



REPÚBLICA DEL ECUADOR

Escuela Politécnica Nacional

" E S C I E N T I A H O M I N I S S A L U S "

La versión digital de esta tesis está protegida por la Ley de Derechos de Autor del Ecuador.

Los derechos de autor han sido entregados a la "ESCUELA POLITÉCNICA NACIONAL" bajo el libre consentimiento del (los) autor(es).

Al consultar esta tesis deberá acatar con las disposiciones de la Ley y las siguientes condiciones de uso:

- Cualquier uso que haga de estos documentos o imágenes deben ser sólo para efectos de investigación o estudio académico, y usted no puede ponerlos a disposición de otra persona.
- Usted deberá reconocer el derecho del autor a ser identificado y citado como el autor de esta tesis.
- No se podrá obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.

El Libre Acceso a la información, promueve el reconocimiento de la originalidad de las ideas de los demás, respetando las normas de presentación y de citación de autores con el fin de no incurrir en actos ilegítimos de copiar y hacer pasar como propias las creaciones de terceras personas.

Respeto hacia sí mismo y hacia los demás.

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

**ESTUDIO E IMPLEMENTACIÓN DE UN PROTOTIPO DE UNA
CENTRAL DOMÓTICA VOIP BASADOS EN LA DISTRIBUCIÓN
DEL SISTEMA OPERATIVO GNU/LINUX “TRIXBOX” USANDO LA
TECNOLOGÍA X10, PARA OFRECER SEGURIDAD Y CONFORT
EN EL HOGAR.**

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN
ELECTRÓNICA Y TELECOMUNICACIONES**

VLADIMIR STALIN ACURIO MOREJÓN
stalin.acurio@gmail.com

MAYRA ALEXANDRA CRUZ BAÑO
cruz_mayalexa@hotmail.com

DIRECTOR: ING. PABLO EFRAÍNSALINAS LEÓN
psalinas@pcservicios.com.ec

Quito, Septiembre 2011

DECLARACIÓN

Nosotros, Vladimir Stalin Acurio Morejón, Mayra Alexandra Cruz Baño, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Vladimir Stalin Acurio Morejón

Mayra Alexandra Cruz Baño

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Vladimir Stalin Acurio Morejón y Mayra Alexandra Cruz Baño, bajo mi supervisión.

ING. Pablo Salinas
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Agradezco a mi Madre por todo su apoyo incondicional y sacrificio a lo largo de mi carrera, al igual que a mis hermanos por su apoyo, compañía y ánimo en todas las diferentes etapas y circunstancias de mi vida. Gracias por su paciencia.

A todos mis amigos, mil gracias por brindarme su amistad y confianza y por los momentos que hemos pasado juntos.

Vladimir Stalin Acurio Morejón

AGRADECIMIENTO

Quiero agradecer a Dios , a mi madre Judith, porque sé que puedo contar contigo incondicionalmente, por tus palabras de apoyo cuando más las necesitaba, por aquellas noches que te desvelabas para acompañarme mientras estudiaba, por tu amor, por todos los momentos de felicidad que vivimos juntas y a mi padre Vicente por enseñarme el valor de la perseverancia, enseñarme a ser fuerte y luchadora, gracias a los dos por su apoyo y consejo , hoy he llegado a realizar la más grande de mis metas, la cual es la herencia más valiosa que me han entregado.

Aunque no encuentre la forma de agradecerles por toda una vida de sacrificio y esfuerzo, quiero que sientan que este logro alcanzado también es de ustedes y que la fuerza que me ayudó a conseguirlo fue su amor y su fé en mí.

Gracias a ti amor Carlos por estar ahora a mi lado, por tu comprensión y tolerancia, por brindarme lo mejor de ti, por saber escuchar y por creer en mí.

A todos mis amigos Vladi, Germán, San, Carito, Bolo, Guillo, Dieguito, Vivilu, Andrés, Cabo, George, Charas, Diana, Pao y Olí gracias por todos los momentos que pasamos juntos, noches de estudio y de farras, por su amistad sincera y por todos los recuerdos que llevaré en mi corazón.

A mis amigos de Consejo Politécnico con los cuales trabajamos por una poli mejor y justa donde estudiantes, trabajadores y maestros tengamos iguales derechos.

Finalmente a mis maestros porque fueron un pilar importante durante mi permanencia en la EPN, y a todos los que influyeron de alguna manera en mi vida y aportaron de cierta forma para realizar este proyecto.

Con Amor

Mayra Alexandra Cruz Baño

DEDICATORIA

En especial a mi Madre por haberme enseñado a valorar lo que realmente es importante en la vida y mostrarme como ser mejor persona, dando lo mejor de mí para alcanzar las metas de la vida.

A mis hermanos, por darme siempre su apoyo en los momentos que en que se necesitaba una palmadita en el hombro para seguir adelante aún cuando el camino quizá no estaba tan claro.

A mi novia por darme su apoyo y su inspiración para ser mejor cada día.

Vladimir Stalin Acurio Morejón

DEDICATORIA

Dedico este proyecto a mis padres Judith y Vicente, sin ustedes, sin su apoyo y sin su confianza, no lo hubiera logrado, gracias por apoyarme, gracias por creer en mí, son mi mayor orgullo y los amo tanto.

A ti amor Carlos por estar junto a mí y por darme la fuerza y el apoyo para culminar este sueño, te amo.

Mayra Alexandra Cruz Baño

ÍNDICE DE CONTENIDOS

RESUMEN	X
PRESENTACIÓN.....	XI
CAPÍTULO 1	1
1.1 INTRODUCCIÓN	1
1.2 DOMÓTICA	2
1.2.1 DEFINICIÓN E HISTORIA	2
1.2.2 ÁREAS Y OBJETIVOS DE LA DOMÓTICA:	2
1.2.3 BENEFICIOS DE LA DOMOTICA	3
1.2.4 DESCRIPCIÓN DE ELEMENTOS QUE INTEGRAN EL SISTEMA DOMÓTICO	5
1.2.4.1 Módulos.....	5
1.2.4.2 Medios de interconexión.....	5
1.2.4.3 Software para sistemas domóticos	6
1.2.5 ARQUITECTURA DOMÓTICA.....	6
1.2.6 PROTOCOLOS	7
1.2.6.1 Protocolos abiertos.....	7
1.2.6.1.1 KNX	7
1.2.6.1.2 X10	7
1.2.6.2 Protocolos propietarios o cerrados.....	8
1.2.6.2.1 LonWorks	8
1.2.7 X10.....	8
1.2.7.1 Introducción.....	8
1.2.7.2 Protocolo X10.....	9
1.2.7.2.1 Funcionamiento del protocolo X10	9
1.2.7.2.2 Trama X10.....	11
1.2.7.3 Ventajas de la tecnología X10	15
1.2.7.4 Clasificación de los módulos X10.....	16
1.2.7.5 Arquitectura del sistema X10.....	17
1.2.7.6 Productos X10	19
1.2.7.6.1 CM11	19
1.2.7.6.2 CM17A	19
1.2.7.6.3 LM465 Modulo actuador de lámpara X10.....	20

1.2.7.6.4 TM751 Módulo Transceptor X10	20
1.2.7.6.5 MS16A sensor de movimiento.....	21
1.3 GNU/LINUX.....	21
1.3.1 VOIP	22
1.3.1.1 Definición VoIP	22
1.3.1.2 Aplicaciones de VoIP.....	23
1.3.1.3 Señalización de VOIP y protocolos de transporte de voz.....	24
1.3.1.3.1 Estándar H.323	24
1.3.1.3.2 Sip (protocolo de inicio de sesiones)	25
1.3.1.3.3 Comparación entre H.323 y SIP	29
1.3.1.3.4 Calidad de servicio (quality of service, QOS)	30
1.3.1.3.5 Ancho de banda	31
1.3.1.3.6 Porcentaje de pérdida de paquetes.....	32
1.3.1.3.7 Retardo o latencia	32
1.3.1.3.8 JITTER	32
1.3.1.4 Ventajas y desventajas de VOIP	33
1.3.1.5 Seguridad en redes IP.....	33
1.3.1.6 Filtrado de paquetes IP	34
1.3.1.7 Traslado de direcciones de red (NAT)	34
1.3.1.8 Arquitectura IP seguridad.....	35
1.3.1.9 Firewall.....	35
1.3.2 TRIXBOX DISTRIBUCIÓN LINUX PARA CENTRAL TELEFÓNICA VoIP...39	
1.3.2.1 DEFINICIÓN.....	39
1.3.2.2 Componentes principales de TRIXBOX	40
1.3.2.2.1 CentOS.....	40
1.3.2.2.2 ASTERISK.....	40
1.3.2.2.3 FreePBX.....	43
1.3.2.2.4 Flash operator panel (FOP)	45
1.3.2.3 Hardware y software compatible con Asterisk en Trixbox	45
1.3.3 SOFTWARE COMPATIBLE CON LA TECNOLOGÍA X-10	51
1.3.3.1 HEYU	51
1.3.3.2 MOTION	52

CAPÍTULO 2	55
2.1 INTRODUCCIÓN	55
2.2 SITUACIÓN ACTUAL DE LA DOMÓTICA	55
2.3 ESTUDIO PARA LA VIABILIDAD DEL PROTOTIPO DE LA CENTRAL DOMÓTICA VoIP	56
2.3.1 ESTUDIO DEL DESARROLLO TECNOLÓGICO EN EL ECUADOR.....	56
2.3.2 ANÁLISIS DEL CABLEADO ELÉCTRICO EN EDIFICACIONES	59
2.3.3 EQUIPOS (FACILIDAD DE USO, COSTOS Y BENEFICIOS).	59
2.3.4 ANÁLISIS DE MERCADO (ENCUESTA)	60
CAPÍTULO 3	66
3.1 INTRODUCCIÓN	66
3.2 DIMENSIONAMIENTO DE HARDWARE DE VoIP	66
3.3 REQUISITOS DE HARDWARE PARA LA CENTRAL DOMÓTICA VoIP.....	66
3.3.1 SERVIDOR.....	66
3.3.2 TARJETA PCI	67
3.3.3 MÓDULOS X10.....	67
3.3.4 CÁMARA WEB.....	68
3.4 CARACTERÍSTICAS DE SOFTWARE.....	68
3.4.1 SISTEMA OPERATIVO.....	68
3.4.2 SOFTPHONES.....	68
3.4.3 HEYU	69
3.4.4 MOTION.....	69
3.5 PROGRAMAS EN PHP.....	69
3.5.1 COMANDOS AGI Y LECTURA DE ENTRADA DE ASTERISK	70
3.6 CONSTRUCCIÓN DE SCRIPTS.....	70
3.6.1 SCRIPTS DE CONTROL	71
3.6.1.1 Bloque IVR1	71
3.6.1.2 Bloque IVR2	72
3.6.1.3 Script monitoreo	72
3.6.1.4 Script seguridad	74
3.6.1.4.1 Programa en php para activar seguridad	76
3.6.1.4.2 Programa en php para llamada de emergencia	77

3.6.1.5 Script usomotion.....	78
3.6.1.6 Bloque IVR3	78
3.6.1.6.1 Programa en php para activar módulos X10	79
3.6.1.6.2 Programa php para desactivar módulos X10	80
3.6.1.6.3 Programa php para verificar el estado de módulos X10.....	81
CAPÍTULO 4.	82
4.1 IMPLEMENTACIÓN DEL PROTOTIPO	82
4.1.1 CONFIGURACIÓN DE LA CENTRAL VoIP	84
4.2 PRUEBAS Y RESULTADOS.....	90
4.2.1 PRUEBAS DE FUNCIONAMIENTO DE MONITOREO Y CONFORT.....	91
4.2.2 PRUEBAS DE FUNCIONAMIENTO DE SEGURIDAD.....	92
4.2.3 PRUEBAS DE FUNCIONAMIENTO DE VIDEO SEGURIDAD	95
4.3 COSTOS DE IMPLEMENTACIÓN Y DISEÑO	98
4.4 ANÁLISIS DE COSTOS	99
CAPÍTULO 5.	100
5.1 CONCLUSIONES.....	100
5.2 RECOMENDACIONES	102
BIBLIOGRAFÍA	104
ANEXO A: FORMATO DE LA ENCUESTA REALIZADA	I
A.1 FORMATO DE ENCUESTA	II
A.2 RESULTADOS DE LA ENCUESTA	V
ANEXO B: ESPECIFICACIONES DE HARDWARE PARA UNA CENTRAL DOMÓTICA VOIP	XII
B.1 CARACTERÍSTICAS DE MÓDULOS FXO Y FXS	XIII
B.2 CARACTERÍSTICAS DE LA TARJETA PCI FAX MODEM AMBIENT 3200, X100P, TDM400P	XIV
B.3 CARACTERÍSTICAS DE LOS MÓDULOS X10 Y CÁMARA WEB.....	XIVIII

ANEXO C: INSTALACIÓN DE SOFTWARE PARA EL DISEÑO DE UNA CENTRAL DOMÓTICA VoIP BASADA EN TRIXBOX	XXIV
C.1. OBTENCIÓN DE TRIXBOX.....	XXV
C.2. INSTALACIÓN DE TRIXBOX	XXVI
C.3. CONFIGURACIONES INICIALES.....	XXXI
C.4. INSTALACIÓN DE ZOIPER	XXXIV
C.5. INSTALACIÓN DEL SOFTWARE HEYU	XXXIVII
C.6. INSTALACIÓN DEL SOFTWARE MOTION	XXXIVIII
ANEXO D: SCRIPTS.....	XLII
D.1. SCRIPT MONITOREO	XLIII
D.2. SCRIPT SEGURIDAD	XLV
D.3. SCRIPT USOMOTION	XLVII

ÍNDICE DE FIGURAS

CAPÍTULO 1

Figura (1.1) Ejemplo de una red domótica en el hogar	4
Figura (1.2) Muestra la relación entre los pulsos y el pulso cero de la corriente alterna.	10
Figura (1.3) código X-10.....	10
Figura (1.4) ventana del receptor en 0.6ms	11
Figura (1.5). Representación de un bit en el protocolo X10	11
Figura (1.6). Código de inicio	12
Figura (1.7) Código de casa	12
Figura (1.8) Código de número	13
Figura (1.9) Envío de una trama con redundancia	13
Figura (1.10) Código de comando	14
Figura (1.11) Ciclos de espera entre transmisores	14
Figura (1.12) Transmisión completa de la trama X10.....	15
Figura (1.13): Código de comienzo + código de casa	16
Figura (1.14) Arquitectura del sistema X10.....	18
Figura (1.15) CM11	19
Figura (1.16) FireCracker CM17A	20
Figura (1.17) Módulo actuador de lámpara LM465	20
Figura (1.18) Módulo de transceptor TM751	20
Figura (1.19) Sensor de movimiento MS16A	21
Figura (1. 20) Proceso del transporte de VoIP	23
Figura (1.21) Red SIP	28
Figura (1.22) Comunicación SIP entre terminales	28
Figura (1.23) Comunicación del servidor proxy SIP entre terminales	28
Figura (1.24) Servidor de redirección SIP entre terminales	29
Figura (1.25) Logo de la distribución TRIXBOX	39
Figura (1.26) Muestra una tarjeta Digium 8 puertos	46
Figura (1.27) Muestra el módulo FXS	47
Figura (1.28) Muestra de un módulo FXO	48
Figura (1.29) Teléfono IP	49
Figura (1.30) Softphone XTEN, EXPRESS TALK	50

Figura (1.31) Adaptador ATA	50
Figura (1.32): logo HEYU	51
Figura (1.33): logo MOTION	52
CAPÍTULO 2	
Figura (2.1.): Cuadro estadístico general del acceso internet en el Ecuador	56
Figura (2.2.): Cuadro estadístico del área urbana del acceso internet en el Ecuador	57
Figura (2.3.): Cuadro estadístico del acceso internet del área rural en el Ecuador	57
Figura (2.4.): Cuadro estadístico general sobre la tenencia de computadores en el Ecuador	58
Figura (2.5.): Resultados de la encuesta pregunta 1.....	62
Figura (2.6.): Resultados de la encuesta pregunta 2.....	62
Figura (2.7.): Resultados de la encuesta pregunta 3.....	63
Figura (2.8.): Resultados de la encuesta pregunta 5.....	63
Figura (2.9.): Resultados de la encuesta pregunta 8.....	63
Figura (2.10.): Resultados de la encuesta pregunta 9.....	64
Figura (2.11.): Resultados de la encuesta pregunta 9 parte 2	64
Figura (2.12.): Resultados de la encuesta pregunta 10.....	64
Figura (2.13.): Resultados de la encuesta pregunta 10 resultados	64
CAPÍTULO 3	
Figura (3.1) Distribución de los IVR por bloques	71
Figura (3.2) Diagrama de flujo del script monitoreo	73
Figura (3.3) Diagrama de flujo del script seguridad.....	75
Figura (3.4) Diagrama de flujo del programa seguridadactiva_rev2.php.....	76
Figura (3.5) Diagrama de flujo del programa llamadapolicia_rev2.php	77
Figura (3.6) Diagrama de flujo del script Usomotion	78
Figura (3.7) Diagrama de flujo del programa onx10_rev1.php	79
Figura (3.8) Diagrama de flujo del programa offx10_rev1.php	80
Figura (3.9) Diagrama de flujo del programa stadox10_rev1.php	81
CAPÍTULO 4	
Figura (4.1) Configuración de la troncal zap.....	84
Figura (4.2) Configuración de la troncal SIP	85
Figura (4.3) Configuración de la troncal SIP.....	85

Figura (4.4) Configuración de una extensión SIP	86
Figura (4.5) Configuración de una extensión SIP	86
Figura (4.6) Configuración de rutas entrantes	87
Figura (4.7) Configuración de rutas entrantes	87
Figura (4.8) Configuración de rutas salientes	88
Figura (4.9) Configuración del IVR1	89
Figura (4.10) Configuración del IVR2	89
Figura (4.11) Configuración del IVR3	90
Figura (4.12) Inicio del script de monitoreo	91
Figura (4.13) Representación del acceso a las opciones de confort y seguridad .	92
Figura (4.14) Inicio del script de seguridad	92
Figura (4.15) Activación del informe de la violación al sistema de seguridad	93
Figura (4.16) Representación de la llamada de alarma de la central al usuario ...	93
Figura (4.17) Llamada de emergencia (policía, bomberos)	94
Figura (4.18) Pantalla Flash Operator Panel de pruebas de llamada realizadas .	95
Figura (4.19) Representación del uso de la cámara web para monitoreo desde el internet	95
Figura (4.20) Visualización de la prueba del uso de la cámara web	96
Figura (4.21) Captura de imagen computador 1	97
Figura (4.22) Captura de imagen computador 2	97

ÍNDICE DE TABLAS

CAPÍTULO 1

Tabla (1.1) Comparación entre protocolos H.323 y SIP	30
Tabla (1.2) Tabla de códecs de audio.	31
Tabla (1.3) representa los porcentajes de calidad en el audio para la VoIP.	32
Tabla (1.4) Organización de archivos del FREEPBX	45
Tabla (1.5) Tarjetas Digium utilizadas en servidores VOIP	48

CAPÍTULO 2

CAPÍTULO 3

Tabla (3.1) Softphones (protocolo y sistema operativo)	68
Tabla (3.2) Comandos usados en Heyu.....	69
Tabla (3.3) Códigos para comandar los dispositivos X10	79

CAPÍTULO 4

Tabla (4.1) Descripción de hardware usado en el prototipo	83
Tabla (4.2) Descripción de software usado en el prototipo	83
Tabla (4.3) Precios de los materiales utilizados para el prototipo	99
Tabla (4.4) Precios total del prototipo.....	99

RESUMEN

El presente proyecto tiene como fin diseñar una central domótica VoIP, basándose en el software libre de GNU/Linux Trixbox y utilizando los módulos X10 para brindar seguridad y confort en el hogar, aprovechando las características y beneficios de una central VoIP se puede acceder a las opciones domóticas de seguridad y confort.

Para esto, en el primer capítulo se da una introducción, explicación de conceptos de domótica y VoIP, protocolo de comunicación X10, funcionamiento de los módulos X10, componentes del software libre Trixbox que permiten el desarrollo del presente proyecto.

En el segundo capítulo se realiza un análisis de la situación actual y viabilidad de la implementación de la central domótica VoIP, a través del análisis de estudios del desarrollo tecnológico en el Ecuador, y por medio de una encuesta efectuada a personas profesionales afines al área para conocer el grado de aceptación de la central domótica VoIP, la encuesta se realizó vía internet a través de la herramienta proporcionada por gmail, donde fue necesario la creación de un producto ficticio llamado EASYHOME.

Siguiendo con el proyecto, en el capítulo tres se detalla el dimensionamiento, requisitos del hardware y software para la central domótica VoIP, también define el desarrollo y funcionamiento de los scripts de control de los módulos X10 utilizando las aplicaciones de Asterisk, y mediante programas en php se utiliza las respuestas interactivas de voz para que el usuario pueda recurrir a las opciones de seguridad y confort mediante una llamada telefónica.

El capítulo cuatro trata sobre la configuración de los parámetros básicos que permiten al usuario acceder a la central domótica VoIP mediante una llamada telefónica desde la PSTN puede ingresar a las opciones de seguridad y confort, además contiene las pruebas de funcionamiento y análisis de costo del prototipo.

Finalmente se da un conjunto de conclusiones y recomendaciones recopiladas en transcurso de las diferentes etapas del proyecto.

PRESENTACIÓN

La domótica se consolida como parte fundamental de un sector en plena transformación como es el de la construcción. La automatización de determinados elementos del hogar es algo que viene haciéndose desde mucho tiempo atrás generando comodidad y seguridad para los usuarios, actualmente existen varias tecnologías domóticas, X10 es la tecnología más antigua que aún permanece en el mercado caracterizándose por su protocolo de comunicación basado en la transmisión de información por medio de la línea eléctrica.

Las comunicaciones en Internet han proporcionado ayuda al desarrollo de la domótica. Hoy en día, el amplio despliegue de las redes de acceso de banda ancha, sumada a la optimización de los mecanismos de compresión y transmisión, abre la posibilidad de ofertar servicios de voz y video en tiempo real. En este entorno también se desarrolla la voz sobre IP siendo aplicada principalmente en centrales telefónicas.

CAPÍTULO 1. FUNDAMENTOS TEÓRICOS

1.1 INTRODUCCIÓN

La rápida evolución tecnológica de la electrónica e informática, ha inundado nuestro entorno con televisores, teléfonos, equipos de fax, módem, redes y sistemas informáticos tanto en oficinas como en viviendas. Hasta los electrodomésticos están experimentando una vertiginosa evolución, hoy en día los fabricantes ofrecen frigoríficos inteligentes capaces de hacer telefónicamente pedidos o indicarnos que al regresar de la oficina hagamos determinadas compras. Este desarrollo ha generado que el confort y la seguridad en los hogares se los pueda ver desde un punto tecnológico, la domótica y la VoIP (voz sobre protocolo IP) han dado soluciones a bajo costo a estas necesidades. Los sistemas domóticos actuales integran automatización, informática y nuevas tecnologías de la información. Las tecnologías actuales, aplicadas a las viviendas como: sistemas de climatización, juegos de luces, persianas, gas, red telefónica, seguridad e incluso sistemas informáticos requieren un esmerado control. Hasta el momento, en un edificio todos los sistemas eran independientes, hoy la domótica ofrece soluciones que integran y relacionan entre sí dichos elementos suponiendo una clara ventaja para el usuario.

La VoIP ha estado presente por mucho tiempo en el mercado, pero la aparición de nuevos e innovadores servicios en esta tecnología han hecho realidad que las comunicaciones a través de redes de datos sean más eficientes y efectivas. Las herramientas y servicios utilizados en la VoIP tienen la ventaja de utilizar estándares que brindan soluciones flexibles y escalables, dejando a libertad de ejecutar, modificar, estudiar y mejorar las aplicaciones que son realizadas con software libre.

Como es natural, aspiramos a una mejor calidad de vida y parece lógico que esa aspiración se refleje en nuestro propio entorno empezando por el más importante y cercano: el hogar, al que todos nos esforzamos en dotar de mayor confort y comodidad, esperando disfrutar de un ambiente protector para nuestra familia.

1.2 DOMÓTICA

1.2.1 DEFINICIÓN E HISTORIA

La automatización del hogar y las tecnologías empleadas en este objetivo se conocen como domótica. En si la domótica es el término que define la incorporación de elementos que permiten el control y gestión de un hogar, aumentando el bienestar y la seguridad de sus habitantes, y racionalizando los consumos de energía, agua, teléfono, etc.

En Francia se acuñó la palabra "Domotique". De hecho, la enciclopedia Larousse definía en 1988 el término domótica como el siguiente: "el concepto de vivienda que integra todos los automatismos en materia de seguridad, gestión de la energía, comunicaciones, etc.". Es decir, el objetivo es asegurar al propietario del hogar un aumento de confort, seguridad, ahorro energético y las facilidades de comunicación. La evolución hacia el concepto de Domótica proviene de la integración de dos conceptos, los sistemas de gestión y los sistemas de control de edificios. Los sistemas de gestión de edificios dirigen acciones por software, proporcionando informes detallados de consumos de energía y ahorros, en cambio los sistemas de control están enfocados más hacia el control de los dispositivos eléctricos. Ambos sistemas son totalmente complementarios, juntos formarían el "Edificio Inteligente" completo, llegando a formar lo que hoy es el concepto de domótica.

1.2.2 ÁREAS Y OBJETIVOS DE LA DOMÓTICA:

Las principales áreas y objetivos de esta tecnología son:

- **Automatización y control:** la domótica nos permite abrir, cerrar, apagar, encender, regular dispositivos y actividades domésticas (iluminación, climatización, persianas, toldos, puertas, ventanas, cerraduras, riego, electrodomésticos, suministro de agua, gas, electricidad, etc.).
- **Seguridad:** Vigilancia automática de bienes mediante alarmas de intrusión, cámaras de vigilancia, alarmas personales, alarmas de incendio, humo, agua, gas, fallo de suministro eléctrico, etc.

- **Comunicaciones:** Transmisión de voz y datos, incluyendo textos, imágenes, sonidos con redes locales (LAN) compartiendo acceso a Internet.
- **Ocio y tiempo libre:** Descansar y divertirse con radio, televisión, cine en casa, videojuegos, captura, tratamiento y distribución de imágenes fijas (foto) y dinámicas (vídeo) y de sonido (música) dentro y fuera de la casa, a través de Internet.
- **Monitorización de salud:** Actuar en la sanidad mediante asistencia sanitaria, consultoría sobre alimentación y dieta, telecontrol y alarmas de salud, medicina monitorizada, cuidado médico.
- **Compra:** Compra y venta desde la casa mediante la telecompra, televenta.
- **Finanzas:** Gestión del dinero y las cuentas bancarias mediante la telebanca, consultoría financiera.
- **Aprendizaje:** Aprender mediante la tele-enseñanza, cursos a distancia.
- **Lecturas y varios:** Búsqueda y procesamiento de otra información: Museos, bibliotecas, libros, periódicos, información meteorológica, jurídica, fiscal, etc.

Otros: Todas las posibles ideas que la creatividad y la innovación puedan aportar. Lo indicado hasta aquí es sólo una muestra del actual estado de conocimiento y progreso de la domótica.

1.2.3 BENEFICIOS DE LA DOMÓTICA

La domótica permite en la vivienda tradicional la posibilidad de controlar y gestionar de forma eficiente los dispositivos eléctricos (Sistemas de alarma, TV, teléfono, cocina, refrigerador, etc), mediante un sistema de gestión inteligente, con el objetivo de permitir una mejor calidad de vida al propietario de dicha vivienda.

Entre los beneficios que la domótica brinda al usuario están:

- **Control remoto en el interior de la vivienda:**

A través de un sistema de comunicación entre los distintos dispositivos de la vivienda (mando a distancia, bus de comunicación, etc.), reduce la necesidad de

moverse dentro del hogar, siendo un beneficio importante en el caso de personas de la tercera edad o minusválidos.

- **Control remoto fuera de la vivienda:**

El usuario puede aprovechar mejor su tiempo, ya que puede realizar tareas domésticas fuera del hogar a través del control remoto externo. Por ejemplo: la posibilidad de activar la cocina desde el exterior de su vivienda, implica que previa a su llegada puede preparar sus alimentos.

- **Programación de eventos:**

Los dispositivos de la vivienda pueden ser programados para realizar ciertas funciones con sólo tocar un botón, generando un aumento del confort y un ahorro de tiempo.

- **Acceso a servicios externos:**

El acceso a servicios de información, telecompra, telebanco, etc, es un beneficio de gran utilidad, ya que producen un ahorro de tiempo.

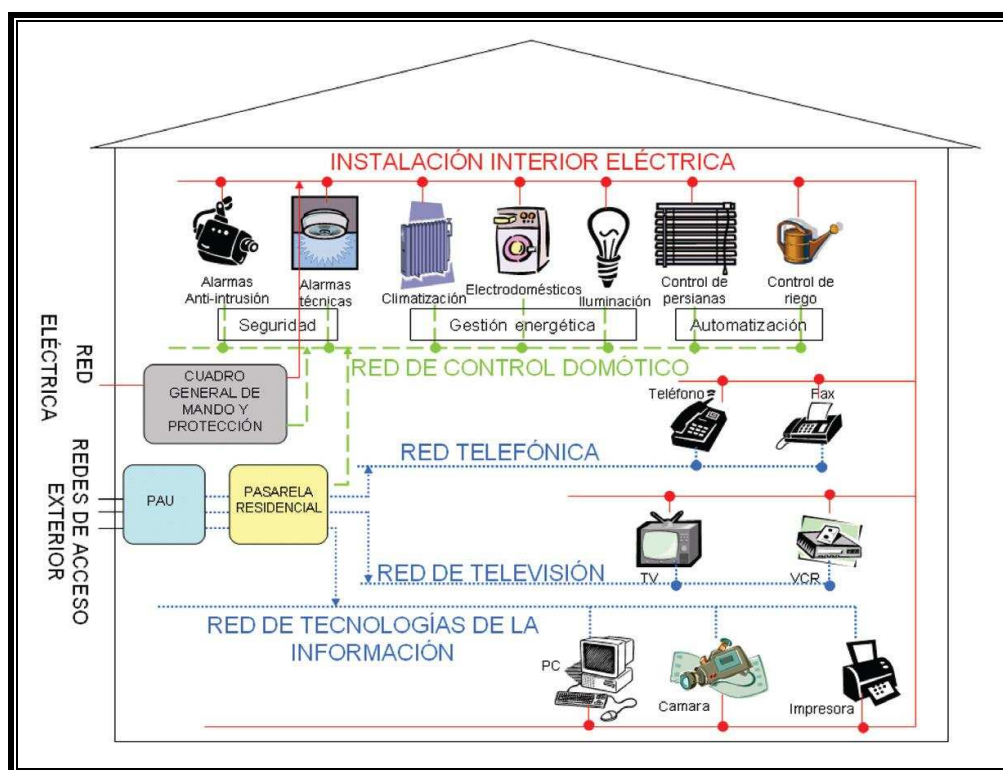


Figura (1.1) Ejemplo de una red domótica en el hogar [7]

1.2.4 DESCRIPCIÓN DE ELEMENTOS QUE INTEGRAN EL SISTEMA DOMÓTICO

Está conformado por la integración de diferentes elementos:

1.2.4.1 Módulos

- **Módulo Controlador**

Es el módulo principal del sistema domótico y su función primordial es el control de los módulos de activación y sensores, proporcionan una interfaz con el usuario, mediante: pantallas, teclados, incluso control remoto vía telefónica o internet.

- **Módulo Sensores**

Son los módulos que utiliza el sistema para conocer el estado de ciertos parámetros, están encargados de monitorear constantemente el entorno, la vivienda, y de enviar información al módulo controlador para que éste pueda tomar las decisiones oportunas. Por ejemplo encender una luz en cuanto empieza a oscurecer.

- **Módulos de activación (Actuadores)**

Es un modulo que recibe y ejecuta las órdenes que le llegan del módulo controlador. Los actuadores realizan acciones concretas como por ejemplo encender o apagar un electrodoméstico, o una lámpara. Incluso pueden abrir o cerrar el paso del agua, o del gas, mediante electroválvulas.

1.2.4.2 Medios de interconexión

- **Cableados:**

- Fibra óptica.
- Cable (coaxial, par trenzado, AWG).

- **Inalámbricos:**

- Wifi.
- GPRS.

- Bluetooth.
- Radiofrecuencia.
- Infrarrojos.

1.2.4.3 Software para sistemas domóticos

Para dotar al sistema domótico de inteligencia y control desde un PC, es necesario un módulo controlador y un software que se encargue del control. Según el sistema operativo que se utiliza tenemos los siguientes:

Para Mac:

- Xtension.
- Indigo.

Para Windows:

- Multidomo.
- Domoelite.
- ActiveHome.

Para Linux:

- Heyu.
- MisterHouse.
- Domopic.

1.2.5 ARQUITECTURA DOMÓTICA

La arquitectura de un sistema domótico establece la ubicación de dispositivos y módulos, siendo las siguientes:

- **Arquitectura Centralizada:** hay un módulo controlador centralizado, que recibe información de múltiples sensores y, una vez procesada, genera las órdenes para los módulos actuadores.
- **Arquitectura Distribuida:** en esta arquitectura toda la inteligencia del sistema está distribuida por todos los módulos sean sensores o

actuadores. Suele ser típico de los sistemas de cableado en bus, o redes inalámbricas.

- **Arquitectura mixta:** dispone de varios módulos controladores capaces de adquirir y procesar la información de múltiples sensores y transmitirlos al resto de actuadores distribuidos en el hogar.

1.2.6 PROTOCOLOS:

La red domótica usa diferentes tecnologías que se caracterizan por su protocolo de comunicación, éste es el idioma que utilizan los diferentes módulos para comunicarse entre ellos. Dentro de los protocolos existentes se tiene la siguiente clasificación:

1.2.6.1 Protocolos abiertos:

Estos protocolos son usados por diferentes compañías con el fin de unificar criterios, buscando compatibilidad entre ellos. Se les denomina abierto debido a que no son patentados, sus características son de libre acceso, tanto a empresas como a usuarios, los cuales pueden obtener la suficiente documentación para su implementación, de manera que cualquier fabricante puede desarrollar aplicaciones y productos usando estos protocolos de comunicación.

Entre los protocolos abiertos tenemos los siguientes: KNX, X10, etc.

1.2.6.1.1 KNX

Es un protocolo abierto de comunicaciones basado en un bus de datos, normalizado en Europa, su aplicación en viviendas permite transmitir las señales utilizando su propio cableado. El funcionamiento de KNX se basa en el uso de un cable con dos hilos conductores, a través del cual se comunican entre sí los dispositivos. Este sistema funciona a 9.6 Kbps y suministra un voltaje de 24 Vdc a través de los hilos conductores.

1.2.6.1.2 X10

Es un protocolo de comunicaciones para el control remoto de dispositivos eléctricos. Utiliza la línea eléctrica (220V o 110V), como único medio, para transmitir señales de control entre los dispositivos que utilizan el protocolo X10.

1.2.6.2 Protocolos propietarios o cerrados:

Son aquellos desarrollados por una compañía en particular, este tipo de protocolos solo pueden ser usados por esta compañía. Se denominan cerrados porque solo el fabricante puede hacer cambios, mejoras y creación de nuevos dispositivos que se comunican en el mismo idioma. Al ser patentados se protege los derechos del fabricante, pero limita la aparición de continuas evoluciones en los sistemas domóticos y si la empresa desaparece, el sistema desaparece y las instalaciones pueden quedar sin soporte técnico ni cambio, un ejemplo de ello es el protocolo de LonWorks.

1.2.6.2.1 LonWorks

LONWorks es un estándar propietario desarrollado por la empresa Echelon. El estándar LONWork se basa en el esquema propuesto por LON(Local Operating Network). Este consiste en un conjunto de dispositivos inteligentes, o nodos, que se conectan mediante uno o más medios físicos y se comunican utilizando un protocolo común. Por inteligente se entiende que cada nodo es autónomo y proactivo, de forma que puede ser programado para enviar mensajes a cualquier otro nodo como resultado de cumplirse ciertas condiciones o llevar a cabo ciertas acciones, en respuesta a los mensajes recibidos.

1.2.7 X10

1.2.7.1 Introducción

X10 es la tecnología más extendida gracias al bajo costo de los equipos, a la variedad de dispositivos disponibles, y a la facilidad de instalación y configuración. Es un sistema modular, escalable con una gran oferta de dispositivos X10, el lenguaje que utilizan estos dispositivos es el protocolo X10, él que permite comunicarse aprovechando el cableado de la red eléctrica de 110V o 220V como medio de comunicación, permitiendo controlar dispositivos eléctricos como televisores, radio, horno microondas, y más, siempre que se encuentren conectados a la red eléctrica.

Fundamentalmente X10 se basa en el envío de mensajes muy simples entre módulos X10 compatibles y combinando con señales de radio frecuencia permiten realizar acciones de control inalámbrico.

Todos los productos X10 son compatibles entre sí, se pueden combinar para formar un sistema adecuado a las preferencias del usuario. Entre los principales distribuidores de esta tecnología X10 basados en el protocolo estándar X10, están: Netzbuss, Timac y Home Systems totalmente compatibles entre ellos.

1.2.7.2 Protocolo X10

X10 es uno de los primeros protocolos usados en aplicaciones domóticas. Diseñado en Escocia por Pico Electronics of Glenrothes entre los años 1976 y 1978 con el fin de transmitir un código binario por las líneas de baja tensión (110V o 220V) que permite el control remoto de los dispositivos domésticos. El protocolo X10, es un protocolo abierto, es decir, cualquier fabricante puede producir dispositivos X10.

1.2.7.2.1 Funcionamiento del protocolo X10

La transmisión del protocolo X10 consiste en el envío de señales en alta frecuencia (120KHz) a través del cableado eléctrico tomando como referencia el cruce por cero de la onda senoidal de voltaje. ^[17]

Un uno binario del mensaje se representa por un pulso de 120 KHz durante un milisegundo en el cruce por cero, y un cero binario del mensaje se representa por la ausencia del pulso de 120Khz.

El máximo retraso entre el comienzo del envío y los pulsos de 120 KHz es de 50 μ seg. La transmisión completa de una orden X10 necesita once ciclos de voltaje.

Los receptores para evitar el ruido eléctrico de la red, abren su ventana de recepción con una duración de 0.6ms, dos veces cada período de la onda senoidal (Figura 1.4), esto es 120 veces cada segundo, para una frecuencia de 60Hz y 100 veces cada segundo para una frecuencia de 50Hz.

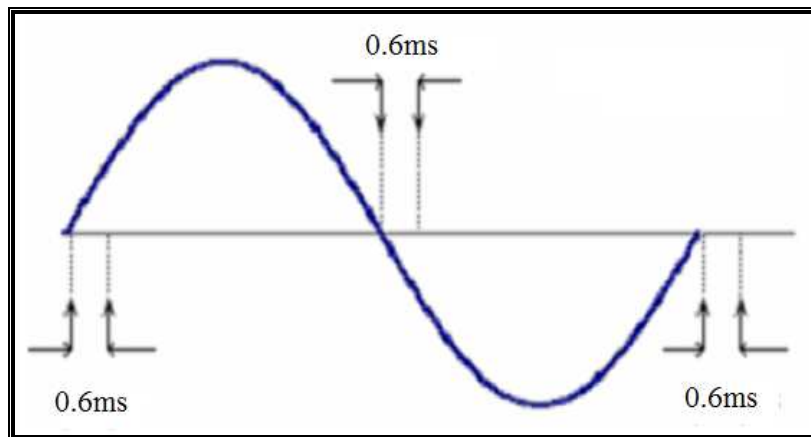


Figura (1.4) ventana del receptor en 0.6ms ^[11]

1.2.7.2.2 Trama X10

Un bit es transmitido cuando la onda senoidal de 110V a 60Hz pasa por cero voltios. El "1" lógico es definido como la presencia de pulso, inmediatamente seguido por la ausencia de pulso. Un "0" lógico es definido como la ausencia de pulso, inmediatamente seguido de la presencia de pulso (Figura 1.5).

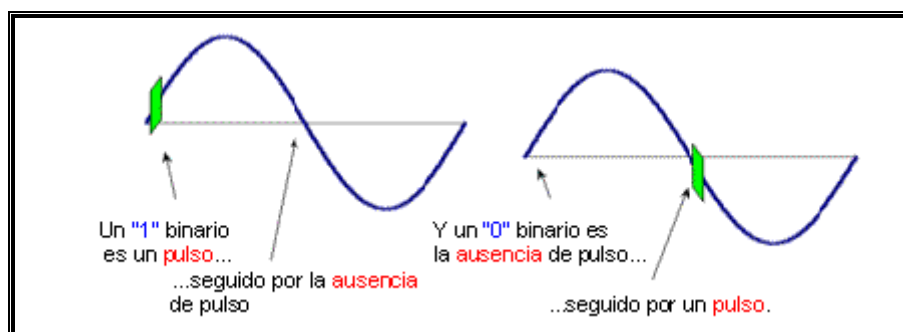


Figura (1.5). Representación de un bit en el protocolo X10 ^[17]

Para establecer un punto predecible de envío, cada grupo de datos empiezan siempre con al menos 6 pasos por cero limpios (000000 en binario), luego se envía un código de inicio (Start code), el cual es 1110 en binario.

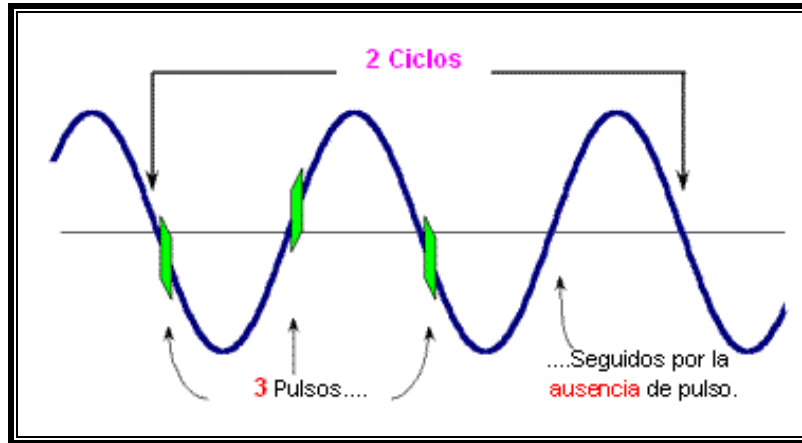


Figura (1.6). Código de inicio ^[17]

Después que el código de inicio se ha transmitido, se envía el primer nibble de datos (un nibble contiene 4 bits o medio byte), estos cuatro bits asignan un código de casa que facilita el manejo de los dispositivo (Figura 1.7).

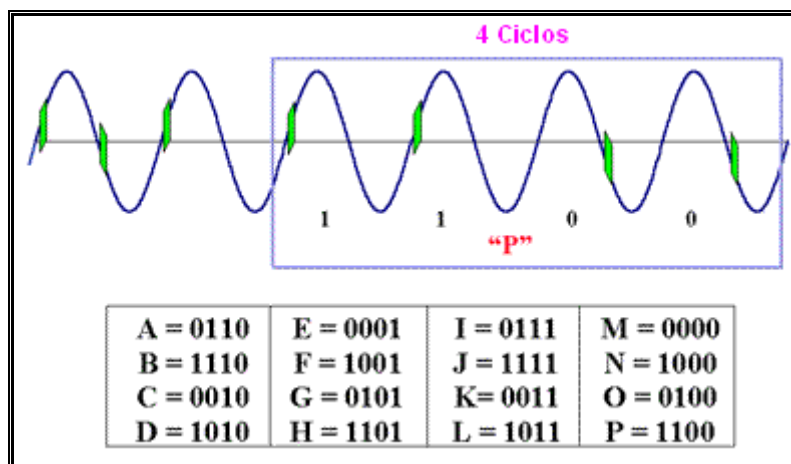


Figura (1.7) Código de casa ^[17]

A continuación se envía un segundo nibble, el cual proporciona la segunda mitad de la dirección del dispositivo (Figura 1.8.). El último bit de este segundo nibble permite identificar entre un código de número o un código de comando. Cuando este bit es un "0", significa que es un código de número y si es un "1", es un código de comando.

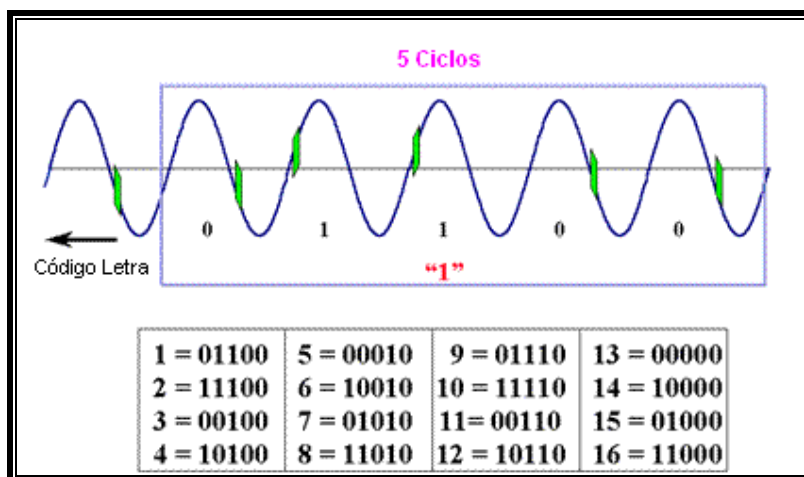


Figura (1.8) Código de número ^[17]

Para tener seguridad que los datos fueron enviados y recibidos correctamente, cada trama (código de inicio, código de casa, código de número o de comando), debe ser transmitido 2 veces.

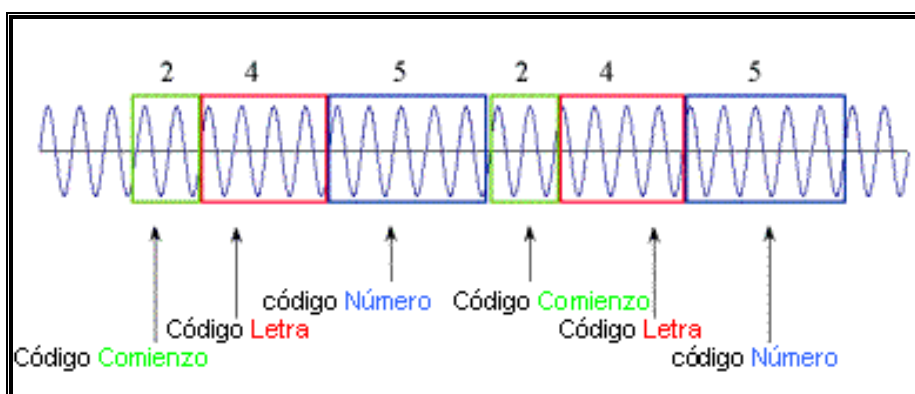


Figura (1.9) Envío de una trama con redundancia ^[17]

Luego que el receptor reconoce su dirección, está listo para recibir el comando de función, entonces el transmisor nuevamente envía el código de inicio, luego envía el primer nibble con el código de letra o casa y finalmente envía el segundo nibble con el código de comando (Figura 1.10). El receptor reconoce al segundo nibble como comando al verificar que el último bit es un "1". Todos los códigos de comandos terminan en un uno binario.

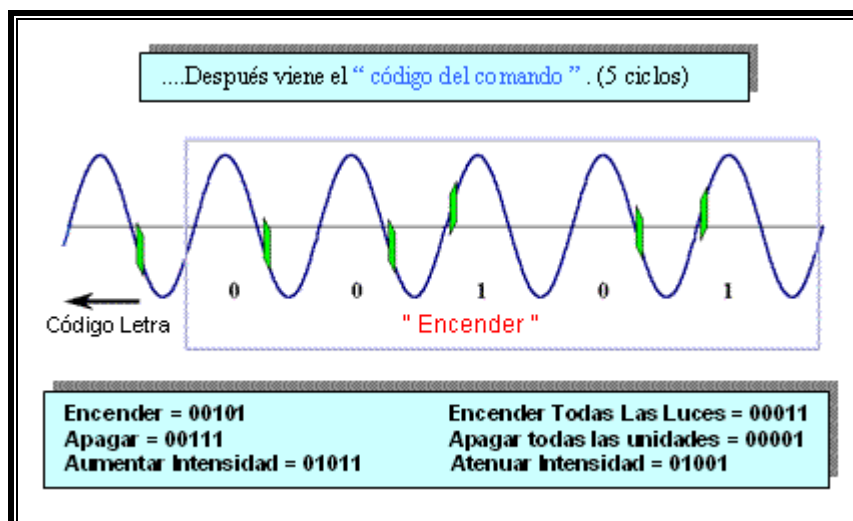


Figura (1.10) Código de comando ^[17]

Para transmitir un código de comando después del código de número se debe esperar por lo menos 3 ciclos de silencio, es decir por lo menos 6 pasos por cero limpios (000000).

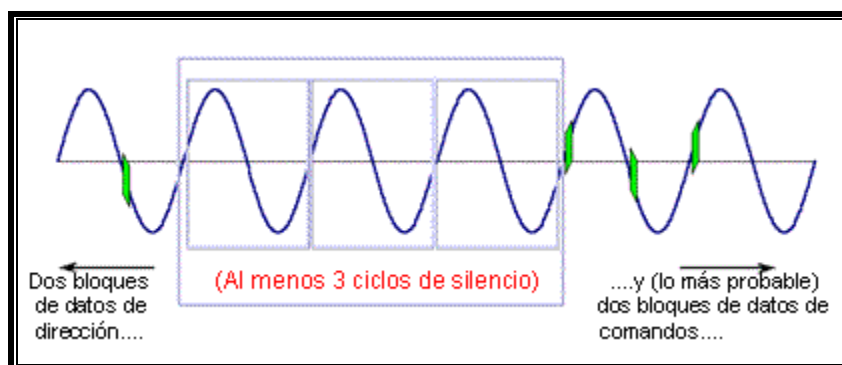


Figura (1.11) Ciclos de espera entre transmisores ^[17]

En la Figura 1.12 se muestra los ciclos totales que necesita un transmisor para realizar una transmisión completa. Para transmitir un dato completo en X10 se necesita 47 ciclos de la onda senoidal de 60Hz.

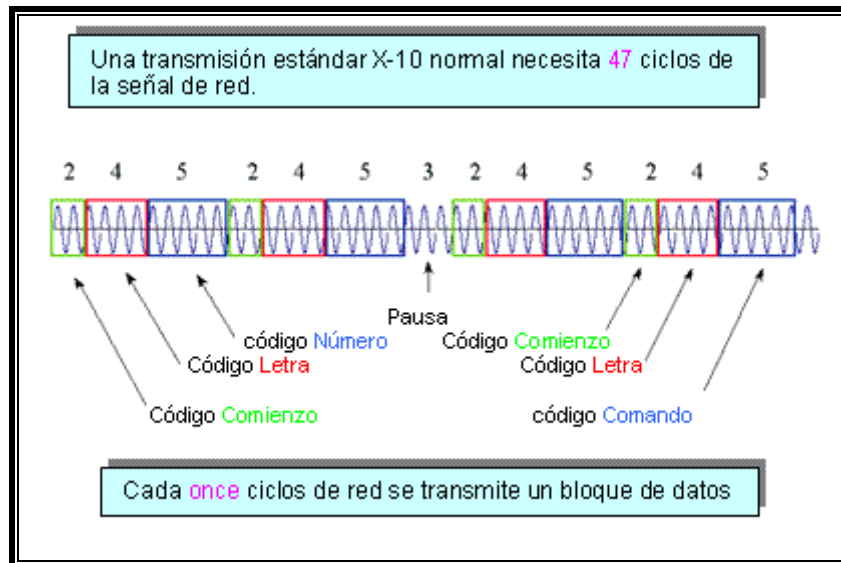


Figura (1.12) Transmisión completa de la trama X10^[17]

En funciones de regulación de intensidad se transmite de forma continua (por lo menos dos veces) sin la separación de los 3 ciclos de silencio entre tramas.

1.2.7.3 Ventajas de la tecnología X10

El sistema X10 tiene las siguientes ventajas:

- Protege el Hogar trabajando con los sistemas de alarma. Se puede controlar y comprobar el estado de la casa a distancia.
- Añade valor a la propiedad, una casa con un sistema domótico se cotiza a mayor valor en el mercado inmobiliario.
- Mejora la calidad de vida brindando un confort en el hogar, todas las actividades rutinarias como encender la luz pueden ser automatizadas.
- Permite el ahorro de energía al supervisar, controlar las luces y electrodomésticos, apagándolos cuando no son necesarios.
- Visión de Futuro: Una de las cosas que se analiza cuando se invierte en tecnología hoy en día es su vida útil. De entre los varios sistemas domóticos que tratan de imponerse en la actualidad, el sistema X10 es

el único que sigue vigente después de más de 25 años y con más de cien millones de aparatos funcionando por todo el mundo.

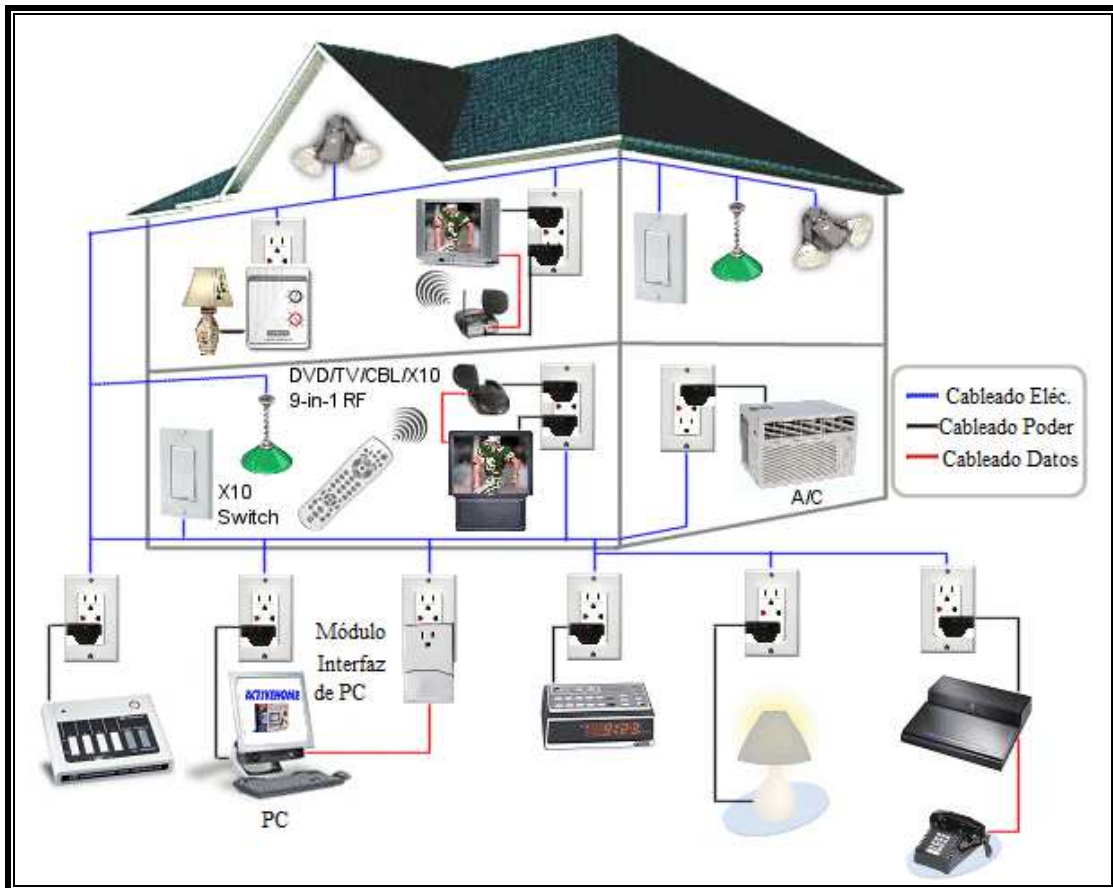


Figura (1.13): Esquema de un hogar con tecnología X10^[14]

1.2.7.4 Clasificación de los módulos X10

Los módulos X10 se clasifican y se asignan ciertos logos para identificar su función.



Transmisores: Un transmisor envía una señal especialmente codificada de bajo voltaje que es superpuesta sobre el voltaje del cableado, es capaz de enviar información hasta 256 dispositivos sobre el cableado eléctrico. Múltiples transmisores pueden enviar señales al mismo módulo.



Receptores: un receptor toma la seña enviada por los dispositivos transmisores. Una vez que la seña es recibida el dispositivo responde encendiéndose (ON) o apagándose (OFF).



Bidireccionales: Estos dispositivos funcionan como transmisores y receptores a la vez, tomando la seña enviada por los dispositivos transmisores o enviando una seña para los dispositivos receptores.



Inalámbricos: Permiten enviar señas de radio desde una unidad inalámbrica e inyectar la seña X10 en el cableado eléctrico (como los controles remotos para abrir los portones de los garajes). Estas unidades no están habilitadas para controlar directamente a un receptor X10, debe utilizarse un módulo transceptor.



Todos los productos etiquetados con este símbolo significa que transmiten y reciben el código X10 por radio frecuencia (RF).

1.2.7.5 Arquitectura del sistema X10

La arquitectura del sistema es totalmente flexible y, por tanto, la disposición de los módulos receptores y emisores pueden cambiar variando su código de identificación (código de casa y código de número, ejemplo C14). Del mismo modo, un emisor de seña puede activar distintos receptores, o al contrario distintos emisores pueden gobernar un mismo receptor. En la figura 1.14 se observa un esquema de la arquitectura del sistema X10.

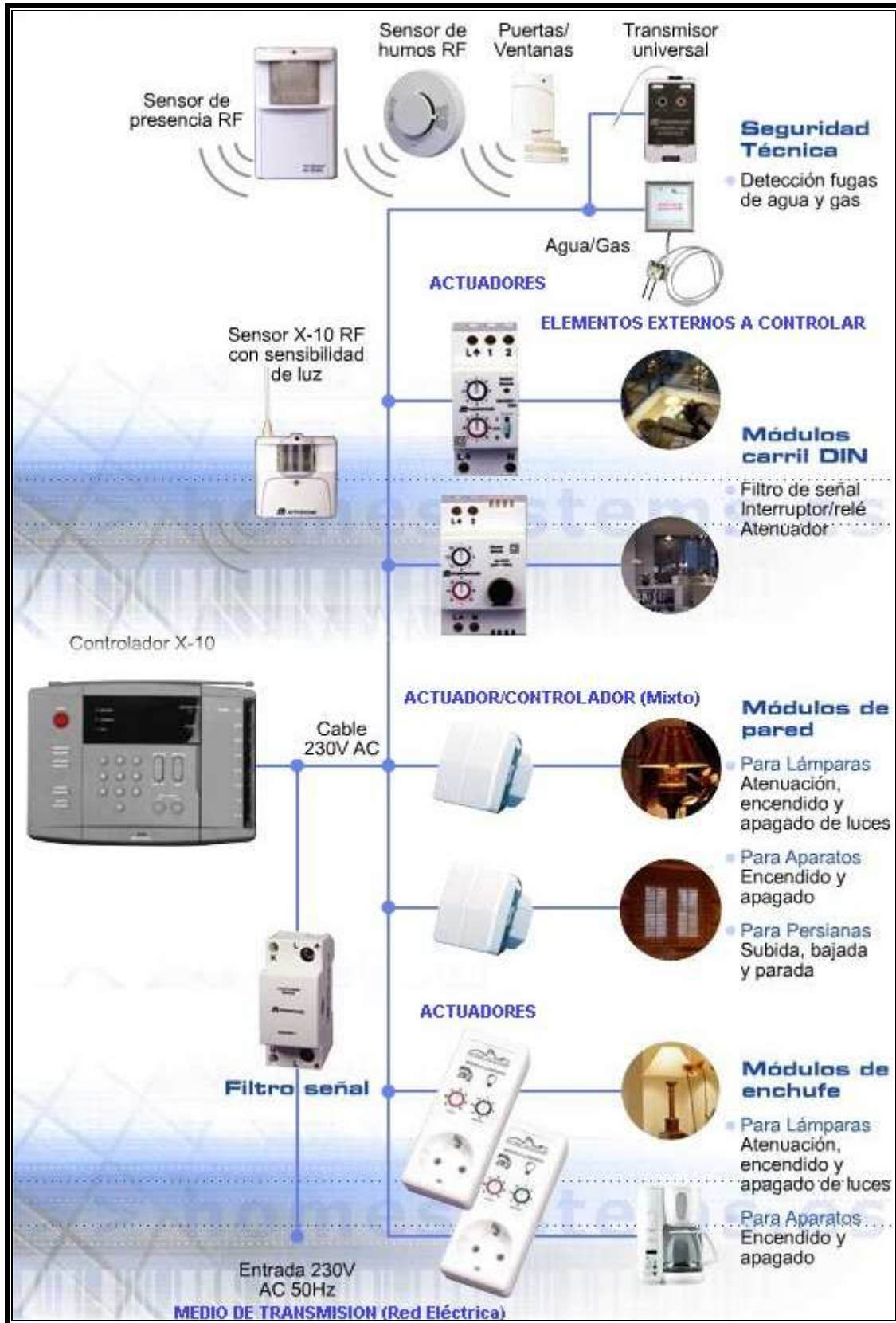


Figura (1.14) Arquitectura del sistema X10^[14]

1.2.7.6 Productos X10

Las funciones básicas de los módulos X10 son transmitir y recibir comandos por medio del protocolo X10, aceptar y transferir los datos desde y hacia el PC.

1.2.7.6.1 CM11

El dispositivo CM11, es un módulo que funciona como una interfaz entre los dispositivos X10 a través de la línea de corriente y la PC. Permite establecer programaciones, escenas pre-programadas y simulaciones de presencia desde el PC.

La conectividad entre el CM11 y el PC es posible realizarse por medio de una conexión Serial (RS-232) o mediante USB.

Características Técnicas:

- Alimentación: 110V o 220V +10% - 15%, 60 Hz.
- Señal X-10: $f=120$ Khz, $V= 2,5V_{pp}$
- Pila: 2 x AAA
- Conexiones: Conector macho y hembra de red y RJ11 para en cable serie. USB mediante cable adaptador.



Figura (1.15) CM11

1.2.7.6.2 CM17A

El CM17A posee la característica de enviar señales vía radiofrecuencia a los módulos X10 instalados en el hogar. Comercialmente se le conoce como

“FireCracker”. Se conecta al puerto serial del PC (no necesita pilas), y nos permite enviar comandos a un módulo de radiofrecuencia, que convertirá la señal recibida vía radio



Figura (1.16) FireCracker CM17A

1.2.7.6.3 LM465 Módulo actuador de lámpara X10

Este módulo está diseñado para enchufarlo en un tomacorriente, es programable a través de otro módulo controlador X10, de forma tal que el módulo reconoce y memoriza el mismo.



Figura (1.17) Módulo actuador de lámpara LM465

1.2.7.6.4 TM751 Módulo Transceptor X10

El transceptor TM751 capta las señales de radio de frecuencia de comandos a distancia X10, envía las señales a través del cableado existente en la vivienda para todos los módulos actuadores conectados.



Figura (1.18) Módulo de transceptor TM751

1.2.7.6.5 MS16A sensor de movimiento

El sensor de movimiento y presencia envía señales de radiofrecuencia (RF) a los transceptores o a las bases receptoras de los sistemas de alarma y emergencia personal X10. Los receptores a la vez envían esta información por la red eléctrica existente de la casa a los módulos receptores X10 instalados en cualquier parte del hogar.



Figura (1.19) Sensor de movimiento MS16A

1.3 GNU/LINUX

GNU/LINUX (más conocido como Linux) es un sistema operativo, compatible con Unix. Su desarrollo es uno de los ejemplos de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU) y otra serie de licencias libres.

A las variantes de este sistema operativo, que se les adicionan diversos programas de aplicación, con propósitos específicos o generales se las denomina distribuciones. Su objetivo consiste en ofrecer ediciones que cumplan con las necesidades de un determinado grupo de usuarios. Algunas de ellas son especialmente conocidas por su uso en servidores y supercomputadoras. Además del núcleo Linux, las distribuciones incluyen habitualmente las bibliotecas y herramientas del proyecto GNU y el sistema de ventanas X Window System. Dependiendo del tipo de usuarios a los que la distribución esté dirigida se incluye también otro tipo de software como procesadores de texto, hoja de cálculo,

reproductores multimedia, herramientas administrativas, etc. Entre las distribuciones Linux más populares se incluyen:

- CentOS, una distribución creada a partir del mismo código del sistema Red Hat pero mantenida por una comunidad de desarrolladores voluntarios.
- Debian, una distribución mantenida por una red de desarrolladores voluntarios con un gran compromiso por los principios del software libre.
- Fedora, una distribución lanzada por Red Hat para la comunidad.
- Gentoo, una distribución orientada a usuarios avanzados, un sistema que automatiza la compilación de aplicaciones desde su código fuente.
- gOS, una distribución basada en Ubuntu para netbooks.
- Knoppix, la primera distribución live en correr completamente desde un medio extraíble. Está basada en Debian.
- Linux Mint, una popular distribución derivada de Ubuntu.
- Mandriva, mantenida por la compañía francesa del mismo nombre, es un sistema popular en Francia y Brasil. Está basada en Red Hat.
- Red Hat Enterprise Linux, derivada de Fedora, es mantenida y soportada comercialmente por Red Hat.
- Ubuntu, una popular distribución para escritorio basada en Debian y mantenida por Canonical.

1.3.1 VOIP

1.3.1.1 Definición VoIP

La Voz sobre el Protocolo Internet (VoIP, Voice Over Internet Protocol) es una tecnología que permite la transmisión de la voz a través de las redes IP en forma de paquetes de datos.

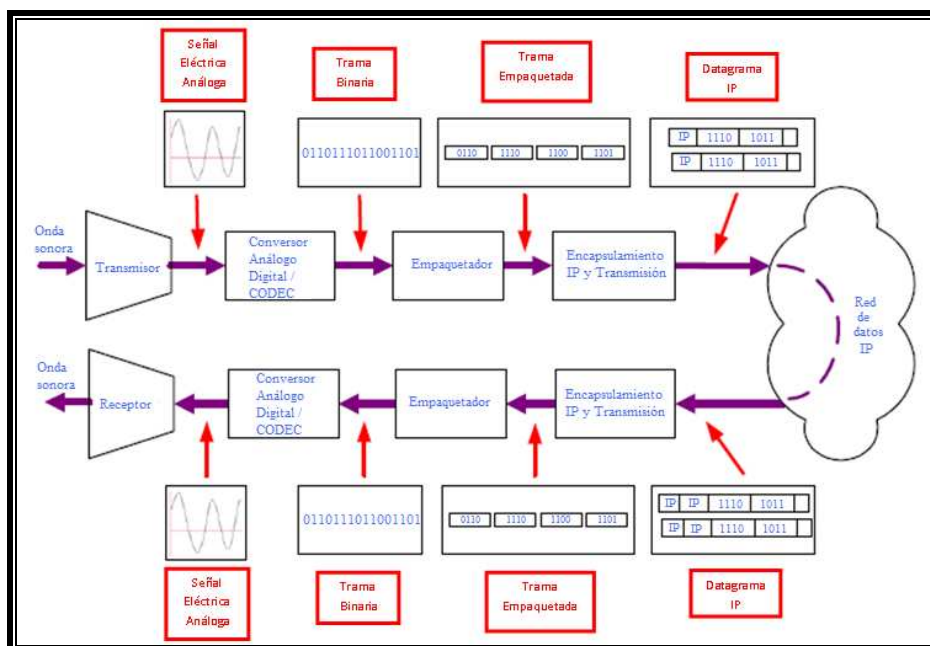


Figura (1. 20) Proceso del transporte de VoIP ^[1]

El protocolo VoIP permite la transmisión de la voz en forma de paquetes, primero convierte la señal analógica del teléfono en digital, a través de un proceso de digitalización de señales PCM con un codificador/decodificador de voz, luego son comprimidas mediante un algoritmo que segmenta señales para ser transmitidas por las redes de datos en forma de paquetes, después en el otro extremo esa señal se convierte nuevamente en analógica con el proceso inverso, haciendo posible el uso de teléfonos regulares en la Internet.

Todos estos pasos constan de varios procesos interconectados, convierten una señal de voz en una corriente de paquetes dentro de una red de datos como se puede observar en la Figura 1.20. Ejemplo: Permiten a la voz humana y a la información de fax viajar a través de una red de paquetes de datos concurrentemente junto con paquetes de datos tradicionales.

1.3.1.2 Aplicaciones de VoIP

VoIP podría aplicarse a cualquier comunicación de voz, desde una simple comunicación entre oficinas hasta complejas teleconferencias multipunto con ambiente de pantallas compartidas. La calidad de la reproducción de la voz puede ser ajustada de acuerdo a la aplicación.

Las aplicaciones de VoIP que actualmente se realizan son:

- Teléfonos IP para Pymes (Pequeñas y medianas Empresas).
- Acceso remoto desde una sucursal o desde la oficina de la casa a la PBX de la empresa.
- Central Telefónica IP
- Proveedores de llamadas de larga distancia y celular a través de IP (o de Internet).

1.3.1.3 Señalización de VOIP y protocolos de transporte de voz

Por el Protocolo Internet (IP) se desplazan básicamente dos tipos de tráfico: el Protocolo de datagrama de usuario (UDP) y el Protocolo para el control de la transmisión (TCP). En general, se utiliza TCP cuando se necesita una conexión fiable y UDP protocolo no orientado a la conexión.

Debido a la naturaleza sensible del tráfico de voz, UDP/IP fue la elección lógica para transportar la voz, y para que la comunicación de voz sobre una red IP pueda llevarse a cabo es necesario el establecimiento de sesiones RTP (*Real-time Transport Protocol*). Estas sesiones son, a grandes rasgos, flujos de paquetes UDP extremo a extremo en los que se transporta la información de voz, previamente codificados y empaquetados de acuerdo con alguno de los estándares existentes.

El mecanismo para una conexión de VoIP involucra un conjunto de transacciones de señalización entre los puntos finales y entre ellos además de una gran cantidad de protocolos y recomendaciones.

Los estándares más utilizados en la señalización de VoIP son H.323 y SIP

1.3.1.3.1 Estándar H.323

El protocolo H.323, es un estándar creado por la Unión Internacional de Telecomunicaciones (ITU) H323, ya que cubre la mayor parte de las necesidades para la integración de la voz sobre una red de datos.

Soporta la tecnología de voz empaquetada. Fue diseñado con el objetivo fundamental de proveer a los usuarios de un servicio de tele-conferencia capaz de transmitir voz, video y datos a través de redes de conmutación de paquetes.

Sin embargo H.323 resulta complejo en algunos aspectos para utilizarlo solo como VoIP. Esto motivó que se desarrollara un protocolo alternativo denominado SIP (Session Initiation Protocol), con la intención de ser un estándar más práctico y orientado a la voz sobre IP.

En resumen actualmente H.323 y SIP realizan básicamente las mismas funciones, si bien son protocolos incompatibles, existen pasarelas entre H.323 y SIP que permiten su interconexión en las redes de datos.

1.3.1.3.2 Sip (protocolo de inicio de sesiones)

Desarrollado por el IETF MMUSIC Working Group con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual.

La sintaxis de sus operaciones se asemeja a las de HTTP y SMTP, los protocolos utilizados en los servicios de páginas Web y de distribución de e-mails respectivamente. Esta similitud es natural ya que SIP fue diseñado para que la telefonía se vuelva un servicio más en la Internet.

Funciones de señalización

- Establecer, modificar y finalizar llamadas/sesiones.
- Registro y localización de participantes. Movilidad.
- Gestión del conjunto de participantes y de los componentes del sistema.
- Descripción de características de las sesiones y negociación de capacidades de los participantes.

Componentes

Agentes de Usuario (Terminales) Son los puntos extremos del protocolo, es decir son los que emiten y consumen los mensajes del protocolo SIP (figura 1.22).

Un videoteléfono, un teléfono, un cliente de software (softphone) y cualquier otro dispositivo similar es para el protocolo SIP un agente de usuario.

Todos los agentes de usuario se comportan como clientes (UAC: User Agent Clients) y como servidores (UAS: User Agent Servers). Algunos terminales por software que soportan charlas de audio y vídeo a través de SIP son Microsoft Windows Messenger, Apple iChat, Ekiga entre otros.

Servidores de Registro (Registrar) Al iniciarse el agente de usuario SIP envía una petición con el método REGISTER a un Servidor de Registro, informando a qué dirección física debe asociarse la dirección lógica del usuario (binding). Esta asociación tiene un período de vigencia y si no es renovada, caduca. También puede terminarse mediante el método Deregister. El protocolo SIP no determina la forma en que se debe gestionar los registros.

Servidores Intermediarios (Proxy) y de Redirección

Para encaminar un mensaje entre un UAC y un UAS normalmente se recurre a los servidores (figura 1.24). Estos servidores a su vez se sirven del sistema DNS para localizar los dominios y pueden actuar de dos maneras:

1. Como intermediario, encaminando el mensaje hacia destino.
2. Como redirector, generando una respuesta que indica al remitente la dirección del destino o de otro servidor que lo acerque al destino.

La principal diferencia es que el servidor intermediario forma parte de la comunicación, mientras que el servidor de redirección una vez que indica al UAC cómo encaminar el mensaje ya no interviene más.

Un mismo servidor puede actuar como redirector o como intermediario dependiendo de la situación.

Esquema de comunicación

En este ejemplo se utiliza servidores (figura 1.21).

- Un usuario indica a su terminal la dirección lógica de la persona con la que quiere comunicarse.
- El agente de usuario SIP actuando como UAC envía la petición (en este caso con el método INVITE) al servidor de registro local (si la llamada es a un miembro del mismo dominio) o bien al servidor intermediario que tiene configurado como servidor saliente.
- El servidor intermediario se vale del sistema DNS para determinar la dirección del servidor SIP del dominio del destinatario. Una vez obtenida la dirección del servidor del dominio destino, encamina hacia allí la petición.
- El servidor del dominio destino se vale de la información de registro de dicho usuario para establecer su ubicación física. Si la encuentra encamina la petición hacia dicha dirección.
- El agente de usuario destino, si se encuentra desocupado, comenzará a alertar al usuario destino y enviará una respuesta hacia el usuario llamante (código 180) que sigue el camino inverso de la comunicación. Cuando el usuario destinatario finalmente acepta la invitación, se genera una respuesta con un nuevo código de estado (200) cuya recepción es confirmada por el UAC llamante mediante el método ACK.
- Cuando cualquiera de las partes termina la sesión, actuando como UAC, envía una petición con el método BYE.

Normalmente la petición con el método INVITE lleva un cuerpo donde viaja una descripción de la sesión que quiere establecer, esta descripción es realizada con el protocolo SDP. En ella se indica el tipo de contenido a intercambiar (voz, vídeo, etc.) y sus características (códecs, direcciones, puertos donde se espera recibirlos, velocidades de transmisión, etc.). Esto se conoce como oferta de sesión SDP. La respuesta a esta oferta viaja, en este caso, en el cuerpo de la respuesta definitiva a la petición con el método INVITE. La misma contiene la descripción de la sesión desde el punto de vista del destinatario. Si las descripciones fueran incompatibles la sesión debe terminarse (mediante una petición con el método BYE).

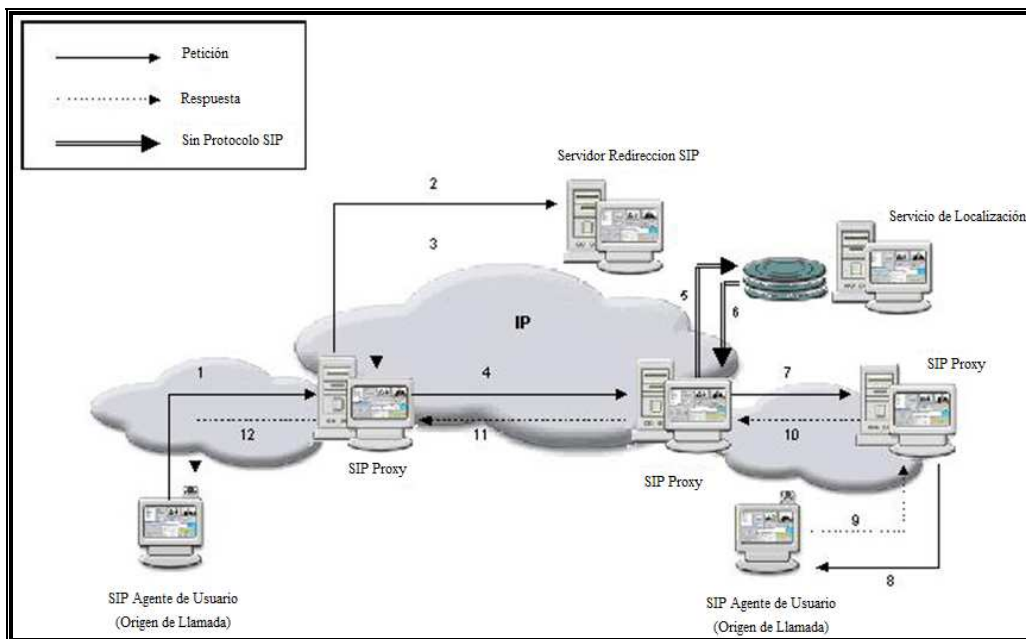


Figura (1.21) Red SIP ^[15]

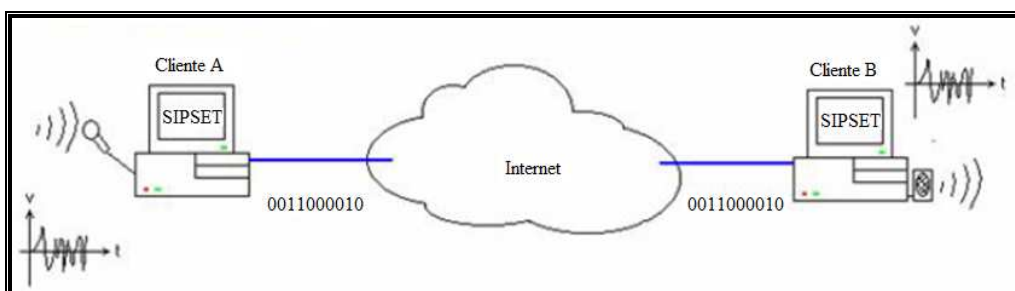


Figura (1.22) Comunicación SIP entre terminales ^[14]

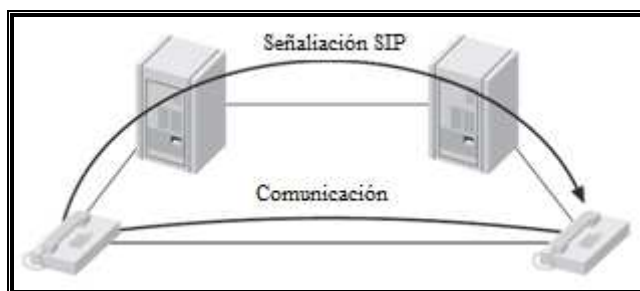


Figura (1.23) Comunicación del servidor proxy SIP entre terminales ^[14]

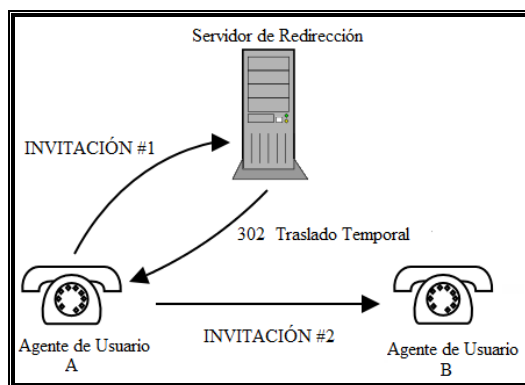


Figura (1.24) Servidor de redirección SIP entre terminales ^[16]

1.3.1.3.3 Comparación entre H.323 y SIP

Las diferencias entre ambos protocolos se las realiza para observar cual de los dos ofrece mejores condiciones para el trato de la calidad de servicio. En la tabla se muestran las diferencias más relevantes entre ambas aproximaciones.

H.323	SIP
Se diseña con requerimientos de conferencia multimedia, siguiendo una estructura unificada que pretende dar el mismo nivel de robustez e interoperabilidad que la RTB(Red Telefónica Básica).	Se diseña de forma modular y su propósito es establecer una sesión genérica entre dos puntos, sin centrarse específicamente en una conferencia multimedia de vídeo y audio.
Estandarización de control de llamada y servicios suplementarios perfectamente definida y compatible con los servicios de telefonía tradicional.	Falta de madurez en cuanto a dicha estandarización, el IETF está trabajando sobre ello para dotar de un sistema de servicios suplementarios robusto a SIP, que incluya interoperabilidad con la telefonía tradicional, así como con H.323.
Provee mejor funcionalidad e interoperabilidad con respecto a servicios suplementarios. Esto es porque se separa perfectamente la parte de servicios suplementarios de la parte de control de la llamada básica.	La llamada básica en SIP se extiende incluyendo elementos como servicios suplementarios, lo que puede dar lugar a problemas de interoperabilidad y compatibilidad entre distintas plataformas.

<p>H.323 está diseñado para dar soporte a VoIP, su soporte para otras aplicaciones es muy limitado, y ha sido añadido posteriormente.</p>	<p>SIP permite que un amplio rango de aplicaciones funcione bajo el mismo protocolo, donde VoIP es sólo una posibilidad más. Provee de mecanismos mucho más efectivos para manejar sesiones que no sean VoIP.</p>
<p>Los clientes H.323 han de implementar toda la funcionalidad de H.323, incluso si parte de la misma no es requerida en un momento dado.</p>	<p>Los clientes SIP son ligeros, dado que sólo han de implementar el protocolo SIP y aquellas cosas que sean necesarias para la aplicación, pudiendo ignorar las que no lo sean.</p>

Tabla (1.1) Comparación entre protocolos H.323 y SIP ^[15]

De cualquier forma, en un futuro parece que la tendencia conlleva a una convergencia SIP-H.323, o al menos a una coexistencia donde ninguno suplantarán al otro, sino que serán utilizados en función de las necesidades de cada escenario. Lo que cobra especial relevancia es el diseño de pasarelas SIP-H.323 para la interoperabilidad entre estas redes.

1.3.1.3.4 *Calidad de servicio (quality of service, QoS)*

La calidad de servicio (Quality of Service, QoS) hace referencia tanto a la clase de servicio (Class of Service, CoS) como al tipo de servicio (Type of Service, ToS). El objetivo básico de CoS y ToS es conseguir el ancho de banda y la latencia necesarios para una aplicación eficaz determinada.

Una CoS permite al administrador de la red agrupar diferentes flujos de paquetes, teniendo cada uno requisitos de latencia y ancho de banda diferentes. Un ToS es un campo en una cabecera de Protocolo Internet (IP) que permite que tenga lugar una clase de servicio.

Voz sobre IP (VoIP) viene con su propio conjunto de problemas. La QoS puede ayudar a resolver algunos problemas, como la pérdida de paquetes, la fluctuación de fase, retardos, el retraso de señalización, etc.

La recomendación G.114 de la ITU-T sugiere que no haya más de 150 ms de retraso de extremo a extremo para mantener una "buena" calidad de la voz. [4]

1.3.1.3.5 Ancho de banda

Hay que tener presente el ancho de banda para una comunicación de VoIP y el número de comunicaciones simultáneas que se requieran. Habitualmente en el entorno LAN, donde se utiliza tecnología Switch a 10 o 100 Mbps, se elige cierta codificación de la señal de audio o vídeo con dos objetivos principales, mantener un nivel alto de calidad y reducir el ancho de banda utilizado en la red de datos.

Comúnmente en la red LAN se utiliza la compresión G711 con un ancho de banda de 79.60 Kbps ya que se obtiene mayor calidad y se dispone suficiente ancho de banda. En cambio en el entorno WAN, donde el ancho de banda es más escaso y costoso, se elige la compresión G723 con un ancho de banda de 21.73 Kb/s

Afortunadamente el ancho de banda de las comunicaciones de voz no aumentará en el futuro y en cambio el ancho de banda en la WAN tiende a aumentar a la vez que los precios se reducen.

Esto permitirá que cada vez sea más barato aumentar el número de comunicaciones de voz en la WAN.

Nombre	Tasa (Kbps)	Tamaño de paquete(octetos sin cabeceras)	Duración de un paquete(ms)	Puntuación MOS	Patentado
G.711	64	160	20	4.1	No
G.723.1	5.3/6.4	24	30	3.65/3.9	Sí
G.726	16/ 24/ 32/ 40	80	20	3.85 para 32kbps	Sí
G.728	16	60	30	3.61	Sí
G.729A	8	20	20	3.7	Sí
GSM	13	33	20	3.5-3.7	No
iLBC	13.3/15	50	30/20	4.1/4.2	Dudoso
LPC-10	2.4	30	30	2.5	No
Speex-narrow	2.15-24.6	30-100	20	3.5-4 (estimado)	No

Tabla (1.2) Tabla de códecs de audio [15]

1.3.1.3.6 *Porcentaje de pérdida de paquetes*

Los equipos de la red Routers y Firewall debido a la prioridad de flujo y a los picos de tráfico pueden perder paquetes de datos y producir retardos en la transmisión. Estos paquetes perdidos son retransmitidos y de este modo no se pierde información, no obstante mientras en las aplicaciones de datos no suelen tener impacto, sí lo tiene en la VoIP. La pérdida de paquetes debe ser inferior al 5%.

1.3.1.3.7 *Retardo o latencia*

El retardo puede afectar al tiempo de tránsito de los paquetes desde el origen al destino y viceversa. Las personas son capaces de mantener una conversación cómodamente aunque exista cierto retardo, sin embargo llegando a un umbral puede empezar a ser incómodo para mantener una conversación. El retardo máximo debe ser de 250 ms (calidad media) y de 150 ms (calidad alta).

1.3.1.3.8 *JITTER*

Es la variación del tiempo de tránsito de los paquetes. No todos los paquetes sufren un retardo constante, este retardo variable o Jitter disminuye la calidad de la voz al pasar de cierto umbral. El Jitter debe ser inferior a 50 ms.

La calidad de la voz resultante depende de la combinación de estos tres últimos parámetros (Pérdida de Paquetes, Retardo y Jitter). Siendo los niveles de calidad los siguientes:

	Calidad alta	Calidad media	Calidad baja
Pérdida de paquetes	1.00%	3.00%	5.00%
Retardo	150 ms	250 ms	400 ms
Jitter	20 ms	50 ms	75 ms

Tabla (1.3) representa los porcentajes de calidad en el audio para la VoIP^[18]

1.3.1.4 Ventajas y desventajas de VOIP

- La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía (principalmente de larga distancia) que son usuales de las compañías de la Red Pública Telefónica Conmutada (PSTN). Algunos ahorros en el costo son debidos a utilizar una misma red para llevar voz y datos. Las llamadas de VoIP a VoIP entre cualquier proveedor son generalmente gratis en contraste con las llamadas de VoIP a PSTN que generalmente cuestan al usuario de VoIP.
- El desarrollo de codecs para VoIP ha permitido que la voz se codifique en paquetes de datos cada vez más pequeños. Esto deriva en que las comunicaciones de voz sobre IP requieran anchos de banda muy reducidos.
- Una desventaja importante es la calidad de la transmisión, los datos viajan en forma de paquetes, lo que puede generar algunas pérdidas de información y demora en la transmisión.
- El problema en sí de la VoIP, no es el protocolo si no la red IP.
- Robos de Datos. Un cracker puede tener acceso al servidor de VoIP y a los datos de voz almacenados y al propio servicio telefónico para escuchar conversaciones o hacer llamadas gratuitas. Si no está bien protegido pueden sufrir de fraudes por medio de suplantación de identidad.

1.3.1.5 Seguridad en redes IP

El acelerado desarrollo de la Internet nos dio la posibilidad de intercambiar información entre una gran cantidad de instituciones públicas o privadas, esta facilidad también fue aprovechada para vulnerar la confidencialidad de la información y en consecuencia, obligó a los administradores a establecer un esquema de seguridad confiable y de este modo permitir que la información solo sea procesada por el personal autorizado para ello.

Los siguientes protocolos y sistemas se utilizan para proporcionar diversos grados de seguridad a las redes IP.

- Filtrado de paquetes IP.
- Traslado de direcciones de red (NAT).
- Arquitectura IP seguridad (IPSec).
- Firewalls.

1.3.1.6 Filtrado de paquetes IP.

El filtrado de paquetes se realiza por medio de un Router que puede transferir información dentro o fuera de la red, de acuerdo con las reglas de filtrado establecidas por el administrador. Cuando el ruteador procesa un paquete de datos, extrae información del encabezado del paquete y aplica las reglas de filtrado, de acuerdo a los resultados obtenidos, el paquete es enviado a su destino o en su caso es descartado. La siguiente información se extrae del encabezado del paquete:

- Dirección IP origen.
- Dirección IP destino.
- Puerto TCP o UDP origen.
- Puerto TCP o UDP destino.
- Información del protocolo encapsulado (SMTP, Telnet, http, etc).

1.3.1.7 Traslado de direcciones de red (NAT)

Cuando se implementa el traslado de direcciones de red, automáticamente se genera un firewall entre la red interna y las redes externas o la Internet. La tecnología NAT solo permite las conexiones que se generan desde el interior de la red, esto significa que una computadora externa no puede conectarse a una computadora interna a menos que la computadora interna haya solicitado la conexión.

El traslado de direcciones de red es una solución para redes que cuentan con direcciones privadas y desean comunicarse con host en redes externas o en Internet.

1.3.1.8 Arquitectura IP seguridad

La arquitectura IP Seguridad (IPSec) suministra seguridad en la capa de red para las versiones del protocolo IP en IPv4 e IPv6. IPSec es una arquitectura abierta y ofrece las siguientes ventajas:

- Provee mecanismos de autenticado, encriptado e integridad de datos.
- Utiliza algoritmos robustos de criptografía.
- Provee seguridad para los protocolos de acceso remoto.

1.3.1.9 Firewall

Un firewall es un sistema de seguridad que implementa una política de control de acceso entre dos o más redes; restringe el acceso de usuarios externos a una red interna y de usuarios internos al exterior, por lo que siempre su configuración se encontrará ligada a la política de seguridad de la compañía.

Estas políticas de seguridad deberán prevenir cualquier acceso no autorizado a la red como pueden ser los hackers o usuarios de una misma corporación para que no tengan acceso a ciertos recursos del sistema. Si usamos firewalls como pasarela a Internet éste podrá examinar el contenido y poseer la capacidad de decidir si es aceptable o no y si lo retransmitirá a su destinatario.

Los firewalls proveen las siguientes funciones:

- Servicio Network Address Translator (NAT): permite que un servidor que se encuentre en la Intranet se presente en Internet con un número IP válido sin necesidad de reconfigurarlo.
- Previenen de ataques.

- Pueden dividir la red en zonas con distintas necesidades de seguridad.
- Monitorizan el uso de Internet en cuanto a anchos de banda y problemas de saturación.

Un firewall puede ser un dispositivo software o hardware que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que se conecta a Internet.

El propósito de las redes con un firewall es mantener a los intrusos fuera del alcance de los trabajos que son propiedad privada. Muchas empresas usan en su sistema, un firewall como un lugar donde pueden almacenar información pública acerca de los productos de la empresa, ficheros que pueden ser recuperados por personal de la empresa y otra información de interés para los miembros de la misma.

Algunos firewall solamente permiten tráfico de correo a través de ellos, de modo que protegen de cualquier ataque sobre la red distinta de un servicio de correo electrónico. Otros proporcionan menos restricciones y bloquean servicios que son conocidos por sus constantes problemas de intrusión. Esto, ayuda principalmente, a prevenir actos de vandalismo en máquinas y software de la red.

El Firewall por Software es un Software que se puede instalar en la computadora. Son también llamados 'desktop firewall' o 'software firewall'.

Son firewalls básicos que monitorean y bloquean, siempre que sea necesario, el tráfico de Internet. Casi todas las computadoras vienen con un firewall instalado, Windows XP y Windows Vista lo traen.

Las características de un firewall por software son:

- Se incluyen con el sistema operativo y normalmente son para uso personal.
- Pueden ser fácilmente integrados con otros productos de seguridad.

- Es muy simple de instalar, normalmente ya viene activado y el Sistema Operativo alerta cuando no tenemos ningún tipo de firewall en funcionamiento.

Firewall por Software comercial funciona de la misma forma que uno gratuito (como el de Windows), pero normalmente incluye protecciones extra y mucho más control sobre su configuración y funcionamiento.

Las empresas que producen software de seguridad venden la aplicación firewall exclusivamente o como parte de un paquete de seguridad que incluye otros productos que complementan esta protección, como es el caso de los antivirus.

Firewall por Hardware viene normalmente instalado en los routers que utilizamos para acceder a Internet, lo que significa que las computadoras que estén detrás del router estarán protegidas por un firewall incluido en el dispositivo.

La configuración de un firewall por hardware es más complicada que una instalación de un firewall por software y es normalmente realizada a través del navegador que se utiliza para acceder a Internet.

Firewalls de nivel de aplicación generalmente son host con servidores proxy, que no permiten el tráfico directamente entre dos redes, sino que realizan un seguimiento detallado del tráfico que pasa por él. Los firewalls de nivel de aplicación pueden ser usados como traductores de direcciones de red; según pasa el tráfico de un lado a otro, enmascara la dirección de origen, lo que dificulta observar la topología de la red en el exterior. Estos sistemas proporcionan informes de auditoría más detallados que los firewalls de nivel de red; se usan cuando la política de control de acceso es más conservadora.

Aspectos de instalación de un firewall:

Se tiene en cuenta una serie de aspectos para la instalación de un firewall:

- Se define la política de seguridad que se quiere llevar a cabo, según los puertos a los que se permita acceder, ya que:

- Todo lo que no esté específicamente permitido se negará. Opción más segura.
- Todo lo no es específicamente negado se permite, no es muy usada ya que no se recomienda su uso en redes con conexión a Internet.
- Determinar el nivel de vigilancia, redundancia y control. Estableciendo un nivel de riesgo aceptable ya que como la efectividad de los firewall no es del 100%.
- El costo del firewall va en función de los servicios a filtrar y de la tecnología a emplear.

Aplicaciones de firewall:

- Aislamiento de Internet. Aislar la red privada de Internet, restringiendo el acceso a la red sólo a ciertos servicios, a la vez que se analiza todo el tráfico que pasa a través de ella. Si una red de una empresa se encuentra conectada a Internet, entonces todos los host pueden acceder a direcciones en el exterior y pueden ser igualmente accedidos desde fuera, presentándose un peligro a todo tipo de ataques, con que uno de los host sea accedido, toda la red será vulnerable. El firewall tendrá que permitir aquellos servicios que se consideren como seguros.
- Cuello de botella. El firewall se constituye en un cuello de botella que prohíbe aquellos servicios vulnerables; y sirve de protección ante algunos tipos de ataques. Se busca concentrar la administración y monitorización de la seguridad de la red en un solo punto en vez de intentar proteger a fondo cada una de las máquinas de la red.
- Auditoria y registro de uso. Con el firewall podremos recopilar información sobre el uso de la red, ya sea en el interior como desde el exterior. Con todos estos datos, se observa el tipo de tráfico, las horas de mayor carga de trabajo, el ancho de banda consumido.
- Seguridad de contenidos. Los firewall son vulnerables frente a los virus de computadora, aunque actualmente poseen filtros para detectarlos.

- Autenticación. La determinación de la identidad de las personas o entidades que acceden a la red se realiza mediante nombres de usuario y contraseñas, aunque no es una técnica muy fiable, por eso algunos cortafuegos permiten autenticarse utilizando métodos sofisticados, basados en tarjetas inteligentes, contraseñas de un solo uso, llaves de hardware, etc.
- Con la función ya mencionada antes de traducción de direcciones de red NAT (Network Address Translation) se puede ocultar el rango de direccionamientos internos de la empresa hacia el exterior, realizando una traducción de direcciones.

1.3.2 TRIXBOX DISTRIBUCIÓN LINUX PARA CENTRAL TELEFÓNICA VoIP

1.3.2.1 DEFINICIÓN

Trixbox es una distribución del sistema operativo GNU/Linux, basado en CentOS, que tiene la funcionalidad de ser una central telefónica por software utilizando Asterisk PBX. Permite interconectar teléfonos internos, softphones con la red telefónica convencional (RTB - Red telefónica básica).



Figura (1.25) Logo de la distribución TRIXBOX^[5]

Incluye características como creación de extensiones, envío de mensajes de voz a e-mail, llamadas en conferencia, menús de voz interactivos y distribución automática de llamadas. Al ser un software de código abierto, posee varios beneficios, como es la creación de nuevas funcionalidades. Además ofrece servicios VoIP, permitiendo así ahorros muy significativos en el costo de las llamadas internacionales, dado que éstas se realizan por Internet.

Trixbox es una distribución de fácil configuración e instalación que incluye FreePBX, una plataforma gráfica para configurar Asterisk facilitando la posterior

administración del sistema, y con las bondades de una interfaz web, también incluye un servidor Web Apache, con soporte a PHP y Perl, administración de Base de Datos, así como integración fax-a-email, autoconfiguración del hardware Zaptel de Digium y Text-to-Speech.

1.3.2.2 Componentes principales de TRIXBOX

1.3.2.2.1 CentOS

CentOS (Community ENTERprise Operating System) es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat.

Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública, bajo los términos de la licencia pública general de GNU. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat.

Las utilidades para la programación en GNU tienen capacidad para compilar C, C++, Java, Ada, entre otros muchos lenguajes. CentOS es la distribución de Linux que sirve como Sistema Operacional en Trixbox.

1.3.2.2.2 ASTERISK

Asterisk fue concebido y desarrollado por Mark Spencer. En un principio por una necesidad personal pues necesitaba una central telefónica para la pequeña empresa de soporte que estaba fundando, llamada "Linux Support Services". Inicialmente pensó en adquirir una pero pronto se dio cuenta que estaba muy lejos de su presupuesto, así que luego de pensarlo un poco decidió crear la suya y comenzó a codificar lo que hoy conocemos como Asterisk. En 1999, cuando tuvo un código digno de mostrar al mundo decidió liberarlo bajo licencia GPL.

En cierto momento Mark se dio cuenta de que su software necesitaba interactuar con hardware telefónico y se topó con el proyecto Zaptel, un proyecto de código abierto creado por Jim Dixon, que tenía el objetivo de crear drivers abiertos para tarjetas telefónicas de computadora. A partir de allí Asterisk y Zaptel caminarían de la mano; tanto así que en la actualidad los dos proyectos son mantenidos por la misma compañía. En el 2002 Linux Support Services se convertiría en Digium, quien actualmente ofrece productos y servicios relacionados con Asterisk y se encarga del desarrollo del producto. Asterisk es un software que emula a una central telefónica que se distribuye bajo licencia libre. Asterisk da conectividad en tiempo real a redes PSTN y de VoIP, incluyendo características de sistemas de mensajería unificados de última generación, como:

- Música en espera para los clientes que esperan en cola, soportando streaming así como música MP3.
- Integración de sistemas Text-to-speech, es decir la reproducción, por medios automáticos, de una voz artificial que genera sonido idéntico al producido por una persona al leer un texto en voz alta.
- El registro detallado de llamadas de Asterisk (CDR) para la integración con los sistemas de facturación.
- Integración con sistemas de reconocimiento de voz.

Los PBX emuladas con Asterisk tienen la posibilidad de establecer conexiones de trunking entre varias oficinas usando un protocolo especial de Asterisk (IAX). Este protocolo soporta muchas conexiones simultáneas y trabaja fácilmente sobre conexiones NAT. De esta manera, se pueden realizar ruteos de bajo costo para las llamadas y tener balanceo de carga entre los servidores Asterisk de una red.

Características

Asterisk es una Central avanzada que maneja interconexión interna del PBX, utiliza protocolos específicos, códecs, e interfaces de hardware de aplicaciones de telefonía. Esto le permite al Asterisk utilizar cualquier hardware conveniente y tecnología disponible, para realizar sus funciones esenciales, conectando hardware y aplicaciones. Internamente Asterisk maneja módulos que le permiten

integrar hardware de telefonía y tecnología de paquetes de voz y son los siguientes:

- **PBX SWITCHING:** Sistema de conmutación de intercambio de rama privada (PXB). La base de conmutación conecta a los usuarios llegando a varios de ellos mediante software y hardware de interfaz.
- **LANZADOR DE APLICACIONES:** Envía aplicaciones que mejoran servicios para usos tales como, correo de voz, archivos, grabaciones y lista de directorio.
- **TRADUCTOR DE CÓDECS:** Usa módulos de códecs para codificar y decodificar varios formatos de compresión de audio usadas en la telefonía.
- **MÓDULOS CARGABLES API(Attachment Packet Interface):**
 - **CANAL API:** El canal API maneja el tipo de conexión al cual el cliente está llegando, sea una conexión VoIP, RDSI, o algún otro tipo de tecnología.
 - **APLICACIÓN API:** Esta aplicación permite a varios módulos de tareas cumplir varias funciones, conferencias, lista de directorios, correo de voz en la línea de transmisión de datos y cualquier otra tarea que la PBX sea capaz de cumplir.
 - **TRADUCTOR DEL CÓDEC API:** Carga módulos de códecs para apoyar varios tipos de audio, codificando y decodificando formatos tales como wav, mu-law, a-law, e incluso mp3.
 - **FORMATO DE ARCHIVO API:** Maneja la lectura y escritura de varios formatos de archivos para el almacenaje de datos en el sistema de archivos.

Asterisk basado en soluciones de telefonía ofrece un variado y flexible set de características. Además ofrece funcionalidades básicas de PBX y características más avanzadas, así como también es interoperable con sistemas básicos de telefonía estándar y sistemas VoIP.

CARACTERÍSTICAS DE LLAMADAS:

- Receptor de alarma.

- Añade mensajes.
- Auto identificación.
- Monitoreo de llamadas.
- Llamadas en espera.
- Grabación de llamadas.
- Recuperación de llamadas.
- Guía de llamadas (DID y ANI).
- Transferencia de llamadas.
- Identificación de usuarios.
- Bloque de identificación de usuarios.
- Identificación de usuarios en llamadas de espera.
- Conferencias.
- Recuperación de base de datos almacenados.
- Marcado por nombre.
- Acceso directo al sistema interno.
- Mensajes SMS.
- Correo de voz.
 - Indicador visual para los mensajes en espera.
 - Correo de voz a emails.
 - Grupos de correos de voz.
 - Interfaces de web a correos de voz.

1.3.2.2.3 FreePBX

FreePBX es un software que permite la configuración de Asterisk que ha sido integrado como parte de Trixbox, se encarga de generar los archivos de configuración de Asterisk incluido el plan de marcado en base a la configuración ingresada por el usuario desde la Web.

Para realizar esta tarea FreePBX la divide en dos pasos:

- 1) Recaba la configuración deseada por el usuario en una base de datos de configuración. En el caso de Trixbox se usa el motor de base de datos MySQL.
- 2) Luego convierte esa información almacenada en MySQL principalmente en archivos de configuración a través de una herramienta de análisis de texto llamada `retrieve_conf`.

Permite configurar fácilmente un sistema Asterisk, cubriendo los requisitos tanto de pequeñas como de grandes empresas. Puede mantener las bases de datos de usuarios y extensiones, así como las funciones de valor añadido. Por citar las más importantes:

- Plan de marcado de llamadas entrantes y salientes.
- IVR (Recepcionista digital interactiva) operadora automática.
- Gestión de llamadas entrantes según horario y fecha.
- Grupo de llamadas.
- Sistema de colas.
- Monitorización de llamadas.
- Sistema de mensajería.
- Música en espera.
- Conferencias.
- Grabación de las llamadas.

Organización de archivos de FreePBX

Directorio	Descripción
<code>/var/www/html/admin/</code>	El directorio principal donde reside el GUI (interfaz gráfica de usuario) de freePBX.
<code>/var/www/html/panel/</code>	Directorio del Flash Operator Panel.
<code>/etc/asterisk/</code>	El directorio donde residen los archivos de configuración de Asterisk que escribe FreePBX.
<code>/var/lib/asterisk/agi-bin/</code>	Aquí se encuentran los <i>scripts</i> AGI (interfaz entrada de Asterisk). FreePBX cuenta con algunos <i>scripts</i> en esta carpeta como el <code>dialparties.agi</code> .
<code>/var/lib/asterisk/bin/</code>	Algunos binarios utilizados por freePBX. Algunos de ellos son links simbólicos a las carpetas de los módulos.

Directorio	Descripción
<code>/usr/local/sbin/</code>	Aquí reside el <i>script</i> amportal. Se encuentra en esta carpeta porque puede ser manipulado solo por root.
<code>/var/lib/asterisk/sounds/</code>	Aquí residen los sonidos que se utilizan en el plan de marcado por freePBX.
<code>/var/lib/asterisk/sounds/custom/</code>	Aquí residen los sonidos que han sido creados por el usuario. Por ejemplo cuando se crea un IVR de bienvenida.
<code>/var/spool/asterisk/voicemail/</code>	Directorio donde se almacenan los <i>correos de voz</i> .
<code>/var/spool/asterisk/monitor/</code>	En este directorio se almacenan las grabaciones de voz.
<code>/var/log/asterisk/cdr-csv/</code>	Directorio donde se escriben los CDRs en formato texto.

Tabla (1.4) Organización de archivos del FREEPBX. ^[6]

1.3.2.2.4 *Flash operator panel (FOP)*

Flash Operator Panel muestra información sobre la actividad de las llamadas en tiempo real a través de un navegador web estándar de Asterisk. También se puede tener un servidor que ejecuta y muestra diferentes clientes. Puede monitorear varios servidores Asterisk a la vez. Se puede ver:

- Las extensiones que están ocupadas, timbrando o disponibles.
- La extensión que se encuentra llamando y al número que llama.
- SIP estado de registro y asequibilidad.
- Estado de cola (número de usuarios en espera).
- Indicador de mensaje en espera y cuenta.
- Detalles de la última llamada.

1.3.2.3 **Hardware y software compatible con Asterisk en Trixbox**

Para la interconexión con equipos telefónicos analógicos o digitales, Asterisk soporta un gran número de dispositivos de hardware, en especial todo el hardware manufacturado por Digium, patrocinador de Asterisk. Se tienen interfaces desde 1 hasta 8 E1s para interconexión de líneas E1 PRI, también se tienen tarjetas de 4, 8 y 24 puertos para la conexión de líneas y anexos analógicos.

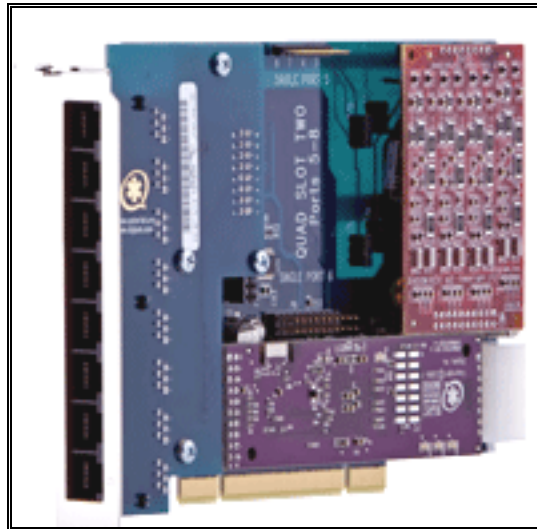


Figura (1.26) Muestra una tarjeta Digium 8 puertos.^[2]

Asterisk se enlaza con las conexiones de telefonía analógica y digital a través de una tarjeta de puerta de enlace que está instalado en el PC o a través de un dispositivo de puerta de enlace externo.

Las tarjetas de puerta interior de enlace generalmente se conectan a través del bus del equipo de expansión interna. Las tarjetas están disponibles en la forma de "PCI" y "PCI Express", los gateways externos se conectan con el Asterisk en la red de área local (LAN) o el bus USB del PC.

Tarjetas Digitales

Las tarjetas digitales permiten conectar Asterisk con T1, E1 y J1 líneas digitales, pueden ser de uno o más puertos, cada uno de ellos se conecta a un circuito digital individual.

La mayoría de tarjetas digitales se conectan mediante conectores RJ-45 (el mismo tipo de conector que se utiliza comúnmente para conexiones Ethernet). Las conexiones entre la tarjeta y una compañía de teléfonos de línea E1 se conectan utilizando un dispositivo "integrado" por cable.

Tarjetas analógicas

Las tarjetas analógicas están disponibles en varias capacidades, que van desde un solo puerto (que conecta una línea telefónica analógica y por lo tanto una

llamada telefónica) hasta un máximo de 24 puertos, generalmente utilizan el mismo tipo de conector, el conector RJ-11. Cada toma de la parte posterior de la tarjeta tiene un terminal para el conector RJ-11 del teléfono y el otro extremo del cable está conectado a un teléfono o a un puerto análogo en el PBX.

Para su funcionamiento utilizan ciertas interfaces de conexión:

Interfaz FXS

También denominada interfaz de abonado. Es el que envía la línea analógica hacia el abonado. Se trata de interfaces que permiten conectar dispositivos terminales, como un teléfono. Una interfaz FXS proporciona alimentación eléctrica, señalización de llamada y tono al dispositivo terminal. Estas interfaces son las que permiten conectar un teléfono analógico convencional a un router o central de telefonía IP.



Figura (1.27) Muestra el módulo FXS

Interfaz FXO

Es el puerto que recibe la línea analógica, es decir la interfaz que permite conectar un dispositivo terminal a un servicio de telefonía como el servicio de telefonía pública (PSTN) o una PBX. Se encarga de enviar al sistema telefónico una señal de colgado o descolgado (cierre de bucle). FXS y FXO son siempre pares que se corresponden mutuamente: una interfaz FXS se conecta en el otro extremo de la línea a una interfaz FXO.



Figura (1.28) Muestra de un módulo FXO

Las tarjetas analógicas y digitales disponibles en Digium para Asterisk son:

Tarjetas	Descripción
Wildcard TDM400p	Un puerto cuadrangular FXS tarjeta de interfaz PCI para interconectarse con teléfonos análogos estándar y o teléfonos ADSI.
Wildcard X100p	Un solo puerto FXO tarjeta de interfaz PCI para interconectarse con líneas de teléfonos análogos estándar.
Wildcard TE410P	Un palmo cuadrangular de media longitud T1/E1/PRI, tarjeta PCI que ayuda a ambos, telefonía y modos de datos en formato T1 o E1 sobre una base de puerto seleccionable. (Solo 3.3voltios PCI).
Wildcard TE405P	Tarjeta digital con 5.0 voltios PCI.
WildcardT100P	Un solo palmo T1 de media longitud (disponible con soporte 2u) tarjeta PCI portando las mismas características que el TE410P.
WildcardE100p	Tarjeta digital E1.
X100P GENERIC	Clon de la tarjeta Wildcard X100P desarrollado por intel. Este producto no incluye servicio técnico.

Tabla (1.5) Tarjetas Digium utilizadas en servidores VOIP^[3]

TELÉFONOS ANALÓGICOS

Los teléfonos analógicos utilizan la primera tecnología telefónica que convierte las vibraciones del aire en frecuencias eléctricas analógicas. Incluso hoy en día, a

menos que se utilice un sistema telefónico de teclas, un PBX digital o voz sobre IP (VoIP), la mayoría de los hogares y las pequeñas oficinas siguen usando teléfonos analógicos.

TELÉFONOS IP

Un teléfono IP utiliza tecnologías de Voz sobre IP, lo que permite que las llamadas telefónicas se realicen sobre una red IP, utilizando protocolos de control, tales como SIP (Session Initiation Protocol), Skinny Client Control Protocol o uno de varios protocolos propietarios, como el utilizado por Skype. Los teléfonos IP pueden ser simples Softphones basados en software o dispositivos de hardware contruidos expresamente que se parecen mucho a un teléfono normal o un teléfono inalámbrico.



Figura (1.29) Teléfono IP^[9]

SOFTPHONES

Un Softphone es un software que hace una simulación de teléfono convencional por computadora. Es decir, permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales usando un VSP (Proveedor de servicio de VoIP).

Normalmente, un Softphone es parte de un entorno Voz sobre IP y puede estar basado en el estándar SIP/H.323 o ser privativo. Hay muchas implementaciones disponibles como Microsoft Windows Messenger o NetMeeting.

Los Softphone típicos basados en SIP actualmente comprenden: eyeBeam de CounterPath (anteriormente Xten figura 1.29), OpenWengo, Nexge, sipXphone, Adore Softphone, Express Talk (figura 1.29), Zoiper, y SJphone. Se puede

conectar usando un teléfono USB o un enlace usb a un SoftPhone y obtener un servicio gratuito VoIP de teléfono a teléfono.



Figura (1.30) Softphone XTEN, EXPRESS TALK^[9]

Al realizar una llamada en un softphone, se utiliza un entorno de centro de llamadas, para comunicarse desde un directorio de clientes. En estos casos la información del cliente aparece en la pantalla de la computadora cuando el teléfono suena, mostrando determinada información sobre quién está llamando, advirtiéndolo cómo recibirlo y dirigirse a esa persona.

ADAPTADORES ATA

Un ATA consiste en una pequeña caja que se intercala entre un teléfono analógico regular y la red IP. A pesar de su pequeño tamaño y bajo costo, en su interior tiene un UA (Agente de Usuario) para la señalización SIP, más una pequeña tarjeta electrónica con un códec para adaptar los contenidos de voz o telefax entre el lado IP y el terminal analógico. De hecho, la parte electrónica de un ATA es similar a la de un teléfono IP, con su pequeño procesador, sistema operativo y servidor web para facilitar la configuración.

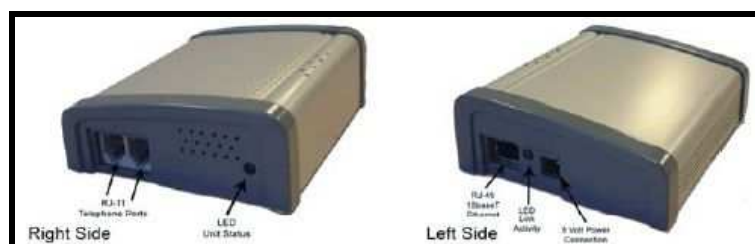


Figura (1.31) Adaptador ATA^[9]

1.3.3 SOFTWARE COMPATIBLE CON LA TECNOLOGÍA X-10

1.3.3.1 HEYU

Heyu es un programa basado en consola completamente libre que tiene a la disposición el código fuente en su página web <http://www.heyu.org>, este programa permite enviar señales de apagado y encendido de aparatos electrónicos, aumento de brillo en caso de lámparas.

Heyu para su funcionamiento utiliza el convertidor serie CM11A o CM17A que actúa como un interfaz entre la aplicación y los módulos X10 a través del puerto serial del PC, enviando señales de control de los dispositivos X10 sobre las líneas de corriente, para poder encender, apagar dar grados de intensidad a lámparas y aparatos electrónicos.

Si utiliza el interfaz CM11A este software es capaz de almacenar un calendario de eventos con hora en la memoria CM11A para su ejecución cuando el ordenador está apagado o desconectado.

Heyu admite a dispositivos adicionales de control como el MR26A o receptor RF conectado a un segundo puerto como un dispositivo de entrada auxiliar para señales de RF de X10 y otros transmisores compatibles.



Figura (1.32): logo HEYU ^[12]

Características

- Altamente configurable y capaz de transmitir y recibir señales X10 con el apoyo del módulo CM11A.
- Con el uso del CM17A solo puede enviar señales de control X10.
- Puede mantener un registro del estado (On, Off, el nivel Dim) de módulos basados en las señales recibidas o transmitidas X10.

- Control de múltiples CM11A interfaces conectadas a los distintos puertos de serie en el mismo equipo.
- Con un dispositivo opcional CM17A, se puede transmitir señales de RF X10 a un transceptor para la conversión de las señales de línea de energía (posiblemente en una rama separada de la línea de CA), o para un receptor RF X10 conectado a un equipo diferente.

Requisitos

Sistema Operativo

Heyu es desarrollado y usado bajo Linux.

Hardware

El CM11A es fabricado por X10 (USA) y distribuido como parte del kit CK11A ActiveHome. También se vende bajo el nombre de IBM HD11 Home Director y la RCA HC60CRX Home Control Interface, para su funcionamiento se conecta a una toma de CA y se conecta al ordenador a través de un puerto serie RS232.

Heyu integra soporte para el X10 CM17A "Firecracker", un pequeño dispositivo serie que transmite señales de RF X10. (El CM11A y el CM17A coexisten en el mismo puerto serie – no necesitan ningún puerto adicional.)

El soporte técnico para Heyu se proporciona a través del foro heyu_users del grupo Yahoo, desarrolladores y miembros de la Comunidad de Usuarios Heyu, Donde se reciben y responden a las preguntas relacionadas a Heyu, brindando ayuda con errores y dando soluciones a nuevas funcionalidades. Cualquier nuevo avance o temas de innovación sobre Heyu son publicados allí.

1.3.3.2 MOTION



Figura (1.33): logo MOTION ^[13]

Motion es un programa que monitoriza la señal de vídeo de una o más cámaras y es capaz de detectar si una parte significativa de la imagen ha cambiado, es decir, se puede detectar el movimiento.

El programa está escrito en C y se hace para el sistema operativo Linux. Motion es una herramienta de línea de comandos basada en jpeg, mpeg o secuencias de vídeo. Motion es la herramienta perfecta para mantener un ojo en su propiedad, manteniendo sólo las imágenes que son interesantes.

Algunas de las características de motion son las siguientes:

- Toma fotos de movimiento
- Añade a múltiples dispositivos de vídeo al mismo tiempo
- Añade múltiples entradas de tarjeta de captura al mismo tiempo
- Webcam en directo de streaming
- La creación en tiempo real de MPEG películas usando las bibliotecas de ffmpeg
- Toma instantáneas automáticas a intervalos regulares
- Toma instantáneas automática a intervalos irregulares utilizando cron
- Ejecutar comandos externos cuando se detecta movimiento (y por ejemplo, enviar SMS o correo electrónico)
- Seguimiento de movimiento (la cámara sigue el movimiento - hardware especial requerido).
- Control a través del navegador
- Control automático de ruido y control de umbral
- Motion es un demonio con un bajo consumo de CPU y la huella de memoria pequeña.

La detección de movimiento

Motion detecta el movimiento mediante la comparación de la intensidad de los píxeles de una imagen fresca con una imagen de referencia. Si no hay movimiento ni ruido `new_image ref_image` debe ser cero.

Si ha habido un cambio en la imagen el resultado será diferente. Para evitar ruidos en la imagen como el movimiento del cambio debe superar un umbral y

tiene que haber un cierto número de píxeles cambiado antes de que un movimiento es declarado. Motion no hace uso del color en la detección de movimiento.

Webcam

Desde la versión 3.0.0 Motion tiene una cámara web incorporada. Esto se hace con un mini servidor http que sirve las imágenes jpeg con el tipo MIME (serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos). Esto puede ser visto con navegadores como firefox y otros.

CAPÍTULO 2. ANÁLISIS DE LA SITUACIÓN ACTUAL Y VIABILIDAD DE LA IMPLEMENTACIÓN DEL PROTOTIPO DE UNA CENTRAL DOMÓTICA VOIP.

2.1 INTRODUCCIÓN

Este capítulo analiza la situación actual de las tecnologías necesarias para la implementación de la central domótica VoIP como el internet, VoIP y la tecnología X10. Además un estudio sobre la viabilidad de su implementación en el Ecuador, detallando aspectos como el desarrollo tecnológico, tipos y condiciones del cableado eléctrico, grado de aceptación en el mercado.

2.2 SITUACIÓN ACTUAL DE LA DOMÓTICA

La situación actual de la domótica varía en función del área geográfica considerada. En EEUU está orientado hacia el hogar interactivo, con servicios tales como el teletrabajo o la tele enseñanza. Mientras en Japón se busca alcanzar el máximo nivel de confort, con un hogar automatizado, incorporando al máximo aparatos electrónicos de consumo (televisores, radios, hornos microondas, etc).

El sector domótico en Europa se encuentra en un proceso de expansión y desarrollo exponencial, donde se da una aceptación generalizada. A la domótica, se unen otras ramas de la tecnología como la telefonía móvil, el Internet, la informática, la VoIP útiles para su implementación permitiendo el crecimiento de este sector.

Los beneficios que se pueden ofrecer en la domótica son varios, siendo un tema desconocido por muchos, al hablar de casas inteligentes se puede evidenciar que para la mayor parte de la sociedad la domótica es considerada como un servicio de exclusividad y sobre todo de altos costos. Esta falta de información ha generado en el usuario, una definición errónea sobre la domótica, por ejemplo considerarlos sistemas caros, de difícil programación, de poca utilidad, etc., siendo todo lo contrario es un nuevo servicio para el hogar.

2.3 ESTUDIO PARA LA VIABILIDAD DEL PROTOTIPO DE LA CENTRAL DOMÓTICA VoIP

2.3.1. ESTUDIO DEL DESARROLLO TECNOLÓGICO EN EL ECUADOR

El diseño e implementación de una red domótica implica que el usuario pueda tener acceso a ciertas tecnologías, como el acceso a internet, ya que será la vía de comunicación para controlar estos sistemas, también es importante conocer otros datos estadísticos que reflejen la situación tecnológica actual en el Ecuador. El acceso al servicio de internet y a la adquisición de productos tecnológicos en el Ecuador es bajo, casi inaccesible debido a sus altos costos, es el reporte según un estudio estadístico realizado por el INEC.

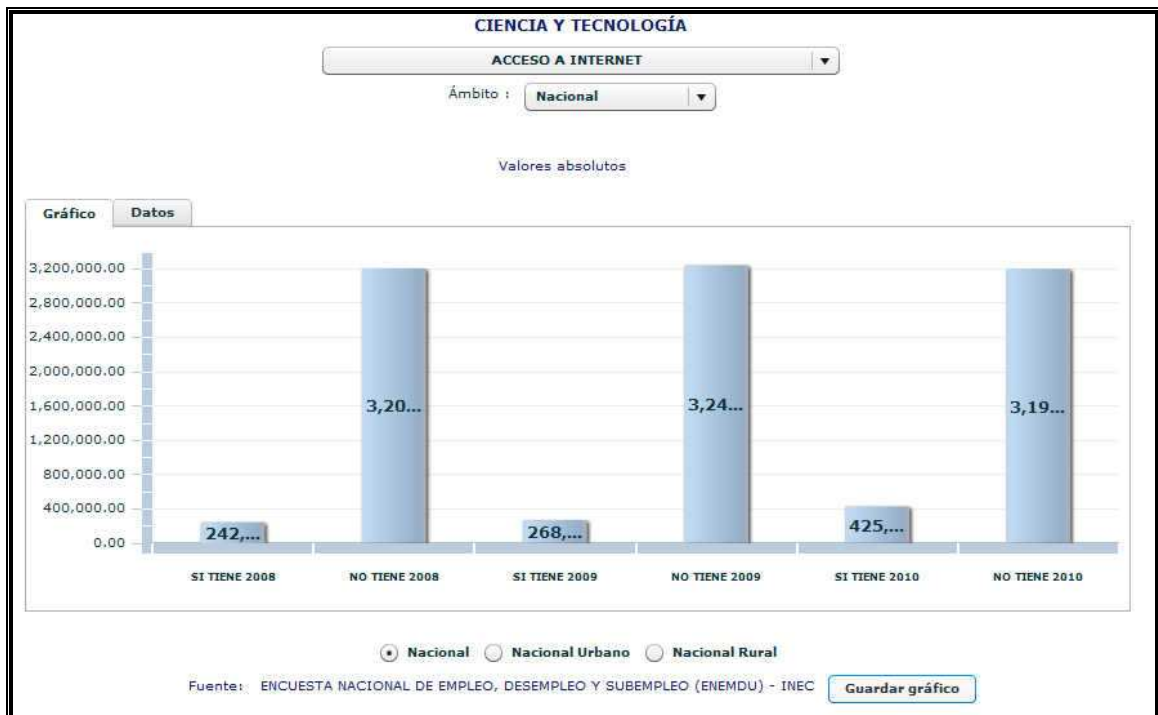


Figura (2.1.): Cuadro estadístico general del acceso internet en el Ecuador [2]

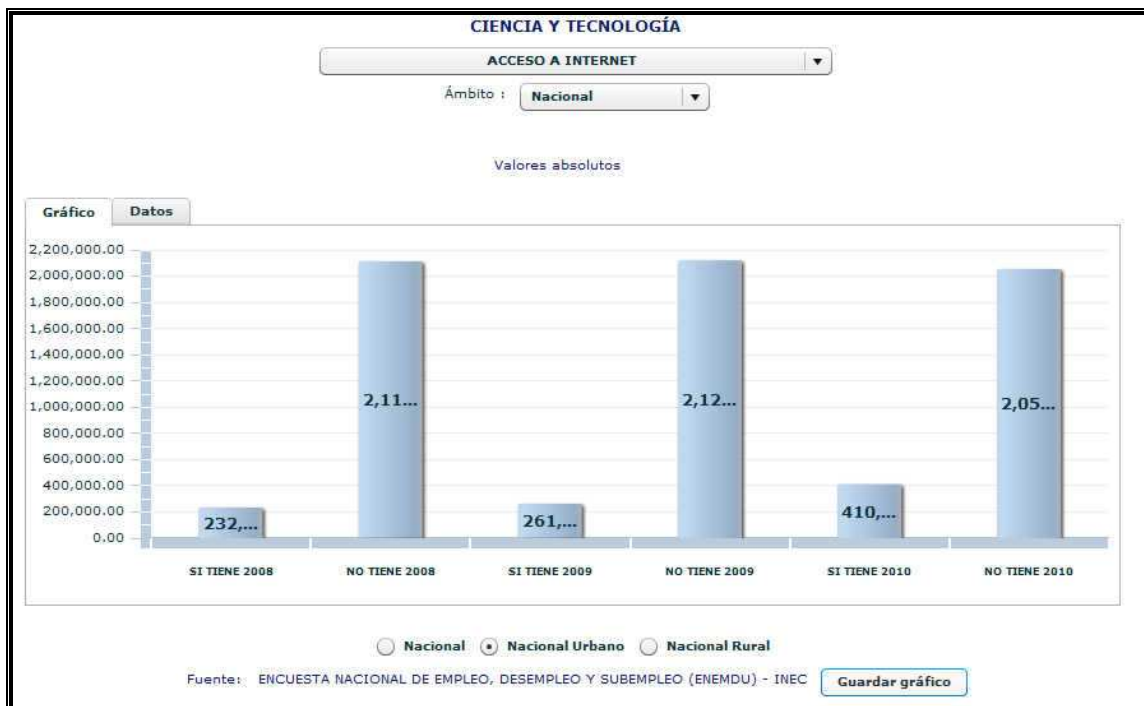


Figura (2.2.): Cuadro estadístico del área urbana del acceso internet en el Ecuador [2]

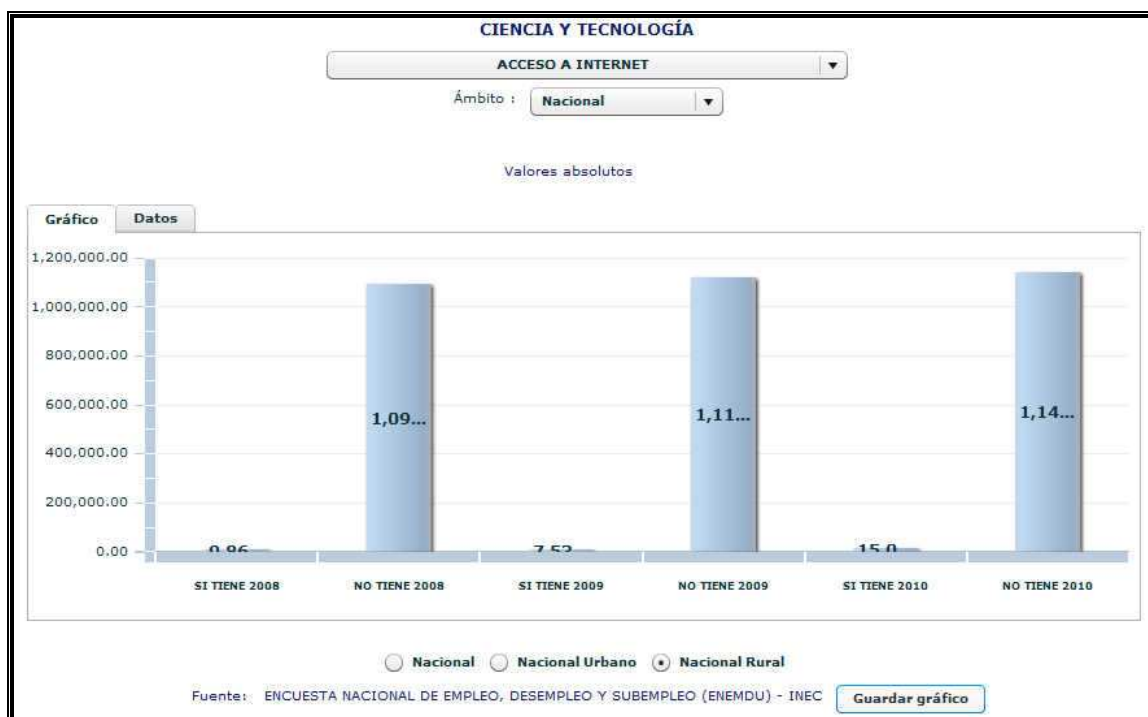


Figura (2.3.): Cuadro estadístico del acceso internet del área rural en el Ecuador [2]

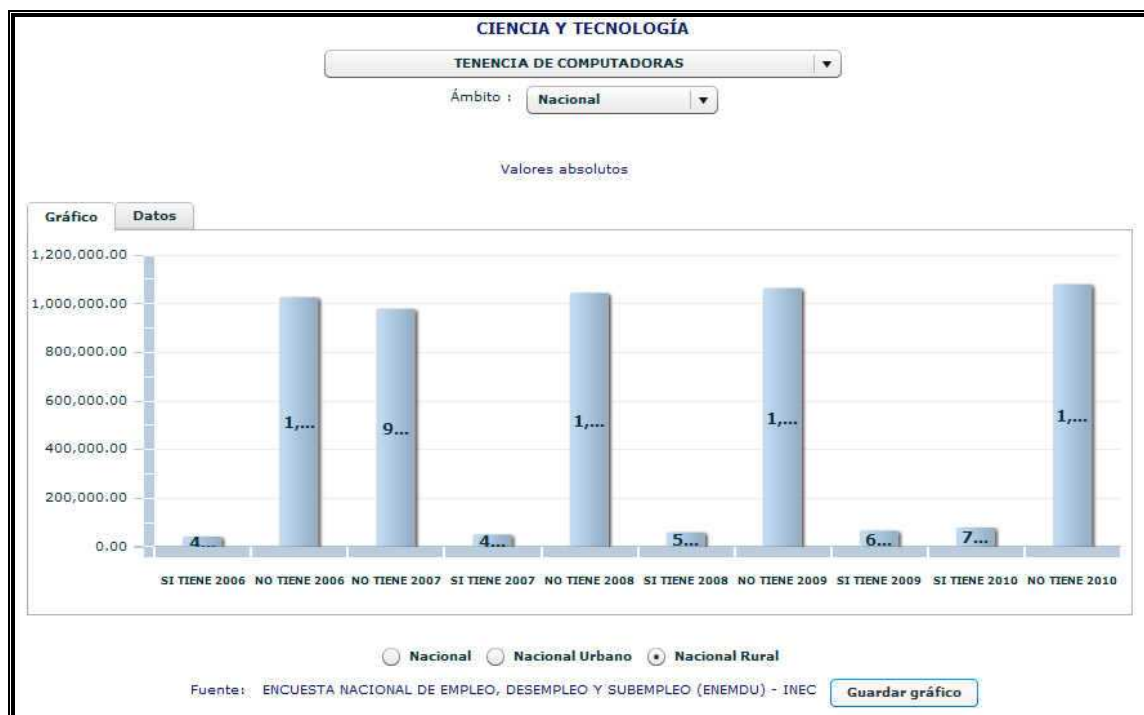


Figura (2.4.): Cuadro estadístico general sobre la tenencia de computadores en el Ecuador [2]

Según el INEC (Instituto Nacional de Estadísticas y Censos), en su último estudio realizado en el año 2010 en el área de Ciencia y Tecnología, muestra que casi el 7 % de la muestra poblacional tiene acceso a internet. Al estudiar por sectores se obtiene que en el área urbana nacional alrededor del 6.3% tiene acceso a internet, mientras que en el sector rural no se alcanza ni el 1 % de población que pueda acceder a este servicio, se estima que en nuestro país el acceso a la tecnología tiene un índice muy bajo y es para un sector de la población con una cierta ventaja económica.

Al igual que el acceso a internet, el porcentaje de ciudadanos que puede adquirir productos tecnológicos como un computador está en la misma relación, cabe notar que Ecuador es el último país de América Latina en el ranking de exportaciones de productos de media y alta tecnología como porcentaje del total de las exportaciones.

El Programa de Desarrollo de las Naciones Unidas (PNUD) reporta en el 2010, que Brasil es el país de América latina que lleva la delantera en inversión tecnológica, Brasil invierte cerca del 1% de su producto bruto en investigación y

desarrollo, mientras que Chile invierte el 0,5%; México, Argentina y Venezuela, el 0,4% cada uno, y Colombia, Ecuador y Perú, el 0,1% cada uno.

El Foro Económico Mundial (FEM) presenta el Informe Global sobre Tecnología 2007-2008, que lleva por subtítulo “Fomentando la Innovación mediante la Preparación en la Red”, financiado por Cisco Systems, y realizado en 127 países, indica que nuestro país se encuentra en la posición 107 del ranking mundial de desarrollo tecnológico.

2.3.2. ANÁLISIS DEL CABLEADO ELÉCTRICO EN EDIFICACIONES.

El tipo de cableado eléctrico de una edificación sobre la cual se va a implementar la central domótica VoIP es un parámetro determinante para su diseño, ya que puede generar complejidad al proyecto o brindar la facilidad para el desarrollo del mismo.

Si la vivienda o edificación será construida ayuda a la implementación de la central domótica, porque en los planos de la construcción se tomará en cuenta, todas las normas internacionales establecidas para la instalación eléctrica y así garantizar el uso correcto de los módulos X10, ya que estos utilizan la línea eléctrica (110V) para transmitir señales de control de automatización entre sí, mientras en una vivienda construida, es donde se pueden presentar inconvenientes, ya que por lo general las edificaciones no cumplen con las normas de cableado eléctrico, llevando un desorden en sus instalaciones, e impidiendo la aplicación de esta tecnología cuya comunicación es realizada a través de la misma línea eléctrica, entonces es necesario instalar un cableado eléctrico alterno para utilizar los módulos X10.

2.3.3. EQUIPOS (FACILIDAD DE USO, COSTOS Y BENEFICIOS).

Un punto donde destaca el protocolo X10 así como KNX, LonWorks y otros, es por su amplia difusión y aplicaciones en este mercado. X10, es ampliamente usada por su sencillo protocolo de comunicación, sus dispositivos son fáciles de manejar, ofrecen control y automatización de equipos en nuestro hogar, a pesar de sus limitaciones como el ancho de banda, aun así, son muy útiles debido a su bajo costo. En cambio LonWorks y KNX ofrecen ciertos beneficios como mayor

ancho de banda y son usados para la implantación de servicios domóticos más complejos, pero sus dispositivos tienen elevados costos.

2.3.4. ANÁLISIS DE MERCADO (ENCUESTA)

Fue necesario establecer un método correcto para el análisis del mercado, para esto se consideró los siguientes factores:

La domótica en los países desarrollados avanza firmemente, y los nuevos diseños arquitectónicos prestan atención a los beneficios que esta tecnología ofrece antes de empezar sus construcciones. Pero aun así las expectativas que se preveían para la incorporación de sistemas domóticos en el diseño y construcción de viviendas no han cubierto los índices de mercado esperados. En Ecuador el mercado de la domótica es muy reducido, las empresas dedicadas a esta área en su mayoría importan productos domóticos, por lo cual es difícil obtener un historial con datos estadísticos definidos de productos similares y sus ventas.

El internet y el uso de ordenadores para acceder a este servicio, día a día van tomando más espacio entre la sociedad, como se vió en el estudio de desarrollo tecnológico en el Ecuador, en nuestro país el índice de acceso a tecnología va incrementándose y a su vez convirtiéndose en una necesidad básica para los usuarios, al tener todo este conjunto de dispositivos en el hogar, es fácil considerar la implementación de una central domótica que permita su automatización y control.

Además los datos brindados por la Asociación de Empresas de Seguridad Integral e Investigación Privada (ANESI) de Ecuador, da a conocer que existen más de 700 empresas de seguridad en el país, pero tan solo el 10% de estas empresas trabajan con monitoreo electrónico desde hace 10 años aproximadamente. Entre las empresas líderes en el campo de seguridad por monitoreo electrónico están Wackenhut, VICOSA y Respuesta Armada.^[3]

Obteniendo así que el método cualitativo de demanda es el más apto en este caso, para realizar un pronóstico del mercado del producto, ya que las técnicas cualitativas se usan cuando los datos son escasos, y son útiles para pronósticos a largo y mediano plazo, pronósticos de ventas y desarrollo de nuevos productos,

inversiones de capital, planeación estratégica y pronósticos tecnológicos, con el riesgo de que el mercado puede ser variable y estos pueden fallar.

Dentro de las opciones de métodos cualitativos se halla la encuesta, para el producto se realizó una encuesta a posibles clientes, se tomó una muestra de 40 personas profesionales y afines al área, que tengan noción sobre el tema expuesto, y se la ejecutó vía internet a través de la herramienta proporcionada por gmail para la elaboración de encuestas, al llevarla a cabo se creó un producto ficticio llamado EASYHOME que es la central domótica VoIP basado en la distribución del sistema operativo GNU/Linux "Trixbox" usando la tecnología X10 para ofrecer servicios de confort y seguridad en el hogar, el formato de la encuesta se encuentra en el anexo A.1,

Objetivo del producto:

"EASYHOME" es un producto innovador que le proporciona todos los elementos necesarios para automatizar y gestionar su hábitat, desde la instalación de sistemas básicos para la detección de gas, fuego, agua, etc., hasta sistemas de control de electrodomésticos, creación de ambientes para su confort y sistemas de vigilancia, brindando con éxito seguridad y confort en su hogar, para obtener estos servicios, el usuario podrá acceder vía remota desde cualquier PC o vía telefónica.

La prioridad al ofrecer EASYHOME es la satisfacción del cliente, disponiendo para tal efecto de nuevas tecnologías usadas en el diseño de una central domótica que engloba varios servicios. Además ofrece una serie de ventajas a los usuarios como:

- Sencillez de manejo y configuración.
- Capacidad de crecimiento en servicios según sus necesidades de confort o seguridad.
- Mantenimiento necesario para el sistema durante la vida del producto.

Resultados:

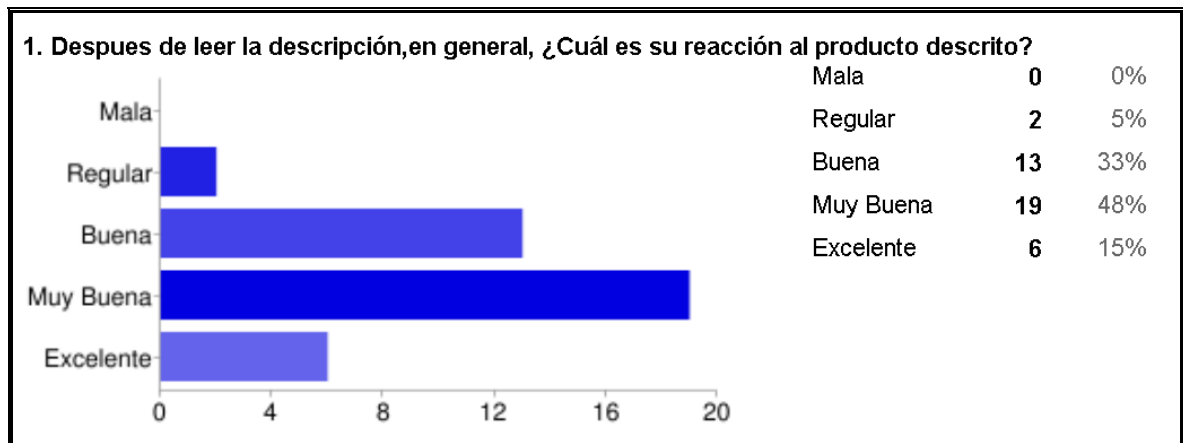


Figura (2.5.): Resultados de la encuesta pregunta 1

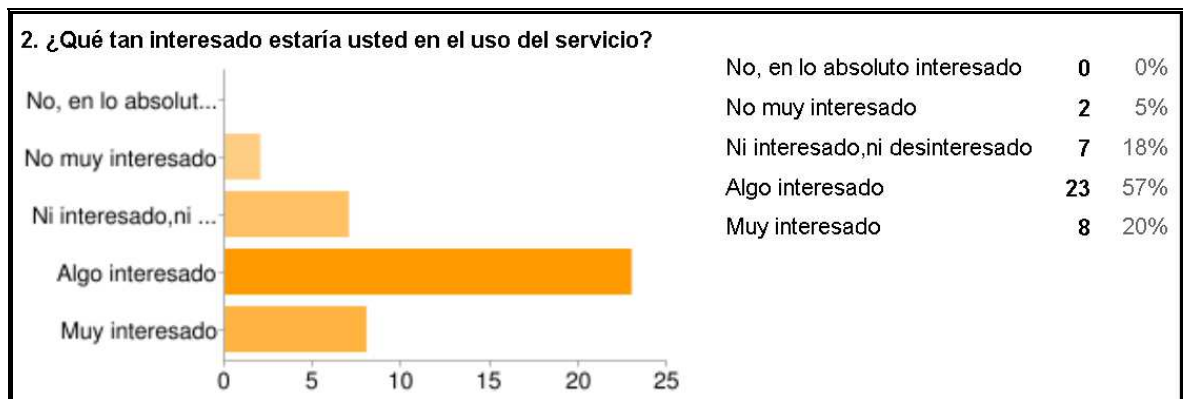


Figura (2.6.): Resultados de la encuesta pregunta 2

Los resultados obtenidos en las preguntas 1 y 2 de la encuesta respecto a su grado de aceptación frente al prototipo EASYHOME indican que el 96% de los encuestados cree que sus características están entre excelentes, buenas y muy buenas, de los cuales el 77 % se encuentra interesado en el uso del mismo, mientras el resto de encuestados no mostraron ningún interés por EASYHOME, esto se puede observar en la figura 2.5 y 2.6 en donde se encuentra en forma gráfica la tabulación de los datos.



Figura (2.7.): Resultados de la encuesta pregunta 3

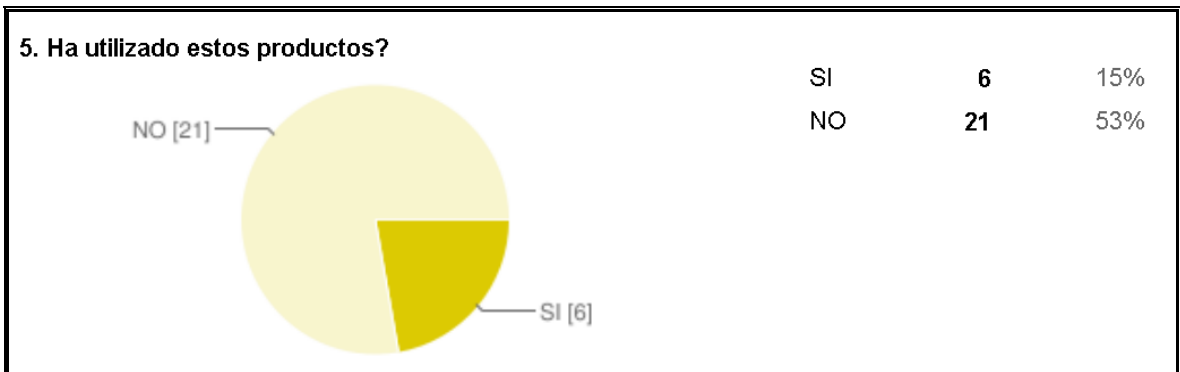


Figura (2.8.): Resultados de la encuesta pregunta 5

Las preguntas 3, 4, 5, 6 y 7 dan información sobre el conocimiento, uso, marcas, beneficios y desventajas de productos domésticos similares a EASYHOME, el 18% conocía de productos similares y de entre ellos el 15 % los había utilizado. Al recoger sus opiniones, la mayoría los había usado por curiosidad y por tener confort en su hogar, además expresaron que al usarlos sintieron una invasión por parte de la tecnología en las actividades del ser humano, que tenían poca información sobre el tema y que pagaron altos costos.

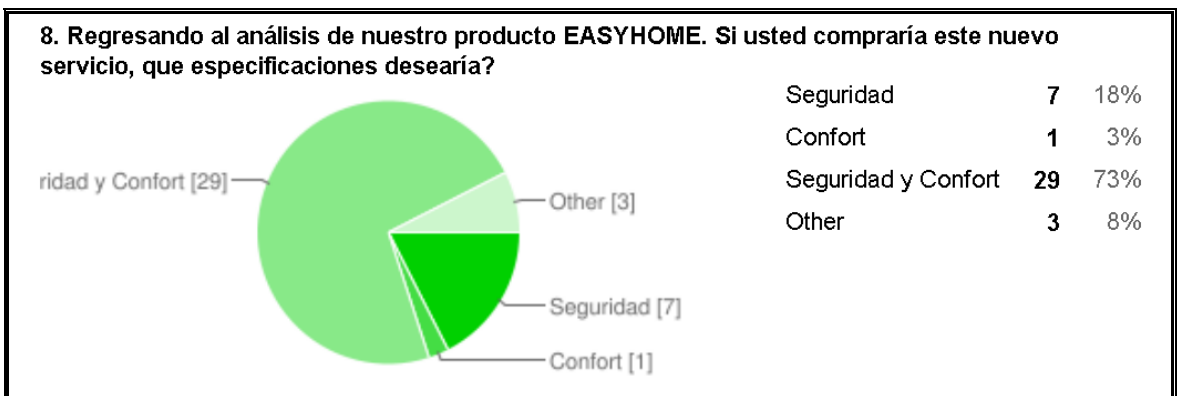


Figura (2.9.): Resultados de la encuesta pregunta 8

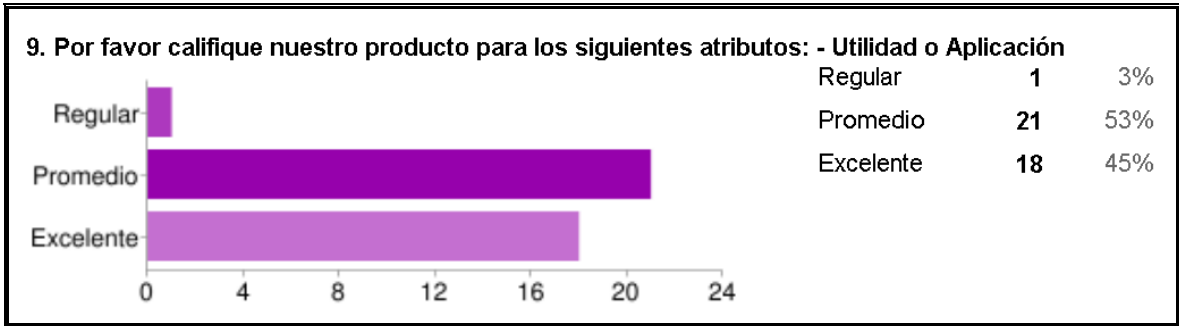


Figura (2.10.): Resultados de la encuesta pregunta 9



Figura (2.11.): Resultados de la encuesta pregunta 9 parte 2

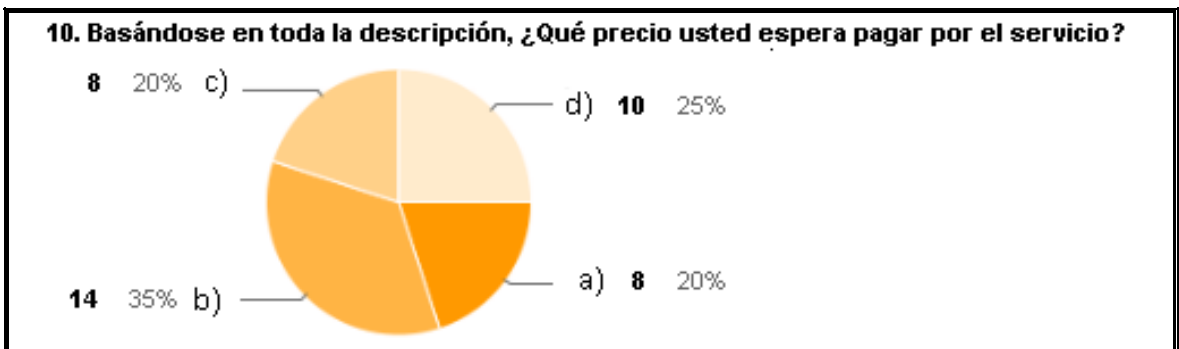


Figura (2.12.): Resultados de la encuesta pregunta 10

a) \$150 Se ofrece seguridad : alarma via telefónica activada por irrupción	8	20%
b) \$200 Se ofrece seguridad: alarma telefónica por irrupción + camaras de vigilancia a través de la web	14	35%
c) \$300 Se ofrece seguridad y confort: alarma telefónica+camaras de vigilancia+ creacion de ambientes	8	20%
d) \$350 Se ofrece seguridad y confort: alarma via telefónica+camaras de vigilancia+ creacion de ambiente+ alarmas para la detección de gas, fuego, agua	10	25%

Figura (2.13.): Resultados de la encuesta pregunta 10 resultados

Al continuar con la evaluación, sobre la aceptación de la central domótica para el hogar, en las preguntas 8, 9 y 10 se obtuvo que el 73% desea los servicios de

confort y seguridad, el 18% solo seguridad, el 7% confort y 8% otros servicios. La mayoría de los encuestados consideran que EASYHOME es un producto innovador con varias aplicaciones, están de acuerdo con la asignación de precios según el número de servicios que se oferta.

En el Anexo A.2 se muestra de todas las respuestas obtenidas frente a cada pregunta de los encuestados.

La encuesta generó como resultado global un alto grado de aceptación del producto doméstico ficticio EASYHOME, debido a los servicios de seguridad y confort que ofrece, a un costo accesible al usuario.

CAPÍTULO 3. DISEÑO DEL PROTOTIPO DE UNA CENTRAL DOMÓTICA VoIP BASADO EN TRIKBOX

3.1 INTRODUCCIÓN

Actualmente en el mercado existen equipos domóticos que permiten acceder al sistema vía telefónica, la limitante de estos aparatos es su nula escalabilidad y flexibilidad, por este motivo se utiliza software libre que permite unir dos tecnologías como la domótica y las centrales telefónicas VoIP, para permitir de forma escalable y flexible añadir aplicaciones a bajo costo.

3.2 DIMENSIONAMIENTO DE HARDWARE DE VoIP

Para realizar un dimensionamiento de hardware en la instalación de un servidor TriKbox se tiene en cuenta los siguientes aspectos:

- Número de extensiones (terminales) y de qué tipo: analógicas o SIP.
- Cuántas llamadas simultáneas y qué tipo: analógicas o VoIP.
- Red de datos: LAN, MAN, WAN.

Para no saturar el procesador se debe trabajar con archivos de audios no codificados, wav para los Playbacks de grabaciones entrantes y música en espera, ulaw para las grabaciones internas del sistema, etc.

Es útil implementar VoIP sobre una red LAN (red de área local) que tenga acceso a internet, con una topología en estrella que permita la escalabilidad del sistema.

3.3 REQUISITOS DE HARDWARE PARA LA CENTRAL DOMÓTICA VoIP

3.3.1 SERVIDOR

Los requisitos mínimos para la instalación de TriKbox y su correcto funcionamiento en un PC son:

- 400MHz del procesador de la CPU.

- 128 MB de memoria RAM.
- 6GB de disco duro.
- Tarjeta de red.
- Tarjetas Troncales.
- Unidad de CD-ROM (temporal).

Debido a los requerimientos de la empresa Pc-servicios que cuenta con 3 departamentos de trabajo se requiere un grupo pequeño de extensiones, sin embargo se debe tomar en cuenta el crecimiento propio de la empresa y su ampliación, por lo tanto las características de hardware necesarias al servidor son las siguientes:

- Procesador Pentium III con 500MHZ.
- 1 GB de memoria RAM.
- 1 disco duro de 150GB.
- 1 tarjeta de red de 10/100 Mbps.

3.3.2 TARJETA PCI

El servidor de la central domotica VoIP necesita de una tarjeta PCI para conectarse a la PSTN y así realizar llamadas a cualquier número convencional y celulares. En la implementación del prototipo de una central domótica VoIP se utiliza una tarjeta PCI clon Ambient 3200 de un solo puerto FXO, una línea de teléfono debe conectarse al modulo FXO y la red LAN de la empresa se conecta a través de la tarjeta de red hacia un switch, considerando un crecimiento futuro de la empresa se recomienda el uso de una tarjeta Digium modelo TDM400P con dos módulos FXO y dos módulos FXS. En el anexo B.2 se especifica las características de estas interfaces.

3.3.3 MÓDULOS X10

En el diseño del prototipo de la central domótica VoIP se usa un módulo controlador CM11A bidireccional, un módulo actuador LM465, un módulo MS16A sensor de presencia RF que actúa en conjunto con el módulo transceptor TM751,

esenciales para brindar seguridad y confort. Las características de los módulos se detallan en el anexo B.3.

3.3.4 CÁMARA WEB

El monitoreo por video se realiza mediante una cámara web, Motion es compatible con varias marcas de cámaras web, se eligió para diseñar el prototipo la cámara INTEL CS430. Las características de la cámara web INTEL CS430 están en el anexo B.3.

3.4. CARACTERÍSTICAS DE SOFTWARE

3.4.1 SISTEMA OPERATIVO

El paso inicial luego de tener listo el hardware es instalar un sistema operativo fiable para obtener un correcto funcionamiento de la central domótica VoIP. Trixbox es una distribución del sistema operativo GNU/Linux basado en Centos, diseñado especialmente para una central telefónica, que cuenta con herramientas como Asterisk, FreePBX, Flash Operator Panel útiles en la implementación del prototipo. Los pasos para su instalación se encuentran en el anexo C1.

3.4.2 SOFTPHONES

Esta aplicación se puede aprovechar en empresas, ya que cada miembro generalmente cuenta con una estación de trabajo, los softphones o teléfonos de software se puede configurar fácilmente con la dirección IP de la máquina host. Los usuarios de la central domótica VoIP pueden comunicarse empleando los dispositivos de entrada y salida de la tarjeta de sonido del PC.

Se debe considerar el sistema operativo instalado en las estaciones de trabajo, en Pc-servicios utilizan Windows y Linux. En el internet se puede descargar varias aplicaciones de softphones según las características que se desea, estas opciones incluyen soporte para protocolo SIP. Entre los softphones utilizados están:

SOFTWARE DE SOFTPHONES	SITIO WEB DE DESCARGA	PROTOCOLO	SISTEMA OPERATIVO
X-Lite	http://www.xten.com	SIP	LINUX
Zoiper	http://www.zoiper.com/softphone/	SIP	WINDOWS O LINUX

Tabla (3.1) Softphones (protocolo y sistema operativo)

La instalación de un softphone Zoiper se encuentra en el anexo C3.

3.4.3 HEYU

Heyu es el software utilizado para el control de los módulos X10, a través de comandos de control.

Lista de comandos Heyu:

Comandos HEYU CM11A	Comando HEYU CM17A
Heyu on A1(código del módulo X10)	Heyu fon A1(código del módulo X10)
Heyu off A1(código del módulo X10)	Heyu foff A1(código del módulo X10)
Heyu dim A1 10	Heyu fdim A1 10
Heyu alloff A	Heyu falloff A

Tabla (3.2) Comandos usados en Heyu

Su instalación se detalla en el anexo C.4.

3.4.4 MOTION

El monitoreo de vigilancia con una cámara web se lo realiza instalando el software motion, se ejecuta en Linux y a través de un servidor web muestra imágenes tomadas desde la cámara web en tiempo real. La instalación se detalla en el anexo C5.

3.5. PROGRAMAS EN PHP

Los programas en php localizados en la carpeta /var/lib/asterisk/agi-bin permiten extender las funcionalidades de Asterisk a través del Asterisk Gateway Interface (AGI), realizando un enlace entre las aplicaciones externas y el núcleo de Asterisk. Para que un programa en php sea ejecutado debe tener permisos de escritura, lectura y ejecución, el comando “chmod 755 /var/lib/asterisk/agi-bin/*.php” otorga estos permisos. Los programas realizados en php que permiten la interacción con el usuario son:

- llamadapolicia_rev2.php.
- offx10_rev1.php.
- onx10_rev1.php.

- seguridadactiva_rev2.php.
- stadox10_rev1.php.

Estos programas utilizan los comandos AGI y las lecturas de entrada de Asterisk para ejecutar una respuesta interactiva de voz (IVR) permitiendo la comunicación con el usuario, una vez realizada la interacción, los programas mencionados crean archivos de texto para identificar las opciones que el usuario desea que la central ejecute.

3.5.1 COMANDOS AGI Y LECTURA DE ENTRADA DE ASTERISK

Los comandos de AGI utilizados para ejecutar funciones de Asterisk son:

- **answer:** la respuesta.
- **exec:** ejecuta una determinada aplicación (Las aplicaciones son las funciones que utiliza para crear un plan de marcado en extensions.conf).
- **get data:** Obtiene los datos en un canal.
- **hangup:** Colgar el canal actual.
- **noop:** No hace nada.
- **set callerid:** Establece identificador de llamadas para el canal actual.
- **set variable:** Establece una variable de canal.
- **wait for digit:** Espera a que un dígito que se presiona.

Las lecturas de entrada para leer la información que pasa por Asterisk son:

- **agi_channel** - El canal de origen (el teléfono).
- **agi_type** - El tipo de canal de origen (por ejemplo, "SIP" o "ZAP").
- **agi_extension** - El número de llamada.
- **agi_priority** - La prioridad que fue ejecutado como en el plan de marcado.

3.6. CONSTRUCCIÓN DE SCRIPTS

Un script (cuya traducción literal es 'guion') o archivo de órdenes es un programa, que se almacena en un archivo de texto. Los scripts son identificados por el sistema a través uno de los siguientes encabezados en el contenido del archivo, conocido como shebang: `#!/bin/bash` ; `#!/bin/ksh` ; `#!/bin/csh`

Aunque en entornos UNIX la mayoría de los scripts son identificados por dicho encabezado, también son identificados a través de la extensión ".sh", así el usuario puede identificar estos archivos a través de una interfaz de línea de comandos sin necesidad de abrirlo.

En el diseño de la central domótica VoIP se crearon scripts de monitoreo, seguridad, y para el uso de la cámara web.

3.6.1 SCRIPTS DE CONTROL

Los scripts de seguridad, monitoreo, usomotion están destinados para funcionar como una interfaz entre la comunicación de los módulos X10 y las características de Asterisk, son scripts que permiten realizar el control de la seguridad y el confort en el hogar. Se establece el orden de funcionamiento de acuerdo al siguiente diagrama:

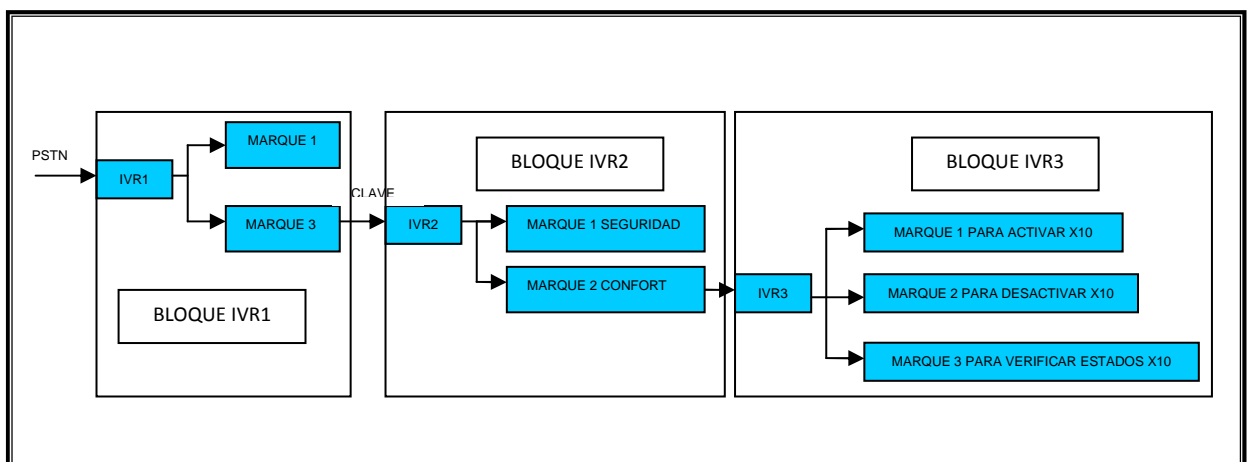


Figura (3.1) Distribución de los IVR por bloques

3.6.1.1 Bloque IVR1

Este bloque permite el acceso a la central domótica, la voz de respuesta interactiva indica un mensaje para que cualquier persona pueda continuar la llamada, de manera oculta (Opción: marque tres) se encuentra la opción para ingresar a la central domótica, por medio de autenticación mediante una clave, admite el acceso al bloque IVR2 con opciones de seguridad y confort.

3.6.1.2 Bloque IVR2

Este bloque activa el sistema de seguridad o accede al servicio de confort, mediante una llamada de teléfono por medio de la PSTN o a través de la red de comunicaciones VoIP del hogar. Con el uso de AGI-Asterisk se accede a la seguridad que está controlada por el programa en lenguaje php “seguridadactiva_rev2.php” para elegir las opciones de activar o a su vez desactivar la seguridad. El control de verificación de seguridad y confort es realizada por los scripts de monitoreo y seguridad, que permiten el control de las opciones ejecutadas al haberse establecido la llamada.

3.6.1.3 Script monitoreo

Al ejecutar el script monitoreo se genera una dirección de identidad del proceso (PID), utilizada para detener el proceso del script monitoreo en cualquier momento mediante el comando KILL.

Además este script detiene los procesos de los scripts de seguridad y usomotion, para evitar que se saturen las funciones de Asterisk y así garantizar que el computador esté libre de procesos innecesarios, se encuentra en un lazo infinito realizando la lectura de los archivos de texto creados por los programas en php que indican las acciones que el usuario ha elegido para que le central domótica las ejecute.

El script de monitoreo permite la ejecución del script de seguridad, mediante la lectura de un archivo de texto generado por el programa seguridadactiva_rev2.php, también controla las opciones de confort, realiza las actividades para activar, desactivar o incluso permite reconocer los estados de los dispositivos X10. En el anexo D.1 se encuentra el código del script monitoreo.

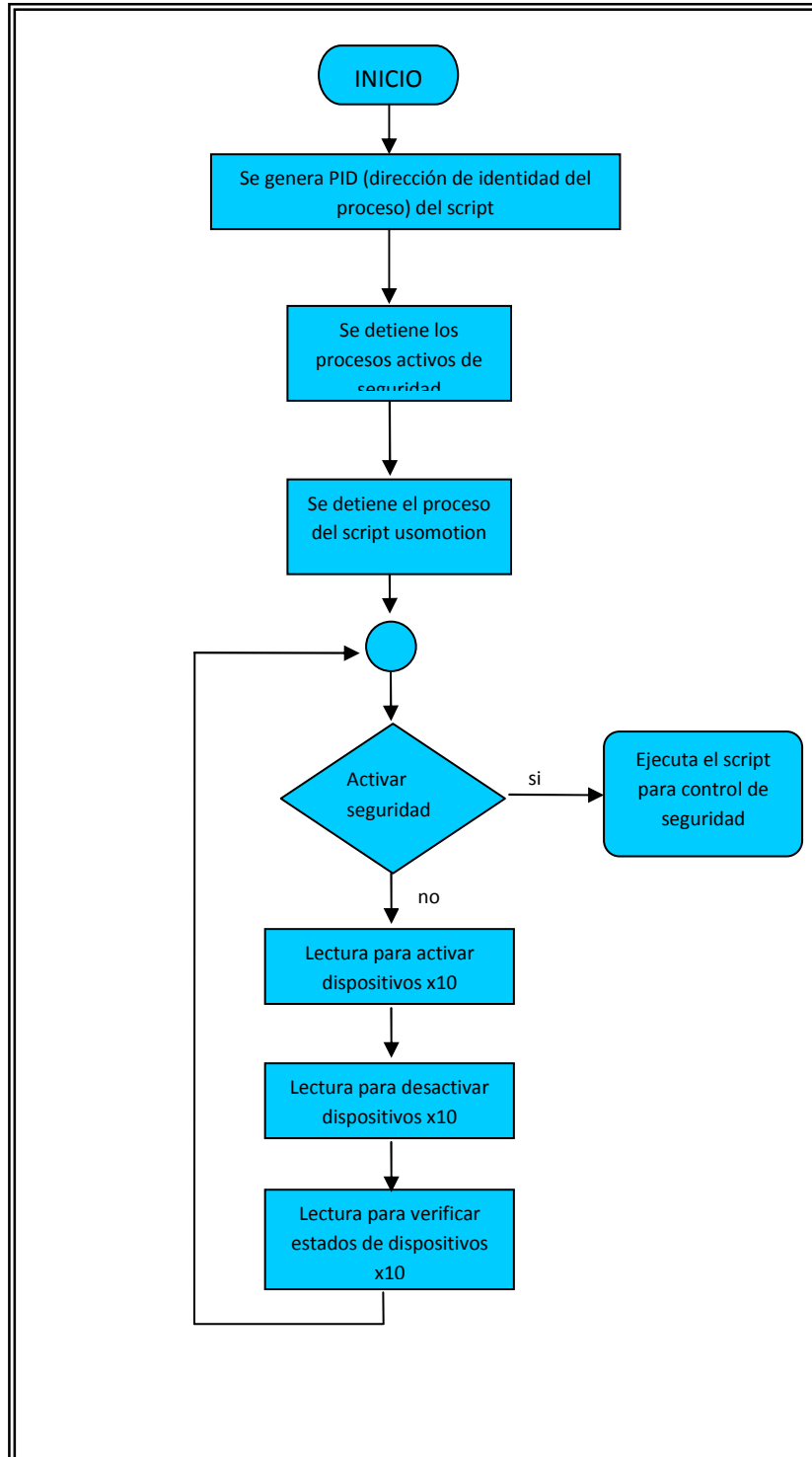


Figura (3.2) Diagrama de flujo del script monitoreo

3.6.1.4 Script seguridad

Al iniciar el script seguridad genera un PID que permite identificarlo entre los procesos ejecutados, detiene a los scripts monitoreo y usomotion, se encuentra en constante lectura del sensor de presencia nombrado como A3, cuando el estado del sensor cambia, automáticamente se genera el archivo alarmevent.call en la carpeta /var/spool/asterisk/outgoing.

El archivo con la extensión “.call” crea una llamada automática, en su configuración se asigna un número de teléfono al cual va dirigida la llamada (celular del usuario), y activa el programa llamadapolicia_rev2.php que indica las opciones de seguridad establecidas por el usuario.

Si existe una violación en la seguridad se genera una llamada automática para informar que la seguridad ha sido violentada, dándole al usuario la opción para detener el proceso de la llamada de emergencia, o le permite verificar el estado de la vivienda mediante el uso de una cámara web por Internet y así luego generar la llamada de emergencia. En el anexo D.2 se detalla el código del script seguridad.

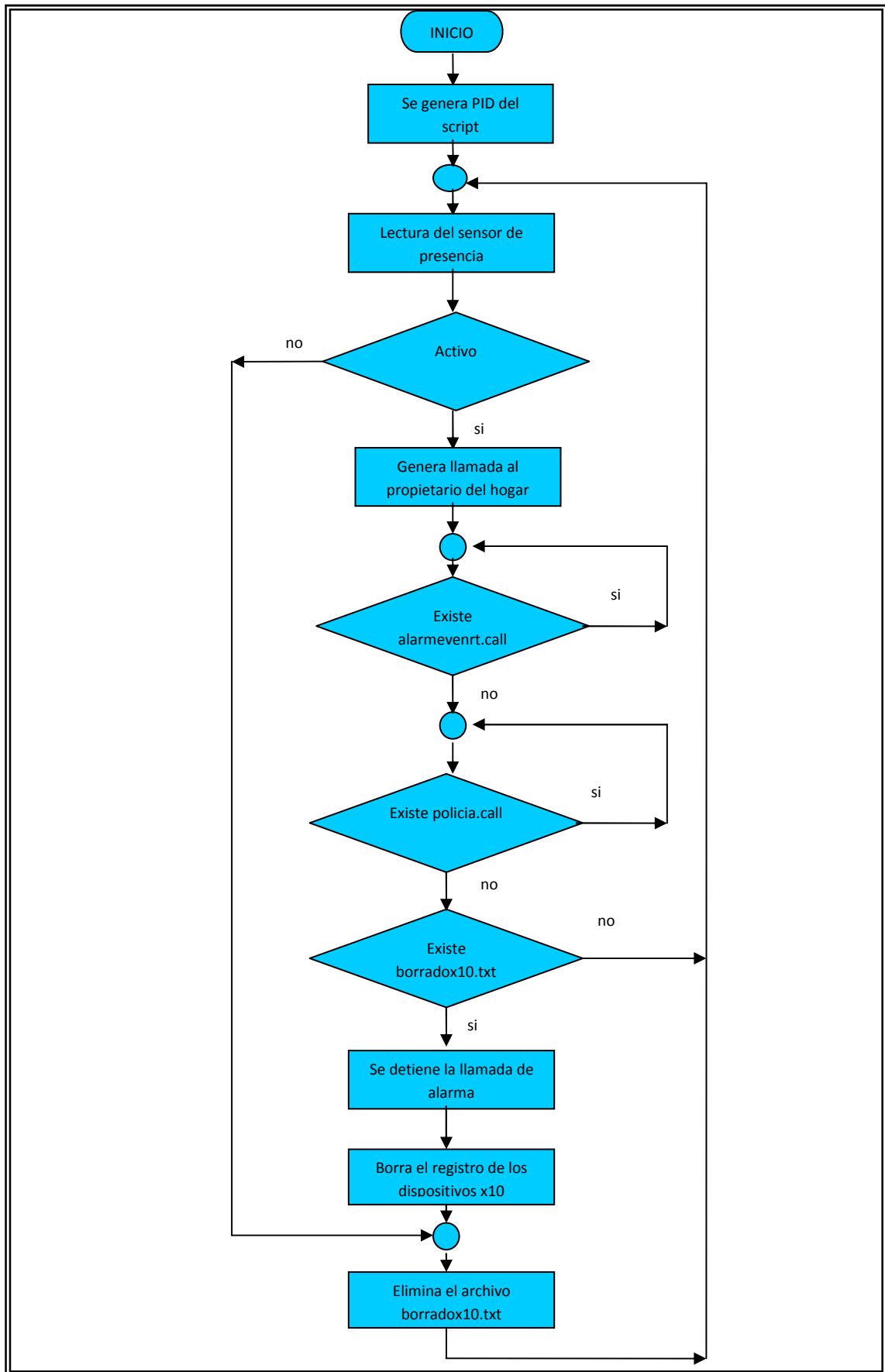


Figura (3.3) Diagrama de flujo del script seguridad

3.6.1.4.1 Programa en php para activar seguridad

El programa en php seguridadactiva_rev2.php se encuentra en la carpeta agi-bin, permite la creación de archivos de texto que indican las acciones de activar, desactivar el sistema de seguridad mediante una respuesta interactiva de voz, estos archivos de texto son leídos por el script monitoreo permitiendo que se ejecute o se detenga el script seguridad.

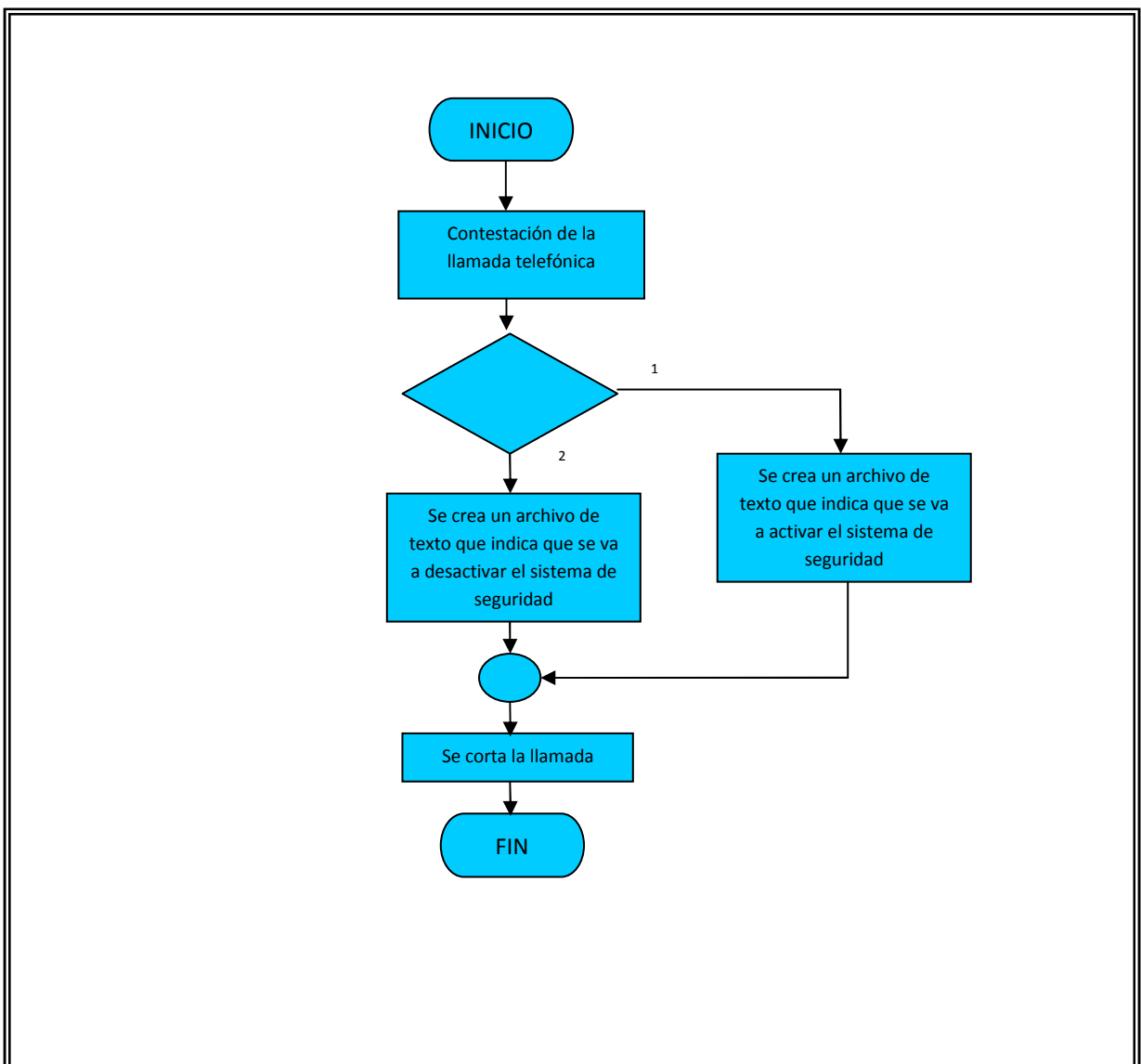


Figura (3.4) Diagrama de flujo del programa seguridadactiva_rev2.php

3.6.1.4.2 Programa en php para llamada de emergencia

El programa en php `llamadapolicia_rev2.php` genera una llamada automática para informar que la seguridad ha sido violentada, da opciones para detener el proceso de la llamada de emergencia, o incluso permite la opción para verificar el estado de la vivienda mediante el uso de una cámara web por Internet, esto lo realiza creando archivos de texto que indican las opciones de continuar con la llamada, detener la llamada o activar la cámara web.

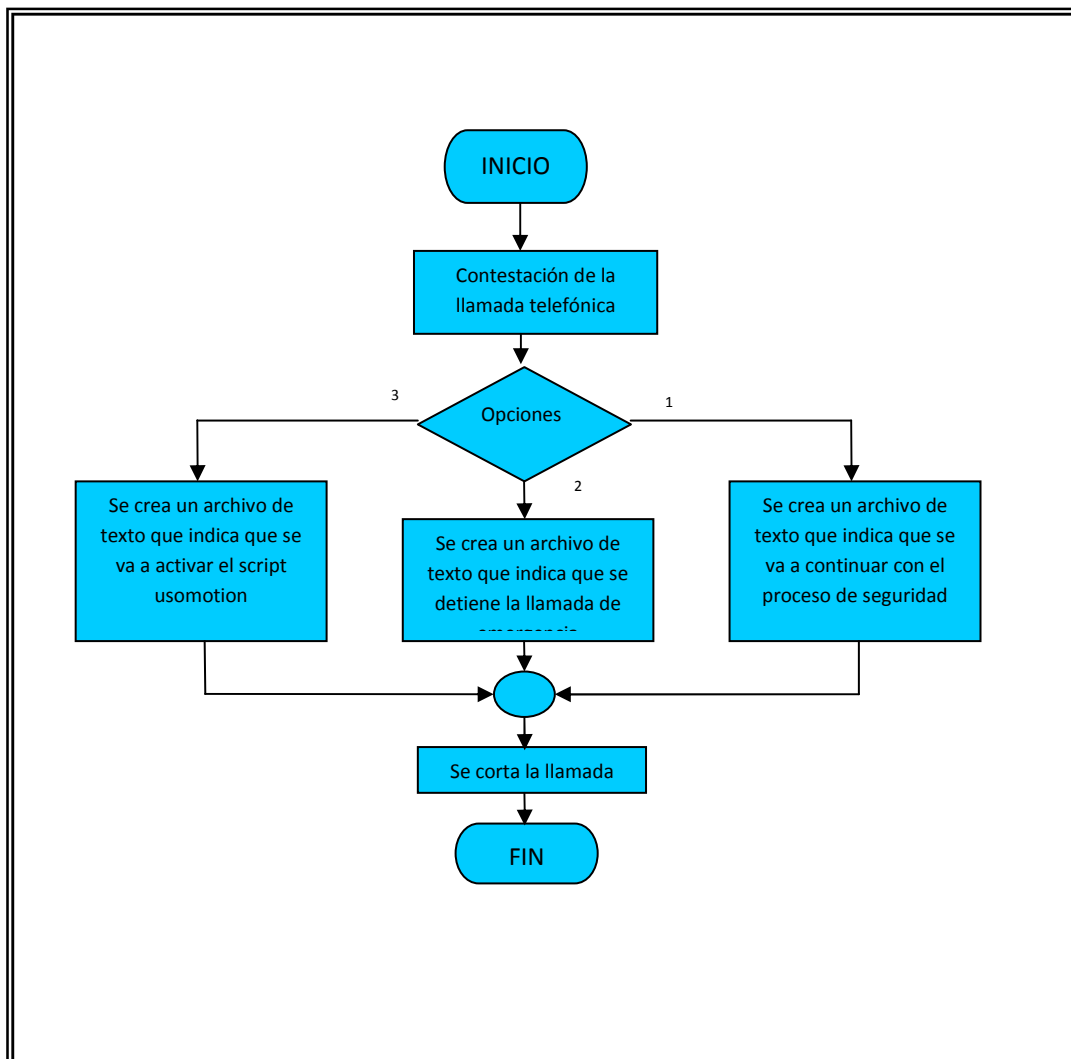


Figura (3.5) Diagrama de flujo del programa `llamadapolicia_rev2.php`

3.6.1.5 Script usomotion

El script usomotion permite activar el software motion para comandar la cámara web, esto lo realiza a través del puerto 8081, permitiendo observar un streaming de imágenes obtenidas desde la cámara en la internet.

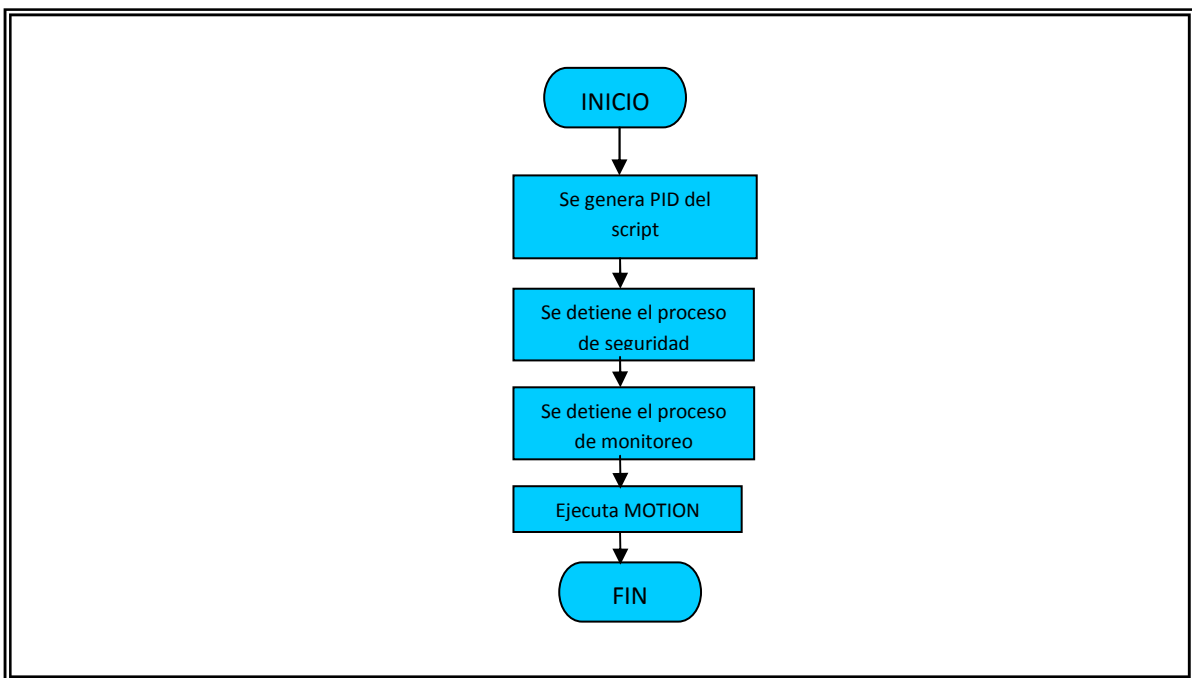


Figura (3.6) Diagrama de flujo del script Usomotion

3.6.1.6 Bloque IVR3

Este bloque genera las opciones de confort en el hogar, el IVR3 permite activar, desactivar y verificar los estados de los módulos X10, estas acciones son ejecutadas por los programas en php onx10_rev1.php, offx10_rev1.php y stadox10_rev1php.

Los programas en php mencionados crean archivos de texto, donde guardan el código de los módulos X10 permitiendo encender, apagar y verificar su estado. El script monitoreo realiza la lectura de estos archivos de texto ejecutando los comandos de control de los módulos X10.

DISPOSITIVOS X10	CÓDIGO
A1	11
A2	12
A3	13
A4	14
A5	15
A6	16
A7	17
A8	18
A9	19

Tabla (3.3) Códigos para comandar los dispositivos X10

3.6.1.6.1 Programa en php para activar módulos X10

El programa onx10_rev1.php sirve para activar un módulo X10, digitando en el teclado del teléfono el código del módulo X10 que se desea encender, este código es almacenado en un archivo de texto nombrado activarx10.txt para que el script monitoreo lo lea y realice el envío del comando de encendido al módulo X10 asignado.

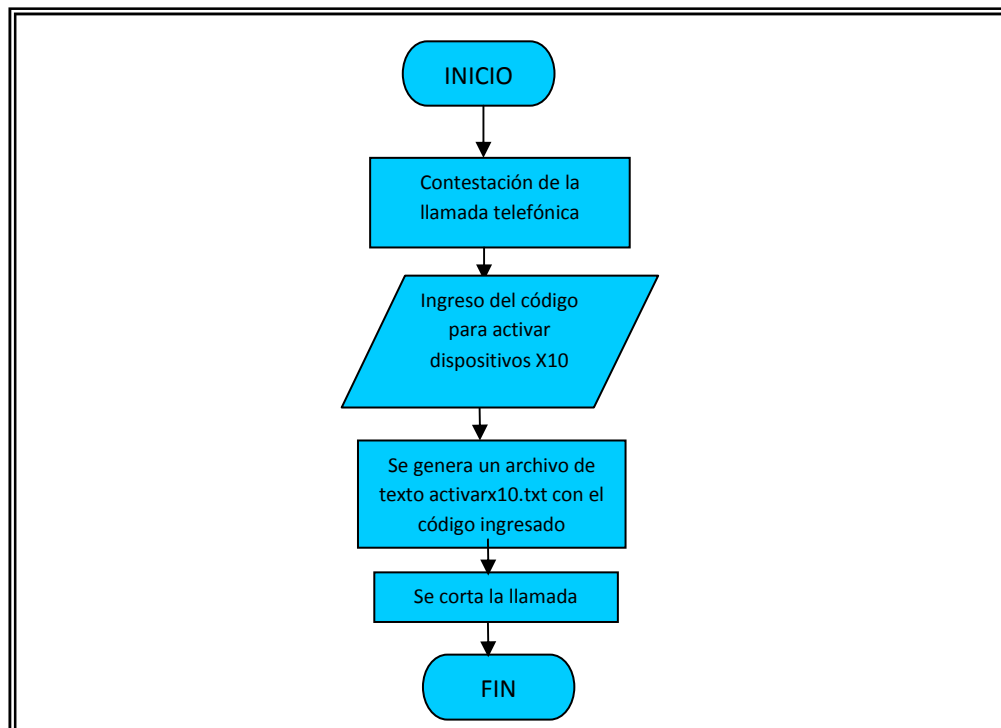


Figura (3.7) Diagrama de flujo del programa onx10_rev1.php

1.3.6.1.2 Programa php para desactivar módulos X10

El programa `offx10_rev1.php` permite apagar un módulo X10 mediante la digitación del código del módulo X10 en el teclado del teléfono, se guarda este código en un archivo de texto nombrado como `desactivarx10.txt` para que el script monitoreo realice el envío del comando `heyu` para desactivar el módulo X10 asignado.

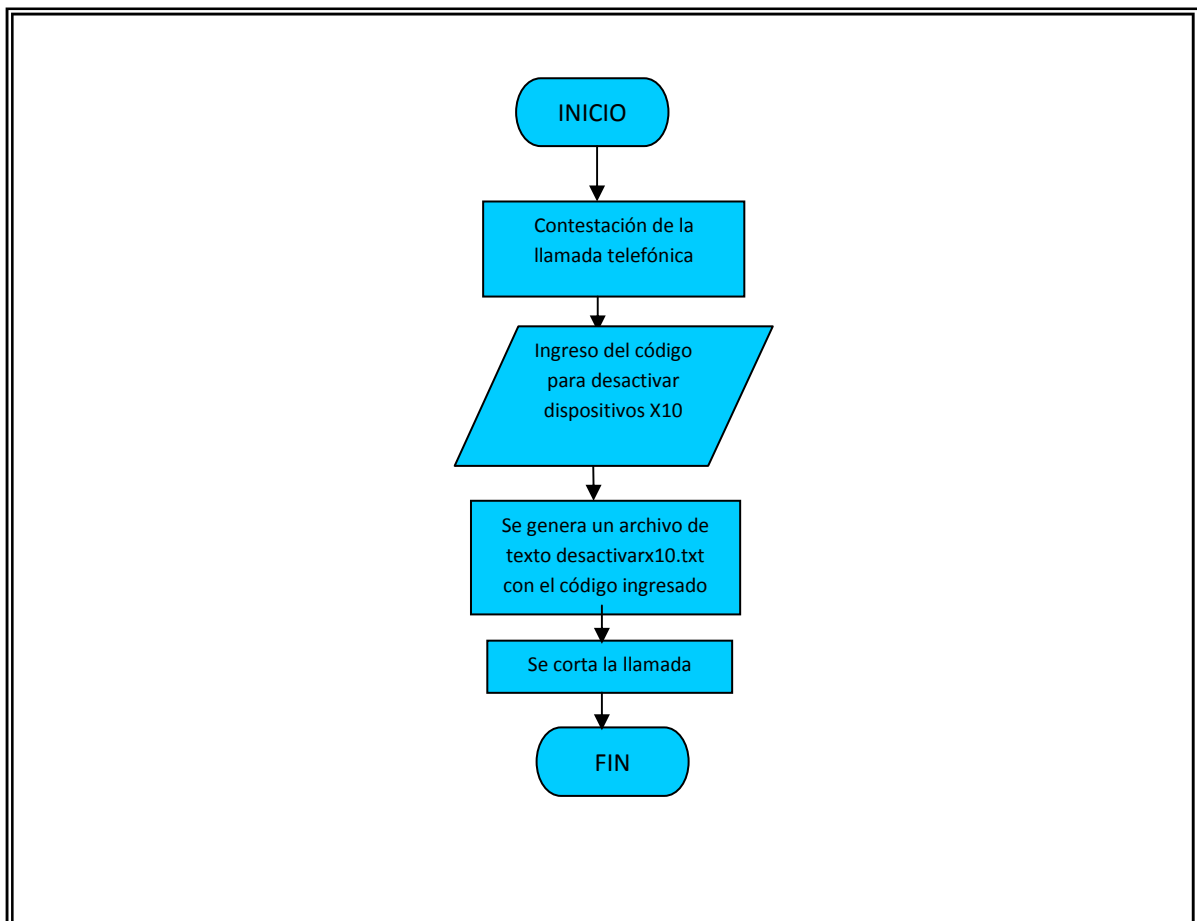


Figura (3.8) Diagrama de flujo del programa `offx10_rev1.php`

1.3.6.1.3 Programa php para verificar el estado de módulos X10

El programa stadox10_rev1.php sirve para verificar el estado de un módulo X10, al igual que los otros programas en php se digita el código del módulo X10 del cual se desea verificar su estado, este código se almacena en un archivo de texto que tiene por nombre stadox10.txt, el script de monitoreo busca la creación de este archivo de texto y realiza la lectura, guardando en una variable esta información. La variable es utilizada para generar el comando de verificación del estado del módulo X10, este estado se lo guarda en otro archivo de texto nombrado igual que el código del módulo X10, entonces el programa stadox10_rev1.php almacena en una variable el dato del archivo de texto con la información sobre el estado y lo ejecuta como una grabación indicando si está encendido o apagado el módulo X10.

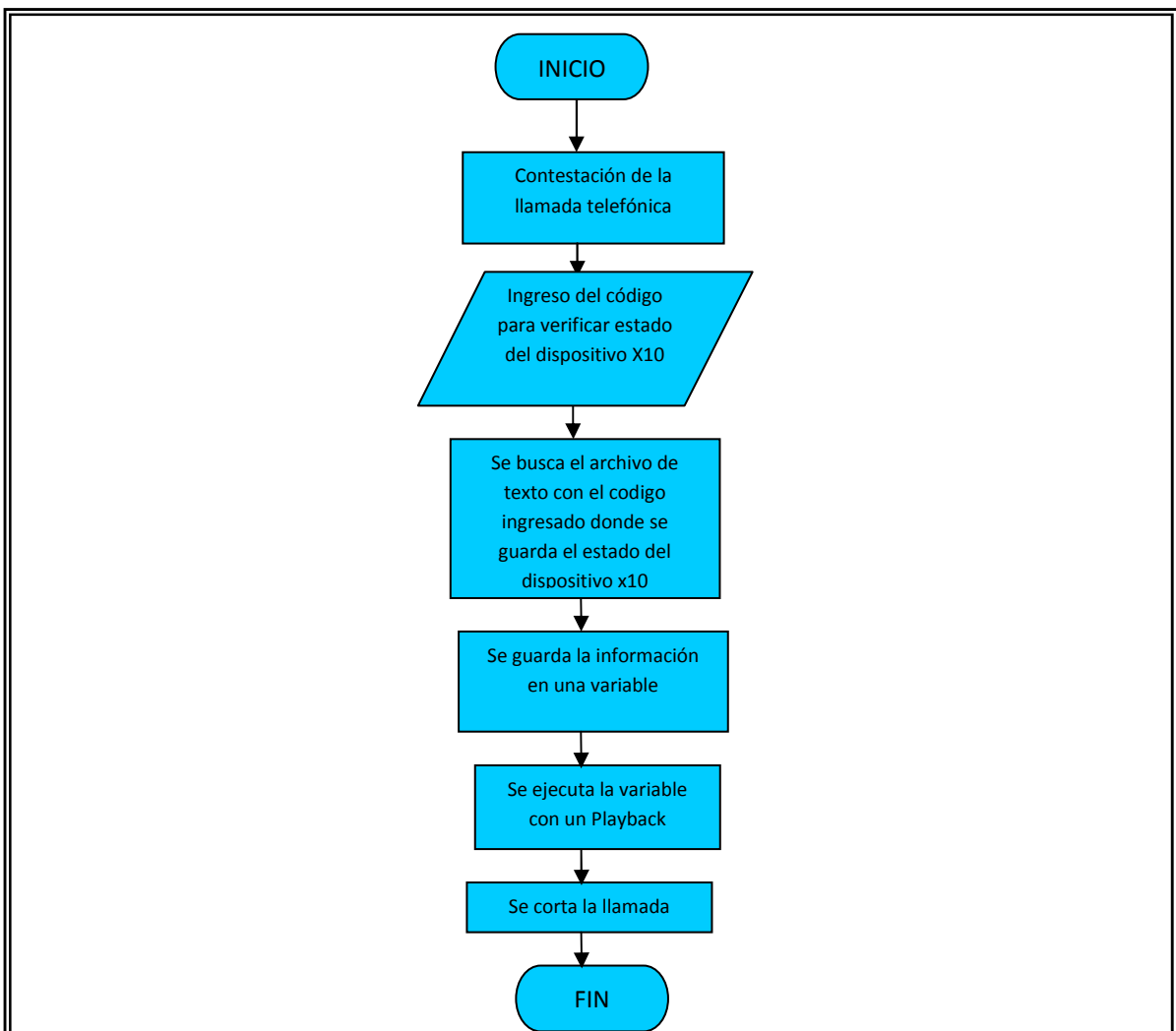


Figura (3.9) Diagrama de flujo del programa stadox10_rev1.php

CAPÍTULO 4. IMPLEMENTACIÓN, ANÁLISIS DE COSTOS Y PRUEBAS DEL PROTOTIPO DE LA CENTRAL DOMÓTICA VoIP

4.1 IMPLEMENTACIÓN DEL PROTOTIPO

Para la implementación del prototipo se utilizó los datos obtenidos en la encuesta de estudio de mercado, esta información indicó que el 77% de la muestra escogida están interesados en el producto y el 73% prefieren un sistema de seguridad y confort en sus hogares.

Además con el análisis de tecnologías compatibles se optó por utilizar módulos actuadores X10 para el encendido y apagado de luces, en el área de seguridad un sensor de movimiento, que apoyado por una cámara web nos brinda la facilidad de monitorear por internet un sector específico del hogar, y para el acceso de llamadas al servidor se uso una tarjeta Fax-modem Ambient 3200 que emula a una tarjeta Digium X100p.

El prototipo de la central domótica VoIP se lo implementó en la oficina de la empresa Pc-servicios, donde fue necesario efectuar un cableado alterno de las instalaciones eléctricas para el uso de los módulos X10, debido a que el cableado eléctrico existente en la oficina no cumplía con las normas internacionales de IEEE para instalaciones eléctricas residenciales, se comprobó que la línea de fase continuamente cambiaba con la línea de neutro, ocasionando que la señalización de los módulos X10 no se pueda enviar ni recibir correctamente.

También se utilizó la central telefónica análoga de la oficina de Pc-servicios para tener acceso al servidor de VoIP y realizar las pruebas necesarias, junto al Firewall existente.

Para la implementación del sistema de seguridad y confort se recurre a la tabla 4.1 que describe el hardware utilizado en el prototipo de la central domótica VoIP basada en Trixbox.

DESCRIPCIÓN	CANTIDAD	UNIDAD
CPU: Procesador Pentium III con 500MHZ, Disco duro 150GB, 1GB de RAM, 1 tarjeta de red 10/100 Mbps	1	unidad
Módulo actuador X10 LM465	2	unidad
Módulo controlador X10 CM11A	1	unidad
Módulo X10 Sensor de presencia MS16A	1	unidad
Módulo transceptor X10 TM751	1	unidad
Tarjeta PCI fax-modem(FAX modem Intel 537PG y 537PU , Motorola 62802-51, Ambient 3200)	1	unidad
Cámara web Intel CS430	1	unidad

Tabla (4.1) Descripción de hardware usado en el prototipo

El software utilizado en la implementación de la central domótica VoIP se aprecia en la siguiente tabla:

Software	Función
Trixbox	Sistema operativo
Softphone Zoiper	Teléfono IP
Motion	Control cámara web
Heyu	Control módulos X10

Tabla (4.2) Descripción de software usado en el prototipo

Además se crearon 3 scripts (monitoreo, seguridad, uso de la cámara web) como interfaz entre Asterisk(Trixbox), el comando de los módulos X10 y el manejo de la cámara web.

Los 3 scripts nunca funcionan al mismo tiempo para evitar que la memoria virtual del procesador se sature y las funciones de la central VoIP operen inadecuadamente, cada script trabaja independientemente, a la espera de las necesidades del usuario.

La interacción mediante una llamada telefónica entra la central domótica VoIP y el usuario se la realiza aplicando los comandos AGI de Asterisk ejecutados por programas php localizados en la carpeta /var/lib/asterisk/agi-bin/.

La dirección IP pública permite el acceso a la página web donde se puede visualizar las imágenes tomadas por la cámara.

4.1.1 CONFIGURACIÓN DE LA CENTRAL VoIP

Se configuró la central VoIP Trixbox para realizar llamadas telefónicas entrantes y salientes desde y hacia la PSTN, creando una troncal ZAP (figura 4.1) llamada g0 que permite un plan de marcación para el acceso hacia la PSTN.

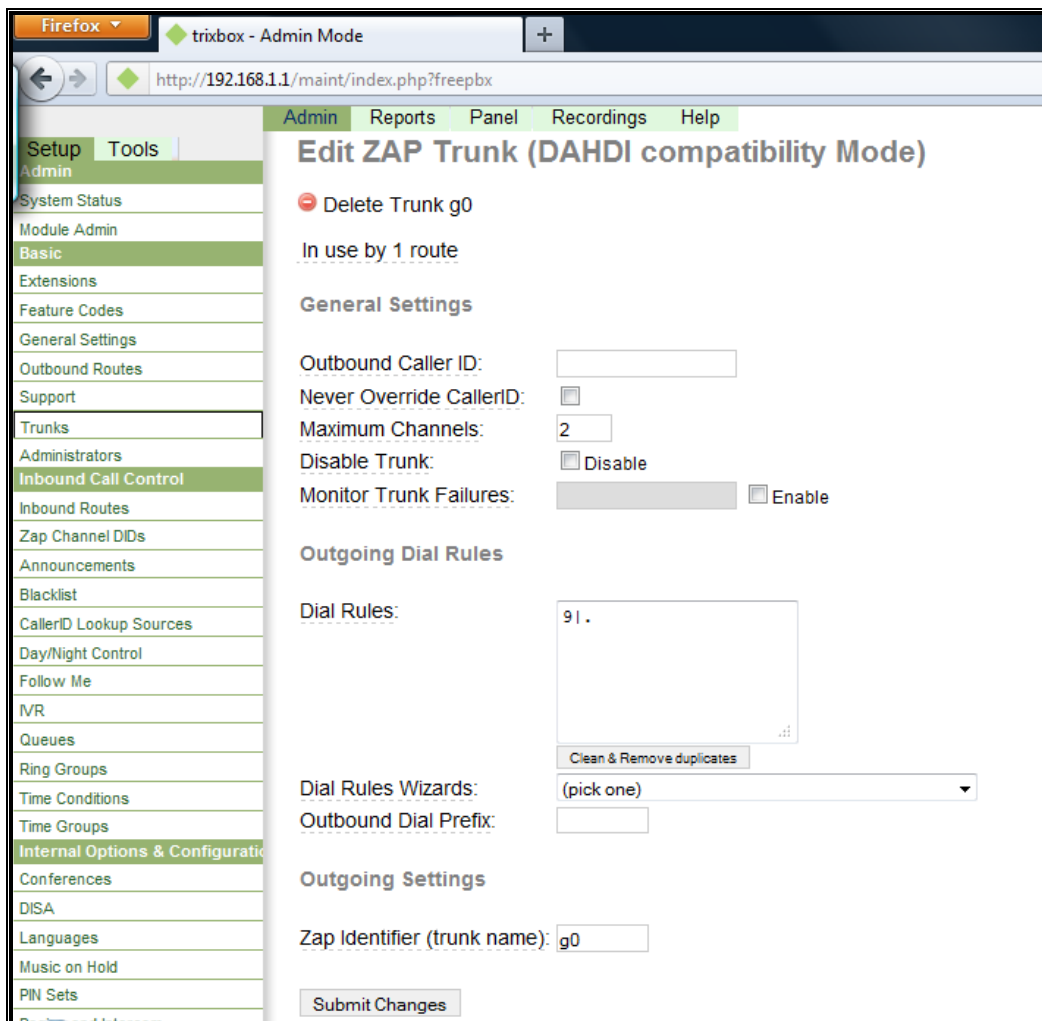


Figura (4.1) Configuración de la troncal zap.

Para realizar llamadas entre extensiones con protocolo SIP, también es necesario crear una troncal SIP, en las figuras 4.2 y 4.3 se observa su configuración.

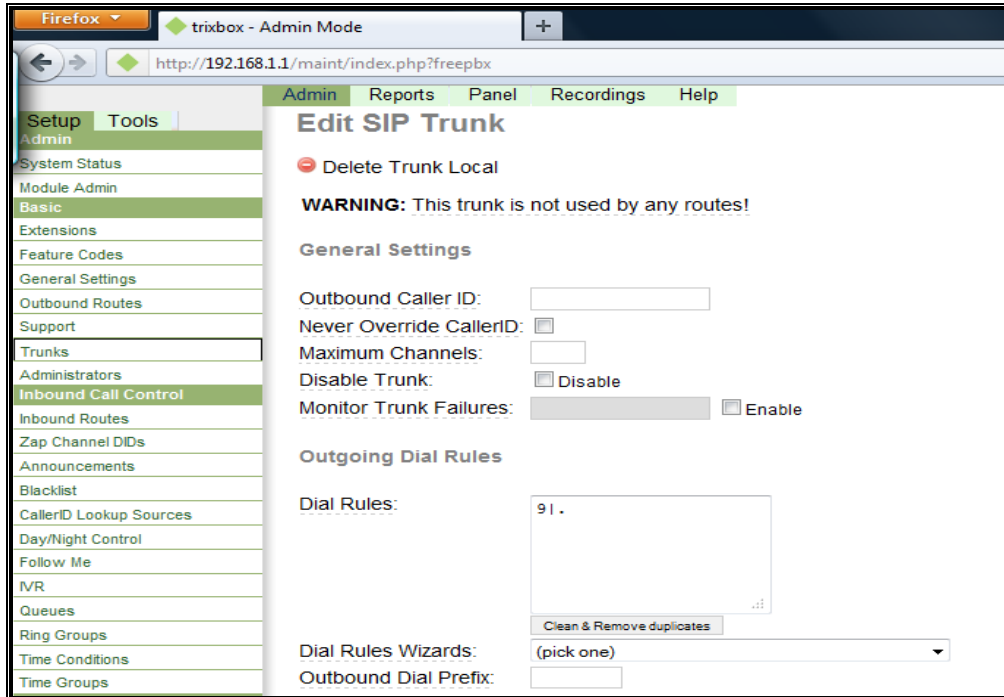


Figura (4.2) Configuración de la troncal SIP

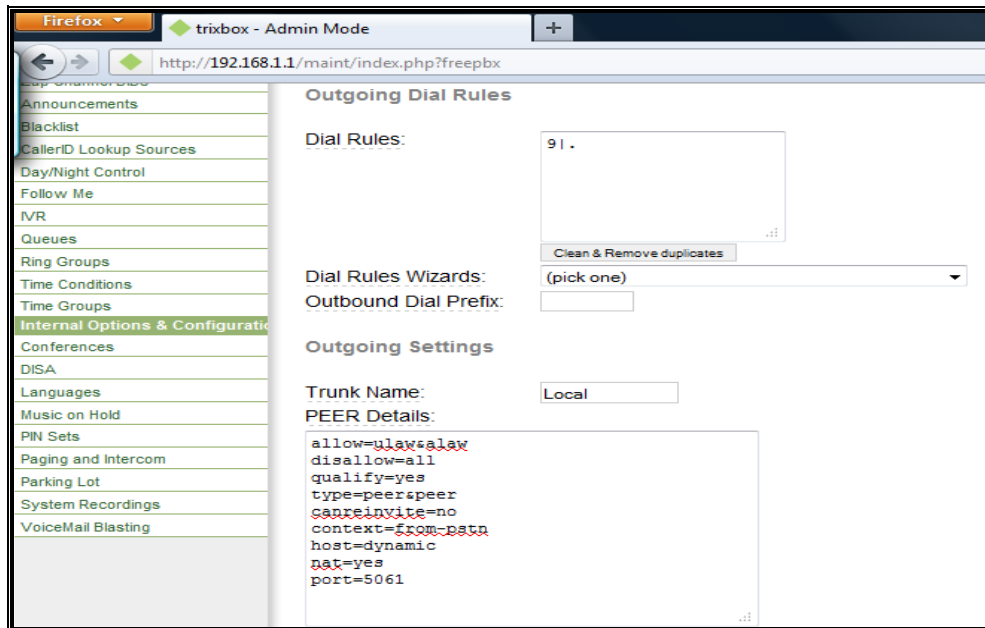


Figura (4.3) Configuración de la troncal SIP

El número de extensiones que la central requiera obedece a las necesidades del usuario, por ejemplo en el hogar dependerá del número de personas que integren una familia o en el caso de una oficina el número de empleados a los cuales se les asigne una extensión. En las figuras 4.4 y 4.5 se indica la configuración de una extensión.

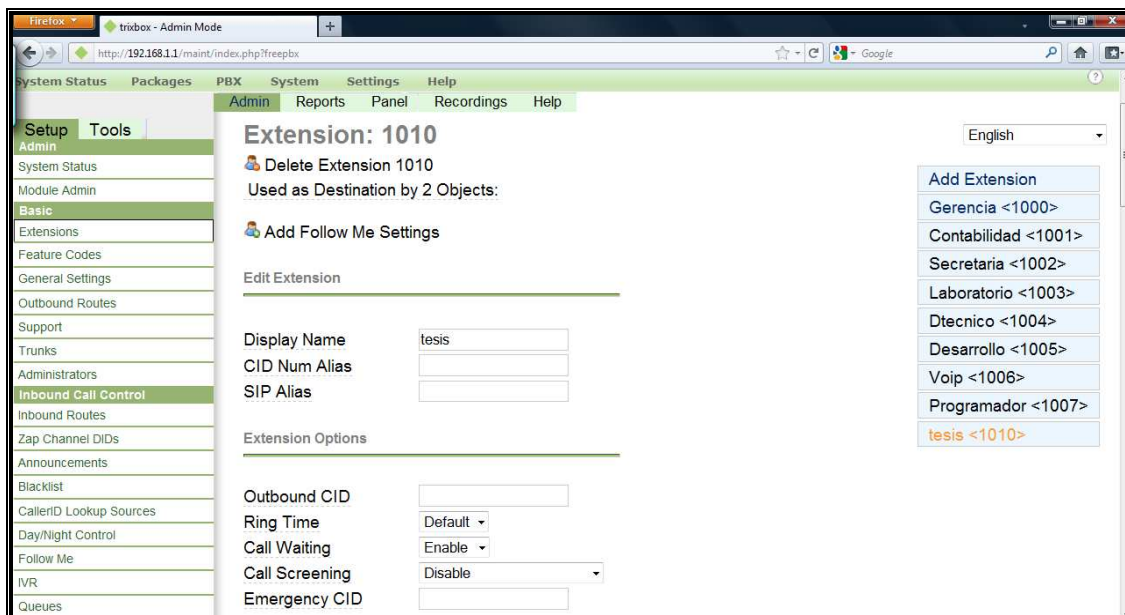


Figura (4.4) Configuración de una extensión SIP

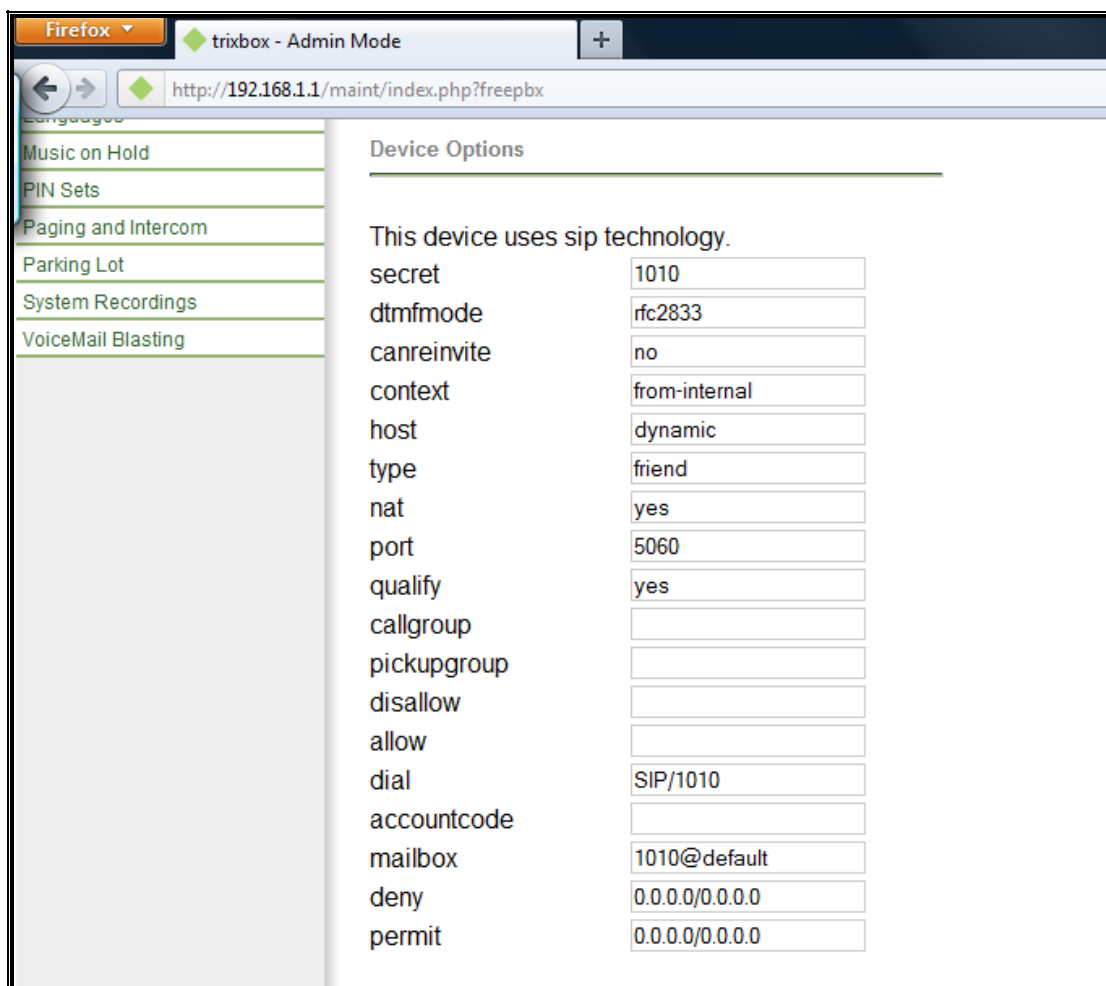


Figura (4.5) Configuración de una extensión SIP

Para el acceso de llamadas desde la PSTN es necesario realizar una configuración general (figura 4.6 y 4.7) que permite que una llamada ingrese al servidor por la tarjeta PCI, se pueden realizar restricciones de números de teléfono que no se desea que accedan al servidor de VoIP, al realizar esta configuración se debe verificar que el sistema de reconocimiento de números de teléfono este activo.

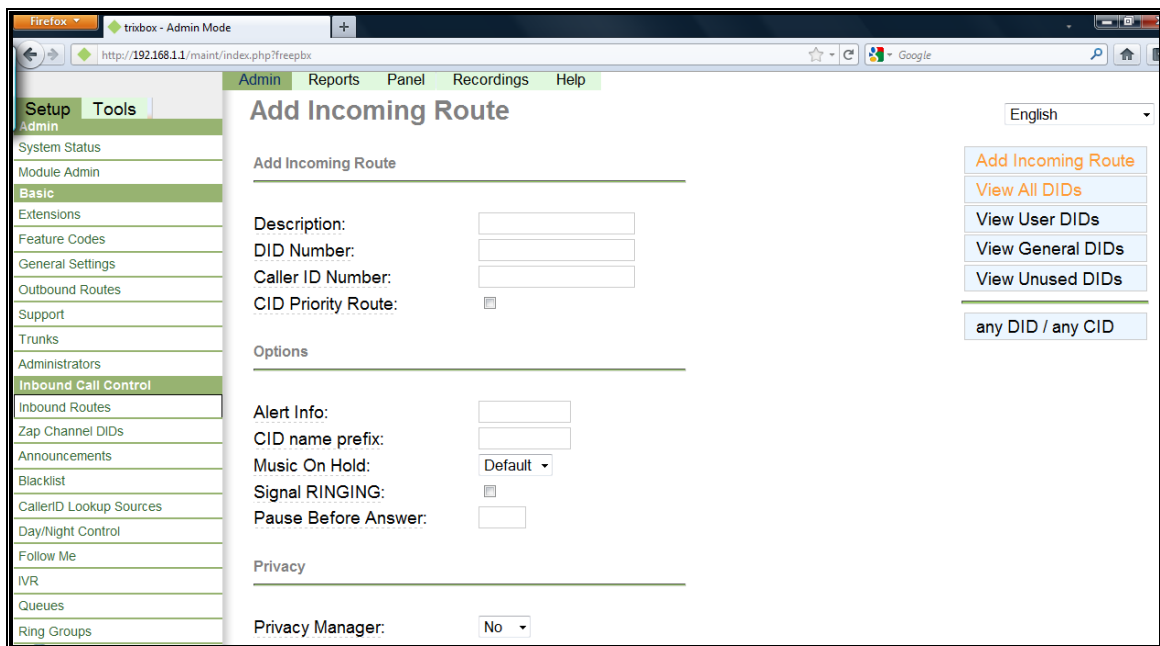


Figura (4.6) Configuración de rutas entrantes

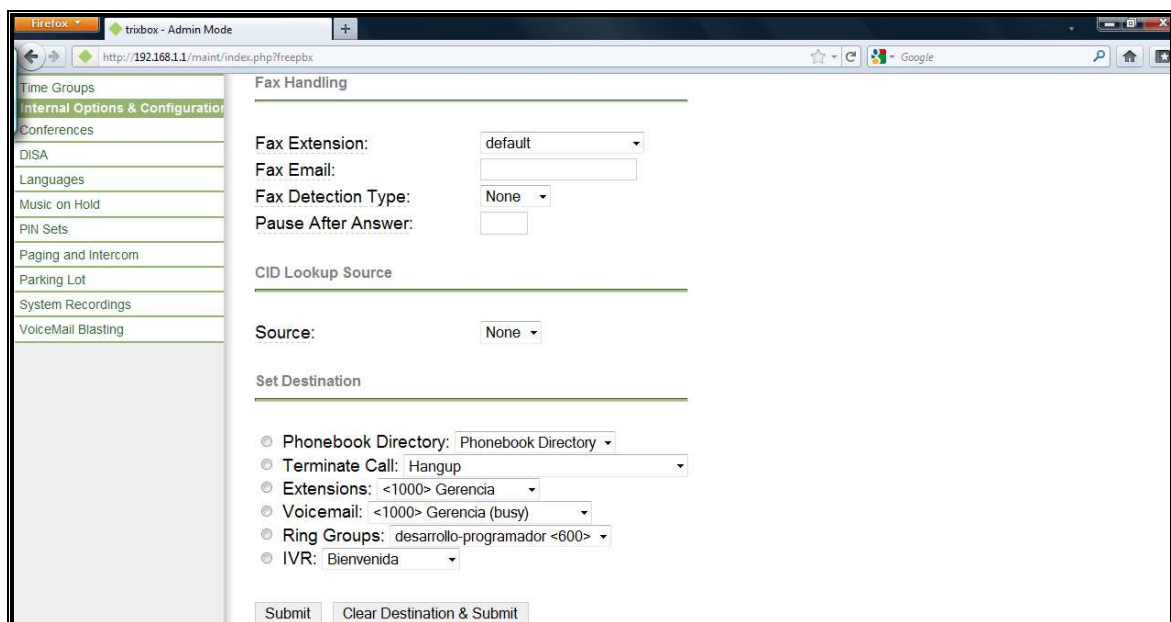


Figura (4.7) Configuración de rutas entrantes

Al implementar el prototipo se habilitó las llamadas salientes por el puerto FXO de la tarjeta PCI Ambient 3200, se configuraron las rutas salientes (figura 4.8) que permiten acceder a la marcación de números existentes en la PSTN.

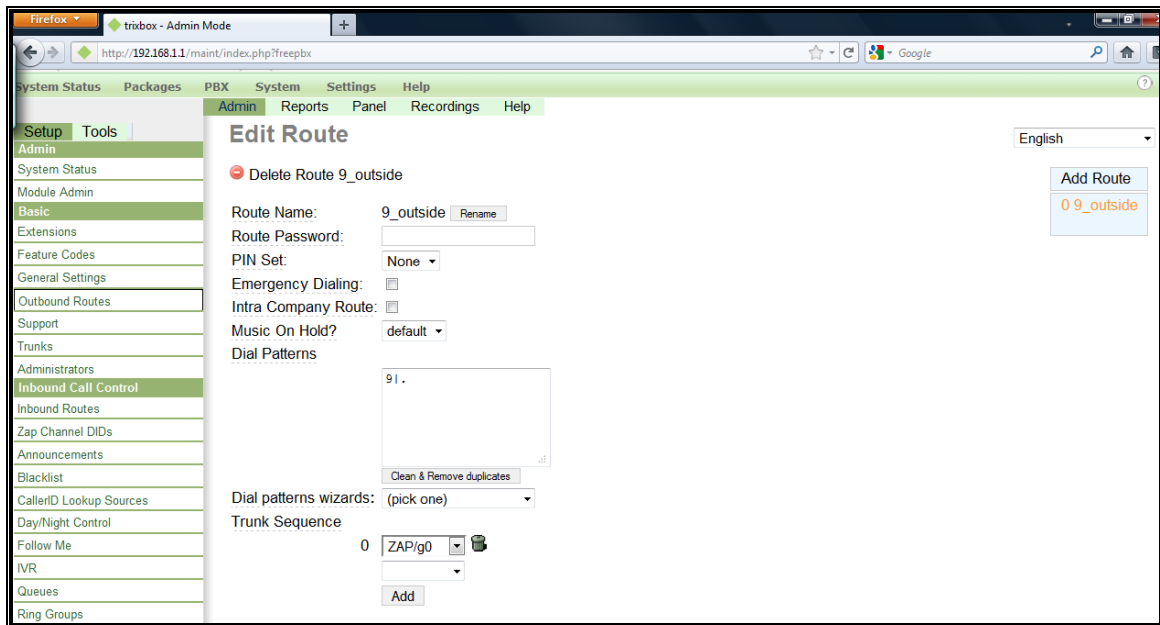


Figura (4.8) Configuración de rutas salientes

El acceso a la central domótica se lo realizó con la configuración de IVRs que permiten al usuario el ingreso a las opciones de seguridad (figura 4.9) utilizando los scripts en php que funcionan con AGI, de acuerdo al diseño planteado en el capítulo anterior se realizó la creación de los IVRs 1, 2 y 3.

El IVR1 (figura 4.9), está configurado con un saludo inicial y permite el acceso a la central domótica. El IVR2 (figura 4.10) permite el acceso a las opciones de seguridad y al IVR3 (figura 4.11). En el diseño planteado se utiliza al IVR3 para acceder a las opciones de confort como el encendido, apagado y estado de los módulos X10.

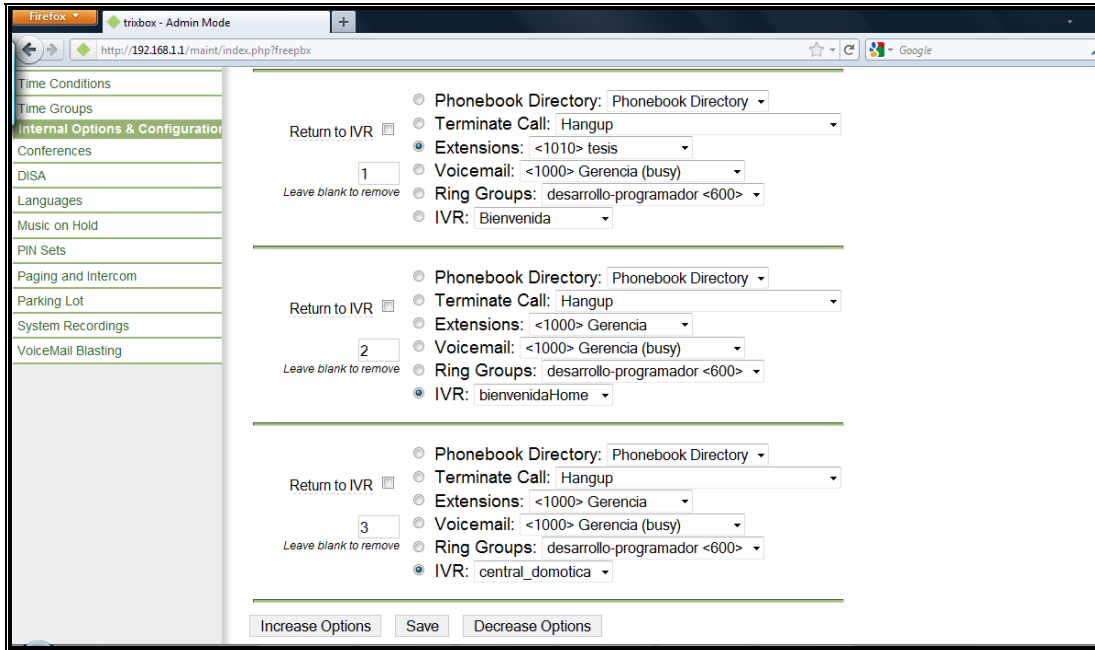


Figura (4.9) Configuración del IVR1

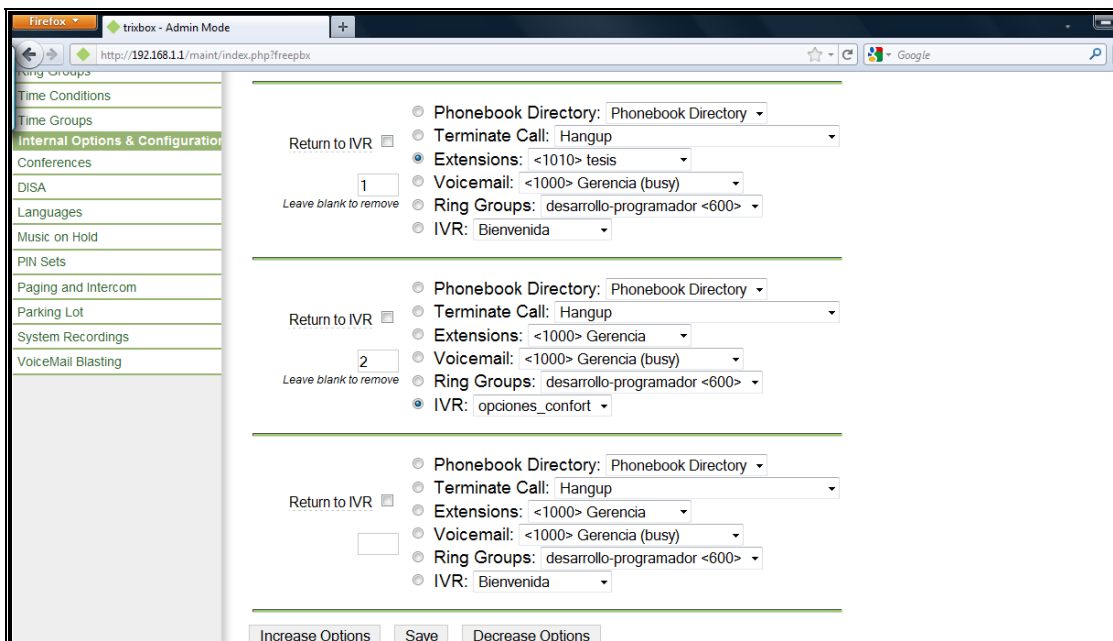


Figura (4.10) Configuración del IVR2

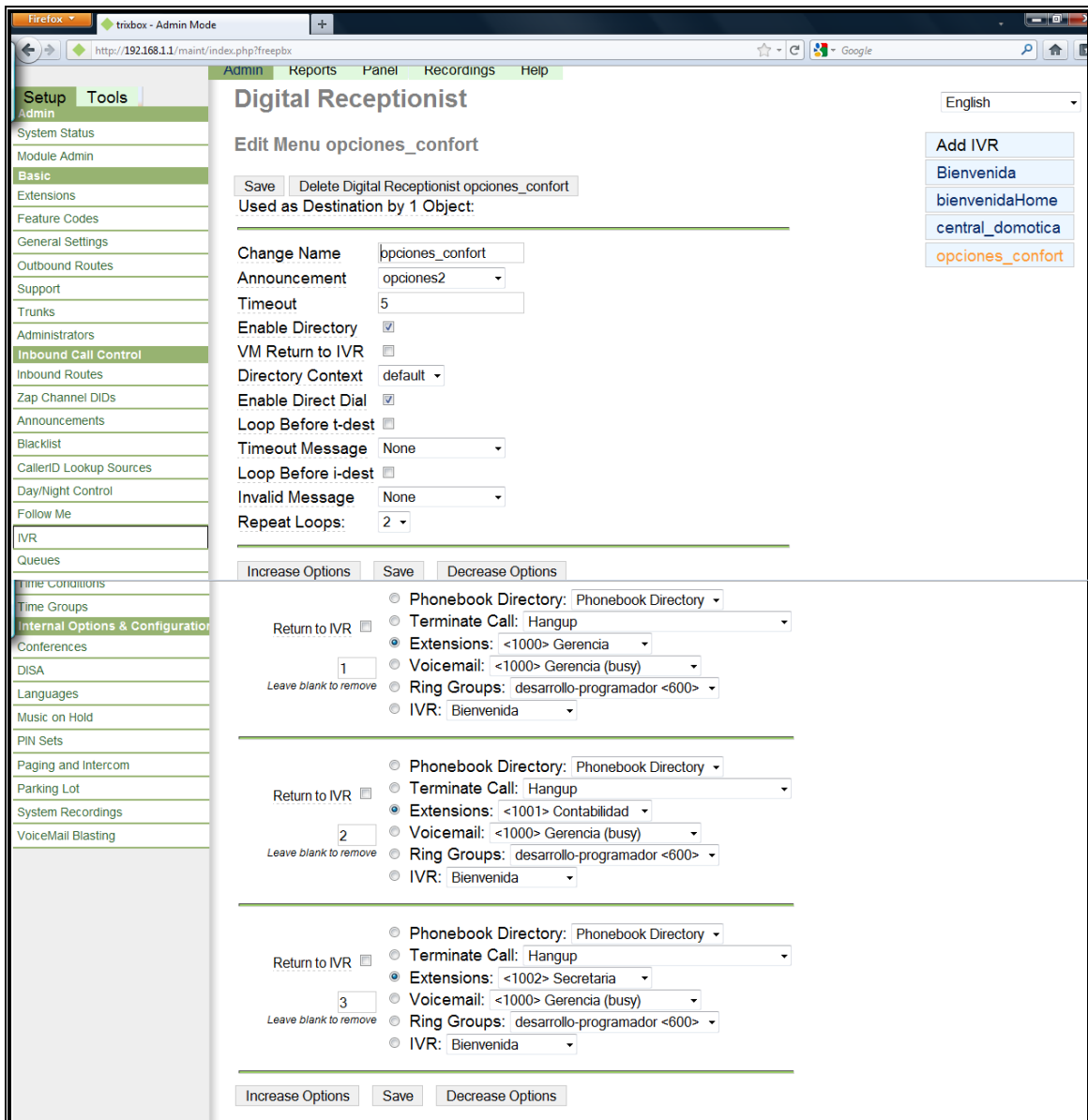


Figura (4.11) Configuración del IVR3

4.2 PRUEBAS Y RESULTADOS

Después de comprobar el correcto funcionamiento del Hardware y del Software, es necesario realizar pruebas de funcionamiento de todo el sistema, para comprobar que la red de módulos X10 y los scripts de control funcionen correctamente según las necesidades del usuario.

El análisis de pruebas y resultados está enfocado a comprobar que los objetivos planteados en este proyecto se hayan cumplido a cabalidad, verificando que los scripts diseñados para confort funcionen adecuadamente permitiendo el control

de los módulos X10, y comprobando que el sistema de seguridad funcione mediante el monitoreo con la cámara web.

4.2.1. PRUEBAS DE FUNCIONAMIENTO DE MONITOREO Y CONFORT

Estas pruebas consistieron en correr el script de monitoreo (figura 4.12), él que verifica el encendido, apagado de los módulos X10 y el estado en que se encuentran.

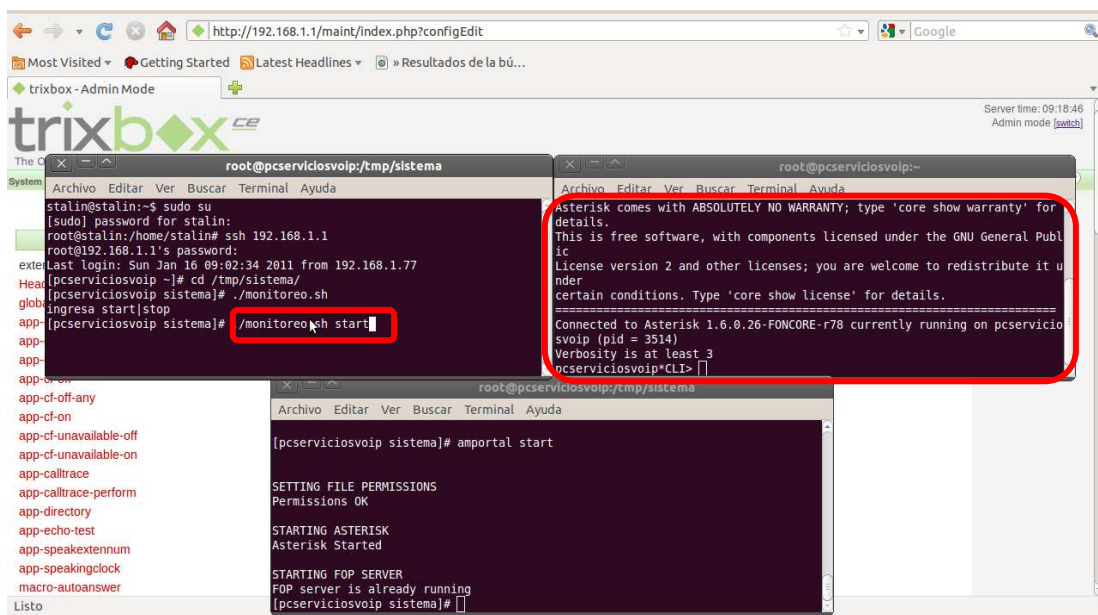


Figura (4.12) Inicio del Script de monitoreo

La consola de Asterisk provee información en tiempo real de su actividad y de los programas en php usados en las aplicaciones de seguridad y confort. Esta información es útil para diagnosticar fallas o errores en la configuración de la central VoIP.

Realizando una llamada telefónica desde un celular móvil se comprobó el encendido y apagado de los módulos X10 con el uso del código de la tabla 3.1 (Código para comandar los módulos X10), el mismo código se utilizó para conocer el estado de los módulos X10 disponibles (figura 4.13), también se verificó el acceso a la central mediante una clave de digitación conocida solo por el usuario, que permite ingresar a las opciones de seguridad y confort, y se evidenció que los intervalos de retardo en el envío de los comandos X10 son aceptables.

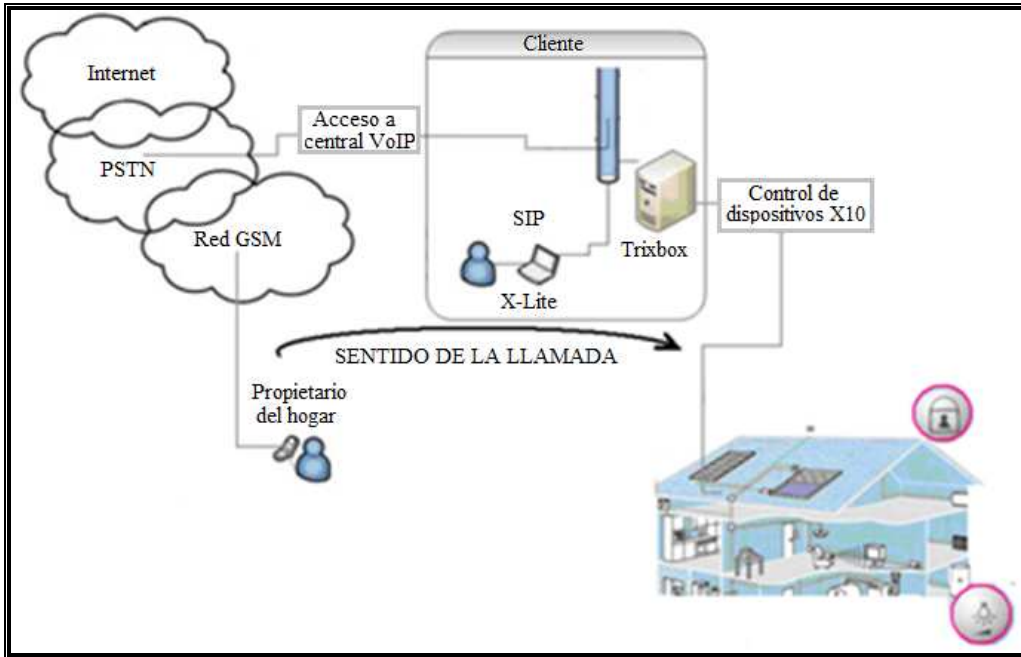


Figura (4.13) Representación del acceso a las opciones de confort y seguridad

4.2.2 PRUEBAS DE FUNCIONAMIENTO DE SEGURIDAD

Se hizo la activación de la seguridad por medio de una llamada desde un teléfono celular, activándose inmediatamente después de 3 minutos (figura 4.14).

```

trixbox - Admin Mode-Mozilla Firefox
http://192.168.1.1/maint/index.php?configEdit
trixbox - Admin Mode
Server time: 09:21:21
Admin mode [login]

root@pcserviciosvoip/tmp/sistema
[pcserviciosvoip ~]# cd /tmp/sistema/
[pcserviciosvoip sistema]# ./monitoreo.sh
[pcserviciosvoip sistema]# ./monitoreo.sh start
[pcserviciosvoip sistema]# ./seguridad.sh
[pcserviciosvoip sistema]# ./usomotion.sh: line 43: kill: (2664) - No such process
motion: no process killed
Killed
[pcserviciosvoip sistema]# /tmp/sistema/./usomotion.sh: line 43: kill: (
2664) - No such process
[pcserviciosvoip sistema]#
[pcserviciosvoip sistema]# amportal start
SETTING FILE PERMISSIONS
Permissions OK
STARTING ASTERISK
Asterisk started
STARTING FOP SERVER
FOP server is already running
[pcserviciosvoip sistema]#
  
```

Figura (4.14) Inicio del script de seguridad

Mediante una simulación se violentó la seguridad del hogar comprobando instantáneamente que la central VoIP genera una llamada hacia un número

telefónico dado por el usuario, en donde se puede localizar al propietario del hogar e informarle lo sucedido.

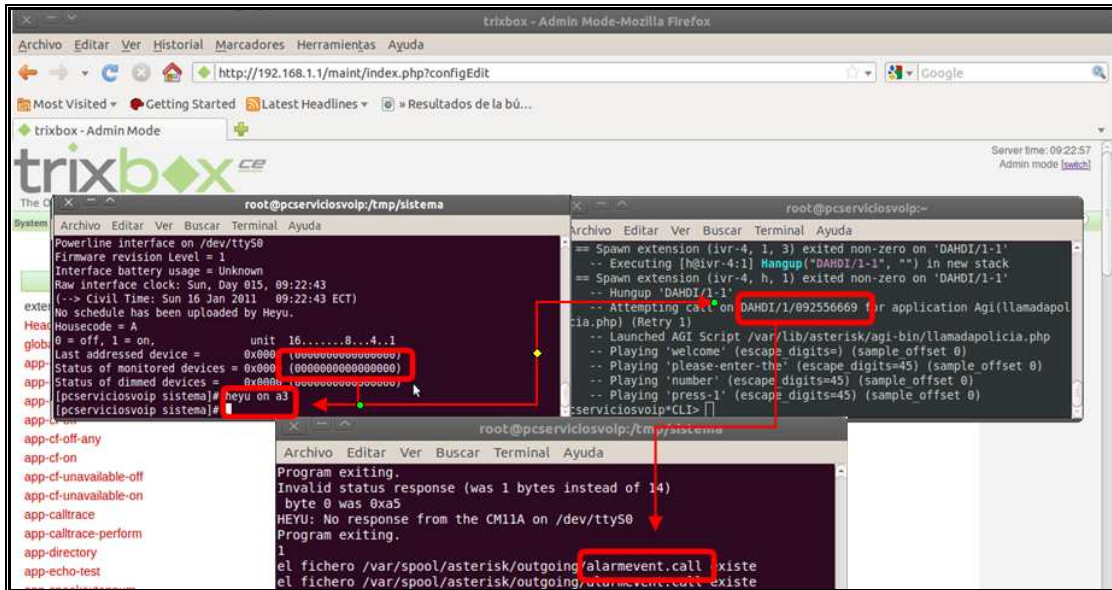


Figura (4.15) Activación del informe de la violación al sistema de seguridad

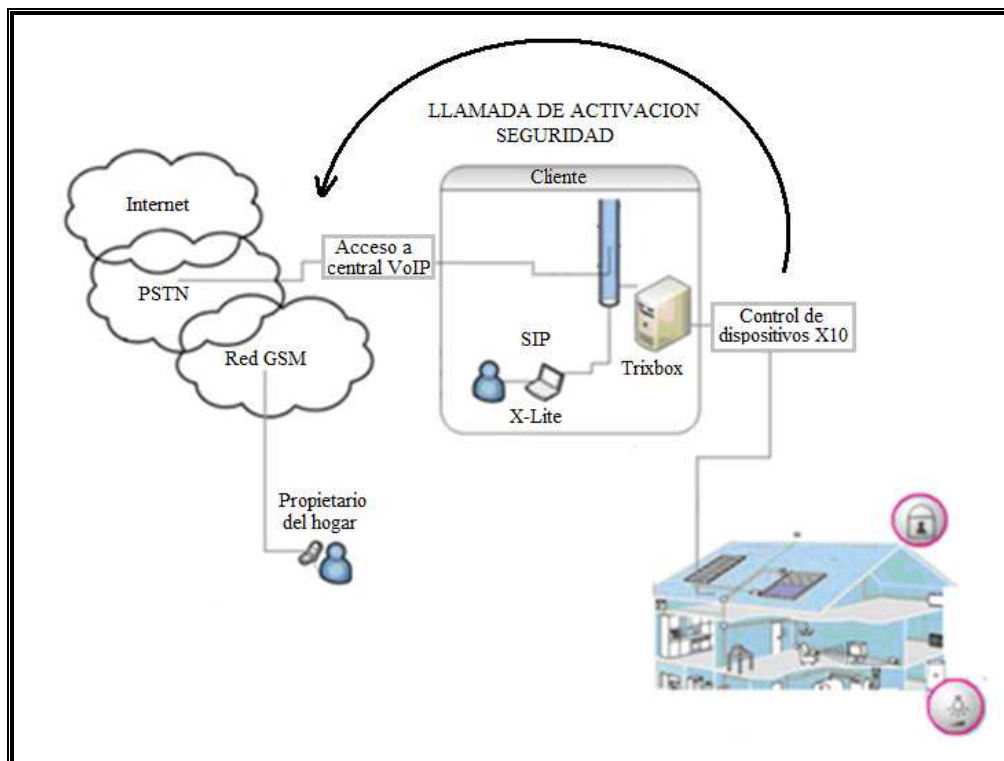


Figura (4.16) Representación de la llamada de alarma de la central al usuario

Una vez activada la llamada de alarma (figura 4.16), el usuario puede decidir si se genera una nueva llamada con una grabación donde se indica a otro número que se ha violentado la seguridad (policía, bomberos), para comprobar esta opción se configuró que la siguiente llamada se realice a la extensión 1010 (figura 4.17) del servidor VoIP.

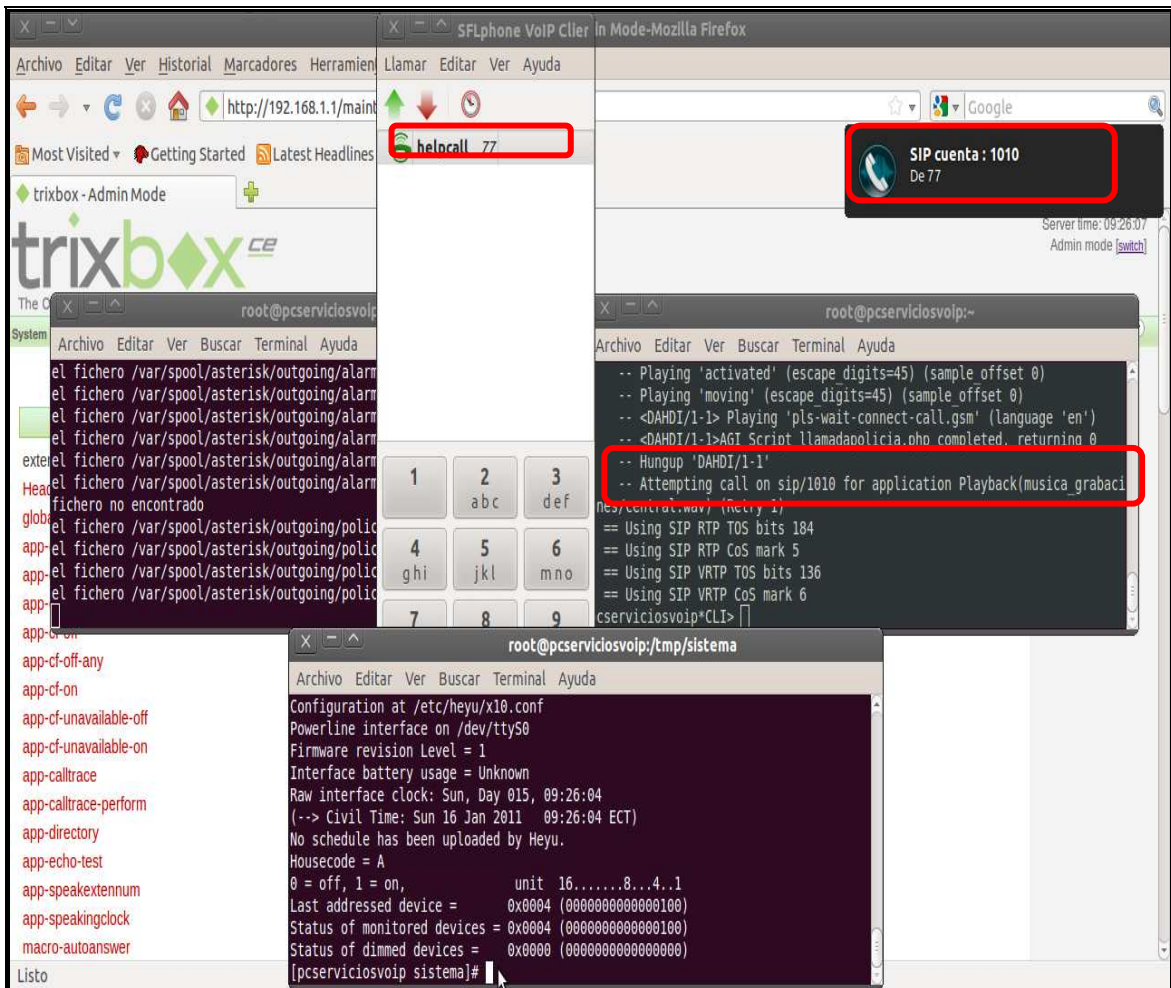


Figura (4.17) llamada de emergencia (policía, bomberos)

Flash Operator Panel (figura 4.18) permite observar el resultado de las llamadas realizadas en el PBX de Asterisk, comprobando que las llamadas de alarma y la llamada con la grabación “la seguridad ha sido violentada” han sido generadas al finalizar la primera llamada.

Number of calls: 118

	Calldate	Channel	Source	CLid	Dst	Disposition	Duration
1.	2011-08-25 10:45:17	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:38
2.	2011-08-25 10:45:02	SIP/1010-0...	1010	"device" <1010>	s	ANSWERED	00:08
3.	2011-08-25 10:42:07	SIP/1010-0...	1010	"tesis" <1010>	1000	ANSWERED	00:34
4.	2011-08-25 10:38:44	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:36
5.	2011-08-25 10:37:47	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:34
6.	2011-08-25 10:35:26	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:32
7.	2011-08-25 10:32:07	SIP/1010-0...	1010	"device" <1010>	7777	ANSWERED	00:32
8.	2011-08-25 10:30:14	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	01:09
9.	2011-08-25 10:21:33	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:32
10.	2011-08-25 08:36:46	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:59
11.	2011-08-25 08:35:28	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:47
12.	2011-08-25 08:34:35	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:41
13.	2011-08-25 08:32:57	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:57
14.	2011-08-25 08:31:27	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:54
15.	2011-08-25 08:28:38	SIP/1000-0...	1000	"device" <1000>	1	ANSWERED	00:53
16.	2011-08-25 08:25:59	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:53
17.	2011-08-25 08:25:03	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:46
18.	2011-08-25 08:23:56	SIP/1000-0...	1000	"device" <1000>	1	ANSWERED	00:40
19.	2011-08-25 08:20:51	SIP/1010-0...	1010	"device" <1010>	1	ANSWERED	00:40

Figura (4.18) Pantalla Flash Operator Panel de pruebas de llamadas realizadas

4.2.3 PRUEBAS DE FUNCIONAMIENTO DE VIDEO SEGURIDAD

Se realizó la activación de la cámara web mediante la opción de la llamada de alarma, que permite usar la cámara mediante una dirección IP pública por medio del puerto 8081 (figura 4.19).

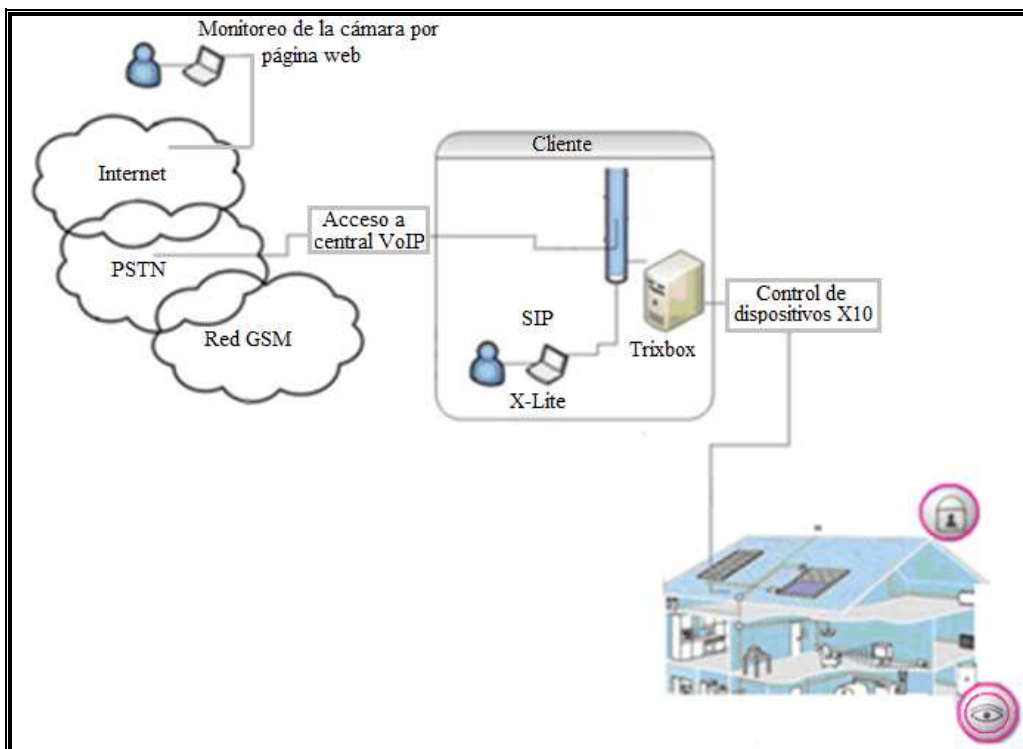


Figura (4.19) Representación del uso de la cámara web para monitoreo desde internet

El script para el uso de la cámara web desactiva los scripts de monitoreo para el confort y el script de seguridad que verifica el estado del detector de movimiento, de esta forma se asegura que el servidor no sature la memoria virtual.

Mediante esta prueba se pudo hacer efectivo el intercambio de imágenes con un retardo de 4 segundos desde la cámara web hasta un computador remoto, además se realizó un tracert (figura 4.20) en Windows para seguir la pista de los paquetes enviados por el servidor VoIP.

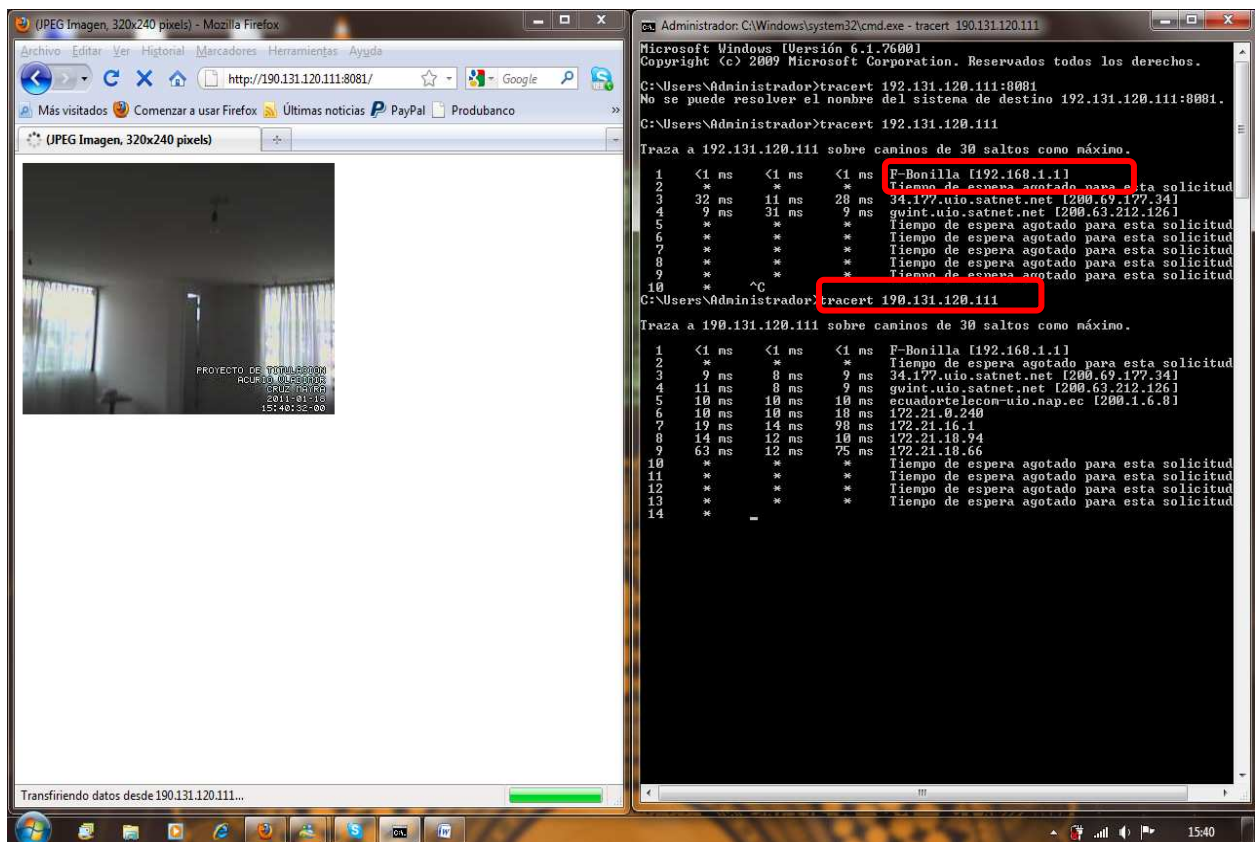


Figura (4.20) Visualización de la prueba del uso de la cámara web

Para realizar esta prueba se hizo un NAT(Network Address Translation - Traducción de Dirección de Red) en el servidor de VoIP.

Con el uso del puerto 8081 se pudo acceder a la cámara web por dos computadores distintos, evidenciando un tiempo de 4 segundos de retardo en la recepción de las imágenes. (Figura 4.21-4.22)

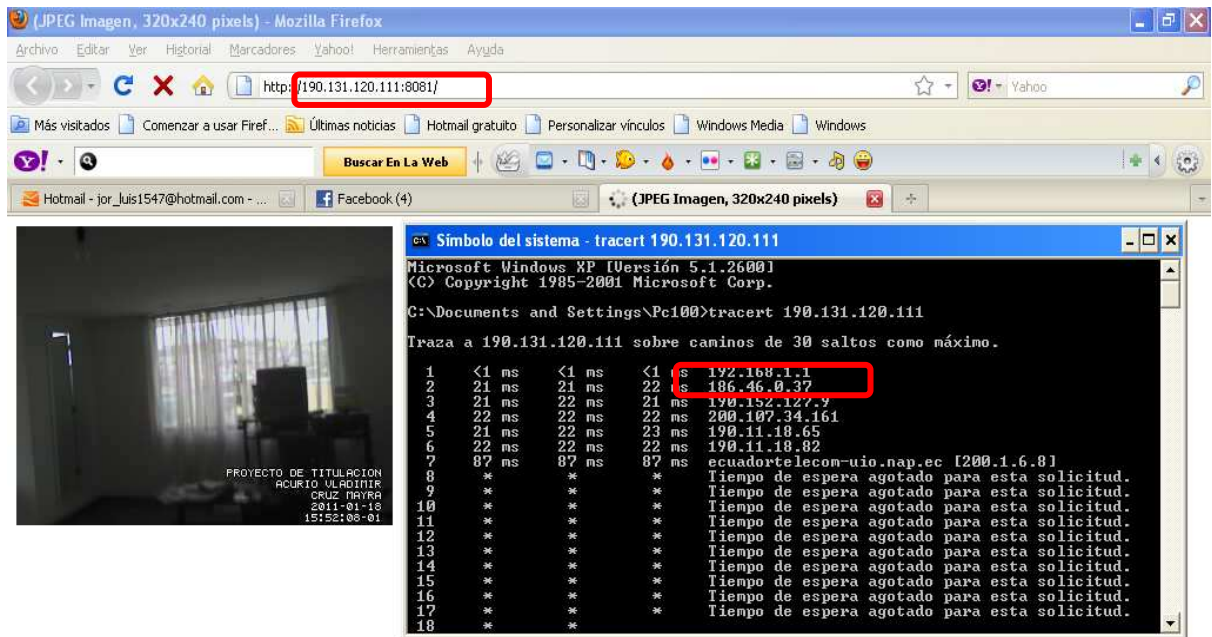


Figura (4.21) Captura de imagen computador 1

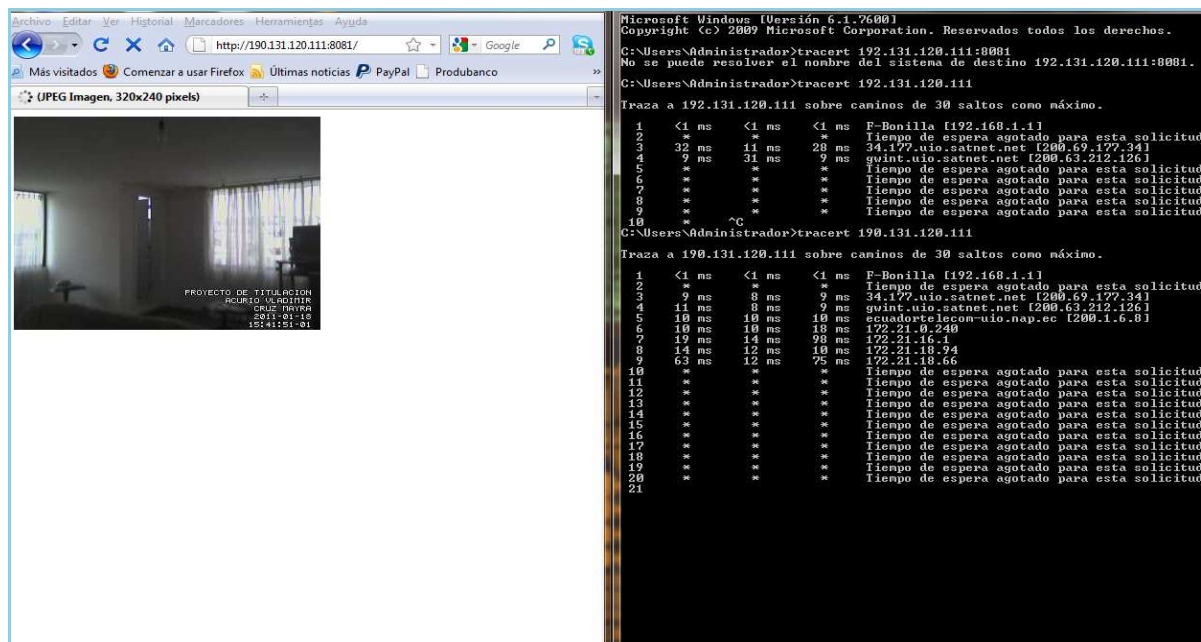


Figura (4.22) Captura de imagen computador 2

RESULTADOS:

La configuración de la central domótica VoIP fue exitosa, el registro de cada una de las cuentas SIP para los usuarios y la configuración de los softphones Zoiper tanto en el sistema operativo Windows y Linux funcionaron correctamente, la tarjeta PCI Ambient 3200 nos permitió realizar llamadas hacia la PSTN desde la

central domótica o desde cualquier cliente SIP, así como el ingreso de comunicaciones desde la red telefónica pública al interior de la red de VoIP.

Para comprobar esto se realizó:

- Una llamada por parte del cliente desde un número convencional y un número celular a la central domótica.
- Al activar la llamada de emergencia violando la seguridad se comprobó las llamadas desde la central hacia fuera de la red VoIP.

Las llamadas se establecieron sin problemas y con resultados favorables, cuando una llamada es contestada, automáticamente una grabación de voz de bienvenida es reproducida por la central, el cliente tiene dos opciones puede continuar la llamada normalmente digitando 1 o ingresar a la central domótica digitando 3.

Al digitar 3 la central solicita la clave de acceso, el usuario debe digitar una clave de 4 números para acceder a las opciones de seguridad y confort, se evidenció retardos en la comunicación cuando la central se encuentra ejecutando varios procesos.

El CDR de Asterisk guardó la información de los registros de llamadas realizadas, donde se puede verificar horarios, duración e identificación de llamadas entrantes y salientes.

Los servicios de seguridad y confort, fueron satisfactorios a las necesidades del cliente o usuario, se realizaron pruebas en el área de seguridad activando el sensor de movimiento y la cámara web, y en el área de confort encendiendo y apagando luces y equipos electrónicos (televisor, radio).

4.3 COSTO DE IMPLEMENTACIÓN Y DISEÑO

La tabla 4.2 detalla el hardware necesario para la implementación de la central domótica VoIP basada en Trixbox y sus respectivos costos, para la selección del CPU se utilizó las características dadas en el capítulo 3.

DESCRIPCIÓN	CANTIDAD	PRECIO U. (USD)	PRECIO T. (USD)
CPU: Procesador Pentium III con 500MHZ, Disco duro 150GB, 1GB de RAM, 1 tarjeta de red 10/100 Mbps	1	70	70,00
Módulo actuador X10 LM465	2	12,99	25,98
Módulo controlador X10 CM11A	1	42,79	42,79
Módulo X10 Sensor de presencia MS16A	1	24,99	24,99
Módulo transceptor X10 TM751	1	15	15,00
Tarjeta PCI fax-modem(FAX modem Intel 537PG y 537PU , Motorola 62802-51, Ambient 3200)	1	12	12,00
Cámara web Intel CS430	1	12	12,00
PRECIO DEL PROTOTIPO			202,76

Tabla (4.3) Precios de los materiales utilizados para el prototipo

El costo del diseño se ejecuta según los requerimientos mínimos para brindar confort, seguridad y la creación de los scripts para monitorear los módulos X10.

DESCRIPCIÓN	PRECIO TOTAL (USD)
Scripts y diseño	60,00
Precio del prototipo	202,76
PRECIO TOTAL DEL PROTOTIPO	262,76

Tabla (4.4) Precio total del prototipo

4.4 ANÁLISIS DE COSTOS

El bajo precio del CPU es porque son equipos que se encuentran en el hogar (computadores antiguos), con su uso se busca fomentar el reciclaje, los valores de los módulos X10 se los tomó de la página de ActiveHome y los costos de una cámara web varían de acuerdo al fabricante y a sus características, se escogió una cámara económica que se pueda utilizar en el sistema operativo Linux. El costo del diseño dependerá de las características que el propietario del hogar desee para el nivel de confort y de seguridad, ya que si desea mayor confort será necesario mayor del número de módulos X10 que permitan satisfacer los requerimientos del propietario del hogar.

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

La implementación del prototipo de una central domótica VoIP basada en Trixbox funcionó según los objetivos planteados, brindando al usuario seguridad y confort mediante la integración de hardware y software a un bajo costo.

- La central domótica basada en el software Trixbox se convierte en una central flexible y fácil de administrar, con varias aplicaciones y servicios VoIP, y con tarjetas PCI compatibles soporta la conexión con la telefonía tradicional.
- Trixbox al ser un software de código abierto basado en Centos puede integrarse con aplicaciones desarrolladas para sistemas operativos Linux como Heyu y Motion.
- La central domótica VoIP basada en Trixbox permite ofrecer varias funcionalidades que pueden activarse por medio de una llamada a la central, obteniendo los siguientes atributos:
 - Confort: como creación de ambientes según los intereses y necesidades del usuario en todas las estancias de la casa.
 - Seguridad importante para el hogar mediante una alarma que recoge información del sensor de movimiento y de una cámara de vigilancia, informando cualquier anomalía al usuario o departamento de policía.
- La domótica ha dado un giro a la estructura del hogar, dándole vida propia, bajo la integración de cuatro pilares básicos: confort, seguridad, comunicaciones y gestión energética, su desarrollo está basado en la combinación de varias tecnologías al beneficio del usuario como telecomunicaciones, electrónica, informática.

- La implementación de la central domótica VoIP dió una mayor visión sobre los Sistemas de Vigilancia caseros, no sólo se profundizó en el estudio de los protocolos de comunicación como SIP, sino que permitió observar de forma general las grandes ventajas de Trixbox como PBX, considerándolo como un buen recurso en cualquier empresa por su facilidad de uso.
- Existen diversas tecnologías y protocolos que se utilizan actualmente para el desarrollo de sistemas domóticos, en el presente proyecto se eligió X10 por su sencillo protocolo de comunicación a través de las líneas eléctricas, ofreciendo automatización y control de los equipos eléctricos del hogar.
- El análisis de costos de la implementación de una central domótica VoIP en una casa u oficina, indicó que es accesible para la economía de la población de clase media y alta del país.
- Para realizar un pronóstico de mercado se optó por un método cualitativo de demanda, ya que no se tenía datos históricos de productos domóticos similares, al ser la central domótica VoIP un nuevo producto fue necesario efectuar una encuesta para conocer su grado de aceptación.
- Los scripts tienen como función principal interpretar órdenes, son programas basados en Shell que conectan las órdenes de un usuario con el núcleo del sistema, y al ser programables se puede modificar para adaptarlo a las necesidades de seguridad y confort

5.2 RECOMENDACIONES

- Difundir las aplicaciones y beneficios de la Domótica es un factor importante para su desarrollo. Todos los profesionales afines al área arquitectos, ingenieros, etc., deben involucrarse con esta nueva tecnología para dar a conocer mejor sus beneficios y alcances.
- Al implementar el prototipo sobre una vivienda construida se presentan varios inconvenientes respecto al cableado eléctrico, los módulos X10 realizan su comunicación a través de la línea eléctrica, y al tener un desorden en las instalaciones y un incumpliendo de las normas de cableado eléctrico es difícil la implementación de la central domótica.
- Es recomendable realizar la implementación de la central domótica sobre una vivienda o edificación a construirse, porque en los planos de la construcción se puede considerar el cableado eléctrico y exigir que se cumpla con todas las normas internacionales de la ICE para instalaciones eléctricas residenciales, así se podrá garantizar el uso correcto de los dispositivos X10, los que funcionan sobre la línea eléctrica (110V) transmitiendo señales de control de automatización entre sí.
- Para la implementación, en una edificación construida, es necesario realizar previamente un estudio sobre el estado del cableado eléctrico existente, conocer que normas eléctricas cumple y adecuarlos a su estructura.
- El acceso a la carpeta de imágenes que genera el Sistema de Vigilancia debe tener restricciones para que sólo personal autorizado tenga acceso, realizando una revisión periódica de las fotografías evitando una acumulación en el disco duro del servidor.
- Buscar que la visión de cobertura de la cámara web sea la más acorde, abarcando la mayor parte del hogar o en el caso del presente proyecto la

mayor parte de la oficina, y verificar que el rango de funcionamiento del detector de movimiento alcance al objetivo deseado.

- El bajo índice de desarrollo tecnológico en Ecuador es debido a factores como la pequeña inversión del producto interno bruto en el campo de la ciencia y tecnología, generando una brecha tecnológica con las grandes potencias mundiales, el gobierno debe buscar una alternativa para mejorar la inversión privada especialmente en el sector de la investigación, y además se debe incrementar el aporte económico por parte del estado al desarrollo de ciencia y la tecnología en las universidades, cumpliendo así con los artículos de la Constitución Nacional que garantizan el apoyo al avance tecnológico en nuestro país.

BIBLIOGRAFÍA

REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 1

LIBROS

- [6] LANDIVAR, Edgar, "Comunicaciones Unificadas con Elastix", primero edición, 2008, Págs. 180-181
- [15] DE SALAZAR, Rodrigo, "Sistema de voz sobre IP para redes inalámbricas en zonas rurales aisladas", Págs. 17,19,24

INTERNET

- [1] <http://www.jeuazarru.com/docs/VoIP.pdf>
- [2] <http://www2.tiendalinux.com/catalogs/tiendalx/DGM-TDM-FXS.html>
- [3] http://pdf-esmanual.com/books/3002/que_es_el_asterisk.html
- [4] <http://www.cs.columbia.edu/~andrea/new/documents/other/T-REC-G.114-200305.pdf>
- [5] <http://fonality.com/trixbox/>
- [7] <http://www.electricasas.com/page/13/>
- [8] <http://www.marmitek.com/es/soporte/marmitek-university/protocolo-x-10.php>
- [9] <http://neutron.ing.ucv.ve/revista-e/No5/JRozada.html>
- [10] <http://personales.com/venezuela/caracas/ucabx10/TSx10.htm>
- [11] <http://www2.udec.cl/~racuna/domotica/x10.htm>
- [12] <http://www.heyu.org/>
- [13] <http://www.lavrsen.dk/foswiki/bin/view/Motion/WebHome>
- [14] <http://www2.tiendalinux.com/catalogs/tiendalx/DGM-TDM-FXO.html>
- [16] http://ftp.iptel.org/pub/ser/0.8.14/doc/html/sip_introduction.html
- [17] <http://www.aquihayapuntes.com/x-10.html?start=1>
- [18] http://pitagoras.usach.cl/~eflores/lcc/cd_redes/VoIPAudit.pdf

REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 2

TESIS

- [3] http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-36625.pdf

LIBRO

- [1] ESTUDIO DE MERCADO SOBRE DOMOTICA, CIEN S.A., Pág.14

INTERNET

- [2] <http://www.ecuadorencifras.com/cifras-inec/cienciaTecnologia.html#>

REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 3

INTERNET

- [1] <http://www.x10.com/whatsincluded/CK12AS-12PC.html>
- [2] <http://www.nova.es/~mromero/domotica/esquema.htm>
- [3] <http://www.telephonyware.com/telephonyware/products/digium-x100p.html>
- [4] <http://www.packtpub.com/article/asterisk-gateway-interface-scripting-with-php>