PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

SISTEMA DE CONTROL DOMÓTICO UTILIZANDO UNA CENTRAL IP PBX BASADO EN SOFTWARE LIBRE

Tesis para optar el Título de Ingeniero Electrónico, que presenta el bachiller:

Wally Mauro Rodríguez Bustinza

ASESOR: Gumercindo Bartra Gardini

Lima, Agosto del 2012

RESUMEN

Se entiende como domótica o inmótica a sistemas cuyos elementos nos permiten automatizar una vivienda o edificio, considerando sus cuatro pilares: comodidad, seguridad, comunicaciones y un eficiente consumo energético. Actualmente la domótica no sólo está enfocada a la gestión de estos elementos, sino también en darle al usuario una visión única y sencilla frente a los diferentes elementos que existen en el sistema, dándole un control al usuario de su sistema tanto de la misma área como desde otra ubicación, es decir brindarle una total interoperabilidad al usuario.

Sin embargo, la incompatibilidad que es generada debido a los diferentes estándares y protocolos que existen en la actualidad, la falta de cultura domótica en el Perú, y los costos muy elevados de controladores que permiten el acceso remoto al sistema, hacen que esta tecnología sea inaccesible al público en general.

El presente trabajo de tesis titulado “Sistema de Control domótico utilizando una central IP PBX basado en software libre” plantea una solución enfocada a brindarle una interoperabilidad al usuario considerando resolver los problemas arriba mencionados. Se plantea una arquitectura que permite el sistema sea escalable y heterogéneo. Se utilizan protocolos de Internet que integran al sistema domótico a una actual convergencia de comunicaciones, y la implementación del servidor IP PBX en Asterisk permiten que el usuario tenga un control del sistema de una forma sencilla, confiable y accesible para el público en general.

Demostrando que la plataforma implementada puede incorporar al sistema domótico no sólo a las redes de telefonía, sino también, puede brindar una flexibilidad para desarrollar otras plataformas como servidores web en el mismo sistema. Todo considerando un presupuesto bajo comparado con otros productos en el mercado.

ÍNDICE

Anexos

INTRODUCCIÓN

El presente trabajo se basa en el diseño de un sistema de control domótico utilizando una IP PBX basado en software libre como solución de interoperabilidad para el usuario; las pruebas se realizaron en dos localidades ubicadas en diferentes zonas geográficas.

La gran mayoría de soluciones domóticas que existen en la actualidad brindan al usuario una interoperabilidad que le permite controlar el sistema y recibir notificaciones desde la ubicación en donde se encuentre.

En el desarrollo de esta tesis se hizo un estudio de las diferentes soluciones en la actualidad, de acuerdo a esto se planteó una arquitectura escalable, heterogénea, y de bajo costo. Además de tener un sistema de notificaciones confiable, que le permita al usuario recibir alarmas de su sistema de una manera rápida y segura.

A través del documento se presenta de manera ordenada tanto la teoría, las tecnologías, soluciones y arquitecturas planteadas, y los procesos desarrollados. En el primer capítulo se da una breve introducción a la domótica y la influencia de esta tecnología en el Perú, así mismo se presenta la problemática que intenta resolver esta tesis. En el segundo capítulo se definen conceptos teóricos sobre los elementos básicos de un sistema domótico y se describen las diferentes arquitecturas y soluciones en la actualidad. Luego en el tercer capítulo se explican los requerimientos que se consideraron para el diseño de cada uno de los elementos del sistema y de la arquitectura en sí. Además de explicar el desarrollo y descripción de cada elemento del sistema. Finalmente, en el cuarto capítulo se muestran algunas de las pruebas realizadas con el sistema según el escenario planteado, y se hace un análisis de costos con respecto a otros productos similares en el mercado.

CAPITULO 1

MARCO PROBLEMÁTICO Y OBJETIVOS

1.1 Domótica e Inmótica

1.1.1 Definición

Podemos entender por domótica o inmótica a sistemas cuyos elementos son capaces de automatizar una vivienda o edificio; cuyo objetivo principal es gestionar la seguridad, comodidad, comunicación y un eficiente consumo energético.

1.1.2 Interoperabilidad

Tradicionalmente las soluciones domóticas eran proporcionadas por escasos vendedores que usaban estándares de comunicaciones cerrados y costosos. Sin embargo esto ha ido cambiando debido al desarrollo de elementos domóticos heterogéneos en todos los aspectos. Gran variedad de proveedores presentan productos con distintos tipos de hardware, protocolos de red, y sistemas operativos; sin embargo los usuarios necesitan tener una vista única frente a los diferentes estándares, protocolos y software usados en el sistema; por lo tanto hoy en día se busca entonces la total interoperabilidad del sistema domótico. Podemos definir entonces *Interoperabilidad,* en el contexto de domótica, como la posibilidad de comunicación entre dos o más tecnologías.

1.2 Problemática Actual

1.2.1 Domótica en el Perú y en el mundo

En el Mundo

El incremento de nuevas tecnologías en la automatización de hogares, junto con el avance del área de redes y comunicaciones, ha servido de motivación para el desarrollo de nuevas alternativas para el área de la domótica.

Podemos diferenciar las distintas perspectivas que existen en la actualidad con respecto a la domótica según la zona geográfica que se analice. Por ejemplo en EEUU, se orienta hacia el hogar interactivo con servicios tales como el trabajo o la

tele-enseñanza. En Japón apunta a un hogar automatizado, incluyendo la mayor tecnología posible en el hogar e incorporando gran variedad de aparatos electrónicos de consumo. En España, actualmente está en un importante desarrollo, así como otros países de Europa. En general podemos observar, de los países mencionados, que están en un desarrollo constante debido a que hay un reconocimiento del valor añadido que la domótica proporciona a las viviendas, edificios, etc.

En el Perú

Como se ha investigado existen muchas empresas en diferentes países generando gran desarrollo en la domótica o inmótica, pero en el Perú ésta es una tecnología que se encuentra sin mucho desarrollo en la actualidad. Una de las principales razones es que la mayoría de los profesionales de las carreras afines no se encuentran investigando ni desarrollando temas relacionados a este tipo de tecnología.

Debido a la falta de información de esta tecnología, podemos decir que no existe una suficiente cultura domótica en el Perú. El cliente, frente a la domótica, realmente no sabe que solicitar o que criterios elegir a la hora de la compra. No se conoce realmente en qué consiste y se ve como una necesidad superflua, un gasto innecesario o lujoso desde el punto de vista del cliente.

Además, de percibir como algo muy costoso todo lo relacionado a la domótica. Existe también el problema de desconocimiento de la tecnología, es decir el cliente se siente incapacitado para manejar aparatos complicados en base a tecnologías demasiado complejas para ellos.

Por ende, el desarrollo de la domótica tiene que ir de la mano con la correcta difusión de esta tecnología.

El Perú tiene la posibilidad de adquirir y desarrollar esta tecnología, si bien se sabe esto significaría una inversión inicial, la calidad de vida del usuario se vería mejorada, incrementando la seguridad, el confort y generando un considerable ahorro.

1.2.2 Presentación del problema

Actualmente, la domótica no sólo está enfocada a una eficiente gestión de los elementos del sistema, sino también de brindarle al usuario la capacidad y facilidad de poder controlar y monitorear su vivienda, oficina, negocio, etc. desde cualquier

lugar, sin importar la ubicación donde esté, y sin tener dificultades, de una manera eficaz y eficiente.

Sin embargo, la gran variedad de estándares usados en la comunicación y conexión de dispositivos domóticos, ya sea por cable o inalámbrico, conlleva a una incompatibilidad entre los diferentes dispositivos.

Muchas de las alternativas en la actualidad implican el uso de una arquitectura en la cual se utilizan controladores que se comunican con los dispositivos, y gracias a esos es factible el acceso remoto al sistema. Sin embargo, el protocolo utilizado para la comunicación entre los dispositivos domóticos y el controlador son cerrados. Esta es una solución común de compañías que quieren monopolizar el mercado de la domótica (Echelon's LonWorks, BTicino's Myhome, Sistema de Casa, etc.), obligando a los usuarios a comprar sus equipos, actuadores, sensores y aplicaciones para las interfaces del usuario.

Además, la implementación de un sistema domótico como el planteado, implicaría un costo muy elevado, ya que no sólo se necesitaría adquirir los dispositivos básicos de un sistema domótico (actuadores, sensores, etc.) que de por sí implica un costo significativo; sino también de controladores y equipos especiales que nos permitan el acceso y control remoto del sistema.

Por ejemplo, para empresas adquirir un sistema que le permita monitorear y controlar diferentes áreas remotamente (desde un móvil por ejemplo) no sólo en una misma localidad sino en diferentes localidades de una forma fiable y segura, implicaría un costo elevado, ya que implica comprar equipos adicionales para establecer la comunicación, y sólo podría usarse desde dispositivos que sean compatibles con el sistema.

El desarrollo de esta tesis tiene la intención de reducir costos, obtener una compatibilidad y escalabilidad necesaria en un sistema domótico. Para esto se diseñará un sistema de control domótico que nos permita controlar y monitorear sensores y actuadores, desde la misma área y remotamente desde cualquier otra ubicación con cobertura de señal telefónica o Internet; utilizando una IP PBX basado en software libre como medio de comunicación entre el usuario y el sistema. El usuario tendrá acceso desde su oficina, hogar o desde cualquier dispositivo móvil; esto mediante un IVR que le brindará opciones o accediendo vía web al sistema.

1.3 Objetivos

Objetivos Generales

Diseñar un sistema de control domótico que nos permita controlar y monitorear desde la misma área y remotamente desde cualquier otra ubicación (con señal telefónica o Internet), utilizando una IP PBX basado en un software libre como medio de comunicación entre el usuario y el sistema.

Objetivos Específicos

- Diseño del módulo de control.
- Diseño e implementación del módulo de comunicaciones
- Configuración y Diseño de la red de comunicaciones y programación de sockets.
- Instalación y Configuración del servidor IP PBX.
- Implementación de la base de datos de los clientes para la plataforma domótica.
- Diseño del interfaz de usuario.
- Comunicación del sistema con dos zonas geográficas diferentes, cada uno con dos sensores y un actuador.

CAPÍTULO 2

CONSIDERACIONES TEÓRICAS Y ESTUDIO DE LAS ARQUITECTURAS DOMÓTICAS EN LA ACTUALIDAD

Tradicionalmente, la domótica era un producto vendido por muy pocas empresas. Estas empresas manejaban estándares únicos y donde la mayoría eran cerrados. Esto provocaba que las soluciones domóticas sean productos costosos, y sólo ciertos usuarios con capacidad económica puedan invertir en un sistema automatizado para tener los beneficios que la domótica brinda. Actualmente, los dispositivos domóticos son considerados heterogéneos en todos los aspectos, es decir funcionan bajo diferentes protocolos, sistemas operativos, interfaces, estructura, etc.

Frente a esto, el objetivo principal es buscar un manejo estándar frente a la heterogeneidad de los diferentes dispositivos en el sistema. Además de brindarle al usuario una total interoperabilidad del sistema. Para lograr un manejo estándar y una interoperabilidad total de sistema para el usuario, debemos entender los roles de cada estructura de nuestro sistema domótico. Estas estructuras son: *Sensores, actuadores y controladores, Medios de Comunicación, Protocolos, Interface con el Usuario.*

2.1 Sensores, Actuadores y Controladores

Los sensores, o receptores, son elementos que reciben información del entorno del sistema. Por ejemplo variables atmosféricas e intensidad luminosa. De la misma manera, pueden recoger información de las actividades que el usuario u otras personas en el entorno realizan, como por ejemplo entrar a un ambiente o cuarto, prender algún aparato, etc.

Los actuadores son elementos que reciben órdenes de activarse o desactivarse. Realizan acciones que permiten cambiar el ambiente o entorno del sistema domótico. Como por ejemplo: el prendido o apagado de una luz, el cierre y apertura de una ventana, etc.

En la presente tesis se referencia a los sensores y actuadores como **dispositivos domóticos.**

Los controladores son encargados de recibir la información proveniente de los sensores y procesarla mediante una programación ya definida. De acuerdo a esto, se produce una activación o desactivación de los actuadores.

2.2 Medios de Comunicación

Distintas soluciones se han desarrollado por empresas líderes, para lograr una interoperabilidad entre los diferentes dispositivos domóticos. Según el paper *Domotic House Gateway* [9] podemos diferenciar tres principales enfoques relacionados a la comunicación con los dispositivos domóticos, que se explicarán a continuación:

El primer enfoque se desarrolla sobre la instalación de una red alámbrica específica y separada. Existen distintos estándares que buscan tener un reconocimiento global como por ejemplo el estándar abierto Konnex desarrollado mayormente en Europa, tiene un gran auge y expansión a nivel global, sin embargo hasta ahora ningún protocolo es totalmente reconocido a nivel global. Dentro de este enfoque podemos encontrar los protocolos: X10, CEBus, HBS, EIB, EHS, BatiBus. Los tres últimos desarrollados bajo el estándar Konnex.

Un segundo enfoque usado actualmente es el uso de los métodos de conexión alámbrica usando las líneas de alimentación o de teléfonos. Uno de los protocolos más usados en este enfoque es el X10. Sin embargo, estas soluciones tienen la desventaja de presentar mucho ruido.

Un tercer y último enfoque es el desarrollo de tecnologías inalámbricas como radiofrecuencia, WiFi, Zigbee, Bluetooth; usados mayormente para comunicaciones entre distancias mayores y donde sea necesario evitar el cableado.

Características de los estándares inalámbricos

Analizaremos el último enfoque mencionado, ya que nos ofrece facilidades en comunicación en distancias importantes entre diferentes dispositivos, la capacidad de crear sistemas centralizados y distribuidos sin la necesidad de existir un cableado.

En el Perú, las estructuras actuales, en la gran mayoría no están preparadas para tener una instalación domótica, por lo que el uso de estas tecnologías sería de gran aporte para una reducción del presupuesto de la instalación. Se mencionan en la tabla 2.1 las tres principales tecnologías orientadas a la comunicación inalámbrica.

Tomando en cuenta dos rasgos importantes: la transmisión y consumo de potencia. Se observa claramente tanto Zigbee como Bluetooth tienen bajo consumo de potencia a diferencia de WiFi. Sin embargo, la desventaja de Bluetooth es la poca cantidad de nodos que soporta (8 nodos). A diferencia de Zigbee que soporta hasta 65536 nodos agrupados hasta en 255 subredes. Además, la tasa de transmisión que ofrece la tecnología Zigbee es suficiente para las aplicaciones de un sistema domótico. Si bien no es alta, los dispositivos domóticos están en la mayoría de tiempo en reposo, por lo que no es necesario altas velocidades.

Tabla 2.1 Diferencias entre las tres principales tecnologías orientadas a la comunicación inalámbrica, estas son WiFi, Bluetooth y Zigbee (Elaboración: [8])

Estándar	**Ancho de Banda**	**Consumo de potencia**	**Ventajas**	**Aplicaciones**
Wi-Fi	Hasta 54Mbps	400ma transmitiendo, 20ma en reposo	Gran ancho de banda	Navegar por Internet, redes de ordenadores, transferencia de ficheros
Bluetooth	1 Mbps	40ma transmitiendo, 0.2ma en reposo	Interoperatividad, sustituto del cable	Wireless USB, móviles, informática casera
ZigBee	250 kbps	30ma transmitiendo, 3ma en reposo	Batería de larga duración, bajo coste	Control remoto, productos dependientes de la batería, sensores , juguetería

2.2.1 Pasarela Residencial

Pasarela Residencial o Gateway Domótico son dispositivos que permiten adaptar las diferentes comunicaciones interiores del sistema domótico (tales como protocolos y estándares de los dispositivos domóticos) a una red exterior. Es decir, permite la comunicación entre los dispositivos domóticos con redes externas como pueden ser telefonía fija, móvil, Internet, etc. Cabe resaltar que este es el elemento fundamental para la interoperabilidad de un sistema domótico.

2.3 Protocolos

Es el formato de los mensajes que los diferentes elementos de control del sistema deben utilizar para entenderse. Se pueden clasificar según su estandarización:

- Estándar abierto: El uso es libre para todos.
- Estándar abierto bajo licencia: El uso es abierto para todos bajo licencia.
- Propietario o cerrado: Uso exclusivo del fabricante o los propietarios.

2.4 Interfaz de Usuario

Permite al usuario interactuar con el sistema domótico mediante interfaces de comunicación como por ejemplo: la línea telefónica, el teléfono móvil, Internet, etc. Varios factores han acelerado el desarrollo de nuevas interfaces, como por ejemplo: el desarrollo de Internet, el teléfono móvil como dispositivo personal y personalizado, desarrollo de los sistemas inalámbricos dentro del hogar, etc. En esta tesis se aprovechan estos factores y se implementa, mediante la gestión de llamadas telefónicas, una interfaz que le permita al usuario interactuar con una grabación de voz que le brindará opciones al usuario. Además, de poder controlar y monitorear accediendo a una Web.

2.5 Arquitecturas y Soluciones domóticas en la actualidad

Como ya se mencionó, la *Interoperabilidad,* en el contexto de domótica, es la posibilidad de comunicación entre dos o más tecnologías. De acuerdo a esta definición, podemos analizar las diferentes tecnologías que se han ido desarrollando en los últimos años y en la actualidad, buscando darle al usuario final una total interoperabilidad del sistema domótico.

Empezando con la tecnología X10, un protocolo propuesto en los 70, el cual usa la línea eléctrica para transmitir señales de control entre equipos. Puede mandar hasta 16 mensajes a un máximo de 256 dispositivos. Se puede recalcar que este protocolo es aún usado en la actualidad por su simplicidad y su compatibilidad de muchos equipos para implementarlo. Luego podemos nombrar otros estándares que han sido propuesto luego del X10, como el *Open Services Gateway Initiative* (OsGi), European Home System (EHS), European Installation BUS (EIB), Home Audio Video Interoperability (HAVi), Universal Plug and Play (UPnP), Konnex-KNX, LonWorks, Jini, etc. Todos estos estándares pretenden ofrecer al cliente una interoperabilidad; sin embargo cada uno con sus propias ventajas y desventajas.

2.5.1 Escenarios Planteados

Un estudio del Departamento de Información y Telecomunicaciones de la Universidad de Trento [10] nos ayuda a clasificar la gran variedad de estándares en 4 escenarios, tomando en cuenta las siguientes cualidades fundamentales de un sistema domótico:

Abierto: Si el protocolo es público y existe la posibilidad de poder implementarlo

Escalabilidad: La posibilidad de agregar o remover nuevos elementos en nuestro sistema sin afectar la funcionalidad y rendimiento de éste.

Heterogeneidad: Los diferentes protocolos, redes, sistemas operativos y hardware que el sistema puede aceptar.

Topología: La manera en la cual los equipos están interconectados (centralizada, bus, etc.) y qué tipo de relación existe entre estos elementos (cliente-servidor, punto a punto).

Considerando estos aspectos, el estudio realizado en la Universidad de Trento clasifica los diferentes estándares en los cuatro siguientes escenarios:

Escenario1: Bus Simple

Básicamente es un bus al cual se conectan los diferentes dispositivos. Es un protocolo cerrado. Presenta una baja escalabilidad, ya que solo soporta un número predefinido de dispositivos a conectar. Baja heterogeneidad, debido a que todos los elementos tienen que conectarse a un tipo de red bus con un único tipo de hardware;

Un claro ejemplo son los sistemas que interactúan únicamente con dispositivos X10.

Escenario 2: Centralizado cerrado

Permite el control remoto, añadiendo un Gateway a la arquitectura del sistema. El control remoto puede ser por parte del usuario o un proveedor de servicios de control remoto. En estas arquitecturas el protocolo usado es cerrado, un método muy usado por empresas que pretenden mantener el monopolio sobre la infraestructura del sistema domótico, tales como: LonWorks (de Echelon B.9), MyHome (de BTicinoE.2.1), Sistema de Casa (E.2.5), etc.

Esto se da por ejemplo, obligando al usuario a comprar únicamente dispositivos, aplicaciones, sistemas, etc. de la misma marca del Gateway. Estos tipos de soluciones son cerrados, relativamente escalables, y manejan muy poca heterogeneidad.

Escenario 3: Servidor abierto basado en jerarquía

Se busca tener un sistema abierto que se base en algún estándar. La tendencia es usar estándares públicos para la comunicación. Se introduce una capa intermedia de comunicaciones formando con ésta una jerarquía con los dispositivos domóticos. Los elementos domóticos se comunican mediante un controlador al Gateway o un servidor central que permite el control remoto. Este a su vez nos puede comunicar a Internet o cualquier otro tipo de red.
Esta arquitectura es abierta, presenta heterogeneidad y escalabilidad; sin embargo, el servidor central puede convertirse en un cuello de botella afectando la confiabilidad del sistema.

Escenario 4: Arquitectura Servidor Web punto a punto

Se busca eliminar las desventajas del escenario anterior, se construye una arquitectura descentralizada punto a punto. El servidor no es el único punto de acceso para el control remoto del sistema, ya que los dispositivos se pueden comunicar por medio de otras redes. Soluciones como Jini y HAVIB están dentro de este escenario.

2.5.2 Soluciones Domóticas en la actualidad

En la tabla 2.2 se encuentra un resumen de las principales ventajas y desventajas de algunas de las diferentes arquitecturas que se han planteado y que han servido de base para muchos proyectos.
Cabe resaltar, que se han planteado distintas soluciones en los últimos años, sin embargo resaltamos las más importantes y las que sirvieron de base para esta tesis. En el Anexo se puede encontrar información más a detalle de cada trabajo realizado.

Tabla 2.2 Ventajas y desventajas de los trabajos estudiados (Elaboración: Propia)

Trabajo	Ventajas	Desventajas
A Solution for the Integration of Domestic Devices on Network Management Platforms[4]	Uso del protocolo SNMP, simple y bajo consumo de procesador.	Accesible solo vía Internet. Requiere de Cableado (LAN) por cada Agente.
Domotic House Gateway[9]	Alta heterogeneidad. Comunicación versátil.	Accesible solo vía Internet, Utilizan mensajería pesada usa JVM
Alarma Remota y sistema de comandos para residenciales domóticas a través de GSM-SMS[2]	Uso de SMS para la comunicación. Es generalmente accesible y disponible para todas las personas. Es un servicio global inalámbrico muy comúnmente usado y aceptado. Es barato y fácil de usar.	Solo accesible de SMS. Los SMS tienen baja confiabilidad.
Mobile Interaction with Smart Enviroments through Linked Data[1]	Fácil de usar y amigable.	Solo accesible desde un Aplicativo, y solo desde Smartphone con cierto S.O., cámara y con acceso a Internet.
The Role of Web Services at Home[10]	Fácil de usar y amigable.	Accesible solo vía Internet.

2.6 Análisis de la Interoperabilidad con respecto a las arquitecturas estudiadas

En la tabla 2.3 se puede apreciar las distintas soluciones de como brindarle al usuario la interoperabilidad deseada. Sin embargo, como ya se mencionó, existen ciertas desventajas que podemos encontrar en cada una de éstas. Si bien solo hemos mencionado algunas soluciones, podemos encontrar estas desventajas en diversos trabajos en la actualidad.

Por ejemplo, se están desarrollando diversos aplicativos en el área de la domótica para Sistemas Operativos Android. Este sistema ha ido creciendo tanto en desarrollo como en usuarios; sin embargo, no podemos dejar de lado otros sistemas operativos como Symbian, iOS, Blackberry OS, etc. Si bien algunos sistemas operativos han disminuido su popularidad, aún existen usuarios y clientes interesados en adquirirlos. El objetivo de esta tesis, no es cerrarnos en un mercado específico; por lo contrario, es dar una solución de interoperabilidad que sea lo más

estándar, compatible y de fácil adquisición para el usuario.

Otras de las alternativas, como se observa en los trabajos planteados es el uso de Internet para la comunicación. Si bien es una alternativa estándar, el usuario se ve limitado a acceder al sistema desde algún dispositivo que tenga acceso a Internet. Es decir, el usuario para tener una comunicación ininterrumpida con el sistema debe contar, como por ejemplo, con un Smartphone con un plan de datos que le permita tener acceso a Internet permanentemente.

Una posible solución podría ser la planteada en [2] donde se utiliza los SMS como medio de comunicación entre el usuario y el sistema, ya que es generalmente accesible y disponible para todas las personas. Sin embargo, el SMS no es un medio confiable, ya que su diseño fue creado como una forma alternativa para comunicarse. Un estudio realizado por la Asociación 4G de las Américas [15] analizó el sistema de recepción de mensajes SMS y aseguró lo indicado, además de reafirmar que los SMS no pueden ofrecer una comunicación en tiempo real y confiable, como lo hacen las llamadas de voz. Esto puede ser crítico en casos de alarmas, o situaciones de emergencia.

Tabla 2.3 Interoperabilidad de las arquitecturas estudiadas (Elaboración: Propia)

Arquitectura Planteada	**Interoperabilidad**
A Solution for the Integration of Domestic Devices on Network Management Platforms	SNMP-LAN-Internet
Domotic House Gateway	JVM-Internet
Alarma Remota y sistema de comandos para residenciales domóticas a través de GSM-SMS	Móvil GSM-SMS
Mobile Interaction with Smart Enviroments through Linked Data	Smartphone con cámara y S.O. que soporte aplicativo
The Role of Web Services at Home	Web Server-Internet

Por otro lado, podemos resaltar de las soluciones planteadas varias cualidades, como por ejemplo el uso de Internet. Esta alternativa incorpora al sistema domótico a una actual convergencia de comunicaciones. Además, de darle la capacidad al usuario de comunicarse desde su oficina o casa con cualquier dispositivo con

conexión a Internet. El uso de celulares es otra gran ventaja para el usuario, ya que evita la compra de equipos adicionales para la comunicación. El uso de SMS, que busca de una forma tratar que el sistema sea compatible para cualquier modelo de celular.

De acuerdo a estos puntos, se planteó en esta tesis una solución que busque estas cualidades y mejore los problemas ya mencionados. Tomando en cuenta el uso del celular como medio de comunicación para el usuario, pero optando por las llamadas de voz en vez de envíos de SMS para la comunicación. Esto resulta ventajoso para generar llamadas cuando una alarma se activa, aumentando la confiabilidad de la notificación del sistema al usuario. Además, se incluyó un servidor WEB, una alternativa que le permita al usuario poder controlar y monitorear su sistema desde su PC, Smartphone, Tablet, etc.

2.7 VoIP

2.7.1 Definición

La voz sobre IP o VoIP es la transmisión de la voz sobre el protocolo IP.

2.7.2 PBX

PBX o *Private Branch eXchange*, es el sistema que nos permite conectar llamadas dentro de la misma compañía. Comúnmente puede tener desde 2 a 10000 extensiones y una conexión al sistema telefónico tradicional (PSTN) para llamadas hacia y desde el exterior de la compañía.

IP PBX

Una IP PBX es un completo sistema telefónico que provee llamadas telefónicas a través de la red IP. Todas las conversaciones son enviadas como paquetes a través de la red. [17]

CAPÍTULO 3
DISEÑO DE LOS MÓDULOS DE CONTROL, COMUNICACIÓN E IMPLEMENTACIÓN DEL SERVIDOR IP PBX

3.1 Descripción y justificación del diseño de la arquitectura del sistema

3.1.1 Requerimientos de la Arquitectura del sistema

El sistema domótico, según lo comentado en [10], podemos clasificarlo según las cualidades: abierto, escalabilidad, Heterogeneidad y topología. Se buscará en el diseño, tal como se comentará posteriormente, el uso de protocolos y software libres, que no solo reducirá costos, sino también permitirá desarrollos futuros en la plataforma. El sistema no debe limitarse a un solo protocolo, ni a un solo estándar; tanto para la comunicación con los dispositivos domóticos como para comunicación con el usuario.

Además, debe ser capaz de agregar nuevos elementos domóticos en el sistema sin afectar la funcionalidad y rendimiento de éste.

Por otro lado, la topología a implementar será centralizada. Si bien en [10] afirma que una Arquitectura punto a punto (Escenario 4), resuelve la desventaja *"cuello de botella"* de una arquitectura centralizada (Escenario 3); en un sistema domótico no hay una constante transmisión de eventos o información, ya que los elementos domóticos están en la mayoría de tiempo en reposo.

3.1.2 Módulos y elementos de la arquitectura

Para el diseño de la arquitectura se basó en los proyectos realizados y descritos en los papers Domotic House Gateway [9] y *A Solution for the Integration of Domestic Devices on Network Management Platforms* [4]. Se puede observar la arquitectura planteada en la figura 3.1.

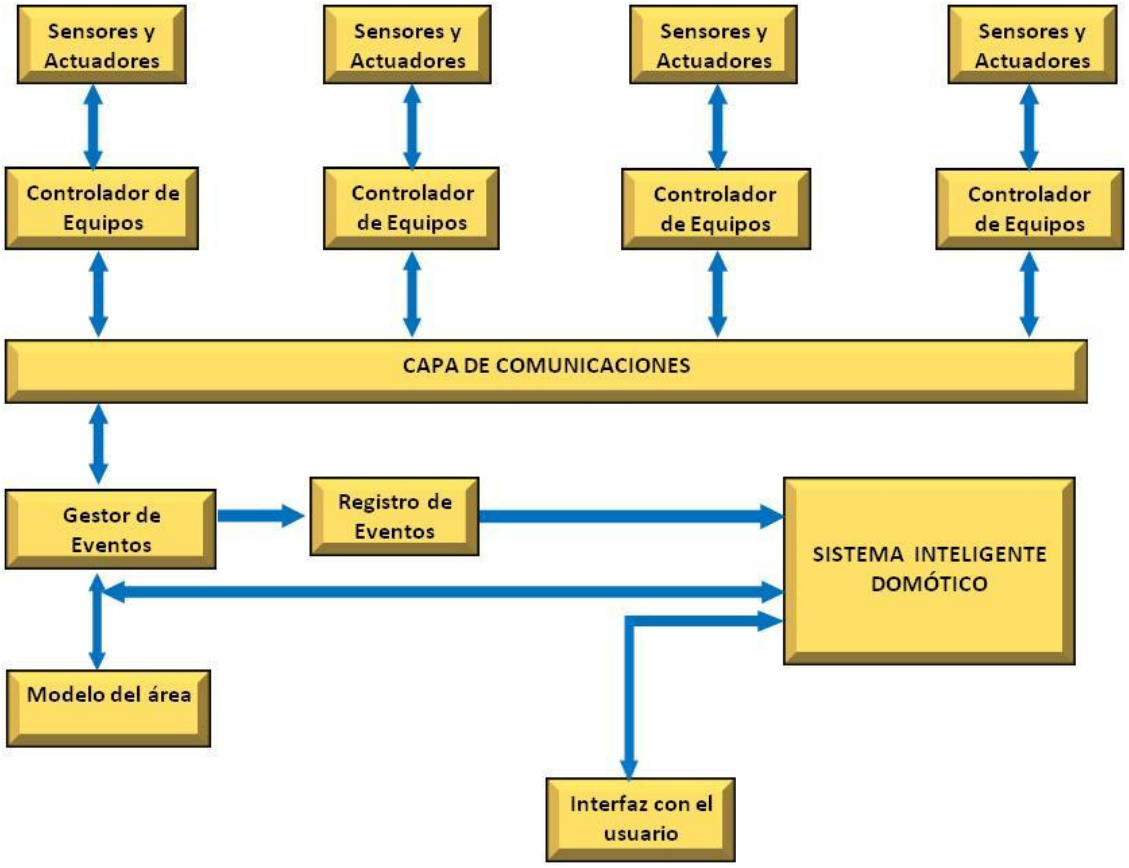

Figura 3.1 Arquitectura del sistema domótico (Basado en [9] y en [4])

Estos trabajos, nos ayudan a tener una heterogeneidad en nuestro sistema, ya que podemos incluir Controladores de Equipos que nos permitan acondicionar algún tipo de señal y comunicarlos con nuestro gestor de eventos vía la capa de comunicaciones. Se entiende por evento, un suceso lógico o físico. Los elementos de la arquitectura se detallan a continuación:

- **Controlador de equipos:** Manejará sus dispositivos y enviará la información (eventos) y estados de los diferentes dispositivos, a un gestor de Eventos. Este controlador consiste en adaptar las señales del dispositivo (actuador, sensor) para ser enviadas al gestor de eventos. El objetivo es estandarizar los tipos de señales, es decir transformar diferentes tipo de señales a una sola, para un mejor manejo al momento de agregar un nuevo dispositivo (escalabilidad). En la tesis planteada el Controlador de Equipos constará de dos Módulos:

Módulo de control: Nos permitirá obtener las señales de nuestros dispositivos domóticos y enviárselas al Módulo de Comunicaciones y viceversa.
Módulo de comunicaciones: Recibirá la información del módulo de control y se la enviará al gestor de eventos y viceversa.

- **Gestor de eventos:** Transformará la información (eventos) de bajo nivel obtenida por los controladores de equipos en información de alto nivel. Esta información incluye ubicación, características y eventos que soporta los distintos dispositivos de los controladores de equipos.

- **Modelo del área:** Es una base de datos donde la información de todos los dispositivos del área se registrarán. Esta información consta de las características, estados actuales y eventos que soportan los dispositivos.

- **Registro de eventos:** Base de datos que registra los eventos recibidos y enviados.

- **SID (Sistema Inteligente Domótico)**: Permite procesar los eventos recibidos del gestor de eventos y generar otros en respuesta a estos. Además, de acuerdo al registro de eventos se puede autogenerar eventos, o generarse según alguna regla establecida. Mediante esta estructura la comunicación se establece con el usuario, ya sea por acceso de parte del usuario, o por alguna petición generada por el sistema al usuario.

- **Interfaz con el Usuario:** En la tesis planteada consta de una voz grabada interactiva (IVR) que le va indicando al usuario opciones, y este puede ir escogiéndolas mediante el marcado de tonos DTMF. Este IVR se genera cuando el usuario quiere acceder al sistema mediante una llamada, o cuando el sistema genera una llamada al usuario. Además de poder acceder mediante el servidor WEB al sistema.

La Capa de Comunicaciones se detallará más adelante.
Por otro lado, cabe resaltar que para el diseño de esta tesis, el gestor de eventos, el modelo de área, el registro de eventos, y el SID estarán instalados en un mismo servidor. Debido a que en estos bloques se requiere mayor flujo de información, y capacidad de procesamiento; ya que se generan consultas a base de datos, se

establecen llamadas y se interactúa con el usuario. Puede considerarse, implementar cada uno de estos bloques en servidores diferentes, pero siempre teniendo en cuenta que estos deben pertenecer a la misma red local. De esta manera, la comunicación entre estos bloques será más rápida, segura y eficiente.

3.2 Requerimientos y selección de los elementos del sistema

Debemos considerar en nuestro diseño, según los objetivos planteados, los siguientes puntos:

- El usuario podrá enviar y recibir notificaciones hacia y desde dos áreas en diferentes zonas geográficas.
- El usuario podrá controlar un actuador y recibir notificaciones de dos sensores en cada zona geográfica.

Además, se debe tomar en cuenta que las pruebas se realizarán en las tiendas de la empresa Kyari Import S.A.C. con RUC 20477940138. Esta empresa está en el sector económico de Venta Mayorista de Otros Productos, y tiene 6 tiendas en Lima ubicadas en diferentes distritos, y una tienda en Huaral. Cabe resaltar que en sus tiendas tiene instaladas cámaras IP de marca Foscam que le permite monitorear de vez en cuando a sus empleados, y verificar la cantidad de mercadería disponible. Es decir cuenta con servicio de Internet en cada local. Sin embargo, no cuenta con un sistema de alarmas seguridad, como sensores de movimiento, de presencia, o algún tipo de alarma que le pueda enviar una notificación a la ubicación donde esté. De acuerdo a los puntos mencionados se describen los requerimientos de cada elemento de la arquitectura planteada.

3.2.1 Sensores y Actuadores

Con respecto a estos elementos, los requerimientos son básicos: sus salidas y entradas deben ser controlables y tienen que ser de bajo costo, ya que el objetivo de las pruebas es ensayar el funcionamiento del sistema. Los dispositivos a utilizar serán los siguientes:

<u>Sensor de Movimiento PIR</u>
Dimensiones y Peso: 92 mm x 62.5 mm x 40 mm /58 gr
Voltaje de entrada y consumo de corriente: 8.2-16VDC10mA
Salida: 0.1 Amp @ 28 VDC

Funcionamiento: El sensor cuenta con los terminales NC y C, que son los contactos del relé de salida de la alarma del detector. Cuando no está activado el detector, se encuentra normalmente cerrado. Cuando se activa, el circuito se abre durante un tiempo definido.

Figura 3.2 Detector PIR LC -100 PI (Imagen obtenida en [28])

Contacto magnético para puerta o ventanas

No requiere de alimentación. (Rango de apertura: 50.8 mm)

1 Amp. / 10 VDC (máx.)

Funcionamiento: Son sensores magnéticos que mantienen un switch cerrado mientras están en contacto. Cuando se separan, el circuito eléctrico se abre.

Figura 3.3 Contacto magnético para puerta o ventanas (Imagen obtenida en [29])

Diodo Led

El Led representa al actuador que permitirá mediante el prendido y apagado de éste, comprobar la comunicación entre el usuario y el sistema.

3.2.2 Controladores de Equipos

De acuerdo a lo comentado estos controladores se comunican con los distintos dispositivos domóticos (sensores y actuadores), y además con el Gestor de Eventos. El Controlador de Equipos consta de dos módulos: Control y Comunicaciones. En la figura 3.4 se observa un esquema de este bloque.

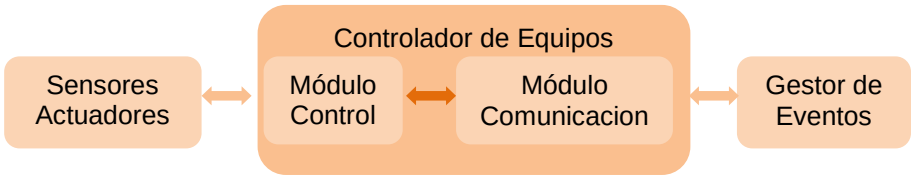

Figura 3.4 Controlador de Equipos (Elaboración: Propia)

Considerando la gran variedad y disponibilidad de microcontroladores en el mercado local que permiten la implementación del Módulo de Control; se buscó analizar y seleccionar primero el Módulo de Comunicaciones. De acuerdo a esta selección se buscan los requerimientos del microcontrolador.

Módulo de Comunicaciones

Este módulo le permite al Controlador de Equipos comunicarse con el Gestor de Eventos. Considerando esto, se define que tipos de protocolos y medios se deben utilizar para esta comunicación. Se tiene que tener en cuenta que el Gestor de Eventos, junto con el SID, Modelo de área y el Registro de eventos estarán en un mismo Servidor.

Inicialmente se consideró la comunicación usando el estándar RS232, RS485 o USB. Sin embargo, existía el limitante de la distancia entre el Controlador de Equipos y el Gestor de Eventos. Para eliminar esta limitante, se planteó el estándar Ethernet que permite la comunicación con el router y de esta manera la comunicación por Internet.

Según lo considerado, los requerimientos del módulo son: Compatible con Ethernet, soporte de 10Base-T (para la comunicación con el router o switch), que permita el envió y recepción de paquetes (Full o Half Duplex), que permita comunicarse con un microcontrolador de una manera sencilla, estándar y con la menor cantidad de pines (de preferencia serial), que sea barato y de preferencia que esté disponible en el mercado local, alimentación en el rango de 3-5 V para evitar implementar fuentes adicionales.

Se puede apreciar en la tabla 3.1 las diferentes opciones que cumplen los requerimientos planteados. Se eligió el ENC28j60 debido al costo, la disponibilidad en el mercado local, y por la cantidad de pines (bus SPI) para la comunicación con el microcontrolador. Si bien los otros controladores manejan mayor velocidad (bus paralelo), esta no es necesaria en la tesis propuesta, ya que los dispositivos

domóticos en la mayoría de tiempo están en reposo. Considerando también que el ahorro de pines en el microcontrolador permitirá conectar mayor cantidad de dispositivos adicionales a este.

Tabla 3.1 Controladores Ethernet (Elaboración: Propia)

Controlador	Precio	Cantidad de Pines para la Comunicación con el microcontrolador	Disponibilidad
CS8900A	$12.65 (Digikey)	14 pines	Importar
LAN91C111	$21 (Digikey)	8-16 pines	Importar
RTL8019	$7 (Digikey)	8-16 pines	Importar
ENC28J60	$9	4 pines(bus SPI)	Mercado local

Módulo de Control

Considerando el módulo de comunicaciones y los objetivos, los requerimientos mínimos de este módulo son: Pines Necesarios para dos sensores y un actuador (considerando interrupciones externas para los sensores), comunicación SPI para el controlador ENC28j60, comunicación UART para el módulo Zigbee (en caso se necesite conectar dispositivos inalámbricos que estén lejos del microcontrolador), Voltaje de Alimentación entre 3 V - 5.5 V permite tener una sola fuente de alimentación en el Controlador de Equipos (ENC28J60 necesita 3.3 V).

Se encontraron diversas opciones que cumplen los requisitos arriba mencionados, dentro las cuales destacaron: PIC18F242, PIC16F874, Atmega88, Atmega8L.

Se eligió el Atmega8L debido al bajo costo, la disponibilidad en el mercado local, y al conocimiento previo de este microcontrolador. Además de lo mencionado, tiene las siguientes características:

- 13 pines adicionales que permiten conectar otros dispositivos.
- Memoria programable FLASH de 8 KB, permite implementar los protocolos necesarios para la comunicación por Internet y en la red local.
- Voltaje de Alimentación de 3.3 V
- Frecuencia de oscilación de hasta 8 MHz utilizando el oscilador interno.
- Precio de bajo costo (S/.8) y disponibilidad en el mercado local.

3.2.3 Capa de Comunicaciones

El controlador de equipos se comunica al Gestor de Eventos mediante el estándar Ethernet, utilizando el Protocolo de Internet. Considerando el modelo OSI, en la tesis propuesta el protocolo de transporte a utilizar será UDP. Si bien es un protocolo sin conexión, la información que se envía es reducida. Este protocolo se caracteriza por ahorrar recursos de red, es un protocolo rápido y adecuado para transmisiones en tiempo real. Además, se utilizó un protocolo basado en Modbus ASCII para la comunicación de mayor nivel entre el Gestor de Eventos y el Controlador de Equipos. Se usó este protocolo debido a que es abierto, simple y muy usado en la actualidad. En la figura 3.5 se observa los diferentes niveles de la Capa de Comunicaciones.

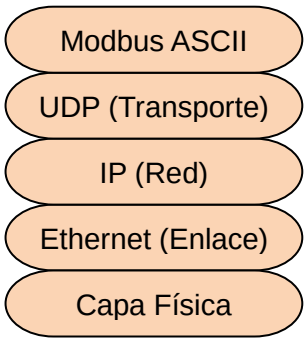

Figura 3.5 Capas de Comunicaciones del sistema implementado, según modelo OSI (Elaboración: Propia)

3.2.4 Gestor de Eventos

Este bloque tiene que ser capaz de interactuar con Base de Datos (Modelo de área y Registro de Eventos), debe tener facilidad en manejo de cadenas de caracteres para convertir la información de bajo nivel recibida por los Controladores a alto nivel, tiene que ser capaz de recibir y diferenciar las peticiones de los distintos Controladores de Equipos que puede haber, considerando que pueden estar en la misma red local, o en cualquier zona geográfica con conexión a Internet. Para este desarrollo se utilizará la programación de sockets. Un socket es un concepto abstracto por el cual dos programas pueden intercambiar información. En un servidor, se utilizan las direcciones IP de los diferentes clientes para poder

diferenciarlos. En caso dos o más clientes tengan la misma IP, se pueden diferenciar por un número de puerto diferente asignado a cada uno. Entonces, un socket queda definido por una dirección IP, un protocolo (en este caso UDP) y un número de puerto.

Para la programación de sockets se utilizó PHP, un lenguaje de programación interpretado de alto nivel. El cual permite con gran facilidad trabajar con Base de Datos, interactuar con diversas plataformas, implementar servidores WEB, programación de sockets, manejo de cadenas de caracteres, entre otros.

3.2.5 Modelo de área y Registro de Eventos

Es muy importante identificar cada elemento de nuestro sistema, y estos elementos no necesariamente tienen que ser físicos, sino tienen que representar información adecuada para que nuestro sistema pueda procesarla de la manera más eficiente y eficaz. De acuerdo a lo descrito, es implícita la necesidad de manejar una base de datos que pueda almacenar toda la información de los elementos de nuestro sistema. Por lo que es necesaria una base de datos que sea compatible y accesible para nuestro sistema.

Structured Query Language (SQL) es un lenguaje estándar de comunicación con bases de datos. Es un lenguaje normalizado que nos permite realizar trabajos con cualquier tipo de lenguaje en combinación con cualquier tipo de base de datos. Con el SQL disponible es necesaria la elección de un software de base de datos que nos permita administrar nuestra información. MySQL es la elección idónea a los requerimientos del sistema propuesto. MySQL es un gestor de datos muy rápido y muy sencillo de usar. Es muy recomendado ya que es uno de los más usados en Internet, y lo más importante se desarrolla como software libre. Las características más importantes de MySQL son: Potente Gestor de base de datos, es una base de datos relacional, es *Open Source* (código de fuente accesible), es una base de datos muy rápida, y existen una gran cantidad de base de datos que la usan [13].

3.2.6 Sistema Inteligente domótico (SID)

Este es el bloque más importante, ya que gestionará la información recibida por el gestor de eventos, y además de acuerdo al Log de eventos podrá generar nuevos

eventos, todos estos de alto nivel. Este bloque también nos permitirá controlar la interfaz con el usuario.

El SID a partir de eventos recibidos podrá relacionarlos y generar nuevos eventos. Esto permitirá por ejemplo, en caso se active una alarma de incendio generar una llamada a la estación de los bomberos con una grabación indicando la dirección del lugar, además de notificar al usuario del accionamiento de la alarma.

Además, si el usuario desea puede requerir información de la zona automatizada, podrá obtenerla llamando desde su móvil a un número definido por el sistema; de esta manera de acuerdo a lo solicitado por el cliente, podrá obtener la información del sistema como el estado de las alarmas, interruptores, e inclusive gracias al Registro de eventos el SID será capaz de brindarle reportes de consumo energético, de activación de alarmas, etc.

De acuerdo a lo descrito es necesario que este bloque pueda recibir información sin mayor problema del gestor de eventos, además de poder acceder a la información del Modelo del área y el Registro de eventos (MySQL), y lo más importante, debe ser capaz de manejar la interfaz de usuario. Esto incluye la generación y recepción de llamadas, y el manejo de la interfaz WEB.

En la actualidad existen diversas plataformas que integran los diversos protocolos de telefonía VoIP como por ejemplo: Clarent, Entice, Nextone, Cisco, Nortel, etc. Sin embargo, estos productos no son sólo muy costosos, sino también, no tienen las características y flexibilidad necesarias para implementar una plataforma de solución múltiple. Entonces considerando los puntos descritos, el SID debe contener los siguientes requerimientos:

IP PBX

Para poder incluir la telefonía en nuestro sistema, el SID no sólo debe ser una PBX, sino también una IP PBX. De esta manera, permitirá de una forma sencilla la comunicación con los demás elementos de nuestra arquitectura. Además, de incluir al sistema a una actual convergencia de comunicaciones dentro de Internet.

Gateway

Esta característica me permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. A esto no sólo refiere a la comunicación entre el sistema domótico y la voz sobre IP, sino también la capacidad de interconectar otros tipos de redes como la telefonía fija, celular, servidor de correos, fax, etc.

Plataforma como solución múltiple

Esta característica es la más importante. El servidor IP PBX debe tener la capacidad de poder implementar la plataforma domótica. Además de tener la facilidad de interactuar con Bases de datos (MySQL) y los otros elementos de la arquitectura.

Soporte de protocolos y diferentes CODECs

Debe ser capaz de interactuar con los diferentes protocolos de VoIP que son utilizados en la actualidad, además de los diferentes CODECS. Esto permitirá que el sistema sea heterogéneo.

Basado Software Libre

Esto es necesario para reducir costos de implementación.

Evaluando estos requerimientos, se optó que la solución idónea para esta tesis es el software libre Asterisk. Si bien existen otras plataformas libres, Asterisk es la solución más estable, flexible y confiable en la actualidad para desarrollos e implementación de centrales IP PBX a bajo costo.

Asterisk

Es un software de central telefónica con capacidad para voz sobre IP que es distribuido bajo licencia libre. Se tiene que recalcar que Asterisk no es una central telefónica cualquiera; es una central rica en características que en otros tiempos solo eran accesibles mediante la compra de productos costosos. [11]

Además de cumplir con los requisitos arriba mencionados, maneja una extensa lista de funcionalidades como: Capturas de llamadas, Autenticación, Bloqueo por Identificación del Llamante, Colas de Llamada, Conferencias, Conversión de Protocolos, Correo de voz, correo electrónico, Detección de voz, enrutamientos de llamadas, Grabación de llamadas, Identificación del llamante, Integración con Base de datos, IVR, Listas Negras, Llamada en espera, Lógica de Extensiones Flexible, Macros, Marcación por nombre, Mensajería SMS, Monitoreo de llamada, música en espera, No molestar, registros de llamadas, transferencias, texto a voz, timbre distintivo, transcodificación, entre otros. La ventaja de Asterisk es que, gracias su código abierto, muchos han ido desarrollando nuevas funcionalidades, siendo entonces una herramienta muy importante en las comunicaciones de telefonía.

3.2.7 Servidor Domótico

El servidor tendrá los bloques: SID, Registro de Eventos, Modelo de área, Gestor de Eventos. Asterisk puede instalarse en la mayoría de sistemas operativos basados en Linux. En esta tesis se optó por Centos, una distribución de Linux gratuita. Este sistema operativo es una bifurcación a nivel binario de la distribución Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat. [18]. Es un sistema operativo estable y eficiente. Además, es una herramienta perfecta para aplicaciones de servidor. Se puede utilizar para ejecutar programas en PHP, servidores WEB, gestión de Base de Datos, y otros servidores de aplicaciones. Por estas razones, hace que Centos sea la alternativa para implementar el servidor domótico.

Según el autor Meggelen [7], para implementar un Asterisk en un Servidor considerando como máximo 5 llamadas simultáneas, es necesario que las características mínimas de nuestro servidor sean las siguientes: Procesador 400 MHz x86, 256 MB RAM. Si bien se está considerando 5 llamadas simultáneas cuando el sistema a controlar como máximo generará dos llamadas simultáneas (dos controladores de equipos), existen otros factores que son necesarios considerar, como los programas Festival (un traductor de texto a voz), Gestor de Eventos y consultas a base de datos; estos tienen un consumo de procesador y memoria mínimos comparados con Asterisk pero se deben tener en cuenta en la implementación.

Se tiene disponible en un servidor con las siguientes características: Procesador Intel Core2Duo 1.866 GHz, Disco Duro Samsung 160 GB 7200 RPM S-ATA, 1 GB de Memoria RAM. Éste supera los requerimientos arriba mencionados, sin embargo se eligió este último para evitar gastos adicionales en la compra de otro servidor con las características mínimas arriba mencionadas.

Cálculo y consideraciones de Ancho de Banda de Internet

Con respecto al ancho de banda necesario para la comunicación por Internet, se debe considerar el máximo de llamadas simultáneas que se generaran en el sistema. En este caso son 2. Considerando que se usará el CODEC G711 para la compresión de audio. Este estándar por cada canal utiliza 87.2 Kbps [5], utilizando por los dos canales 174.4 Kbps en el caso que las dos llamadas se generen simultáneamente. Este es el consumo de ancho de banda en la comunicación por VoIP, es decir lo mínimo requerido en la zona de Surco donde estará el servidor

domótico. El proveedor de Internet ofrece al usuario un ancho de banda de 1Mbps por lo que supera los requerimientos mínimos. Cabe resaltar que no se está considerando los datos enviados por los controladores, ya que la información enviada por estos tiene un tamaño máximo de 50 bytes, el cual es menor que una llamada con CODEC G711 (160 Bytes) [5].
En las zonas de Ventanilla y Abancay se tiene también un ancho de Banda de 1 Mbps, velocidad más que suficiente para la comunicación entre los controladores de equipos y el servidor domótico.

3.3 Diseño e Implementación del Controlador de Equipos

La ventaja del Controlador de Equipos en la arquitectura planteada, es la capacidad de incorporar varios de estos controladores en el sistema, de manera que cada uno pueda controlar los sensores y actuadores con protocolos y medios de comunicación diferentes. Además, debido a que se divide en dos Módulos, en caso se requiera añadir un Controlador de Equipos más, solo será necesario modificar el diseño del Módulo de Control, más no del Módulo de Comunicaciones, ya que existe una independencia entre estos que permite reemplazar el módulo de Control por otro, sin afectar el diseño del módulo de comunicaciones. Esto debido a la comunicación estándar SPI que maneja el ENC28J60, soportado por la mayoría de microcontroladores en el mercado. Dándole así una heterogeneidad deseada al sistema.

3.3.1 Módulo de Control

Se tienen dos comunicaciones en este módulo. La primera para los dispositivos domóticos (sensores y actuador), y la segunda para la comunicación SPI con el controlador Ethernet.
Para los dispositivos domóticos se utilizaron los puertos D y C del microcontrolador Atmega8L. Específicamente se utilizaron los pines PD3 y PD2 (interrupciones externas INT1 e INT0) para los sensores Detector PIR y Contactores Magnéticos de Puerta. Cada uno de estos elementos, como se comentó, tienen dos terminales que forman un circuito el cual se abre o cierra dependiendo si el sensor está activado o no. Uno de los terminales está conectado a una de los pines de interrupción y el otro a tierra, esto para ambos sensores. Para el LED se utilizó el pin PC5.

Para la comunicación SPI se utilizaron sólo 4 pines PB5, PB4, PB3, PB2 (SCK, MISO, MOSI, CS respectivamente), mediante este ahorro de pines se tiene la posibilidad de agregar 13 dispositivos domóticos más. Cabe resaltar que si bien la comunicación con el Controlador Ethernet ENC28J60 es mediante SPI, para poder comunicar el Atmega8L a través de Internet es necesario implementar los protocolos IP (ICMP, UDP) y ARP. El protocolo ICMP permite realizar notificaciones de errores del Protocolo IP. Este protocolo permite comprobar la conectividad y disponibilidad del Controlador de Equipos con la Red local. El protocolo ARP permite encontrar la dirección física (MAC) que corresponde a una dirección IP.

El ENC28J60 implementa las funciones de las dos primeras capas del Modelo OSI: La capa Física, y la capa de Enlace de Datos. Las capas superiores necesarias se implementaron en el Atmega8L desarrollando y programando los protocolos arriba mencionados. La programación del Amtega8L se realizó en lenguaje C, utilizando las librerías avr-libc [19], y librerías desarrolladas para el manejo del controlador Ethernet definidas en [20].

Se utilizó un protocolo basado en Modbus ASCII para la comunicación de mayor nivel entre el Gestor de Eventos y el Controlador de Equipos. Básicamente consiste en el siguiente formato: ":XY1310". Donde ":" indica el comienzo de la trama. "X" es un número decimal (1-255) que es el identificador del dispositivo. "Y" es un carácter que en caso se desee puede representar el valor actual del dispositivo (Ejemplo H=apagado/L=Prendido), y 1310(CR/LF) significa final de la trama. En la figura 3.6 se observa un diagrama de flujo general sobre el desarrollo del programa en el microcontrolador Atmega8L.

Cálculo de resistencia para el LED

Considerando una corriente de 20 mA (intensidad luminosa apreciable) para el Led, y la caída de voltaje para el Led rojo de 2 V, la resistencia necesaria será:

(Vcc-Vled)/R=I => R= (3.3 V – 2 V)/ 20 mA= 65 Ohmios

Entonces se elige una Resistencia de 68 Ohmios.

Consideraciones para los sensores

El Detector PIR se conecta directamente al Atmega8L, ya que internamente maneja un temporizador al momento de activarse, lo que elimina un efecto de rebote. Con respecto al Contacto Magnético también se conecta directamente, sin embargo, el temporizador se realizó mediante un retardo de 20 ms en el software del Atmega8L al momento de ejecutarse la interrupción para eliminar el efecto rebote.

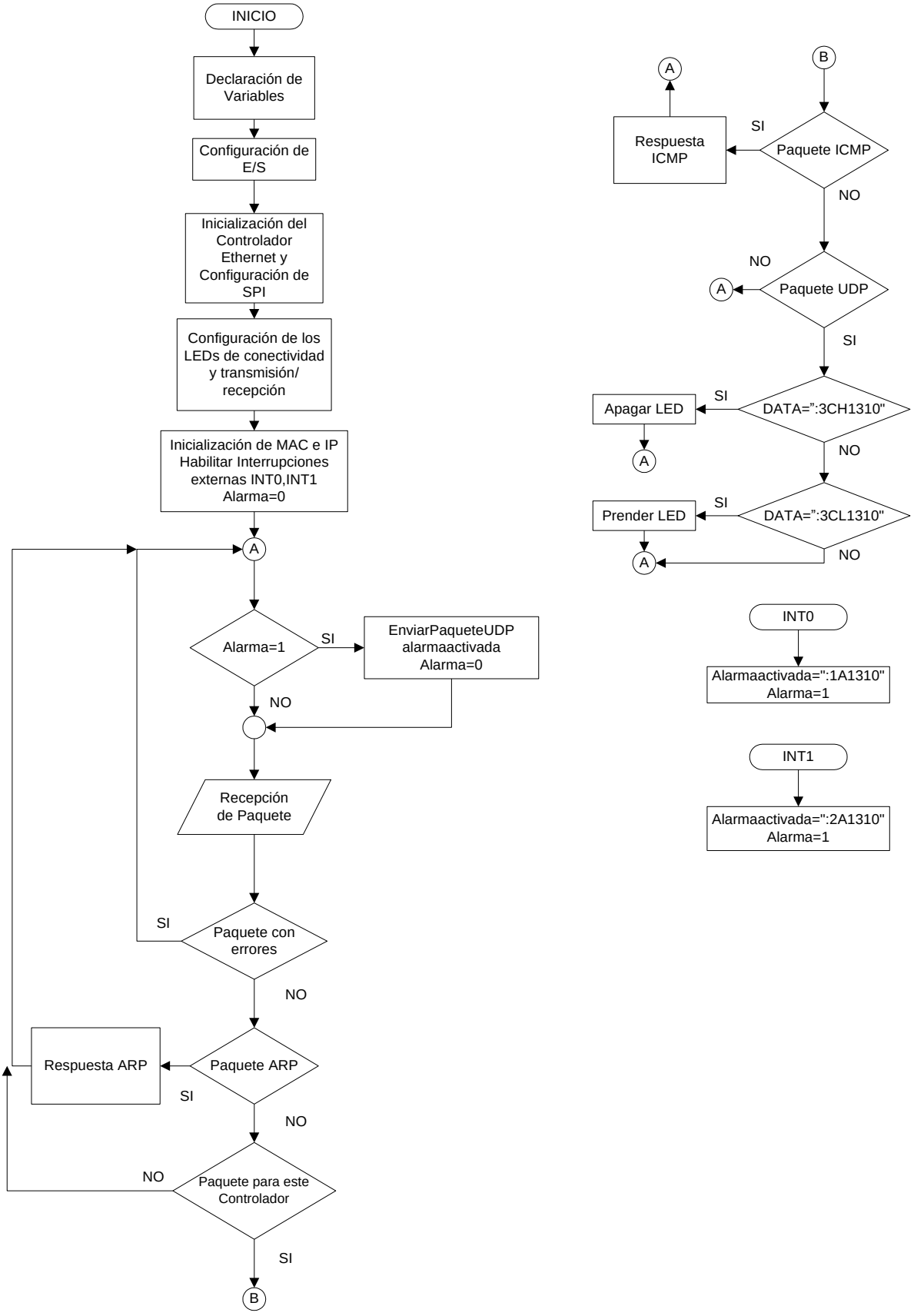

Figura 3.6 Diagrama de Flujo del programa implementado en el Atmega8L

3.3.2 Módulo de Comunicaciones

El controlador ENC28J60 le va a permitir al Atmega8L la comunicación por Internet o LAN. Para la implementación de este, se necesitan pocos componentes externos. En la figura 3.7 se observa un esquemático obtenido de la hoja de datos del fabricante [21]. Es necesario además un cristal de 25 MHz, no incluido en este esquemático pero indicado en la hoja de datos.

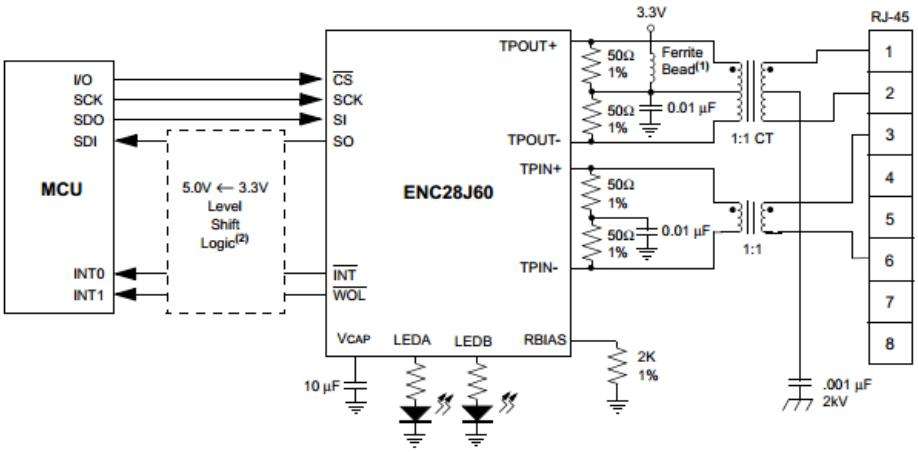

Figura 3.7 Esquemático extraído de la hoja de datos del fabricante [21]

Para el conector RJ45, se utilizó el MIC25113-0141 [22] que tiene además el embobinado y los dos Leds necesarios según el esquemático de la Figura 3.7.

Fuente de Alimentación para el Controlador de Equipos

El consumo de corriente del Atmega8L@3.3 V, 8 MHz, 25 C = 7 mA. Del Enc28j60=180 mA. Para la fuente de alimentación se utilizó el regulador de voltaje LM2937-3.3 500 mA, que proporciona un voltaje fijo de 3.3 V sin resistencias externas(a diferencia de otros como el LM317), y además tiene una caída de tensión baja de 1.4V. El esquemático completo se encuentra en la figura 3.8, el circuito impreso en la figura 3.9, y el circuito implementado en la figura 3.10. Para alimentar el circuito, por facilidad, se utilizó un transformador 220V AC/12V DC 1A.

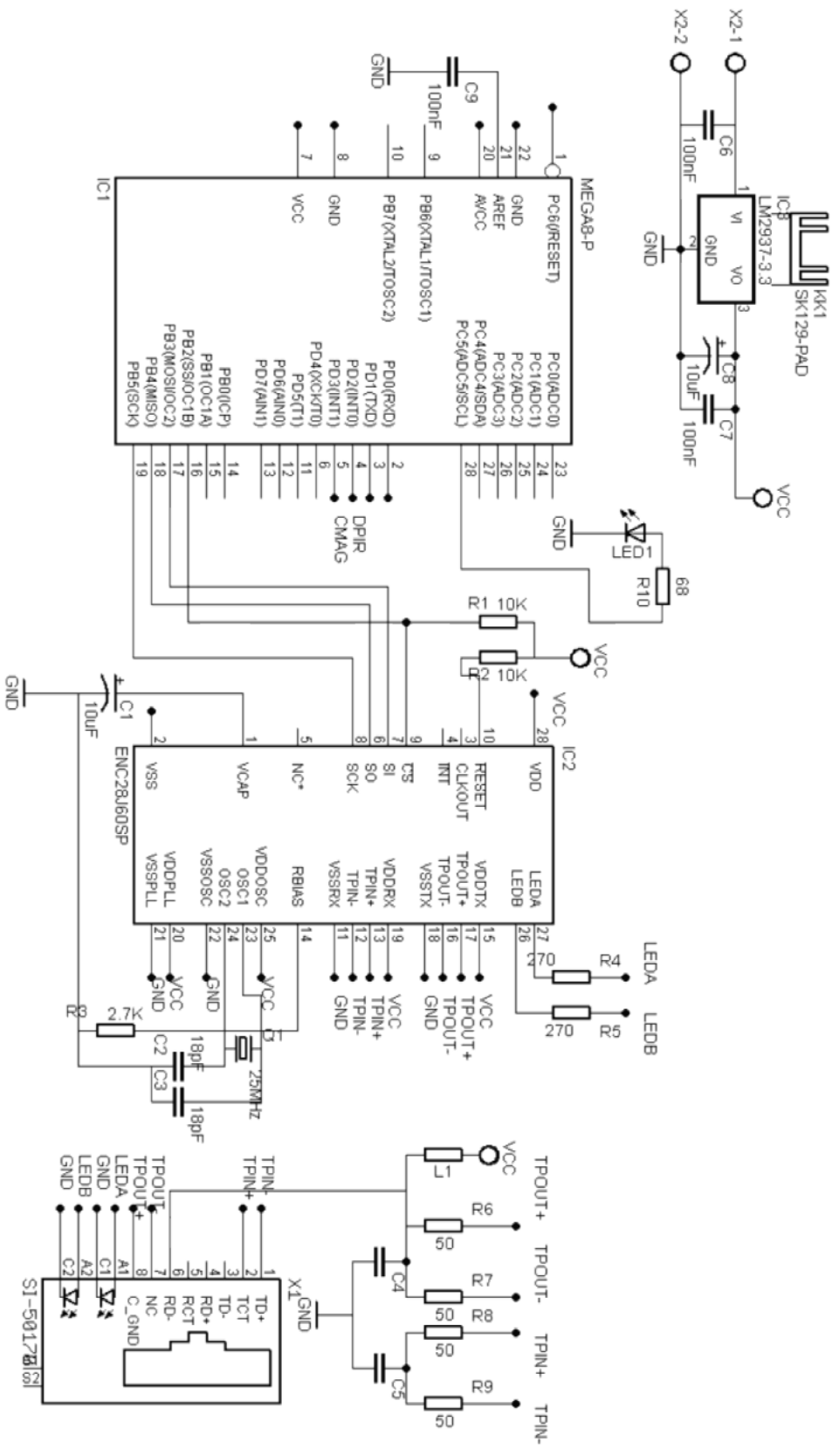

Figura 3.8 Esquemático del circuito Controlador de Equipos

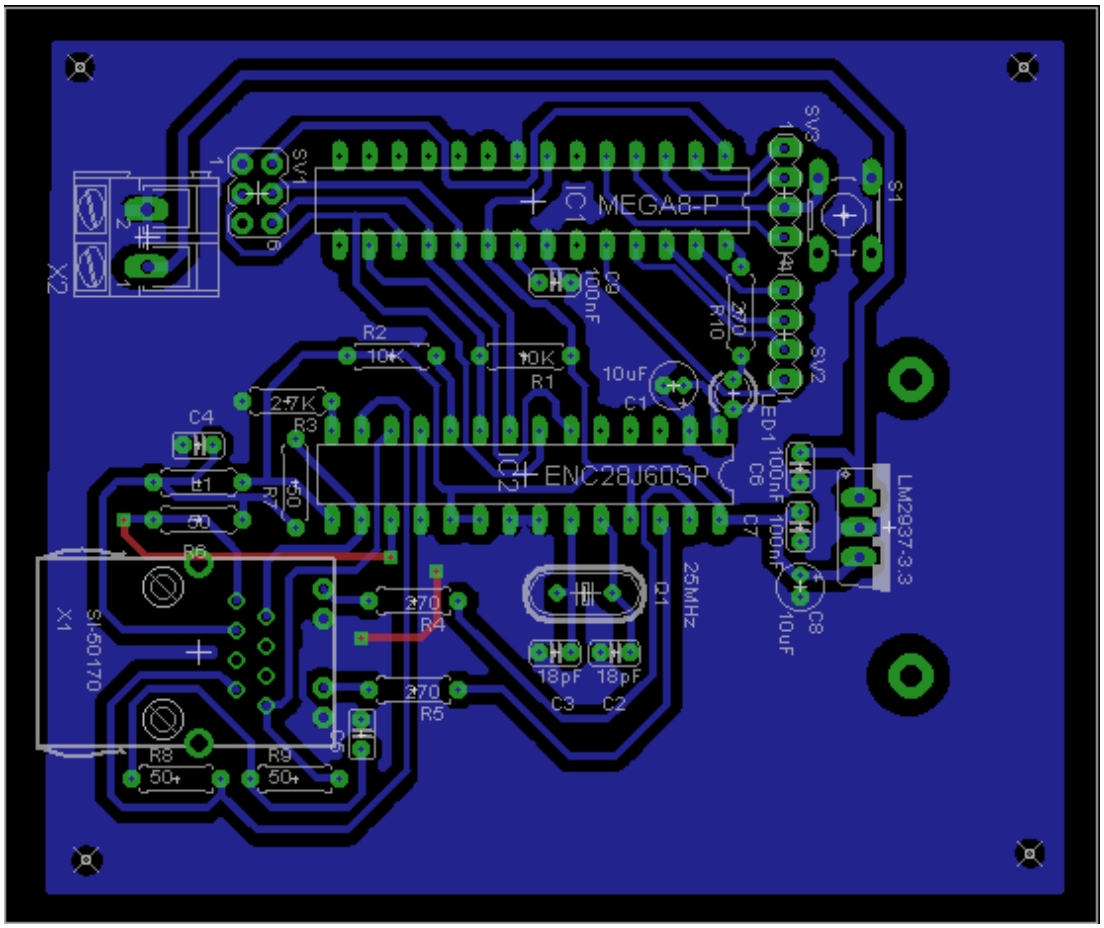

Figura 3.9 Circuito Impreso del Controlador de Equipos

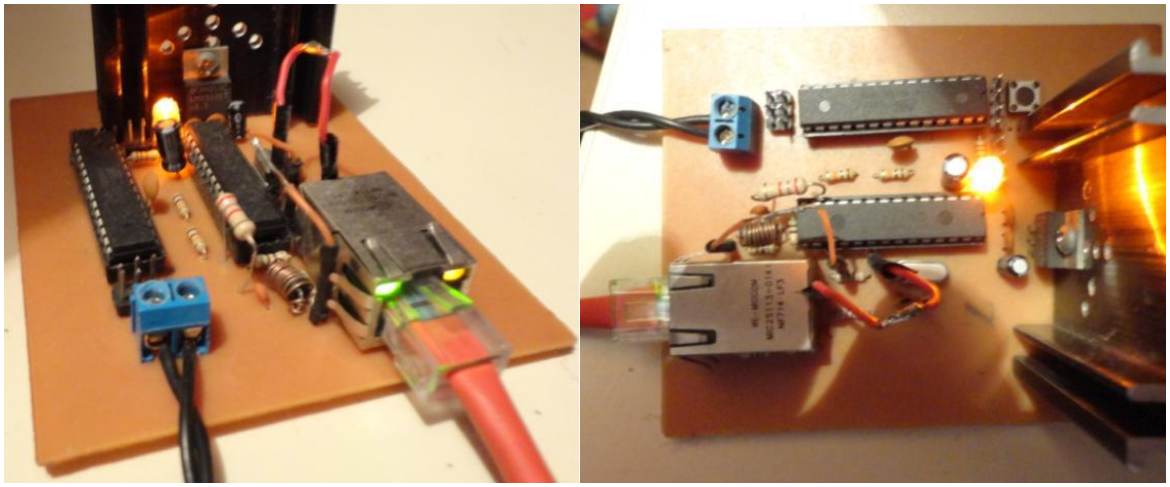

Figura 3.10 Vista Frontal y Superior del circuito Controlador de Equipos Implementado

3.4 Desarrollo del software de Gestor de Eventos

Se pudo implementar el Sistema Inteligente Domótico y el Gestor de eventos gracias a que Asterisk es una plataforma de solución múltiple. Asterisk tiene dos interfaces importantes que le permiten comunicarse con programas y servidores externos:

AGI (Asterisk Gateway Interface): Es una manera de interactuar con Asterisk desde un programa de línea de comandos. Este puede ser escrito en prácticamente cualquier lenguaje y es invocado por Asterisk desde el plan de marcado. [11]

AMI (Asterisk Manager Interface): Es una manera de comunicarse con Asterisk a través del protocolo IP. Es un concepto similar al AGI, pero la ventaja que tiene AMI es la capacidad de ser ejecutado desde equipos remotos. Cabe resaltar que es necesario abrir puertos para la comunicación. Resultando entonces una herramienta poderosa, pero insegura a comparación del AGI. [11].

Una de las características de AMI, es la capacidad de poder generar llamadas a partir de un programa externo. Esto es fundamental para realizar notificaciones cuando se active una alarma.

Para la comunicación con el Controlador de Equipos y el Gestor de Eventos se usó UDP como protocolo de transporte; y el protocolo Modbus ASCII como protocolo de comunicación de alto nivel entre ambos puntos (ver Figura 3.5).

En la tesis planteada, el gestor de eventos consta de dos programas. Un programa para recibir notificaciones de los Controladores de Equipos para luego enviárselas al SID; y otro para que pueda recibir información del SID, y enviárselas a los Controladores de Equipos. Además, ambos actualizan la información del Modelo de área, y registra cada evento en el Registro de Eventos. Los programas mencionados del Gestor de Eventos son el *Servidorudp* y *Clienteudp*.

3.4.1 Servidorudp

Básicamente es un Servidor UDP, programado en PHP basado a *Sockets.* Este programa permite recibir información, de Internet o LAN (usando el Protocolo UDP), de los Controladores de Equipos y enviárselos al SID (AMI). El servidor UDP, puede recibir múltiples conexiones, considerando siempre que todas éstas deben ser diferenciadas por la dirección IP o el Puerto, es decir cada Controlador de Equipos tiene que tener una dirección diferente, para que el Servidor UDP pueda diferenciarlos. En caso dos controladores de Equipos tengan la misma dirección IP,

es necesario que ambos manden la información de un puerto diferente, para que el Servidor pueda diferenciarlos. El Servidor UDP está instalado en el Servidor Domótico, tiene una IP Pública 181.65.29.159 y una IP Privada 192.168.1.100. La información proveniente de Internet y enviada al puerto 5151 por los Controladores de Equipos es direccionada a esta IP, ya que previamente se realizó Direccionamiento de Puertos en el router, para que toda esta información sea enviada al Servidor Domótico.

3.4.2 Clienteudp

Es un Cliente UDP, también programado en PHP basado en Sockets. Este programa controlado por el SID (AGI) le permite enviar información, a través de Internet o LAN (usando el Protocolo UDP), a los Controladores de Equipos. De la misma manera que el Servidor UDP, es necesario que cada Controlador de Equipos tenga una IP diferente o que reciba la información de un puerto diferente.
Cada Controlador de Equipo, de la misma manera que el Servidor Domótico, tiene que tener una IP Pública y Privada. Además debe haber un direccionamiento de puertos. Es decir, toda la información enviada a la IP Pública del Controlador de Equipos al puerto 1200, debe ser direccionada a su IP Privada.
En la Tesis propuesta, se tienen dos Controladores de Equipos en diferentes zonas geográficas, ambas con diferentes IPs públicas:

Controlador de Equipos Ventanilla
IP Pública 190.235.19.211
IP Privada 192.168.1.99 (Puerto 1200)
Controlador de Equipos Abancay
IP Pública 190.238.143.214
IP Privada 192.168.1.99 (Puerto 1200)

3.5 Implementación de la base de datos Modelo de área y Registro de Eventos

En la tesis planteada el modelo de área es una base de datos con tres tablas: Usuarios, Dispositivos, Teléfonos. A continuación se describen las tablas mencionadas:

Usuarios

Consta de los siguientes campos: Nombre, Cuenta, PinyPass, Priv (Privilegios).Cada usuario tiene registrado su “Nombre”, y tiene su propio Pin y contraseña (“PinyPass”) para poder acceder al sistema. Además, cada Controlador de Equipo tiene asociada una única Cuenta. Como se observa en la tabla 3.2 varios usuarios pueden controlar los dispositivos de un mismo Controlador de Equipos, debido a que tienen asociados la misma cuenta. El campo Privilegios indica que dispositivos puede controlar el usuario, ‘1’ indica el mayor privilegio, ‘5’ el menor.

Dispositivos

Esta tabla (tabla 3.3) muestra las características de los dispositivos. El campo “Ident” (Identificador) es el número que está asociado a un único dispositivo. También se especifica el “tipo” de dispositivo: S (Sensor), A (actuador), y el “estado” (ON, OFF). Cabe resaltar que se puede agregar otros tipos para algún dispositivo en especial. Por ejemplo se puede agregar el “tipo”: R para el aire acondicionado, y en el campo “estado” estaría la temperatura actual en vez de ON/OFF. El campo “IPaddress” son los del Controlador de Equipos de la respectiva cuenta. El campo “cuenta” indica a que controlador de equipos pertenece el dispositivo, y en “Priv” (Privilegios) se indica del 1 al 5 para indicar que usuarios pueden controlarlo. Es decir, un usuario con Privilegios ‘3’ solo podrá controlar equipos con privilegios iguales o mayores a este (3, 4, 5).El campo Opción indica que dígito debe presionar el usuario desde su dispositivo telefónico para elegirlo.

Teléfonos

En esta tabla 3.4 se indican los teléfonos o extensiones los cuales el sistema debe llamar cuando se active cierto sensor. Además de la grabación que se genera en la llamada.

El Registro de Eventos se realizó también en una Base Datos. Por cada evento generado o recibido se va registrando en la tabla “RegistrodeEventos”. Ver Anexo el log.

Tabla 3.2 Tabla Usuarios del Modelo de área (Elaboración: Propia)

id	Extension	Nombre	Cuenta	PinyPass	Priv
1	1001	Juan	1000002	26088891234	1
2	1002	Pepe	1000001	78964511245	1
3	1003	Lucho	1000001	47895235478	5
4	1004	Luis	1000000	45312642552	5
5	101	Wally	1000000	27475303887	1
6	1006	Urpi	1000003	34812941234	1

Tabla 3.3 Tabla Dispositivos del Modelo de área (Elaboración: Propia)

Ident	Dispositivo	Tipo	Estado	Cuenta	Priv	Opcion	IPaddress
1	Sensor de Movimiento Ventanilla	S	OFF	1000000	5	2	190.235.19.211
3	Led 1 Ventanilla	A	ON	1000000	4	3	190.235.19.211
2	Sensor de Puerta Ventanilla	S	OFF	1000000	5	1	190.235.19.211
13	Pulsador 2	S	OFF	1000003	5	1	-
14	Led 3	A	OFF	1000003	5	2	-
15	Sensor de Movimiento Abancay	S	OFF	1000000	5	4	190.238.143.214
16	Led 1 Abancay	A	ON	1000000	4	5	190.238.143.214
17	Sensor de Puerta Abancay	S	OFF	1000000	5	6	190.238.143.214

Tabla 3.4 Tabla Teléfonos del Modelo de área (Elaboración: Propia)

id	Ident	Teléfono	Grabación
1	1	101	Se activó el sensor
2	2	101	Se activó el sensor
3	13	102	Se ha activado el Pulsador 2
4	15	101	Se activó el sensor
5	17	101	Se activó el sensor

3.6 Interfaz de Usuario

La interface de usuario consta de dos bloques. El primero es el Control y Notificación por llamadas telefónicas, el segundo mediante una página Web. Cabe resaltar que para las pruebas se utilizó solamente VoIP ya que debido a falta de presupuesto no se pudo realizar pruebas con telefonía fija o móvil. Sin embargo, en el último capítulo se tomará en cuenta el presupuesto necesario para implementar un sistema considerando ambas redes telefónicas.

3.6.1 Control y notificación por llamadas telefónicas

En la figura 3.11 se observa el escenario donde se implementó el sistema. Estas se realizaron en dos locales de la empresa Kyari Import S.A.C., ambos en zonas geográficas diferentes: Ventanilla y Abancay. El servidor domótico está ubicado en Surco.Se detallará como el usuario interactúa con el sistema para poder comprender el funcionamiento de cada elemento

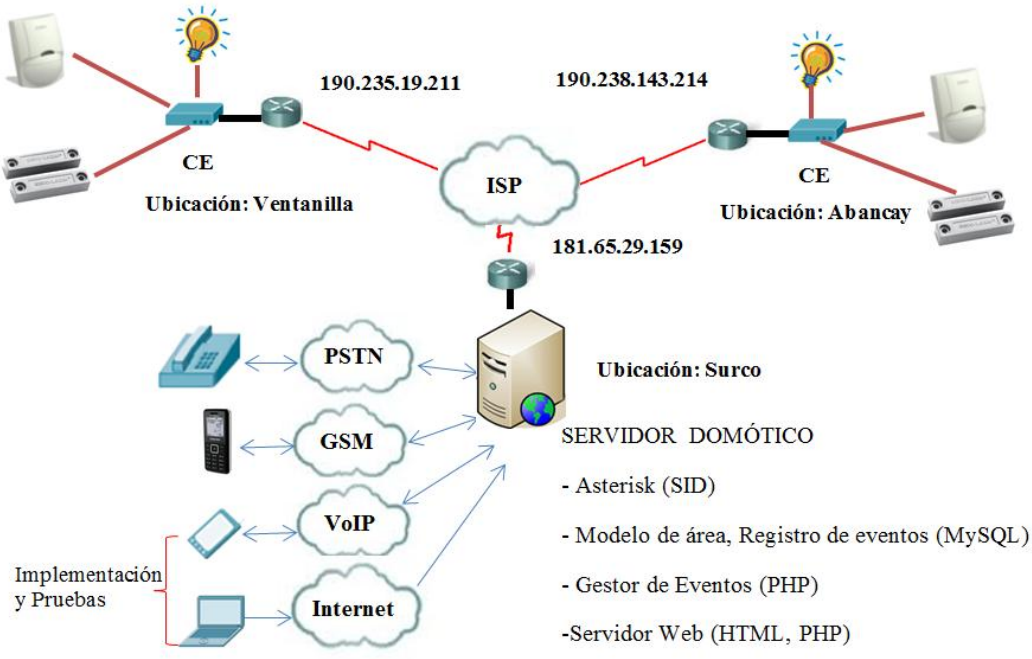

Figura 3.11 Escenario de Pruebas (CE: Controlador de Equipo, ISP: Proveedor de servicios de Internet, Elaboración: Propia)

Control por Menú Interactivo utilizando IVRs generados por Asterisk

Esta interface funciona de la siguiente manera:

1. El usuario llama a la extensión configurada en Asterisk para interactuar con el sistema. En este caso, tiene que marcar la extensión 804. El usuario puede llamar desde un IP phone o softphone, previamente registrados en el servidor Asterisk.
2. Asterisk contestará la llamada y generará un IVR, pidiéndole al usuario su PIN (7 dígitos) y contraseña (4 dígitos).

3. El usuario digita mediante su dispositivo telefónico la información solicitada mediante los DTMF y el Asterisk confirma esta información, si es inválida Asterisk volverá a pedir nuevamente sus datos de seguridad. Si el usuario falla tres veces, Asterisk corta la llamada.
4. Una vez confirmada la información, el sistema (de acuerdo al pin y contraseña ingresados) busca la cuenta asociada al usuario.
5. Asterisk generará otro IVR indicándole un menú de opciones con los dispositivos que tiene asignados a su cuenta. Este es el Menú principal.
6. El usuario elige el dispositivo digitando la opción respectiva a éste.
7. El sistema de acuerdo a la opción marcada por el usuario, le brinda las opciones de control o monitoreo del dispositivo elegido. Además de darle la alternativa de marcar '0' en caso se desee regresar al menú principal.

Por ejemplo, el usuario "Wally" de la tabla 3.2 marca la extensión 804.

- Asterisk genera el IVR: *"Bienvenido marque su PIN y Password y presione numeral"*
- El usuario marca "27475303887#"(ver tabla 3.2)
- Asterisk genera el IVR: *"Después del tono Marque 1 para el sensor de Puerta Ventanilla , Marque 2 para el sensor de Movimiento Ventanilla, Marque 3 para el Led1 Ventanilla, Marque 4 para el sensor de Movimiento Abancay, Marque 5 para el Led 1 Abancay, Marque 6 para el sensor de puerta Abancay"* (se generan las opciones de acuerdo al campo "OpcionMenu" de la tabla 3.3)
- Usuario marca opción 3.
- Asterisk genera el IVR: *"Marque 1 para apagarlo, Marque 2 para prenderlo, Marque 0 para volver al menú principal"*
- El usuario marca 2. El Dispositivo Led se prende.
- Asterisk genera el IVR: *"Marque 1 para apagarlo, Marque 2 para prenderlo, Marque 0 para volver al menú principal"*
- El usuario marca 0.
- Asterisk genera el IVR: *"Después del tono Marque 1 para el dispositivo sensor de Puerta Ventanilla , Marque 2 para el dispositivo sensor de Movimiento Ventanilla, Marque 3 para el dispositivo Led 1Ventanilla, Marque 4 para el dispositivo sensor de Movimiento Abancay, Marque 5 para el dispositivo Led 1 Abancay, Marque 6 para el dispositivo sensor de puerta Abancay"*
- El usuario cuelga la llamada.

Cabe resaltar que para un acceso más rápido, si el usuario ya conoce las opciones, puede marcar directamente la extensión 801. Esta extensión luego de confirmar su Pin y Password le pedirá que marque la opción del dispositivo, sin especificar todo el menú principal completo.

Notificaciones por voz

Cuando se genere una alarma, por la activación de algún sensor, el controlador de equipos informará al sistema vía Internet o LAN. El Sistema buscará, según el identificador del dispositivo, a que teléfono se deberá notificar con su respectiva grabación (tabla 3.4). Por ejemplo, se activa el dispositivo con Identificador 13. Se realizará una llamada a la extensión 102, con la siguiente grabación que se repetirá tres veces: "*Se ha activado el Pulsador 2"*.

3.6.2 Servidor WEB en HTML y PHP

Para la interfaz web se realizó mediante la programación en lenguaje PHP y HTML (CCS). Esta interfaz es independiente del SID, ya que no interactúa directamente con este. Por otro lado se comunica con el gestor de eventos y con el Modelo de área. Cabe resaltar que esta interfaz sólo envía eventos al controlador, más no los recibe. Las notificaciones de alarmas activadas por los sensores, solamente interactúan con el SID (Asterisk) ya que como se comentó, las notificaciones por voz son las más confiables. Para ingresar a la interfaz web, el usuario debe acceder a la web colocando en la URL: wallyrouter.dyndns.org:82/web.php (Ver figura 3.12d).

Se observa en la Figura 3.12a la primera página que aparecerá cuando el usuario acceda al sistema. Donde el usuario deberá ingresar su PIN y PASSWORD según esté registrado en la tabla 3.2. En la Figura 3.12b se observa un mensaje de bienvenida con el nombre del usuario y sus dispositivos asociados a su cuenta. En la Figura 3.12c se observan las opciones que el usuario tiene cuando escogió el Led 1 Abancay: Prender, Apagar, Volver al Menú Principal. Esta última opción le permite regresar al menú de dispositivos.

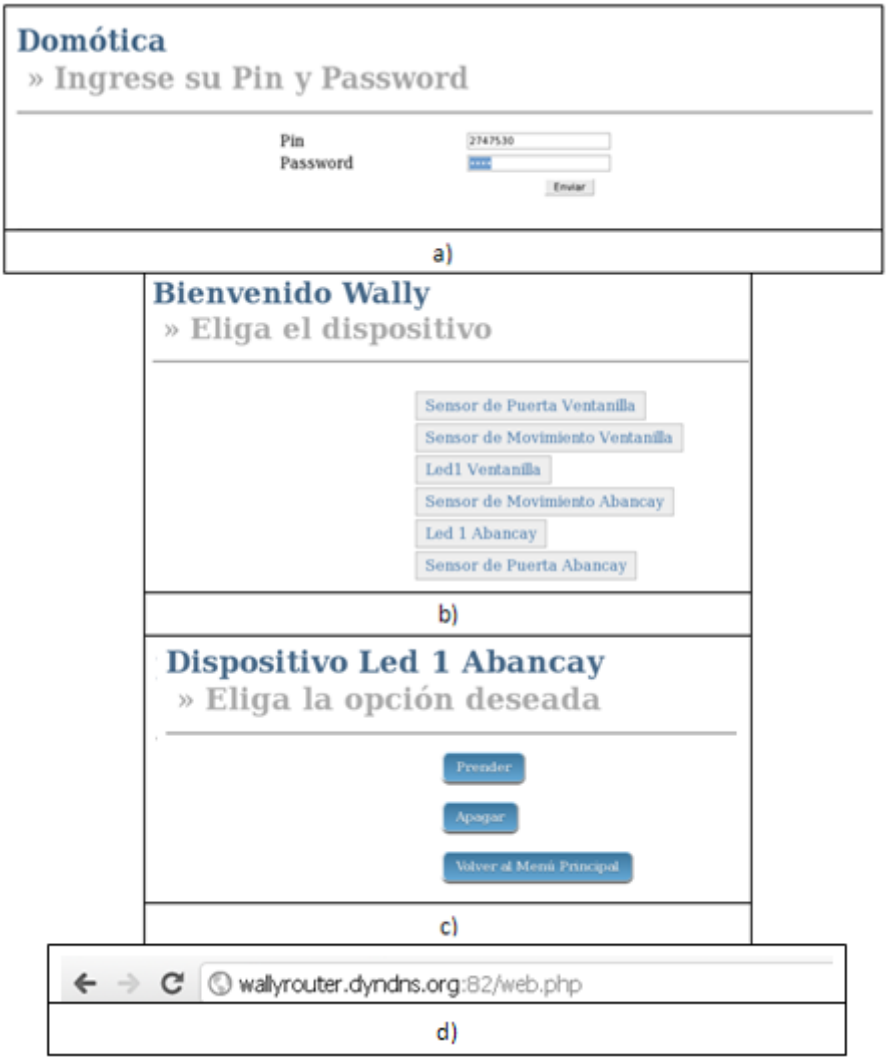

Figura 3.12 Interfaz Web (Elaboración: Propia)

3.7 Desarrollo del Sistema Inteligente Domótico

Considerando los bloques previamente descritos, se observa en la figura 3.13 como el SID interactúa con todos los elementos del sistema.

Para implementar una plataforma en Asterisk debe tenerse en cuenta los archivos de configuración que este tiene. Los básicos son dos: *sip.conf* y *extensions.conf*.

Sip.conf

En este archivo se configura los dispositivos SIP, troncales SIP o proveedores que soportan este protocolo. Se tienen distintos archivos dependiendo del protocolo a usar: iax.conf (protocolo IAX), sip.conf (protocolo sip), zapata.conf (tarjetas

telefónicas análogicas), etc. En este caso se utilizó sólo el sip.conf debido a que se utilizó el protocolo SIP. (Ver en anexo detalle de este protocolo). Como se comentó este protocolo establece y finaliza las llamadas es SIP. Un protocolo que por su simplicidad, escalabilidad y flexibilidad es uno de los protocolos más usados en la actualidad por la mayoría de las empresas de telecomunicaciones.

Para la Codificación de Voz se utilizó el estándar G711 que a diferencia de otros es libre. Además proporciona un flujo de datos de hasta 64kbit/s.
El método para el envío de los DTMF es Outband usando el estándar RFC2833, que permite el envío de los DTMF como eventos. Para más detalle de lo mencionado ver en el anexo.

Extension.conf

Este archivo contiene el Plan de Marcado. Cabe resaltar que una "*extensión"* en el contexto de Asterisk no necesariamente refiere a un dispositivo telefónico dentro de la red de una PBX como se conoce normalmente. Una extensión es una regla o conjunto de reglas que se tiene dentro de un plan de marcado. Por ejemplo, la extensión 800 puede referir a un mensaje de bienvenida, luego una reproducción de una música, y luego de tres segundos colgar la llamada. Es decir cuando el usuario marque la extensión 800 seguirá todo este procedimiento. Para establecer estas reglas se tienen distintos comandos propios de Asterisk. Uno de estos comandos es el llamado AGI, que me permite ejecutar un script dentro del plan de marcado.

Para el diseño del Plan de Marcado se utilizaron los comandos propios del Asterisk, y además gracias a la flexibilidad que tiene este software con otros lenguajes de programación, se utilizó una librería de PHP llamada *phpagi*. Una librería muy utilizada para implementar plataformas en Asterisk, debido a que facilita el manejo de comandos, ejecución de programas externos, interactúa con Festival (traductor de texto a voz) y consulta con base de datos. Se puede observar la figura 3.14 un diagrama de flujo general del SID cuando un Usuario genera una llamada para poder interactuar con el sistema; y además un diagrama de flujo cuando una alarma se activa y genera una llamada de alerta a un dispositivo telefónico.
Otros de los programas que se utilizó e interactuaron con Asterisk es Festival. Si bien no está incluido en la arquitectura, se utiliza en algunos momentos en la interfaz de usuario.

Texto a voz usando Festival

Festival es una aplicación de software libre que traduce texto a voz que se puede llamar desde el plan de marcado de Asterisk. Si bien la voz es un poco robotizada, es entendible y muy útil. Se debe tener en cuenta que no es muy recomendable usarla en tiempo real cuando se establecen muchas llamadas simultáneas, ya que consume mucho procesador. En la tesis planteada si bien no se manejan muchas llamadas simultáneas, se trató de no utilizarla mucho.

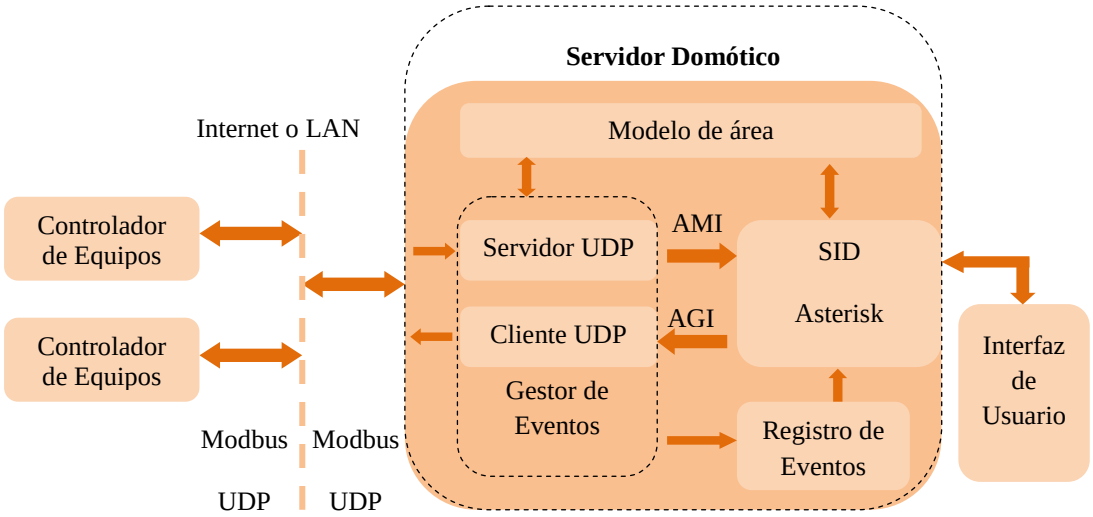

Figura 3.13 Interacción del SID con la arquitectura (Elaboración: Propia)

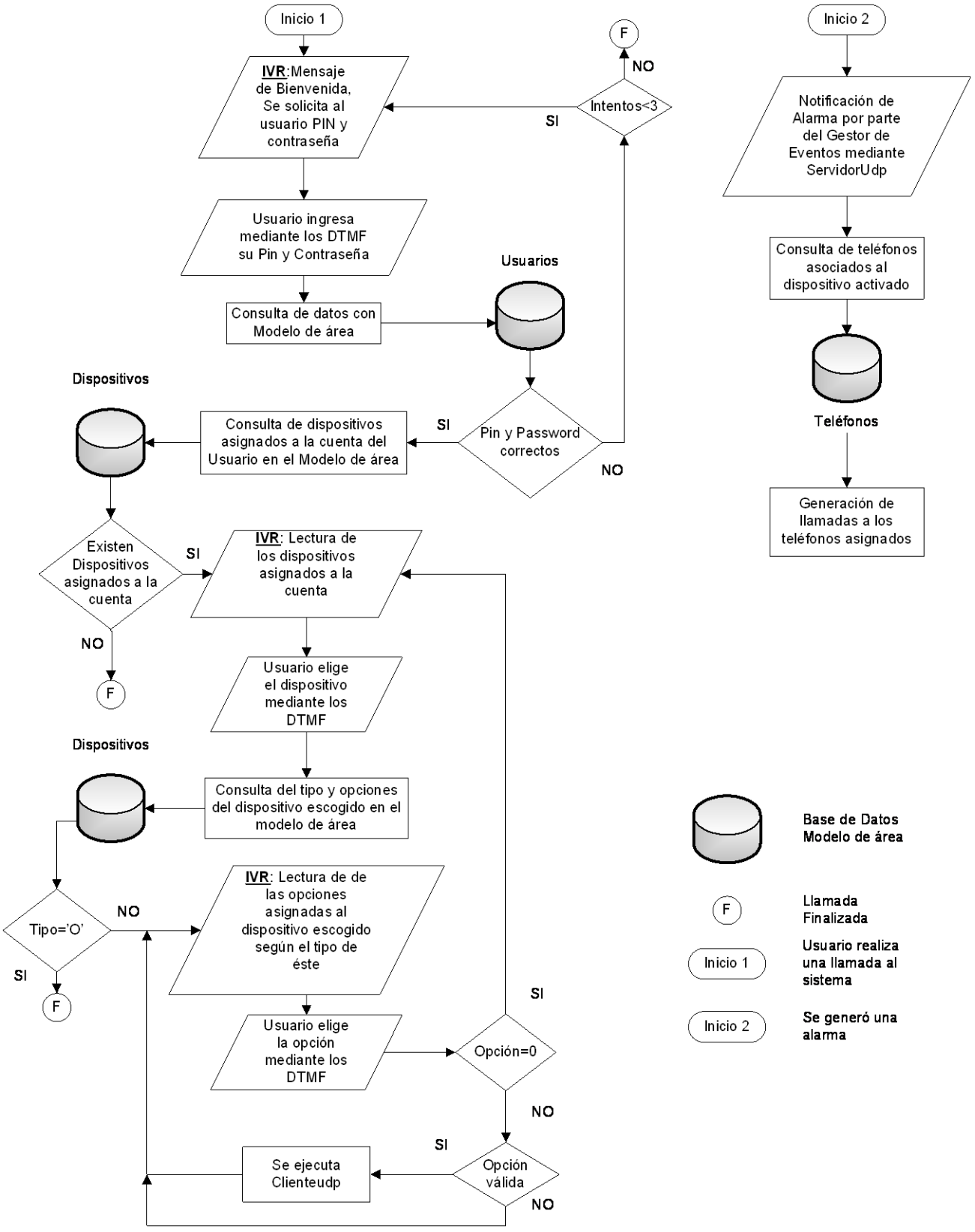

Figura 3.14 Diagrama de Flujo del SID (Elaboración: Propia)

CAPÍTULO 4
PRUEBAS Y RESULTADOS, ANÁLISIS DE COSTOS Y PRESUPUESTO DEL SISTEMA A IMPLEMENTAR

4.1 Pruebas y Resultados

Las primeras pruebas con la plataforma se realizaron sólo en la red Local del servidor domótico (sin acceso a Internet, todos los elementos en la misma zona geográfica). En estas pruebas se consideró lo siguiente:

192.168.1.35: Teléfono VoIP, desde un Smartphone se instaló un aplicativo gratuito (CSipSimple) para registrarse como extensión *101* en el Asterisk.
192.168.1.100: Asterisk (SID)
192.138.1.99: Controlador de Equipos. Para estas pruebas, temporalmente se modificó la tabla Dispositivos (tabla 3.3) específicamente se puso para la Cuenta "1000000" la "IPaddress" 192.168.1.99. (Para todos los dispositivos asociados)

Cabe resaltar que todas las pruebas se realizaron utilizando el programa *Wireshark*, un software libre que permite capturar los paquetes entrantes y salientes de una interfaz de red en una computadora. En este caso se capturaron los paquetes de la tarjeta de red del Servidor Domótico.

Se observa en la figura 4.1 el flujo de tráfico cuando se realiza una llamada a la plataforma Asterisk y este genera el **Menú interactivo** explicado en la sección 3.7.1. En este gráfico se tienen 3 campos, el primero es el tiempo, el segundo es el flujo de cada paquete enviado, y el tercero es una breve descripción de cada paquete. En este caso el usuario 'Wally' realiza una llamada a la extensión 804. Como se comentó en la sección 3.7.1, Asterisk le da un mensaje de Bienvenida solicitando su Pin y Password. En el intervalo A se establece la llamada e inmediatamente Asterisk genera este mensaje. En el intervalo B se observa como el usuario ingresa mediante los tonos DTMF su Pin y Password (27475303887#), estos se observan como eventos RTP en el flujo de la llamada. Ejemplo para el tono 2: "*RTP EVENT: Payload type=RTP Event, DTMF **Two 2**(end)"*

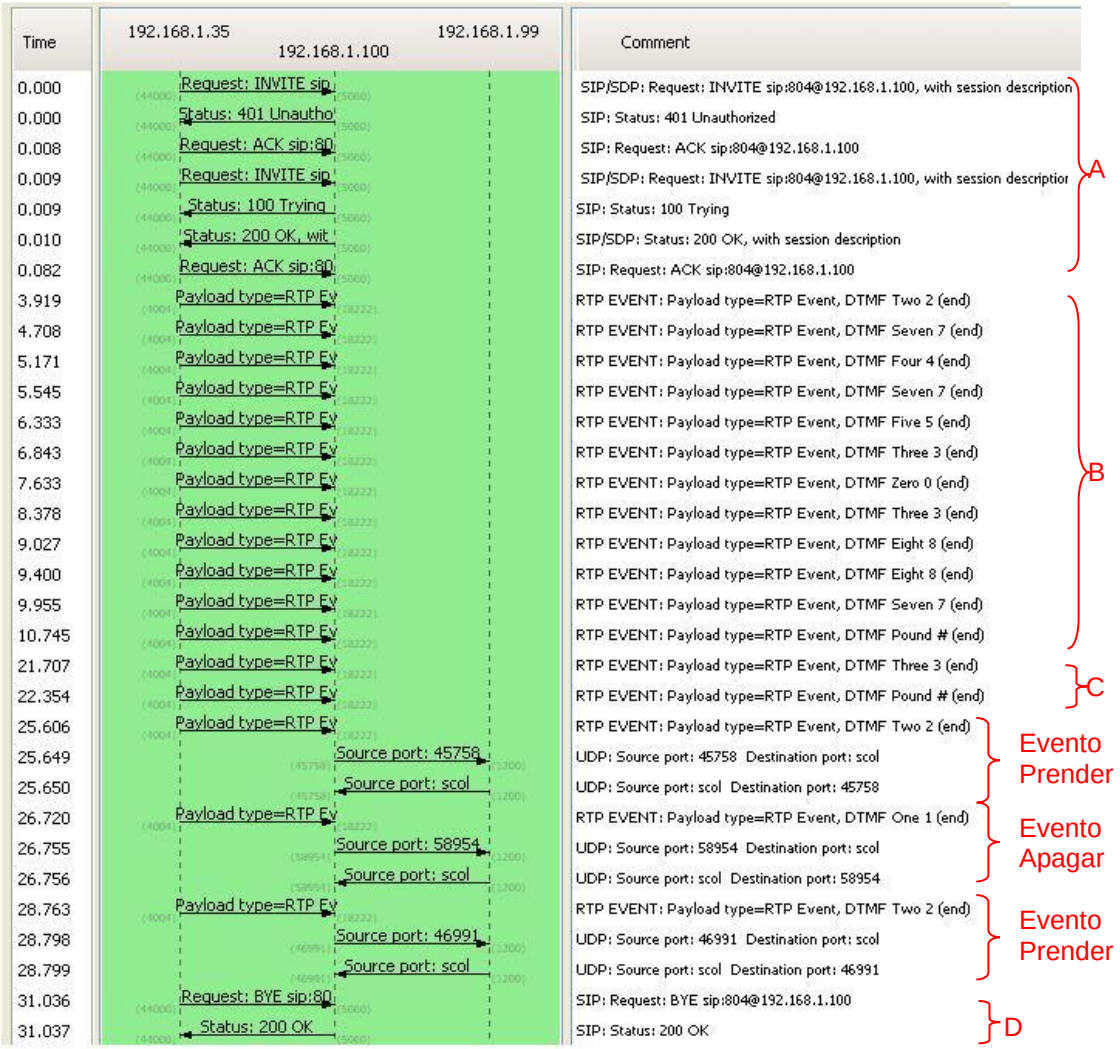

Figura4.1 Flujo de tráfico del Menú interactivo (Traza obtenida de *Wireshark*)

Asterisk verifica en el Modelo de área en la tabla Usuarios (tabla 3.2) que la información es correcta, entonces Asterisk genera un mensaje brindándole los dispositivos asociados a su cuenta. En el intervalo C se observa que el usuario marca la opción 3(“3#”), según la tabla Dispositivos en el Modelo de área (tabla 3.3) es el dispositivo *“Led 1 Ventanilla”.* Luego que Asterisk confirma esta información genera otro mensaje indicando que opciones tiene el usuario con este dispositivo, en este caso: Prender y Apagar. Cabe resaltar que hasta el momento no hay comunicación alguna con el Controlador de Equipos (192.168.1.99). A continuación el usuario marca la opción 2 que en este caso es Prender, e inmediatamente Asterisk manda un paquete UDP al controlador de equipos, este último prende el Led y luego manda un mensaje de confirmación (notar que el tiempo de respuesta

del Controlador de Equipos es de alrededor de 1 ms) .Luego el usuario marca el “1” para apagarlo y luego el “2” nuevamente para prenderlo. En el intervalo D se observa cuando el usuario cuelga la llamada. De estas pruebas se puede concluir que el número de eventos enviados (NEE) es igual al número de eventos recibidos (NER), en este caso son tres.

Para las **notificaciones por voz,** descritos en la sección 3.7.1, en la figura 4.2 se observa el flujo de tráfico cuando éstas se realizan. Se observa que luego del paquete enviado por el controlador, Asterisk genera una llamada a la extensión 101 (*INVITE sip:101@192.168.1.35),* ya que está asociada a este dispositivo (ver tabla 3.4). En la figura 4.3 se observa la información del paquete enviado por el Controlador de Equipos al Servidor Domótico: Puerto e IP Destino y Origen, Protocolos, Data, etc. Se puede apreciar en el campo Data (Modbus ASCII) *“:2A1310”.* Siendo “2” el identificador del dispositivo, en este caso según tabla 3.3, es el Sensor de Puerta, y “A” el indicativo de Alarma. . De estas pruebas se puede concluir que el NEE es igual al NER, en este caso es uno.

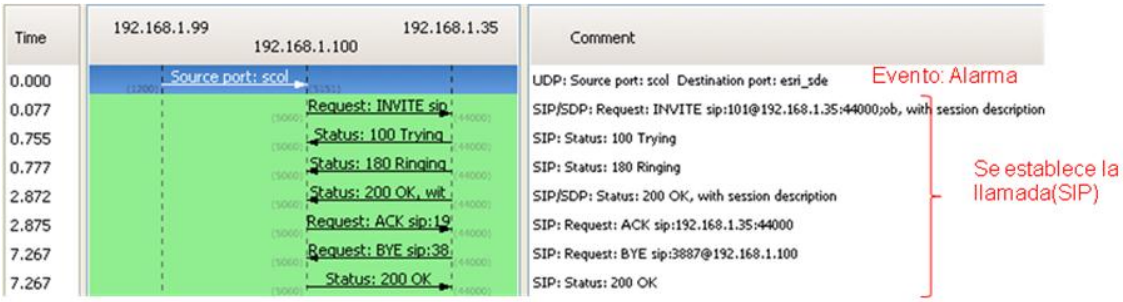

Figura 4.2 Flujo de tráfico de notificaciones por voz (Traza obtenida de *Wireshark*)

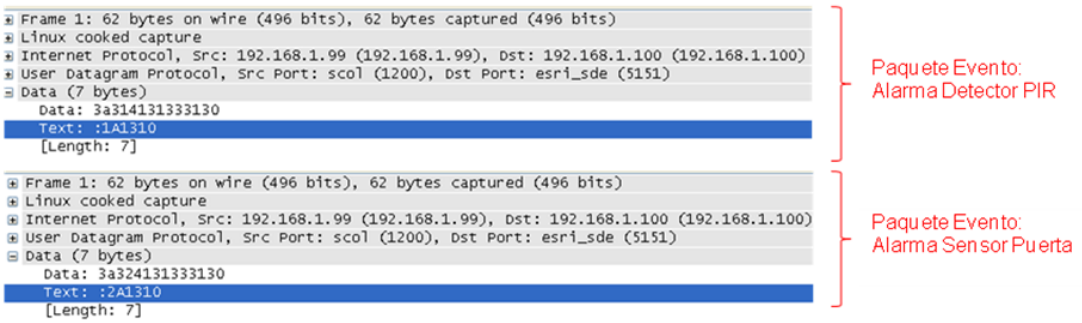

Figura 4.3 Paquete enviado por el Controlador de Equipos cuando se activa una alarma (Traza obtenida de *Wireshark*)

Las siguientes pruebas se realizaron en base al escenario de la figura 3.11. Considerando las IP públicas según la tabla 3.3.

Controlador de Equipos Ventanilla

IP Pública 190.235.19.211

Controlador de Equipos Abancay

IP Pública 190.238.143.214

Servidor Domótico

IP Pública 181.65.29.159

Teléfono VoIP (Extensión 101)

IP Pública 190.235.19.211(en mismo local de Ventanilla), 190.238.143.214(en mismo local de Abancay), 190.113.194.57 (Surco), 190.113.194.134(La Molina)

Notar que existen dos IPs diferentes para el Teléfono VoIP debido a que también se hicieron pruebas desde diferentes zonas geográficas, desde Surco (diferente a la zona del servidor) y desde La Molina. Por otro lado se observa en las pruebas que en algunos casos la IP pública del Controlador de Equipos es la misma que la del Teléfono VoIP, debido a que ambos pertenecen a la misma red, es decir ambos están en la misma zona geográfica y en la misma red local. Tener en cuenta que de las trazas adjuntas en el anexo, el servidor Domótico se distingue por su IP privada 192.168.1.100 debido a que las capturas se hicieron en este servidor. En la tabla 4.1 se observan todas las pruebas realizadas, según el escenario planteado en la figura 3.11. El detalle de estas trazas puede encontrarse en los anexos, en el campo “Traza” de esta tabla se puede apreciar su identificador. Las primeras pruebas realizadas solo en la red local mencionadas anteriormente se pueden encontrar en las trazas 29, 30,31. Se observa que en todas las pruebas todos los eventos enviados fueron recibidos correctamente, sin errores. Demostrando la confiabilidad del sistema.

Consumo del Procesador del Servidor Domótico

Para observar el rendimiento del procesador se realizaron capturas en la consola usando el comando Top. Se hicieron estas pruebas considerando 5 llamadas simultáneas (dos en espera, y tres activas) accediendo a la plataforma y el consumo del CPU utilizado por Asterisk fue de 0.7% y de memoria 1.8%. Las capturas de estas pruebas pueden encontrarse en el anexo.

Tabla 4.1 Pruebas realizadas con el servidor Domótico (Elaboración: Propia)

Traza	Controlador de Equipos	Teléfono Voip(Extensión 101)	NEE	NER	Dispositivo/Ubicación
1	190.238.143.214	190.113.194.57	3	3	Led 1 Abancay
2	190.238.143.214	190.113.194.57	8	8	Led 1 Abancay
3	190.238.143.214	190.113.194.57	2	2	Led 1 Abancay
4	190.238.143.214	190.238.143.214	2	2	Led 1 Abancay
5	190.235.19.211	190.235.19.211	1	1	Sensor de Movimiento Ventanilla
6	190.235.19.211	190.235.19.211	1	1	Sensor de Movimiento Ventanilla
7	190.235.19.211	190.113.194.134	1	1	Sensor de Movimiento Ventanilla
8	190.235.19.211	190.113.194.134	1	1	Sensor de Movimiento Ventanilla
9	190.235.19.211	190.113.194.134	1	1	Sensor de Movimiento Ventanilla
10	190.235.19.211	190.235.19.211	1	1	Sensor de Puerta Ventanilla
11	190.235.19.211	190.235.19.211	1	1	Sensor de Puerta Ventanilla
12	190.235.19.211	190.235.19.211	1	1	Sensor de Puerta Ventanilla
13	190.235.19.211	190.113.194.134	1	1	Sensor de Puerta Ventanilla
14	190.235.19.211	190.113.194.134	1	1	Sensor de Puerta Ventanilla
15	190.235.19.211	190.113.194.134	1	1	Sensor de Puerta Ventanilla
16	190.238.143.214	190.113.194.57	1	1	Sensor de Movimiento Abancay
17	190.238.143.214	190.113.194.57	1	1	Sensor de Movimiento Abancay
18	190.238.143.214	190.113.194.57	1	1	Sensor de Movimiento Abancay
19	190.238.143.214	190.113.194.57	1	1	Sensor de Puerta Abancay
20	190.238.143.214	190.113.194.57	1	1	Sensor de Puerta Abancay
21	190.238.143.214	190.113.194.57	1	1	Sensor de Puerta Abancay
22	190.235.19.211	190.235.19.211	2	2	Led1 Ventanilla
23	190.235.19.211	190.235.19.211	20	20	Led1 Ventanilla
24	190.235.19.211	190.235.19.211	7	7	Led1 Ventanilla
25	190.235.19.211	190.113.194.134	2	2	Led1 Ventanilla
26	190.235.19.211	190.113.194.134	3	3	Led1 Ventanilla
27	190.235.19.211	190.113.194.134	5	5	Led1 Ventanilla
28	192.168.1.99	192.168.1.35	7	7	Led1 Surco
29	192.168.1.99	192.168.1.35	3	3	Led1 Surco
30	192.168.1.99	192.168.1.35	1	1	Sensor de Movimiento Surco
31	192.168.1.99	192.168.1.35	1	1	Sensor de Puerta Surco

Tiempo de repuesta del Controlador de Equipos en la Red Local e Internet

Como se comentó en las pruebas realizadas en la Red local del servidor domótico, se observa en la figura 4.1 un tiempo de respuesta de 1 ms por parte Controlador de Equipos una vez que el Servidor domótico envió el evento. En el anexo se observa también pruebas realizadas utilizando el protocolo ICMP. El envío de estas notificaciones permitió también tener una noción del tiempo de repuesta del Controlador de Equipos. En promedio se obtuvo un tiempo de 1.34 ms. Cabe

resaltar que estas pruebas realizadas en la Red local son las que más se acercan al tiempo de respuesta del Controlador de Equipos, ya que solo existe un salto. En las pruebas realizadas enviando los paquetes por Internet existe mayor cantidad de saltos, por lo que el tiempo varía. Sin embargo, como se observan en las trazas (anexo) el tiempo sigue siendo bajo entre 20 y 48ms.

Para las notificaciones del Controlador de Equipos(Activación de alarmas), considerando según la figura 4.2 y las pruebas adjuntas al anexo, el tiempo entre que el servidor recibe el evento del Controlador de Equipos hasta que genera la llamada es de alrededor de 77 ms. Es decir cuando se active una alarma, Asterisk tardará menos de 80 ms en realizar una llamada telefónica de notificación. Un tiempo bastante aceptable para notificaciones en caso de emergencias. El tiempo en que el usuario reciba la llamada no se está considerando ya que no depende del funcionamiento del sistema implementado, sino de factores externos como cobertura de señal, si dispositivo está ocupado, o apagado, etc.

Pruebas con la Interfaz Web

Las pruebas con la interfaz web se hicieron utilizando un Smartphone (ver Figura 4.4), y una computadora portátil. Capturas y más fotos están adjuntas en el anexo.

Figura 4.4 Acceso Web mediante Smartphone

4.2 Análisis de costos y presupuesto del sistema a implementar

En la tabla 4.2 se pueden observar productos similares al implementado, es decir ofrecen interoperabilidad al usuario frente a un sistema domótico. La elección de

estos productos se basan en los requerimientos de esta tesis, si bien algunos de estos soportan diferente comunicación con el usuario y características adicionales, todos tienen el objetivo de darle a este un forma sencilla y remota de controlar el sistema. Cabe resaltar que cada uno de estos equipos es capaz de controlar dispositivos en diferentes zonas dentro de un rango limitado de distancia. Por lo tanto, para la tesis planteada se necesitaría dos de cualquiera de estos equipos (para Abancay y Ventanilla), de modo que el usuario pueda controlar remotamente las dos localidades. Si el usuario quisiera expandir su sistema a todos sus locales, necesitaría en total de 7 de estos equipos. Si consideramos el producto menos costoso (GSM22X a $363), el presupuesto necesario sería de $2541 considerando sólo los controladores (sin sensores, actuadores, instalación, gastos de importación, ni impuestos).

Tabla 4.2 Productos similares al sistema implementado (Elaboración: Propia)

Producto	Descripción	Precio
DD-5230	4 entradas digitales, 4 salidas relé 220V. Control y configuración por Mensajes SMS. [23]	$619
DD-6321	Enciende o apaga dispositivos a través de la red (LAN/WAN) ó vía TCP / IP (INTERNET). Es posible encender o apagar hasta ocho dispositivos [24]	$590
Nexho NT	Control de su instalación desde cualquier teléfono o dispositivo con conectividad Wi-Fi. Desde dentro de la vivienda o desde cualquier lugar con conexión a Internet. Conectividad con cualquier dispositivo Nexho. [25]	$479
GSM22X	Control y configuración por Mensajes SMS/2 Salidas (relé), Salida conexión domótica X10 (conectable a ref. X10XM10) 2 Entradas de alarma (por contacto libre de tensión)[26]	$363
DD-6390	8 Entradas de sensores, 8 Salidas relé/Control por Internet, soporta (WAN/LAN), HTTP, TCP/IP, DHCP, DDNS, WAP por GPRS / Servidor SMTP, alertas vía e-mail cuando se producen eventos, Compatible con IP Video [27]	$732

En la tabla 4.3 se detalla el presupuesto de implementación del Controlador de Equipos y en la tabla 4.4 considerando la implementación del servidor domótico; no se está incluyendo los costos de ingeniería (investigación, diseño, tiempo gastado, etc.) debido a que es un producto como los descrito en la tabla 4.2, y tiene que estar sujeto a una incremento dependiendo de lo que se quiera ganar en el mercado. Los costos de ingeniería se estiman alrededor de los $9000, debido al tiempo, creatividad e investigación puestos en esta tesis. Tampoco se están

considerando costos de sensores y actuadores, ya que el sistema en sí es un controlador que permite el acceso remoto. Cabe resaltar, sobre el presupuesto indicado en la tabla 4.4, que se está incluyendo el servidor domótico con las características similares al usado en esta tesis. Este precio es referencial obtenido en páginas web. Solo incluye la computadora (no mouse, monitor, ni teclado). Se debe tener en cuenta, según las pruebas realizadas y los requerimientos mínimos del servidor planteado en la sección 3.2.7 que las características indicadas en esta tabla son innecesarios, por lo que comprar un servidor con los requerimientos mínimos reduciría el presupuesto considerablemente.

Tabla 4.3 Presupuesto del Controlador de Equipos (Elaboración: Propia)

Componente	P.U(S/.)	P.T(S/.)
10 Resistencias	0,1	1
9 Condensadores	0,3	2,7
Atmega8L	8	8
Enc28j60	25	25
Conector RJ45 embobinado con 2 Leds	15	15
1 Led	0,2	0,2
1 Cristal de 25 MHz	3	3
1 Pulsador	0,4	0,4
1 Bornera	0,5	0,5
Conector	0,5	0,5
Costo de Tarjeta	14	14
Regulador LM2937-3.3	2,5	2,5
Ferrita	0,3	0,3
Transformador 220V/12V 1A	15	15
Precio Total		88,10

Tabla 4.4 Presupuesto del Servidor domótico (Elaboración: Propia)

Componente	Precio
X100P: 1 puerto FXO con conector RJ11. Tarjeta PCI(3.3V ó 5.5V)	$38.95
Servidor Domótico: Intel Core2duo 2.33GHZ/ 1 GB RAM/ 80 GB	$212
Total	$250.95

Si bien el servidor es un gasto adicional, y es el elemento más costoso no es necesario comprar uno nuevo si el usuario ya tiene una computadora disponible, ya que el sistema puede ser implementado en cualquier computadora con características similares o superiores y con sistema operativo Linux (en esta tesis

se planteó esta solución). Si el usuario no tiene el sistema operativo Linux instalado, y le resulta fastidioso tener dos sistemas operativos, tiene la alternativa de instalar una máquina virtual con Linux y los requerimientos mínimos necesarios para poder implementar el sistema. Además se está incluyendo una tarjeta PCI X100P, muy utilizada para servidores con Asterisk. Esta tarjeta permite conectar su puerto FXO al puerto FXS proporcionado por el proveedor telefónico. De esta manera le permite a Asterisk recibir y hacer llamadas desde y hacia la red Pública. Esta tarjeta no se consideró en la implementación de esta tesis debido a falta de tiempo y presupuesto. Así mismo, el objetivo de esta tesis es el funcionamiento en sí de la plataforma Asterisk con la arquitectura planteada. Por lo que también se consideró innecesario probar el funcionamiento de Asterisk con la red pública, ya que de por sí el propósito principal de Asterisk es este; además que la confiabilidad, eficacia y heterogeneidad de este propósito vienen respaldadas por grandes empresas de telecomunicaciones en los últimos 10 años. Entonces de acuerdo las tablas 4.3 y 4.4 el costo del sistema (incluyendo el servidor domótico) sería de $33.37(S/.88.10) + $250.95= $284.32. Este precio incluye un controlador de equipos y un servidor domótico. Considerando que es necesario el control de dos zonas geográficas es necesario un segundo controlador de equipos el costo total sería de $317.69, el cual puede reducirse considerablemente si se tiene disponible el servidor domótico y comprando los componentes al por mayor. En la figura 4.5 se hace una comparación de los diferentes productos similares con la tesis planteada. Se puede observar que a más zonas geográficas a controlar, la diferencia de costos es mayor, siendo el sistema planteado el más rentable. Los costos están en dólares, se ha considerado el tipo de cambio 2.64 para soles.

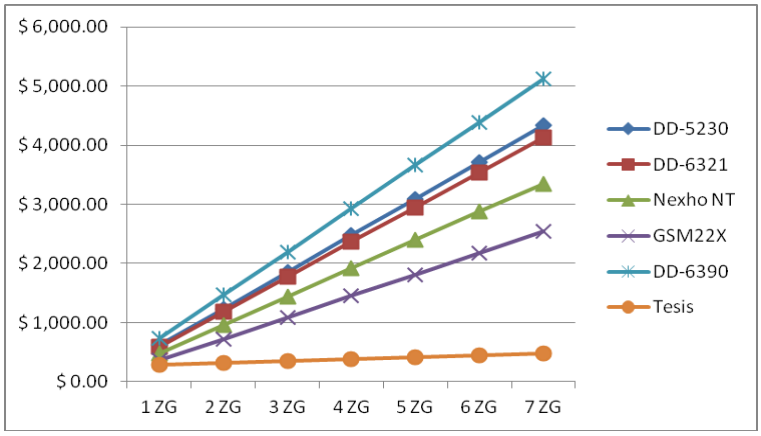

Figura 4.5 Comparación de costos con productos alternativos (ZG: Zona geográfica, Elaboración: Propia)

CONCLUSIONES

1. El módulo de control implementado con el microcontrolador Atmega8L permitió el control de dos actuadores y el monitoreo de un sensor. Además de poder agregar 13 dispositivos adicionales y la posibilidad de agregar un módulo Zigbee (mediante UART).

2. El uso del controlador ENC28J60 en el módulo de comunicaciones permitió al Controlador de Equipos la comunicación vía Internet o LAN. Permitiendo así eliminar cualquier limitante de distancia con el Servidor Domótico. Además, gracias a la arquitectura planteada, a la independencia entre el Módulo de Control y Comunicaciones en el Controlador de Equipos, y al estándar SPI que soporta el controlador ENC28j60 el sistema planteado es heterogéneo y escalable.

3. La implementación del Gestor de eventos mediante lenguaje de programación PHP basado en sockets y el mapeo de puertos en los router, permitió la comunicación por Internet o LAN entre el Servidor Domótico y los Controladores de Equipos.

4. El servidor IP PBX se implementó en el software libre Asterisk, permitiendo incorporar al sistema domótico a la red amplia de telefonía fija, celular y VoIP.

5. La implementación de la base de datos Modelo de área en MySQL permitió no solo integrar las tablas con el SID, sino también con el servidor WEB.

6. El uso de IVR y notificaciones por voz le permite al usuario controlar su sistema de una forma remota y confiable sin necesidad de comprar algún equipo adicional. Además, con la implementación del servidor Web se demuestra la gran variedad de comunicaciones que puede soportar el Servidor Domótico planteado.

7. Mediante las interfaces, se pudo controlar y recibir notificaciones de dos zonas geográficas diferentes, comunicándose desde distintos lugares de una manera eficiente y eficaz.

RECOMENDACIONES

1. Si se desea implementar el sistema planteado como un producto, debe considerarse en el presupuesto final el costo del chasis ya que no está incluido en esta tesis.

2. Para dispositivos ubicados lejos del Controlador de Equipos, debe considerarse añadir al diseño un módulo Zigbee para comunicaciones inalámbricas. Si bien no se consideró en la implementación, el módulo de control (Atmega8L) mediante comunicación UART puede comunicarse con un módulo Zigbee (por ejemplo Xbee Pro Series 2)

3. En las pruebas realizadas, el sistema se planteó con un servidor Intel Core2Duo 1.866GHz/1GB de Memoria RAM, ya que el usuario contaba con este servidor disponible; sin embargo, en caso no se tenga esta disponibilidad, para reducir costos de implementación debe considerarse realizar pruebas con un servidor con los requerimientos mínimos planteados en esta tesis.

4. Debe aprovecharse las comunicaciones por VoIP mediante el uso de la IP PBX. Se recomienda adquirir un teléfono IP para cada zona geográfica, de manera que el usuario pueda comunicarse sin costo alguno con cada uno de sus locales, reduciendo así costos de telefonía fija o celular.

5. En caso se registren una gran cantidad de usuarios, por ende mayor cantidad de llamadas simultáneas, debe considerarse separar los bloques de la arquitectura (gestor de eventos, SID, Modelo de área) en servidores diferentes.

6. Es recomendable que el servidor domótico utilice una IP fija, para evitar que el Controlador de Equipos por cada envío de paquetes consulte la IP a un servidor DNS, de esta manera la respuesta del Controlador será más rápida.

BIBLIOGRAFÍA

[1] D. Bonino F., Corno F., Razzak. 2010. Mobile Interaction with Smart Environments through Linked Data

[2] Mafalda Seixas, João Palma. Remote Alarm And Command System For Residential Domotics Trough Gsm – Sms

[3] J. Picerno, K. Tenzer. 2010. API de alto nivel genérica para desarrollo de aplicaciones de domótica.

[4] A. E. Martínez, R. Cabello, F. J. Gómez, J. Martínez. 2003. A Solution for the Integration of Domestic Devices on Network Management Platforms

[5] Cisco – Voice Over IP: Per Call Bandwidth Consumption. Consulta 20 Mayo 2012.
<www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml>

[6] S. Soucek, G. Russ, C. Tamarit. 2001. The Smart Kitchen Project -An Application of Fieldbus Technology to Domotics.

[7] J. V. Meggelen, J. Smith, L. Madsen. 2007. Asterisk: The Future of Telephony. Segunda Edición. O'Reilly Media

[8] Domodesk - A fondo: Zigbee. Consulta 8 Junio 2012.
<http://www.domodesk.com/content.aspx?co=97&t=21&c=47>

[9] P. Pellegrino, D. Bonino, and F. Corno. 2006. Domotic house gateway.

[10] Marco Aiello. 2006. The role of web services at home.

[11] Edgar Landívar. 2008. Comunicaciones Unificadas con Elastix Volumen 1. Primera Edición. GNU Free Documentation License, Versión 1.3.

[12] Alfredo Certain. Asterisk. 2005 Comunicaciones de Código Abierto. Gecko Networks.

[13] Webestilo - Introducción a MySQL. Consulta 15 Febrero 2012
<http://www.webestilo.com/mysql/intro.phtml>

[14] Atmgel – Atmega8L Datasheet Download. Consulta 16 Noviembre 2011.
<http://www.atmel.com/dyn/resources/prod_documents/doc2486.pdf>

[15] Asociación 4G Américas. 2010. Textos al 9-1-1: Análisis del diseño y limitaciones de SMS

[16] W. Chamorro, D. Guerrón. 2008. Diseño e implemetanción del control de acceso y seguridad del laboratorio de instrumentación utilizando el protocolo X-10

[17] 3CX – 10 reasons to switch to an IP PBX. Consulta 20 de Febrero 2012
<http://www.3cx.com/PBX/pbx-benefits-wp.html>

[18] Wikipedia- Centos. Consulta 20 Febrero 2012
< http://es.wikipedia.org/wiki/CentOS>

[19] Savannah - Download. Consulta 1 Noviembre 2011.
<http://savannah.nongnu.org/projects/avr-libc/>

[20] Ethershield - Download. Consulta 1 Noviembre 2011.
< http://ethershield.thiseldo.co.uk/index.html>

[21] Microchip – Enc28j60 Datasheet Download. Consulta 16 Noviembre 2011.
<http://ww1.microchip.com/downloads/en/devicedoc/39662a.pdf>

[22] Midcom – Download. Consulta 16 Noviembre 2011.
<http://products.midcom-inc.com/Products/Catalog/LANCatalog.pdf>

[23] Domodesk - DD-5230 SMS. Consulta 20 Mayo 2012.
<http://www.domodesk.com/product/9/14/12/1/SMS_Control_ADVANCE_USB_SOFTWARE_(ENCENDIDO_ALERTA_REMOTO_por_M%C3%93VIL).htm>

[24] Domodesk - DD-6321. Consulta 20 Mayo 2012.
<http://www.domodesk.com/product/58/14/52/1/CONTROLADOR_IP_POWER_ON_OFF_8_SALIDAS_(_ENCENDIDO_APAGADO_INTERNET_).htm>

[25] Nexho - Nexho NT. Consulta 20 Mayo 2012.
<http://www.nexho.com/market/product.php?id_product=15>

[26] Domodesk - CCGSM22X. Consulta 20 Mayo 2012.
<http://www.domotia.com/tienda/product.php?id_product=19>

[27] Domodesk - DD-6390. Consulta 20 Mayo 2012.
<http://www.domodesk.com/product/22/14/37/1/CONTROL_IP_por_INTERNET_RACK_8_entadas_Digitales_8_salidas_Rel%C3%A9.htm>

[28] Detector PIR LC -100 PI – Download. Consulta 18 Julio de 2012
< http://www.hestia-france.com/downloads/Notice_LC100PI-1.pdf >

[29] Contacto magnetic SM-217Q- Download. Consulta 18 Julio de 2012
<http://www.seco-larm.com/pdfs/SM-x17Q_PI_P0908.pdf>