Desarrollo de un Servicio para Monitoreo y Notificación de eventos utilizando el protocolo Contact ID y componentes de libre distribución

Kathlyn Nathaly Gallego Salazar
Diana Marcela Semanate Garzón

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telemática
Servicios Avanzados de Telecomunicaciones
Popayán, 2015

Desarrollo de un Servicio para Monitoreo y Notificación de eventos utilizando el protocolo Contact ID y componentes de libre distribución

Trabajo de Grado presentado como requisito para obtener el título de Ingeniero en Electrónica y Telecomunicaciones

Kathlyn Nathaly Gallego Salazar
Diana Marcela Semanate Garzón

Director
Javier Alexander Hurtado Guaca

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telemática
Servicios Avanzados de Telecomunicaciones
Popayán, 2015

Hoja de Aprobación

_____
_____
_____
_____
_____
_____
_____
_____

Director: _____
Javier Alexander Hurtado Guaca

Jurado _____

Jurado _____

Popayán, 4 de Marzo de 2015

DEDICATORIAS

A Dios por brindarme siempre nuevos comienzos, por permitirme llegar a este momento tan especial en mi vida, por ser mi fortaleza y mi respaldo en todos los triunfos y momentos difíciles que me han enseñado a valorarle cada día más. Con todo mi cariño y mi amor A mis padres, a quienes les debo todo en la vida, gracias por sus consejos, por el amor que siempre me han brindado y por su apoyo incondicional en todos mis proyectos. A mi hermano y mi abuelita, quienes con su amor aumentaban la fe ante los momentos de debilidad. A mi amado Jose, por cambiar mi vida y llenarme de alegrías con su apoyo constante y su amor incondicional. A Diana, mi compañera de tesis, por su valiosa amistad y grandiosa compañía en esta experiencia tan enriquecedora.

KATHLYN

A Dios por guiar cada paso en mi camino por estar siempre presente en cada etapa de mi vida. A mis amados padres Carmen Rosa y Pedro Antonio por ser la fuente de mi energía que me ilumino para enfrontar las dificultades que día a día se me presentaron y que al recordarlas me llena de orgullo saber que gracias a sus enseñanzas, las pude sobrepasar.

A mis hermanos David y Juan Daniel por su apoyo y amor con que me acompañaron en estos años de estudio y A Kathlyn por ser mi amiga y compañera en la obtención de este gran logro, y a todas las personas que de una u otra manera me ayudaron a llegar hasta lograr este objetivo.

DIANA

AGRADECIMIENTOS

Al director de este trabajo de grado, el Ingeniero Javier Alexander Hurtado Guaca, por su guía en el desarrollo de este proyecto.

Al Ingeniero Víctor Manuel Mondragón Maca, por brindarnos su colaboración en el ámbito intelectual y personal para la realización de este proyecto, contribuyendo con sus enseñanzas y experiencias.

A la empresa Advisor SAS por su apoyo en el desarrollo del servicio y en la ejecución del plan de pruebas, permitiéndonos contar con los recursos disponibles en sus instalaciones.

A la Universidad del Cauca, especialmente a la Facultad de Ingeniería Electrónica y Telecomunicaciones que con sus docentes y administrativos siempre han estado a nuestro servicio.

A los evaluadores de este proyecto que con su visión incrementarán el aporte científico de este proyecto.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ECUACIONES

LISTA DE ACRÓNIMOS

AGI *Asterisk Gateway Interface,* Interfaz Pasarela de Asterisk.

AMI *Asterisk Manager Interface,* Interfaz de Manejo de Asterisk.

CentOS *Community Enterprise Operating System.*

CLI *Command Line Interface,* Interfaz de Commandos.

CRM C*ustomer Relationship Management,* Administración basada en la Relación con los Clientes.

DANE Departamento Administrativo Nacional de Estadística.

DTMF *Dual-Tone Multi-Frequency* , Tonos Duales de Multi-Frecuencia.

FER *Frame Error Rate,* Tasa de Errores de Trama

FSK *Frequency Shift Keying,* Modulación por Desplazamiento de Frecuencia.

GPRS *General Packet Radio Service,* Servicio General de Paquetes vía Radio.

IP *Internet Protocol,* Protocolo de internet.

IVR *Interactive Voice Response,* Respuesta de Voz Interactiva.

ITSP *Internet Telephone Service Provider,* Proveedor de Servicios de Telefonía sobre Internet.

LAN *Local Area Network,* Red de Área Local.

WAN *Wide Area Network,* Red de Área Amplia.

PBX *Private Branch Exchange,* Ramal Privado de Conmutación Automática.

PSTN *Public Switched Telephone Network*, Red Pública de Telefonía Conmutada.

SIA *Security Industry Association,* Asociación de Industrias de Seguridad.

TTS *Text To Speech,* Sintetizador de Voz.

UL *Underwriters Laboratories Inc.*

VoIP *Voice over Internet Protocol,* Voz sobre IP.

WBAN *Wireless Body Area Network,* Red Inalámbrica de Área Corporal.

CAPÍTULO 1. MOTIVACIÓN Y OBJETIVOS DEL TRABAJO DE GRADO

1.1 INTRODUCCIÓN

En los últimos años, Colombia se ha caracterizado por ser un país inseguro. En el 2013 el Departamento Administrativo Nacional de Estadística (DANE) realizó una encuesta de convivencia y seguridad ciudadana [1] [2] donde 20 ciudades fueron encuestadas, obteniendo como resultados un incremento de actos ilícitos contra las personas. Los hurtos y robos en las viviendas, conjuntos cerrados y edificios que se encuentran en los estratos 4, 5 y 6 denotan un aumento sustancial. La inseguridad ha pasado a ser un problema de coyuntura nacional y de búsqueda de soluciones constantes por parte de la sociedad en general.

A lo largo de la historia, el hombre siempre ha mostrado la necesidad de obtener seguridad para proteger su integridad física y sus pertenencias. En esta búsqueda ha utilizado medios y recursos para protegerse de las amenazas de toda índole, construyendo sistemas de seguridad mediante la tecnología existente, permitiendo mitigar la inseguridad, que es difícil de erradicar pero posible de monitorear. Esta también es una de las propuestas del actual gobierno, utilizar la tecnología en la seguridad ciudadana, pues según palabras del presidente de la república, Juan Manuel Santos, “La tecnología ya existe no tenemos que inventarla tenemos que usarla” [3]. Actualmente vivimos en una sociedad donde la tecnología es un factor muy importante, con la que es posible crear sistemas de seguridad aplicables a viviendas o empresas sin la presencia física de personas.

En el presente trabajo de grado se desarrolló un servicio para monitoreo y notificación de eventos usando el protocolo Contact ID[1], haciendo uso también de herramientas de libre distribución y aplicable a un sistema de alarmas convencional. Este sistema permite brindar seguridad ante robos en cualquier entorno ya sea hogares o empresas haciendo uso de canales de notificación como llamada telefónica o correo electrónico, entre otros canales complementarios.

[1] Contact ID: Formato frecuentemente usado y respetado para las comunicaciones digitales entre los sistemas de alarmas para seguridad y centrales de monitoreo.

1.2 ESTRUCTURA DEL TRABAJO DE GRADO

El documento está conformado por cinco capítulos estructurados de la siguiente forma: El primer capítulo presenta la motivación y objetivos del trabajo de grado. El segundo capítulo una descripción general de conceptos típicos en un sistema de alarma convencional. El tercer capítulo describe la metodología e implementación seguida para el desarrollo del servicio planteado. El cuarto capítulo consigna el plan de pruebas y análisis de resultados para el sistema propuesto donde se documenta varias pruebas de funcionamiento y calidad realizadas. Por último, en el quinto capítulo se muestran las conclusiones y trabajos futuros.

1.3 PLANTEAMIENTO DEL PROBLEMA

Todo ingeniero tiene la tarea de brindar soluciones, en este caso ante problemas presentes en el campo de la electrónica y las telecomunicaciones, de tal forma que se puedan suplir ciertas necesidades de la sociedad actual. Una necesidad identificada, es el alto costo que demanda la implementación de servicios para monitoreo y notificación de eventos, debido a que los elementos utilizados implican gran inversión en su instalación, configuración y mantenimiento [4]. La mayoría de las empresas que ofrecen actualmente estos servicios, instalan en los hogares o empresas un sistema de seguridad que permite el monitoreo de diferentes tipos de eventos desde la central de monitoreo, como es el caso de la empresa *Fortox Security Group* [5]. En la central disponen de personal que trabaja las 24 horas verificando que dichas instalaciones estén en completa normalidad, en caso contrario se activa el proceso de notificación según la empresa. Es posible notar que además de los equipos, el personal de vigilancia también implica altos costos para la prestación del servicio.

Teniendo en cuenta lo mencionado anteriormente, se buscó la manera de poder disminuir los costos de implementación y generar mayores funcionalidades en el servicio, aprovechando las ventajas que brinda el uso de un software libre y herramientas de libre distribución para el desarrollo de sistemas que generen servicios para monitoreo y notificación de eventos. Estos sistemas permiten que no sea necesaria la presencia constante de personal de vigilancia en la central.

Surge entonces la necesidad de desarrollar un servicio para monitoreo y notificación de alarmas basado en herramientas de libre distribución, que permita supervisar un entorno que cuenta con diferentes tipos de eventos a ser monitoreados, y que según el estado que estos presenten, se notifica a un usuario mediante diversos canales de comunicación como llamada telefónica, correo

electrónico y mensaje de texto. Todo esto realizado sin la necesidad de una persona a cargo.

1.4 MOTIVACIÓN

Existe una gran demanda de soluciones tecnológicas orientadas hacia la seguridad, que mediante este proyecto se suplen al integrar un sistema de monitoreo con el uso de un sistema de alarmas convencional, una central telefónica, el protocolo de comunicación Contact ID, una arquitectura de gestión de relaciones con el cliente SugarCRM [2] y diferentes canales de notificación al usuario final.

Esta gran demanda se ve beneficiada en la implementación de un sistema como el propuesto en este trabajo de grado, debido a que utiliza un software libre y herramientas de libre distribución que permiten desarrollar sistemas para monitoreo en hogares y empresas (grandes, medianas y pequeñas), y notificación a través de los tradicionales canales de comunicación como lo son llamada telefónica y correo electrónico a precios muy razonables. De igual forma promoverá un espacio en la innovación para el desarrollo de nuevos servicios en el mercado de la seguridad electrónica.

Además, el diseño, implementación y documentación de éste sistema se validará en un ambiente real para la empresa Advisor SAS localizada en la ciudad de Cali.

1.5 OBJETIVOS

1.5.1 Objetivo General

Diseñar un servicio autómata[3] que permita realizar el monitoreo y notificación de eventos, soportando una arquitectura basada en componentes de libre distribución que permita integrar los sistemas existentes de alarmas soportados con el Protocolo Contact ID.

1.5.2 Objetivos Específicos

- Definir las características y funcionalidades a ser integradas dentro del servicio.

[2] SugarCRM: Es un sistema para la administración de la relación con los clientes, que permite gestionar de una forma eficiente y segura los datos de cada cliente.
[3] Servicio Autómata: Ejecuta instrucciones almacenadas, generando ordenes o señales de mando a partir de las señales de entrada leídas, para posteriormente notificar a los clientes.

- Proponer la arquitectura de un sistema para monitoreo y notificación de eventos que permita la integración de los componentes funcionales identificados para el servicio.

- Implementar un prototipo que permita evaluar la funcionalidad de la arquitectura propuesta para el desarrollo del sistema de monitoreo y notificación de eventos, utilizando componentes de libre distribución.

- Validar la funcionalidad del sistema a través de un esquema de plan de pruebas en un ambiente de prueba piloto.

- Realizar un esquema de plan de pruebas que permita validar la calidad del sistema en un ambiente de prueba piloto de la empresa Advisor SAS[4].

1.6 CONTRIBUCIÓN

Este proyecto se encuentra enmarcado dentro de las líneas de investigación: Servicios Avanzados de Telecomunicaciones y Servicios sobre Internet, explorando tecnologías, aplicaciones, protocolos y estándares especificados para alarmas como Contact ID. Logrando aportes en el entorno social, académico e investigativo, los cuales son expuestos en los siguientes puntos:

- Integra tecnologías basadas en centrales telefónicas como Asterisk [6] y Sistemas de Información de Clientes (CRM, *Customer Releshionship Management*). Al tiempo que integra sistemas autómatas de voz y canales de comunicación tradicionales como correo electrónico y mensaje de texto.

- Promueve un espacio en la innovación para el desarrollo de nuevos servicios en el mercado de la seguridad electrónica, basado en tecnologías existentes e integradas a canales de comunicación con el cliente.

- Desarrolla un módulo receptor de alarmas para el protocolo Contact ID integrable a Asterisk, además de los bajos costos para su implementación ya que el proyecto está elaborado con componentes de libre distribución

[4] Advisor SAS: Empresa encargada de brindar servicios de seguridad electrónica ubicada en la ciudad de Cali. Se cuenta con el apoyo de esta empresa para los recursos tecnológicos y de investigación en infraestructura, herramientas software y acompañamiento en el desarrollo del servicio propuesto.

- A partir de este trabajo de grado se desarrolló el artículo "***Development of a Medical Monitoring System and Alarm Notification with a Contact ID Protocol and conventional Alarm System***", el cual fue aceptado y sustentado en la 7ma Conferencia de Ingeniería Biomédica de la Universidad de Concepción (ISCC, *International Student Conference Chile 2014*) [7] en conjunto con el Instituto de Ingeniería Eléctrica y Electrónica (IEEE, *Institute of Electrical and Electronics Engineers)* y la Sociedad de Ingeniería en Medicina y Biología (EMBS, *Engineering in Medicine and Biology Society*), llevada a cabo en la ciudad de Concepción, Chile. Donde se propone una aplicación adicional del sistema desarrollado para el campo del monitoreo médico, el cual resulta ser útil para usuarios que deseen monitorear el estado de salud en familiares o pacientes a partir de un sistema de alarma instalado en su propio hogar o entidad de salud, sin recurrir a contratar servicios especiales y de alto costo.

Todo lo anterior se enmarca dentro de la aplicación práctica de los conocimientos adquiridos en el Programa de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca.

CAPÍTULO 2. GENERALIDADES

2.1 INTRODUCCIÓN

A continuación se describen las características más relevantes de las tecnologías estudiadas y utilizadas en el diseño e implementación del servicio propuesto para monitoreo y notificación de eventos, adicionalmente se plantean los criterios de diseño para la viabilidad e implementación de este.

Con el trabajo realizado en este capítulo se da cumplimento al primer objetivo específico propuesto: Definir las características y funcionalidades a ser integradas dentro del servicio.

2.2 CARACTERÍSTICAS GENERALES

El término seguridad se define como la ciencia interdisciplinaria encargada de evaluar, estudiar y gestionar los riesgos a que se encuentra sometida una persona, un bien o el ambiente, realza la propiedad de algo donde no se registran peligros, daños ni riesgos [8]. En el área de la seguridad se han desarrollado avances tecnológicos con los cuales se han implementado diferentes formas de gestionar la seguridad en un hogar o empresa, debido a factores imprevistos como delincuencia o accidentes a los cuales están expuestas las personas. Ante esto se han desarrollado diversos tipos de sistemas de alarmas para hogar o empresa disponibles en el mercado, que varían según el nivel de protección ofrecido por la empresa que presta el servicio. En este contexto, un sistema de seguridad está conformado por diversos equipos instalados en hogares o empresas tales como cámaras, controladores de acceso, y varios tipos de sensores que ofrecen información de lo que está ocurriendo. El nivel de protección incrementa según sea el monitoreo de la información brindada por estos equipos, por lo cual es acertada la presencia de una central de monitoreo que centralice toda esta información y pueda ser visualizada.

Generalmente los paneles de alarmas verifican a través de sensores el estado de las puertas o ventanas, el movimiento de personas, o la presencia de humo en el lugar, con el objetivo de discernir si el establecimiento está siendo objeto de una intrusión[5] o de un evento inesperado como un incendio [9]. Estos paneles son

[5] Intrusión: Entrada de personas fuera del horario normal de desarrollo de actividades para un sitio en particular.

configurables y constan de un determinado número de zonas, donde se pueden disponer los sensores deseados para instalar. La idea no es solo utilizar la alarma audible[6] ya que el establecimiento puede estar vacío, también es necesaria una comunicación con la central de monitoreo y con los propietarios del establecimiento donde está instalado el panel de alarma [10].

En resumen, un sistema de seguridad está conformado por tres componentes básicos, los cuales se explican a continuación:

Sistema de detección: Se encuentra ubicado en la casa o empresa donde se desea monitorear los eventos ocurridos. Conformado por el panel de alarma y sensores, estos equipos dependen de lo que se desee monitorear y las aplicaciones para las que se desee el servicio de seguridad.

Sistema o Estación de monitoreo: Esta estación es la encargada recibir y monitorear todos los eventos enviados por el panel de alarmas.

Sistema o Estación de Notificación: Esta estación supervisa los eventos leídos en la estación de monitoreo y notifica del evento ocurrido al cliente de alarmas por medio de una llamada. Tradicionalmente, lo anterior está a cargo de personal encargado de monitorear el sistema las 24 horas del día.

2.3 SISTEMAS DE DETECCIÓN

2.3.1 Panel de Alarma y Generalidades

Como se mencionó en la **Sección 2.2**, un panel de alarmas es un dispositivo programable que consta de un determinado número de zonas como se muestra en la Figura 2.1. Se entiende por zona a un arreglo de sensores que definen un espacio limitado [9].

[6] Alarma Audible: Sirena instalada en el panel de alarmas, que suena en caso de una intrusión o emergencia.

Figura 2.1 Panel de alarma.

Al programar un panel de alarma se reúnen varias zonas para conformar particiones, estas son áreas de vigilancia independientes comandadas con teclados numéricos. El panel es el encargado de ejecutar las alarmas en función del estado de los sensores y la programación que se le haya administrado. El principal parámetro que define la activación de alarmas es el estado de las particiones, si están armadas o no [11].

Al panel, además de los sensores se conectan dispositivos como sirenas, marcadores automáticos, cerraduras magnéticas y salidas de relé que pueden ser utilizadas para accionar señales visuales entre otros dispositivos.

El panel de alarmas, además de su alimentación eléctrica normal, es respaldado por una batería que entra en funcionamiento en caso de que falle el suministro eléctrico, asegurando un correcto funcionamiento en todo momento. El estado de la misma, al igual que el resto de parámetros de mantenimiento es transmitido por el panel, que adicionalmente tiene la característica de comunicar todos los eventos de alarma a la estación de monitoreo [11].

2.3.2 Programación de Zonas y Particiones

2.3.2.1 Zonas

El panel de alarma está compuesto de varias zonas, que corresponden a arreglos de varios tipos de sensores conectados en serie o en paralelo según el área que se quiera monitorear.

2.3.2.2 Particiones

Partición es una reunión de diferentes zonas definiendo un espacio de tiempo limitado, esta área puede ser monitorea independientemente del estado del resto de particiones o sensores instalados en el panel de alarma, y cada una puede ser controlada por un teclado diferente, por ejemplo pisos o departamentos de un edificio. El panel de alarma puede vigilar simultáneamente varias particiones independientes compartiendo las mismas alarmas audibles o canales de comunicación.

2.3.2.3 Programación

Para personalizar el sistema de alarma, y programar según las necesidades del cliente se utilizan ciertos códigos y claves introducidos en el teclado alfanumérico. A continuación se presentan algunas características que pueden ser implementadas:

- Activar o desactivar la alarma.
- Definir el tipo de zona.
- Definir sensores conectados al panel de alarma.
- Cambiar claves de usuario.
- Definir horarios de activación.

En el **Anexo A** se puede visualizar algunos de los códigos más utilizados para la programación y configuración del panel de alarmas.

2.3.3 Sensores

Un sensor es un dispositivo que permite adquirir información de variables físicas reales de cierto entorno para su posterior procesamiento [10].

Existen diferentes tipos de sensores, los cuales van conectados a una zona del panel de alarmas, ya sea un solo sensor o un arreglo de estos. Es recomendable usar resistencias de fin de línea para la conexión. Por esta resistencia circula una corriente limitada, si la corriente deja de circular o tiene un valor infinito, o muy bajo, el panel considera que uno de los sensores ha sido activado o que la zona ha sido violentada, lo cual activa la alarma y envía notificación del evento [11].

En el **Anexo A** se explica detalladamente el tipo de conexión de los sensores con el panel y toda la programación que se debe realizar para esto.

Actualmente en el mercado existen diferentes clases de sensores utilizados en sistemas de seguridad, a continuación se explican los principios de funcionamiento de algunos de ellos.

2.3.3.1 Sensores Detectores de Humo

Los sensores detectores de humo detectan la presencia de humo en el aire y emiten una señal que avisa de peligro de incendio.

Existen varios tipos de sensores detectores de humo según el método de detección que utilicen, los más comerciales son: [12]

- Detectores ópticos: Foto-eléctricos, análogos y digitales. Detectan humo visible mediante la absorción y difusión de luz que se recibe en la cámara de humo del detector.
- Detector iónico: Detectan gases y humos de combustión no visibles a simple vista.
- Detectores termo-velocimétricos: Miden el cambio de temperatura en determinado tiempo.

Estos sensores, como el mostrado en la Figura 2.2, son utilizados en centrales de seguridad para informar eventos de alarma de incendios.

Figura 2.2. Sensor detector de humo. [12]

2.3.3.2 Sensores de movimiento

Los sensores de movimiento utilizan la perturbación de las ondas infrarrojas, las cuales se ubican en el espectro electromagnético en una longitud de onda más larga que la luz visible [4]. Se identifica el movimiento de una persona detectando los campos solapados por el haz de infrarrojos, como se muestra en la Figura 2.3.

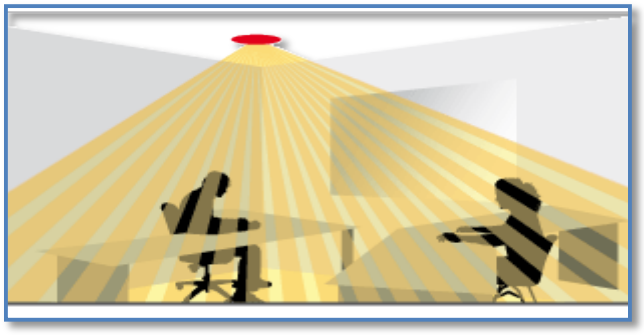


Figura 2.3. Barrido del sensor de movimiento [13].

2.3.3.3 Contactos magnéticos

El sensor de contacto magnético mostrado en la Figura 2.4 es un dispositivo sensor de apertura comúnmente utilizado para alertar de una apertura de puertas o ventanas [10]. Este dispositivo está compuesto por dos unidades en una posición determinada y ante cualquier separación de estas produce un cambio mecánico informando el cambio de estado. Entre las más comunes están los sensores que en presencia de un cambio magnético se mantienen cerrados y se abren cuando desaparece o disminuye notoriamente el campo magnético [10].

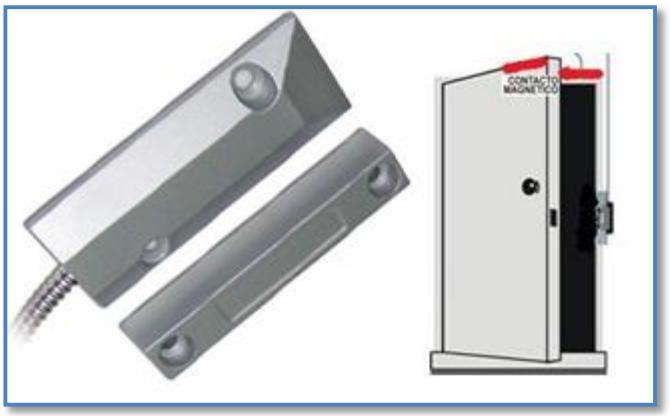


Figura 2.4. Sensor de contacto magnético [13].

2.4 COMUNICACIÓN REMOTA DE EVENTOS

Si se encuentra vacío el lugar en el que ocurre el evento o no está cerca el propietario, el sonido de la alarma audible generada por el panel puede resultar una molestia para las personas cercanas al lugar y no garantiza que el propietario del lugar se entere de la activación de la alarma. Por tal razón la alarma audible no es suficiente y se hace necesario asignar un medio de comunicación al panel para que pueda transmitir la información referente a los eventos ocurridos hacia la

central de monitoreo y esta a su vez pueda notificar al usuario que utiliza el servicio de seguridad.

2.4.1 Medios de Comunicación de Eventos de Alarma

2.4.1.1 Comunicación Vía Telefónica

El medio de comunicación más común es la línea telefónica convencional o fija debido a su simplicidad para utilizarlo, prácticamente todos los paneles de alarma lo usan como estándar.

Al enviar el reporte de los eventos de alarma por medio de la línea telefónica, se hace uso de la Red Pública Telefónica Conmutada (PSTN, *Public Switched Telephone Network*) [14] donde se envía la información por medio de Tonos Duales de Multi-frecuencia (DTMF, *Dual-Tone Multi-Frequency*) [15] estableciendo un circuito de comunicación.

2.4.1.2 Comunicación Vía Internet

En el caso de enviar la información de eventos a la central de monitoreo por medio de comunicación vía internet se utiliza Voz sobre IP (VoIP[7], *Voice over IP*) el cual hace posible que la señal de voz o tonos DTMF viajen a través de internet por medio del Protocolo de Internet (IP, *Internet Protocol*).

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, por lo tanto se pueden comunicar los eventos de alarma desde la Red de Area Local (LAN, *Local Area Network)* del cliente de alarma.

2.4.1.3 Comunicación Vía GPRS

Otro medio para la comunicación del panel de alarmas con la central de monitoreo es el envío de información de eventos a través del Servicio General de Paquetes vía Radio(GPRS, *General Packet Radio Service*) donde se utiliza la red celular para enviar la información de eventos, este es un servicio adicional que pueden ofrecer los proveedores de monitoreo residencial, ya que como servicio básico se ofrece la comunicación telefónica pues generalmente todos los hogares disponen de esta [10]. En caso de que la línea telefónica falle o sea violentada se hace uso de este medio de comunicación para enviar la información del evento a la central

[7] VoIP: Grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP.

de monitoreo, todo esto para respaldar y asegurar el reporte de alguna emergencia ocurrida.

En el **Anexo B** se amplía el tema de señalización DTMF y PSTN.

2.4.2 Protocolos de Comunicación para Eventos de Alarma

Un protocolo de comunicación es el lenguaje que utiliza el panel de alarma para enviar toda la información de los eventos a la estación de monitoreo siguiendo las normas establecidas por los fabricantes de los equipos.

Las empresas fabricantes de equipos de seguridad y monitoreo como *CESA 200*, *Scantronics*® y *Ademco*®[8] han creado protocolos para comunicar sus equipos, entre los más utilizados actualmente están los formatos de comunicación: *Ademco Slow, Ademco Fast, Contact ID, SIA FSK*.

2.4.2.1 Ademco Slow

Este protocolo de comunicación es de los más antiguos y lentos, pues utiliza pulsos para transmitir, volviendo la información vulnerable a posibles distorsiones por presencia de ruido en las líneas [16]. Además envía muy poca información del evento ocurrido, 4 dígitos por el número de abonado y 2 dígitos para el evento. Por ejemplo:

Evento Ademco Slow: (ABCD + EF)
Dónde: (ABCD: número de abonado, EF evento)

2.4.2.2 Ademco Fast

Este protocolo es un poco más rápido que el Ademco Slow, puesto que no utiliza pulsos dedicados si no tonos DTMF, siendo un protocolo sencillo y confiable pero con la limitante del envió de poca información del evento. Además implementa un sistema de comprobación de errores, enviando una sumatoria de verificación *Checksum* de los números que conforman el paquete de datos. La estación receptora realiza la sumatoria de los datos recibidos, si coincide con el *Checksum* recibido acepta la señal [16].

Evento Ademco Fast: (ABCD +EF+Z)
Dónde: (ABCD: número de abonado, EF evento, Z Checksum)

[8] CESA 200, Scantronics® y Ademco®: Empresas fabricantes de equipos de seguridad y monitoreo más reconocidas actualmente.

2.4.2.3 Contact ID

La mayoría de fabricantes de paneles de alarma han adoptado el protocolo Contact ID, desarrollado por Ademco®. Este ha sido aceptado como estándar por la Asociación de Industrias de Seguridad (SIA, *Security Industry Association*) [17], al brindar más información sobre el evento ocurrido y mayor velocidad de trasmisión. Es más robusto en la comunicación de eventos y presenta una amplia variedad de tipos de mensajes, el mensaje codificado en el protocolo Contact ID es el siguiente y se explica ampliamente en la **Sección 2.5**.

Evento Contact ID: (ABCD+MT+ Q+EFG+ $N_1N_2N_3$+ $C_1C_2C_3$+Z)
Dónde: (ABCD: Numero de abonado, MT: Tipo de mensaje, Q: Calificador del evento, EFG: Código del evento, $N_1N_2N_3$: Número de zona, C_1C_2: Numero de partición, Z: *checksum*)

2.4.2.4 SIA FSK

El protocolo SIA transmite los eventos en modulación por desplazamiento de frecuencia (FSK, *Frequency Shift Keying*), en el cual se envía la información en binario y se hace un cambio en la frecuencia sobre una señal portadora como lo muestra la Figura 2.5.

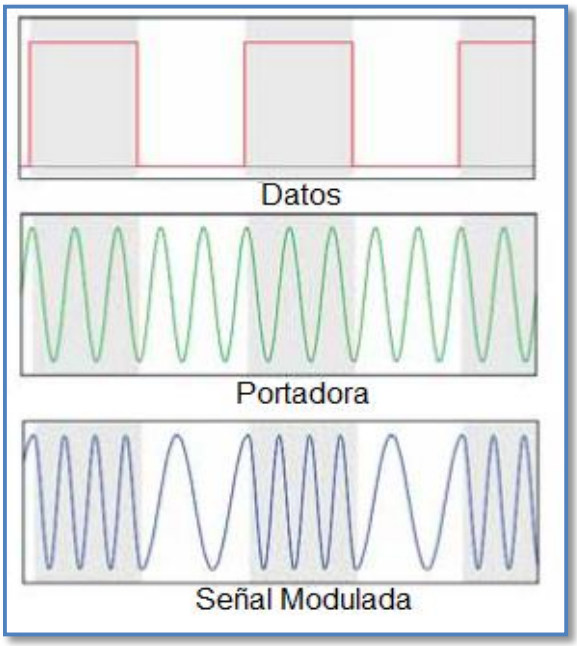


Figura 2.5 Señal Modulada con FSK.

Los datos son la información a enviar, Carrier o portadora es la señal sobre la que se hace el cambio de frecuencia facilitando la transmisión y brindando seguridad, y

por último la señal modulada es el resultado de la mezcla de señales, que finalmente se transmite a la central de monitoreo.

Este protocolo presenta una transmisión más resistente a ruidos en la línea y mejor velocidad [16].

Evento SIA FSK: (N+ABCD+EF+N_1N_2)
Dónde: (N: Nuevo evento, ABCD: Identificador de la partición, EF: Evento, N_1N_2: Número de zona)

2.4.2.5 Tabla Comparativa entre Protocolos de Comunicación de Eventos de Alarmas

En la Tabla 2.1 se pueden observar las principales características y los mensajes enviados por el panel de alarma en el formato de los protocolos mencionados anteriormente, además se realizó una comparación entre estos.

Formato	Paquete Transmitido	Numero de Abonado	Tipo de mensaje	Evento	Checksum	Nuevo Evento	Numero de Zona	Numero de Partición
Ademco Slow	ABCD + EF	ABCD	----------	EF	----------	--------	--------	----------
Ademco Fast	ABCD + EF+Z	ABCD	----------	EF	Z	--------	--------	----------
SIA FSK	N+ ABCD+ EF+ N_1N_2	ABCD	----------	EF	----------	N	N_1N_2	----------
Contact ID	ABCD+MT+ Q+XYZ+ $N_1N_2N_3$+ C_1C_2+Z	ABCD	MT	EFG	Z	Q	$N_1N_2N_3$	C_1C_2

Tabla 2.1. Tabla comparativa de los diferentes tipos de protocolos.

Según lo mostrado anteriormente se concluyó que el protocolo Contact ID es el formato de comunicación más completo, mostrando más información sobre el evento ocurrido. Es el preferido por los fabricantes al ser más robusto en la comunicación de eventos y presenta una amplia variedad de tipos de mensajes. Brinda la opción de seguridad mediante el campo de Checksum a diferencia del SIA FSK que es otro protocolo utilizado, lo que le da una ventaja mayor. La explicación del protocolo Contact ID se ampliará más adelante en la **Sección 2.5**.

2.5 FORMATO DE COMUNICACIÓN CONTACT ID

El protocolo Contact ID fue desarrollado por *Ademco* para comunicar sus equipos, es un formato reconocido por la SIA [18] como estándar sugerido y adaptado por

muchos otros fabricantes para aumentar la compatibilidad entre los paneles de alarma y las estaciones centrales de monitoreo. Este protocolo optimiza el tiempo de transmisión de eventos y permite transmitir más información. El formato Contact ID está compuesto por una serie de dígitos con información relacionada a los eventos que transmite el panel de alarmas, basado en señalización DTMF.

2.5.1 Proceso de Transmisión

El proceso de trasmisión de eventos utilizando el protocolo Contact ID se realiza mediante los tonos *"Handshake*" y "*KissOff*", los cuales sirven de señalización para el inicio y finalización de la trasmisión de los tonos que llevan información. En la Figura 2.6 se observa el diagrama de procesos para la transmisión de los tonos.

El proceso mediante el cual el panel envía la señal a la estación receptora se observa en la Figura 2.7. Inicialmente el panel marca el número de la receptora, esta atiende y ofrece al panel distintos tipos de "*Handshake*", este se refiere a un tono DTMF emitido en un espacio de tiempo definido. Cuando el panel "escucha" el *Handshake* que le corresponde al protocolo Contact ID le pasa el paquete de datos a la receptora, es decir a la central telefónica, cuando el panel finaliza el envío de datos espera para recibir la señal "*Kissoff*", esta es otro tono DTMF emitido por la receptora para indicarle al panel de alarmas que debe finalizar la transmisión de datos [18].

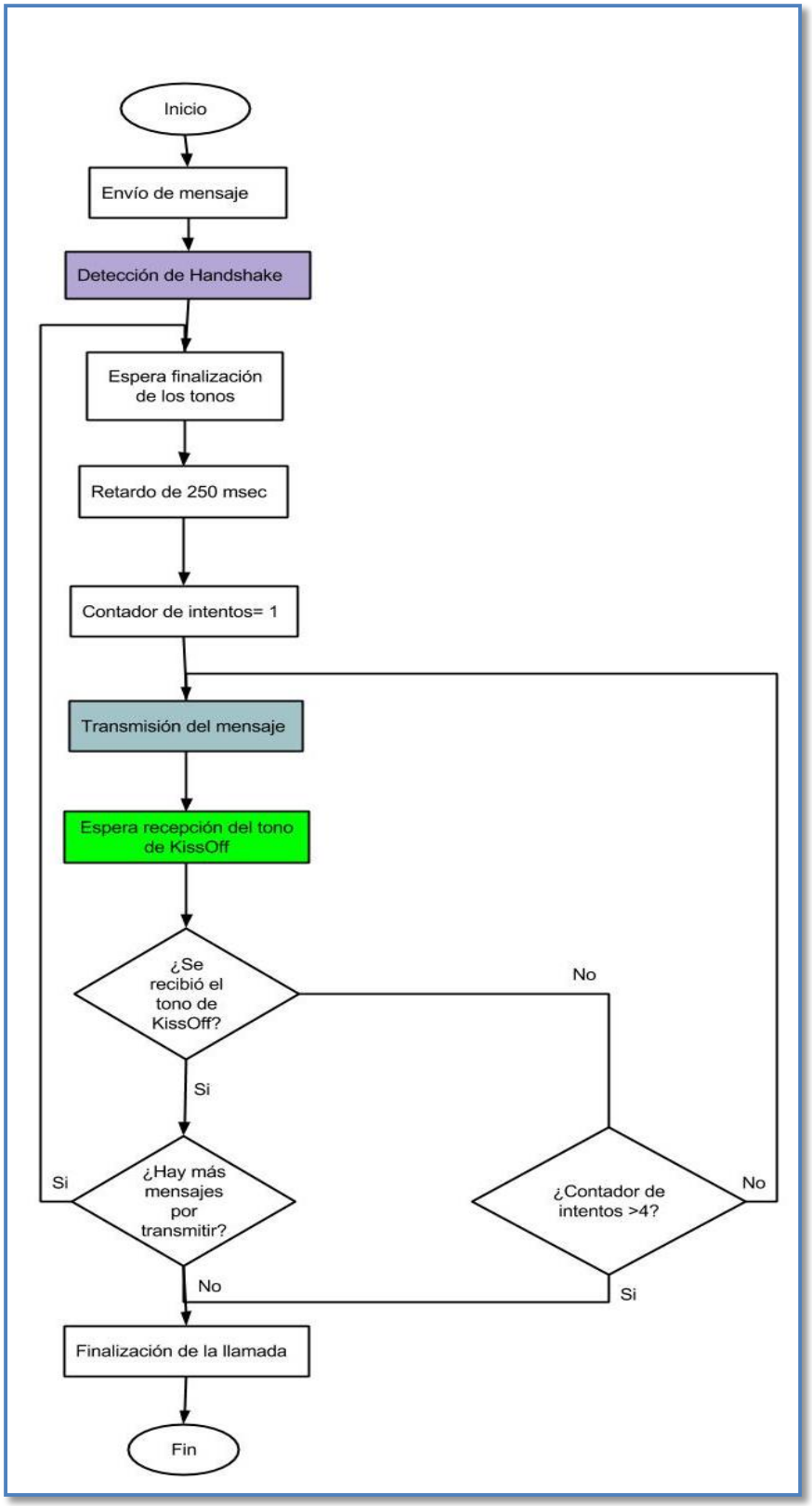


Figura 2.6 Diagrama de flujo del proceso de transmisión.

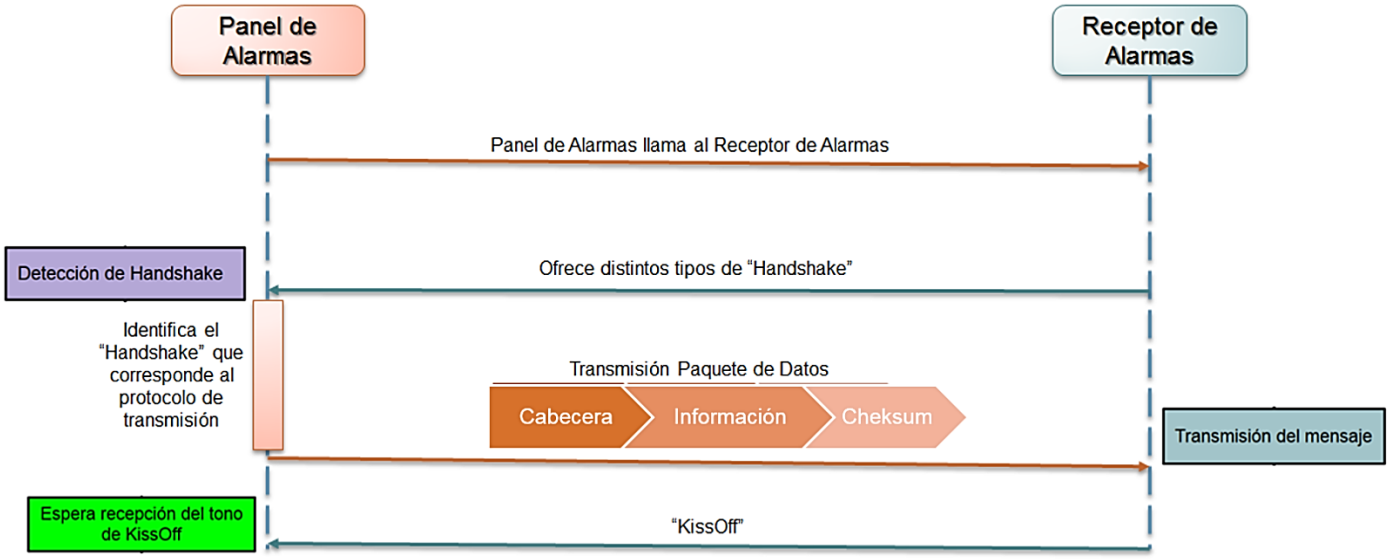


Figura 2.7 Proceso de transmisión del evento.

Cuando finaliza la transmisión de la información, se puede observar en la Figura 2.8 el evento codificado con el Protocolo Contact ID de la siguiente manera:

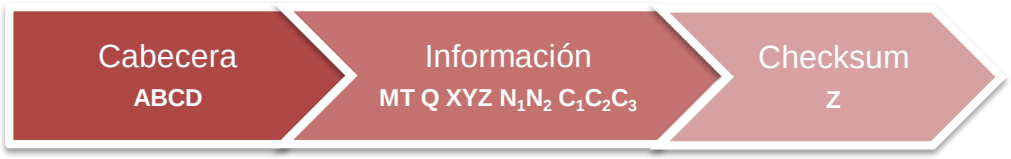


Figura 2.8 Evento Contact ID.

Definición de la nomenclatura:

ABCD: Son 4 dígitos del número de cuenta del cliente (0-9, B-F).

MT: Tipo de mensaje (*Message Type*), 2 dígitos para que el mensaje sea identificado como Contact ID, estos valores son "18" de preferencia o "98" opcional.

Q: Calificador del evento, informa específicamente del evento ya sea

- **1:** Nuevo evento.
- **3:** Armado del panel de alarma.
- **6:** Reporte de estado.

XYZ: Código del tipo de evento ocurrido (3 dígitos Hexadecimales 0-9, B-F).
N_1N_2: Indica el número de partición (2 dígitos Hexadecimales 0-9, B-F).

$C_1C_2C_3$: Indica el número de zona (3 dígitos Hexadecimales 0-9, B-F).
Z: Checksum, para comprobación de errores.

El cálculo del *checksum* se muestra en la Ecuación 2.1

$$S = \left(\left(Parte\ entera \left(\frac{Suma\ de\ los\ dígitos\ de\ la\ trama}{15} \right) \right) + 1 \right) * 15$$

$$Z = S - Suma\ de\ los\ dígitos\ de\ la\ trama$$

Ecuación 2.1. Cálculo del Checksum.

Teniendo en cuenta que para la suma de los dígitos de la trama todos los ceros 0 se deben cambiar por 10 [19].

La verificación del checksum se realiza para comprobar si es correcta o no la información en la respectiva trama de comunicación, y se calcula mediante la Ecuación 2.2 como se muestra a continuación:

$$(Suma\ de\ los\ dígitos\ de\ la\ trama + Z) MOD\ 15 = 0$$

Ecuación 2.2. Verificación Checksum.

El resultado debe ser siempre cero, de lo contrario indica que la trama presenta errores.

2.5.2 Códigos de Eventos

Como se mencionó anteriormente el Protocolo Contact ID envía información del evento ocurrido mediante un código de 3 dígitos (XYZ), este código clasifica el tipo de evento brindando información específica de lo ocurrido. En la Tabla 2.2 se muestra la clasificación de códigos para eventos básicos y su definición avalados por *Ademco* [20].

CÓDIGO	DEFINICIÓN
100 - 102	Emergencias medicas
110 - 118	Alarmas de fuego
120 - 125	Alarmas de pánico
130 - 139	Alarmas contra robo
140 - 147	Alarmas generales
150 - 163	Alarmas 24Horas anti-robo
200 - 206	Supervisión de Incendios

300 - 314	Problemas del sistema
320 - 327	Problemas Sirena/Relé
330 - 344	Problemas del sistema perimetral
350 - 357	Problemas de comunicación
370 - 378	Protección de lazo
380 - 393	Sensor
400 - 466	Alarmas de apertura y cierre
411 - 416	Acceso remoto
421 - 434	Control de acceso
501	Desactivación del sistema
520 - 527	Desactivación Sirena/Relé
531 - 532	Sistema perimetral desactivado
551 - 553	Comunicaciones desactivadas
570 - 579	Circunvalaciones
601 - 616	Pruebas
621 - 628	Registro de eventos
630 - 632	Programación
641 - 642	Monitoreo personal
651 - 789	Códigos especiales

Tabla 2.2 Clasificación de Códigos de eventos Contact ID.

Los códigos más frecuentes son:

- 100 Tipos de alarma: Medica, Fuego, Pánico, General, etc.
- 200 Supervisión: Fuego.
- 300 Errores: Fallos en el sistema o en su programación.
- 400 Acceso Remoto: Abierto/cerrado, Acceso remoto, Control de acceso.

En el **Anexo C** se aprecia con detalle la clasificación de cada evento usando la codificación del protocolo Contact ID.

2.6 MONITOREO, SUPERVISIÓN Y NOTIFICACIÓN DE EVENTOS

2.6.1 Estación de Monitoreo

La información de la alarma es transmitida hacia una estación de monitoreo, ésta puede recibir los datos de cientos de paneles de alarma cada uno identificado con un número. La comunicación generalmente es de tipo telefónico mediante la PSTN o mediante Internet, y haciendo uso del protocolo Contact ID como se mencionó anteriormente. La estación de monitoreo también recibe información adicional relacionada con el mantenimiento de los paneles como fallas en las baterías, fallas de alimentación eléctrica, fallos en la programación o errores en la comunicación.

En los sistemas de alarma tradicionales se cuenta con un operador o supervisor encargado de estudiar las alarmas recibidas en la estación de monitoreo y posteriormente tomar una decisión relacionada con ésta [10]. Así el evento de alarma no queda sólo registrado en la central, sino que también se ha entregado una respuesta a este evento ocurrido. Para poder realizar estas acciones se cuenta con una interfaz hombre-máquina que consiste de un software con la característica de desplegar toda la información necesaria como ubicación de la alarma o número de teléfono al cual llamar para la respectiva toma de acciones.

2.6.2 Funciones del Operador o Supervisor

Las empresas de seguridad asignan funciones a su operador de monitoreo dependiendo de la información recibida en la estación y la interfaz hombre-máquina, entre las acciones que puede realizar el operador se encuentran contactar a los guardias asignados para ese espacio, comunicarse con los dueños del establecimiento si la alarma es de intrusión, llamar a la policía, bomberos o entidad dependiendo del evento y finalmente informar sobre mal funcionamiento del sistema. Luego, cuando todas las acciones son tomadas, el operador registra en el software que el evento ha sido atendido con éxito.

2.6.3 Notificación de Eventos

El medio de notificación de eventos al cliente del sistema de seguridad depende de cada empresa, entre los más utilizados actualmente se tiene llamada telefónica y mensaje de texto, ambos son realizados por el operador de monitoreo para informar el evento o emergencia ocurrido.

2.7 CRITERIOS DE DISEÑO

Un sistema de seguridad presenta criterios de diseño que se pueden resumir en los siguientes aspectos:

2.7.1 Seguridad

Todo sistema que maneje datos de usuarios debe tener ciertas características de seguridad en el manejo de la información, tales como confidencialidad, integridad de los datos y disponibilidad [21]. La información que maneja la central de monitoreo es estrictamente privada y confidencial, con la intención de que los datos que se manejan sean utilizados únicamente por el sistema y con fines de notificación al cliente en caso de activarse alguna alarma.

- Confidencialidad: El sistema de monitoreo brinda confidencialidad en los datos, de tal manera que no tiene acceso cualquier persona al sistema, solamente el administrador del receptor de alarmas.

- Integridad: Se garantiza la integridad realizando controles de seguridad para el acceso restringido, almacenando registros en diferentes medios y haciendo un *Backup* de cada uno de ellos.

- Disponibilidad: El sistema siempre está disponible para brindar el servicio, por lo tanto se asegura:
    - Disponibilidad de conectividad: El sistema cuenta con dos SIP Trunk[9] entre el Panel de Alarma y la Central de monitoreo, en caso de que una SIP Trunk falle y no se pueda comunicar, la alarmas cuentan con números alternos de marcado para comunicarse con el receptor de alarmas.
    - Disponibilidad del Receptor de Alarmas: Se utilizan servidores que poseen *hardware* de alta disponibilidad.

Por lo anterior, la gestión de seguridad de la información se rige bajo la serie de normas de la Organización Internacional de Estandarización (ISO, *International Organization for Standardization*) 27000 [22]. Especialmente ISO 27001, la cual describe cómo gestionar la seguridad de la información en una empresa. ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Mediante el uso de esta norma se persiguen tres objetivos [23]:

- Preservar la confidencialidad de los datos de la empresa.
- Conservar la integridad de estos datos.
- Hacer que la información protegida se encuentre disponible.

2.7.2 Interoperabilidad

Un sistema se caracteriza por ser un conjunto de elementos interrelacionados e interdependientes que trabajan en conjunto para obtener un resultado deseado [24]. Para un sistema de seguridad, se tiene el mismo concepto solo cambia la finalidad, su fin u objetivo principal es establecer un cierto nivel de protección frente a posibles riesgos, peligros, carencias o delitos que puedan afectar de

[9] SIP Trunk: Permite la interconexión de las llamadas IP entrantes o salientes de la Red Pública de Telefonía Conmutada (PSTN).

forma negativa la integridad de las personas en todos los aspectos y generar un sentimiento de tranquilidad frente a cualquiera de ellos [25]. Para estos sistemas se debe garantizar un correcto intercambio de información, pues la tendencia de estos es a la convergencia entre diferentes tecnologías y sistemas de comunicación, logrando así tener la información disponible en cualquier momento que sea requerida. Por lo tanto, es importante que un sistema de seguridad sea capaz de interconectar sus diferentes módulos para capturar información, transmitirla y utilizarla para dar una respuesta ante el evento presentado. Garantizando de esta forma una interoperabilidad sintáctica, ya que en una primera etapa el sistema es capaz de comunicar e intercambiar datos, y posteriormente una interoperabilidad semántica para interpretar de forma automática la información comunicada de manera significativa y con precisión para brindar resultados útiles [26].

2.7.3 Complejidad

Los sistemas de seguridad tienden a ser difíciles y costosos, pues se requiere de una central receptora de alarmas y de todo un sistema de monitoreo [16]. Es importante contar con sistemas de seguridad complejos ya que se generan nuevas propiedades, compuestos por varias partes interconectadas entre sí, permitiendo el intercambio de información y la obtención de nuevas propiedades y beneficios que antes no poseían estos sistemas, tales como notificación autómata y disminución de costos de implementación a partir de herramientas de libre distribución.

2.7.4 Confiabilidad

En un sistema de alarmas es de vital importancia que éste brinde precisión y fiabilidad de los datos, garantizando que estos sean recibidos correctamente por el usuario propietario, no se pueden presentar falsas alarmas que alteren la tranquilidad del usuario y hagan perder mérito de credibilidad al funcionamiento y efectividad del sistema [10].

La confiabilidad en la trasmisión puede ser considerada de extremo a extremo o por cada enlace [27], esta se debe garantizar en el proceso de envío de información del panel de alarmas hacia la central telefónica. Mediante el protocolo de comunicación Contact ID se tiene una verificación de los datos, este protocolo cuenta con una comprobación de errores y con tonos DTMF de inicio y fin de sección que garantizan la confiabilidad de los datos recibidos por el panel de

alarma, así de esta forma poder utilizar esta información para la respectiva notificación al usuario.

2.8 ALTERNATIVAS TECNOLÓGICAS PARA EL PROTOTIPO

A continuación se presenta una base teórica de las tecnologías o arquitecturas más importantes en el diseño e implementación del presente trabajo.

2.8.1 Centrales Telefónicas

Las centrales telefónicas son el lugar donde se establecen las conexiones directas entre los abonados o retransmisiones entre centrales con la señal de información [6]. A continuación se presentan algunas tecnologías existentes que brindan todas las características de una central telefónica permitiendo comunicaciones a bajos costos.

2.8.1.1 PBX

Una centralita privada o PBX es un dispositivo de telefonía que actúa como conmutador de llamadas en una red telefónica o de comunicación de circuitos. La centralita es un dispositivo de telefonía que se suele utilizar en la mayoría de las medianas y grandes empresas, no es muy usual en los hogares, donde los terminales existentes son pocos y las exigencias no son tan importantes. [6]

Permite a los usuarios o abonados compartir un determinado número de líneas externas (analógicas o digitales) para hacer llamadas telefónicas entrantes o salientes, así como establecer comunicaciones internas entre todos los dispositivos que dependen de la PBX.

Entre las muchas ventajas que ofrece, una PBX es una solución más económica que proporcionar a cada usuario de la empresa una línea telefónica externa. A una PBX se le pueden conectar teléfonos, máquinas de fax, módems y otros dispositivos de comunicación [6].

2.8.1.2 Asterisk

Asterisk es una centralita privada de conmutación (PBX, *Private Branch Exchange*) de código abierto. Esta herramienta de libre distribución puede controlar y gestionar comunicaciones analógicas, móviles, tradicionales y digitales por medio del protocolo VoIP. Por lo tanto es el mejor, más complejo y económico sistema de comunicaciones, gracias a su capacidad de ser programado [6].

Asterisk funciona como cualquier PBX o centralita tradicional incorporando funcionalidades como [6]:

- Conexión de un número determinado de teléfonos para comunicación entre sí.
- Conexión con líneas telefónicas tradicionales.
- Extensiones analógicas para terminales telefónicos analógicos.
- Soporta líneas IP o *Sip Trunk.*
- Extensiones IP, para terminales telefónicos digitales.
- Buzón de voz y Audio conferencias, entre otras.
- Respuesta de Voz Interactiva (IVR, *Interactive Voice Response*).
- Sistema integrable con arquitecturas de gestión de relaciones con cliente.
- Distribución automática de llamadas, entre otras.

Mark Spencer [6] es el creador original de *Asterisk,* perteneciente a la compañía *Digium*. Sin embargo al ser de código libre, en la actualidad existen multitud de desarrolladores que han aportado funciones y nuevas aplicaciones.

2.8.1.3 Trixbox

Trixbox es una distribución del sistema operativo GNU/Linux, basado en CentOS[10], incluye FreePBX, una plataforma gráfica para configurar Asterisk que facilita la administración del sistema y con las bondades de una interfaz web y la facilidad de actualizarse por éste mismo medio.

Trixbox incluye todo lo deseado de una PBX, desde un servidor web *Apache,* con soporte a *PHP* y *Perl*, administración de base de datos, correo de voz e integración de este con correo electrónico. Al ser un software de código abierto, posee varios beneficios, como es la creación de nuevas funcionalidades. Algo muy importante es que no sólo soporta conexión a la telefonía tradicional, sino que también ofrece servicios VoIP. Trixbox está diseñado para empresas de 2 a 50 empleados [28].

2.8.1.4 Elastix

Elastix es un servidor de comunicaciones unificadas que integra en un solo paquete PBX, Fax, mensajería instantánea y correo electrónico.

[10] CentOS: Es la distribución de Linux que sirve como Sistema Operacional. Está basado en Linux Red Hat Enterprise [45].

El proyecto Elastix se inició como una interfaz para reportar llamadas de Asterisk y fue liberado en Marzo del 2006 por la empresa ecuatoriana PaloSanto Solutions. Elastix se convirtió en una de las distribuciones para Asterisk más utilizadas en el mundo. Las tecnologías que conforman Elastix son las siguientes:

- Sistema Operativo: Linux CentOS.
- VoIP PBX: Asterisk.
- FreePBX para entorno de gestión web.
- Fax: HylaFax.
- Mensajería Instantánea: Openfire.
- Correo Electrónico: Postfix, además de otros paquetes de código abierto.

Las versiones disponibles de Elastix son versiones completas sin limitación de uso o características. No tiene costo relacionado con licenciamiento o con funcionalidades, ni con la adicción de módulos y de usuarios [29].

2.8.1.5 Comparación entre Herramientas

A continuación se presenta una tabla comparativa de las principales herramientas utilizadas en la implementación de centrales telefónicas, destacando cinco características de cada una para una mejor visualización y comprensión.

Nombre	Autor	Sistema operativo	Tecnologías	Ventaja	Desventaja
Asterisk	Mark Spencer Digium	Debian Ubuntu CentOS	Central Telefónica privada	Total control Actualizable	Programación por línea de comandos Mayor tiempo implementación
Trixbox	Fonality	CentOS	Servidor web: *Apache* Lenguaje: *PHP* y *Perl* Gestión Web: FreePBX	Mucho tiempo en el mercado	Poco desarrollo plataforma Empresas de 2-50 empleados
Elastix	PaloSanto Solutions	CentOS	VoIP: Asterisk Gestión Web: FreePBX Fax: HylaFax Mensajería: Openfire Correo Electrónico: Postfix	Sistema todo en uno	Instala componentes por *default*

Tabla 2.3. Comparación de características herramientas de centrales telefónicas digitales

A partir de la Tabla 2.1 se observa que la herramienta Elastix es un sistema completo de libre distribución, además de contar con la central telefónica Asterisk incluye también una interfaz web de configuración FreePBX, un sistema de base

de datos MySQL, un sistema de mensajería instantánea Openfire, entre otras aplicaciones más. Es una de las distribuciones basada en Asterisk más utilizada actualmente.

2.8.2 Arquitecturas CRM

La arquitectura de gestión sobre la relación con los clientes (CRM, *Customer Relationship Management*), es una estrategia de negocios centrada en el cliente. Por lo tanto, una arquitectura CRM es la respuesta de la tecnología a la creciente necesidad de las empresas de fortalecer las relaciones con sus clientes [30].

Estas arquitecturas CRM permiten maximizar la información del cliente mejorando el servicio ofrecido gracias a procesos optimizados y más personalizados, convirtiéndose en una excelente estrategia de negocio basada en la satisfacción del cliente y en las tecnologías que dan soporte a esta estrategia.

En la actualidad existen diferentes plataformas CRM licenciadas y otras de software libre, estas últimas de gran uso para pequeñas y medianas empresas que desean aprovechar las características de estas arquitecturas sin necesidad de pagar por una licencia. Algunas de estas arquitecturas son: Zoho CRM, vTiger y SugarCRM [29].

2.8.2.1 Zoho CRM

La arquitectura Zoho CRM fue desarrollada por la compañía americana *AdventNet* en el año 2005. Por medio de aplicaciones informáticas y los servicios de telecomunicación comúnmente utilizados en la gestión de una empresa, propone una solución para mejorar el desempeño laboral [31].

2.8.2.2 Vtiger

Esta arquitectura es un software gratuito implementado para fortalecer las relaciones de las empresas con sus clientes.
Vtiger es personalizable y realiza funciones dinámicas para facilitar y agilizar el proceso de actividades, y además permite al cliente desarrollar nuevas funciones de acuerdo a sus necesidades específicas ya que es OpenSource [29].

2.8.2.3 SugarCRM

SugarCRM fue desarrollado por la empresa estadounidense *SugarCRM Inc*, es un sistema modular que integra diferentes aspectos para la administración de la relación con el cliente [32].

Esta arquitectura posee módulos como cuentas, actividades, oportunidades y alianzas. Todo esto basado en un servidor LAMP cuyas siglas provienen de *Linux, Apache, MySQL, Php*. Es decir: maneja un servidor web Apache, una base de datos MySQL, un lenguaje de programación PHP y todo esto sobre una distribución del sistema operativo Linux.
Esta arquitectura es uno de los sistemas líderes en CRM gracias a su robustez y flexibilidad [29] ya que se encuentra en la nube, por lo tanto no requiere estar instalada en un equipo pudiendo acceder a este desde cualquier lugar solamente con una conexión a internet. Se diferencia de otras soluciones porque es la primera arquitectura en código abierto que se ha posicionado como líder en el mercado, y además posee otras versiones licenciadas más completas y funcionales. SugarCRM ofrece la capacidad de integrarse con otras herramientas, tales como la central telefónica digital de código abierto Asterisk, lo cual es una de las características principales del presente trabajo de grado.

2.8.2.4 Tabla Comparativa entre Arquitecturas

A continuación se presenta una tabla comparativa con siete características de las principales arquitecturas CRM para una mejor visualización y comprensión de estas.

Nombre	Origen	Lanzamiento	Lenguaje	Sistema operativo	Base de datos	Autor	Licencia
Zoho CRM	EEUU	2009	Java	Windows Linux, Unix, Mac	No disponible	Advent Net	Saas
vTiger	EEUU	2004	Php	Cross-Plataform	No disponible	Advent Net	Mozilla Public Licence (MPL)
Sugar CRM Inc	EEUU	2004	Php	Cross-Plataform	MySQL, Microsoft SQL Server, IBM DB", Oracle	John Roberts, Clint Oram, Jacob Taylor	GNU AGPL3

Tabla 2.4. Comparación de características en las arquitecturas CRM

A partir de la Tabla 2.4 se observa que la arquitectura SugarCRM es una herramienta de libre distribución que permite contar con una arquitectura de relaciones con el cliente de primer nivel a bajos costos de implementación, dado que es distribuida bajo la Licencia Publica General de Affero Versión 3 (AGPL3, *Affero General Public License*)[11] permitiendo acceso al código fuente a quienes utilicen el software a través de la red.

2.9 APLICACIONES

Las aplicaciones de un sistema de alarmas dependen del tipo de sensores conectados al panel de alarma, estas aplicaciones se pueden clasificar en dos grupos que se exponen a continuación:

2.9.1 Aplicaciones de Seguridad en Hogares o Empresas

Los sistemas de seguridad han pasado de ser implementados solamente en grandes empresas, a ser también necesarios en viviendas, buscando mayor protección ante problemas de inseguridad. Es por esto que las aplicaciones tecnológicas tienden a suplir estas necesidades creando sistemas de seguridad para hogares y empresas, algunos compuestos de sensores de apertura de puertas o ventanas, sensores contra fuego etc.

2.9.2 Aplicaciones de Monitoreo Médico

Por medio del uso de sensores biométricos y de los códigos de eventos del protocolo Contact ID, se puede dar uso a los paneles de alarma para monitoreo de eventos médicos. La vigilancia del estado de salud de pacientes con enfermedades que requieren de un constante monitoreo, es en la actualidad un tema innovador entre las últimas soluciones tecnológicas desarrolladas y de gran aporte en el campo de la salud. De igual forma como se instalan sensores de seguridad en el hogar, se adaptan al paciente sensores biométricos no invasivos, para monitoreo de variables médicas, como presión arterial, temperatura corporal, ritmo cardiaco, entre otras.

[11] Affero General Public License (AGPL3): Garantiza la libertad de usar, estudiar, compartir, copiar y modificar software, además de acceso al código fuente a quienes utilicen el software a través de la red.

CAPÍTULO 3. DISEÑO E IMPLEMENTACIÓN

3.1 INTRODUCCIÓN

En el presente capítulo se muestra la metodología utilizada para el diseño e implementación del servicio de monitoreo y notificación de eventos, basado en herramientas de libre distribución

Además, se muestran las características básicas del sistema y análisis de requerimientos donde se plantea el problema de estudio y se establecen los requerimientos para darle solución. Posteriormente se hace un diseño del servicio donde se definen los diferentes módulos que lo componen y los dispositivos utilizados para su desarrollo, mostrando detalladamente el proceso de implementación de este.

Con el trabajo realizado en este capítulo se da cumplimento al segundo y tercer objetivo específico propuesto:

- Proponer la arquitectura de un sistema para monitoreo y notificación de eventos que permita la integración de los componentes funcionales identificados para el servicio.

- Implementar un prototipo que permita evaluar la funcionalidad de la arquitectura propuesta para el desarrollo del sistema de monitoreo y notificación de eventos, utilizando componentes de libre distribución.

3.2 METODOLOGÍA DE DESARROLLO

La metodología usada para el desarrollo del trabajo de grado es el modelo lineal secuencial o modelo en cascada [33], el cual sugiere un enfoque sistemático o secuencial a través del seguimiento de fases ordenadas que deben cumplirse de forma lineal, facilitando la gestión del desarrollo, diseño e implementación, para así dar solución al problema planteado. En la Figura 3.1 se observan las fases que definen el modelo.

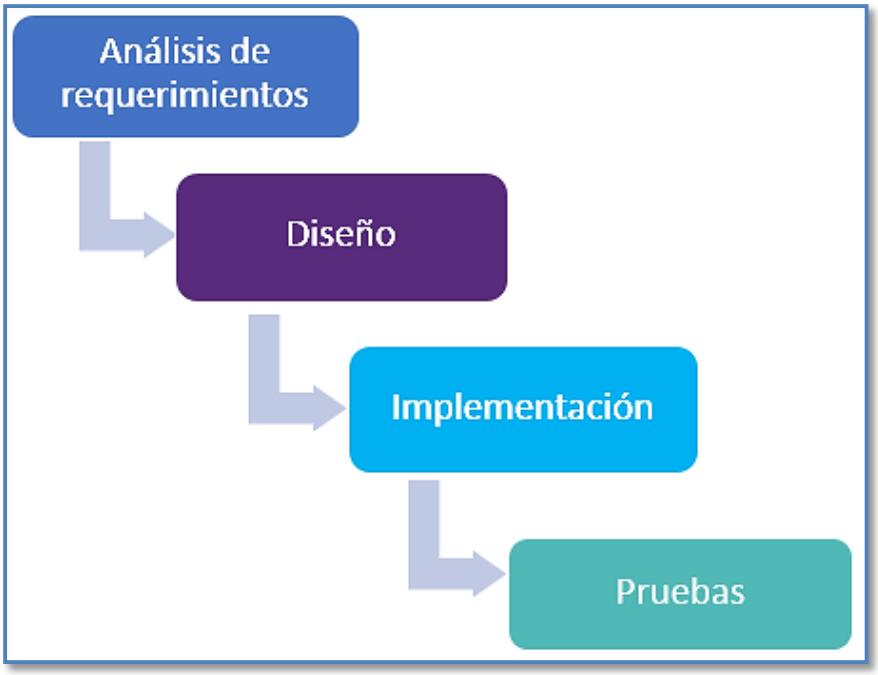


Figura 3.1 Modelo Lineal Secuencial.

Cada una de las fases se desarrolla como se muestra a continuación [33]:

- **Análisis de requerimientos:** Se realiza un análisis del problema de estudio y una recopilación de los requisitos y necesidades del proyecto, con el fin de enlistar detalladamente las acciones que el sistema realizará.

- **Diseño:** Se enfatiza en el modelado del sistema que permita brindar el servicio para monitoreo y notificación de eventos de alarmas. Mediante la creación de un método de trabajo se estudian las herramientas compatibles para el proyecto y necesarias para la fase de implementación.

- **Implementación:** Los resultados de la fase de diseño permiten el desarrollo hardware y software del proyecto.

- **Pruebas:** Se efectúa un plan de pruebas para verificar el funcionamiento y cumplimiento de los objetivos de la fase de análisis y requerimientos.

3.3 ANÁLISIS DE REQUERIMIENTOS

En el análisis de requerimientos se define el problema de estudio y se explican los requerimientos funcionales y no funcionales del servicio para monitoreo y notificación.

3.3.1 Problema de Estudio

Los servicios de monitoreo y notificación que se ofrecen actualmente, instalan un sistema de seguridad en hogares o empresas para monitorear diferentes tipos de eventos desde una central de monitoreo, donde se dispone de personal que trabaja las 24 horas verificando que dichas instalaciones estén en completa normalidad, o en caso contrario se active un proceso de notificación de alarma según la empresa.

Lo anterior permite identificar que además de los equipos, el personal de vigilancia también genera altos costos para la prestación de estos servicios. Por lo anterior y con el propósito de poder disminuir los costos de implementación y generar mayor eficiencia en estos sistemas, surge la idea de desarrollar un servicio para monitoreo y notificación de eventos que utilice el protocolo Contact ID, herramientas de libre distribución y que sea aplicable a un sistema de alarmas convencional, permitiendo supervisar un entorno que cuente con diferentes tipos de eventos a ser monitoreados, y que según el estado que estos presenten se brinde un canal de notificación al usuario como llamada telefónica, correo electrónico y mensaje de texto. Todo lo mencionado anteriormente lo realiza el sistema sin la necesidad de una persona a cargo en la central de monitoreo y permite brindar seguridad en cualquier entorno ya sea hogares o empresas.

3.3.2 Requerimientos

Una vez se tiene claro el problema de estudio, se presenta a continuación los requerimientos que fueron sugeridos por la empresa Advisor SAS y se tuvieron en cuenta para el desarrollo del servicio de monitoreo y notificación, permitiendo alcanzar los objetivos planteados en el trabajo de grado.

Requerimiento 1: Monitorear el estado de seguridad de un establecimiento con el objetivo de discernir si está siendo objeto de intrusión u otro tipo de alarma.

Requerimiento 2: Los dispositivos sensores a utilizar deben ser comerciales, actualizables y capaces de permitir la incorporación a futuro de nuevos

dispositivos. Además, no deben ser un obstáculo para el desplazamiento de las personas dentro del establecimiento donde está instalado el sistema de seguridad.

Requerimiento 3: Asegurar una comunicación continua entre sensores, panel de alarma y receptor de alarmas.

Requerimiento 4: Desarrollar un sistema autómata capaz de realizar todo el proceso de análisis del evento y brindar una respuesta que notifique a los usuarios sin la necesidad de intervención humana.

Requerimiento 5: Desarrollar un medio que permita gestionar la información captada por los sensores y la transmitida al receptor de alarmas. Además de notificar estos eventos.

Requerimiento 6: Brindar diversos canales de comunicación con el usuario para asegurar la notificación de los eventos.

3.4 DISEÑO

En esta etapa se definen características básicas del sistema que permitan brindar el servicio propuesto y posteriormente realizar la implementación del prototipo final que dé solución al problema de estudio. Por lo tanto, se propone implementar un sistema que permita brindar un servicio para monitoreo y notificación de eventos usando el protocolo Contact ID y herramientas de libre distribución. También, se define el modelo de trabajo con sus respectivos módulos de comunicación, notificación, y dispositivos.

3.4.1 Definición del Modelo del Servicio

Los servicios de seguridad que ofrecen las empresas actualmente, instalan diferentes tipos de sensores en los hogares o empresas, con el fin de supervisar las 24 horas desde una central de monitoreo mediante personal calificado que notifica en caso de alguna emergencia al usuario. Debido al personal se pueden presentar errores humanos, ya que el sistema en general depende del desempeño de este personal a cargo.

El diseño e implementación del servicio para monitoreo y notificación de eventos, se caracteriza por ser autómata, capaz de monitorear y notificar sin la presencia de personal supervisando los sensores las 24 horas del día. Esto permite más eficiencia en los sistemas de seguridad, pues ante un evento detectado la estación de notificación se encarga de comunicar sobre éste a todos los usuarios de

notificación, reemplazando de esta forma todas las acciones que haría una persona en una estación.

El sistema planteado está compuesto por seis bloques interconectados como es posible observar en la Figura 3.2

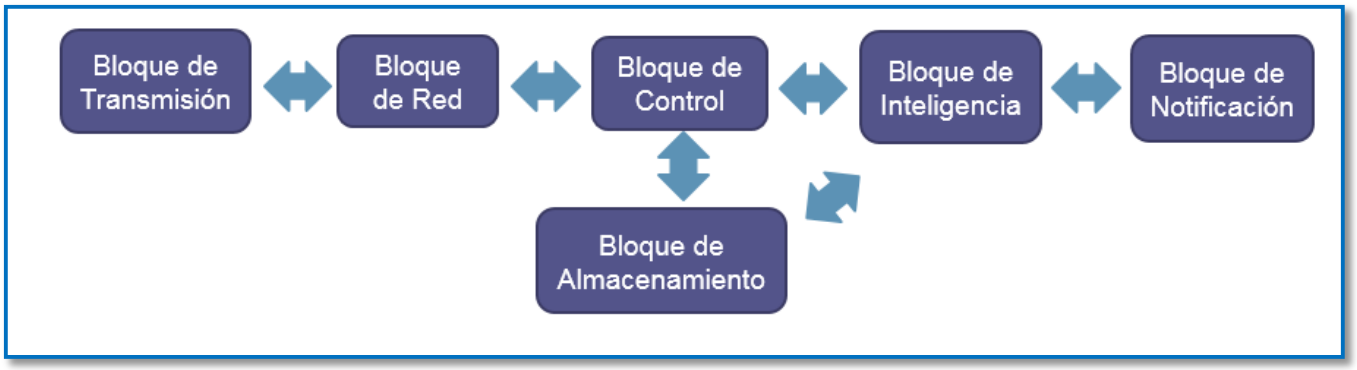


Figura 3.2. Bloques de comunicación.

Descripción general de los bloques:

El primero es el Bloque de Transmisión conformado por el sistema de sensores y el panel de alarma conectados entre sí.

El segundo es el Bloque de Red, conformado por el medio de comunicación a través del cual se transmite la información del Bloque de Transmisión al Bloque de Control.

El Bloque de Control está conformado por el Receptor de alarmas y el Bloque de Almacenamiento por el Servidor de Monitoreo. Hay una comunicación de procesos entre estos bloques y de igual forma éstos se comunican con el Bloque de Inteligencia, el cual realiza la parte autómata del sistema.

Finalmente el Bloque de Notificación está compuesto por los canales de notificación al usuario.

3.4.2 Arquitectura General del Sistema

Se expone en la Figura 3.3 la arquitectura general del sistema, en la cuál es posible visualizar de una mejor forma la conexión de los bloques mencionados anteriormente y los elementos que conforman cada bloque.

Se tiene una empresa u hogar donde se desea monitorear y notificar eventos relacionados con su seguridad, por ejemplo entrada de personas no autorizadas y

eventos de emergencia como robos o incendios. Para esto, mediante sensores de intrusión, apertura de puertas/ventanas y detectores de humo, se monitorea y se comunica al panel de alarmas sobre los eventos ocurridos. Este panel una vez instalado correctamente se comunica por medio de la red LAN y posteriormente con una SIP Trunk hacia el receptor de alarmas.

La central anuncia los eventos recibidos del panel de alarmas al servidor de monitoreo. Una vez se estudia el tipo de evento en la parte inteligente del sistema, y se conoce la acción que se debe tomar, se hace conexión con la estación de notificación y por medio de canales de comunicación como correo electrónico, llamada telefónica y mensaje de texto se informa del evento ocurrido a los usuarios, que para este caso han sido nombrados *Usuarios de Notificación*. De esta forma se asegura un medio de notificación para que el Usuario de notificación se entere del evento ocurrido y realice una respuesta ante la emergencia presentada por la alarma emitida. Esta respuesta que comunica a los Usuarios de notificación con la casa o empresa, no hace parte del sistema, pero es una acción que se debe realizar para poder dar solución al evento.

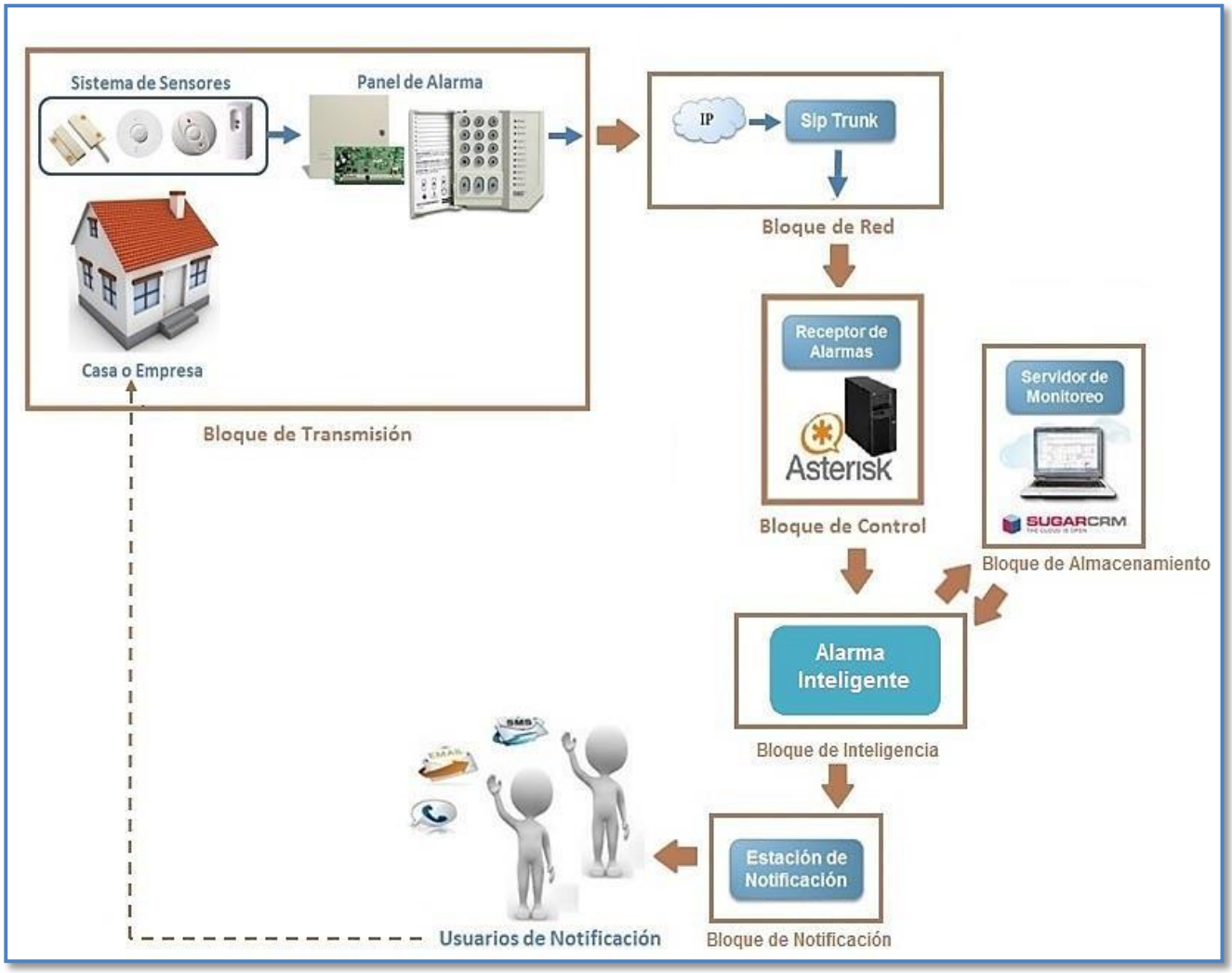


Figura 3.3 Arquitectura General del Sistema.

3.4.2.1 Bloque de Transmisión

En este primer bloque de transmisión se cuenta con:

I. *Sistema de Sensores*

Aquí encontramos los diferentes dispositivos sensores empleados para el monitoreo de eventos, tales como sensores de apertura de puertas y ventanas, sensores de intrusión o movimiento y sensores detectores de humo. Son muchos los sensores disponibles en el mercado, éstos se instalan en el hogar o empresa según las necesidades y planificación de cada ubicación.

II. Panel de Alarma

En este punto se recibe la lectura mostrada por los sensores, se codifica y se realiza el proceso de transmisión de las alarmas detectadas, por medio del Protocolo Contact ID, hacia el Receptor de alarmas.

El panel de alarmas recibe la señal proveniente de los sensores y según su lectura codifica el evento y envía toda la información referente a éste. Por ejemplo: número identificador de la alarma, zona donde ocurrió el evento, partición, y tipo de evento.

3.4.2.2 Bloque de Red

En este bloque de Red se comunica la información del panel de alarmas a través de un medio de comunicación y posteriormente una SIP Trunk.

I. *Medios de Comunicación:*

El panel se comunica con el receptor de alarmas, es decir con la central telefónica para enviarle toda la información del evento ocurrido, esto lo puede realizar por medio de los siguientes canales de comunicación:

- Utilizando la red celular a través del formato de comunicación GPRS.
- Utilizando la red pública de telefonía PSTN.
- A través de internet utilizando el protocolo IP.

En este caso, para el sistema planteado, la transmisión de los eventos es a través de Internet utilizando el protocolo IP. Para esto, es necesario que el panel de alarmas se conecte a una puerta de enlace o *Gateway*, encargada de realizar la conexión del panel de alarmas, permitiendo la transmisión del protocolo Contact ID a través de la LAN del usuario.

II. *SIP Trunk*

Posteriormente con una *SIP Trunk* se establece comunicación hacia el siguiente bloque. Una *SIP Trunk* permite la interconexión de las llamadas IP entrantes o salientes de la PSTN.

Esta *Sip Trunk* es la conexión entre la central telefónica digital y un Proveedor de Servicio de Telefonía IP (ITSP, *Internet Telephone Service Provider*), teniendo disponible todas las aplicaciones ofrecidas por este proveedor. Esto permite que el receptor esté conectado y disponible a las comunicaciones entrantes o salientes para cada una de las diferentes ubicaciones de cada panel de alarma. Además

brinda la posibilidad de incrementar los canales según vayan aumentando el número de clientes.

3.4.2.3 Bloque de Control

El bloque de Control está conformado por el Receptor de Alarmas, es decir una central telefónica digital. La central lee los eventos recibidos del panel de alarmas, para esto se implementó una central telefónica digital utilizando la herramienta de libre distribución Asterisk.

Con Asterisk tenemos todas las características de una central telefónica y las ventajas que ofrece al ser de tipo IP, por lo tanto la resultante serían comunicaciones más eficientes a bajos costos. Esta central recibe e interpreta los tonos DTMF emitidos por la alarma, los almacena en la base de datos para el respectivo análisis de los eventos y según este análisis realiza la comunicación con el Bloque de Almacenamiento.

3.4.2.4 Bloque de Almacenamiento

En el Bloque de Almacenamiento se encuentra el Servidor de Monitoreo, éste se implementó sobre una arquitectura CRM, aquí se almacenan datos del cliente e información sobre las características de las variables a ser monitoreadas de manera ordenada y segura. Permite visualizar también el tipo de sensores instalados en el hogar o empresa, e información del cliente de alarma y de los usuarios a notificar en caso de presentarse un evento. Toma una decisión según los datos recibidos.

3.4.2.5 Bloque de Inteligencia

Conformado por la Alarma Inteligente, cuyo elemento clave es un archivo donde se encuentran todas las funciones necesarias que permiten realizar un análisis adecuado de los eventos ocurridos, eventos que han sido anunciados por la central telefónica Asterisk y de los cuales se cuenta con información adicional en la base de datos del Servidor de Monitoreo, SugarCRM. Por lo tanto este archivo recibe la información proveniente de la central telefónica y la analiza, según lo que analice y la inteligencia que realice, se comunica con el Servidor de Monitoreo para alimentarse de su base de datos con la información complementaria que permita tomar una decisión acerca de la forma de notificación por la que se debe informar al usuario a notificado. Este bloque es la parte autómata del servicio.

3.4.2.6 Bloque de Notificación

En este último bloque se encuentra la estación de notificación, ésta es la encargada de informar al Usuario de notificación sobre una alarma activada o un evento detectado por el panel de alarma. Notifica por medio de diferentes canales de comunicación como: Llamada telefónica, por medio un sintetizador de voz (TTS, *Text to Speech*), mensaje de texto y correo electrónico. Brindando de esta forma diversos medios de comunicación para garantizar que por alguno de éstos o por todos, el usuario será notificado del evento ocurrido.

3.4.3 Selección de Herramientas

A continuación se especifica cada una de las herramientas utilizadas para el diseño e implementación del servicio de monitoreo y notificación de eventos.

3.4.3.1 Protocolo de Comunicaciones

El formato de comunicación seleccionado fue el Protocolo Contact ID, permitiendo la interpretación de los tonos telefónicos, los cuales llevan información relacionada con el evento y la zona donde ocurrió. Los criterios para su selección fueron: Es el protocolo estándar aceptado por la SIA para los sistemas de alarma, es uno de los más utilizados actualmente por la mayoría de fabricantes de paneles de alarma y mediante este protocolo es posible transmitir más información de los eventos ocurridos.

3.4.3.2 Herramientas del receptor de alarmas

Para la implementación del receptor de alarmas se instaló una central telefónica digital usando la herramienta de libre distribución Elastix, ya que crea un sistema de telefonía IP e integra las mejores herramientas disponibles para PBX en una interfaz simple y fácil de usar [34].

Se implementó Elastix debido a sus ventajas de confiabilidad, modularidad y robustez, y además porque integra las ventajas de Asterisk para la central telefónica, convirtiéndose en la mejor opción para implementar el receptor de alarmas.

3.4.3.3 Herramientas del Servidor de Monitoreo

Para la implementación del servidor de monitoreo se requirió de una distribución de Linux que soporta una arquitectura CRM. El sistema Operativo Linux

seleccionado fue la distribución CentOS, cuyas siglas provienen de *Community Enterprise Operating System* en su versión 6.5. Este sistema operativo es robusto, estable, fácil de instalar y utilizar.

La implementación de la arquitectura CRM se realizó utilizando el software SugarCRM en su versión libre SugarCE-6.5.16 Community Edition. Su función es facilitar la gestión de clientes, usuarios de notificación e información de alarmas instaladas, generando fidelidad, interacción y confiabilidad de notificación personalizada para cada cliente o usuario del servicio de monitoreo y notificación.

SugarCRM se implementó sobre un servidor **LAMP** compuesto de:

- Distribución **L**inux: Centos 6.5.
- Servidor Web **A**pache.
- Base de datos **M**ySQL.
- Lenguaje de programación **P**HP.

Gracias a la integración de estas herramientas, es posible obtener un bajo costo de adquisición del servicio, ya que vienen pre-instaladas en la mayoría de distribuciones de Linux y además soportan los servidores de aplicaciones, para este caso el servidor de monitoreo.

3.4.4 Diseño del Proceso de Notificación.

Una de las partes más importantes del servicio propuesto es el diseño e implementación de las herramientas que permitan el proceso de notificación, esto mediante la unión de los módulos Receptor de alarmas y Servidor de monitoreo.

En este proyecto se integró los dos módulos con el fin de poder ofrecer un servicio autómata. Con Asterisk se tienen todas las características de una central telefónica funcionando como receptor de alarmas y con la arquitectura SugarCRM se tiene el Servidor de monitoreo para la gestión de toda la información de las alarmas y de contacto de los clientes.

La resultante de esta integración son comunicaciones más eficientes a bajos costos para quienes la apliquen [35], además de un poderoso sistema CRM con más funciones para agilizar los procesos de notificación y permitir una plena satisfacción del cliente en el monitoreo y notificación de los eventos. Finalmente los beneficios de esta unión permiten que la estación de notificación se comunique de manera autómata con el *Usuario de Notificación,* logrando una comunicación ágil y confiable entre el usuario y el sistema.

3.4.5 Arquitectura Funcional del Proceso de Notificación.

A continuación, en la Figura 3.4 se expone la arquitectura funcional del Receptor de alarmas y del Servidor de monitoreo, indicando las funciones y flujos de trabajo que hacen posible la comunicación entre estos dos subsistemas, logrando un servicio más robusto y complejo.

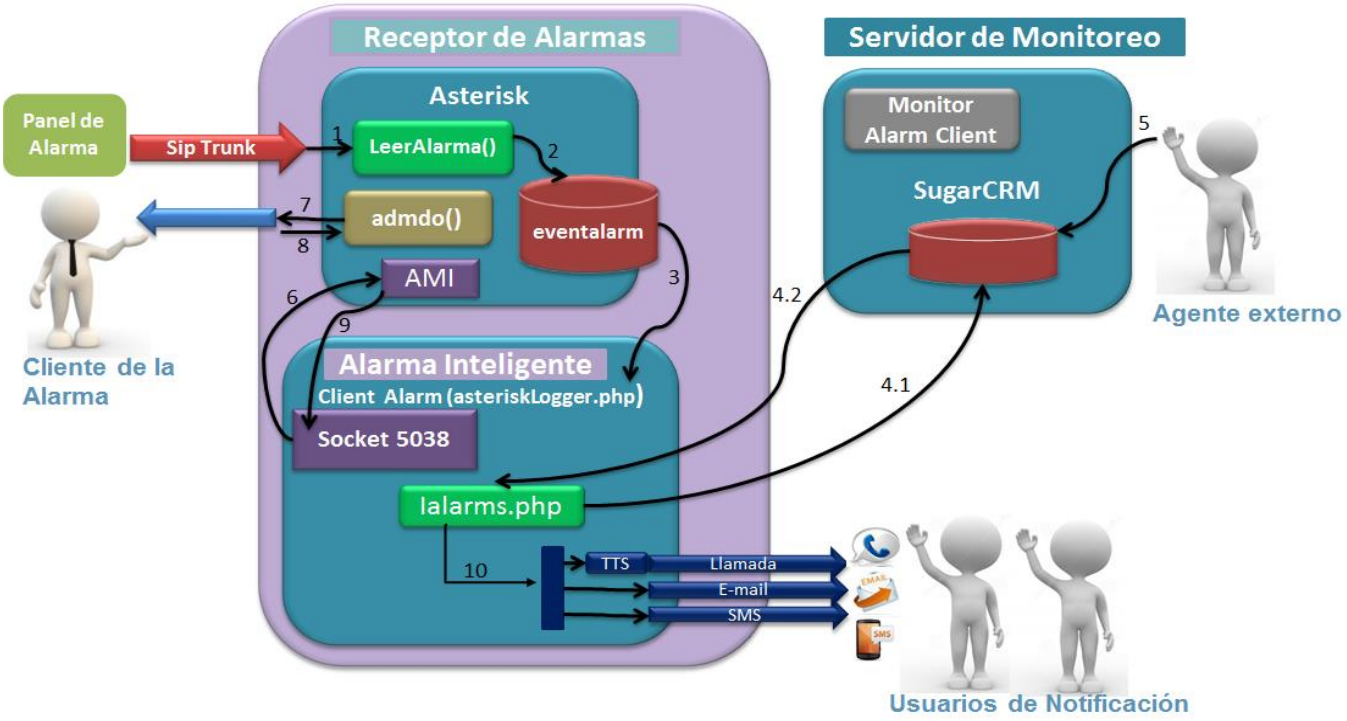


Figura 3.4 Arquitectura Funcional del Proceso de Notificación.

En la Figura 3.4 se muestra el proceso desde que se activa una alarma y se notifica al *Usuario de Notificación*, todo esto mediante la comunicación de los módulos y bloques anteriormente mencionados. El proceso de notificación es el siguiente:

Se activa un sensor produciendo una alarma, este evento es detectado por el panel de alarmas, dando inicio al proceso de notificación:

Paso 1: El panel de alarmas marca el número de la central telefónica o Receptor de Alarmas y se comunica por medio de la SIP Trunk, enviándole al Receptor de alarmas toda la información relacionada con el evento ocurrido, en tonos DTMF.

Paso 2: La central telefónica Asterisk o receptor de alarmas contesta la llamada y mediante la función *LeerAlarma()* recibe la información de los tonos DTMF y los

guarda en la base de datos *eventalarm,* donde se registran todos los eventos ocurridos.

Paso 3: Cuando se cuelga la llamada, quiere decir que ocurrió un evento o se activó una alarma, entonces *ClientAlarm (asteriskLogger.php)*, el cual es un archivo conectado a Asterisk, se encarga de analizar los eventos de la siguiente forma:

¿Qué sensor se activó? ¿Cuál es la respuesta que se debe dar? ¿A quién se debe notificar? ¿Cómo se debe notificar? Es decir, *ClientAlarm* realiza la parte inteligente del sistema y brinda una respuesta de forma autómata.

Paso 4: La inteligencia del paso anterior se realiza mediante el archivo l*alarms.php,* el cual se alimenta de la base de datos del SugarCRM **(4.1)** y obtiene la información necesaria **(4.2)** para decidir a quién se debe notificar y cómo se debe hacer.

Paso 5: Un Agente Externo como el administrador de la central, ingresa los datos a la base de datos del SugarCRM, datos como nombres, teléfonos direcciones y correos electrónicos, toda esta información es la que utiliza el archivo lalarms.php.

Monitor Alarm Client es un agente externo, no propio de todo el sistema, que indica cuando el sistema de alarmas está activado, por lo tanto envía una alarma cuando la plataforma se cae o se apaga.

Paso 6: *ClientAlarm* se conecta a Asterisk mediante el puerto Socket5038 y la interfaz para la Gestión de Asterisk (AMI, *Asterisk Manager Interface*), éste se comunica con Asterisk para realizar una llamada al propietario de la alarma.

Paso 7: Mediante la función *admdo()* se realiza la llamada al cliente para preguntar la acción inmediata que desee realizar, es decir si se trata de una falsa alarma o si desea continuar con el proceso de notificación.

Paso 8: El *Cliente de la Alarma* tiene la opción de responder si desea continuar o no con el proceso de notificación. Cabe resaltar que si el *Cliente de la Alarma* no responde esta llamada, igual se procede con el proceso de notificación. Se entiende por *Cliente de la Alarma* a la persona propietaria del hogar o empresa donde está instalado el sistema de seguridad.

Paso 9: Después de obtener la respuesta del *Cliente de la Alarma* con la autorización de iniciar el proceso de notificación, se procede a informar al *Usuario de Notificación* del evento ocurrido. Todo esto mediante la comunicación de Asterisk con *ClientAlarm*. La diferencia entre *Cliente de la alarma* y el *Usuario de*

*Notificació*n, es que el primero es el dueño de la alarma y el segundo es el usuario a notificar, la diferencia radica en las prioridades de notificación.

Paso 10: La estación de notificación informa al *Usuario de Notificación* del evento ocurrido mediante los siguientes canales de comunicación:

En el archivo *lalarms.php* se tienen sub funciones para cada tipo de notificación:

- La función *crearVoz()* para notificar por medio de llamada telefónica, mediante un sintetizador de voz TTS realiza la llamada a fijo o móvil mediante las funciones *llamar_fijo* o *llamar_movil*.
- La función *enviar_sms()* para notificar por mensaje de texto
- La función *enviar_email()* para notificación por correo electrónico.

Con el *Usuario de notificación* enterado del evento ocurrido, se finaliza la comunicación de procesos en la arquitectura funcional del sistema.

Esta arquitectura funcional le brinda al sistema la posibilidad de realizar las mismas funciones que realizaría una o varias personas en una central telefónica o servicios de alarmas actuales, donde se rotan los siete días de la semana por 24 horas para vigilar los datos entrantes e iniciar el proceso de notificación de forma manual.

3.4.6 Descripción de Dispositivos

El sistema de alarmas utilizado cuenta con salidas programables que pueden cumplir funciones como activar una sirena o cualquier dispositivo que pueda ser considerado como ayuda en el monitoreo o acción de alerta frente a una emergencia.

Posteriormente, la idea es implementar una central de monitoreo de alarmas mediante tonos telefónicos DTMF, utilizando el formato de comunicaciones Contact ID y notificando al usuario del evento ocurrido mediante diversos canales de comunicación.

Los dispositivos utilizados se dividen en cuatro bloques principales. El primer bloque consta de los dispositivos sensores que permiten el monitoreo de las instalaciones del hogar o empresa según las necesidades de cada cliente. El segundo es el Emisor de alarma que consta del Panel de Alarma y todos los equipos existentes en el mercado que cumplen los requisitos para transmisión del protocolo Contact ID, permitiendo un buen funcionamiento y configuración. El tercer bloque es el Receptor de Alarma, es decir la central telefónica que permite

la transmisión de los tonos DTMF y la recepción de los eventos, también está conformado por el Servidor de Monitoreo.

3.4.6.1 Bloque de dispositivos Sensores

Para la instalación de alarmas o sensores en una vivienda o empresa, se tuvo en cuenta las zonas con las que se trabajó, estas zonas indican con detalle cuál es el sensor o dispositivo que se activó mientras estaba bajo vigilancia. La determinación de una zona brinda a la persona encargada de monitoreo la facultad de discernir la localización precisa del evento en una instalación [4].

A continuación se listan los dispositivos sensores utilizados en el sistema.

- Sensor de contacto magnético.
- Sensores de movimiento.
- Sensores detectores de humo.

3.4.6.2 Bloque de Emisor de Alarma

En este bloque emisor de alarma se utilizan dos dispositivos: Panel de alarma con su respectivo teclado y una *Gateway*, los cuales se especifican a continuación:

3.4.6.2.1 Panel de Alarmas

La selección del Teclado y Panel de Alarmas depende del número de sensores o dispositivos que se van a conectar al mismo y la distribución de zonas que se quiera tener para mantener un monitoreo efectivo [4].

En la Figura 3.5 se muestran los dispositivos seleccionados. Se trabajó con el panel especificación **(a)** DSC 1832 y teclado **(b)** PC1555. Este panel está disponible para 8 zonas y es expandible a 32 zonas. Pude programarse hasta 4 particiones y 8 teclados numéricos. Es un equipo para uso interno y conexión permanentemente. Especificado para trabajar a temperaturas desde 0°C hasta 49°C con una humedad relativa máxima del 93%.

(a) **(b)**

Figura 3.5 (a) Panel de Alarmas DSC 1832 V4.2 y (b) Teclado PC1555.

A continuación se exponen las características generales del panel DSC1832 [10] :

- *Alimentación eléctrica normal*

El panel de alarma se alimenta con 16.5 VAC a través de un trasformador MC Electronics Modelo MGT1640.

- *Respaldo de baterías*

El panel de alarmas tiene un respaldo en caso de que la red eléctrica falle, usando una batería recargable de plomo acido sellada, marca Yuassa 12V y 7Amp/h. [36].

- *Consumo eléctrico*

El consumo de energía eléctrica del panel por si solo es de 110mA. El consumo de los equipos activos conectados en sus salidas auxiliares, la sirena y el Keybus (por donde la central se comunica con el teclado, una receptora inalámbrica o varios módulos de la línea DSC) debe ser de 2.5 Amperios.

- *Conexión de teclados – Keybus*

Las borneras del Keybus permiten con cuatro hilos (Rojo, Negro, Amarillo y Verde) la conexión entre el panel con el teclado, módulos de expansión o módulos de comunicación.

- *Conexión de Zonas*

En estas borneras se conectan los diferentes sensores o arreglos de estos pertenecientes a cada zona. El calibre del cable es de 18AWG hasta 2377 metros. Sin embargo para distancias menores a 900 metros el calibre del cable es 22AWG.

- *Conexión de Sirena*

Para la conexión de la sirena se usan los terminales Bell (+ y -) que proveen un voltaje de 12VCC, y 2A de alimentación.

- *Salidas Auxiliares*

Estas salidas auxiliares proveen un voltaje permanente de 12.6VCC con un consumo de 700mA utilizados para alimentar módulos, detectores, relés y avisos luminosos entre otros.

- *Conexión a Línea Telefónica*

La conexión a la línea telefónica se realiza en las borneras (Ring, Tip, T-1, R-1) del panel de alarmas.

3.4.6.2.2 Gateway

En la Figura 3.6 se muestra el adaptador telefónico análogo o Gateway Cisco SPA 100 [37], en el slot *Phone 1* perteneciente a éste, se conecta la línea telefónica proveniente del panel de alarmas y en el slot *Internet* se conecta la red internet LAN del usuario, así las llamadas del panel de alarmas se envían a través del Protocolo IP por medio de esta pasarela.

Figura 3.6 Adaptador telefónico análogo o Gateway.

La *Gateway* se comunica con el panel de alarmas por medio de la conexión a las líneas telefónicas en las borneras del panel de alarmas.

3.4.6.3 Bloque de Receptor de Alarma y Servidor de Monitoreo

Para la implementación y prácticas en laboratorio, en estos dos bloques se utilizó un computador que soporta las siguientes herramientas: Asterisk mediante la distribución libre Elastix, SugarCRM Community Edition en su versión libre por medio de la distribución de Linux CentOS 6.5, y todos sus componentes mencionados en la **Sección 3.4.3**.

- Sistema Operativo: Windows 8
- Máquinas Virtuales: Centos 6.5, Elastix 2.5.0
- Fabricante: Dell
- Procesador: Intel Core I5 CPU 1.60Ghz 2.30Ghz
- Memoria RAM: Intel con mínimo 6Gb RAM
- Disco Duro: 1Terabyte

3.5 IMPLEMENTACIÓN

El esquema de funcionamiento implementado en la etapa de laboratorio se observa en la Figura 3.7. Este esquema muestra que el panel de alarmas se comunica con la *Gateway* para convertir los tonos DTMF en señalización IP, y enviarlos a través de la red LAN y el proveedor de Servicios vía Internet. Por medio de la SIP Trunk se comunica la central a Internet para recibir la información proveniente del panel de alarmas.

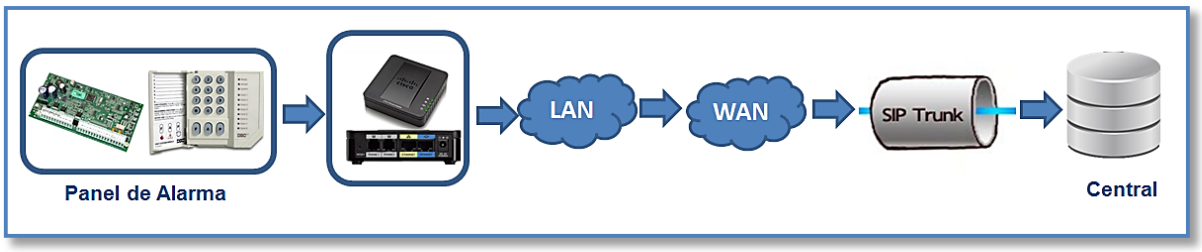


Figura 3.7. Esquema de conexión entre el panel de alarmas y la central de monitoreo mediante comunicación vía IP.

En caso de que la transmisión de información del panel sea a través de la red PSTN, se conecta el panel de alarmas mediante el cable telefónico a la red telefónica, éste realiza una llamada que se dirige a una central telefónica conmutada para convertir los tonos DTMF en señalización IP y utiliza con el

Operador TELCO[12] una intranet para enviarla de esta forma por la WAN, finalmente a través de la SIP Trunk la central recibe la información proveniente del panel de alarmas.

Figura 3.8. Esquema de conexión entre el panel de alarmas y la central de monitoreo mediante comunicación vía PSTN.

Se expone a continuación la implementación de cada uno de los componentes principales del servicio propuesto, es decir el Receptor de Alarmas y el Servidor de Monitoreo, la Alarma inteligente y la Estación de notificación.

3.5.1 Implementación del Bloque de Control

Como se mencionó en la Figura 3.3 al Bloque de control le pertenece el Receptor de alarmas, conformado por la central telefónica digital Asterisk. Entre las aplicaciones de Asterisk se encuentra *AlarmReceiver()*, que permite a la herramienta recibir alarmas usando el protocolo Contact ID.

La aplicación funciona de la siguiente forma, cuando se recibe una llamada proveniente del panel de alarma, se dirige a un contexto que llama a la aplicación *AlarmReceiver()*, ésta lee el fichero de configuración y realiza las acciones configuradas según se requiera [38].

La aplicación responde la llamada y espera 1250 mili-segundos, luego envía la secuencia de tonos ACK o *Handshake*, y espera a que el panel le envíe un evento en tonos DTMF. Para cada evento se comprueba la integridad de los datos, y si estos son válidos se envía el tono *Kissoff* como señal de despedida [39].

Sin embargo, esta aplicación *AlarmReceiver()* no es recomendada para ser usada en aplicaciones donde sea el medio principal o único de recepción de mensajes o eventos de alarma, ya que no ha sido totalmente aprobada por Laboratorios Underwriters (UL, *Underwriters Laboratories*) [40] quien es una empresa de consultoría de seguridad, encargada de ofrecer certificación relacionada con la

[12] TELCO: Es un nombre genérico utilizado para designar a una gran empresa de telecomunicaciones.

seguridad, validación, pruebas, inspección, auditoria, asesoría y capacitación de servicios.

Debido a que en el receptor de alarmas la aplicación *AlarmReceiver()* sería el único medio de recepción de los eventos del panel, para el servicio propuesto se estudió la posibilidad de poder realizar una nueva aplicación nombrada *LeerAlarma(),* basándose en la lógica funcional de la aplicación *AlarmReceiver()* y ajustándola con el fin de poder obtener todos los eventos del panel de alarmas y brindar un funcionamiento confiable del receptor de alarmas, pues de esto depende la eficacia del servicio de notificación. En el **Anexo D** se encuentra el código completo para la aplicación *LeerAlarma().*

Para construir la lógica de funcionamiento y de lectura del protocolo Contact ID para el receptor de alarmas, se utilizó la herramienta Visual Dialplan versión 3.5.00 [41], la cual es una plataforma de modelado visual que permite a los usuarios de Asterisk crear, mantener y desplegar un plan de marcación de una manera fácil, rápida y cómoda. Se aprovecha la comodidad de la interfaz de usuario con funciones de arrastrar y soltar. Otras ventajas que se tienen al trabajar con esta herramienta son:

- Fácil aprendizaje de plan de marcado.
- Facilita el mantenimiento de los contextos.
- Integración sencilla con otros servicios como base de datos, correo, etc.

Visual Dialplan presenta herramientas que permiten realizar un plan de marcado por medio de contextos que hacen referencia a la unión de varios macros, y los macros a su vez contienen funciones en bloques y objetos. Mediante el manejo de la interfaz, Dialplan crea los requerimientos necesarios de cada función en el plan de marcado y permite identificarlos de una forma más clara en la interfaz.

Un macro hace referencia a una caja negra con funciones y objetos al interior de esta. Cuenta con entradas, que para este caso son parámetros, dígitos o tonos que llevan información y deben ser estudiados. Dentro del macro se realizan procesos para estudiar detalladamente la información de entrada, y de esta forma poder generar la información de salida necesaria para la creación de los códigos de lectura. El esquema general se muestra en la Figura 3.9.

Figura 3.9. Esquema de entradas y salidas en un macro.

A continuación se presentan todos los bloques que conforman el Receptor de alarmas y sus respectivas aplicaciones de funcionamiento.

La lógica de funcionamiento para la creación de los macros, funciones y objetos en la herramienta Visual Dialplan se presenta a continuación en el diagrama general de procesos del sistema de la Figura 3.10.

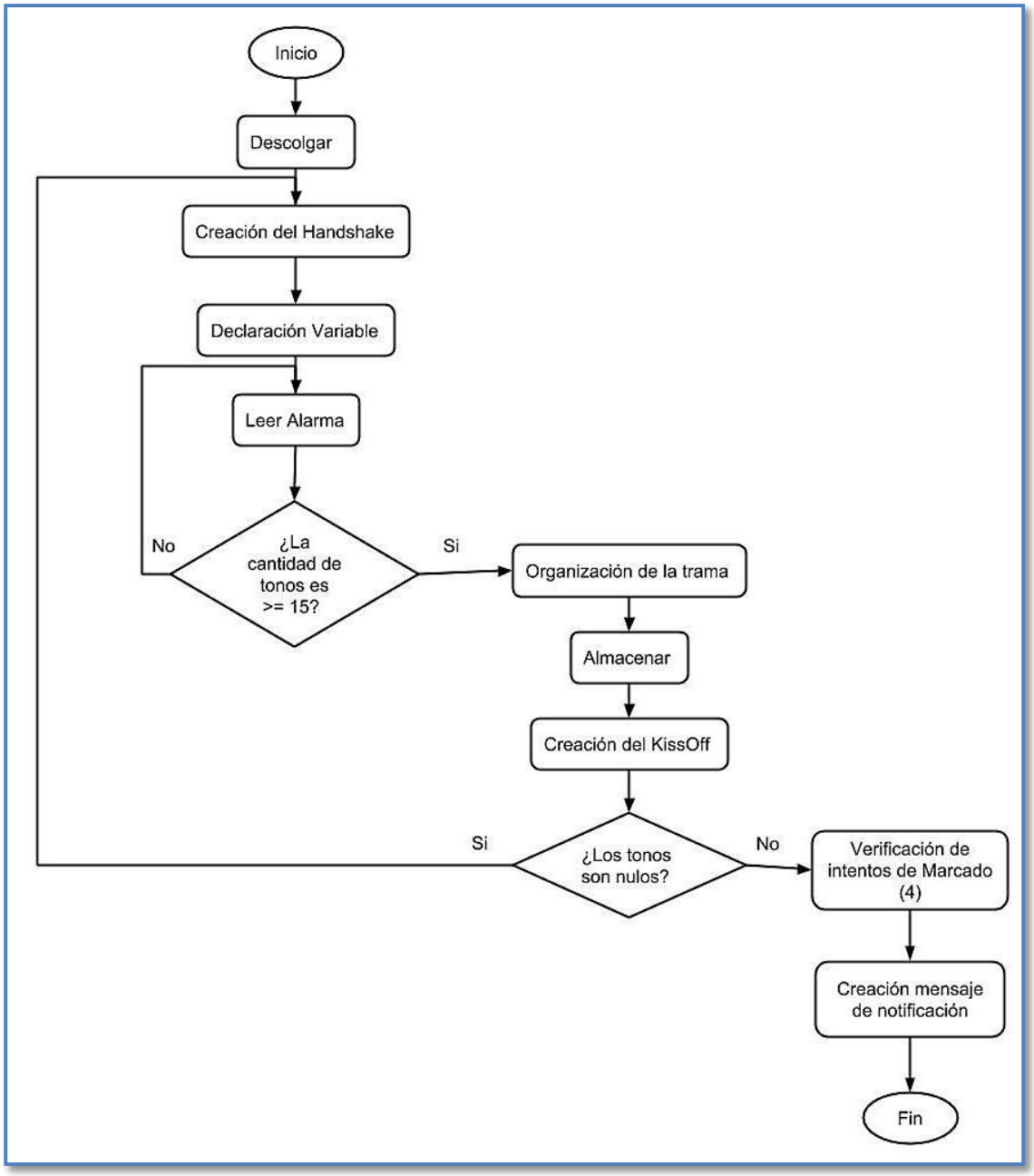


Figura 3.10 Diagrama general del proceso del plan de marcado.

Se recibe la llamada proveniente del panel de alarmas, la central telefónica descuelga esta llamada, es decir brinda la respuesta mediante un cambio de señal de la polaridad para poder establecer la llamada y poder identificar que ha ocurrido un evento que debe ser notificado. Como se está trabajando con el protocolo Contact ID, es necesario implementar un esquema de lectura, por eso el primer paso en el proceso es la creación y envío del Handshake correspondiente a este

protocolo. Handshake es la señal de autorización que espera el panel de alarmas para poder transmitir la información que ha detectado de los sensores.

Una vez comienza el proceso de transmisión, se declara una variable *TONOS,* donde se almacena la información proveniente del panel de alarmas. Esta variable es utilizada en todos los procesos a partir de éste.

Se procede a ejecutar la función *LeerAlarma()*, mediante ésta se almacenan todos los tonos DTMF en la variable *TONOS*.

Se almacenan los tonos en la variable hasta que la cantidad sea mayor o igual a 15 para poder continuar con el siguiente proceso, de lo contrario se sigue ejecutando la función ya que esta cantidad es lo permitido para crear la trama de información según el protocolo Contact ID (**Sección 2.5.1**).

Con la cantidad de tonos aceptada se procede a crear la trama de información, dándole el significado a cada campo que la conforma según la agrupación de los tonos. Se almacenan los tonos en el siguiente proceso y se crea la señal KissOff correspondiente al protocolo Contact ID que permite indicarle al panel de alarmas que debe finalizar el envío de tonos.

Se verifica si los tonos almacenados son o no nulos, con nulos se refiere si la trama presenta errores o está incompleta, en caso de serlo vuelve a iniciar el ciclo para enviar la trama de manera correcta, de lo contrario se verifica cuántos intentos de marcado se han realizado con la misma trama, siendo 4 el límite máximo de intentos para no colapsar al servidor con el mismo evento. Una vez realizada la verificación se crea el mensaje de notificación del evento ocurrido.

Éste diagrama general de procesos del plan de marcado, se implementó de forma gráfica en la herramienta Visual Dialplan.

En la Figura 3.11 se muestran los macros creados en la herramienta Visual Dialplan para el plan de marcado del servicio desarrollado, con una pequeña descripción de su funcionamiento en general.

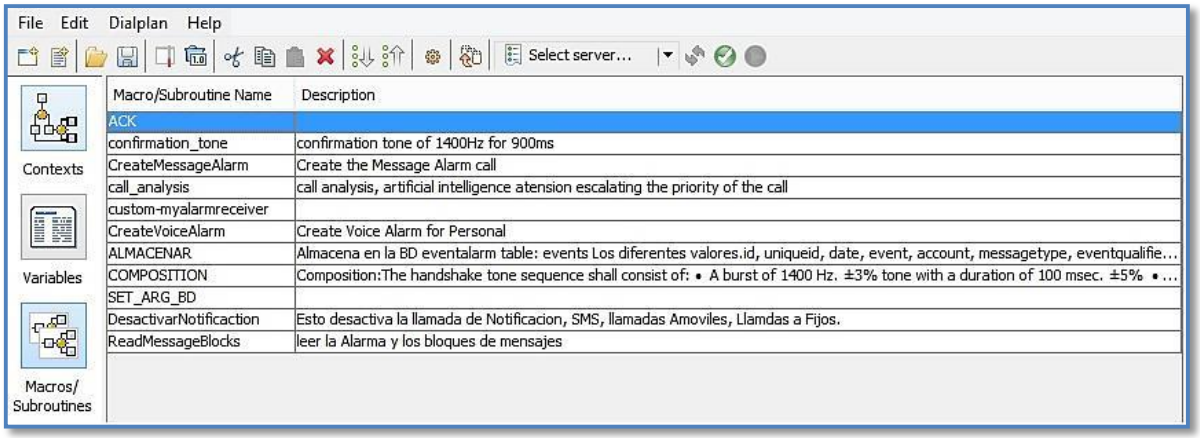


Figura 3.11. Macros creados en la herramienta para el plan de marcado.

Para este proyecto el contexto general en el que se trabaja tiene por nombre *principal,* y dentro de éste se presenta el esquema general del plan de marcado como se muestra en la Figura 3.12.

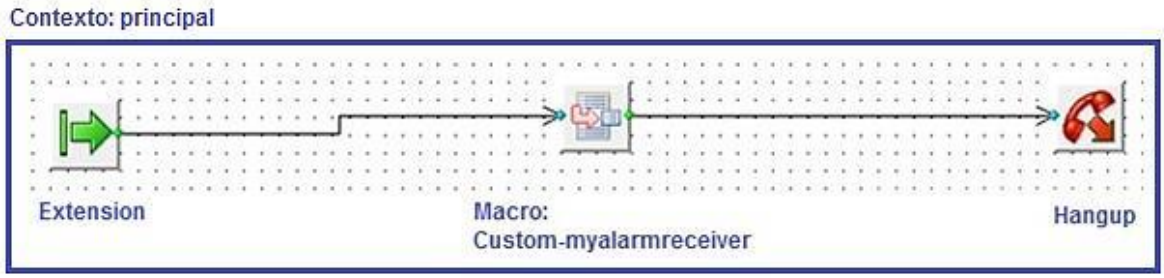


Figura 3.12 Esquema general del plan de marcado en el Receptor de Alarmas.

La llamada entrante es la proveniente del panel de alarmas y es capturada por el macro *Custom-myalarmreceiver* en cual se encuentra un conjunto de macros o funciones en bloque que analizan e identifican características de la llamada y el protocolo Contact ID. Para lo anterior, en la Figura 3.13 se muestran los llamados a otros macros y las funciones en bloque dentro del macro *Custom-myalarmreceiver*.

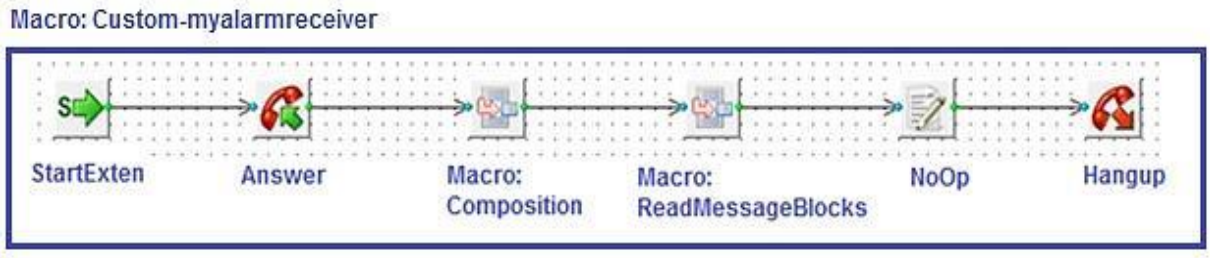


Figura 3.13 Esquema general del macro *Custom-myalarmreceiver.*

A continuación se explica el esquema general del macro *Custom-myalarmreceiver:*

I. **StartExten:** Entra la llamada proveniente del panel de alarmas. Se recibe la llamada entrante pero sólo se realiza un proceso de recepción, para posteriormente enviar la llamada hacia el siguiente bloque.

II. **Answer:** Este componente responde la llamada, si se cuenta con una especificación de tiempo Asterisk espera para responder, de lo contrario continua con la respuesta a la llamada entrante.

III. **Macro Composition:** La llamada continúa por este macro donde se especifica la creación del tono de invitación para el envío de la información del panel de alarmas. Según el protocolo Contact ID y como se explicó en la **Sección 2.5.1**, para la invitación de recepción de tonos el protocolo emplea el *Handshake* [18] que consiste en una ráfaga de tonos de 1400Hz durante 1000 milisegundos, una pausa de 100 milisegundos y otra ráfaga de 2300Hz durante 1000 milisegundos. En la Figura 3.14 se observa la implementación del *Handshake* mediante los valores de frecuencias y tiempos que identifican al protocolo Contact ID.

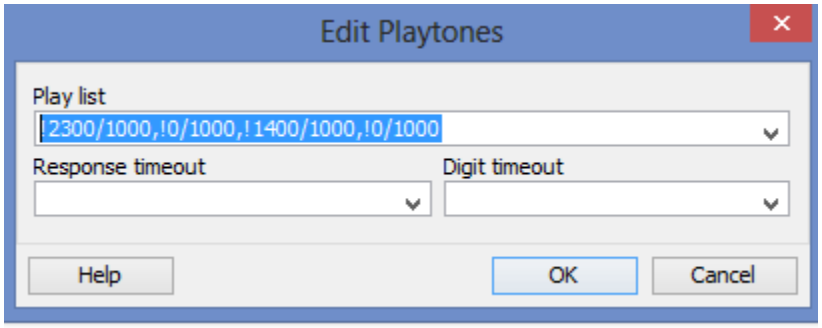


Figura 3.14. Lista de frecuencias y tiempos del Handshake.
(¡2300/1000,!0/1000,..) Significa f=2300 Hz durante 1000 milisegundos.
(…,!1400/1000,!0/1000) Significa f=1400 Hz durante 1000 milisegundos.

En resumen, el macro *Composition* es un bloque creado con la finalidad de que el receptor de alarmas pueda identificar el protocolo Contact ID en las frecuencias y tiempos de los tonos del *Handshake* correspondiente a este protocolo. También es la invitación que envía la central al panel para enviar la información.

III. Macro ReadMessageBlocks:

La llamada continúa por este macro en el cual se implementó la lógica mostrada en el diagrama de procesos de la Figura 3.15.

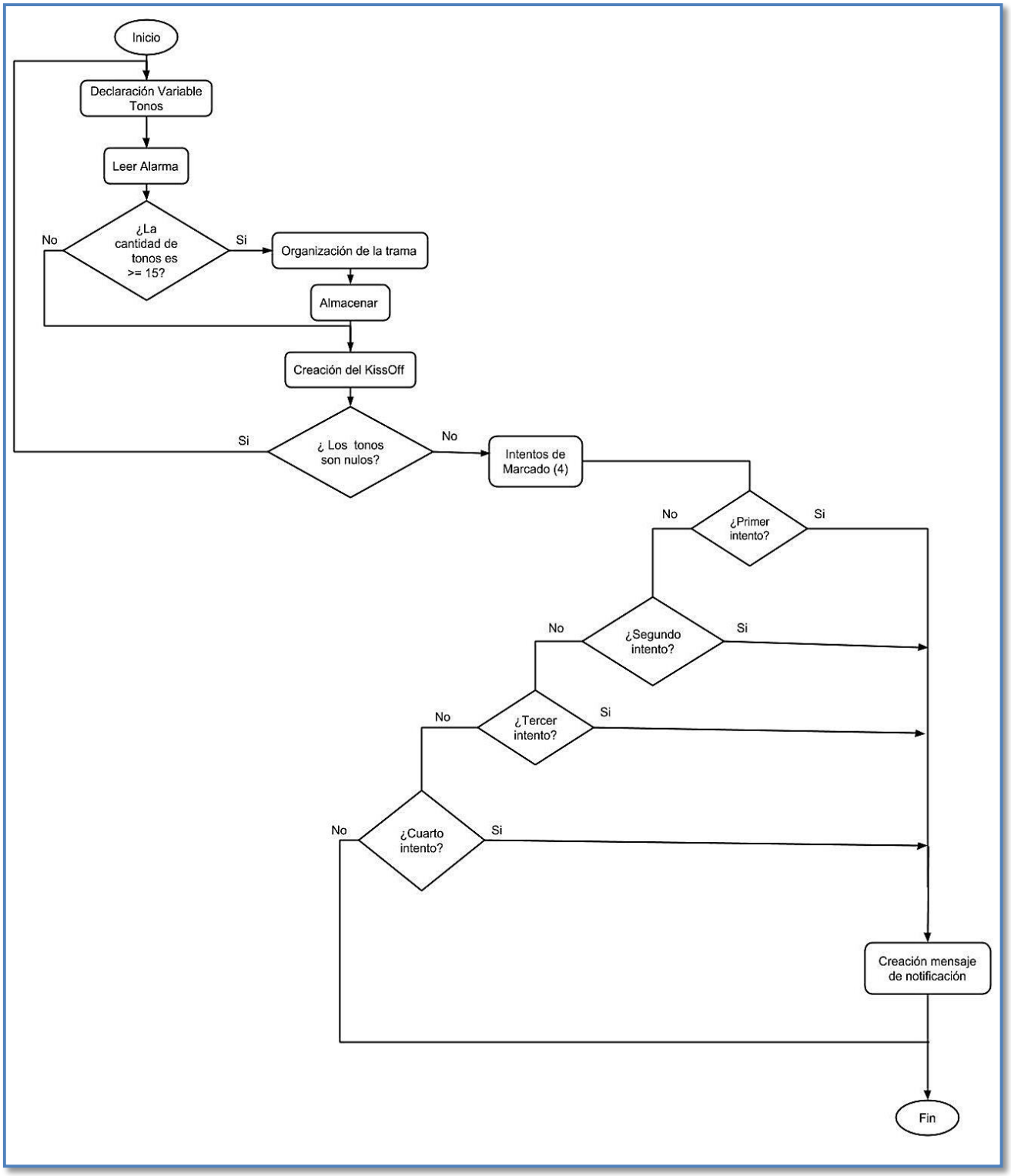


Figura 3.15. Diagrama del proceso de funcionamiento del macro ReadMessageBlocks.

La lógica de funcionamiento consiste: En primer lugar se hace la recepción de la llamada y se declaran variables para poder hacer una lectura del mensaje

proveniente del panel de alarma. Para poder armar la trama, primero se obtiene la información que ha sido almacenada en la variable TONOS en el archivo *LeerAlarma(),* luego se verifica que la cantidad de tonos almacenados para formar la trama de información sea igual a 15. Si cumple con esta primera condición, se procede a la formación de la trama, de lo contrario se envía al panel de alarmas el tono para la finalización de envío de información y se realiza un nuevo intento. Una vez armada la trama con la información, se almacena y se envía el tono para finalizar la recepción de la información. Continuando con el proceso de comunicación de la trama armada, a ésta se le realiza una nueva verificación para comprobar que los tonos no son nulos, en caso de ser nulos se vuelve a iniciar el ciclo para enviar la trama de manera correcta, de lo contrario se verifica cuántos intentos de marcado se han realizado con la misma trama. Con esto finaliza el funcionamiento del macro *ReadMessageBlocks.*

Para poder realizar la lógica de procesos en la herramienta Visual Dialplan, se implementaron doce bloques de acuerdo a los elementos y macros que ésta brinda. El resultado de la representación gráfica del diagrama de procesos es posible observarlo en la Figura 3.16.

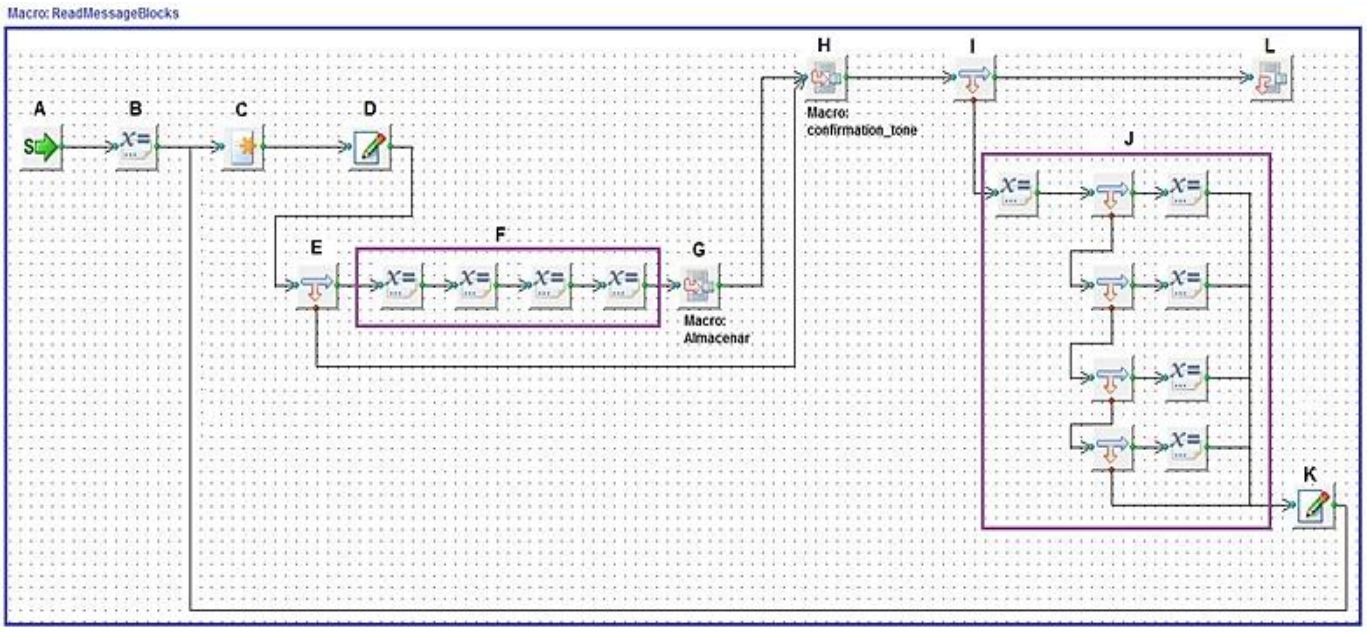


Figura 3.16. Esquema general del macro *ReadMessageBlocks.*

A. StartExten

Como se explicó anteriormente, en este bloque se hace la recepción de la llamada.

B. Set

Este componente es usado para fijar o declarar una variable de funciones de Dialplan.

C. Custom code

Mediante las características de este bloque, se utilizó en Visual Dialplan el código de Asterisk de la función *LeerAlarma()*, cuyo código es la versión con las mejoras realizadas al archivo *AlarmReceiver()* desarrollado para este proyecto. Como se mencionó anteriormente, la función de *LeerAlarma()* lee la información de los tonos DTMF provenientes del panel de alarma y la guarda en la variable *TONOS*.

D. Log

Mediante este componente es posible visualizar qué información se tiene hasta el momento y si está llegando el dato o la variable que se está necesitando, en este caso se espera recibir la variable *TONOS.*

E. GotoIf

Este componente es un condicional en el plan de llamada que permite verificar la cantidad de tonos recibidos para poder armar la trama correspondiente al mensaje con el protocolo Contact ID.

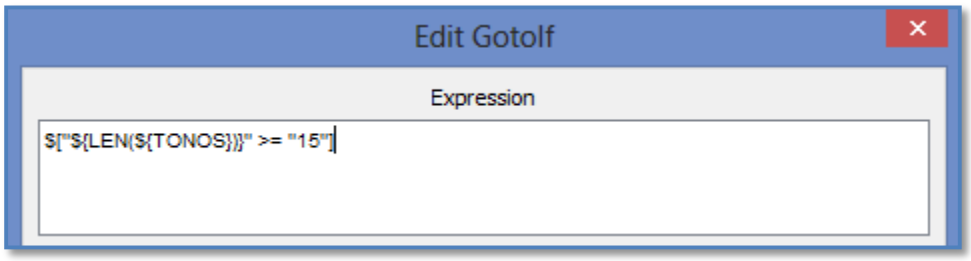


Figura 3.17. Configuración del Bloque GotoIf.

Como se observa en la Figura 3.17, la variable *TONOS* debe ser mayor o igual a 15 para continuar con el plan de llamadas y armar la trama, de lo contrario envía el tono de finalización de envío de información. El número 15 equivale al número de componentes en el mensaje que conforman la trama de información explicada en la **Sección 2.5.1**.

F. Set

En este bloque se arma la trama del protocolo Contact ID mediante la asignación de variables a partir de la información almacenada en la variable *TONOS.* Como se muestra en la Figura 3.18 las cuatro variables creadas son:

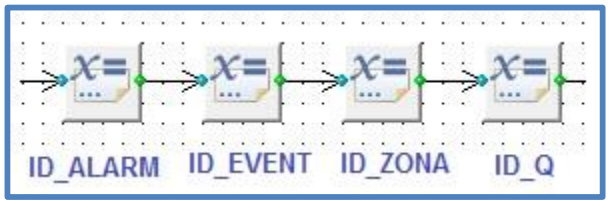


Figura 3.18. Variables del bloque Set.

- ID_ALARM
  Esta variable lee la cadena de tonos y almacena los 4 primeros, asignándolos a la identificación del cliente alarma.

- ID_EVENT
  Esta variable lee la cadena de tonos y almacena los 3 siguientes, asignándolos al código del evento ocurrido que se clasifica según la Tabla 2.2.

- ID_ZONA
  Esta variable lee la cadena de tonos y almacena los 3 siguientes, asignándolos como la zona en la que ocurrió el evento detectado por el panel de alarma.

- ID_Q
  Esta variable lee la cadena de tonos y almacena el siguiente tono, asignándolo como calificador del evento para informar específicamente que tipo de evento se presentó.

G. Macro: Almacenar

Para este macro se implementó la lógica de funcionamiento mostrada en la Figura 3.19.

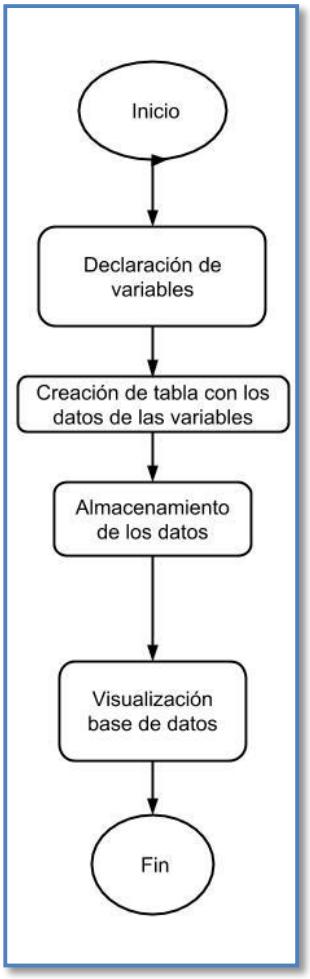


Figura 3.19 Diagrama de procesos del macro *Almacenar.*

La llamada continúa por este macro, en el cual se implementó de forma gráfica la lógica creada anteriormente. Esto es posible observarlo en la Figura 3.20.

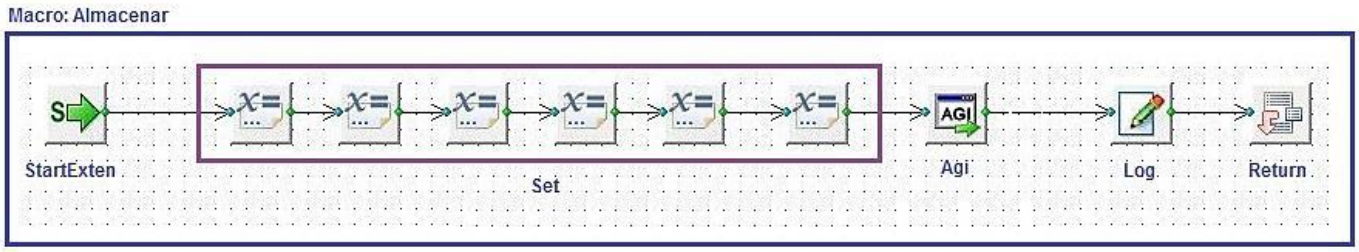


Figura 3.20. Esquema general del macro *Almacenar.*

- En **StartExten** se hace la recepción de la llamada.
- En **Set** fija variables como:
  - HostDB: La dirección IP de la base de datos.
  - UserDB: Usuario de la base de datos, en este caso root.

- PasswordDB: La contraseña para acceder a la base de datos, en este caso 031466.
- NameDB: Nombre de la base de datos, en este caso *eventalarm.*
- Fecha_Hora: Para indicar fecha y hora.
- Query: Pide información de las variables anteriores para completar la tabla mostrada por MySQL con todos los detalles del evento.

El resultado de esta configuración se observa en MySQL. Se muestra el resultado en la Tabla 3.1 creada con los respectivos datos consultados con la variable Query del evento ocurrido, esta tabla continua almacenando la información a medida que el panel de alarmas envía información al Receptor de alarmas.

```
mysql> select * from events;
+-----+--------------+---------------------+------------------+---------+-------------+----------------+-----------+---------+------------+-----------+
| id  | uniqueid     | date                | event            | account | messagetype | eventqualifier | eventcode | group_a | zonenumber | checksum  |
+-----+--------------+---------------------+------------------+---------+-------------+----------------+-----------+---------+------------+-----------+
| 915 | 1406192082.27 | 2014-07-24 03:54:49 | 6611181110000004 | 6611    | 18          | 1              | 110       | 00      | 000        | 4         |
| 916 | 1406192082.27 | 2014-07-24 03:54:53 | 6611183110000002 | 6611    | 18          | 3              | 110       | 00      | 000        | 2         |
| 917 | 1406192138.29 | 2014-07-24 03:55:44 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 918 | 1406192437.30 | 2014-07-24 04:00:44 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 919 | 1406192738.31 | 2014-07-24 04:05:45 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 920 | 1406193038.32 | 2014-07-24 04:10:44 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 921 | 1406193338.33 | 2014-07-24 04:15:45 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 922 | 1406193638.34 | 2014-07-24 04:20:44 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 923 | 1406193938.35 | 2014-07-24 04:25:44 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 924 | 1406194238.36 | 2014-07-24 04:30:44 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 925 | 1406194539.38 | 2014-07-24 04:35:46 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 926 | 1406194838.39 | 2014-07-24 04:40:44 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 927 | 1406195138.40 | 2014-07-24 04:45:44 | 6611181608000007 | 6611    | 18          | 1              | 608       | 00      | 000        | 7         |
| 983 | 1406895723.12 | 2014-08-01 07:22:09 | 6611181120000003 | 6611    | 18          | 1              | 120       | 00      | 000        | 3         |
| 984 | 1406895723.12 | 2014-08-01 07:22:14 | 6611183120000001 | 6611    | 18          | 3              | 120       | 00      | 000        | 1         |
+-----+--------------+---------------------+------------------+---------+-------------+----------------+-----------+---------+------------+-----------+
15 rows in set (0.00 sec)
```

Tabla 3.1. Información mostrada por MySQL con todos los detalles del evento.

- En **Agi** se realiza almacenamiento de los datos ejecutando la Interfaz Pasarela de Asterisk (**AGI,** *Asterisk Gateway Interface*). La AGI permite pasar variables creadas en la herramienta Visual Dialplan a otro lenguaje de programación, en este caso al lenguaje de programación Perl, para realizar consultas de la existencia de la llamada en curso y evitar que la central siga enviando en la llamada varias tramas con la misma información ya analizada. Mediante la AGI se retorna de nuevo a la herramienta Visual Dialplan con la información necesaria para continuar con el plan de marcado.
- En **Log** se visualiza la información que está llegando.
- En **Return** regresa hacia el macro ReadMessageBlocks para continuar con el plan de marcado.

En resumen, mediante este macro se captura toda la información proveniente del panel de alarmas y se almacena en la base de datos del Receptor de alarmas, *eventalarm.*

H. Macro: Confirmation_tone

La llamada continúa por este macro el cual realiza la configuración de frecuencias para la finalización de envío de datos que según el protocolo Contact ID se denomina KissOff y el cual se explicó en la **Sección 2.5.1**. Para KissOff el protocolo emplea frecuencias de 1400Hz y 1900Hz [18]. En la Figura 3.21 se observa la implementación del *Kissoff* mediante los valores de frecuencias según el protocolo Contact ID.

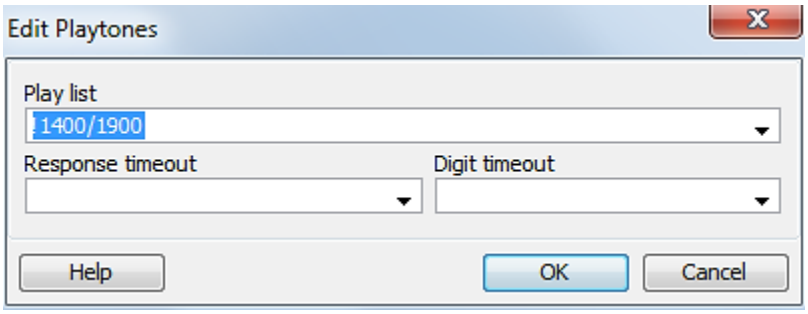


Figura 3.21. Configuración de frecuencias de KissOff para bloque Playtones.

En resumen, el macro *confirmation_tone* es un bloque creado con la finalidad de que el receptor de alarmas informe al transmisor, al panel de alarmas, que el mensaje ha sido recibido satisfactoriamente. Con este bloque se finaliza la implementación para la lectura del protocolo Contact ID.

Si el panel de alarmas no recibe esta señal de confirmación o KissOff, continua enviando datos. Cuando llega el tono de confirmación o KissOff al panel, éste automáticamente cierra el ciclo y no envía más datos.

I. *GotoIf*

Este bloque verifica si los tonos son o no NULL, como se mencionó anteriormente con NULL se refiere a verificar si la cadena de datos presenta errores o está vacía, en caso de serlo vuelve a iniciar el ciclo para enviar la trama de manera correcta, de lo contrario continua con el plan de llamada.

J. Intentos de Llamada

Si los tonos no son NULL comienza a analizarlos, se verifica cuántos intentos de marcado se han realizado con la misma trama, siendo 4 el límite máximo de intentos para no colapsar al servidor con el mismo evento.

K. Log

Permite visualizar la información que está llegando y verificar si es correcta.

L. Return:

Retorna al macro *Custom-myalarmreceiver* para continuar con el plan de marcado.

IV. NoOp:

Este bloque como su nombre lo indica NoOp (*No Operation*) no realiza ninguna operación, pero es el encargado de visualizar la información de la variable *TONOS* en la Interfaz de Línea de Comandos (CLI, *Command Line Interface*) de Asterisk.

V. Hangup: Finaliza o cuelga la llamada.

Una vez se presenta el estado de *Hangup* se cuelga la llamada, de esta forma se da por finalizado el proceso de comunicación de un evento desde el panel de alarmas hacia el Receptor de alarmas. El paso a seguir es establecer la comunicación del Receptor de alarmas y el Servidor de Monitoreo con la Estación de Notificación mediante la Alarma inteligente.

3.5.2 Comunicación del Bloque de Control y Almacenamiento con el Bloque de inteligencia.

Como se mencionó en la **Sección 3.5.1**, la central se encarga de recibir, guardar en la base de datos del Servidor de monitoreo, analizar la información del evento ocurrido y comunicarse con el Bloque de inteligencia para continuar con el respectivo proceso de notificación al usuario en la Estación de Notificación.

El Bloque de inteligencia está conformado por la Alarma Inteligente, cuyo elemento clave es el archivo *Ialarms.php,* donde se encuentran todas las funciones necesarias que permiten realizar un análisis adecuado de los eventos ocurridos, eventos que han sido anunciados por la central telefónica Asterisk y de los cuales se cuenta con información adicional en la base de datos del Servidor de Monitoreo. Este bloque es la parte autómata del servicio.

A continuación se presenta en la Figura 3.22, la comunicación de procesos entre estos bloques.

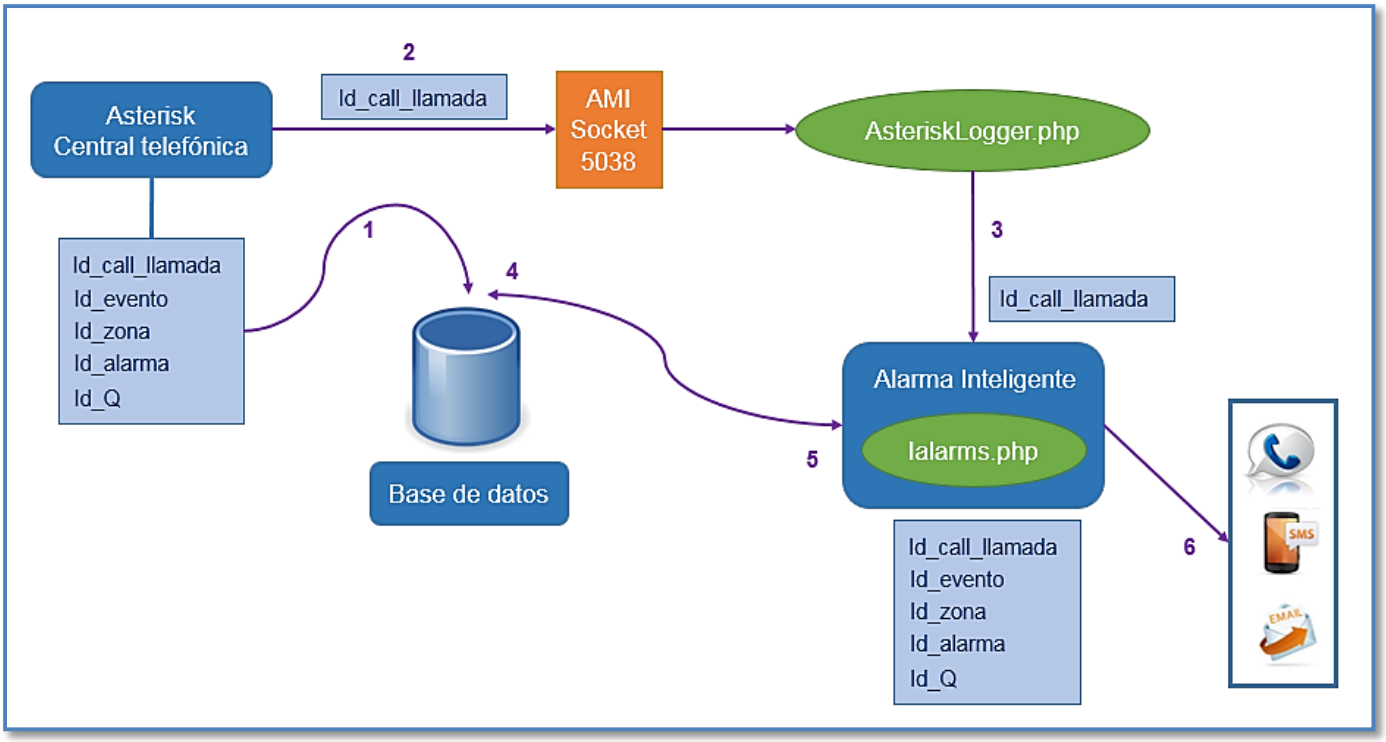


Figura 3.22. Comunicación de procesos entre bloques.

1. El Receptor de alarmas conformado por la central telefónica digital Asterisk, almacena en la base de datos del Servidor de Monitoreo, SugarCRM, toda la información del panel de alarmas almacenada en las diferentes variables.
2. Asterisk se conecta a través de la AMI por el puerto Socket 5038 para establecer comunicación con el archivo *AsteriskLogger.php,* encargado de analizar el evento mediante Alarma inteligente. La central envía únicamente el parámetro identificador de llamada hacia el archivo *AsteriskLogger.php*.
3. *AsteriskLogger.php* se comunica con Alarma inteligente para ejecutar el archivo *Ialarms.php*, enviándole el parámetro identificador de llamada. El archivo *Ialarms.php* permite analizar el evento de la siguiente forma: ¿Qué sensor se activó? ¿Cuál es la respuesta que se debe dar? ¿A quién se debe notificar? ¿Cómo se debe notificar?
4. Con el identificador de llamada recibido, *Ialarms.php* consulta en la Base de datos del SugarCRM la información complementaria del evento.
5. Con esta información consultada en la base de datos, completa los datos necesarios para poder realizar el proceso de notificación según el cliente y el evento ocurrido.
6. Se notifica al Usuario de Notificación por medio de tres canales de comunicación: Llamada telefónica, mensaje de texto y correo electrónico.

3.5.3 Implementación del Bloque de Inteligencia

En el proceso de notificación al usuario se cuenta con el archivo *Ialarms.php*, donde se ha implementado todo el proceso de notificación para los siguientes canales de comunicación: Mensaje de texto, correo electrónico y llamada telefónica. Como es posible observar en la **Sección 3.4.2**, este archivo es la parte fundamental del Bloque de inteligencia, es decir de la Alarma inteligente, que permite automatizar el servicio.

En el **Anexo D** se encuentra el código completo del archivo *Ialarms.php,* en esta sección se indica un resumen de la lógica de lectura en su estructura base.

Con toda la información consultada del evento en el archivo *Ialarms.php*, a partir de los parámetros: identificador de llamada y código del evento (*Id_call, eventcode*) mostrados en la Figura 3.23, se realiza el proceso de notificación.

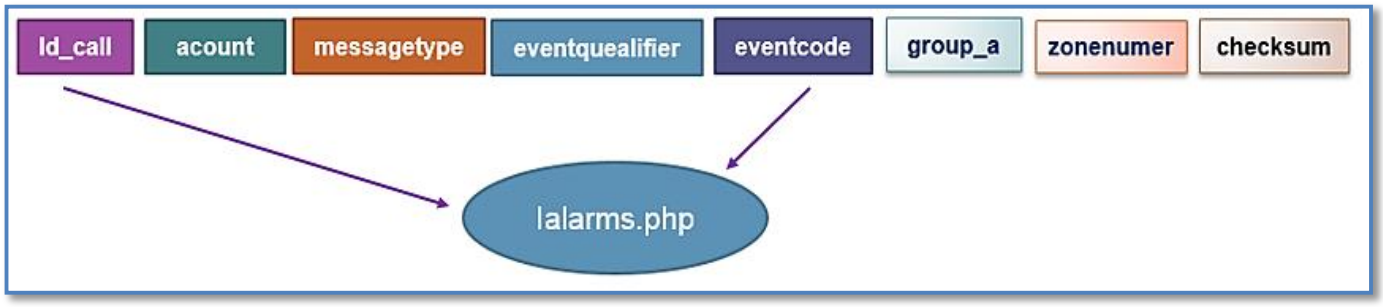


Figura 3.23. Parámetros utilizados por el archivo *Ialarms.php*.

La lógica de programación se presenta en los siguientes pasos:

1. A partir del parámetro identificador de llamada (*Id_call)*, se consulta información necesaria para el proceso de notificación, información como: correo electrónico del cliente, usuarios a ser notificados, información del sensor y el Plan de llamada de cada cliente.
2. Se crearon las funciones para cada tipo de notificación, como se observa en la Figura 3.24.

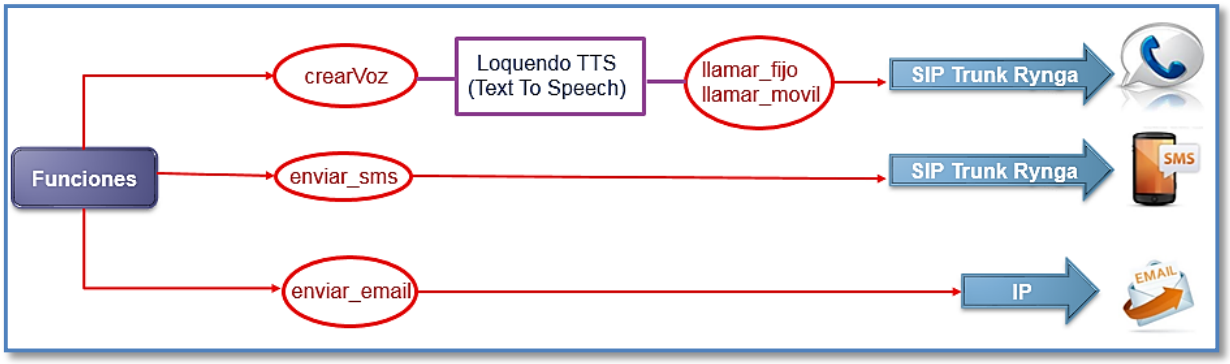


Figura 3.24. Funciones creadas para cada tipo de notificación.

Para notificación por llamada telefónica se tiene la función *crearVoz,* que por medio de un sintetizador de voz, Loquendo TTS, realiza la llamada a fijo o móvil a través de las sub-funciones *llamar_fijo* y *llamar_movil*. Para notificación por mensaje de texto y correo electrónico se tienen las funciones *enviar_sms* y *enviar_email* respectivamente. En la Figura 3.25, la Figura 3.26 y la Figura 3.27 se observa esta parte en el código.

```
function crearVoz($id_call,$mensaje)
{
        echo "\n PILAS IDECALL CREAR: $id_call";
        $path_mensaje="/etc/asterisk/ivr/mensaje_". $id_call .".txt";
        $path_voz="/etc/asterisk/voz/".$id_call;
        echo "\n ". $mensaje . "\n";
        system("/usr/bin/perl /var/lib/asterisk/agi-bin/TTSCreatefile.pl $path_mensaje '$mensaje'",$retorno);
        $COMMANDO="/opt/Loquendo/LTTS7/bin/VoiceExperience -Df=$path_voz.wav  -v Carlos -t -s $path_mensaje";
        echo "\nCOMMANDO: ". $COMMANDO . "\n";
        system("/usr/bin/perl /var/lib/asterisk/agi-bin/TTS.pl '$COMMANDO'");
        system("/usr/bin/sox $path_voz.wav  -r 8000 -c 1 $path_voz.gsm");
        system("/usr/bin/sox $path_voz.wav  -r 8000 -c 1 -t al $path_voz.alaw");
        system("/usr/bin/sox $path_voz.wav  -r 8000 -c 1 -t ul $path_voz.ulaw");
        return  $path_voz;
}
```

Figura 3.25. Función crearVoz.

```
function enviar_sms($N_SMS,$destino,$mensaje, $aep ,$id_callfull,$id_Q)
{

    $stateCall= $aep -> getStateCall($id_callfull,$id_Q);
    echo "\n  \n SMS ACTIVACION : $stateCall \n " ;
        //SI es =0 Termia con LOS.
    if ($stateCall  <> '0')
    {
        for($ne=0; $ne<$N_SMS;$ne++)
            {
                if(!empty($destino[$ne][3]))
                {
                    $desMovil="{$destino[$ne][4]}";
                    echo "\n  SMS A: $desMovil  MENSAJE:$mensaje \n";
                    echo sendSMS($desMovil,$mensaje) ;
                }
                }
    } //fin de If    $stateCall == '0'
}
```

Figura 3.26. Función *enviar_sms*.

```
function enviar_email($numero_email,$destino,$mensaje)
{

    for($ne=0; $ne<$numero_email;$ne++)
    {
     if(!empty($destino[$ne][5]))
      {
       $AG1="{$destino[$ne][5]}";
       $AG2="{$destino[$ne][1]}";
       $AG3 = $mensaje;
       if( strlen(strstr($AG1,'@'))>1 )
            {
                system("/usr/bin/php  /etc/asterisk/informe/enviarEmail.php '$AG1' '$AG2' '$AG3'");
                echo "\n Email $ne enviado a: ".$AG1."\n";
            }
      }
    }
 }
```

Figura 3.27. Función *enviar_email.*

3. Se definió una lista con los códigos de eventos más frecuentes según el Protocolo Contact ID, como se observa en la Figura 3.28.

```
100 => "Alarma Medica",
101 => "Alarma Medica Personal de Emergencia",
102 => "Fallo Reporte",
110 => "Alarma Incendio",
111 => "Alarma Humo",
112 => "Alarma Combustion",
113 => "Alarma Inundacion",
114 => "Heat",
120 => "Alarma Boton Panico",
121 => "Coacción",
122 => "Alarma, Boton Panico Silencioso",
123 => "Alarma,Boton Panico Audible",
130 => "Alarma  Intruzo",
131 => "Alarma,Intruzo en el Perimetro",
132 => "Alarma, Interior",
134 => "Alarma, Entrada / Salida",
135 => "Alarma, Dia  Noche",
139 => "Alarma Intrusion Verifier",
143 => "Alarma, Modulo de Expansion",
146 => "Alarma Silenciosa contra ladrones",
150 => "Alarma, 24 Hour Auxiliar",
301 => "Fallo Enegia alimentacion Aterna(AC)",
302 => "Fallo en la Bateria de Alimentacion",
305 => "Reinicio el Sistema",
333 => "Modulo de Expansion",
351 => "Fallo en la linea de Telecomunicaciones",
353 => "Problemas de Largo Alcance Radio",
354 => "Fallo en la Comunicacion del Evento",
373 => "Fallo de Circuito de Fuego",
374 => "Salir Alarma Error",
380 => "Fallo restaurar zona",
381 => "Supervisión RF ",
383 => "Fallo sensor RF",
384 => "Bateria Baja  Sensor RF ",
400 => "Armado Especial",
401 => "Armado de Alarma",
402 => "Desarmado, Armado",
403 => "Desarmado, Armado",
406 => "Cancelado por  Usuario",
407 => "Armado - Desarmado Remoto",
408 => "Quick Arm AWAY/MAX",
441 => "Armado Especial",
442 => "Armado Especial",
456 => "Armado Tarde para Cerrar",
455 => "Armado Automatico Cancelado",
456 => "Armado Parcial",
458 => "Reporte User on Premises",
459 => "Fallo de Activacion despues de armar",
570 => "Bypass",
601 => "Test Manual",
602 => "Reporte Periodico",
606 => "AAV to follow",
607 => "Test de Sistema",
608 => "Reporte de estado de alarma OK",
623 => "Event Log 80% Full",
629 => "1-1/3 Day No Event",
```

Figura 3.28. Lista de códigos de eventos.

4. El parámetro identificador del código de evento (*eventcode*) recibido, se almacena en una variable de tipo *string* para compararla con palabras claves como: Test manual, comunicación, reporte, desarmado, armado, fallo, alarma y evento desconocido. Estas palabras permiten identificar el tipo de evento según la lista de eventos creada anteriormente.

Figura 3.29. Proceso de identificación del tipo de evento.

5. Se procede con la formación del mensaje a ser enviado a los Usuarios de Notificación. El mensaje es el siguiente: “Alerta se le notifica que la alarma perteneciente a **[Nombre Usuario de notificación]** ubicada en la dirección

[Dirección principal del Cliente de la alarma] se activa, sensor ubicado en **[Descripción zona]**". Es posible observar el código en la Figura 3.30.

```
$this->mensaje = "ALERTA.SE LE NOTIFICA QUE LA ALARMA PERTENECIENTE A: {$destino[0][1]}.
                  UBICADA EN LA DIRECCION: $DIRECCION_ALARMA, SE ACTIVA: $MenEvent ($eventCode).
                  SENSOR ACTIVADO UBICADO EN: $DESCRIPCION_SENSOR";

$this->eventGrupo="1";
echo "\n PILAS IQ=1: " .$this->eventGrupo;
```

Figura 3.30. Mensaje de notificación.

6. Con el mensaje de notificación creado y conocido el plan de llamada del usuario a ser notificado, el Bloque de notificación envía el mensaje. Para notificación de llamada telefónica y mensaje de texto por medio de la SIP Trunk Rynga[13] [42] y la notificación de correo electrónico por medio de la conexión a Internet de la central, como se observa en la Figura 3.31.

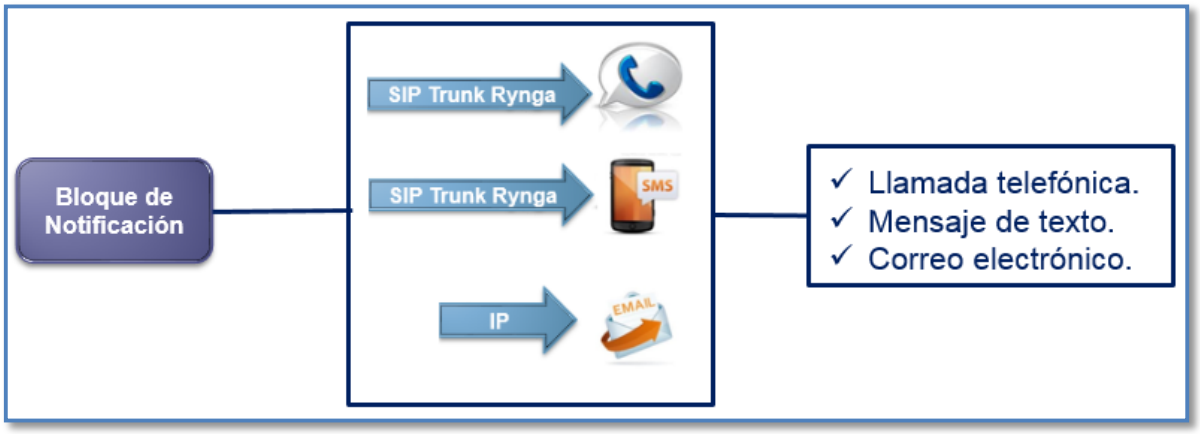


Figura 3.31. Proceso de Notificación.

En resumen, en el archivo *Ialarms.php* se crearon funciones con las cuales a partir de la información recibida, se identifica el tipo de evento ocurrido, se consulta la información del cliente de alarma y de su plan de llamada, y se estructura el mensaje de notificación según el canal de comunicación a notificar.

[13] SIP Trunk Rynga: Es un proveedor de VoIP utilizado como SIP Trunk por la empresa Advisor SAS.

3.6 IMPLEMENTACIÓN DE UN PROTOTIPO PARA ALARMAS DE TIPO MÉDICO

3.6.1 Introducción

Como complemento al trabajo de grado, se realizó una propuesta de implementación de un prototipo que permita monitorear alarmas de tipo médico, brindando una verificación continua de cierta variable clínica del estado de salud de un paciente como temperatura corporal, frecuencia respiratoria, pulso o presión sanguínea. A continuación se indica en esta sección la propuesta presentada de implementación de un prototipo inicial para monitoreo y notificación de alarmas médicas a partir del sistema desarrollado.

La idea surge al notar pacientes que debido a su enfermedad no pueden salir de los hogares y están bajo el cuidado de un familiar o una enfermera de cuidado en casa, si la persona a cargo del paciente se ausenta por un momento, no cuenta actualmente con algún medio para continuar monitoreando el estado de salud del paciente y ser notificado de cualquier emergencia [43]. Generalmente los sistemas utilizados para monitoreo de pacientes son de alto costo, ya que en algunos casos implementan dispositivos inalámbricos, ofreciendo de esta forma un servicio costoso y del cual no todos pueden estar beneficiados.

A diferencia de estos sistemas, en este proyecto se propone que a partir de un sistema de alarma convencional instalado en el hogar o en un centro médico, e integrando sensores de variables clínicas, se pueda notificar una emergencia médica a la persona encargada del paciente, mediante los canales de comunicación trabajados (llamada telefónica, mensaje de texto y correo electrónico), asegurando un medio de notificación para que el paciente sea atendido de manera inmediata y de una manera económica con respecto a otros servicios de monitoreo médico. Esto puede ser de gran interés para entidades de cuidado domiciliario o ancianatos donde no hay un médico o enfermera vigilando constantemente el estado de salud del paciente.

En esta sección se describe todo el procedimiento realizado para la implementación de un prototipo inicial que realiza la medición y monitoreo de la temperatura axilar de un paciente, se especifican los módulos de comunicación utilizados, una demostración de su funcionamiento y por último conclusiones de esta sección y posibles ampliaciones en el trabajo para este prototipo.

3.6.2 Arquitectura del Sistema

En la Figura 3.32 se expone la arquitectura general del sistema.

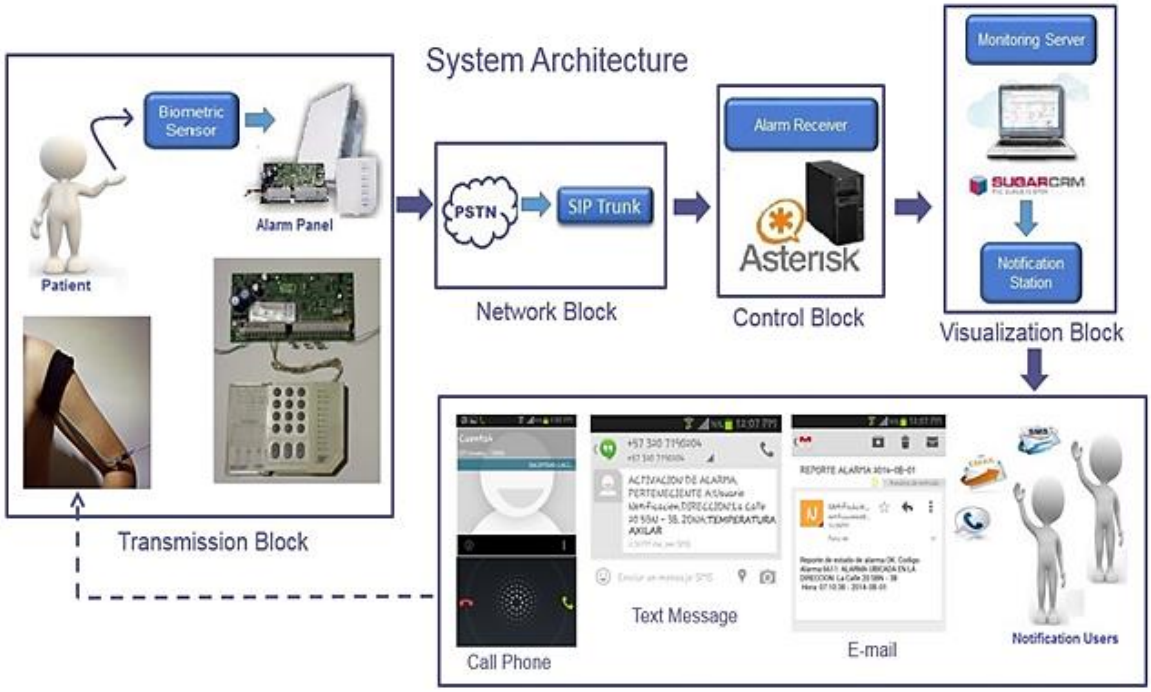


Figura 3.32. Arquitectura general [43].

Como es posible observar, se trabaja con un esquema basado en cuatro bloques de comunicación: Bloque de Transmisión, Red, Control y Visualización. El primer paso a realizar es la configuración del sensor de temperatura axilar, seguido de la configuración de la interfaz que permita la comunicación entre el sensor y el panel de alarmas, para finalmente determinar la comunicación entre los bloques y los usuarios de notificación.

3.6.2.1 Configuración e Implementación del Sensor Biométrico

El tipo de sensor implementado en este proyecto mide la temperatura axilar de un adulto, teniendo en cuenta que su valor en condiciones normales debe estar entre 35.5°C y 37°C [44], si es inferior o superior a este rango se debe alertar sobre este evento. Se trabajó con un sensor LM35 [45] calibrado para mediciones de temperatura corporal. A continuación en la Figura 3.33 se observa la adaptación realizada para que el paciente pueda hacer uso del sensor.

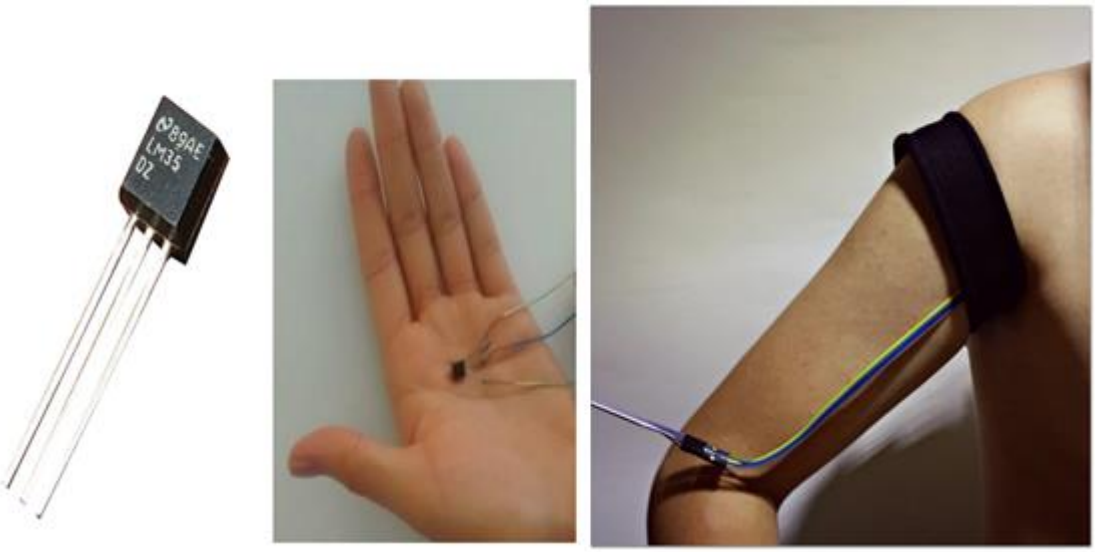


Figura 3.33 Sensor de Temperatura Axilar.

- Interfaz de comunicación entre sensor y panel de alarma:

Fue necesario diseñar la interfaz mostrada en la Figura 3.34 que permite la comunicación entre el sensor y el panel de alarmas [43].

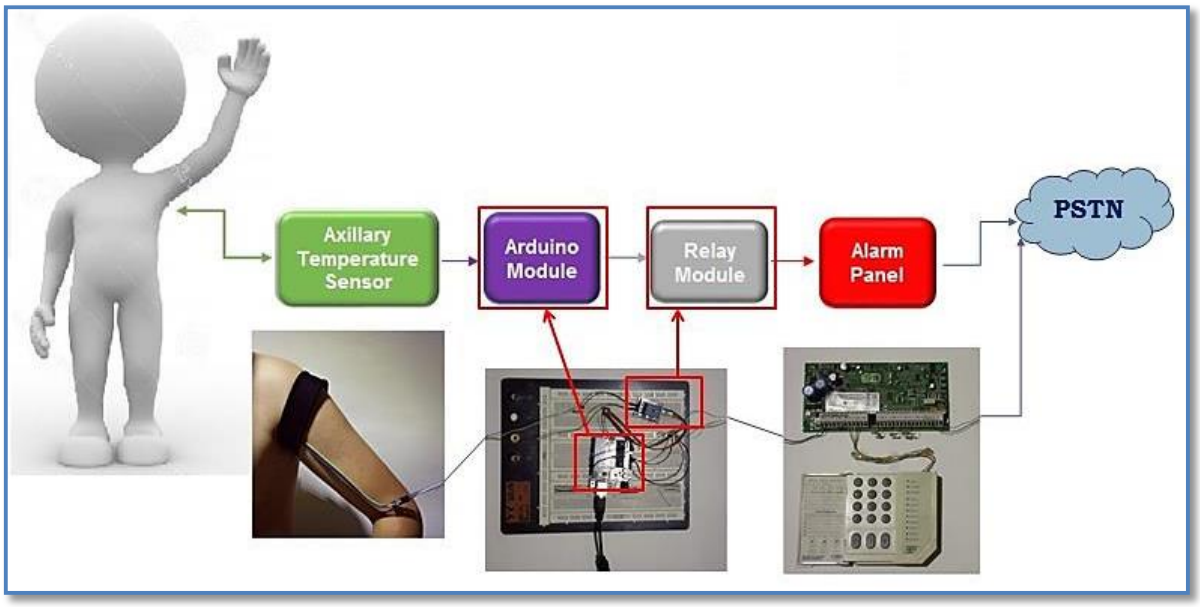


Figura 3.34. Interfaz de comunicación entre el sensor y el panel de alarma [43].

En el primer bloque "*Axillary Temperature Sensor*" se tiene el sensor de temperatura axilar que se comunica con el bloque Arduino o *"Arduino Module",* el cual mediante la utilización de una tarjeta Arduino recibe el voltaje de salida del sensor (con una resolución de 10mV por °C) y lo transforma en temperatura

mediante un conversor Analógico/Digital de 10 bits integrado en la tarjeta Arduino y un código realizado, que además permite visualizar la temperatura en el monitor serial del entorno de programación.

Es necesario adicionar un indicador de alarma que dependa del valor de temperatura final, para esto la lógica creada fue la siguiente: Si la temperatura axilar del paciente se encuentra en el rango de condiciones normales [35.5°C – 37°C] el módulo Arduino NO manda una señal de alarma, de lo contrario si el valor es superior o inferior al rango, éste manda señal de alarma, con esto finaliza toda la inteligencia del bloque Arduino Module. El siguiente bloque a conectar es el bloque Relé o *"Relay Module"*, el cual como su nombre lo indica está conformado por un módulo relé que abre o corta su salida conectada a la alarma de acuerdo a la señal emitida por el bloque Arduino, permitiendo la apertura o cierre hacia el bloque panel de alarma o *"Alarm Panel".* Finalmente el panel de alarma establece comunicación hacia la PSTN.

3.6.2.2 Bloques de Comunicación

En este esquema se trabaja con sensores biométricos y no con sensores de seguridad residencial, y el panel se comunica con la central telefónica por medio de la red telefónica pública conmutada PSTN, no por medio de IP.

El proceso de comunicación del evento de tipo médico es el siguiente y es posible observarlo en la Figura 3.32:

En el primer bloque *Transmission Block*, se tiene un paciente al cual se le desea monitorear cierta variable clínica de su estado de salud, en este caso la temperatura axilar con el sensor especificado. Para esto, mediante el sensor biométrico conectado al paciente se obtiene la medición de la temperatura axilar para su monitoreo, esta lectura del sensor es enviada al panel de alarmas para establecer comunicación con el siguiente bloque, *Network Block*.

En el bloque de Red o *Network Block* se comunica la información del panel de alarmas por medio de la red PSTN y posteriormente con una SIP Trunk hacia el siguiente bloque, *Control Block*.

El bloque de Control o *Control Block* está conformado por el receptor de alarmas, es decir una central telefónica digital Asterisk. El proceso mediante el cual el panel envía la señal al Receptor de alarmas o la central telefónica digital Asterisk es el expuesto en la **Sección 2.5.1**.

El Bloque de Control lee los eventos recibidos del panel de alarmas y los envía a *Visualization Block*.

En el Bloque de Visualización o *Visualization Block* se encuentra el Servidor de monitoreo y la Estación de notificación. El Servidor de monitoreo está formado por una arquitectura SugarCRM que estudia el tipo de evento, una vez conoce la acción que debe tomar hace conexión con la Estación de notificación para informar a los Usuarios de Notificación sobre la emergencia médica por medio de tres canales de comunicación: Llamada telefónica, mensaje de texto y correo electrónico.

Hay una comunicación entre el usuario notificado y el paciente para la debida atención de la emergencia médica, ya que no sólo se informa sobre el estado de salud del paciente, sino que hay una respuesta por parte del personal a cargo. Esta respuesta no hace parte del sistema pero es una acción que se debe realizar.

3.6.3 Demostración

Cuando el prototipo fue montado se realizó un plan de pruebas, los resultados fueron los siguientes:

Las pruebas se realizaron sobre tres personas que dieron su consentimiento para colaborar voluntariamente. Inicialmente la persona estaba en reposo, luego se ubicó el sensor de temperatura sobre su axila. Se quiso hacer una prueba tentativa de disminución de temperatura para probar las alarmas, las medidas obtenidas se observan en la Figura 3.35.

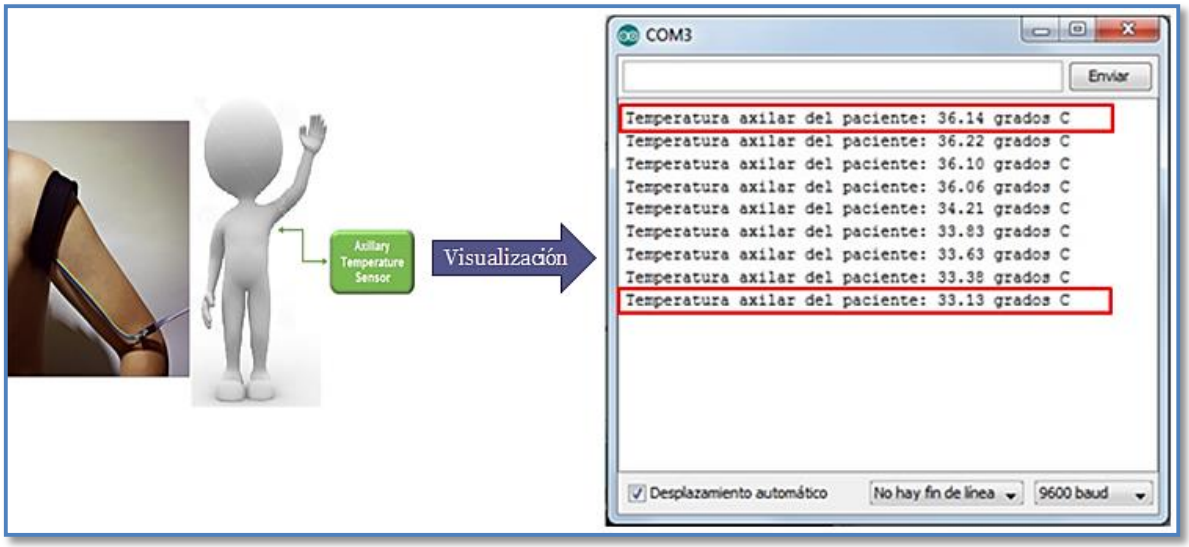


Figura 3.35. Visualización de la temperatura medida en el paciente. [43].

Se observa que la temperatura del paciente disminuyó de un valor normal de 36.14°C hasta 33.13°C, lo que activa la señal de emergencia médica en la zona donde está conectado el sensor.

El panel de alarma recibe esta señal de emergencia y se comunica con la central enviando toda la información del evento ocurrido. Este proceso es posible observarlo en la base de datos MySQL mostrada en la Figura 3.36.

date	event	account	messagetype	eventqualifier	eventcode	group_a	zonenumber	checksum
2014-07-24 03:54:49	6611181110000004	6611	18	1	100	00	008	4
2014-07-24 03:54:53	6611183110000002	6611	18	3	110	00	000	2
2014-08-01 07:22:09	6611181120000003	6611	18	1	120	00	000	3
2014-08-01 07:22:14	6611183120000001	6611	18	3	120	00	000	1

Figura 3.36. Información del evento recibido en el Receptor de alarma. [43]

La Figura 3.37 muestra la trama de comunicación recibida y estructurada según el protocolo Contact ID. La explicación de la trama de comunicación fue explicada en la **Sección 2.5.1**.

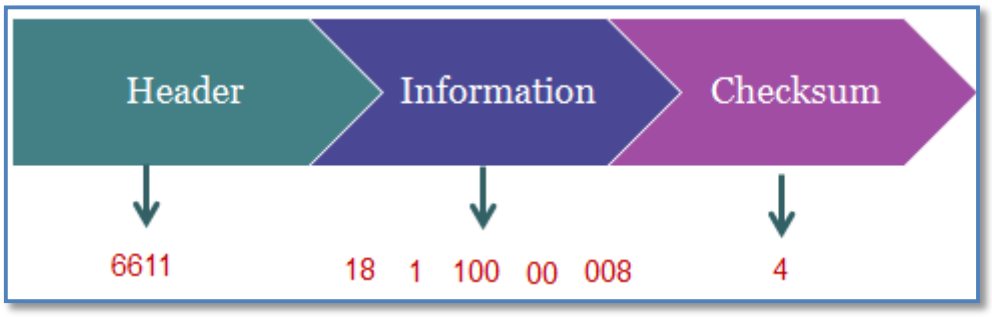


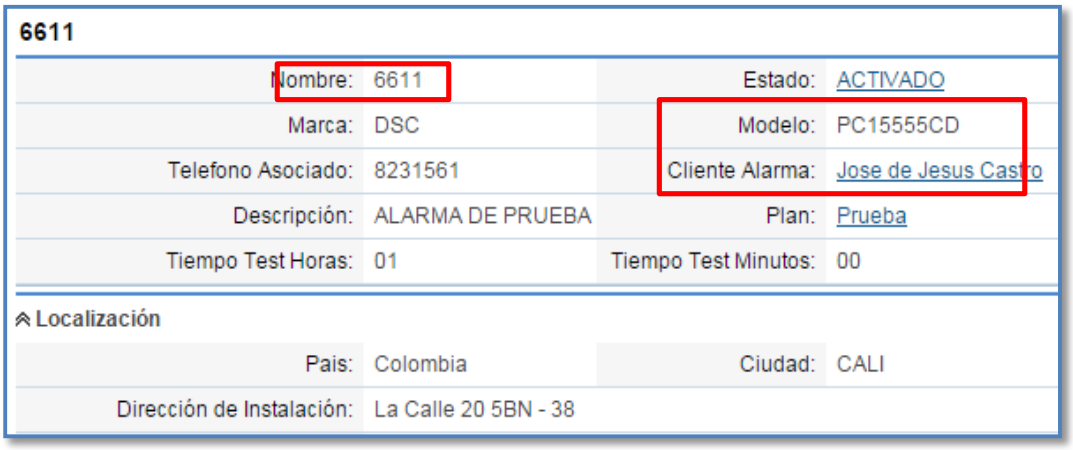
Figura 3.37. Trama de información recibida en el Receptor de alarma. [43]

- En la cabecera se tiene **6611**, el número de cuenta de usuario que identifica la alarma.
- En el campo de información se tiene:

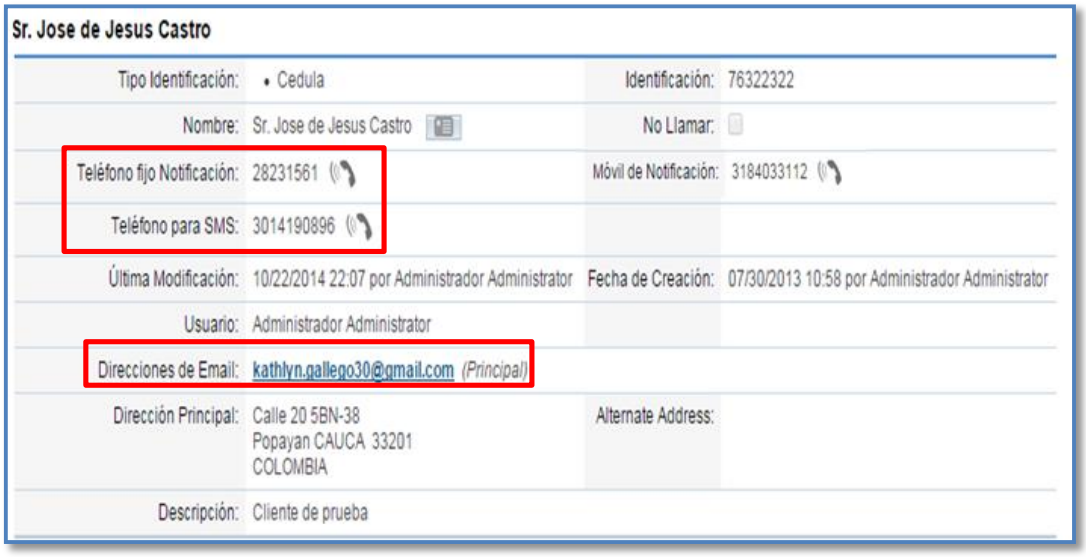
  18 Identifica que el mensaje se encuentra en formato Contact ID.
  1 Es el calificador del evento.
  100 Indica el código del evento, en este caso corresponde a una emergencia médica según el protocolo Contact ID, ya que maneja los códigos 100, 101 y 102 para informar eventos médicos.
  00 Significa la partición del panel de alarma.
  008 Es el número de zona donde se activó el sensor.

- **4** Checksum para comprobación de errores.

Una vez identificado el evento, la central envía el paquete de datos al Bloque de Visualización para la respectiva toma de decisiones según la información del paciente, en este caso se tiene almacenado en el sistema que ante una emergencia médica se debe informar al el señor José de Jesús Castro, del cual se tiene su correo y teléfono. En el SugarCRM también es posible observar la información almacenada del usuario 6611 y los sensores conectados en cada zona de la alarma, para este caso en la Zona 8 se encuentra el sensor de temperatura axilar. Todo lo anterior es posible observarlo en la Figura 3.38.



(a)



(b)

Zonas

Nuevo

Numero de la Zona	Activado	Tipo Sensor	Descripción Zona
006	Activado	CONTACTO	HABITACION NIÑOS
001	Activado	HUMO	COCINA
008	Activado	BIOMETRICO	TEMPERATURA AXILAR

(c)

Figura 3.38. Información almacenada en el SugarCRM (a) del usuario 6611, (b) del usuario de notificación y (c) de los sensores conectados en cada zona. [43]

Finalmente el usuario a cargo del paciente es notificado mediante tres canales de comunicación, en la Figura 3.39 se observa el mensaje recibido por mensaje de texto y por correo electrónico respectivamente. La notificación por llamada telefónica es mediante un mensaje de voz que dice: “Alerta se notifica que el sensor de temperatura axilar del paciente José de Jesús Castro excede su valor normal, alarma ubicada en la calle 20 5B-38”.

(a) (b)

Figura 3.39. (a) Notificación por mensaje de texto y (b) Notificación por correo electrónico. [43]

3.6.4 Conclusiones y Ampliaciones al Prototipo

Se presentan a continuación las conclusiones obtenidas para este prototipo inicial de alarmas de tipo médico:

- Se propone cambiar los sensores de seguridad usados comúnmente en los sistemas de seguridad por sensores biométricos para mediciones de variables clínicas.
- Las pruebas realizadas muestran que es posible implementar el servicio de alarmas de tipo médico y perfeccionarlo para ofrecerlo como un producto o servicio comercial.
- El sistema desarrollado es usable y de gran utilidad para quienes deseen monitorear el estado de salud de un familiar o un paciente, partiendo del sistema de alarma instalado en su propio hogar o centro médico, evitando de esta forma la contratación de servicios especiales y costos adicionales para cuidado domiciliario de un paciente.

Para este prototipo se proponen las siguientes ampliaciones que hacen de la propuesta un proyecto más comercial:

- Implementar el sistema con sensores adicionales, no sólo de temperatura sino también de frecuencia respiratoria, presión sanguínea y pulso, para monitorear otras variables clínicas en el estado de salud del paciente y así brindar un análisis más completo.
- Hacer uso de componentes de radio frecuencia y dispositivos médicos inalámbricos para desarrollar una Red Inalámbrica de Área Corporal (WBAN[14], *Wireless Body Area Network*), que le permita al paciente usar los sensores sin ningún tipo de cableado al panel de alarma para brindar mayor movilidad.
- Conectar más canales al panel de alarma puede permitir no sólo la identificación de una emergencia médica sino también diagnosticar una enfermedad.

[14] WBAN: Es una red de comunicación inalámbrica entre dispositivos de baja potencia utilizados en el cuerpo.

CAPÍTULO 4. PLAN DE PRUEBAS, EVALUACIÓN Y ANÁLISIS DE RESULTADOS

4.1 INTRODUCCIÓN

En el presente capítulo se muestran los resultados de un plan de pruebas realizado con el fin de validar la calidad del sistema y el correcto funcionamiento del servicio de monitoreo y notificación de eventos en un ambiente de prueba piloto de la empresa Advisor SAS.

Con el trabajo realizado en este capítulo se da cumplimento al cuarto y quinto objetivo específico propuesto:

- Validar la funcionalidad del sistema a través de un esquema de plan de pruebas en un ambiente de prueba piloto.
- Realizar un esquema de plan de pruebas que permita validar la calidad del sistema en un ambiente de prueba piloto de la empresa Advisor SAS.

4.2 ESQUEMA DEL PLAN DE PRUEBAS

Teniendo en cuenta el esquema de funcionamiento para las pruebas en laboratorio, especificado en la Figura 3.7, se muestra en la Figura 4.1 la implementación física realizada en un ambiente de prueba piloto de la empresa Advisor SAS.

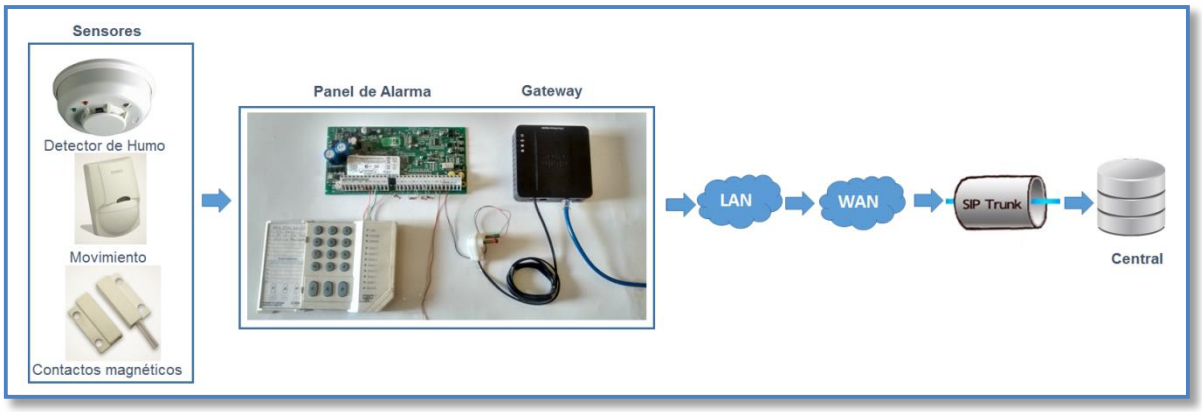


Figura 4.1. Implementación del esquema para pruebas en laboratorio.

Para el desarrollo de estas pruebas y validar el funcionamiento del servicio, se procedió creando siete usuarios según información proporcionada por Advisor SAS en la base de datos del SugarCRM, cada uno representa siete paneles de alarmas ubicados en hogares o empresas que cuentan con un sistema de seguridad.

Después de la creación de los usuarios se procedió a realizar una conexión básica para cada usuario, con una cantidad de sensores probados uno por uno para realizar unas pruebas de laboratorio que consistieron en:

- Verificar la trama de comunicación recibida con la información de los sensores activados y conectados al arreglo de cada usuario.
- Verificar el armado y desarmado de los paneles de alarmas.
- Finalmente se realizó una prueba de la tasa de error de tramas durante un determinado periodo de tiempo.

Con la contribución de la empresa Advisor SAS se realizó el esquema de plan de pruebas mencionado.

4.3 RECURSOS DISPONIBLES POR ADVISOR SAS

Con la autorización de los directores de la empresa Advisor SAS, se ejecutó el esquema de plan de pruebas planteado, haciendo uso de los recursos e instalaciones de la empresa, permitiendo validar el funcionamiento y la calidad del servicio en un ambiente de prueba piloto.

Dentro de las instalaciones se contó con recursos técnicos y humanos para el buen desarrollo del trabajo, como se consignan en la Tabla 4.1.

ADVAISOR SAS	
Recursos Técnicos	Acceso a Servidor PBX Asterisk 11X GNU FREE. S.O Centos 6.4
	Acceso a Servidor de pruebas CRM Sugar CRM FREE. Centos 6.4
	Acceso a IP Publica Red de gestión de LAN-WAN.
	Acceso a Alarma DSC 1555 de pruebas.
	Acceso a Línea telefónica SIP TRUNK de pruebas
Recursos Humanos	Ingeniero de Soporte asesor 2 horas semana.
	Técnico de Soporte Asesor 2 horas semana

Tabla 4.1. Recursos técnicos y humanos brindados por Advisor SAS.

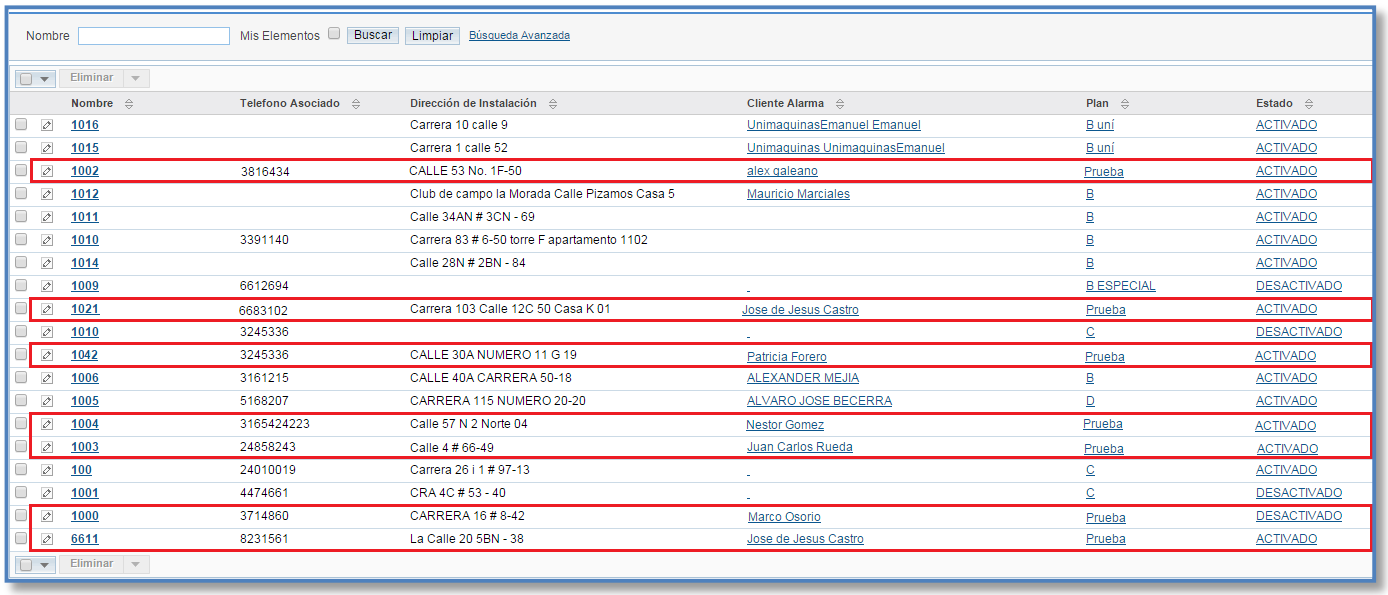
Se contó también con recursos tecnológicos y de investigación en infraestructura, herramientas software y acompañamiento en el desarrollo del servicio propuesto.

En el **Anexo F** se observa la certificación que demuestra que las pruebas se efectuaron en esta empresa con la supervisión del director.

4.4 PRUEBAS ESPECÍFICAS CON CADA USUARIO

En la arquitectura SugarCRM es posible ingresar y visualizar la información de los clientes y sus respectivos planes de alarma, con plan de alarma se hace referencia al paquete de servicios que el cliente escoge a conveniencia suya, definiendo el tipo de notificación, los *Usuarios de Notificación* y la cantidad de mensajes de textos, llamadas telefónicas o correos electrónicos que deseé recibir, con estas especificaciones es posible brindar un servicio personalizado a cada *Cliente de alarma.* Para el esquema de pruebas se planteó un plan de alarma nombrado "Prueba" que consistió en un mensaje de texto, una llamada telefónica y un correo electrónico enviado a un *Usuario de Notificación* creado. De esta forma se cuenta con los siete usuarios, la conexión con sus respectivos sensores y la información de notificación.

La Figura 4.2 muestra los siete usuarios creados en la herramienta SugarCRM y conectados al servidor de la empresa Advisor SAS, en cada uno es posible observar la siguiente información: Nombre, hace referencia al identificador de la alarma antes mencionado como ID de la alarma o *acount*, teléfono asociado, dirección de instalación, nombre del *Cliente de alarma*, plan de alarma y estado.


Nombre Mis Elementos Buscar Limpiar Búsqueda Avanzada

Eliminar

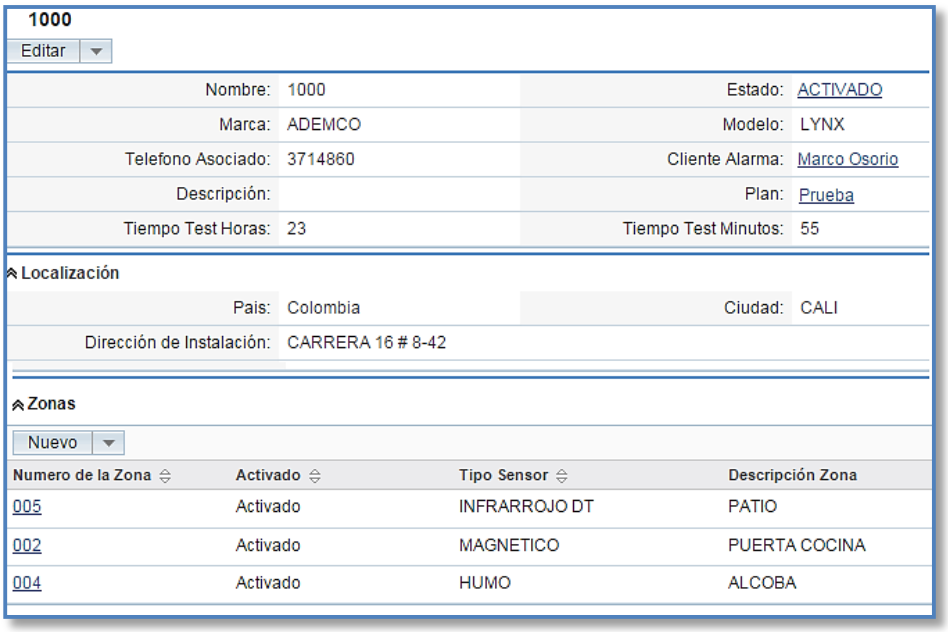
Nombre	Telefono Asociado	Dirección de Instalación	Cliente Alarma	Plan	Estado
1016		Carrera 10 calle 9	UnimaquinasEmanuel Emanuel	B uní	ACTIVADO
1015		Carrera 1 calle 52	Unimaquinas UnimaquinasEmanuel	B uní	ACTIVADO
1002	3816434	CALLE 53 No. 1F-50	alex galeano	Prueba	ACTIVADO
1012		Club de campo la Morada Calle Pizamos Casa 5	Mauricio Marciales	B	ACTIVADO
1011		Calle 34AN # 3CN - 69		B	ACTIVADO
1010	3391140	Carrera 83 # 6-50 torre F apartamento 1102		B	ACTIVADO
1014		Calle 28N # 2BN - 84		B	ACTIVADO
1009	6612694			B ESPECIAL	DESACTIVADO
1021	6683102	Carrera 103 Calle 12C 50 Casa K 01	Jose de Jesus Castro	Prueba	ACTIVADO
1010	3245336			C	DESACTIVADO
1042	3245336	CALLE 30A NUMERO 11 G 19	Patricia Forero	Prueba	ACTIVADO
1006	3161215	CALLE 40A CARRERA 50-18	ALEXANDER MEJIA	B	ACTIVADO
1005	5168207	CARRERA 115 NUMERO 20-20	ALVARO JOSE BECERRA	D	ACTIVADO
1004	3165424223	Calle 57 N 2 Norte 04	Nestor Gomez	Prueba	ACTIVADO
1003	24858243	Calle 4 # 66-49	Juan Carlos Rueda	Prueba	ACTIVADO
100	24010019	Carrera 26 i 1 # 97-13		C	ACTIVADO
1001	4474661	CRA 4C # 53 - 40		C	DESACTIVADO
1000	3714860	CARRERA 16 # 8-42	Marco Osorio	Prueba	DESACTIVADO
6611	8231561	La Calle 20 5BN - 38	Jose de Jesus Castro	Prueba	ACTIVADO

Eliminar

Figura 4.2. Información de los Clientes de Alarma presentes en el SugarCRM.

A continuación se presenta la información de los sensores asignados a cada uno de los usuarios creados con los que se realizó el plan de pruebas. Los sensores utilizados para las pruebas fueron: Sensor de contacto o magnético, sensor detector de humo, sensor de movimiento o infrarrojo y sensor biométrico.

- Usuario 1000:



1000

Editar

Nombre:	1000	Estado:	ACTIVADO
Marca:	ADEMCO	Modelo:	LYNX
Telefono Asociado:	3714860	Cliente Alarma:	Marco Osorio
Descripción:		Plan:	Prueba
Tiempo Test Horas:	23	Tiempo Test Minutos:	55

Localización

Pais:	Colombia	Ciudad:	CALI
Dirección de Instalación:	CARRERA 16 # 8-42		

Zonas

Nuevo

Numero de la Zona	Activado	Tipo Sensor	Descripción Zona
005	Activado	INFRARROJO DT	PATIO
002	Activado	MAGNETICO	PUERTA COCINA
004	Activado	HUMO	ALCOBA

Figura 4.3. Información en el SugarCRM del Usuario 1000.

- Usuario 1002:

1002

Editar

Nombre:	1002	Estado:	ACTIVADO
Marca:	as	Modelo:	
Telefono Asociado:	3816434	Cliente Alarma:	alex galeano
Descripción:		Plan:	Prueba
Tiempo Test Horas:	00	Tiempo Test Minutos:	15

Localización

Pais:	Colombia	Ciudad:	CALI
Dirección de Instalación:	CALLE 53 No. 1F-50		

Zonas

Nuevo

Numero de la Zona	Activado	Tipo Sensor	Descripción Zona
001	Activado	HUMO	COCINA
002	Activado	CONTACTO	SENSOR PASILLO PRINCIPAL

Figura 4.4. Información en el SugarCRM del Usuario 1002.

- Usuario 1003:

1003

Editar

Nombre:	1003	Estado:	ACTIVADO
Marca:	DSC	Modelo:	585
Telefono Asociado:	24858243	Cliente Alarma:	Juan Carlos Rueda
Descripción:		Plan:	Prueba
Tiempo Test Horas:	23	Tiempo Test Minutos:	55

Localización

Pais:	Colombia	Ciudad:	CALI
Dirección de Instalación:	Calle 4 # 66-49		

Zonas

Nuevo

Numero de la Zona	Activado	Tipo Sensor	Descripción Zona
002	Activado	Infrarrojo	Pir Entrada
004	Activado	Magnetico	Puerta Patio

Figura 4.5. Información en el SugarCRM del Usuario 1003.

- Usuario 1004:

1004

Editar

Nombre:	1004	Estado:	ACTIVADO
Marca:	1832	Modelo:	dsc
Telefono Asociado:	3165424223	Cliente Alarma:	Nestor Gomez
Descripción:		Plan:	Prueba
Tiempo Test Horas:	00	Tiempo Test Minutos:	30

Localización

Pais:	Colombia	Ciudad:	CALI
Dirección de Instalación:	Calle 57 N 2 Norte 04		

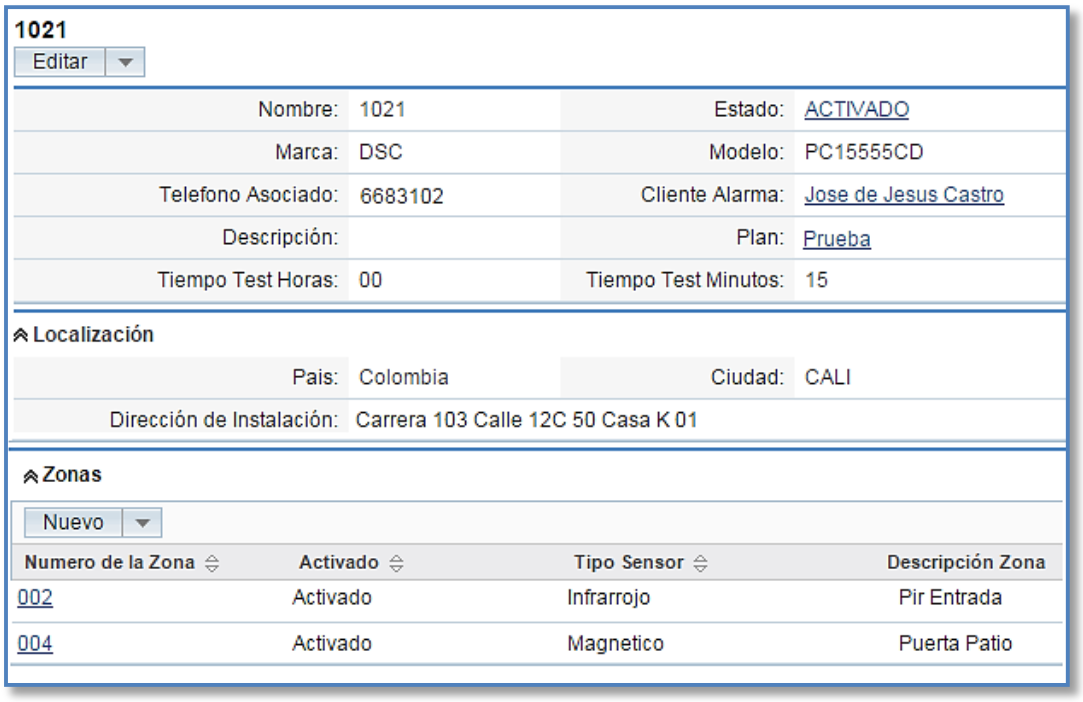
Zonas

Nuevo

Numero de la Zona	Activado	Tipo Sensor	Descripción Zona
003	Activado	MAGNETICOLIVIANO	PUERTA PPAL

Figura 4.6. Información en el SugarCRM del Usuario 1004.

- Usuario 1021:



1021

Editar

Nombre:	1021	Estado:	ACTIVADO
Marca:	DSC	Modelo:	PC15555CD
Telefono Asociado:	6683102	Cliente Alarma:	Jose de Jesus Castro
Descripción:		Plan:	Prueba
Tiempo Test Horas:	00	Tiempo Test Minutos:	15

Localización

Pais:	Colombia	Ciudad:	CALI
Dirección de Instalación:	Carrera 103 Calle 12C 50 Casa K 01		

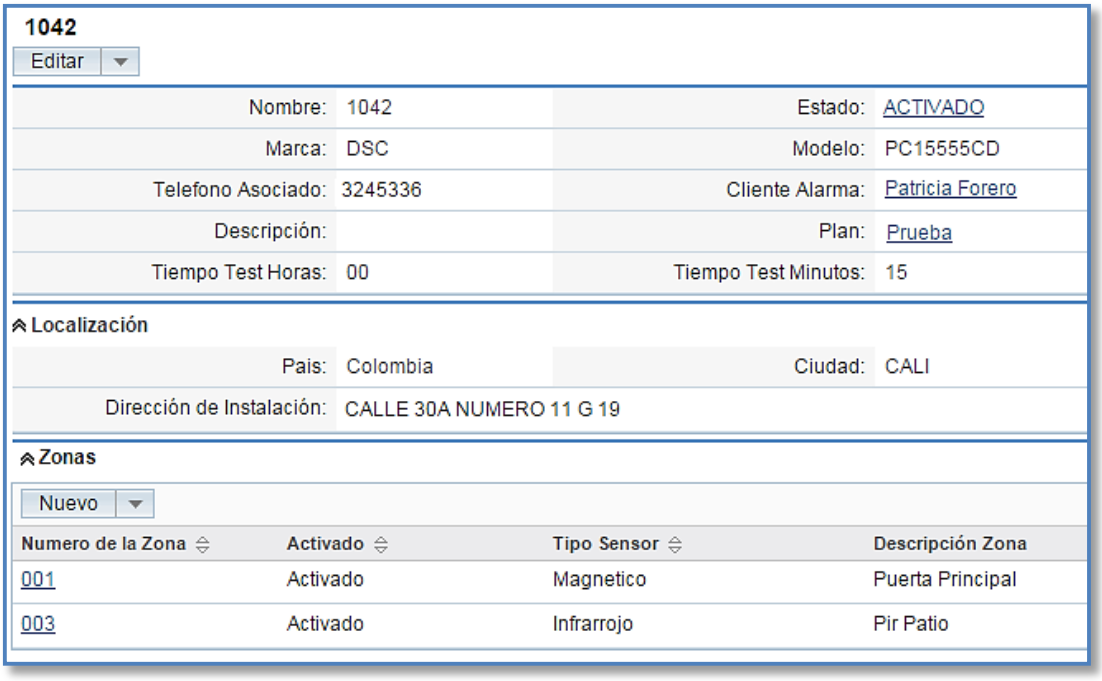
Zonas

Nuevo

Numero de la Zona	Activado	Tipo Sensor	Descripción Zona
002	Activado	Infrarrojo	Pir Entrada
004	Activado	Magnetico	Puerta Patio

Figura 4.7. Información en el SugarCRM del Usuario 1021.

- Usuario 1042:



1042

Editar

Nombre:	1042	Estado:	ACTIVADO
Marca:	DSC	Modelo:	PC15555CD
Telefono Asociado:	3245336	Cliente Alarma:	Patricia Forero
Descripción:		Plan:	Prueba
Tiempo Test Horas:	00	Tiempo Test Minutos:	15

Localización

Pais:	Colombia	Ciudad:	CALI
Dirección de Instalación:	CALLE 30A NUMERO 11 G 19		

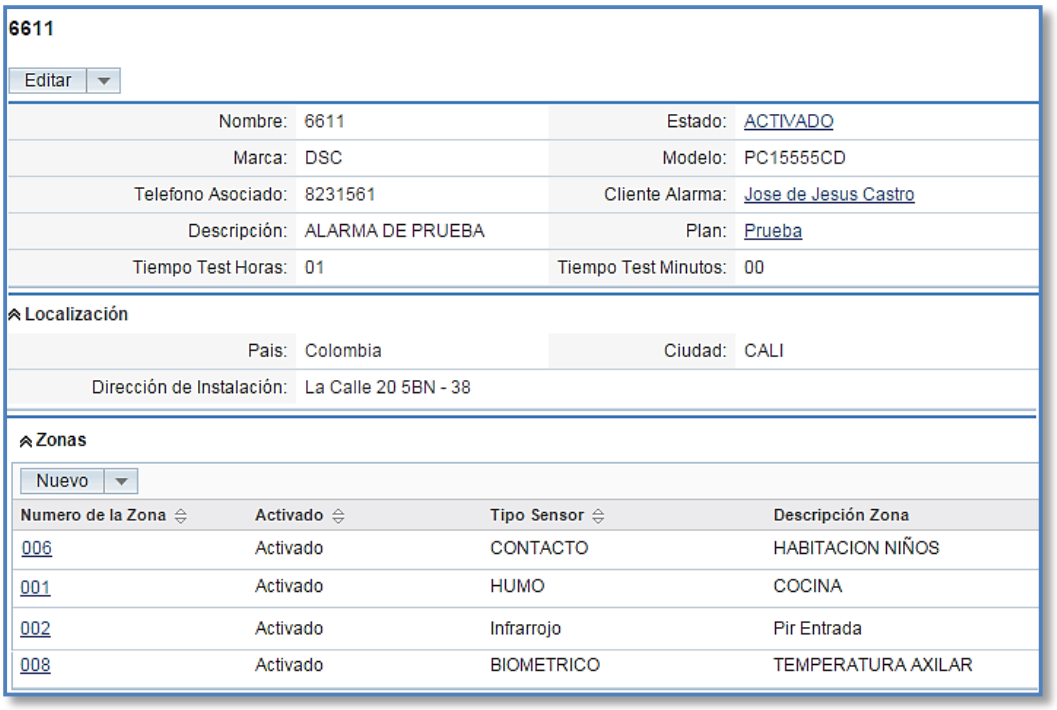
Zonas

Nuevo

Numero de la Zona	Activado	Tipo Sensor	Descripción Zona
001	Activado	Magnetico	Puerta Principal
003	Activado	Infrarrojo	Pir Patio

Figura 4.8. Información en el SugarCRM del Usuario 1042.

- Usuario 6611:



6611

Editar

Nombre:	6611	Estado:	ACTIVADO
Marca:	DSC	Modelo:	PC15555CD
Telefono Asociado:	8231561	Cliente Alarma:	Jose de Jesus Castro
Descripción:	ALARMA DE PRUEBA	Plan:	Prueba
Tiempo Test Horas:	01	Tiempo Test Minutos:	00

Localización

Pais:	Colombia	Ciudad:	CALI
Dirección de Instalación:	La Calle 20 5BN - 38		

Zonas

Nuevo

Numero de la Zona	Activado	Tipo Sensor	Descripción Zona
006	Activado	CONTACTO	HABITACION NIÑOS
001	Activado	HUMO	COCINA
002	Activado	Infrarrojo	Pir Entrada
008	Activado	BIOMETRICO	TEMPERATURA AXILAR

Figura 4.9. Información en el SugarCRM del Usuario 6611.

Teniendo en cuenta la información de estos usuarios, se planteó el siguiente plan de pruebas que permitió validar un correcto funcionamiento del servicio para monitoreo y notificación de eventos:

- **Usuario 1000**: Con este usuario se pretendió probar el armado del panel de alarmas y activación del sensor magnético en la Zona 2, indicado en la Figura 4.10 donde la primera casilla indica la acción que se provocó, la segunda casilla el tipo de sensor utilizado y la tercer casilla la zona de trabajo.

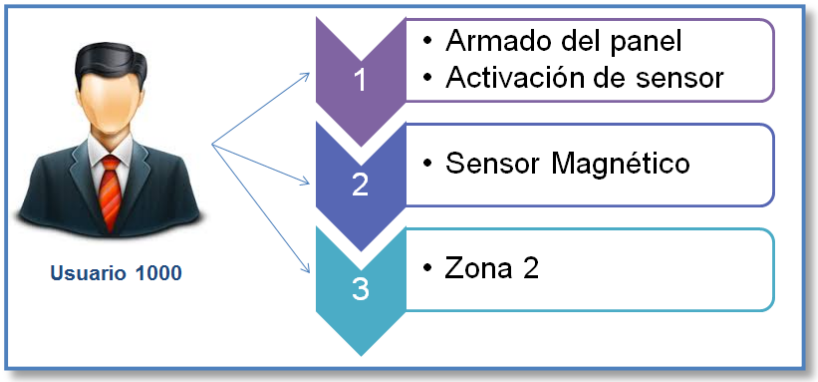


Figura 4.10. Prueba específica en Usuario 1000.

- **Usuario 1002**: Con este usuario se pretendió probar el armado del panel de alarmas y activación del sensor detector de humo en la Zona 4, como se indica en la Figura 4.11.

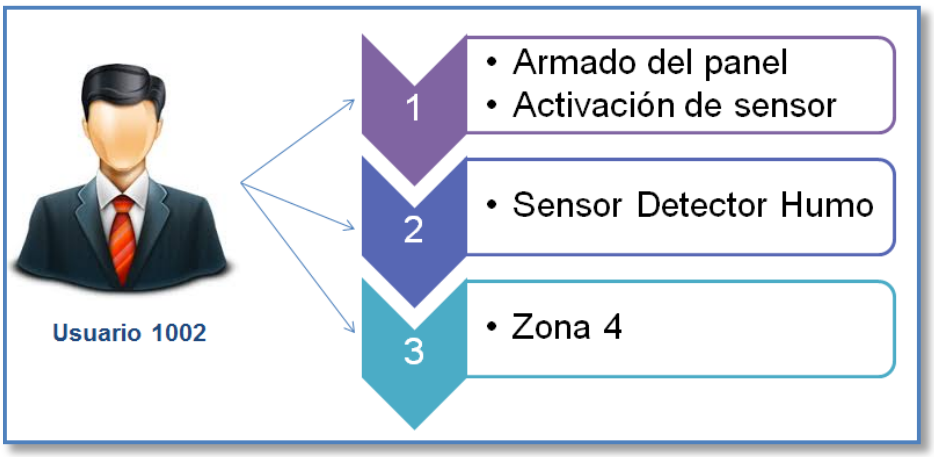


Figura 4.11. Prueba específica en Usuario 1002.

- **Usuario 1003**: Con este usuario se pretendió probar la activación del sensor magnético en la Zona 4, como se indica en la Figura 4.12.

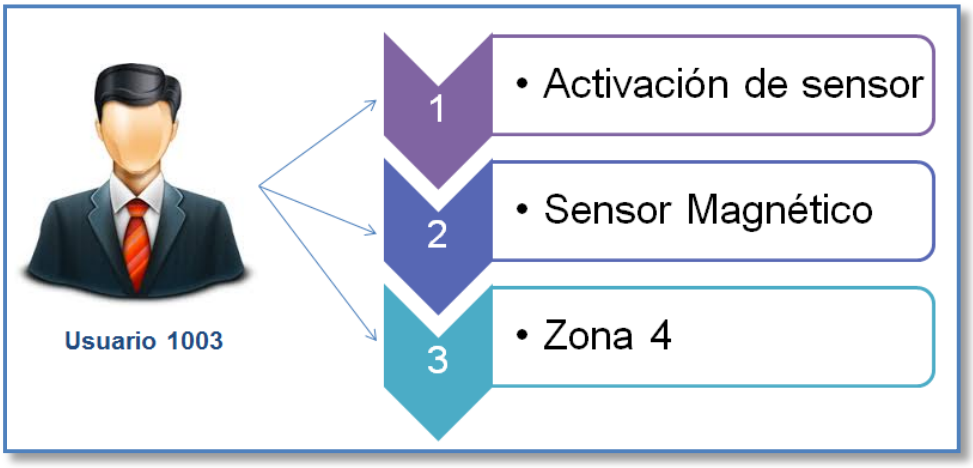


Figura 4.12. Prueba específica en Usuario 1003.

- **Usuario 1004:** Con este usuario se pretendió probar el armado del panel de alarmas y activación del sensor magnético en la Zona 3, como se indica en la Figura 4.13.

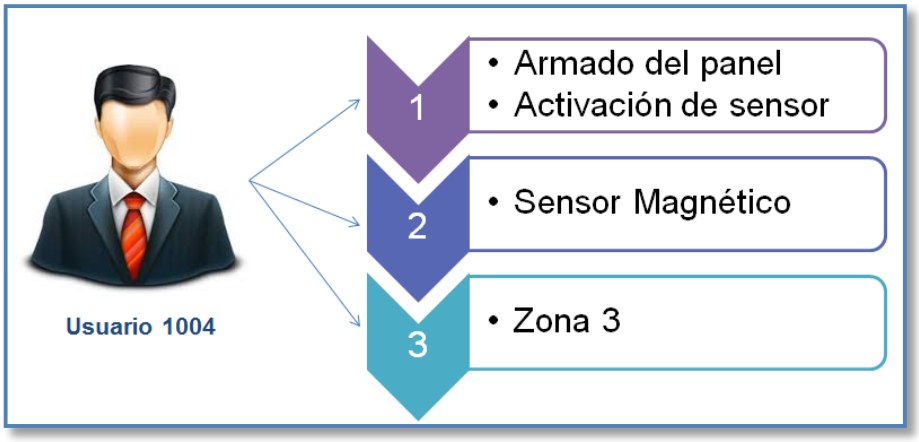


Figura 4.13. Prueba específica en Usuario 1004.

- **Usuario 1021:** Con este usuario se pretendió probar la activación del sensor magnético y de movimiento en las Zonas 4 y 2 respectivamente, como se indica en la Figura 4.14.

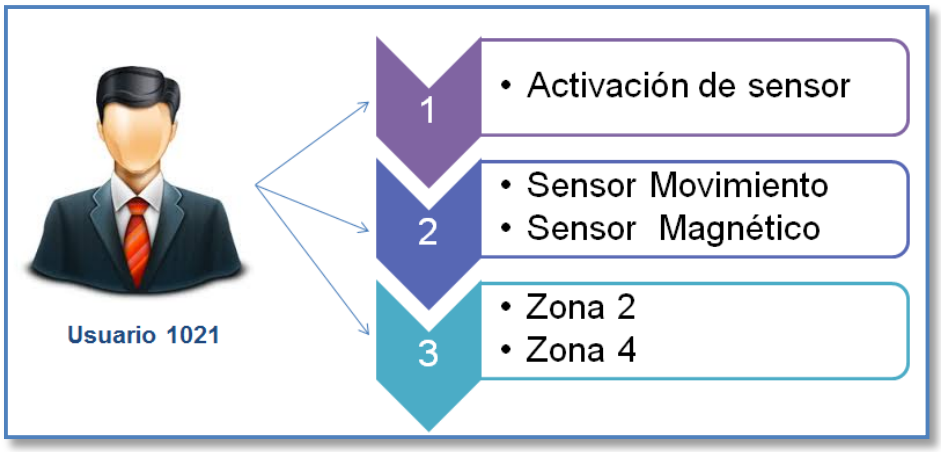


Figura 4.14. Prueba específica en Usuario 1021.

- **Usuario 1042:** Con este usuario se pretendió probar la activación del sensor magnético y de movimiento en las Zonas 1 y 3 respectivamente, como se indica en la Figura 4.15.

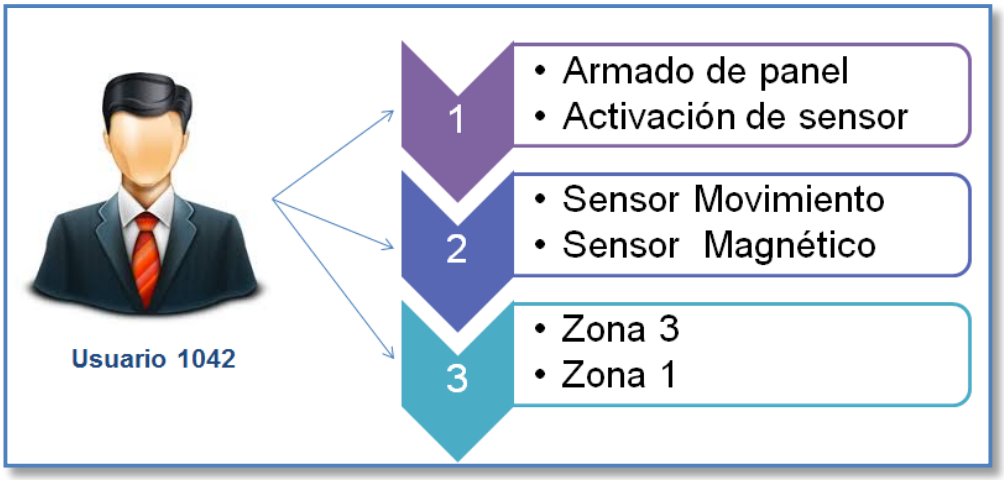


Figura 4.15. Prueba específica en Usuario 1042.

- **Usuario 6611:** Con este usuario se pretendió probar la activación del sensor magnético y sensor detector de humo en las Zonas 6 y 1 respectivamente, como se indica en la Figura 4.16.

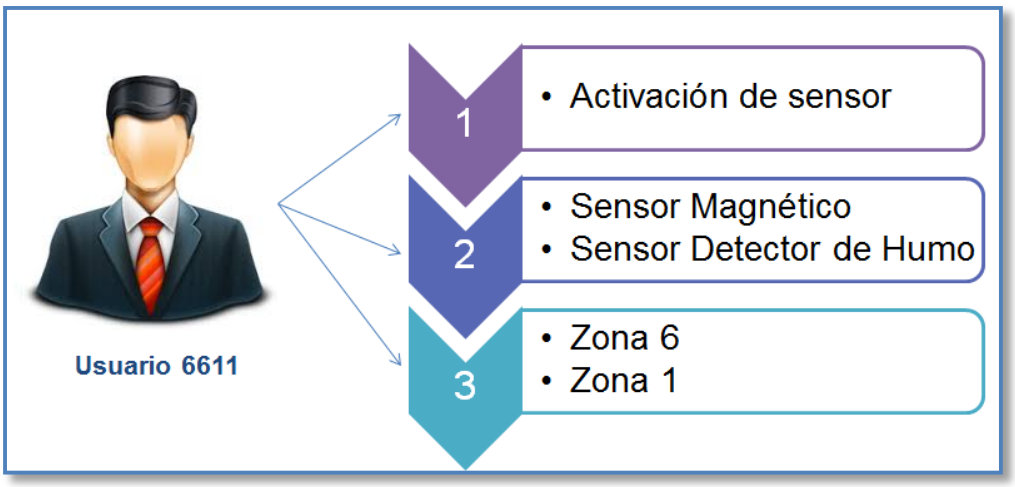


Figura 4.16. Prueba específica en Usuario 6611.

Teniendo en cuenta el esquema de pruebas planteado para cada usuario, se realizaron las pruebas respectivas y se analizaron los resultados.

4.5 OBTENCIÓN Y ANÁLISIS DE RESULTADOS

4.5.1 Obtención de Registros de los Eventos Ocurridos

Todos los eventos ocurridos se almacenan en la base de datos del Receptor de alarmas, la forma de visualizar la información almacenada en la base de datos es por medio del terminal en MySQL o mediante la herramienta DbVisualizer utilizada en este proyecto, ya que permite realizar múltiples conexiones simultaneas a distintas bases de datos, navegar por su estructura, ver características de los objetos de la misma y editar las tablas de una manera gráfica [46].

En primer lugar se deben identificar las bases de datos con las que se está trabajando, la Figura 4.17 muestra esta información obtenida a partir del terminal en MySQL.

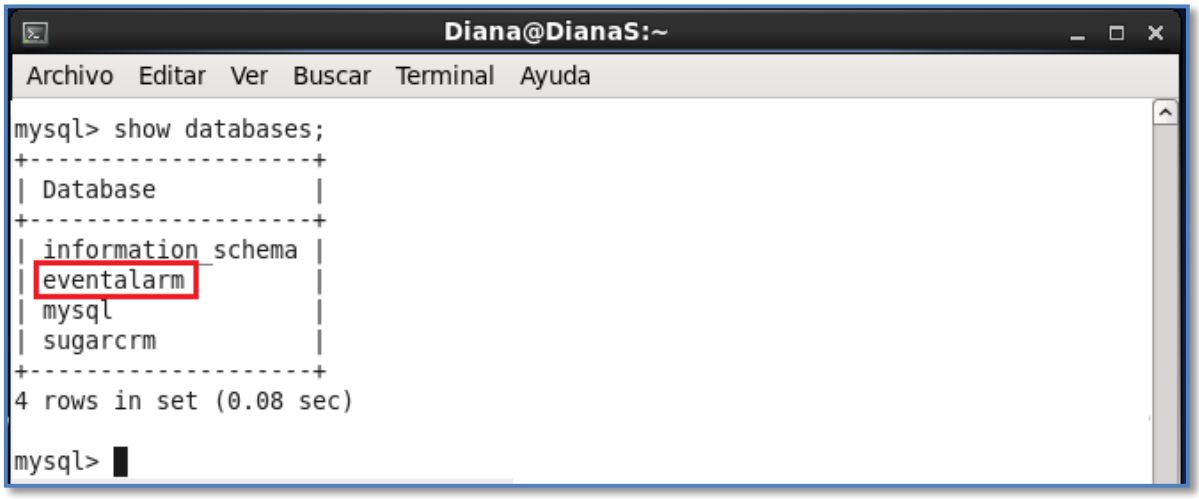


Figura 4.17. Bases de datos almacenadas en el Receptor de Alarmas.

Como es posible observar las bases de datos almacenadas en el Receptor de alarmas son: *information_schema, eventalarm, mysql* y *sugarcrm.* Los reportes de actividad de las alarmas de los siete usuarios se encuentran almacenados en la base de datos *eventalarm*. Para una mejor visualización de ésta base de datos se utilizó DbVisualizer, haciendo conexión desde ésta herramienta con el servidor MySQL del Receptor de alarmas, ingresando los datos de conexión mostrados en la Figura 4.18.

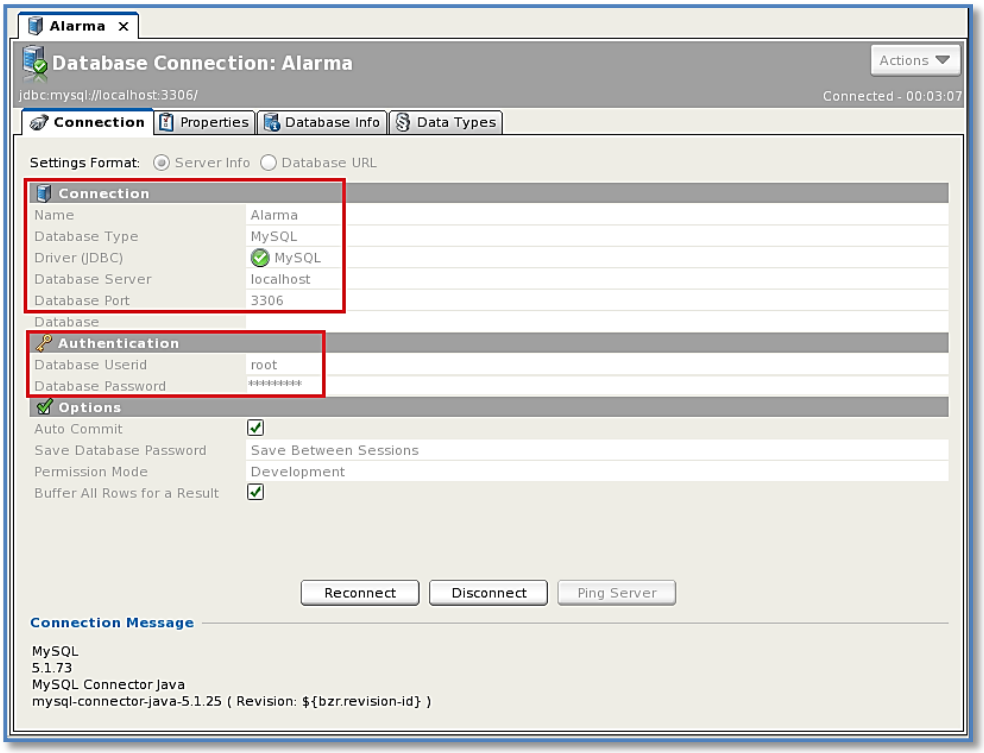


Figura 4.18. Ventana de conexión con MySQL en la herramienta DbVisualizer.

Una vez se logra conexión con el servidor MySQL, todas las beses de datos almacenadas en éste se visualizan en la herramienta como se observa en la Figura 4.19, resaltando *eventalarm* como la base de datos de interés para el plan de pruebas.

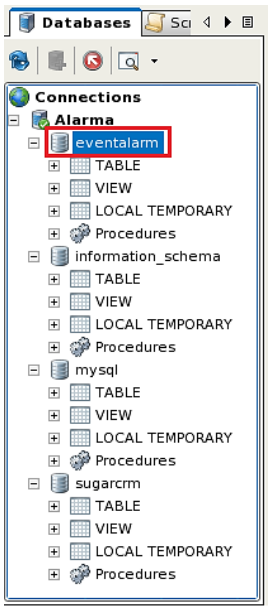


Figura 4.19. Bases de datos visualizadas en la herramienta DbVisualizer.

Cada base de datos contiene sus tablas con los diferentes registros de información, la Figura 4.20 muestra las tablas de la base de datos *eventalarm*, en donde la tabla *events* mostrada en la Figura 4.21 indica lo resultados de la actividad en las alarmas de los siete usuarios.

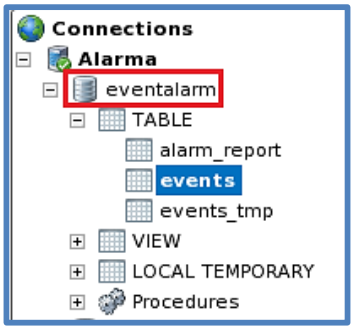
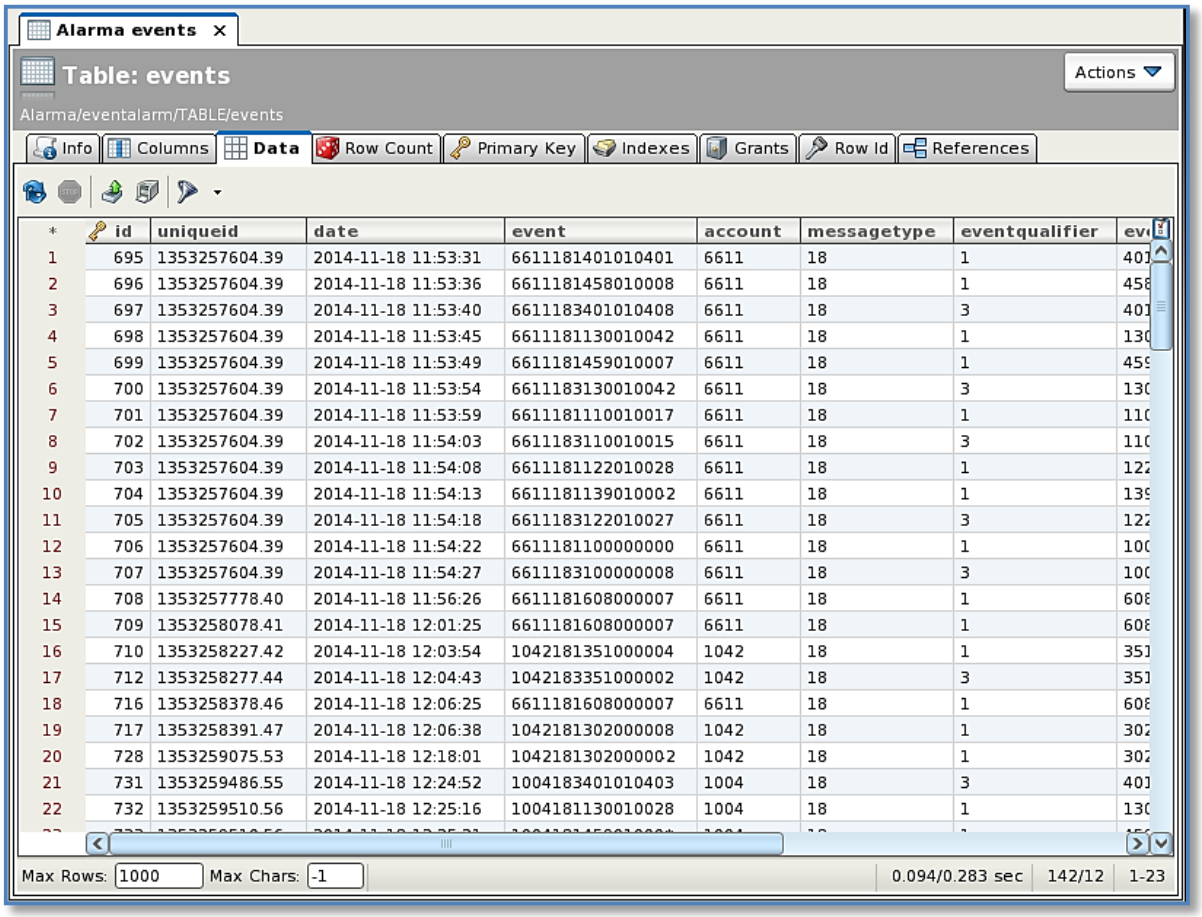


Figura 4.20. Tablas de la base de datos *eventalarm.*



*	id	uniqueid	date	event	account	messagetype	eventqualifier	ev
1	695	1353257604.39	2014-11-18 11:53:31	6611181401010401	6611	18	1	401
2	696	1353257604.39	2014-11-18 11:53:36	6611181458010008	6611	18	1	458
3	697	1353257604.39	2014-11-18 11:53:40	6611183401010408	6611	18	3	401
4	698	1353257604.39	2014-11-18 11:53:45	6611181130010042	6611	18	1	130
5	699	1353257604.39	2014-11-18 11:53:49	6611181459010007	6611	18	1	459
6	700	1353257604.39	2014-11-18 11:53:54	6611183130010042	6611	18	3	130
7	701	1353257604.39	2014-11-18 11:53:59	6611181110010017	6611	18	1	110
8	702	1353257604.39	2014-11-18 11:54:03	6611183110010015	6611	18	3	110
9	703	1353257604.39	2014-11-18 11:54:08	6611181122010028	6611	18	1	122
10	704	1353257604.39	2014-11-18 11:54:13	6611181139010002	6611	18	1	139
11	705	1353257604.39	2014-11-18 11:54:18	6611183122010027	6611	18	3	122
12	706	1353257604.39	2014-11-18 11:54:22	6611181100000000	6611	18	1	100
13	707	1353257604.39	2014-11-18 11:54:27	6611183100000008	6611	18	3	100
14	708	1353257778.40	2014-11-18 11:56:26	6611181608000007	6611	18	1	608
15	709	1353258078.41	2014-11-18 12:01:25	6611181608000007	6611	18	1	608
16	710	1353258227.42	2014-11-18 12:03:54	1042181351000004	1042	18	1	351
17	712	1353258277.44	2014-11-18 12:04:43	1042183351000002	1042	18	3	351
18	716	1353258378.46	2014-11-18 12:06:25	6611181608000007	6611	18	1	608
19	717	1353258391.47	2014-11-18 12:06:38	1042181302000008	1042	18	1	302
20	728	1353259075.53	2014-11-18 12:18:01	1042181302000002	1042	18	1	302
21	731	1353259486.55	2014-11-18 12:24:52	1004183401010403	1004	18	3	401
22	732	1353259510.56	2014-11-18 12:25:16	1004181130010028	1004	18	1	130

Figura 4.21. Registro de actividad de las alarmas.

4.5.2 Validación del Funcionamiento del Sistema

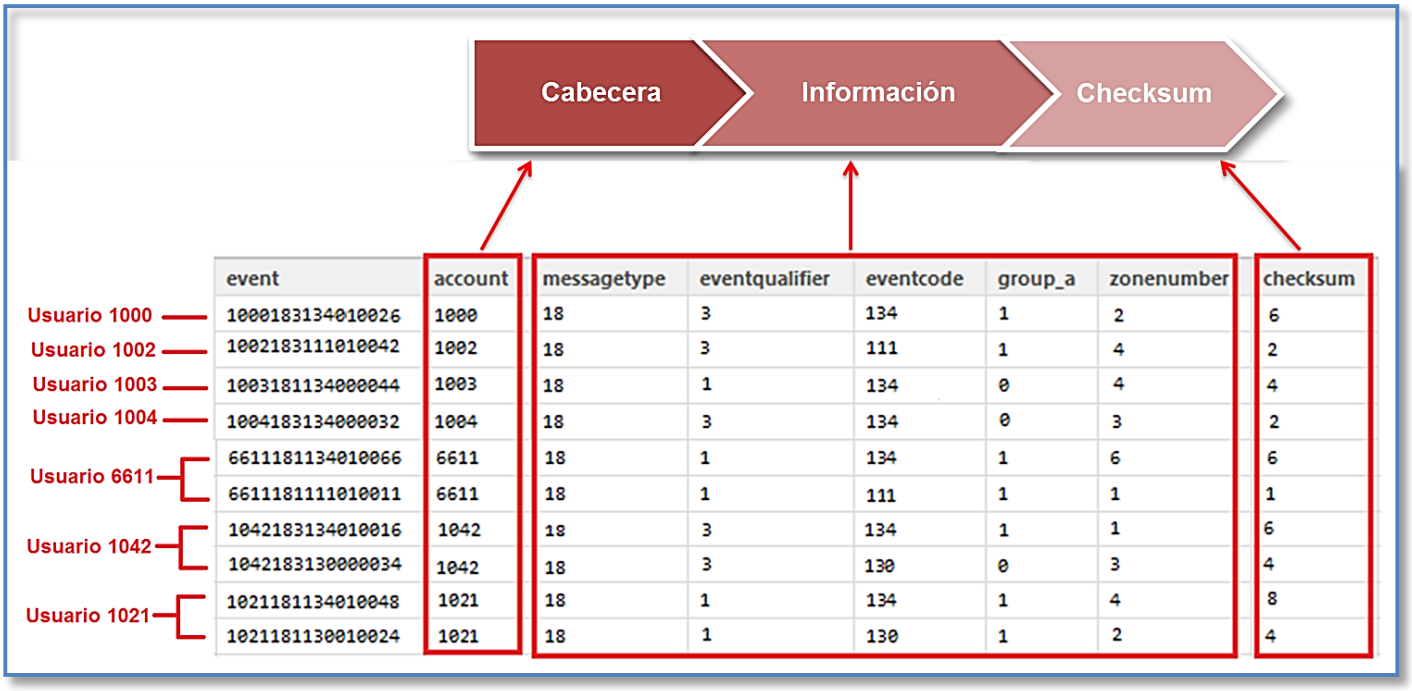
Con el esquema de pruebas planteado para cada usuario en la **Sección 4.4**, se obtuvieron los resultados mostrados en la Figura 4.22.

id	uniqueid	date	event	account	messagetype	eventqualifier	eventcode	group_a	zonenumber	checksum
695	1353339527	2014-11-18 11:53:31	1000183401000025	1000	18	1	401	0	2	5
696	1353379514	2014-11-18 20:08:49	1002183111010042	1002	18	3	111	1	4	2
697	1353541576	2014-11-18 11:53:40	1003181134000044	1003	18	1	134	1	4	4
698	1353259487	2014-11-18 11:53:45	1004183134000032	1004	18	3	134	1	3	2
700	1353257604	2014-11-18 11:53:31	6611181134010066	6611	18	1	134	1	6	6
701	1353257604	2014-11-18 11:53:36	6611181111010011	6611	18	1	111	1	1	1
702	1353258391	2014-11-18 11:54:03	1042183134010016	1042	18	3	134	0	1	6
703	1353258391	2014-11-18 11:53:45	1042183130000034	1042	18	3	130	0	3	4
704	1353379785	2014-11-18 11:53:49	1021181134010048	1021	18	1	134	1	4	8
705	1353379785	2014-11-18 11:53:54	1021181130010024	1021	18	1	130	1	2	4

Figura 4.22. Resultados del plan de pruebas.

La Figura 4.22 permite observar el id de identificación de cada alarma, la fecha de actividad y el evento recibido, el cual ha sido estructurado por el protocolo Contact ID en una trama de comunicación armada según lo explicado en la **Sección 2.5.1**, por tal motivo la columna *event* se divide en las columnas siguientes, especificando cada componente de la trama de comunicación según el protocolo Contact ID.

El armado de la trama de comunicación para lectura del protocolo Contact ID es el mostrado en la Figura 4.23.



	event	account	messagetype	eventqualifier	eventcode	group_a	zonenumber	checksum
Usuario 1000	1000183134010026	1000	18	3	134	1	2	6
Usuario 1002	1002183111010042	1002	18	3	111	1	4	2
Usuario 1003	1003181134000044	1003	18	1	134	0	4	4
Usuario 1004	1004183134000032	1004	18	3	134	0	3	2
Usuario 6611	6611181134010066	6611	18	1	134	1	6	6
	6611181111010011	6611	18	1	111	1	1	1
Usuario 1042	1042183134010016	1042	18	3	134	1	1	6
	1042183130000034	1042	18	3	130	0	3	4
Usuario 1021	1021181134010048	1021	18	1	134	1	4	8
	1021181130010024	1021	18	1	130	1	2	4

Figura 4.23. Trama de comunicación armada según protocolo Contact ID.

La información proveniente de cada usuario se muestra a continuación:

I. Usuario 1000:

De acuerdo a la Figura 4.23 la trama de comunicación del evento recibido para este usuario es 1000183134010026, lo que indica que

1000: Número de cuenta de usuario que identifica la alarma
18: Identifica que el mensaje se encuentra en formato Contact ID.
3: Calificador del evento, en este caso significa armado del panel de alarma.
134: Corresponde al código del evento, en este caso según el protocolo Contact ID indica activación del sensor magnético.
01: Indica la partición del panel de alarma.
002: Indica el número de la zona donde se activó el sensor.
6: Corresponde al checksum.

Con en la Ecuación 2.2 y teniendo en cuenta que para la suma de los dígitos se debe cambiar el 0 por 10, se verificó el checksum de la trama

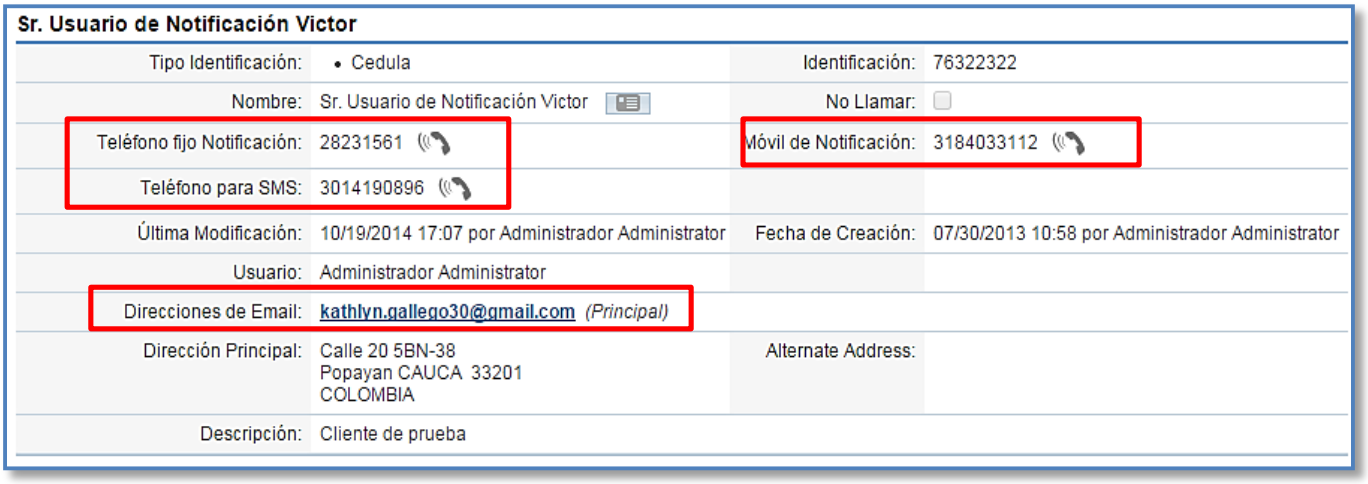
$$(Suma\ de\ los\ dígitos\ de\ la\ trama + Z) MOD\ 15 = 0$$

$$\big((1 + 10 + 10 + 10 + 1 + 8 + 3 + 1 + 3 + 4 + 10 + 1 + 10 + 10 + 2) + 6\big) \text{MOD } 15 = 0$$

$$(84 + 6) MOD\ 15 = 0$$

Lo anterior permite comprobar que la trama no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se armó el panel de alarmas y se activó el sensor magnético en la Zona 2.

Como se mencionó anteriormente, en el SugarCRM se encuentra toda la información de cada usuario, incluyendo los datos de contacto de la persona a la que se debe notificar en caso de activación de una alarma, para estas pruebas se creó un *Usuario de Notificación* mostrado en la Figura 4.24, al cual se notifica las alarmas registradas de los siete usuarios creados. El plan de llamada de los siete usuarios consiste en recibir un mensaje de texto, una llamada telefónica y un correo electrónico notificando el evento de alarma ocurrido.



Sr. Usuario de Notificación Victor

Tipo Identificación:	• Cedula	Identificación:	76322322
Nombre:	Sr. Usuario de Notificación Victor	No Llamar:	
Teléfono fijo Notificación:	28231561	Móvil de Notificación:	3184033112
Teléfono para SMS:	3014190896		
Última Modificación:	10/19/2014 17:07 por Administrador Administrator	Fecha de Creación:	07/30/2013 10:58 por Administrador Administrator
Usuario:	Administrador Administrator		
Direcciones de Email:	kathlyn.gallego30@gmail.com *(Principal)*		
Dirección Principal:	Calle 20 5BN-38 Popayan CAUCA 33201 COLOMBIA	Alternate Address:	
Descripción:	Cliente de prueba		

Figura 4.24. Información de contacto del usuario a ser notificado.

Al usuario se le debe notificar por tres canales de comunicación, la notificación por llamada telefónica es mediante un mensaje de voz que dice: "Alerta se le notifica que la alarma perteneciente a **[Nombre Usuario de Notificación]** ubicada en la dirección **[Dirección Principal del Cliente de la alarma]** se activa, sensor ubicado en **[Descripción Sensor]**".

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 1000.

- ✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Puerta cocina.**"**

✓ **Mensaje de texto y Correo electrónico:**

Figura 4.25. Mensaje de texto y Correo Electrónico de notificación Usuario 1000.

II. <u>Usuario 1002:</u>

De acuerdo a la Figura 4.23 la trama de comunicación del evento recibido para este usuario es 1002183111010042, lo que indica que

1002: Número de cuenta de usuario que identifica la alarma
18: Identifica que el mensaje se encuentra en formato Contact ID.
3: Armado del panel de alarma.
111: Activación del sensor de humo.
01: Indica la partición del panel de alarma.
004: Zona donde se activó el sensor.
2: Corresponde al checksum.

Con en la Ecuación 2.2 se verificó el checksum de la trama:

$$(73 + 2) MOD\ 15 = 0$$

Lo anterior permite comprobar que la trama no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se armó el panel de alarmas y se activó el sensor detector de humo en la Zona 4.

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 1002.

- ✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Cocina."

- ✓ **Mensaje de texto y Correo electrónico:**

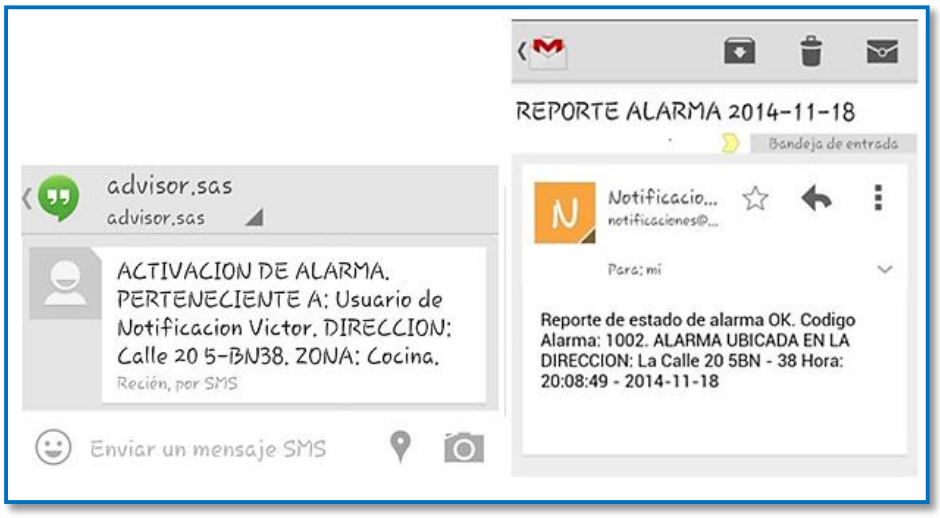


Figura 4.26. Mensaje de texto y Correo Electrónico de notificación 1002.

III. Usuario 1003:

De acuerdo a la Figura 4.23 la trama de comunicación del evento recibido para este usuario es 1003181134000044, lo que indica que

1003: Número de cuenta de usuario que identifica la alarma
18: Identifica que el mensaje se encuentra en formato Contact ID.
1: Nuevo evento.
134: Activación del sensor magnético.
00: Indica la partición del panel de alarma.
004: Zona donde se activó el sensor.
4: Corresponde al checksum.

Con en la Ecuación 2.2 se verificó el checksum de la trama:

$$(86 + 4) MOD\ 15 = 0$$

Lo anterior permite comprobar que la trama no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se activó el sensor magnético en la Zona 4.

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 1003.

- ✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Puerta Patio".

- ✓ **Mensaje de texto y Correo Electrónico:**

Figura 4.27. Mensaje de texto y Correo Electrónico de notificación 1003.

IV. <u>Usuario 1004:</u>

De acuerdo a la Figura 4.23 la trama de comunicación del evento recibido para este usuario es 1004183134000032, lo que indica que

1004: Número de cuenta de usuario que identifica la alarma
18: Identifica que el mensaje se encuentra en formato Contact ID.
3: Armado del panel de alarma.
134: Activación del sensor magnético.
00: Indica la partición del panel de alarma.
003: Zona donde se activó el sensor.
2: Corresponde al checksum.

Con en la Ecuación 2.2 se verificó el checksum de la trama:

$$(88 + 2) MOD\ 15 = 0$$

Lo anterior permite comprobar que la trama no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se armó el panel de alarmas y se activó el sensor magnético en la Zona 3.

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 1004.

- ✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Puerta Principal."

- ✓ **Mensaje de texto y Correo Electrónico:**

Figura 4.28. Mensaje de texto y Correo Electrónico de notificación 1004.

V. <u>Usuario 6611:</u>

De acuerdo a la Figura 4.23 las tramas de comunicación del evento recibido para este usuario son

A. <u>6611181134010066</u>

6611: Número de cuenta de usuario que identifica la alarma
18: Identifica que el mensaje se encuentra en formato Contact ID.
1: Nuevo evento.
134: Activación del sensor magnético.
01: Indica la partición del panel de alarma.

006: Zona donde se activó el sensor.
6: Corresponde al checksum.

Con en la Ecuación 2.2 se verificó el checksum de la trama:

$$(69 + 6) MOD\ 15 = 0$$

Lo anterior permite comprobar que la trama no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se activó el sensor magnético en la Zona 6.

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 6611 en su primer evento notificado.

- ✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Habitación Niños"

- ✓ **Mensaje de texto y Correo Electrónico:**

Figura 4.29. Mensaje de texto y Correo Electrónico de notificación 6611(1).

B. 6611181111010011

6611: Número de cuenta de usuario que identifica la alarma
18: Identifica que el mensaje se encuentra en formato Contact ID.

1: Nuevo evento.
111: Activación del sensor detector de humo.
01: Indica la partición del panel de alarma.
001: Zona donde se activó el sensor.
1: Corresponde al checksum.

Con en la Ecuación 2.2 se verificó el checksum de la trama:

$$(59 + 1) MOD\ 15 = 0$$

Lo anterior permite comprobar que la trama no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se activó el sensor detector de humo en la Zona 1.

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 6611 en su segundo evento notificado.

- ✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Cocina."

- ✓ **Mensaje de texto y Correo Electrónico:**

Figura 4.30. Mensaje de texto y Correo Electrónico de notificación 6611(2).

VI. Usuario 1042:

De acuerdo a la Figura 4.23 las tramas de comunicación del evento recibido para este usuario son:

A. 1042183134010016

1042: Número de cuenta de usuario que identifica la alarma
18: Identifica que el mensaje se encuentra en formato Contact ID.
3: Armado del panel de alarma.
134: Activación del sensor magnético.
01: Indica la partición del panel de alarma.
001: Zona donde se activó el sensor.
6: Corresponde al checksum.

Con en la Ecuación 2.2 se verificó el checksum de la trama:

$$(69 + 6) MOD\ 15 = 0$$

Lo anterior permite comprobar que la trama no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se armó el panel de alarmas y se activó el sensor magnético en la Zona 1.

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 1042 en su primer evento notificado.

- ✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Puerta Principal."

- ✓ **Mensaje de texto y Correo Electrónico:**

Figura 4.31. Mensaje de texto y Correo Electrónico de notificación 1042(1).

B. 1042183130000034

1042: Número de cuenta de usuario que identifica la alarma
18: Identifica que el mensaje se encuentra en formato Contact ID.
3: Armado del panel de alarma.
130: Activación del sensor de movimiento.
00: Indica la partición del panel de alarma.
003: Zona donde se activó el sensor.
4: Corresponde al checksum.

Con en la Ecuación 2.2 se verificó el checksum de la trama:

$$(86 + 4) MOD\ 15 = 0$$

Lo anterior permite comprobar que la trama no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se armó el panel de alarmas y se activó el sensor de movimiento en la Zona 3.

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 1042 en su segundo evento notificado.

- ✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Pir Patio."

- ✓ **Mensaje de texto y Correo Electrónico:**

Figura 4.32. Mensaje de texto y Correo Electrónico de notificación 1042(2).

VII. Usuario 1021:

De acuerdo a la Figura 4.23 las tramas de comunicación del evento recibido para este usuario son:

A. 1021181134010048

1021: Número de cuenta de usuario que identifica la alarma
18: Identifica que el mensaje se encuentra en formato Contact ID.
1: Nuevo evento.
134: Activación del sensor magnético.
01: Indica la partición del panel de alarma.
004: Zona donde se activó el sensor.
8: Corresponde al checksum.

Con en la Ecuación 2.2 se verificó el checksum de la trama:

$$(67 + 8) MOD\ 15 = 0$$

Lo anterior permite comprobar que el evento recibido no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se activó el sensor magnético en la Zona 4.

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 1021 en su primer evento notificado.

- ✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Puerta Patio."

✓ **Mensaje de texto y Correo Electrónico:**

Figura 4.33. Mensaje de texto y Correo Electrónico de notificación 1021(1).

B. 1021181130010024

1021: Número de cuenta de usuario que identifica la alarma.
18: Identifica que el mensaje se encuentra en formato Contact ID.
1: Armado del panel de alarma.
130: Activación del sensor de movimiento.
01: Indica la partición del panel de alarma.
002: Zona donde se activó el sensor.
4: Corresponde al checksum.

Con en la Ecuación 2.2 se verificó el checksum de la trama:

$$(71 + 4) MOD\ 15 = 0$$

Lo anterior permite comprobar que la trama no presenta errores y se recibe el evento planteado en el plan de pruebas de la **Sección 4.4**, donde se activó el sensor de movimiento en la Zona 2.

A continuación se observa el mensaje de voz de la llamada telefónica, el mensaje de texto y el correo electrónico recibido por el Usuario 1021 en su segundo evento notificado.

✓ **Llamada Telefónica:**

"Alerta se le notifica que la alarma perteneciente a Señor Usuario de Notificación Víctor, ubicada en la dirección Calle 20 5-BN38, se activa. Sensor ubicado en Pir Entrada."

✓ **Mensaje de texto y Correo Electrónico:**

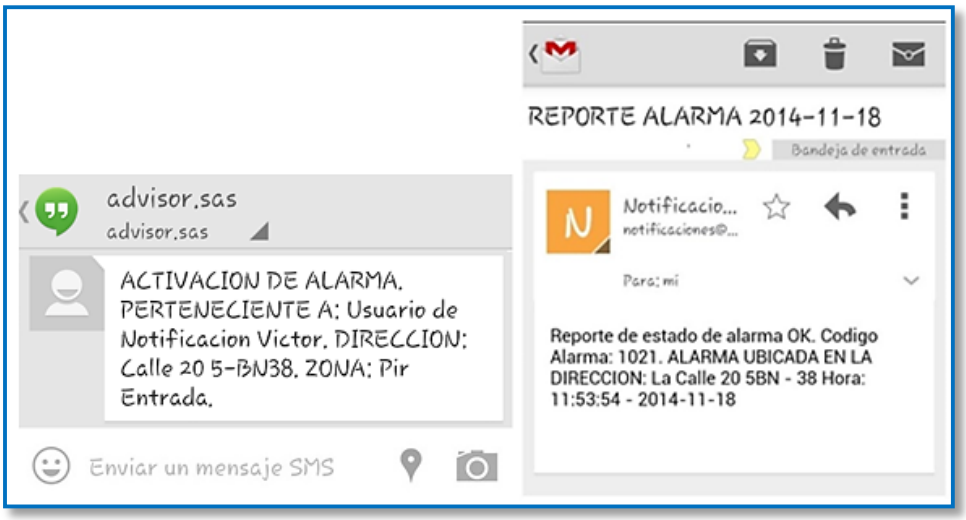


Figura 4.34. Mensaje de texto y Correo Electrónico de notificación 1021(2).

Estas fueron las pruebas realizadas para validar el correcto funcionamiento del servicio de monitoreo y notificación de alarma, al final de estas pruebas durante un periodo de tiempo de una semana se dejó implementado el esquema de pruebas en la empresa Advisor SAS, para que continuará registrando en la base de datos la actividad de los sensores.

4.5.3 Validación de la Calidad del Servicio

Por último se verificó la tasa de errores que se presentó, para esto se dejó activo el sistema por un periodo de una semana, registrando toda la actividad de los sensores y adicionalmente durante el día se activó los sensores intencionalmente con el fin de incrementar la cantidad de registros de activación. Con lo anterior fue posible obtener 200 eventos registrados y se realizó una verificación del checksum a cada uno con la Ecuación 2.2, dando como resultado que en el evento número 71 su verificación de checksum no dio el valor de cero.

Intento	Evento	Verificación del Checksum
71	6611181608000002	10

Se realizó la verificación del checksum recibido para este evento con la Ecuación 2.2:

$$(98 + 2) MOD\ 15 = 10$$

Lo anterior permite analizar que la trama presenta errores. Se realizó el cálculo del checksum para este evento con la Ecuación 2.1 y se obtiene que:

$$S = \left(\left(Parte\ entera\left(\frac{Suma\ de\ los\ dígitos\ de\ la\ trama}{15}\right)\right) + 1\right) * 15$$

$$S = \left(\left(Parte\ entera\left(\frac{98}{15}\right)\right) + 1\right) * 15 = 105$$

$$Z = S - 98 = 105 - 98 = 7$$

Esto muestra que el valor del checksum calculado no coincide con el checksum recibido, por lo tanto esta trama es incorrecta, pero se encontró que en el siguiente evento se transmitió la trama nuevamente de manera correcta, ya que comparando con la trama anterior, el checksum da el valor calculado.

Intento	Evento	Verificación del Checksum
71	6611181608000002	10

Intento	Evento	Verificación del Checksum
72	6611181608000007	0

A partir de estos resultados se realizó el cálculo de la tasa de errores (FER, Frame Error Rate) con el fin de relacionar los datos recibidos con errores con los datos totales recibidos, esta tasa se utiliza para determinar la calidad de conexión de una señal. Si la FER es demasiado alta significa que se presentan demasiados errores y la conexión es inestable.

La FER obtenida para la semana de pruebas fue la siguiente:

$$\%\ FER = \frac{Tramas\ incorrectas\ recibidas}{Tramas\ totales\ enviadas} x\ 100$$

$$\%\ FER = \frac{1}{200} x\ 100 = 0.5$$

El sistema presenta una FER del 0.5%, para 200 eventos ocurridos éste es un valor bajo. La obtención de esta FER del 0.5% para la semana de pruebas indica que de cada 1000 tramas 5 llegan erróneas.

Se observó que el sistema re-transmite la trama para garantizar que la central reciba la información de manera correcta, esto permitió validar la calidad del servicio en un ambiente de prueba piloto.

De acuerdo a las pruebas realizadas anteriormente, la empresa Advisor SAS verificó que el servicio para monitoreo y notificación de eventos era el necesitado, permitiendo monitorear, brindar información y notificar los distintos eventos ocurridos. La empresa emitió una carta de agradecimiento mostrada en el **Anexo G.**

CAPÍTULO 5. CONCLUSIONES Y TRABAJOS FUTUROS

5.1 INTRODUCCIÓN

El presente trabajo de grado enfocó sus esfuerzos en el desarrollo de un servicio para monitoreo de eventos de seguridad en viviendas o empresas y adicionalmente eventos de tipo médico. El servicio permite también notificar a un usuario estos eventos monitoreados mediante tres canales de comunicación, que son llamada telefónica, mensaje de texto y correo electrónico. Lo anterior haciendo uso del protocolo Contact ID y componentes de libre distribución.

Se implementó un prototipo a través de la arquitectura propuesta y posteriormente se realizó un esquema de pruebas con el fin de evaluar la funcionalidad y calidad del sistema en un ambiente de prueba piloto de la empresa Advisor SAS.

En este capítulo se presentan las conclusiones y posibles trabajos futuros de investigación que pueden desprenderse del trabajo de grado realizado, con el fin de ampliar o integrar nuevas aplicaciones al servicio desarrollado.

5.2 CONCLUSIONES

A partir del trabajo realizado y la experiencia adquirida, se plantean las siguientes conclusiones:

1. Se demostró la viabilidad de usar la herramienta de libre distribución Asterisk como un receptor de alarmas comercial, fiable y capaz de interpretar el protocolo Contact ID recibiendo tonos DTMF y resaltando la información del evento contenida en ellos.

2. Este proyecto demuestra que es posible automatizar el servicio de notificación de alarmas disminuyendo al mínimo la intervención humana frente a los actuales sistemas de monitoreo y notificación.

3. Se realizó un aporte a la herramienta Asterisk adaptando el archivo LeerAlarma a sus componentes con el fin de obtener una trama de comunicación más amplia, correspondiente al protocolo Contact ID, detallando más información de los eventos ocurridos en la casa o empresa de los usuarios.

4. La implementación e integración del SugarCRM con la herramienta de libre distribución Asterisk, permitió trabajar en una interfaz más amigable para el manejo de la información de los clientes, además de una fácil integración para la comunicación de los eventos a través de los diversos medios de comunicación.

5. La configuración del plan de alarma del cliente brinda la oportunidad de poder armar diversos paquetes de servicio según los sensores instalados en los hogares o empresas y las necesidades de cada cliente en particular. Por lo tanto, la flexibilidad en el servicio permite la posibilidad de abrir el mercado a diferentes tipos de clientes.

6. El uso de software libre permite el desarrollo de una solución en sistemas de monitoreo y notificación de alarmas para cualquier vivienda o empresa, de una manera económica respecto a su implementación y a la prestación del servicio, disminuyendo la contratación de personal en la central las 24 horas del día debido a que el servicio funciona de manera autómata y eficiente, ofreciendo las funciones y respuestas que realizaría este personal.

7. Se aseguró en el servicio desarrollado diversos medios de notificación al usuario como llamada telefónica, correo electrónico y mensaje de texto. Ampliando de esta forma los canales de comunicación tradicionales utilizados por los sistemas de alarmas convencionales para que de una u otra manera se aseguré un medio para notificar al usuario sobre la activación de la alarma.

8. El servicio desarrollado promueve un espacio en la innovación para el desarrollo de nuevos servicios y aplicaciones específicas para cada usuario en el mercado de la seguridad electrónica, basándose en tecnologías existentes e integradas a diversos canales de comunicación con el cliente.

9. Como resultado de las pruebas realizadas en el desarrollo del servicio, fue posible demostrar el uso del protocolo Contact ID para el monitoreo y notificación de alarmas de tipo médico, comprobando este trabajo con la presentación y sustentación del artículo titulado “Development of a Medical Monitoring System and Alarm Notification with a Contact ID protocol and conventional Alarm System” en el evento anual ISCC 2014 de la IEEE llevado a cabo en la ciudad de Concepción Chile, donde se expuso a partir

de un prototipo inicial la viabilidad y las ventajas de integrar un nuevo modelo de alarmas médicas en el servicio desarrollado.

10. A partir de las pruebas de validación de funcionamiento y calidad del servicio, se realizó una buena adaptación y conversión del protocolo Contact ID desde tonos DTMF a señalización IP para la comunicación de sus componentes, fue factible y además compatible con las herramientas de libre distribución utilizadas. De acuerdo a la FER obtenida, se concluye que el servicio para monitoreo y notificación de eventos presenta baja tasa de errores o pérdida de tramas, garantizando gran confiabilidad de uso del sistema, teniendo en cuenta que en caso de perderse una trama de información el sistema re-transmite la trama para garantizar que la central reciba la información de manera correcta.

5.3 TRABAJOS FUTUROS

Los resultados obtenidos en el desarrollo del servicio para monitoreo y notificación de eventos de alarma, se presentan como referencia para trabajos futuros que busquen desarrollar funcionalidades adicionales a las presentadas y permitan explorar nuevas aplicaciones a los sistemas de seguridad y monitoreo. Para ello se proponen los siguientes trabajos futuros:

1. Ampliar la demanda de canales de notificación, integrando de esta forma como canal complementario el servicio de WhatsApp o integración con las redes sociales como Facebook o Twitter.

2. Buscar la integración del servicio planteado con aplicaciones a la domótica para ampliar los alcances del sistema y ofrecer mayor cantidad de servicios a los clientes, donde no solo se notificaría de manera autómata un evento sino que también se brindarían acciones de respuesta para estos eventos.

3. Integrar en el servicio la implementación de dispositivos médicos inalámbricos para brindar mayor movilidad al paciente y ofrecerlo como un producto o servicio comercial para quienes deseen monitorear el estado de salud de un familiar o un paciente que requiera de un monitoreo continuo, partiendo del sistema de alarma instalado en su propio hogar o centro médico.

BIBLIOGRAFÍA

[1] DANE Departamento Administrativo Nacional de Estadistica, «Encuesta de Convivencia y Seguridad Ciudadana 2013,» DANE, Cali, 2013.

[2] DANE Departamento Administrativo Nacional de Estadistica, «Encuesta de Convivencia y Seguridad Ciudadana ECSC 2013,» DANE, Popayán, 2013.

[3] El Pais, «Presidente Santos quiere usar la tecnología en seguridad ciudadana,» *El Pais,* 1 Febrero 2014.

[4] O. Mendoza, «Estudio para la Implementación de un Sistema de Monitoreo electrónico de Alarmas para la empresa TE&CS S.R.L.,» Tarija.Bolivia, 2010.

[5] Fortox Security Group, «Empresa de Seguridad electrónica,» [En línea]. Available: http://www.fortoxsecurity.com/. [Último acceso: 30 Mayo 2014].

[6] F. Gomez y F. Gil, VoIP y Asterisk, redescubriendo la telefonia, Almería, AlfaOmega, 2008.

[7] ISCC, «International Student Conference Chile,» [En línea]. Available: http://iscc.cl/. [Último acceso: 1 Noviembre 2014].

[8] Definición.de, «Concepto de Seguridad. Definición, Significado y Qué es,» [En línea]. Available: http://definicion.de/seguridad/. [Último acceso: 18 Julio 2014].

[9] D. Valladolid y S. Cordova, «Sistema de alarma para el hogar y negocio,» Juarez, 2010.

[10] D. Rosales, «Implementación de una central de monitoreo de alarmas en base a un computador personal usando formato de comunicacion Contact ID y avisos SMS,» Quito, 2013.

[11] DSC Security Products , «Instruction Manual DSC PC1555,» 1999.

[12] System Sensor, «Detectores de humo para sistemas,» 2004.

[13] Ares Seguridad, «Alarmas Hogar. Sisitemas de Seguridad,» [En línea]. Available: http://www.aresseguridad.es/p/es/particulares/alarmas-hogar.php. [Último

acceso: 15 Octubre 2014].

[14] Elastix Tech, «Interconexion a la PSTN,» [En línea]. Available: http://elastixtech.com/fundamentos-de-telefonia/interconexion-a-la-pstn/. [Último acceso: 12 Noviembre 2014].

[15] Martinez, Marcelino, «Generación y Detección de tonos DTMF,» Universidad de Valencia, [En línea]. Available: http://mural.uv.es/masimo/DTMF.html. [Último acceso: 12 Noviembre 2014].

[16] A. Solé, «Monitoreo Telefónico e IP. Protocolos de Comunicaciones,» *Negocios de Seguridad,* nº 63, pp. 196-200.

[17] Digital Security Controls, «Sur-Gard System III Multi-Platform Digital Telephone Receiver - Operation Manual,» Toronto, Canada, 2005.

[18] Ademco Group, «Digital Communication Standard- Ademco Contact ID Protocol for Alarm System Communications,» 1999.

[19] Security Industry Association, «Digital Communication Standard - Ademco - Contact ID Protocol for Alarm System Communications.,» Ademco Group, 1999.

[20] Alarm Device Manufacturing Company, «Ademco Contact ID Reporting,» New York, 2004.

[21] G. Crosby, T. Gosh, M. Renita y C. Craig, «Wireless sensor networks for healthcare: A survey,» *International Journal of Ad hoc, Sensor & Ubiquitous Computong,* vol. 3, nº 3, pp. 2688-2710, Junio 2012.

[22] International Organization for Standardization, «ISO/IEC TR 20007:2014,» [En línea]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50954. [Último acceso: 28 Octubre 2014].

[23] Integra Consultoria de Calidad, «Sistemas de gestion sectoriales ISO27000,» [En línea]. Available: http://www.consultoresdesistemasdegestion.es/sistemas-de-gestion-sectoriales/iso-27000/. [Último acceso: 28 Octubre 2014].

[24] V. Fernandez, Desarrollo de sistemas de información: una metodología basada en el modelado, Ediciones UPC, 2006.

[25] G. Cruz, «Sistemas de Seguridad,» [En línea]. Available: http://es.slideshare.net/german_cruz/sistemas-de-seguridad-16443711. [Último

acceso: 17 Julio 2014].

[26] Centrodeartigo.com, «Interoperabilidad Sintáctica y semántica,» 14 Marzo 2013. [En línea]. Available: http://centrodeartigo.com/articulos-utiles/article_118558.html. [Último acceso: 2 Octubre 2014].

[27] M. F. GUTIÉRREZ, A. CAJIAO, J. A. HIDALGO, J. D. CERÓN, D. M. LOPEZ, V. M. QUINTERO y A. RENDÓN, «A Vital Signs Telemonitoring System-Interoperability supported by a personal health record system and a cloud service,» *pHealth 2014,* 2014.

[28] J. Acosta, «Trixbox y Asterisk,» Abril 2010. [En línea]. Available: www.aprendeviviendo.org.

[29] A. Saa y D. Velasco, «Diseño de una plataforma CRM integrada con Asteriskpara la direccion comercial de EMCALI Telecomunicaciones,» Santiago de Cali, 2012.

[30] D. Nuñez y M. Perez, «Analisis y adaptación del módulo para la integración entre SugarCRM y Asterisk enfocado hacia las Pymes,» Bogota, Colombia, 2099.

[31] ZOHO, «CRM Software, Customer Relation Manager Zoho,» [En línea]. Available: http://www.zoho.com/crm/. [Último acceso: 12 Octubre 2014].

[32] Sugar Inc, «Sugar Community Edition,» 2009. [En línea]. Available: http://support.sugarcrm.com/02_Documentation/01_Sugar_Editions/05_Sugar_Community_Edition/. [Último acceso: 18 Julio 2014].

[33] R. Pressman, Ingeniería del Software. Un enfoque practico, vol. 5 ed, Mc Graw-Hill, 2001.

[34] Elastix Freedom to Communicate, «Elastix, Open Source Unified Communications Server,» [En línea]. Available: http://www.elastix.org. [Último acceso: 15 Octubre 2014].

[35] C. Rosero, A. Mendoza y R. Estrada, «Integracion de Sugar CRM con Asterisk,» Guayaquil, Ecuador.

[36] Yuasa, «SERIE NP/NPH/NPX Selladas Y Recargables Baterias De Plomo-Acido,» [En línea]. Available: http://www.americanbattery.com.ar/yuasa/CatalogoNPMasBaterias.pdf. [Último acceso: 11 Octubre 2014].

[37] Cisco Systems, Inc, «Cisco SPA100 Series Analog Telephone Adapters, Quick Start Guide,» 2011.

[38] VoIP Info.org, «Asterisk Config AlarmReceiver.conf,» [En línea]. Available: http://www.voip-info.org/wiki/view/Asterisk+config+alarmreceiver.conf. [Último acceso: 15 Noviembre 2014].

[39] VoIP Inf.org, «Asterisk cdm AlarmReceiver,» [En línea]. Available: http://www.voip-info.org/wiki/view/Asterisk+cmd+AlarmReceiver. [Último acceso: 15 Noviembre 2014].

[40] Underwriters Laboratories, [En línea]. Available: http://ul.com/. [Último acceso: 15 Noviembre 2014].

[41] Apstel, «Apstel Downloads,» [En línea]. Available: http://www.apstel.com/. [Último acceso: 11 Septiembre 2014].

[42] Rynga discount voip provider, «Rynga for the cheapest international calls,» [En línea]. Available: www.rynga.com. [Último acceso: 19 Noviembre 2014].

[43] K. Gallego, D. Semanate y V. Mondragrón, «Development of a Medical Monitoring System and Alarm Notification with a Contact ID protocol and conventional Alarm System,» *ISCC 2014,* Noviembre 2014.

[44] S.-L. M, F. C y W. L, «Normal oral, rectal, tympanic and axillary body temperature in adult men and woman: A systematic literature review,» *Scandinavian Journal of Caring sciences,* vol. 16, nº 2, pp. 122-128, 2002.

[45] National Semiconductor, «LM35 Precision Centigrade Temperature Sensor datasheet,» 2000.

[46] DBVis Software, «Database Management Software tools,» [En línea]. Available: http://www.dbvis.com/. [Último acceso: 1 Noviembre 2014].

[47] CentOS.org, «CentOS Project,» [En línea]. Available: http://www.centos.org/. [Último acceso: 02 Octubre 2014].