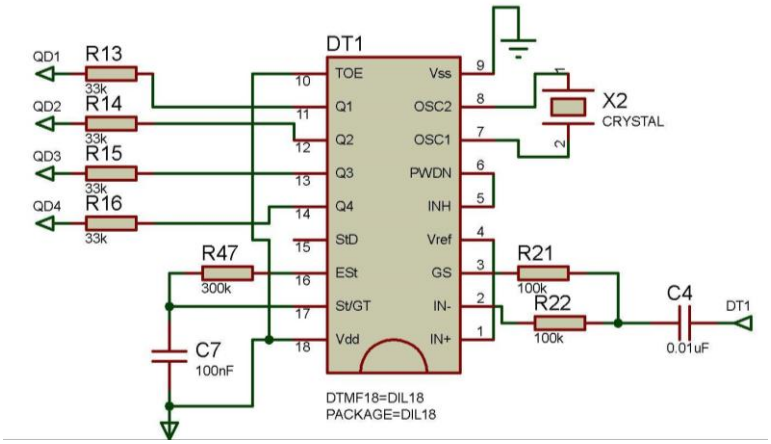


Figura 2.6 Decodificador de tonos DTMF MT88L70

Las señales decodificadas (señales digitales) serán posteriormente enviadas al PIC, que es el centro de operaciones para el establecimiento de la comunicación entre el panel de alarma y la central, sin embargo se puede dar el caso de sobrecargas de corrientes, es por esta razón que se utilizó un circuito de control con un transistor que funciona como un "switch", esto con la intención de proteger al PIC, además se coloca una etapa de inversión luego del "switch" con la intención de asegurar la llegada de un estado lógico alto o bajo a los pines del PIC. El esquema para la decodificación implementado se presenta en la Figura 2.7.

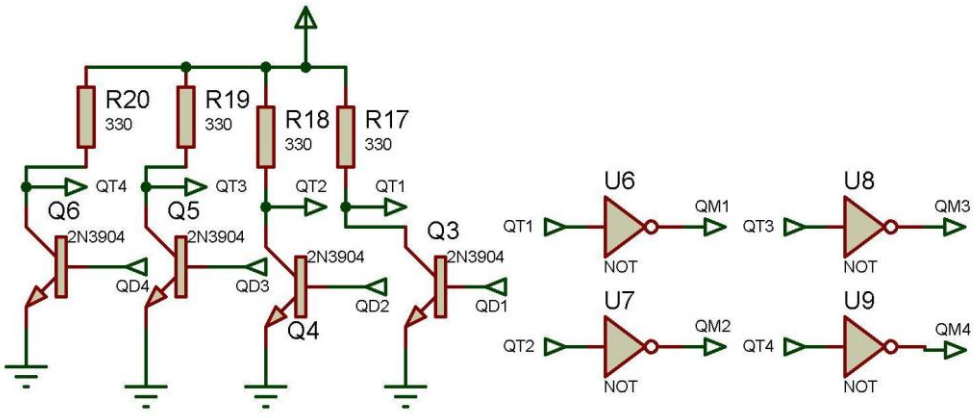


Figura 2.7: Esquema de control e inversión

2.1.3 CIRCUITO DE CONMUTACIÓN

El circuito de conmutación es el encargado de conectar los diferentes componentes del prototipo, como se observa en la Figura 2.8. El relé A es el encargado de enviar la señal de tono de marca hacia la alarma residencial y el relé B se encarga de enviar la señal de tierra para que se cierre el circuito. De igual manera el relé C es el encargado de enviar el tono de Handshake y de Kissoff y el relé D es el encargado de enviar la señal de tierra para que se cierre el circuito, cada relé es accionado por el PIC 16F877A.

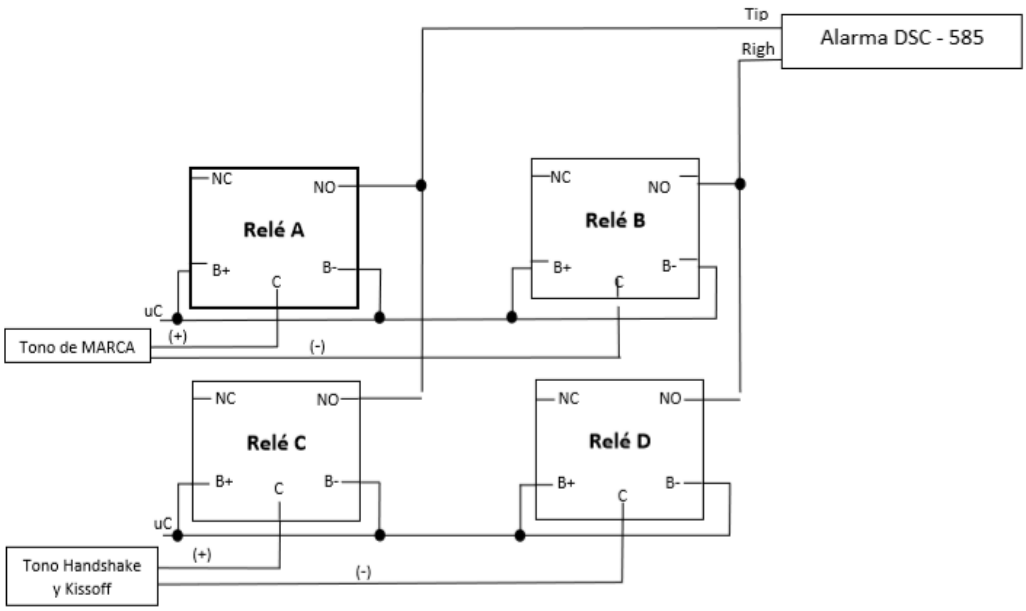


Figura 2.8: Diagrama del circuito de conmutación

2.1.4 CIRCUITO DE CONTROL

El circuito de control es el cerebro de todos los procesos que se realizarán, pues hace la función de una central telefónica para la comunicación con la alarma DSC-585, contiene todos los procesos que conlleva realizar la comunicación, es manipulada por la memoria RAM y la EPROM. El software utilizado para la elaboración del programa fue PIC C Compiler, este software cuenta con todas las librerías necesarias que nos ayudaron al diseño del programa.

Ante la ocurrencia de un evento el PIC 16F877A lo recibe inmediatamente, comprueba si el número recibido es correcto, en caso de no serlo lo rechaza. Cuando el número es correcto inmediatamente se activa el tono de Handshake, indicando a la alarma que ya puede enviar los dígitos de Contact ID.

Una vez recibidos los dígitos de Contact ID el PIC presentado en la Figura 2.9 procede a enviar el tono de Kissoff y se termina la comunicación entre la central y el panel de alarma.

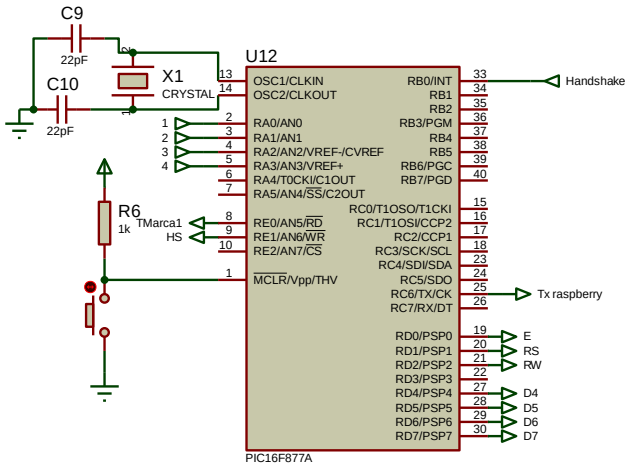


Figura 2.9: Circuito de control

El PIC 16F877A hace la función de una central telefónica para la comunicación con el panel de alarma, donde tenemos programadas las diferentes funciones que cumplirá antes, durante y después de la comunicación con la alarma. En la Figura 2.10 se muestra el diagrama de flujo para el control del prototipo.

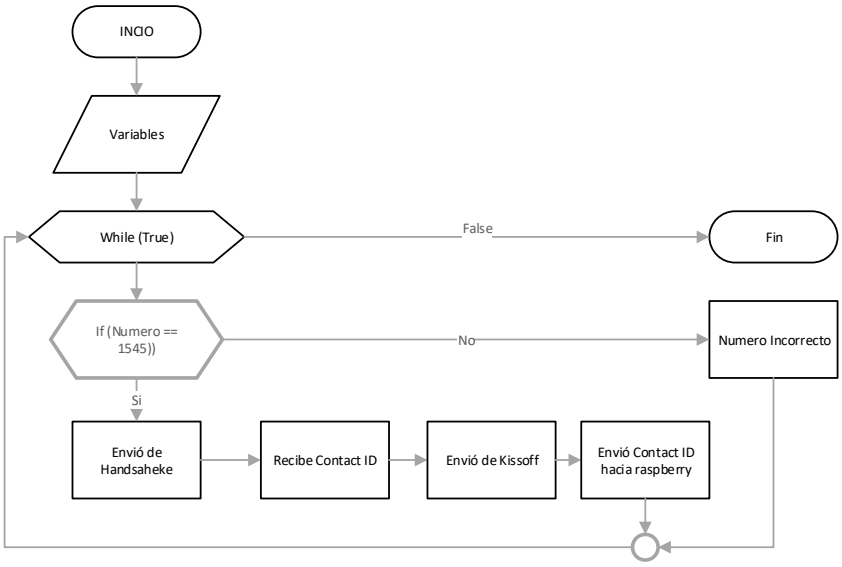


Figura 2.10: Diagrama de flujo de la memoria del prototipo.

2.1.5 COMUNICACIÓN SERIAL ENTRE MICROCONTROLADOR Y RASPBERRY PI 2

Para establecer la comunicación entre el microcontrolador y la Raspberry Pi 2, se utilizó el módulo de comunicación USART como se puede observar en la Figura 2.11, este módulo fue necesario ya que puede transmitir y recibir datos tanto en la Raspberry Pi 2 como en el microcontrolador, además del módulo USART se utilizó un circuito Nivelador de Voltaje, cuyo circuito se observa más adelante en la Figura 2.13.

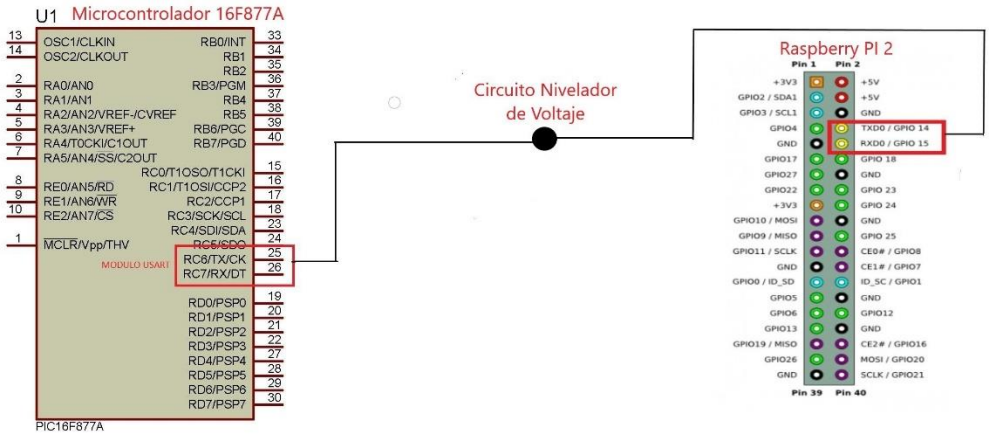


Figura 2.11 Comunicación serial PIC 16F877A y Raspberry Pi 2

2.1.5.1 MICROCONTROLADOR

Dentro del lenguaje de programación “PIC C Compiler” se utilizó la librería “#USE RS32”, esta librería contiene todos los parámetros necesarios para la configuración del módulo USART y establecer la comunicación serial. Para la ejecución de esta tarea, se realizó el siguiente procedimiento de programación correspondiente:

Algoritmo: Recepción y envió del protocolo Contact ID, recibida de una alarma residencial	
Paso 1:	*Inicializamos librerías* *Declaramos variables* *Inicializamos los puertos*
Paso 2:	*Lee el puerto para ver si hay información.* *Compara numero ingresado por la alarma es igual a (1545)*
Paso 3:	*Envió tono a 1400 Hz duración de 100ms* *Espera 100 ms* *Envió segundo tono 2300 Hz duración 100ms*
Paso 4:	*Recibe protocolo Contact ID* *Guarda el protocolo Contact ID*
Paso 5:	*Envió tono a 1400 Hz duración 350ms*

	Finaliza comunicación con Alarma Residencial.
Paso 6:	*Envió protocolo Contact ID hacia la raspberry.*

El programa Completo en C se le puede observar en el Anexo 2.

Para la comunicación de la Raspberry Pi 2 con el microcontrolador se usó el puerto C, el pin 25 para Tx y el pin 26 para Rx del microcontrolador como se observa en la Figura 2.12.

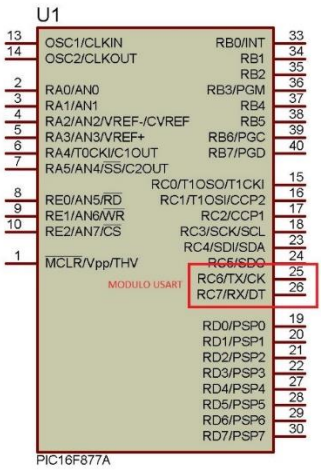


Figura 2.12: Modulo USART en el microcontrolador 16F877A

2.1.5.2 RASPBERRY PI 2

En la Raspberry Pi 2, para la programación se utilizó el software Python. Antes de iniciar el programa, se descarga la librería "python-serial", para ello se utiliza la siguiente línea de código en la consola de la raspberry.

$$pi@raspberrypi: \sim \ \$\ sudo\ apt - get\ install\ python - serial$$

Se abre la librería "import serial", posteriormente se abre el puerto correspondiente al módulo USART a una velocidad de 9600 baudios y se lo guarda en la variable "ser", estos pasos se puede observar en las siguientes líneas de código:

$$import\ serial$$
$$ser = serial.Serial('/dev/ttyAMA0', \quad baudrate\ = 9600)$$

Después de inicializar el puerto, se procede a usar la sentencia "*if"* y la función "*ser.inWaiting",*esta función cumple el procedimiento de leer el puerto a la espera

de nueva información, cuando existe algún dato en el puerto se lee por medio del comando "*ser.read(16)"* hasta 16 valores.

```
if ser.inWaiting > 0:
    msj += ser.read(16)
```

Cuando se recibe los 16 valores pertenecientes al protocolo Contact ID, se divide la información por el número de cuenta e información (apertura, código del evento, particiones y número de zona,) y se lo guarda en el vector AD. Para posteriormente enviarse al sistema de gestión desarrollado en la Universidad Politécnica Salesiana [36], como se indica en el siguiente código.

```
if ser.inWaiting > 0:
    msj += ser.read(16)
    cuenta = '#' + [1:5]
    infor = msj[7:11] + ' ' + msj[11:13] + ' ' + msj[13:16]
    even = "evento"
    AD = [cuenta, infor, even]
    lecturaEvento = False
    return AD
```

Y por último se borra toda la información que se haya guardado en el buffer y se cierra el puerto serial a la espera del próximo evento.

```
ser.reset_input_buffer( )
ser.flushInput( )
ser.setDTR( )
ser.close( )
```

2.1.5.3 CIRCUITO NIVELADOR DE VOLTAJE

Para establecer la comunicación entre el microcontrolador y la Raspberry Pi 2 se requiere que los niveles de voltajes sean iguales. En la Raspberry Pi 2 los niveles de tensión en los pines están comprendidos entre los +3.3v y 0v. El microcontrolador 16F877A los niveles de voltaje están comprendidos entre los +5V y 0V. Para ello es necesario realizar un circuito para nivelar los voltajes entre los 2 dispositivos electrónicos para que se pueda establecer la comunicación. En la Figura 2.13 se presenta el circuito nivelador de voltaje empleado.

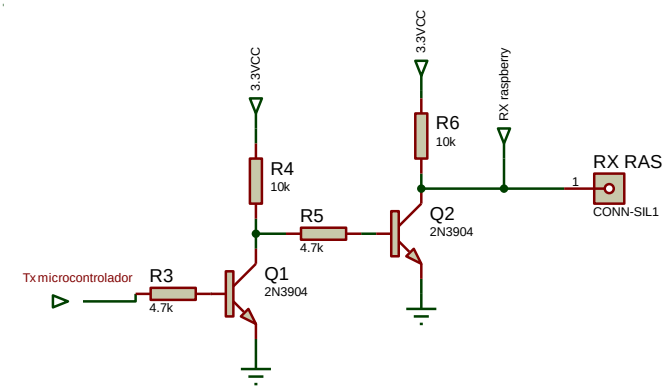


Figura 2.13: Circuito Nivelador de voltaje

Para el diseño del circuito se utilizó 2 transistores NPN configurados como interruptores, alimentados a la fuente de 3.3V, que es el voltaje de los niveles te tensión correspondiente a los pines de la Raspberry PI 2.

2.2 ELABORACIÓN DE LA PCB

2.2.1 DISEÑO DE LA PLACA

Para elaborar el circuito que funciona como central para la alarma DSC-585 utilizamos el software libre Proteus, versión 8.7. En el diseño se tomó en cuenta dos aspectos importantes que son: Elaborar un circuito de potencia en donde se tenga solo los valores de voltaje; alimentación de los elementos electrónicos y el de la alarma. El circuito para el flujo de datos que llegan desde la alarma a la central.

En esta parte también se realizó una ampliación al código del PIC, con el objetivo de poder visualizar los datos que llegan desde la alarma en una pantalla LCD, pudiendo así visualizar futuros problemas. Ver anexo 1.

También se realizó la implementación en 3D para la visualización de los elementos en la placa, que se indica en la Figura 2.14.

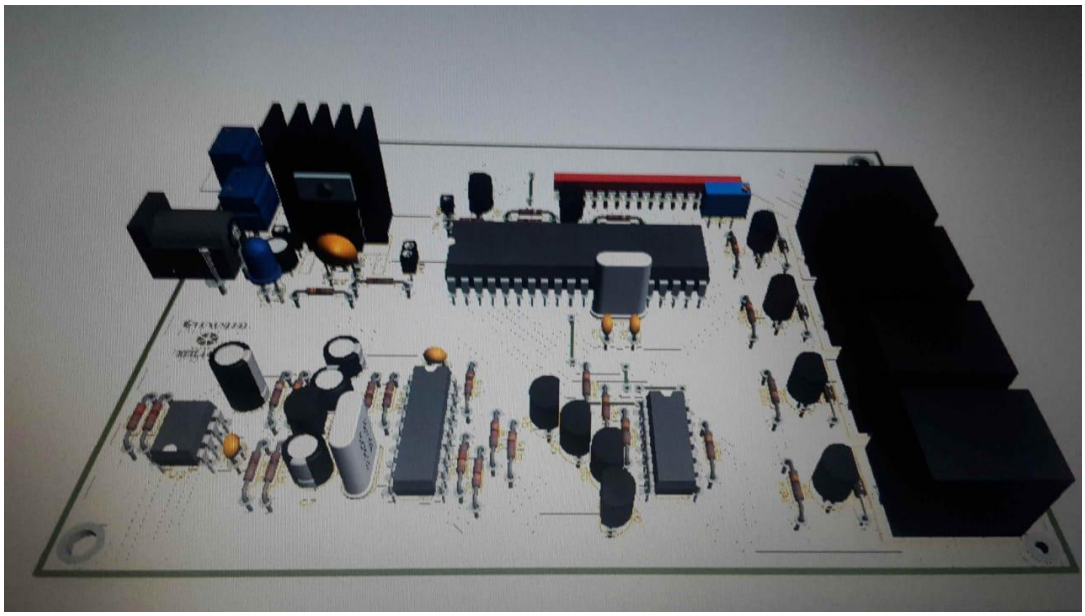


Figura 2.14: Simulación 3D del diseño de la placa del prototipo

2.2.2 IMPLEMENTACIÓN FÍSICA

Una vez realizado la simulación en el software libre Proteus se procedió al ensamblado físico de la placa, como se puede observar en la Figura 2.15.

Figura 2.15: Ensamblado de la PCB

2.3 SISTEMA DE GESTIÓN

El Sistema de Gestión se desarrolló en Java basado en un Prototipo de Sistema realizado por Integrantes del grupo de Investigación GITTEL de la Universidad Politécnica Salesiana [38], donde se realizaron las pruebas previas de validación para el funcionamiento del prototipo. Al Sistema de Gestión prototipo, se realizaron modificaciones en las interfaces con el objetivo que se adapte mejor a los avisos del panel de alarma DSC, así como a la recepción de tramas mediante Contact ID.

2.3.1 VENTANA DE TRÁFICO

La ventana de tráfico como se puede observar en la Figura 2.16, se visualizara todas las tramas que llegan al sistema de gestión (mensajes de Handshake, supervivencia y emergencia).

Además de los eventos también se visualizara la información del usuario tales como, el número de cuenta del usuario, la IP del prototipo que envía el evento, la fecha del evento, la hora y la trama de recepción.

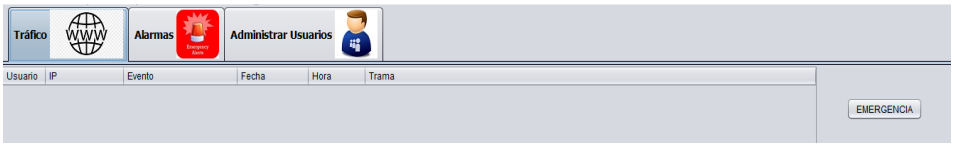


Figura 2.16: Ventana de tráfico [38]

2.3.2 VENTANA DE ALARMAS

El Sistema de Gestión tiene una ventana donde se visualizan todos los eventos de emergencia que llegan al sistema de monitoreo. En esta parte se registra los avisos o emergencias ocurridas en el panel de alarma de un usuario. La emergencia se mantiene con un color rojo hasta ser atendida, cuando se atiende la misma los avisos toman un color verde, esto se aprecia de mejor manera en las pruebas de funcionamiento, presentadas en el siguiente Capítulo.

Por otra parte hay un mensaje de aviso que es importante debido a que el panel de alarmas también envía el protocolo Contact ID cuando se presentan alteraciones físicas tales como el deterioro de la batería o algún daño interno, este mensaje de aviso se presenta con color amarillo.

En la ventana podemos visualizar el número de evento ocurrido, el número de usuarios, la descripción del evento, la zona vulnerada, la fecha de inicio del evento y la del final, además del estado (en espera o atendida). A esta venta se aumentó la opción de visualizar la zona donde ocurre el evento en un panel de alarma, como se puede apreciar en la Figura 2.17 [38].

Figura 2.17: Ventana de emergencia del Sistema de Gestión [38]

2.3.3 VENTANA DE EMERGENCIA

La ventana de emergencia recepta tres mensajes del protocolo Contact ID específicos, sin embargo para este trabajo se requiere receptar más mensajes y es por esto que se realiza una mejora a las líneas de código y la presentación de la ventana con el fin de poder visualizar todos los eventos del panel de alarma.

El Sistema de gestión está realizado en el software libre Java Netbeans y los datos de los usuarios y los eventos se guarda en una base de datos desarrollado en el software MySQL.

2.3.3.1 CONTACT ID RECEPTADO

Como ya se explicó en el Capítulo 1, el protocolo Contact ID que llega al sistema de gestión está dividido en cuatro partes, por esta razón con las siguientes líneas de comando separamos las partes para luego poder analizar el evento teniendo en cuenta cada una de ellas.

$$\text{this.calificador} = \text{contactId.subatring}(0, 1);$$
$$\text{this.codigoEvento} = \text{contactId.subatring}(1, 4);$$
$$\text{this.particion} = \text{contactId.subatring}(5, 7);$$
$$\text{this.ubicacionzona} = \text{contactId.subatring}(8, 11);$$

2.3.3.2 UBICACIÓN DEL EVENTO

Para determinar la ubicación exacta del evento en el panel, se dividió el protocolo Contact ID en partes. Primero se analiza la zona, teniendo en cuenta que el

panel DSC-585 utilizado tiene cuatro zonas. En la Figura 2.18 se presentan las zonas del panel de alarma.

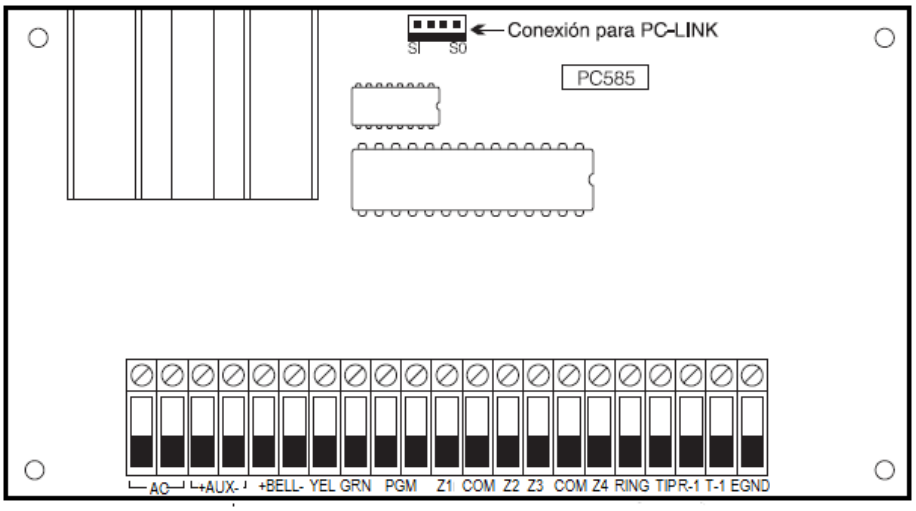


Figura 2.18: Ubicación de zonas en el panel de alarma

Las líneas de código para determinar la zona específica son:

```
switch (nuevaTrama.ubicacionZona)
case "001":
```

La zona especificada en las líneas de código presentada es 001 (zona 1), sin embargo también se programó las otras tres zonas.

Luego de determinar la zona, se analiza el número calificador que puede ser 1 o 3 dependiendo si es de apertura o cierre, según el evento suscitado.

```
switch (nuevaTrama.calificador)
case "1":
```

Si es que los dos casos anteriores se presentan en un evento se analizara el Contact ID con estas características.

```
switch (nuevaTrama.contactId)
case "1130 01 001":
```

Ahora bien si es que por ejemplo tenemos la zona dos y es un evento de cierre, es decir el calificador es tres se analiza otro Contact ID con esas características.

```
switch (nuevaTrama.contactId)
case "3130 01 002":
```

De esta manera en el Sistema de Gestión se realizó la creación de líneas de comando con todos los Contact ID que envía el panel de alarma DSC-585. Para determinar los posibles eventos y los más comunes se tomó en cuenta la información

de la Tabla 1.2, en donde se tiene algunos de los posibles mensajes de aviso o emergencia que puede enviar el panel.

La ventana de emergencia se presenta en la Figura 2.19, en donde se puede observar detalles como la descripción del evento y la zona específica del panel de alarma.

Figura 2.19: Ventana de emergencia [38]

2.3.4 VENTANA DE ADVERTENCIA

Los mensajes de advertencia del panel de alarma son diferentes a los de emergencia, pues en casos específicos el panel de alarma envía mensajes de protocolo Contact ID con notificaciones de aspectos físicos como por ejemplo cuando la batería esta baja.

case "1406 01 000":

Por esto se realizaron mejoras a las líneas de código, ya que por ejemplo para este caso la zona será de valor 000, pues no hay violación de las mismas.

Se realizó cambios a la ventana de emergencia con el objetivo de visualizar de manera diferente los mensajes al recibir un evento de advertencia, para esto se mejoró la presentación de la ventana como se puede observar en la Figura 2.20.

Figura 2.20: Ventana de advertencia

CAPÍTULO 3: IMPLEMENTACIÓN Y ANÁLISIS DE RESULTADOS

3.1 TOPOLOGÍA DE PRUEBAS

Las pruebas de funcionamiento del prototipo se realizaron en primera instancia en una red LAN como se puede observar en la Figura 3.1. Se conectó la alarma residencial mediante las borneras RING y TIP al prototipo, y con un cable Ethernet a un router residencial. Al mismo router se conectó una PC con el Sistema de Gestión.

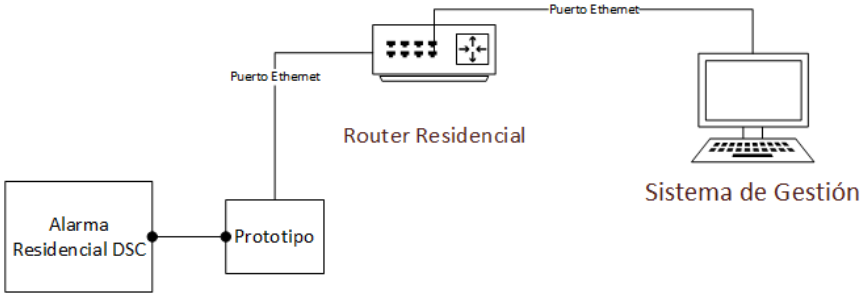


Figura 3.1: *Topología de la red LAN para pruebas*

3.2 VIOLACIÓN DE ZONAS

El prototipo es probado con una alarma residencial DSC-585, como se observa en la Figura 3.2.

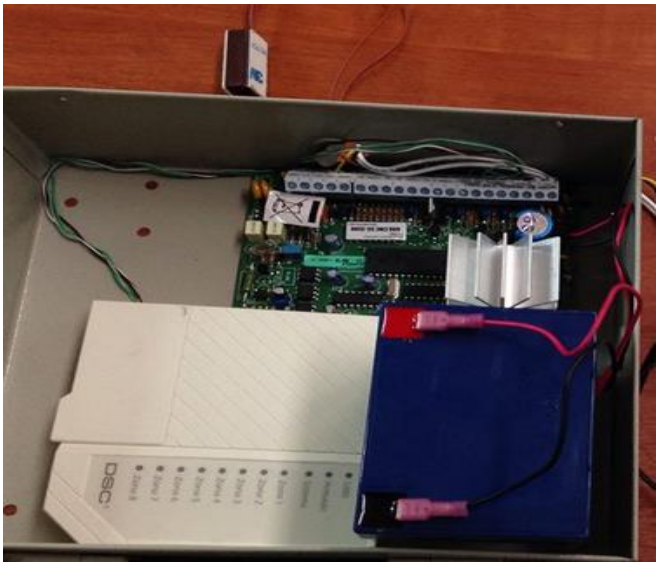


Figura 3.2: Kit alarma DSC-585 básico

Cuando se activa alguna zona, el panel detecta la zona afectada e inmediatamente toma la línea telefónica interna de la alarma, y se comunica con el prototipo, marcando el número “1545”, este número pertenece al prototipo como se indica en la Figura 3.3.

Figura 3.3 Marcación de la alarma hacia el prototipo

3.3 RECEPCIÓN DEL PROTOCOLO CONTACT ID

Una vez establecida la comunicación entre el prototipo y el panel de alarma, el prototipo responde la llamada de la alarma con un saludo o tono Handshake, este tono está compuesto por una serie de 2 tonos, el primer tono es de 1400Hz y el segundo de 2300Hz, con un espacio de tiempo entre los 2 de 100ms.

Después que el panel de la alarma recibe la señal de saludo por parte del prototipo, este procede a enviar los tonos DTMF o señales pertenecientes al Contact ID, como se puede apreciar en la Figura 3.4.

Se realizaron las pruebas con varios eventos posibles.

3.3.1 PRIMERA PRUEBA DE FUNCIONAMIENTO

Figura 3.4: Protocolo Contact ID (apertura de zona)

Como se observa en la Figura 3.4, se tiene el protocolo Contact ID, esta información esta subdividida en 7 grupos de datos que se describe a continuación:

1. 1234: Número de cuenta del usuario.
2. 18: Corresponde al protocolo Contact ID.
3. 1: Apertura en la zona.
4. 130: Código del evento, “alarma en la zona”.
5. 01: Particiones de la zona.
6. 002: El evento se realizó en la zona 2.
7. 8: CheckSum.

3.3.2 SEGUNDA PRUEBA DE FUNCIONAMIENTO

Figura 3.5: Protocolo Contact ID (Alerta de fuego)

En la Figura 3.5, se tiene un evento diferente, en este caso se pulso el botón “F” del teclado del panel de alarma donde se tiene la siguiente información:

1. 1234: Número de cuenta del usuario.
2. 18: Corresponde al protocolo Contact ID.
3. 1: Apertura en la zona.
4. 150: Código del evento, “Alerta de Fuego”.
5. 01: Particiones de la zona.
6. 000: No existe zona activa en el panel, por lo que se activó el botón de pánico “F” del teclado.
7. 8: CheckSum.

Al finalizar la recepción de todas las señales del Contact ID. El prototipo procede a enviar una señal o tono Kissoff, este tono está a una frecuencia de 1400Hz. El propósito de esta señal de Kissoff es para confirmar que se recibió el Contact ID y también para finalizar la comunicación entre los 2 equipos como se observa en la Figura 3.6.

Figura 3.6: Finalización de la comunicación entre el panel de alarma y prototipo

3.4 ENVIO DE CONTACT ID HACIA EL SISTEMA DE GESTIÓN

Después de recibir el Contact ID, esta información se envía hacia una Raspberry Pi 2 que es la encargada de convertir la información en una trama para su envió hacia el Sistema de Gestión como se observa en la siguiente Figura 3.7.

```
<x0A>D8360037"ADM-CID"0001Rb827ebLla3f7c#000001[#000001|1130 01 002]<x0D>
<x0A>D8360037"ADM-CID"0001Rb827ebLla3f7c#000001[#000001|1130 01 002]<x0D>
```

Figura 3.7: Contact ID convertida en trama

La trama está constituida como se presenta en la Tabla 1.

<x0A>	Inicio de la trama
D836	CRC
0037	Longitud de la trama
“ADM-CID”	Mensaje tipo Contact-ID
0001	Numero de secuencia del mensaje
Rb827ebLla3f7c	Número del receptor
#000001	Numero de línea
[#00001|1130 01 002]	[Número de cuenta del usuario | información del Contact ID]
<x0D>	fin de la trama

Tabla 3.1: Trama enviada al Sistema de Gestión.

3.5 PRUEBAS CON EL SISTEMA DE GESTIÓN

3.5.1 PRUEBAS DESDE LA RASPBERRY PI 2 HACIA EL SISTEMA DE GESTIÓN

La comunicación entre la Raspberry Pi 2 y el Sistema de Gestión es a través de tramas de Handshake, supervivencia y emergencia. Para establecer la comunicación entre el dispositivo y el Sistema de Gestión, la Raspberry Pi 2 envía una trama de

Handshake, y como respuesta obtiene una trama de ACK. En la Figura 3.8 se puede observar el envío y recepción de tramas.

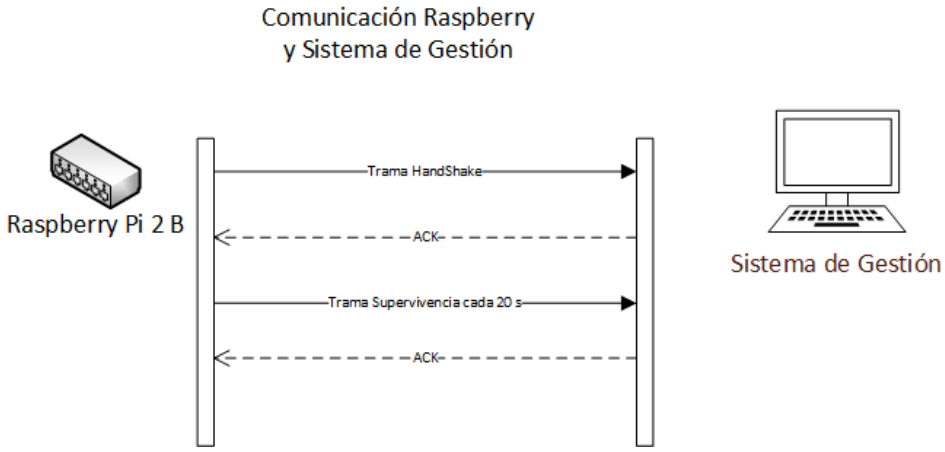


Figura 3.8: Envió y recepción de tramas Handshake y Supervivencia entre Raspberry Pi 2 y Sistema de Gestión.

Envió trama de Handshake desde la Raspberry Pi 2.

```
<x0A>E1F60021"NULL"0000Rb827ebL1a3f7c#12345A[]<x0D>
<x0A>E1F60021"NULL"0000Rb827ebL1a3f7c#12345A[]<x0D>
INFO:AlarmaSocket:Enviado peticion ...
<x0A>E1F60021"NULL"0000Rb827ebL1a3f7c#12345A[]<x0D>
```

El término “NULL” significa que es un mensaje de Handshake ó supervivencia, es decir no hay un evento en el panel de alarma, pues en ese caso en la trama se presenta el término “ADM-CID” que significa que hay un protocolo Contact ID.

Respuesta del Gestor (ACK)

```
INFO:AlarmaSocket:Leyendo respuesta:
<x0A>AA860020"ACK"0000Rb827ebL1a3f7c#000001[]<x0D>
INFO:AlarmaSocket:Cerrando Socket...
```

3.5.1.1 SUPERVIVENCIA

Luego de establecer la comunicación entre la Raspberry Pi 2 y el sistema de Gestión. La Raspberry Pi 2 empezara a enviar tramas de supervivencia

Esta trama es enviada cada 30 segundos, con el propósito de mantener la comunicación. Cuando esta conexión se pierda, la trama recibida será diferente a la enviada y entonces la Raspbery Pi 2 volverá a enviar mensajes de Handshake hasta

reestablecer la comunicación. Esta trama no contiene ninguna información en su interior, ya que son tramas de supervivencia.

Envió de trama de supervivencia de la Rapsberry Pi 2 hacia el Sistema de Gestión:

```
INFO:AlarmaSocket:Ok...
<x0A>09E40021"NULL"0000Rb827ebL1a3f7c#000001[]<x0D>
<x0A>09E40021"NULL"0000Rb827ebL1a3f7c#000001[]<x0D>
INFO:AlarmaSocket:Enviado peticion ...
<x0A>09E40021"NULL"0000Rb827ebL1a3f7c#000001[]<x0D>
```

Respuesta del Sistema de Gestión hacia la Raspberry Pi 2 (ACK)

```
INFO:AlarmaSocket:Leyendo respuesta:
<x0A>AA860020"ACK"0000Rb827ebL1a3f7c#000001[]<x0D>
INFO:AlarmaSocket:Cerrando Socket...
```

3.5.1.2 EMERGENCIA

La trama de emergencia se genera inmediatamente al producirse un evento en el panel de alarma, esta trama lleva en su interior el protocolo Contact ID del evento producido, y es enviada inmediatamente hacia el gestor o central de monitorio.

Envió de la trama emergencia desde la Rapsberry Pi 2:

```
INFO:AlarmaSocket:Ok...
<x0A>D8360037"ADM-CID"0001Rb827ebL1a3f7c#000001[#000001|1130 01 002]<x0D>
<x0A>D8360037"ADM-CID"0001Rb827ebL1a3f7c#000001[#000001|1130 01 002]<x0D>
INFO:AlarmaSocket:Enviado peticion ...
<x0A>D8360037"ADM-CID"0001Rb827ebL1a3f7c#000001[#000001|1130 01 002]<x0D>
```

Cuando la trama de emergencia haya llegado a su destino (Sistema de Gestión). El Sistema enviara un ACK de confirmación que llego correctamente la trama:

```
INFO:AlarmaSocket:Leyendo respuesta:
<x0A>3FDB0020"ACK"0001Rb827ebL1a3f7c#000001[]<x0D>
INFO:AlarmaSocket:Cerrando Socket...
```

3.5.2 PRUEBAS DESDE EL SISTEMA DE GESTIÓN HACIA LA RASPBERRY PI 2

3.5.2.1 HANDSHAKE

La trama de Handshake llega al Sistema de Gestión Una vez comprobado se reenvía un mensaje ACK de respuesta hacia la Raspberry Pi 2 quien a su vez vuelve a enviar un mensaje de supervivencia o emergencia según sea el caso.

Recibida

```
<x0A>E1F60021"NULL"0000Rb827ebL1a3f7c#12345A[]<x0D>
```

Respuesta (ACK)

```
HAND SHAKE><x0A>AA860020"ACK"0000Rb827ebL1a3f7c#000001[]<x0D><
```

3.5.2.2 SUPERVIVENCIA

Este mensaje llega para comprobar la comunicación entre el Sistema de Gestión y el servidor, el tiempo para él envió de cada mensaje es de 20s, en caso superar el tiempo se pierde la comunicación.

Recibida

```
<x0A>09E40021"NULL"0000Rb827ebL1a3f7c#000001[]<x0D>
```

Respuesta (ACK)

```
ACK><x0A>AA860020"ACK"0000Rb827ebL1a3f7c#000001[]<x0D><
```

3.5.2.3 EMERGENCIA

Este mensaje llega cuando se presenta un evento en al panel de alarma DSC-585.

Recibida

```
<x0A>48370037"ADM-CID"0001Rb827ebL1a3f7c#000001[#000001|1130 01 003]<x0D>
```

Respuesta (ACK)

```
ACK><x0A>3FDB0020"ACK"0001Rb827ebL1a3f7c#000001[]<x0D><
```

3.6 PRUEBAS CON EL PROTOTIPO ENSAMBLADO

3.6.1 PROTOTIPO EN COMUNICACIÓN CON EL SISTEMA DE GESTIÓN

Luego de recibir los mensajes de Handshake y supervivencia en el Sistema de Gestión, se mantienen en comunicación constante con el usuario. En el prototipo esto

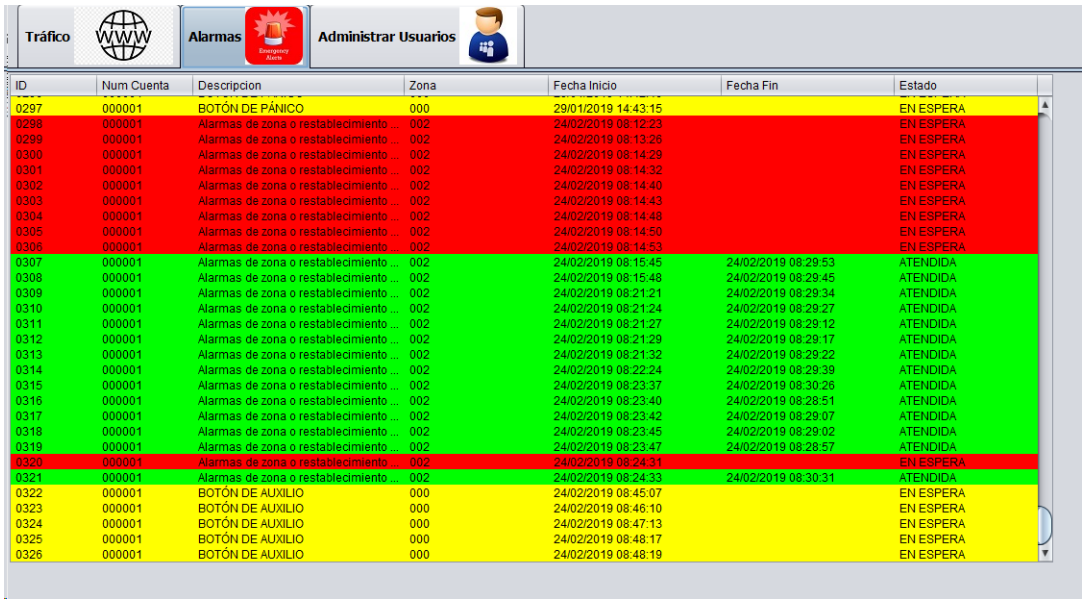
se visualiza mediante una señal luminosa de aviso llamado Sistema de Gestión, este led de color verde indica que el sistema está conectado y permanece con parpadeo constante mientras no se produzca una emergencia. En la 3.9 se presenta una imagen del prototipo conectado al Sistema de Gestión.

Figura 3.9: Comunicación entre usuario y Sistema de Gestión

3.6.2 VISUALIZACIÓN DE EMERGENCIA EN EL PROTOTIPO

Al momento de suscitarse una emergencia en el panel de alarma como por ejemplo la violación de un sensor magnético, en el prototipo se visualiza la emergencia mediante un led de color rojo y a la vez en el Sistema de Gestión se presenta la ventana emergencia (Figura 2.18).

Los eventos se almacenan en la ventana de alarmas como se observa en la Figura 3.10. Los eventos de emergencia se observan de color rojo, mientras que los ya atendidos se observan de color verde, además cuando el evento es una simple advertencia del panel de alarma se visualiza con color amarillo.



ID	Num Cuenta	Descripcion	Zona	Fecha Inicio	Fecha Fin	Estado
0297	000001	BOTÓN DE PÁNICO	000	29/01/2019 14:43:15		EN ESPERA
0298	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:12:23		EN ESPERA
0299	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:13:26		EN ESPERA
0300	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:14:29		EN ESPERA
0301	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:14:32		EN ESPERA
0302	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:14:40		EN ESPERA
0303	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:14:43		EN ESPERA
0304	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:14:48		EN ESPERA
0305	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:14:50		EN ESPERA
0306	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:14:53		EN ESPERA
0307	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:15:45	24/02/2019 08:29:53	ATENDIDA
0308	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:15:48	24/02/2019 08:29:45	ATENDIDA
0309	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:21:21	24/02/2019 08:29:34	ATENDIDA
0310	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:21:24	24/02/2019 08:29:27	ATENDIDA
0311	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:21:27	24/02/2019 08:29:12	ATENDIDA
0312	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:21:29	24/02/2019 08:29:17	ATENDIDA
0313	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:21:32	24/02/2019 08:29:22	ATENDIDA
0314	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:22:24	24/02/2019 08:29:39	ATENDIDA
0315	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:23:37	24/02/2019 08:30:26	ATENDIDA
0316	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:23:40	24/02/2019 08:28:51	ATENDIDA
0317	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:23:42	24/02/2019 08:29:07	ATENDIDA
0318	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:23:45	24/02/2019 08:29:02	ATENDIDA
0319	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:23:47	24/02/2019 08:28:57	ATENDIDA
0320	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:24:31		EN ESPERA
0321	000001	Alarmas de zona o restablecimiento ...	002	24/02/2019 08:24:33	24/02/2019 08:30:31	ATENDIDA
0322	000001	BOTÓN DE AUXILIO	000	24/02/2019 08:45:07		EN ESPERA
0323	000001	BOTÓN DE AUXILIO	000	24/02/2019 08:46:10		EN ESPERA
0324	000001	BOTÓN DE AUXILIO	000	24/02/2019 08:47:13		EN ESPERA
0325	000001	BOTÓN DE AUXILIO	000	24/02/2019 08:48:17		EN ESPERA
0326	000001	BOTÓN DE AUXILIO	000	24/02/2019 08:48:19		EN ESPERA

Figura 3.10: Lista de emergencias en el Sistema de Gestión.

3.7 PRUEBAS DE TIEMPO DE RESPUESTA ANTE UNA EMERGENCIA A TRAVEZ DE LA NUBE

Se realizaron varias pruebas de funcionamiento con el prototipo y el Sistema de Gestión. La topología de pruebas se muestra en la Figura 3.11. El prototipo se lo ubico en la ciudad de Cuenca y el Sistema de Gestión en el cantón Gualaceo. Para la comunicación se utilizó un túnel de comunicación Open VPN con sockets.

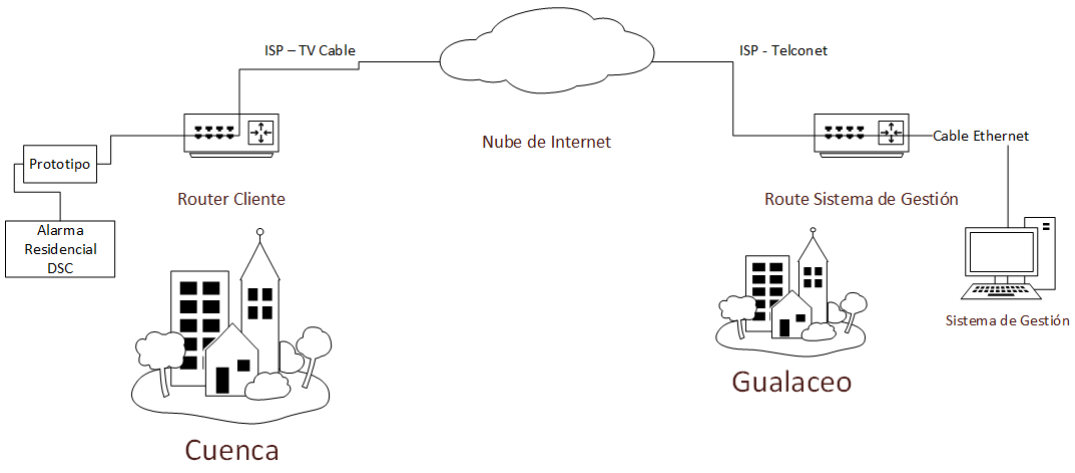


Figura 3.11: Pruebas de funcionamiento con Open VPN

Se realizó pruebas para determinar el tiempo de respuesta de la red VPN por medio de un ping en diferentes horarios del día, los 7 días de la semana. En la Figura 3.12 se muestra una prueba de ping realizado desde el sistema de gestión hacia el

prototipo, se realizó en un horario establecido donde no existe congestión de tráfico en la red.

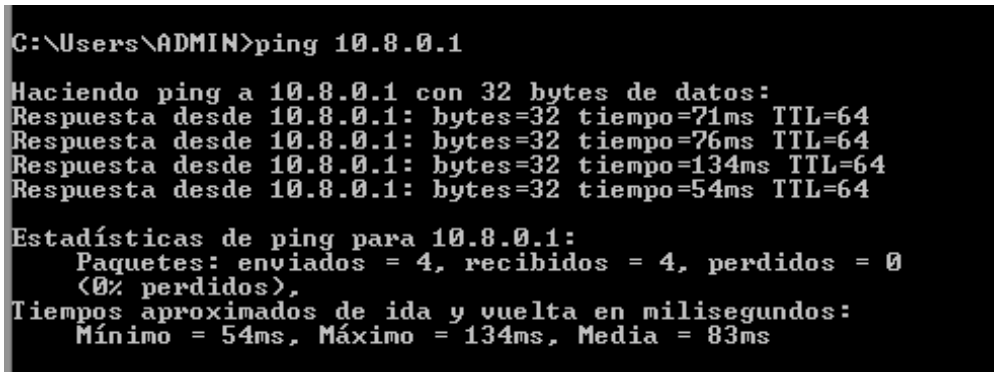


Figura 3.12: Ping desde el Sistema de Gestión hacia el prototipo sin tráfico en la red.

Posteriormente se realizaron las pruebas de establecimiento de comunicación de la red VPN, con el mayor tráfico posible de la red en un hogar, obteniendo los resultados presentados en la Figura 3.13, donde se puede apreciar que el tiempo de respuesta es mayor pues el promedio está en 1,6 segundos, considerando que no existe perdidas de paquete como se observa.

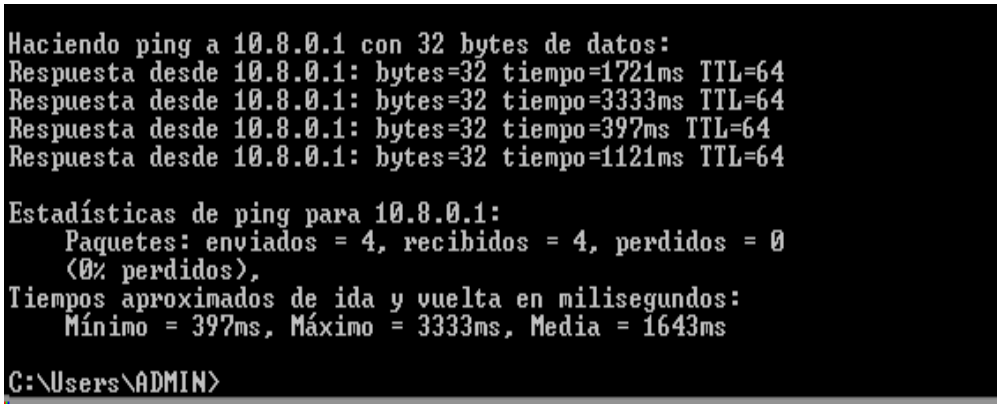


Figura 3.13: Ping desde el Sistema de Gestión hacia el prototipo sin tráfico en la red

Posteriormente de realizar las pruebas de tiempo de comunicación de la red VPN en diferentes horas picos, durante una semana de usos normal de la red domiciliaria se obtuvieron los siguientes resultados que se muestra en la Figura 3.14.

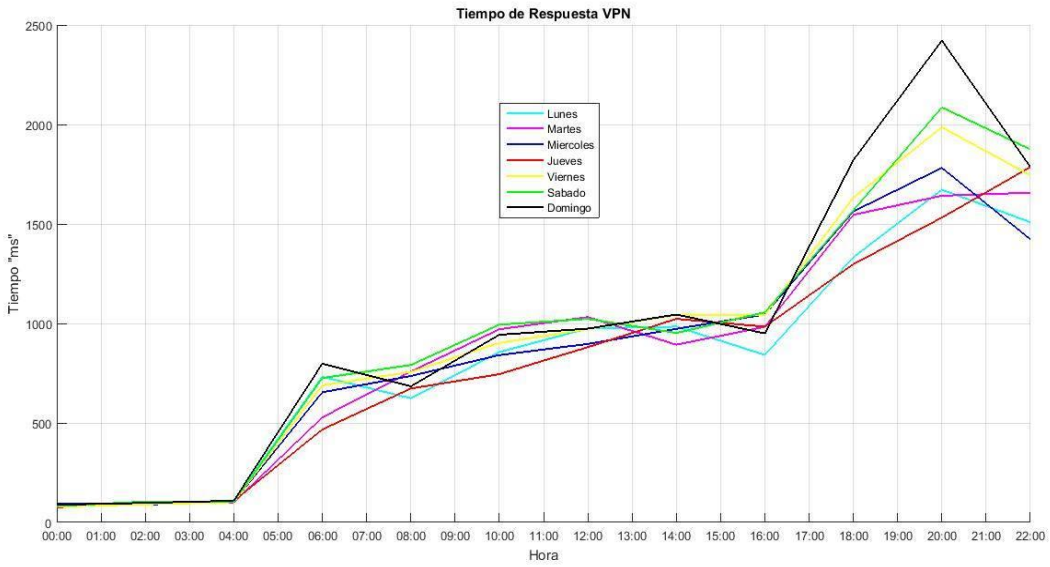


Figura 3.14: Pruebas de comunicación de la red VPN.

En las horas pico con mayor tráfico ocurre en la noche, ya que por lo general la mayor parte de las personas pasan en sus hogares y por ende el tiempo de comunicación de la red VPN aumenta. La variación de los tiempos depende también del modelo de la Raspberry Pi 2, para este caso se utilizó una Raspberry Pi 2 con la cual según [39] tenemos un QoS aceptable del prototipo, y por lo tanto no se dan perdidas de información.

Después de realizar las pruebas de la red VPN, se realizaron las pruebas de respuesta del prototipo, desde que ocurre un evento hasta el Sistema de Gestión. De igual manera las pruebas se las realizaron en diferentes horas del día en un lapso de 7 días.

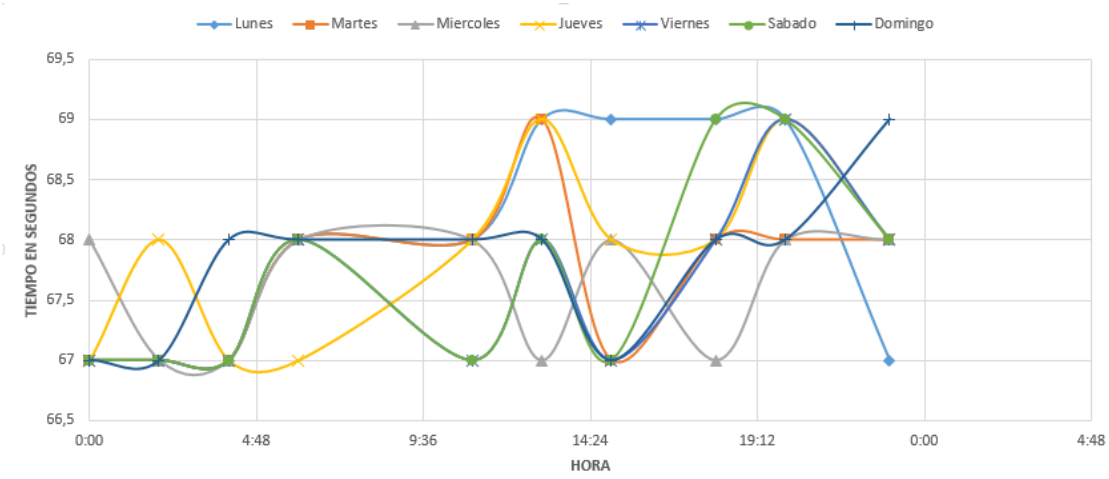


Figura 3.15: Pruebas de tiempos de comunicación del prototipo.

Como se observa en la Figura 3.15, el tiempo real de respuesta es aproximadamente de 67 segundos sin tráfico en la red y de 69 segundos con mayor tráfico en la red, este tiempo puede variar debido a las condiciones diferentes que tiene cada usuario.

Figura 3.16: Pruebas de comunicación con el Sistema de Gestión.

En la Figura 3.16. Se observa el evento que llega al Sistema de Gestión para las pruebas de los tiempos.

Según las pruebas realizadas se estima que el ancho de banda requerido para la comunicación entre el prototipo y el Sistema de Gestión es de 1 Mbps pues el tiempo de respuesta es el mismo cuando se presenta tráfico en la red de TV Cable y Telconet

ubicados en la ciudad de Cuenca y Gualaceo respectivamente como se observa en la Figura 3.11.

3.8 VALIDACIÓN DEL PROTOTIPO

El prototipo fue presentado en una institución educativa de la ciudad de Gualaceo. En el colegio Unidad Educativa Gualaceo se presentó el prototipo ante las autoridades institucionales y estudiantes de las menciones en electrónica de segundo y tercero de bachillerato. En el Anexo 3 se presentan imágenes de la validación.

3.9 ANÁLISIS FINANCIERO

El prototipo desarrollado en este trabajo es adaptable para todos los paneles de alarma que posean en su configuración el protocolo Contact ID y tiene un costo accesible para todos los usuarios pues no sobrepasa los 100 dólares. En este apartado se detalla la vida útil del prototipo realizando una proyección de 0 a 5 años con el fin de determinar los beneficios económicos del mismo al realizar una fabricación y comercialización del dispositivo.

3.9.1 INVERSIÓN

Para realizar el proyecto se plantea contar con un capital de 20000 dólares, los mismos que serán adquiridos mediante un préstamo a una institución financiera a un plazo de dos años con un interés del 12,77% anual.

PRESTAMO	
Segmento de Crédito	Consumo Ordinario
Tipo de Crédito	Crédito con Ahorro 12,77%
Tabla de Amortización	Cuota Decreciente (Alemán)
Monto Solicitado/Financiado	20000
Monto Liquidado	20000
Plazo (meses)	24
Tasa Referencial del BCE	17,30%
Tasa Nominal Anual *	12,77%
Tasa Efectiva Anual	13,55%
Tasa Anual del Costo del Crédito	13,79%
Seguro Desgravamen **	50
Aporte en Reservas **	200
Interés Generado **	2660,42
Total de Carga Financiera	2910,42
Suma Total **	22910,42
CUOTA POSIBLE **	944,1

Tabla 3.2: Valores estimados para realizar un préstamo

3.9.2 GASTOS OPERACIONALES Y GASTOS CAPITALES (OPEX Y CAPEX)

El tiempo estimado de duración del proyecto es de cinco años, por lo cual se realiza una proyección de gastos operacionales (Opex) y gastos capitales (Capex). Para el primer caso se toma en cuenta los gastos para el mantenimiento durante la vida útil del proyecto, estos valores por lo general se mantienen fijos. En el segundo caso se plantean los gastos que se realizan durante la vida del proyecto, dichos gastos están relacionados con los elementos requeridos para la fabricación del prototipo como la Raspberry y los elementos electrónicos, estos valores fluctúan durante el periodo planteado.

GASTOS DE CAPITAL Y GASTOS OPERATIVOS							
	AÑO 0	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**	**TOTAL 5 AÑOS**
OPEX							
Publicidad	2640	2640	240	240	240	240	6240
Transporte	1800	1800	1800	1800	1800	1800	10800
Servicios Básicos	6060	6060	6060	6060	6060	6060	36360
Mano de obra	18960	18960	18960	18960	18960	18960	113760
Mantenimiento Equipos	-	-	-	-	-	960	960
TOTAL	**10500**	**10500**	**8100**	**8100**	**8100**	**28020**	**168120**
CAPEX							
Equipos y Herramientas	1525	-	-	-	-	-	1525
Insumos para Prototipo	4830	11107,9545	23522,72727	14375	17250	18400	89485,68182
Kit Alarma DSC 585 básico	6820	11550	15950	14300	17600	19800	86020
TOTAL	**13175**	**22657,9545**	**39472,72727**	**28675**	**34850**	**38200**	**177030,6818**
TOTAL GASTOS							**345150,6818**

Tabla 3.3: Valores de Gastos de capital y Operativos proyectado para 5 años

Los gastos operativos tienen un valor menor en comparación de los gastos de capital, pues al ser fijos no tienen variación significativa durante el periodo planteado, ya que se planea empezar con un equipo de trabajo fijo y específico para cada labor requerida en el proyecto durante el periodo de vida del mismo. Por el contrario en el otro caso los valores de adquisición de elementos y materiales para el prototipo como la Raspberry Pi 2, el kit DSC-585 (panel de alarma, batería, teclado y sensores) y los elementos electrónicos varían con el pasar de los meses y los años, esto hace que los gastos del proyecto sean más significativos.

También es importante mencionar que los equipos y herramientas adquiridos durante el año cero del proyecto deben tener un tiempo de vida estimado en cinco

años, por lo cual no será necesario remplazarlos, esto se puede observar en la Tabla 3.3 en donde solo se cuenta con el primer valor de Capex y los demás años están en blanco.

En el periodo planteado para la duración del proyecto en el cual se pretende crear prototipos adaptables a las alarmas residenciales se estima tener gastos operacionales y gastos de capital valorados en aproximadamente 345150,68 dólares.

3.9.3 FLUJO DE CAJA

Los valores presentados en la Tabla 3.4 representan los egresos e ingresos que va tener el proyecto mes a mes y año tras año a partir del año cero hasta el año 5. Los valores planteados se obtuvieron mediante la proyección de ventas de la alarma residencial básica DSC-585, el prototipo desarrollado en sí y el prototipo más la alarma residencial básica DSC-585.

VALORES POR AÑO			
AÑOS	**INGRESOS POR AÑO**	**EGRESOS POR AÑO**	**FLUJO TOTAL POR AÑO**
0	35565,91	58198,28455	-22632,37455
1	45726	51835,09	-6109,09
2	61507,62545	60582,72727	924,8981818
3	63339,89818	49435	13904,89818
4	136274,8982	71610	64664,89818
TOTALES	**342414,3318**	**291661,1018**	**50753,23**

Tabla 3.4: Flujo de caja proyectado para 5 años

Los primeros años se obtienen valores negativos en el flujo de caja, pues se estima que las ventas crecerán de manera exponencial a partir del año dos. Uno de los factores que influyen de manera negativa en los primeros años es el pago del préstamo, sin embargo una vez superado esta brecha económica los números tienden a crecer, pues en el año cinco se tiene un valor de 64664,89 dólares lo cual representa una ganancia sustancial para los inversionistas del proyecto.

3.9.4 ANÁLISIS DEL VAN Y TIR

El valor actual neto (VAN) representa la ganancia económica que obtendrá el inversionista del proyecto luego de cumplirse el tiempo de vida del mismo. La tasa interna de retorno (TIR) es el valor en el cual el VAN se hace cero y además debe ser mayor al porcentaje establecido como costo de oportunidad del proyecto.

Para obtener los valores del VAN y el TIR se aplican las siguientes formulas.

$$VAN = \sum_{n=1}^{N} \frac{Q_n}{(1+i)^n} - I_0$$ Ecuación (5)

$$TIR = \sum_{n=1}^{N} \frac{Q_n}{(1+i)^n} - I_0 = 0$$ Ecuación (6)

Los términos utilizados son:

Q_n Es el flujo de caja.

i Es la tasa descuento.

I_0 Es la inversión en el periodo cero.

n Es el tiempo de vida útil del proyecto.

Factibilidad del proyecto		
Costo de oportunidad %	10	
VAN	$ 26.085,78	RENTABLE
TIR	69%	
B/C	1,174014394	SE ACEPTA EL PROYECTO
PRI	1,215030079	AÑOS

Tabla 3.5: Valores que garantizan la factibilidad del proyecto

El costo de oportunidad planteado para el proyecto es de un 10%, con los cual se obtiene un VAN de 92572,28 dólares, es un valor mayor a cero por lo que se garantiza que el proyecto es rentable, además se debe tener en cuenta que es una ganancia considerable con respecto al tiempo estimado para la vida útil del proyecto.

Por otra parte el valor para el TIR calculado es de un 69% con lo cual se comprueba que el proyecto es rentable, pues representa un porcentaje mucho más grande en comparación al porcentaje del costo de oportunidad.

3.9.5 RELACIÓN BENEFICIO COSTO

La relación beneficio costo (B/C) representa la relación entre los ingresos que percibe el proyecto y los egresos que genera el mismo incluyendo el valor de inversión, es así que si este valor es menor a cero se recomienda no invertir en el

proyecto y si el mismo es mayor a cero, el proyecto es rentable. En la Tabla 3.5 podemos apreciar que la relación B/C para el proyecto del prototipo para las alarmas residenciales es de 1,17 valor que garantiza la rentabilidad del proyecto.

3.9.6 PERIODO DE RECUPERACIÓN DE LA INVERSIÓN

El periodo de recuperación de la inversión (PRI) es el valor que indica el tiempo en años en el cual el inversionista podrá recuperar el monto invertido en el proyecto. En la Tabla 3.5 se obtiene un valor para el PRI de 1,21 años, lo cual coincide con los valores del flujo de caja presentado en la Tabla 3.4 en donde se puede ver que en el año cero y año uno se obtiene valores negativos, sin embargo a partir del año dos se visualizan ganancias positivas, es así que el PRI obtenido indica que a partir del año uno más aproximadamente dos meses el inversionista recupera la inversión y empieza a percibir ganancias.

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- El panel de alarma básico DSC-585 usa la marcación por tonos DTMF para establecer comunicación y envió del protocolo Contact ID. Por lo que en este trabajo se presenta un prototipo para receptar el dicho protocolo y posteriormente enviarlo a través de un túnel VPN hacia un Sistema de Gestión.

- El tiempo de respuesta del evento desde la activación de una zona en el panel de alarma hacia el sistema de Gestión tiene un estimado de 68 segundos, estos tiempos analizados se pudieron puede observar en la Figura 3.15. Los cuales representan tiempos aceptables de respuesta para la atención de una emergencia, en comparación con los dispositivos propietarios.

- En el diseño del prototipo fue necesario el uso del circuito integrado 74LS04 para él envió de datos desde el decodificador MT88L70 hacia el microcontrolador. El funcionamiento principal de este integrado es asegurar que le llegue al microcontrolador un valor lógico de 0 ó 1 y no haya alteración en la información del protocolo Contact ID.

- Para la comunicación del prototipo hacia el Sistema de Gestión es necesario que se tenga un servicio de internet. Esto resulta una ventaja del prototipo ya que hoy en día el internet se ha desplegado mediante diferentes accesos en la mayoría de hogares de nuestra sociedad [13].

- El prototipo es adaptable ante cualquier sistema de gestión que sea compatible con el protocolo Contact ID, según el estándar de comunicación digital SIA [16], o también podría ser implementado directamente bajo un sistema de gestión IP.

- Las pruebas de funcionamiento iniciales se las realizaron con el sistema prototipo de Gestión realizado en la Universidad Politécnica Salesiana [38], para posteriormente probarse con el Sistema de Gestión realizado y mejorado en donde el prototipo se adaptó correctamente con los cambios realizados en la interfaz y programa del Sistema para su completa adaptación.

4.2 RECOMENDACIONES

- Se recomienda usar un voltaje de alimentación de 9v mínimo a 15v máximo a 1A, ya que es el voltaje máximo que podría soportar los integrados, relés etc. dentro de la placa. Al sobrepasar los 15v la placa del prototipo tendría inconvenientes en el funcionamiento de igual manera para la corriente.

- Para los trabajos futuros se recomienda diseñar una placa que soporte hasta los 50v. Con este voltaje se pretende que los tiempos de respuesta sean menores ante una emergencia en el panel de alarma de una residencia u hogar.

- Es recomendable usar un circuito nivelador de voltaje para la comunicación serial entre el microcontrolador y la Rapsberry Pi, ya que con este circuito la información llega completa sin ruido. Sin esta consideración, al realizar las pruebas con el integrado MAX232, presentaron inconvenientes en los niveles de voltajes de la Rasberry Pi y el microcontrolador pues la información llega con alteraciones.

REFERENCIAS BIBLIOGRÁFICAS

[1] "Historia de los sistemas de alarma - Sistemas de alarma." [Online]. Available: https://www.abus.com/es/Guia/Proteccion-antirrobo/Sistemas-de-alarma/Historia-de-los-sistemas-de-alarma. [Accessed: 20-Mar-2019].

[2] "HISTORIA DE LOS PRIMEROS SISTEMAS DE ALARMA. | Seguridad Rodych." [Online]. Available: http://rodych.es/historia-de-los-primeros-sistemas-de-alarma/. [Accessed: 20-Mar-2019].

[3] "→ Historia de los detectores de movimiento | Geniolandia." [Online]. Available: https://www.geniolandia.com/13125409/historia-de-los-detectores-de-movimiento. [Accessed: 20-Mar-2019].

[4] P. Saavedra and C. Arturo, "Estudio de Factibilidad del Proyecto de Importación, Comercialización de Equipos Electrónicos de Seguridad," 2010.

[5] S. Yu, C. Tang, K. L.-2013 15th A.-P. Network, and undefined 2013, "Transformation of PSTN to Next Generation Network," *ieeexplore.ieee.org*.

[6] "Indicadores de Seguridad Ciudadana." [Online]. Available: http://cifras.ministeriodelinterior.gob.ec/comisioncifras/inicio.php. [Accessed: 20-Mar-2019].

[7] R. E. Dutari, "Software libre vs. Software propietario: ventajas, desventajas, desafios y oportunidades," *Panama*, no. December, p. 170, 2009.

[8] C. Juárez, M. Gómez Herrera, W. Guadalupe Torres Sánchez, and S. México, "Software libre vs software propietario ventajas y desventajas."

[9] P. A. Barsallo, "Guia de migración de estaciones de trabajo basadas en software propietario a estaciones de trabajo basados en software de libre distribución," *Quito*, p. 208, 2010.

[10] R. G. Sánchez, "SOFTWARE LIBRE VS. SOFTWARE PROPIETARIO: PROGRAMANDO NUESTRO FUTURO Rafael Gómez Sánchez," vol. 2, pp. 125–140, 2004.

[11] S. I. A. Dc-, I. Protocol, and E. Reporting, "SIA Digital Communication Standard – Internet Protocol Event Reporting," 2013.

[12] X. O. Aguirre, “Estudio de la factibilidad para brindar servicio de seguridad electronica en la compañia segproser cia, ltda,” *Cuenca*, p. 115, 2016.

[13] Centro Nacional de Telecomunicaciones, “Boletín estadístico informativo,” no. 2, 2017.

[14] Comisin Nacional de Telecomunicaciones, “Plan Nacional de Telecomunicaciones 2018-2021,” p. 101, 2011.

[15] M. de T. y de la S. de la Información, “Plan nacional de gobierno electrónico 2018-2021,” p. 84, 2018.

[16] S. I. A. Dc-, I. Protocol, and E. Reporting, “SIA Digital Communication Standard – Internet Protocol Event Reporting,” 2016.

[17] PC585, “Manual de Instalación,” p. 60, 2014.

[18] Paradox, “Manual de instalación y consulta,” *Secur. Syst.*, vol. 4, p. 56.

[19] S. Li, P. Gong, Q. Yang, M. Li, … J. K.-2013 F. I., and undefined 2013, “A secure handshake scheme for mobile-hierarchy city intelligent transportation system,” *ieeexplore.ieee.org*.

[20] S. Li, P. Gong, Q. Yang, … X. Y.-16th I., and undefined 2014, “A secure handshake scheme with pre-negotiation for mobile-hierarchy city intelligent transportation system under semi-honest model,” *ieeexplore.ieee.org*.

[21] G. Dong, B. Yang, Y. Ping, W. S.-2015 17th International, and undefined 2015, “A secret handshake scheme for mobile-hierarchy architecture based underground emergency response system,” *ieeexplore.ieee.org*.

[22] D. R. Alvarado, “Implementación de una central de monitoreo de alarmas en base a un computador personal usando formato de comunicación contact id y avisos sms,” 2013.

[23] C. Guacapiña and J. Eduardo, “Diseño e implementación de sistemas de seguridad para vehículos mediante GPS y telefonía celular (SMS Y DTMF),” 2013.

[24] W. B. Rivas, “Interconexión de radios de VHF con plantas telefónicas IP,” 2015.

[25] J. Artal, J. Caraballo, … R. D.-A. a la E. de, and undefined 2014, “DTMF technology applied to the identification and control of a small mobile robot,” *ieeexplore.ieee.org*.

[26] M. Yahyavi, … A. G.-2011 I. 7th, and undefined 2011, “An improvement of MIPS rate in detection of DTMF signals of 64 subscribers using GOERTZEL’s algorithm,” *ieeexplore.ieee.org*.

[27] J. Duarte, “Generación t detección de tonos DTMF sobre FPGA,” 2008.

[28] S. Bhavanam, … P. S.-2014 I. I., and undefined 2014, “Zynq 7000 series FPGA based Efficient DTMF detection,” *ieeexplore.ieee.org*.

[29] I. C. Peraza, “Decodificador de tonos duales multifrecuencia mediante un microcontrolador embebido en un adaptador USB,” 2009.

[30] P. A. Luque and J. R. Astudillo, “Diseño e implementación de un sistema IVR para telecontrol domótico por medio de un teléfono móvil,” 2006.

[31] A. Tabares, J. R.-S. et technica, and undefined 2012, “Aplicación de procesamiento de señales telefónicas usando Labview.,” *revistas.utp.edu.co*.

[32] E. Breijo, “Compilador C CCS y simulador PROTEUS para microcontroladores PIC,” 2012.

[33] “Introducing the Raspberry Pi 2-Model B.”

[34] S. Roy, S. Nag, I. M.-I. Journal, and undefined 2013, “International Journal of Advanced Research in Computer Science and Software Engineering,” *researchgate.net*.

[35] D. Rybin, K. Piliugina, P. P.-2018 I. C. of, and undefined 2018, “Investigation of the applicability of SSL/TLS protocol for VPN in APCS,” *ieeexplore.ieee.org*.

[36] A. B.-I. Potentials and undefined 1999, “Protocols and sockets,” *ieeexplore.ieee.org*.

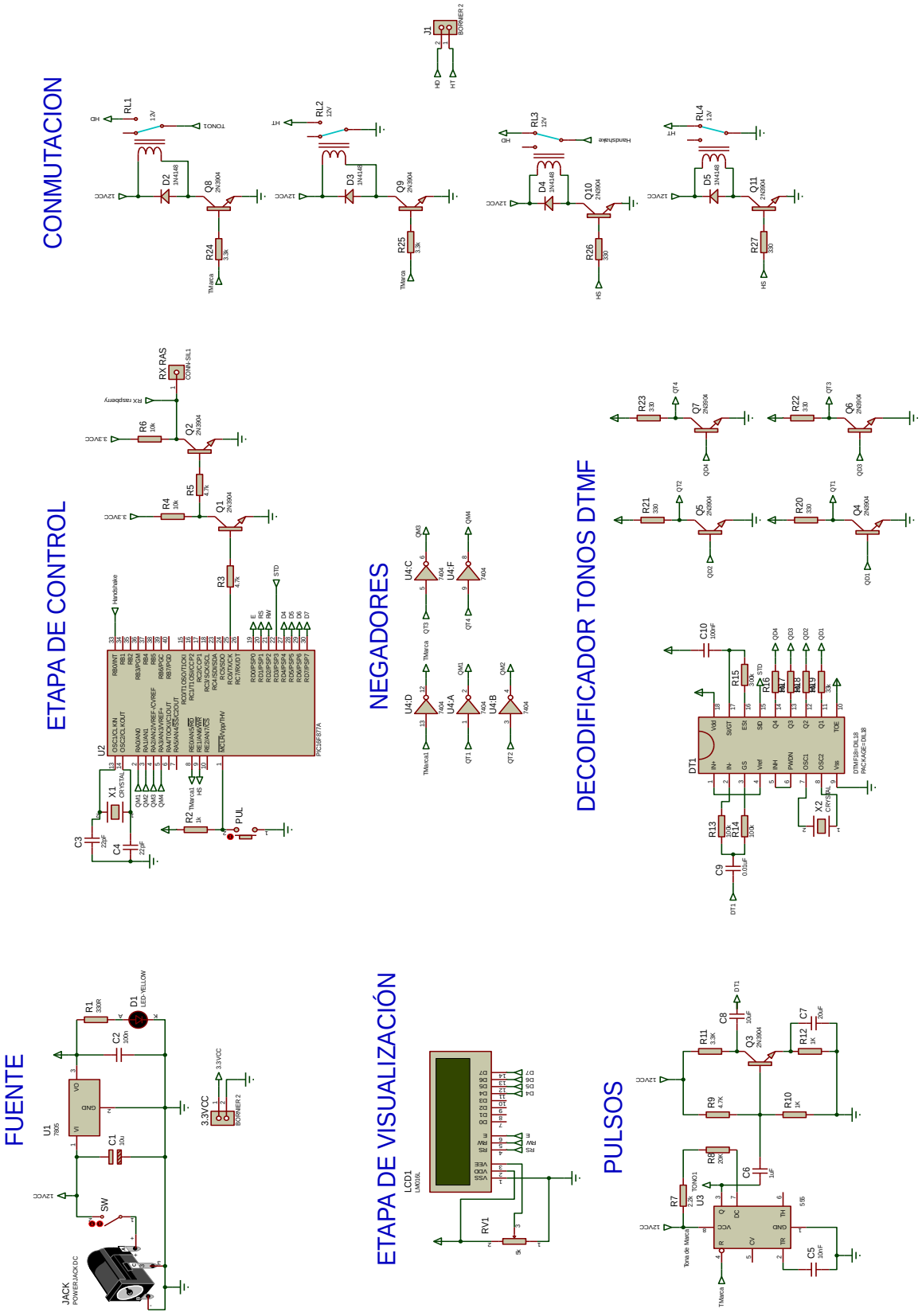
[37] “Socket programming with TCP - Departamento de Informatica.” [Online]. Available: http://wiki.inf.utfsm.cl/index.php?title=Socket_programming_with_TCP&fbclid=IwAR0M8I2DtMjM88LLiQv_AY-m670f_yz3W3faEK2x_dluNvlqiZyNY4-RSfE. [Accessed: 20-Mar-2019].

[38] J. Jara, L. Caldas-Calle, and … E. B.-J. of A. R. in, “Development and Design of the Panic Button System for Community Security in Rural Areas of Pucará-Ecuador,” *jardcs.org*.

[39] L. Caldas-Calle, J. Jara, … M. H.-… C. on D., and undefined 2017, "QoS evaluation of VPN in a Raspberry Pi devices over wireless network," *ieeexplore.ieee.org*.

ANEXOS

Anexo 1



Anexo 2

Programación implementada en microcontrolador 16f877A

```
#include <16F877A.h>
#fuses HS,NOWDT,PUT, NOPROTECT, NOBROWNOUT,NOLVP,NOCPD
#use delay(clock=20000000)
#use rs232(baud=9600, xmit=pin_c6, rcv=pin_c7)
#define use_portB_KBD true
#use fast_io(c)
#include <kbd.c>
#include <TONES.c>
#byte PORTA = 5
#rom 0x2100={'1','5','4','5'}
#define LCD_ENABLE_PIN  PIN_D0                          ////
#define LCD_RS_PIN      PIN_D1                          ////
#define LCD_RW_PIN      PIN_D2                          ////
#define LCD_DATA4       PIN_D4                          ////
#define LCD_DATA5       PIN_D5                          ////
#define LCD_DATA6       PIN_D6                          ////
#define LCD_DATA7       PIN_D7                          ////
#include <lcd.c>
char a[4],b[4], c[16],t[16],k,p;
int i=0,j=0,l=0, valor;
char numero(void){
while(true){
if(input(pin_A0)==0&&input(pin_A1)==0&&input(pin_A2)==0&&input(pin_A3)
==0)
return('A');
else                                                    if
(input(pin_A0)==1&&input(pin_A1)==0&&input(pin_A2)==0&&input(pin_A3)=
=0)
return ('1');
```

```
else if (input(pin_A0)==0&&input(pin_A1)==1&&input(pin_A2)==0&&input(pin_A3)==0)
return ('2');
else if (input(pin_A0)==1&&input(pin_A1)==1&&input(pin_A2)==0&&input(pin_A3)==0)
return ('3');
else if (input(pin_A0)==0&&input(pin_A1)==0&&input(pin_A2)==1&&input(pin_A3)==0)

return ('4');
else if (input(pin_A0)==1&&input(pin_A1)==0&&input(pin_A2)==1&&input(pin_A3)==0)

return ('5');
else if (input(pin_A0)==0&&input(pin_A1)==1&&input(pin_A2)==1&&input(pin_A3)==0)

return ('6');
else if (input(pin_A0)==1&&input(pin_A1)==1&&input(pin_A2)==1&&input(pin_A3)==0)

return ('7');
else if (input(pin_A0)==0&&input(pin_A1)==0&&input(pin_A2)==0&&input(pin_A3)==1)

return ('8');
```

```
else if (input(pin_A0)==1&&input(pin_A1)==0&&input(pin_A2)==0&&input(pin_A3)==1)

return ('9');
else if (input(pin_A0)==0&&input(pin_A1)==1&&input(pin_A2)==0&&input(pin_A3)==1)

return ('0');
else if (input(pin_A0)==1&&input(pin_A1)==1&&input(pin_A2)==0&&input(pin_A3)==1)

return ('B');
else if (input(pin_A0)==0&&input(pin_A1)==0&&input(pin_A2)==1&&input(pin_A3)==1)

return ('C');
else if (input(pin_A0)==1&&input(pin_A1)==0&&input(pin_A2)==1&&input(pin_A3)==1)

return ('D');
else if (input(pin_A0)==0&&input(pin_A1)==1&&input(pin_A2)==1&&input(pin_A3)==1)

return ('E');
else if (input(pin_A0)==1&&input(pin_A1)==1&&input(pin_A2)==1&&input(pin_A3)==1)
```

```
return ('F');

}

}

void TONO1(){
generate_tone(1400,100);
}
void TONO2(){
generate_tone(2300,100);
}
void TONO3(){
generate_tone(1400,800);
}
void main()  {

   kbd_init();
    lcd_init();
   set_tris_B(0b00000000);
   set_tris_A(0b11110000);
  set_tris_C(0b00000000);

output_low(pin_E1);



   while(TRUE)
   {
output_low(pin_E0);
        i=0;
printf(LCD_PUTC, "\f");
        lcd_gotoxy(1,1);
   lcd_putc("BIENVENIDOS '-'");
```

```
     lcd_gotoxy(1,2);
   lcd_putc("PROTOTIPO UP-1.0");
   delay_ms(900);
  printf(LCD_PUTC, "\f");
        lcd_gotoxy(1,1);
   lcd_putc("Enviando");
   lcd_gotoxy(1,2);
   lcd_putc("Tono de Marca");
while(i<=3){

while (input(pin_D3)==0) ;
 while (input(pin_D3)==1) ;
 k=numero();
a[i]=k;
i++;
lcd_gotoxy(1,1);
printf(lcd_putc,"\fSiguiente #: %u\n",i+1);
}

for (j=0;j<=3;j++){
b[j]=read_eeprom(j);

}
 if(a[0]==b[0]&&a[1]==b[1]&&a[2]==b[2]&&a[3]==b[3]){

   printf(lcd_putc,"\fnumero correcto");
delay_ms(200);
   lcd_gotoxy(5,2);
lcd_putc(a[0]);
lcd_gotoxy(6,2);
lcd_putc(a[1]);
lcd_gotoxy(7,2);
lcd_putc(a[2]);
lcd_gotoxy(8,2);
```

```
lcd_putc(a[3]);

delay_ms(900);
printf(LCD_PUTC, "\f");
    lcd_gotoxy(1,1);
   lcd_putc("Conectando....");
   lcd_gotoxy(1,2);
   lcd_putc("llamada..********");
  delay_ms(900);

output_high(pin_E1);
delay_ms(100);
    lcd_gotoxy(1,1);
   lcd_putc("Enviando*******");
    lcd_gotoxy(1,2);
   lcd_putc("Handshake");
      delay_ms(1000);
   TONO1();
delay_ms(100);
   TONO2();
    delay_ms(100);
   printf(LCD_PUTC, "\f");
   output_low(PIN_E1);

 l=0;
  while(l<=15){

while (input(pin_D3)==0) ;
 while (input(pin_D3)==1) ;
 p=numero();
c[l]=p;
l++;
lcd_gotoxy(1,1);
printf(lcd_putc,"\fRecibiendo Infor %u\n",l);
```

```
}

delay_ms(15000);
//Envio de Kissoff
output_high(pin_E1);
    lcd_gotoxy(1,1);
   lcd_putc("Enviando*******");
    lcd_gotoxy(1,2);
   lcd_putc("Kisoff");
delay_ms(2300);
  printf(LCD_PUTC, "\f");

   TONO3();
delay_ms(1100);
output_low(pin_E1);
delay_ms(100);
  printf(LCD_PUTC, "\f");
  lcd_gotoxy(1,1);
   lcd_putc("Informacion:");
   lcd_gotoxy(1,2);
   lcd_putc("Recibida");
    delay_ms(900);
       lcd_gotoxy(1,2);
lcd_putc(c[0]);
    lcd_gotoxy(2,2);
lcd_putc(c[1]);
    lcd_gotoxy(3,2);
lcd_putc(c[2]);
    lcd_gotoxy(4,2);
lcd_putc(c[3]);
    lcd_gotoxy(5,2);
lcd_putc(c[4]);
    lcd_gotoxy(6,2);
lcd_putc(c[5]);
```

```
    lcd_gotoxy(7,2);
lcd_putc(c[6]);
    lcd_gotoxy(8,2);
lcd_putc(c[7]);
    lcd_gotoxy(9,2);
lcd_putc(c[8]);
    lcd_gotoxy(10,2);
lcd_putc(c[9]);
    lcd_gotoxy(11,2);
lcd_putc(c[10]);
    lcd_gotoxy(12,2);
lcd_putc(c[11]);
    lcd_gotoxy(13,2);
lcd_putc(c[12]);
    lcd_gotoxy(14,2);
lcd_putc(c[13]);
    lcd_gotoxy(15,2);
lcd_putc(c[14]);
    lcd_gotoxy(16,2);
lcd_putc(c[15]);
delay_ms(400);



  printf(LCD_PUTC, "\f");
  lcd_gotoxy(1,1);
   lcd_putc("Comunicación");
    lcd_gotoxy(1,2);
   lcd_putc("Finalizada");
    delay_ms(1000);
    output_high(pin_E0);
    delay_ms(800);
     printf(LCD_PUTC, "\f");
  lcd_gotoxy(1,1);
```

```
   lcd_putc("Enviando");
    lcd_gotoxy(1,2);
   lcd_putc("Informacion");
    for(valor=0;valor<=15;valor++){
    t[valor]=c[valor];
    PUTC(t[valor]);
    printf(lcd_putc,"\fenviando=%1D",t[valor]);
    delay_ms(50);
    }
   }
else
printf(lcd_putc,"\fnumero incocorrecto");
delay_ms(100);

   }
}
```

Anexo 3.

Pruebas de validación del prototipo en el Colegio Técnico Industrial Gualaceo.