UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

CARRERA INGENIERÍA ELECTRÓNICA

DISEÑO, CONSTRUCCIÓN E IMPLEMENTACIÓN DE UN DISPOSITIVO DE SEGURIDAD QUE PERMITE LA INTERCOMUNICACIÓN CON AUDIO Y VIDEO ENTRE DOS PUNTOS Y LA ACTIVACIÓN REMOTA DE ELEMENTOS DE SEGURIDAD.

TESIS PREVIA A LA OBTENCION DEL TITULO DE:

INGENIERO ELECTRÓNICO

TESIS PREVIA A LA OBTENCION DEL TITULO DE:

INGENIERA ELECTRÓNICA

Autores:

Mateo Santiago Rengel Rivera.

Mariela Alexandra Jimbo Jérez.

Director:

Ing. Juan Paúl Inga Ortega.

CUENCA, ENERO DE 2015

AUTORIA

Las ideas y contenidos expuestos en el presente proyecto, son de exclusiva responsabilidad de los autores y el patrimonio intelectual le pertenece a la Universidad Politécnica Salesiana

Cuenca, Enero de 2015

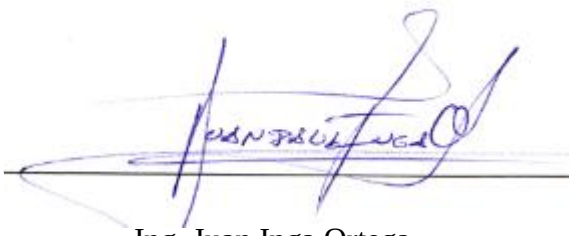
Mateo S. Rengel Rivera.

Mariela A. Jimbo Jérez

CERTIFICO:

En calidad de DIRECTOR DE LA TESIS “Diseño, construcción e implementación de un dispositivo de seguridad que permite la intercomunicación con audio y video entre dos puntos y la activación remota de elementos de seguridad” elaborada por Mateo Rengel Rivera, Mariela Jimbo Jérez, declaro y certifico la aprobación del presente trabajo de tesis basándose en la supervisión y revisión de su contenido.

Cuenca, Enero de 2015



Ing. Juan Inga Ortega.

DIRECTOR DE TESIS

AGRADECIMIENTOS

A mis padres por apoyarme en cada momento de mi carrera en especial en los más difíciles. A Santiago Rivera por la confianza y el apoyo brindado, gracias por ser como un hermano para mí. A Juan Inga por su apoyo incondicional y sabios consejos que han hecho de este proyecto un trabajo excelente. A Edison Segarra que con su gran conocimiento ha brindado asesoría y gran apoyo al proyecto como un amigo que ha estado en las buenas y en las malas. Es innumerable mencionar a todos a quieren debo agradecer, pero lo saben, Rene R, Juan G., Carlos S., sin ustedes esto no se habría logrado, Gracias.

Mateo

Quiero agradecer a Dios por la vida, a mis padres por el apoyo incondicional entregado durante toda mi vida, a mi director de tesis Juan Inga por su entereza y consejos brindados en el transcurso del proyecto. También quiero agradecer de manera muy especial a Edison Segarra por ser un amigo durante el desarrollo de este proyecto, a Jorge y María Criollo, Santiago Rivera, Juan García, Carlos Suqui y a todas las personas que estuvieron involucradas ya que sin su apoyo no hubiera sido posible culminar esta etapa de mi vida.

Mariela

DEDICATORIA

Dedico este trabajo a mis padres ante todo, he aquí el fruto de su trabajo y esfuerzo. También a mis 4 abuelitos, que aún vivos siempre han deseado verme lograr cumplir este objetivo. Finalmente a mis hermanos que me han aguantado y apoyado en todo. Todos ustedes son mi fortaleza día tras día.

Mateo

A mis padres, por el gran esfuerzo que han hecho por mí, por incentivarme a diario a lograr mis metas, a mis hermanos por la paciencia y entusiasmo brindado durante esta etapa de mi vida.

Mariela

INDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ABREVIATURAS USADAS

AES	Advanced Encryption Standard
AFP	Apple File Protocol
AGI	Asterisk Gateway Interface
APT	Apple Talk Protocol
ATM	Asynchronous Transfer Mode
CCTV	Closed Circuit Television
CRM	Customer Relationship Management
CSC	Consejo de Seguridad Ciudadana
DDP	Delivery Datagram Protocol
DTMF	Dual-Tone Multi-Frequency
DVR	Digital Video Recorder
FFTH	Fiber From The Home
FSP	Frames per Second
FTP	File Transfer Protocol
FTTB/C	Fiber To The Building
FTTCab	Fiber To The Cabinet
GEM	GPON Encapsulation Method
GPON	Gigabit-capable Passive Optical Network
GSM	Global System for Mobile
HTTP	HyperText Transfer Protocol
HTTPS	Hyper Text Trasfer Protocol Secure Socket Layer
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPX	Internet Protocol Exchange
ITU	International Telecommunication Union
LAN	Local Area Network
MAC	Media Access Control
MDI	Medium Dependent Interface
MDUs	Multi-Dwelling Units
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MPEG	Moving Picture Experts Group
NetBEUI	Network Basic Extended User Interface

NETBios	Network Basic Input/Output System
NIC	Network Interface Card
ODN	Optical Distribution Network
OLT	Optical Line Termination
ONT	Optical Network Terminal
ONU	Optical Network Unit
OSI	Open System Interconnection
PBX	Private Branch Exchange
PD	Powered Device
PoE	Power over Ethernet
PON	Passive Optical Network
POTS	Plain Old Telephone Service
PSE	Power Sourcing Equipment
PTZ	Pan / Tilt / Zoom
RDSI	Red Digital de Servicios Integrados
RTC	Clock Time Real
RTP	Real Time Protocol
RTPS	Real Time Streaming Protocol
SAI	Sistema de Alimentación Ininterrumpida
SBC	Session Border Controller
SCCP	Skinny Call Control Protoco
SDH	Synchronous Digital Hierarchy
SDHC	Secure Digital High Capacity
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TIC	Tecnología de la Información y Comunicaciones
TIR	Tasa Interna de Retorno
UDP	User Datagram Protocol
VAN	Valor Actual Neto
VCR	Video Cassette Recorder
VoIP	Voz sobre IP

WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
xDLS	x Digital Subscriber Line

INTRODUCCIÓN

La Constitución Ecuatoriana establece en su Régimen del Buen Vivir que: "La seguridad ciudadana es el objetivo que el Estado persigue con la ayuda de la ciudadanía y demás organizaciones de bien público para asegurar la convivencia pacífica de las personas, prevenir formas de violencia y promover una cultura de paz[1]".

Los sistemas de video-vigilancia son ampliamente utilizados en nuestra sociedad con fines de garantizar la seguridad de los bienes y las personas en diferentes entornos. Son herramientas útiles a la hora de ayudar a detectar posibles amenazas, persuasión de delincuentes y busca evitar robos, agresiones y vandalismo.

De esta forma, el uso de sistemas de seguridad en tiempo real está desarrollándose a pasos agigantados y se debe conocer cómo utilizar toda la tecnología disponible acoplándola a nuestras necesidades para brindar servicios de seguridad óptimos y eficaces.

Con el desarrollo de la transmisión de datos por fibra óptica y la avanzada funcionalidad y flexibilidad del protocolo de internet (IP), es posible transmitir datos como voz y vídeo a elevadas velocidades usando un gran ancho de banda. Usar estas características de transmisión de datos permite mejorar sistemas de seguridad implementando comunicación en tiempo real entre personas y dispositivos.

En este sentido, en el avance de la tecnología en seguridad se crearon puntos de auxilio para poder estar al alcance de cualquier situación y poder generar una rápida respuesta.

[1] http://educacion.gob.ec/wp-content/uploads/downloads/2012/08/Constitucion.pdf

Así, el presente proyecto busca combinar “puntos de auxilio” o “puntos seguros” con sistemas de video-vigilancia en conjunto con altavoces, luces estroboscópicas, entre otros, para incrementar las características de seguridad. El proyecto propone emplear estos puntos de auxilio en zonas en donde pueden darse actos delictivos, esperando incrementar la seguridad de la ciudadanía monitorizando la situación, garantizando una atención y acción inmediata.

Además propone colaborar con la seguridad a la ciudadanía en zonas de posible peligro y brindar un mejor control al Servicio Integrado de Seguridad “ECU 911”, proyecto que está a cargo el “Consejo De Seguridad Ciudadana (CSC)”.

ANTECEDENTES

El Consejo de Seguridad Ciudadana del cantón Cuenca es un organismo técnico con autonomía administrativa, operativa, patrimonial y financiera; sin fines de lucro, que tiene como función primordial la de planificar y coordinar con las entidades partícipes de la seguridad ciudadana, las políticas y las acciones que debe desarrollar cada una de las instituciones, en el marco del respeto a sus facultades y funciones establecidas en la Constitución de la República del Ecuador y más leyes pertinentes[2].

El Consejo de Seguridad Ciudadana, en forma permanente y transparente, formula y desarrolla políticas y acciones que contribuyen a promover la seguridad ciudadana en el Cantón Cuenca. Para ese fin impulsa la implementación del trabajo planificado, coordinado, articulado y sostenido de todas las instituciones responsables de su ejecución, así como del seguimiento, evaluación y monitoreo de su efectivo cumplimiento hacia la satisfacción de las necesidades y demandas ciudadanas para su seguridad.

Como ente Coordinador, el Consejo de Seguridad Ciudadana del cantón Cuenca tiene la finalidad de fortalecer y apoyar las acciones operativas que realiza cada institución que forma parte de la Asamblea y del Directorio.

El Consejo de Seguridad Ciudadana del cantón Cuenca cuenta con el Plan de Seguridad y Convivencia Ciudadana, y dentro del mismo en el Eje de Prevención se encuentra el Proyecto: “Puntos y Rutas Seguras”.

[2] Estatuto Orgánico Funcional por Procesos del Consejo de Seguridad Ciudadana del Cantón Cuenca. Julio 2014

El tema de grado propuesto cumplirá las necesidades de dicho proyecto del Consejo de Seguridad Ciudadana, ayudando a combatir la inseguridad en la ciudad, dando un mejor control sobre los lugares de riesgo al “ECU 911” y brindando un servicio eficiente y de calidad.

JUSTIFICACIÓN

En los llamados puntos seguros se implementaran dispositivos de seguridad, los mismos que tienen como objetivo brindar asistencia a personas que así lo requieran, obteniendo respuesta inmediata mediante la comunicación en tiempo real con el ECU-911, con el objeto de prevenir posibles hurtos, persuadir delincuentes, monitorear eventos, obtener ayuda inmediata de las instituciones de seguridad, etc.

El CSC desea que se diseñe e implemente un dispositivo de fabricación nacional, que pueda satisfacer las necesidades que se plantean mejorando la calidad, beneficios y costos de los dispositivos existentes en el mercado internacional.

Por esto, mediante el proyecto de grado propuesto, se busca solventar las necesidades que el CSC propone sobre el proyecto "Puntos y Rutas Seguras", garantizando la eficiencia, funcionalidad ajustada a las necesidades del cantón, y considerables mejoras en el costo, obteniendo un producto nacional de calidad.

Este dispositivo permitirá brindar servicios como:

- Atención inmediata a personas que se encuentren en alguna situación de peligro.
- Monitoreo en tiempo real de la situación.
- Persuasión de delincuentes manejando dispositivos visuales y sonoros remotamente.
- Dispositivo resistente a la intemperie y vandalismo.

CAPITULO 1. FUNDAMENTACIÓN TEÓRICA

1.1. Introducción

El presente capítulo pretende introducir los conceptos básicos de las redes de comunicación IP, características, funcionamiento, topologías de red y tecnologías de red IP. Además para la transmisión de datos se presentaran los protocolos utilizados para el caso de vídeo IP y los métodos para la transmisión del mismo.

Al estar basados en una red GPON[3] (Red Óptica Pasiva con capacidad de Gigabit) se determinará el concepto, características, protocolos, arquitectura y sus elementos.

Para terminar se presentarán los conceptos de video-vigilancia, como ha evolucionado, que tipos de cámaras existen y el estado del arte de los sistemas de seguridad sobre IP.

1.2. Redes de Comunicación IP

1.2.1. Generalidades de una Comunicación de Redes

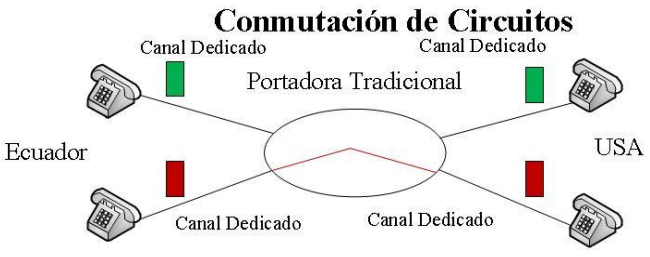
Una red de comunicación de datos o red de computadoras es un conjuntos de equipos, dispositivos y software conectados entre sí por un medio físico de transmisión que envía y recibe impulsos eléctricos, ondas electromagnéticas o luz en el que se trasmite información[1].

[3] Red utilizada para la conexión de la vídeo vigilancia en la ciudad (Ver sección 1.3)

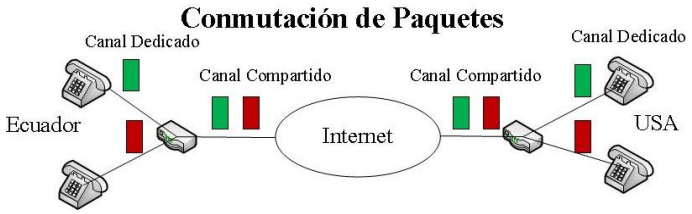
El protocolo de internet es un estándar de comunicación entre dispositivos y servicios integrados de los consumidores para propósitos como telefonía, seguridad, entretenimiento, negocios, entre otros. El Internet es el factor más potente que guía el proceso de convergencia de todos los dispositivos hacia un estándar de comunicación común (IP); la suite del protocolo Internet está compuesto por el protocolo internet (IP) y el protocolo de trasporte (TCP); esto da lugar al término TCP/IP que se refiere a la familia del protocolo completo[2].

Las redes que se basan en la tecnología IP se componen de dos partes principales, estos son: los nodos y enlaces. En una red, se denomina nodo a cualquier dispositivo conectado a esta, como un computador personal, cámara, etc., estos se comunican a través de los enlaces que vienen a ser los medios para la transmisión de la información que son un cable de par trenzado, fibra óptica, cable coaxial o medios inalámbricos.

Existen básicamente dos técnicas de transmisión entre redes. La primera es la denominada red de conmutación de circuitos (figura 1.1.a) que consiste en crear un circuito cerrado entre dos nodos de la red para establecer una conexión física, es la más antigua y es mayormente utilizada en la telefonía. La segunda es la red de comunicación de paquetes (figura 1.1.b), esta es la tecnología que utilizan las redes basadas en IP, aquí cada paquete puede ser trasmitido sobre diferentes rutas.



(a)



(b)

Figura 1.1. *(a) Conmutación de circuitos y (b) conmutación de paquetes*

Como se puede observar en la figura 1.1.a, en la conmutación de circuitos por ejemplo, al realizar una llamada desde Ecuador hasta USA, la portadora conmuta los circuitos de tal manera que genera un canal dedicado para la intercomunicación entre ellos, es decir existe una conexión física entre estos; ningún otro usuario puede usar este canal mientras esté ocupado. En la conmutación de paquetes, la información de cada usuario va hacia un router (enrutador), este se encarga de dividir los mensajes de todos los usuarios en paquetes e irlos ubicando sobre un mismo canal, esta información se envía a través de una red hacia el destino correspondiente, en el router receptor se realiza el proceso inverso obteniendo del canal los paquetes de todos los usuarios.

1.2.2. Fundamentos de Transmisión

La transmisión de datos consiste en enviar información a través de un medio ya sea este guiado (cable coaxial, par de cobre, fibra óptica) o no guiado (microondas, satélite, WiFi, entre otros).

La tecnología de red basada en IP sustituye a las tecnologías de red antiguas como: Frame Relay, Modo de Transferencia Síncrona (ATM) y X.25[3], siendo estas más flexibles y económicas que sus antecesoras a la hora de transmitir información ya que IP puede ser utilizado sin importar el medio de transmisión. Las propiedades de esta tecnología tienen que ver con la representación, gestión y transmisión de la información a través de un medio; la información que se desea transmitir puede estar en dos formas, como datos analógicos o datos digitales.

Los datos analógicos se expresan como ondas continuas variables por lo que representan valores continuos, la voz y el vídeo son ejemplos de ello. Todas las señales que se encuentran en la vida real son analógicas.

Los datos digitales se representan como secuencias de bits, la digitalización de señales permite que la información analógica sea representada como una secuencia de unos y ceros y así se pueda transmitir datos de cualquier tipo, como textos, voz, imágenes, sonidos o vídeo. Los datos digitales pueden ser procesados y modificados según nuestra necesidad, pudiendo comprimirlos, filtrarlos, encriptarlos y otras funcionalidades que los datos analógicos no lo permiten.

1.2.3. Tecnologías de red IP

En la actualidad el protocolo de Internet (IP) constituye el protocolo de comunicación informática más ampliamente utilizado.

El protocolo de TCP/IP se conecta a través de una red Ethernet, la misma que ofrece una red rápida a un precio razonable y es una totalmente escalable, por esto en la actualidad la mayoría de ordenadores modernos se suministran con una interfaz Ethernet integrada o permiten alojar fácilmente una tarjeta de interfaz de red Ethernet (NIC, Network Interface Card[4]). Entre los principales tipos de Ethernet están:

- 10 Mbit/s (10 Mbps) Ethernet
- Fast Ethernet (100 Mbit/s)
- Gigabit Ethernet (1000 Mbit/s)
- 10 Gigabit Ethernet (10 000 Mbit/s)

1.2.3.1. Alimentación a través de Ethernet PoE (Power over Ethernet)

La alimentación a través de Ethernet (PoE) o conocida como el estándar IEEE 802.3af es una tecnología que permite el suministro de energía eléctrica a los dispositivos en una red, utilizando el mismo cable que se usa para la transmisión de datos[5].

La alimentación mediante PoE, elimina el cableado requerido para el suministro eléctrico, permite realizar instalaciones en lugares donde no se cuenta con tomas de energía eléctrica y existe la facilidad de ubicación de equipos. Además, los dispositivos cuentan con alimentación las veinte y cuatro horas del día, incluso en presencia de fallas ya que la alimentación por Ethernet está protegida por el Sistema de Alimentación Ininterrumpida (SAI).

La tecnología PoE puede integrar en una red dispositivos que posean dicha tecnología como los que no. La alimentación a través de Ethernet se activa cuando detecta un terminal de dispositivo compatible y bloquea ante dispositivos que carecen de dicho terminal.

El estándar IEEE 802.3af trabaja con cableado categoría 5[6] o superior, en la red se conocen dos dispositivos, el que proporciona la energía conocido como equipo de suministro eléctrico (PSE) y el dispositivo alimentado (PD). En la tabla 1.1 se presentan los valores de potencia para el PSE como para el PD.

Clase	**Nivel de potencia mínimo en PSE**	**Nivel de potencia máximo de un PD**	**Uso**
0	15.4W	0.44W-12.95W	Predeterminado

1	4.0W	0.44W-3.84W	Opcional
2	7.0W	3.84W-6.49W	Opcional
3	15.4W	6.49W-12.95W	Opcional
4	Tratado como clase 0		Reservado para usos futuros

Tabla 1.1. *Clasificación de potencia según IEEE 802.3af* [5]

Como funciona PoE[7]

La alimentación a través de Ethernet obedece a las normas establecidas en el estándar IEEE 802.3af en la cual se definen entre otras características los voltajes y corrientes necesarios para su funcionamiento, el tipo de cables y conexiones.

PoE, para su correcto funcionamiento consta de cuatro etapas las mismas que son necesarias para realizar la alimentación por el mismo cable de datos.

1. Protección de Polaridad. Sirve para proteger las conexiones ya que este bloque detecta la forma de alimentación ya sea por el mismo par usado para datos o el uso de pares alternativos para enviar la tensión.
2. Clasificación de Corriente y Resistencia. Sirve para determinar si el dispositivo a alimentar implementa PoE o no, para lo cual el PSE envía niveles de tensión definidos. En la tabla 1.2 se muestran dichos niveles, el primero sirve para detectar si el dispositivo implementa PoE, de ser así se aplican los siguientes niveles de voltaje según el dispositivo PD lo requiera.
3. Etapa de Control. Sirve para desactivar el convertidor DC/DC mientras el dispositivo está realizando la clasificación de la etapa 2.

4. Convertidor DC/DC. Para realizar los diferentes cambios de tensión, para lo cual se usa un convertidor Buck[4] DC/DC[8] el cual trabaja en un amplio rango de tensiones (36V-57V) en condiciones de mínima y máxima carga.

Fase	**Acción**	**Voltios**
Detección	Comprueba si el dispositivo conectado tiene una resistencia entre 15-33 kΩ	2.7-10
Clasificación	Comprueba la clase de dispositivo que es (tabla 1.1)	14.5-20.5
Inicio	Inicio de alimentación del dispositivo	>42
Operación Normal	Alimentación del dispositivo	36-57

Tabla 1.2. *Voltaje según IEEE 802.3af[7]*

1.2.4. Transporte de Datos

1.2.4.1. Direcciones IP

Una dirección IP (dirección del Protocolo de Internet) es un número exclusivo utilizado por los dispositivos para poder identificarse y comunicarse entre sí a través de una red utilizando el estándar de Protocolos de Internet[2].

[4] Buck o reductor es un convertidor de potencia DC/DC que obtiene a su salida un voltaje inferior al de su entrada.

1.2.4.2. IPv4

El protocolo de internet versión 4 usa direcciones de 32 bits, limitándola a $2^{32} = 4294967296$ direcciones únicas. Una dirección IPv4 está formada por cuatro números separados por un punto, cada número se encuentra entre un rango de 0 a 255; por ejemplo una dirección es: 192.168.10.20

Algunos bloques direcciones se han reservado para uso privado:

10.0.0.0/8	(mascara de red 255.0.0.0)
172.16.0.0/12	(mascara de red 255.240.0.0)
192.168.0.0/16	(mascara de red 255.255.0.0)

Estas direcciones son destinadas para el uso privado del internet por lo que no se enrutan hacia el internet público.

1.2.4.3. IPv6

Es la versión 6 del protocolo de internet, este ha sido diseñado para permitir que el internet crezca a un ritmo constante, se busca que cada dispositivo conectado a la red tenga su propia dirección IP única. En IPv6 se amplían las direcciones IP con respecto a IPv4 de 32 bits a 128 bits.

1.2.4.4. Protocolos de transmisión de datos

Los protocolos son un conjunto de normas y reglas que se utilizan para el intercambio de datos entre los equipos conectados a una red.

Existen varios protocolos y un mismo equipo puede utilizar estos sin que existan colisiones entre sí. Los adaptadores de red se encargan de recibir los datos dependiendo del protocolo, interpretarlos y llevarlos a la computadora en un idioma entendible para que esta los pueda procesar.

Para poder transmitir información en una red, necesitamos de protocolos de trasporte, protocolos de red y protocolos de aplicación. Los principales son[4]:

- Protocolos de transporte: Apple Talk Protocol (APT), Network Basic Input/Output System (NETBios), Transmission Control Protocol (TCP).
- Protocolos de red: Delivery Datagram Protocol (DDP), Internet Protocol (IP), Internet Protocol Exchange (IPX), Network Basic Extended User Interface (NetBEUI).
- Protocolos de aplicación: Apple File Protocol (AFP), File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP)

1.2.5. Protocolos de Transporte de Datos para vídeo IP[5]

En la actualidad para transmitir datos en redes informáticas se utiliza el conjunto de protocolos TCP/IP, este actúa como portador para los demás protocolos (como el HTTP, SMTP, entre otros).

1.2.5.1. Protocolos IP: TCP y UDP

IP utiliza dos protocolos de transporte, el primero es el protocolo de control de transmisión o TCP, el segundo es el protocolo de datagramas de usuario o UDP. TCP gestiona el proceso de convertir grandes bloques de datos en paquetes más pequeños y nos ofrece un canal de transmisión fiable que está basado en la conexión. UDP en cambio es un protocolo que no garantiza la entrega de datos enviados dejando todo el proceso de control y comprobación de errores a cargo de las aplicaciones finales.

El uso de TCP se da cuando se prefiere una comunicación fiable aunque este produzca retrasos significativos, el UDP no produce retrasos y no ofrece retransmisiones de datos perdidos.

1.2.5.2. Puertos y protocolos para transmitir vídeo IP

Existen varios protocolos que se pueden utilizar para transmitir vídeo IP, cada uno cuenta con su número de puerto, su uso común y su uso para el vídeo IP, estos son:

- File Trasfer Protocol (FTP): Utiliza como protocolo de trasporte TCP, utiliza el puerto 21, se usa generalmente para la trasferencia de ficheros a través de internet y su uso para el vídeo de red se da para la trasferencia de imágenes o vídeo desde una cámara de red a un servidor FTP o una aplicación.
- Send Mail Trasfer Protocol (SMTP): Utiliza como protocolo de transporte TCP, utiliza el puerto 25, se utiliza generalmente para el envío de e-mails y su uso para el vídeo de red se da para que una cámara de red o servidor de vídeo envié imágenes o notificaciones de alarma utilizando un cliente integrado de e-mail.
- Hyper Text Trasfer Protocol (HTTP): Utiliza como protocolo de transporte TCP, utiliza el puerto 80, se utiliza generalmente para recibir páginas de

servidores web y su uso para el vídeo de red se da para transmitir el vídeo desde una cámara de red o servidor de vídeo que funciona como un servidor web hacia el usuario o un servidor de aplicación.

- Hyper Text Trasfer Protocol Secure Socket Layer (HTTPS): Utiliza como protocolo de transporte TCP, utiliza el puerto 443, se utiliza generalmente para recibir páginas de servidores web de forma segura encriptando la transmisión y su uso para el vídeo de red se da para transmitir vídeo desde una cámara de red pero autenticando los datos mediante certificados digitales X.509.
- Real Time Protocol (RTP): Utiliza como protocolo de transporte UDP/TCP, no tiene un puerto definido, se utiliza generalmente para el envió de audio y vídeo a través de internet usando sistemas multimedia o de videoconferencia y su uso para el vídeo de red se da para transmitir vídeo en red MPEG, esta transmisión puede ser Unicast[5] o Multicast[6].
- Real Time Streaming Protocol (RTSP): Utiliza como protocolo de transporte TCP, utiliza el puerto 554, se utiliza para la configuración y control de sesiones multimedia a través de RTP.

1.2.5.3. Métodos para transmisión para vídeo IP

Para transmitir datos en una red informática existen varios métodos, los cuales son:

- Unidifusión (Unicasting): Aquí tanto el emisor como el receptor se comunican a un nivel punto a punto, los paquetes de datos son dirigidos únicamente a este receptor asignado.
- Multidifusión (Multicasting): Aquí un emisor se comunica a múltiples receptores en una red, esta transmisión se la utiliza para reducir el tráfico de la red cuando numerosos receptores desean visualizar la misma fuente de manera

[5] Unicast: Transmisión de uno a uno.
[6] Multicast: Transmisión de uno a varios.

simultánea. La multidifusión se utiliza habitualmente junto con las transmisiones RTP.

- Retransmisión (Broadcasting): Es una transmisión de uno a todos, estas retransmisiones generalmente se restringen a un segmento de red determinado y no se usan para la transmisión de vídeo en la red.

1.2.6. Topologías de red[2]

Una topología de red es la disposición física en la que se conecta una red de ordenadores. Existen varios tipos de topologías, entre las más comunes están:

1.2.6.1. Red de anillo

Una topología en la que los dispositivos se interconectan formando un anillo, cada dispositivo tiene la función de un nodo, este está conectado al siguiente y el último conectado al primero, por lo tanto cada dispositivo tiene un receptor y un transmisor que hace la función de un repetidor. Esta topología se observa en la Figura 1.2.

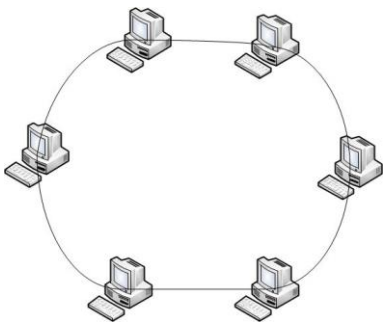


Figura 1.2. *Topología en anillo*

1.2.6.2. Red de árbol

Una topología en la que los nodos están colocados en forma de árbol, esta conexión es parecida a una serie de redes en estrella interconectadas. Aquí la falla de un nodo no implica la interrupción en las comunicaciones y se comparte el mismo canal de comunicaciones. Se puede ver esta topología en la Figura 1.3.

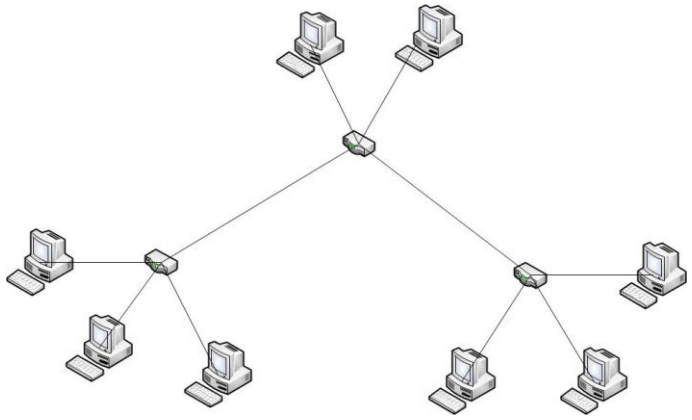


Figura 1.3. *Topología de árbol*

1.2.6.3. Red en malla

Es una topología de red en la que cada nodo está conectado a uno o más nodos, logrando así llevar la información por diferentes rutas, es un enlace en el que si falla una conexión esta no interrumpirá las conexiones. Esta topología se observar en la Figura 1.4.

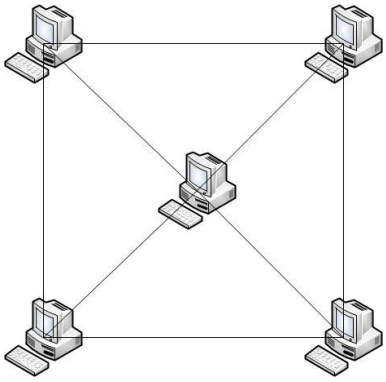


Figura 1.4. *Topología de malla*

1.2.6.4. Red de bus

En esta topología todos los dispositivos están conectados a un único canal de comunicaciones, por lo tanto todos los dispositivos usarán el mismo canal para comunicarse con el resto. Una gran desventaja de esta topología es que todos los dispositivos de red pueden ver todas las señales de los demás dispositivos además aquí es común que se produzcan colisiones y problemas de tráfico. Esta topología se presenta en la Figura 1.5.

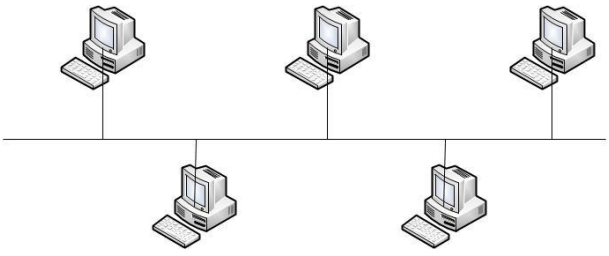


Figura 1.5. *Topología de bus*

1.2.6.5. Red en estrella

En esta topología, los dispositivos se encuentran conectados a un servidor y todas las comunicaciones se deben hacer necesariamente a través de este. Esta red crea una

mayor facilidad de supervisión y control de información ya que toda la información deberá pasar por este nodo central. Esta topología se observa en la Figura 1.6.

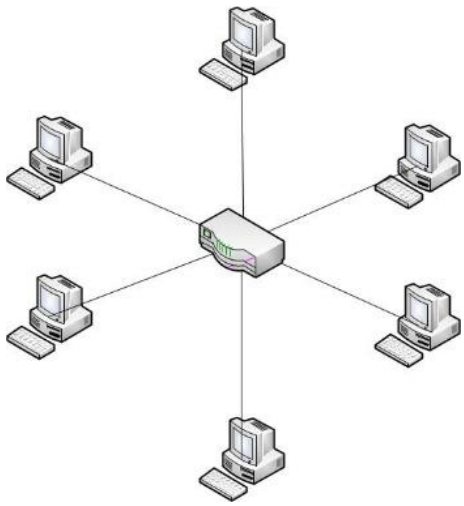


Figura 1.6. *Topología en estrella*

1.3. Redes GPON[9]

El estándar para la Red Óptica Pasiva con Capacidad Gigabit (GPON) consiste de un conjunto de recomendaciones G.984.x de la Unión Internacional de Telecomunicaciones (ITU-T) en donde se establecen los lineamientos para compartir un medio común (Fibra Óptica) para varios usuarios, encapsular la información y gestionar los elementos de red, entre otros aspectos[10]. La figura 1.7 muestra cada uno de los sistemas que componen las redes GPON, los mismos que son:

- Sistema de Terminación de Línea Óptica (OLT).
- Unidad de Red Óptica (ONU) o una Terminación de Red Óptica (ONT).
- Red de Distribución Óptica (ODN) para la interconexión de la OLT con la ONU o la ONT.

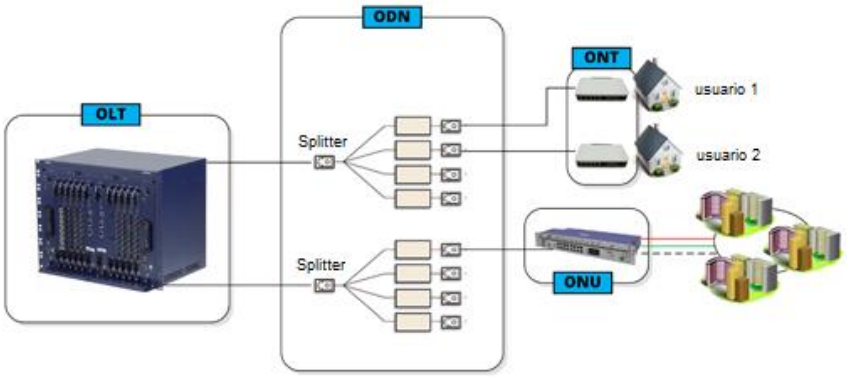


Figura 1.7. *Red de Distribución ODN*[9]

1.3.1. Definición de elementos en una red GPON

1.3.1.1. Red de Distribución Óptica (ODN)

Constituye el conjunto de fibras ópticas, divisores de longitud de onda (splitters), filtros, que brindan comunicación entre un OLT y el usuario, y viceversa. (Figura 1.7).

1.3.1.2. Terminación de Línea Óptica (OLT)

Dispositivo ubicado en la central, desde el cual parte la red de fibra hasta el usuario. La OLT proporciona funciones de gestión y mantenimiento del ODN y las ONUs. (Ver figura 1.8).

Figura 1.8. *OLT*[11]

1.3.1.3. Terminación de Red Óptica (ONT)

Dispositivo de abonado que termina cualquiera de los puntos finales distribuidos de una ODN. En conjunto con la OLT proporciona a los usuarios varios servicios de banda ancha con Voz sobre IP (VoIP), Televisión de alta definición (HDTV), vídeo conferencia. (Ver figura 1.9).

Figura 1.9. *ONT*[12]

1.3.1.4. Unidad de Red Óptica (ONU)

Término genérico que denota un dispositivo que termina cualquier punto final de distribución de una ODN. En algunos contextos una ONU implica un dispositivo multi-abonado. Puede tener desde 1 puerto Ethernet hasta 24 puertos para el caso de brindar servicio a edificios. (Ver figura 1.10).

Figura 1.10. *ONU*[13]

1.3.1.5. Splitter (Divisor Óptico Pasivo)

Figura 1.11. *Splitter*[14]

Dispositivo que retransmite la señal óptica mutiplexanda y/o demultiplexanda. (Ver figura 1.11).

1.3.2. Características de una red GPON

GPON tiene un alcance máximo de 20 km, aunque el estándar lo establece para distancias hasta de 60 km. Posee seguridad para el enlace descendente gracias a la naturaleza multicast de la Red Óptica Pasiva (PON).

1.3.2.1. Topología de una Red GPON

GPON maneja una topología tipo árbol que conecta la OLT con las ONUs mediante divisores ópticos pasivos. La OLT es el dispositivo cuya función es la interconexión de los elementos a la red principal.

1.3.2.2. Servicios que soporta una Red GPON

Las redes GPON soportan todos los servicios: voz, como: Multiplexación por División de Tiempo (TDM), Red Óptica Síncrona (SONET), Jerarquía Digital Síncrona (SDH), Ethernet (10/100 BaseT), Modo de Transferencia Asíncrona (ATM), Frame Relay, etc.

1.3.2.3. Capacidad de una Red GPON

En una red GPON, cada hilo de fibra tiene una capacidad 1 Gbps de información, esta capacidad es repartida entre los usuarios finales conectados a la ONU.

En la red GPON un hilo de fibra puede dar servicio a 64 usuarios, considerando que este sistema podría dar a hasta 128 usuarios.

El rendimiento en una red GPON está limitada por ciertos factores, como[15]:

- El rendimiento de la ONT la misma que es aproximadamente de 400 Mbps.
- El margen de alimentación de la fibra óptica entre la ONT y OLT.
- La capacidad de backplane de la OLT que está a 200 Gbps para dispositivos de gama alta.

- La velocidad de la interfaz entre la OLT y el interruptor principal.

1.3.2.4. Velocidad de Transmisión

Las redes GPON pueden ser establecidas en dos combinaciones de velocidad de transmisión para tráfico asimétrico y simétrico:

- 1.2 Gbit/s uplink, 2.4 Gbit/s downlink.
- 2.4 Gbit/s uplink, 2.4 Gbit/s downlink.

De las cuales la más usada es la de 1.2 Gbits/s uplink y 2.4 Gbit/s downlink.

1.3.3. Protocolos utilizados por la red GPON

Para la transmisión de la información se usa la tecnología TDM para el envío descendente y Acceso Múltiple por División de Tiempo (TDMA) para el envío ascendente, lo que proporciona la ventaja de ausencia de colisiones, utiliza estándares de encriptación como el Estándar de Encriptación Avanzada (AES) brindando confiabilidad en la transmisión y recepción de información.

En el transporte de datos, se ha optado por la aplicación de protocolos usados en estándares anteriores a GPON como lo es ATM y Método de Encapsulación GPON (GEM).

1.3.4. Arquitectura de una red de Acceso Óptico

La sección óptica de un sistema de red de acceso local puede ser activa o pasiva, punto a punto o punto a multipunto.

Existen varias arquitecturas de red: FFTH (Fibra hasta el hogar), FTTB/C (Fibra hasta el Edificio o Acera), FTTCab (Fibra hasta el Gabinete). La red de acceso óptica es común a todas las arquitecturas.

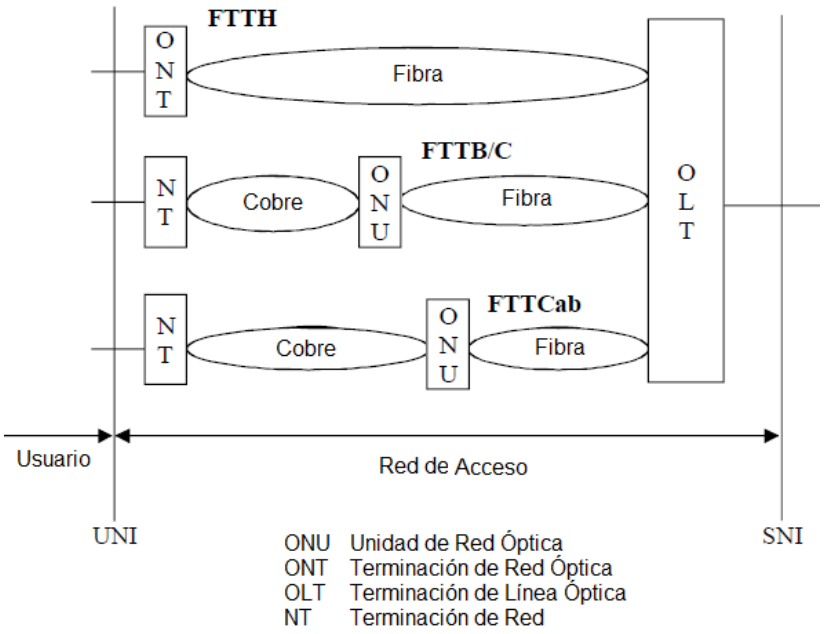


Figura 1.12. *Arquitectura de Red*[10]

Las diferencias que pueden existir entre FFTB, FTTC, FTTCab y FTTH son debidas a los diferentes servicios soportados.

1.3.4.1. Arquitectura FTTB

La arquitectura FFTB se divide en dos escenarios, uno para edificios (MDUs) y otro para empresas.

FTTB para MDU

- Servicios asimétricos de banda ancha (radio difusión digital, VOD, descarga de archivos, etc.).
- Servicios simétricos de banda ancha (difusión de contenidos, e-mail, intercambio de archivos, juegos en línea, etc.).
- POTS y RDSI. La red de acceso proporciona servicio de telefonía de banda estrecha.

FTTB para Empresas

- Servicios simétricos de banda ancha (software de grupo, difusión de contenidos, e-mail, intercambio de archivos, etc.)
- POTS e RDSI. La red de acceso proporciona servicio de telefonía de banda estrecha.
- Servicios de Línea Privada. La red de acceso debe proporcionar servicios privados de línea.

1.3.4.2. Arquitectura FFTC y FTTCab

- Servicios asimétricos de banda ancha (radio difusión digital, VOD, descarga de archivos, juegos en línea etc.).
- Servicios simétricos de banda ancha (difusión de contenidos, e-mail, intercambio de archivos, telemedicina, etc.).
- POTS y RDSI. La red de acceso debe proporcionar servicio de telefonía de banda estrecha.
- Backhaul xDSL.

1.3.4.3. Arquitectura FFTH

- Servicios asimétricos de banda ancha (radio difusión digital, VOD, descarga de archivos, juegos en línea etc.).
- Servicios simétricos de banda ancha (difusión de contenidos, e-mail, intercambio de archivos, telemedicina, etc.).
- POTS y RDSI. La red de acceso debe proporcionar servicio de telefonía de banda estrecha[10].

1.3.5. Configuración de una Red GPON

En la Figura 1.13 se puede apreciar la configuración de referencia de una red GPON.

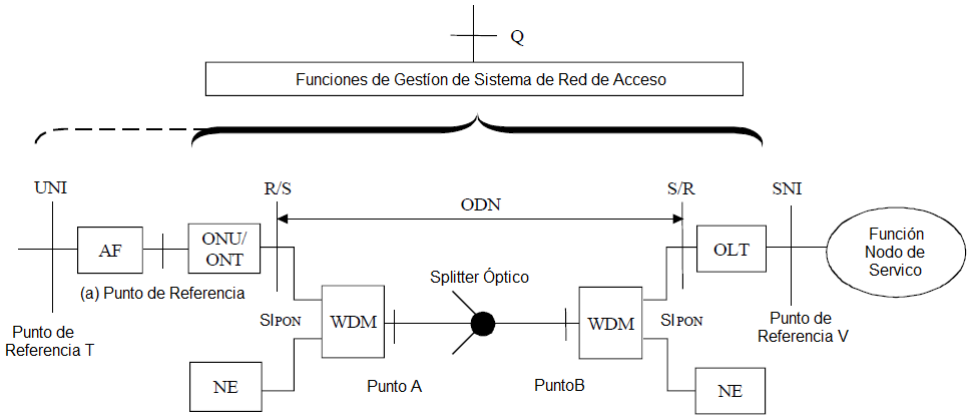


Figura 1.13. *Configuración de Referencia para GPON*[10]

Donde:

- ONU Unidad de Red Óptica.
- ONT Terminal de Red Óptica.
- ODN Red de Distribución Óptica.
- OLT Terminal de Línea Óptica.
- WDM Multiplexación por División de Longitud de Onda. Si no se utiliza WDM, esta función no es necesaria.
- NE Elemento de Red, esta utiliza diferente longitud de onda que la OLT y la ONU.
- AF Función de Adaptación
- SIN Servicio de Nodo Interfaz.
- UNI Interfaz de Red de Usuario.
- S Punto en la fibra óptica justo después del punto de conexión óptica OLT (Downstream) / ONU (Upstream).
- R Punto en la fibra óptica justo antes del punto de conexión óptica ONU (Downstream) / OLT (Upstream).
- (a) Punto de Referencia. Si AF está incluida en la ONU, este punto no es necesario.
- Punto A/B. Si Multiplexación por División de Longitud de Onda (WDM) no es usado, estos puntos no son necesarios.

Nota: Sea o no AF un elemento de la interfaz Q, dependerá del servicio

1.4. Sistemas de Video-Vigilancia

1.4.1. Conceptos de transmisión para la Video-Vigilancia

1.4.1.1. Vigilancia IP

El vídeo IP o vigilancia IP es un sistema que ofrece a los usuarios la posibilidad de controlar y grabar en vídeo a través de una red IP, como: Red de Área Local (LAN), Red de Área Amplia (WAN), Internet. A diferencia de los sistemas de vídeo analógicos, el vídeo IP no necesita cableado punto a punto y utiliza la red como eje central para transportar la información.

El término de "vídeo IP" hace referencia tanto a fuentes de vídeo como de audio disponibles en el sistema[16].

De acuerdo con lo anterior, la avanzada funcionalidad del vídeo IP lo convierte en un medio muy adecuado para las aplicaciones relacionadas con la video-vigilancia y seguridad.

1.4.2. Evolución de Sistemas de Vídeo-Vigilancia[5]

Los sistemas de vigilancia por vídeo existen desde hace 25 años, han empezado siendo sistemas analógicos al 100% y paulatinamente se han ido digitalizando.

En la actualidad, estos sistemas utilizan cámaras y servidores de PC para la grabación de vídeo en un sistema completamente digitalizado. Esta evolución de los sistemas de vigilancia se puede definir en cinco claras etapas.

1.4.2.1. Etapa 1: Sistemas de circuito cerrado de Televisión (TV) analógicos usando VCR

Fueron sistemas de Circuito Cerrado de TV (CCTV). Usaban un VCR (grabador de vídeo) y estaban formados por cámaras analógicas con salida coaxial, conectadas al VCR para grabar. En la Figura 1.14 se puede observar este sistema.

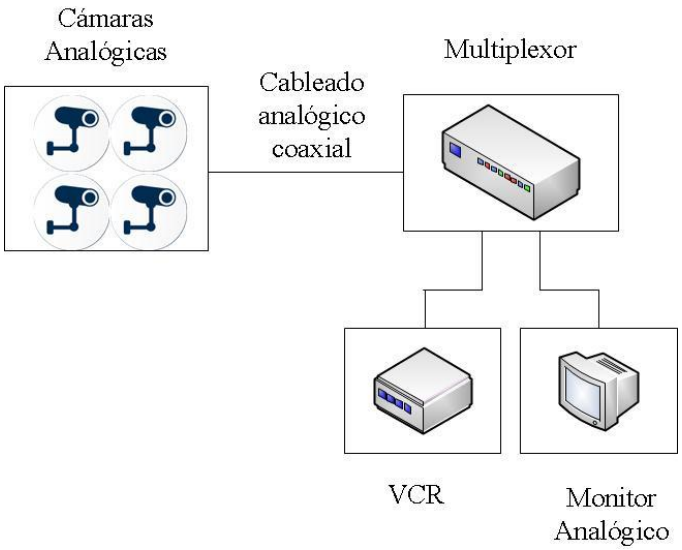


Figura 1.14. *Sistemas de circuito cerrado de TV analógicos usando VCR*

1.4.2.2. Etapa 2: Sistemas de circuito cerrado de TV analógicos usando DVR (grabador de vídeo digital)

Fueron sistemas analógicos con grabación digital. Este sistema añade las siguientes ventajas:

- No es necesario cambiar las cintas
- Tiene una calidad de imagen constante

En la Figura 1.15 se puede observar este sistema.

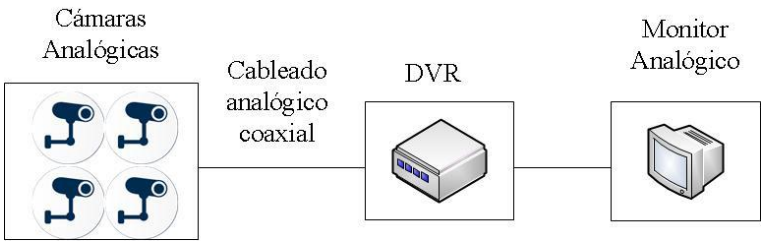


Figura 1.15. *Sistemas de circuito cerrado de TV analógicos usando DVR*

1.4.2.3. Etapa 3: Sistemas CCTV analógicos usando DVR de red

Fueron sistemas CCTV analógicos que usaban un DVR IP, fue un sistema parcialmente digital que incluye un DVR IP equipado con un puerto Ethernet para conectividad de red. El sistema DVR IP añade las siguientes ventajas:

- Monitorización remota de vídeo a través de un computador.
- Funcionamiento remoto del sistema.

En la Figura 1.16 se observa este sistema.

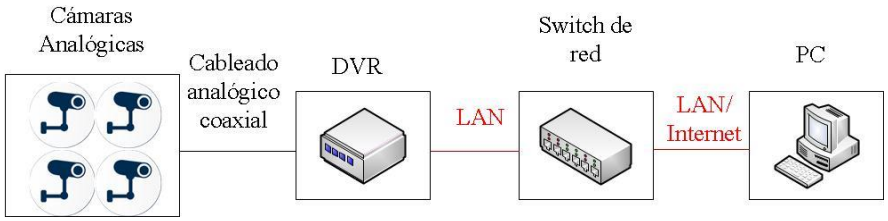


Figura 1.16. *Sistemas CCTV analógicos usando DVR de red*

1.4.2.4. 1.4.2.4. Etapa 4: Sistemas de vídeo IP que utilizan servidores de vídeo

Fueron sistemas de vídeo IP que utilizan servidores de vídeo, conmutador de red y un PC con software de gestión de vídeo. Este sistema de vídeo IP añade las siguientes ventajas:

- Utiliza una red estándar y hardware de servidor de PC para la grabación y gestión de vídeo.
- El sistema es escalable.
- Se puede grabar remotamente.
- Este sistema puede ampliarse fácilmente incorporando cámaras IP.

En la figura 1.17 se puede observar este sistema.

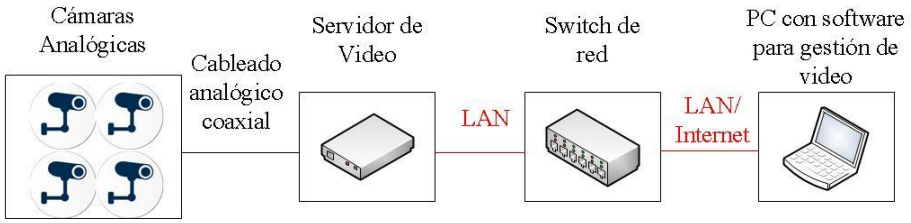


Figura 1.17. *Sistemas de vídeo IP que utilizan servidores de vídeo*

1.4.2.5. Etapa 5: Sistemas de vídeo IP que utilizan cámaras IP

Son sistemas que combinan una cámara IP y un ordenador en una unidad, lo que permite la digitalización y la compresión del vídeo así como un conector de red. El vídeo se transmite a través de una red IP, mediante los conmutadores de red y se graba en un PC estándar con software de gestión de vídeo. Esto representa un verdadero sistema de vídeo IP donde no se utilizan componentes analógicos y presenta las siguientes ventajas:

- Utiliza cámaras de alta resolución.
- Tiene una calidad de imagen constante.
- Su alimentación eléctrica es a través de Ethernet (PoE).
- Tiene funcionalidad inalámbrica.
- Puede incorporarse entradas y salidas digitales a través de IP.
- Tiene flexibilidad y escalabilidad completas.

En la Figura 1.18 se puede observar este sistema.

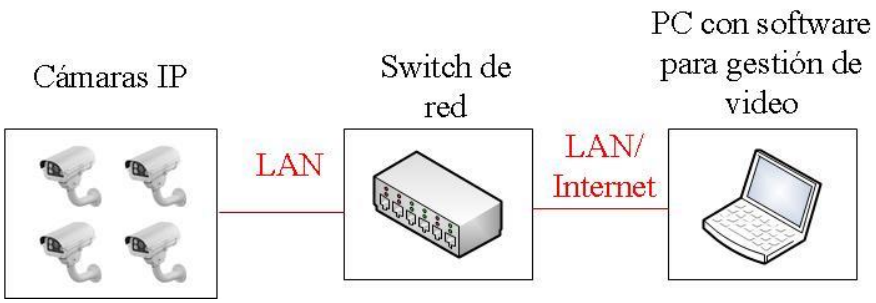


Figura 1.18. *Sistemas de vídeo IP que utilizan cámaras IP*

1.4.3. Cámaras IP

1.4.3.1. Concepto y características de la cámara IP

Una cámara IP es una cámara que emite imágenes y vídeo directamente sobre la red sin necesidad de un ordenador, ya que esta posee un miniordenador que le permite emitir vídeo por sí misma.

Estas cámaras tienen varias funcionalidades, entre las principales están:

- Permiten comprimir el vídeo para enviarlo.
- Pueden enviarse e-mails directamente de las imágenes.
- Pueden activarse y monitorearse remotamente.
- Cuentan con sensores que permiten un mayor control del ambiente.
- Permite la configuración de la calidad de imagen y compresión para adaptarlo al sistema en el que vayamos a implementar.
- Su software puede actualizarse con el fin de mejorar la interfaz y manejo de la cámara.

1.4.3.2. Tipos de Cámaras IP

Cámaras IP fijas

Las cámaras fijas representan el tipo de cámara tradicional, en algunas aplicaciones resulta útil que la cámara sea muy visible. Para una mayor protección, las cámaras fijas

pueden instalarse en carcasas diseñadas para interiores o exteriores. En la Figura 1.19 se ve este tipo de cámara[5].

Figura 1.19. *Cámara IP Fija*[17]

Cámaras IP domo fijas

Las cámaras domo fijas, también conocidas como mini domo, constan básicamente de una cámara fija preinstalada en una pequeña carcasa domo, la cámara puede enfocar fácilmente el punto seleccionado en cualquier dirección. La ventaja principal de estas cámaras es su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. En la Figura 1.20 se muestra una cámara IP de domo fija[5].

Figura 1.20. *Cámara IP de Domo Fija*[17]

Cámaras IP PTZ

Las cámaras con movimiento vertical/horizontal/zoom (PTZ) poseen la ventaja de obtener una visión panorámica, inclinada, alejada o de cerca de una imagen, manual o automáticamente. El zoom óptico oscila entre 18x y 26x. En la Figura 1.21 se puede observar una cámara IP PTZ[5].

Figura 1.21. *Cámara IP PTZ*[17]

Cámaras IP domo

Las cámaras IP domo disfrutan de las mismas ventajas que las cámaras domo fijas: son bastante discretas y, al mirar la cámara, no puede determinarse la dirección hacia la cual apunta. Una cámara IP domo, en comparación con una cámara PTZ, añade la ventaja de permitir una rotación de 360 grados. En la Figura 1.22 se puede observar una cámara IP Domo[5].

Figura 1.22. *Cámara IP Domo*[17]

Cámaras IP PTZ no mecánicas

Gracias al sensor de megapíxels, la cámara puede abarcar entre 140 y 360 grados y el usuario puede obtener una visión panorámica, inclinada, alejada o de cerca con la cámara, en cualquier dirección, sin tener que realizar ningún movimiento mecánico. La ventaja primordial es que no se produce un desgaste de las piezas móviles. Ofrece además un movimiento inmediato a una nueva posición, lo que en una cámara PTZ tradicional puede tardar hasta 1 segundo. Con el fin de garantizar una buena calidad de imagen, el movimiento vertical y horizontal deberá limitarse a 140 grados y el zoom a 3x. Para un zoom o una cobertura mayor, la calidad de la imagen se verá seriamente perjudicada. En la Figura 1.23 se puede observar una cámara IP PTZ no mecánica[5].

Figura 1.23. *Cámara IP PTZ no mecánica*[17]

1.5. Estado del Arte de Sistemas de Seguridad sobre IP

1.5.1. Sistemas de Vídeo-Vigilancia[18]

Los avances tecnológicos en vídeo vigilancia han tenido un crecimiento en la última década debido a la necesidad de seguridad pública y privada.

Se define a la vídeo vigilancia como “vigilancia a través de un sistema de cámaras, fijas o móviles”[19].

La historia de la vídeo-vigilancia se remonta hasta 1965, donde la policía de los Estados Unidos usaba la vigilancia por vídeo en lugares públicos. En 1969 se colocaron cámaras de vigilancia en el Edificio Municipal en la ciudad de Nueva York, a partir de esto, la vigilancia a través de cámaras se extendió a otras ciudades donde la policía podía monitorear espacios públicos mediante el sistema de CCTV o circuito cerrado de televisión.

En 1975, se instalaron en Inglaterra sistemas de vídeo vigilancia en cuatro estaciones de tren subterráneas y en carreteras principales.

En los Estados Unidos en la década de 1980 se comenzó la instalación de sistemas de vídeo vigilancia en estaciones subterráneas de tren y en carreteras, pero se puso más énfasis en la vigilancia de espacios públicos.

En la década de 1990 con la implementación de la multiplexación digital se solucionó el inconveniente de cambiar la cinta de grabación a diario, además que se posibilitó grabar desde varias cámaras a un mismo tiempo.

Con la llegada de la digitalización se mejoró la capacidad de compresión pudiendo grabar hasta un mes de vídeo en el disco duro, además que las imágenes grabadas tenían mejor calidad y podían ser manipuladas.

A partir de los acontecimientos del 11 de septiembre de 2001, la vídeo-vigilancia tuvo un crecida considerable, aumentando programas para vigilancia por cámara, es así que se desarrollaron softwares para reconocimiento facial.

Para mayo de 2002 se instaló un software de reconocimiento facial en las cámaras de vigilancia en la Isla Ellis y la Estatua de la Libertad. Este mismo año el sistema SmartGate fue instalado en el Aeropuerto de Sydney Australia, dicho sistema escanea los rostros de los tripulantes y los compara con las fotografías en el pasaporte, dando la identidad de los mismos en menos de 10 segundos.

En diciembre de 2003, el Royal Palm Middle School en Phoenix Arizona instaló reconocimiento facial en sus cámaras de vigilancia como un programa para el registro de delincuentes sexuales y seguimiento a niños desaparecidos.

El internet revolucionó la vídeo vigilancia, pudiendo evadir los impedimentos para la visualización y control en cualquier parte del mundo[18].

1.5.2. Puntos de Auxilio SOS en la actualidad

Con el despliegue de la vídeo-vigilancia y la significativa respuesta de dicho sistema para la ayuda de la ciudadanía, esta tecnología creció. Pero el problema de una oportuna respuesta por parte de las autoridades ante las emergencias se ha mantenido. Por esto, necesitaba mantener una comunicación fácil y rápida con las entidades de socorro en cualquier momento y lugar.

Como solución se implementó el audio full dúplex en zonas públicas, mediante los conocidos botones de pánico o puntos de auxilio SOS. De esta manera el usuario podía mantener una comunicación con una entidad de socorro en tiempo real, estos fueron implementados en carreteras usándose posteriormente para emergencia en parques, calles y en muchos casos como un medio para información, tal es el caso que se emplean en las estaciones de tren[20].

En la actualidad varias empresas han respondido a esta problemática con la creación de dispositivos que permitan a los transeúntes comunicarse en una situación de emergencia de forma remota con una estación de asistencia y recibir la ayuda pertinente.

1.5.2.1. Modelos Actuales de Puntos de Auxilio SOS

A continuación se presentan algunas de las empresas y dispositivos diseñados para este fin.

La empresa **2N Telecommunications** con sede en República Checa es una empresa dedicada al desarrollo y fabricación de productos en el campo de la Tecnología de la Información y Comunicaciones (TIC) y la seguridad física, centrándose en el diseño y fabricación de intercomunicadores IP[21].

Estos intercomunicadores pueden estar expuestos a las más duras condiciones de ambientes exteriores, además que el intercomunicador puede ser objeto de ataques de ladrones por lo que está preparado para afrontar todos estos retos conservando completamente su funcionalidad.

Dicha empresa sacó al mercado el intercomunicador 2N Helios IP Safety en 2012, figura 1.24, es un moderno intercomunicador para las situaciones de emergencia, el cual puede comunicar bidireccionalmente dos lugares distantes, además dicho dispositivo por su exposición completa al medio ha sido probado bajo estándares anti vandálicos garantizando su completa funcionalidad.

Su llamativo color naranja y teclas iluminadas garantizan su fácil localización incluso en situaciones críticas[21].

Figura 1.24. *2N Helios IP Safety*[21]

La empresa Japonesa **Aiphone Co.**, empresa respetada y confiable en sistemas de comunicación dedicada a la fabricación de sistemas de seguridad de vídeo desde 1970 ha desarrollado intercomunicadores para exterior con grandes prestaciones, hasta sacar al mercado en 2012 su propia estación de asistencia, útil para ofrecer ayuda inmediata a las personas y ayudar a evaluar rápidamente las situaciones de emergencia[22]. En la figura 1.25 se puede apreciar el modelo de la estación de asistencia Aiphone Co.

Figura 1.25. *Elementos de la Estación de Asistencia Aiphone*[22]

La empresa italiana **"ERMES Freedom to communicate"**, brinda la libertad de comunicarse en cualquier momento y en cualquier lugar; de una forma sencilla e inmediata. ERMES produce sistemas de comunicación a través de IP: intercomunicadores, teléfonos de puerta, videoporteros, SOS, sonido.

Figura 1.26. *CityHELP ERMES*[23]

CityHELP de ERMES, figura 1.26, es un sistema de SOS en IP (Help Point) para llamadas de emergencia a través de LAN disponibles en versiones que implementan la comunicación con sólo el audio o el audio y el vídeo.

Estos sistemas SOS pueden manejar las comunicaciones de emergencia a través de IP lo cual permitirá a un usuario que necesita entrar en contacto de una forma sencilla, rápida y eficaz con el personal de un centro de control que puede manejar las llamadas de emergencia de manera oportuna con el fin de prestar la asistencia que necesita. El sistema puede emplear un enlace GSM si no dispone de medios de transmisión para la red[23].

La empresa francesa **Maitrise Technologique** son especialistas en el diseño de redes para llamadas de emergencia en carretera y autopista y equipos de vigilancia de tráfico similar al de la figura 1.27 donde se muestra una fotografía del modelo MT A89.

Figura 1.27. *MT A89*

Su objetivo es mantener la vigilancia y control del tráfico en carreteras y autopistas para lo que se ha implementado paneles de mensaje, panel de llamada de emergencia de la red, sistemas de Vídeo Vigilancia de tráfico de carreteras y autopistas[24].

1.6. Voz sobre IP (VoIP) en Sistemas de Vigilancia

La voz sobre IP es un conjunto de protocolos utilizados para transmitir la voz sobre redes de datos; para realizar la transmisión la voz debe ser digitalizada y empaquetada[25].

También conocida como telefonía IP, VoIP permite integrar en una misma red IP comunicaciones de voz y datos, esta no consta de un único protocolo sino que trabaja en conjunto con varios protocolos que emplean diferentes códecs[7] para digitalizar la voz y diferentes protocolos para enviarla.

[7] Códec: permite la codificación y decodificación de un flujo de datos o una señal.

1.6.1. Ventajas de la VoIP

Las ventajas de la telefonía IP iniciaron al ser utilizada para reemplazar la telefonía tradicional en espacios empresariales, ya que los costos de inversión y mantenimiento son reducidos.

Entre las principales ventajas están[25]:

- Disminución de los costes: ya que VoIP emplea como medio de transmisión el Internet.
- Portabilidad: VoIP no limita la movilidad del usuario ya que se puede acceder al servicio desde cualquier locación con internet.
- Fax Virtual: se puede enviar y recibir fax sin necesidad de una máquina de fax, esto evita los altos costes, la atenuación de la calidad y la incompatibilidad entre máquinas.
- Conferencias: permite que una comunicación sea compartida sin límite de interlocutores en tiempo real.
- Mejor integración: todas las comunicaciones de voz se las puede realizar sobre la red Ethernet así se evita el extensivo cableado telefónico.

1.6.2. Características del Servicio de VoIP[26]

En la figura 1.28 se indican los protocolos de VoIP y en qué capa del modelo OSI se encuentra. A continuación se listan las principales características del servicio de VoIP.

- Utiliza el protocolo SIP para el establecimiento y control de la llamada.
- Utiliza el protocolo RTP (Real-time Transport Protocol) para el transporte de la media.

- La señalización (SIP) será controlada por el Media Gateway Controller (MGC) y Session Border Controller (SBC).
- El ancho de banda definido para la comunicación de voz a nivel IP depende del códec a utilizar.

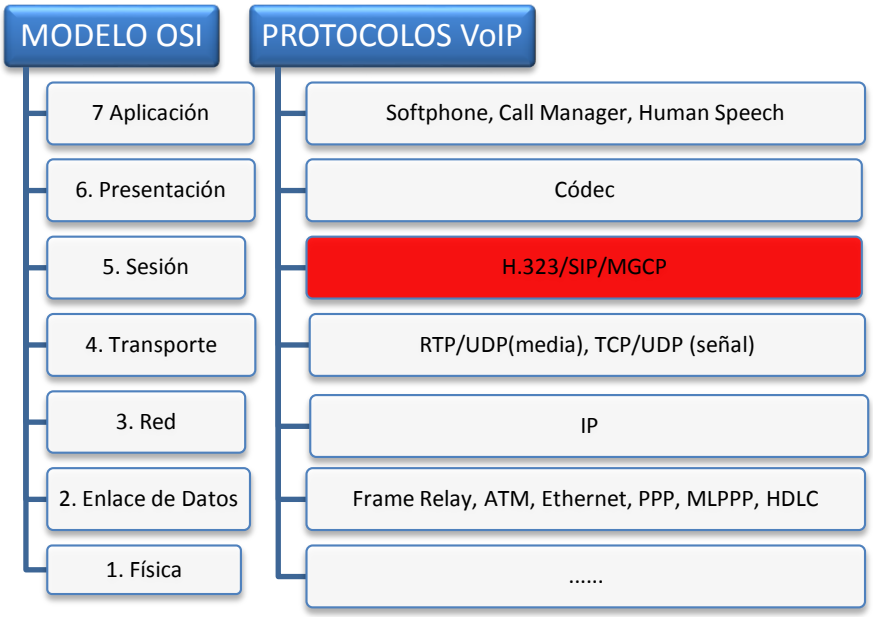


Figura 1.28. *Protocolos VoIP y el Modelo OSI*

1.6.3. Protocolos de Señalización VoIP[26]

1.6.3.1. Protocolo H.323

Protocolo del estándar ITU-T que fue aprobado en 1996 para el transporte de audio y vídeo sobre la red IP, conferencia interactiva que evolucionó del estándar RDSI H.320, además de ser flexible y completo es un protocolo peer-to-peer donde el dispositivo final inicia las sesiones.

1.6.3.2. Protocolo MGCP (Media Gateway Control Protocol)

Fue desarrollado en 1999 por la IETF para simplificar la comunicación con terminales. Es un protocolo Cliente/Servidor que permite a un dispositivo que controla llamadas pueda tomar el control de un puerto específico sobre un gateway. No es considerado como un protocolo estándar.

1.6.3.3. Protocolo SIP

Protocolo IETF para conferencias interactivo y no interactivo. Configuración necesaria del Gateway ya que este debe mantener un dialplan y el patrón de ruteo.

1.6.3.4. Protocolo SCCP o Skinny

Protocolo propietario de Cisco utilizado entre Cisco Unified Communications Manger y teléfonos Cisco VoIP. El cliente Skinny utiliza TCP/IP para transmitir y recibir llamadas, para el audio utiliza RTP, UDP e IP, los mensajes son transmitidos sobre TCP y usa el puerto 2000.

1.6.4. Protocolo SIP

El Protocolo SIP (Session Initiation Protocol) es un protocolo de señalización que inicia, controla y termina una sesión multimedia (voz y vídeo) sobre una red de paquetes.

Este protocolo se basa en una arquitectura cliente-servidor en el cual el cliente realiza una llamada y el servidor responde la llamada.

1.6.4.1. Ventajas de los gateways SIP

- Configuración del Dialplan directamente sobre el Gateway.
- Avanzado soporte para la integración de sistemas de telefonía de otros fabricantes.
- Soporta terminales de otros fabricantes (teléfonos SIP).

1.6.4.2. Funciones SIP[26]

- **Localización de usuario.** Descubre la localización del usuario final para establecer una sesión.
- **Capacidades de usuario.** Cuando una sesión se establece se determina la capacidad del medio.
- **Disponibilidad de usuario.** Determina la tasación del usuario final.
- **Configuración de sesión.** Establece los parámetros para iniciar una sesión.
- **Manejo de sesión.** Activa la modificación, transferencia y terminación de una sesión activa.

1.6.5. Centralita Telefónica IP

Una centralita telefónica o PBX es un equipo en una red privada que permite gestionar llamadas telefónicas internas en una empresa, y compartir las líneas de acceso a la red pública entre varios usuarios, para permitir que estos realicen y reciban llamadas desde y hacia el exterior.

Una centralita IP o IP-PBX es una centralita telefónica que trabaja internamente con el protocolo IP, por lo que utiliza la red de datos para realizar sus funciones. A más de conectarse a servicios VoIP también puede trabajar con líneas convencionales de telefonía analógicas o digitales[27].

1.6.6. Asterisk

Asterisk es un software de licencia libre que simula una central telefónica con capacidad para voz sobre IP[28].

Asterisk fue desarrollado por Mark Spencer para la empresa que estaba fundando llamada “Linux Support Services”, para la cual necesitaba una central telefónica la misma que en ese entonces superaba el presupuesto disponible.

Para 1999, Spencer tenía la codificación de Asterisk lista bajo licencia GPL (General Public License).

En 2002 lo que era Linux Support Service se convirtió en lo que ahora es Digium una empresa que constituye la innovación detrás de Asterisk, el software de telefonía de código abierto más utilizado en el mundo[29].

1.6.6.1. Asterisk AGI

AGI (Asterisk Gateway Interface) se lo conoce como una interfaz de línea de comandos que permite la interacción con Asterisk.

El dialplan de Asterisk llama a los programas AGI los que pueden estar realizados en casi cualquier lenguaje, dichos programas AGI permiten adicionar funcionalidades a la central telefónica[28].

Librerías AGI

Existen algunos lenguajes que cuentan con librerías para desarrollar los scripts AGI, algunos de estos son:

- Pearl
- PHP
- Python
- Ruby
- C
- .NET

1.6.7. Elastix

El proyecto Elastix es una distribución de software libre de un servidor de comunicaciones unificadas que integra tecnologías como[28]:

- VoIP PBX.
- Fax.
- Mensajería Instantánea.
- Email.
- Vídeo conferencia.

Fue presentado en marzo del 2006 por la compañía ecuatoriana PaloSanto Solutions como una interfaz de informe de llamadas de Asterisk para convertirse más tarde en una distribución del mismo.

1.6.7.1. Características

Algunas de las características básicas de Elastix son[30]:

- Correo de voz.
- Fax a correo electrónico.
- Soporte para softphones.
- Configuración de la interfaz web.
- Salas de conferencias virtuales.
- Grabación de llamadas.
- Enrutamiento de menor coste.
- Extensión Roaming.
- Interconexión PBX.
- Identificador de llamadas.
- Informe de avance.

1.6.8. Ventajas y desventajas de Asterisk y Elastix

1.6.8.1. Asterisk

Asterisk no es una herramienta que esté lista para su uso, para poder ejecutar sus funciones se debe realizar descargas, instalaciones, configuraciones, sin embargo es el elemento base para desarrollar cualquier aplicación. Puede instalarse sobre Linux por lo que se puede usar Debian, Ubuntu, Mint, CentOS, RedHat, OpenSource, etc[31].

Ventajas	Desventajas
• Se puede desarrollar cualquier aplicación y actualizarla en cualquier momento. • El conmutador se ajusta a la arquitectura de la PC al momento de compilar. • Se puede elegir los módulos a compilar.	• Mayor tiempo de implementación. • Configuración completa por línea de comandos.

Tabla 1.3. *Ventajas y Desventajas de Asterisk*

1.6.8.2. Elastix

Elastix es un conjunto de herramientas como Asterisk, una interfaz web de configuración (FreePBX), un sistema de base de datos (MySQL), un sistema de mensajería instantánea (OpenFire), soporte para fax (Hylafax), un CRM (vtiger), etc, que permiten hacer de manera más sencilla las labores que se realizarían utilizando un sistema desde línea de comandos[31].

Ventajas	Desventajas
• Sistema todo en uno. • Soporte incluido para señalizaciones de América Latina (R2 MFC). • Amplia comunidad de seguidores.	• Instala muchos componentes por default. • Interfaz gráfica lenta y pesada. • Componentes no actualizados. • Errores de seguridad por muchos componentes extras.

Tabla 1.4. *Ventajas y Desventajas de Elastix*

1.6.9. Dialplan

El dialplan consiste de una serie o cadena de caracteres que maneja o determina la forma en que nuestro equipo gateway de VoIP procesa las entradas ingresadas desde el teclado numérico del teléfono[32].

El Dialplan de Asterisk se define en el archivo extension.conf

Cada extensión en el Dialplan tiene este formato:

exten => extensión,prioridad,Comando(parámetros)

- **Extensión:** puede ser argumentos literales, patrones o predefinidas.
- **Prioridad:** Las prioridades son el orden que debe tener para cada extensión.
- **Comando:** son los parámetros que podemos dar a una extensión en un orden establecido, existen varios comandos, su lista completa se la puede conseguir en:[32].

A continuación se da a conocer los comandos que en este proyecto serán de utilidad.

1.6.9.1. Answer

Contesta el canal al sonar.

Descripción:

exten => s,n,Answer([delay])

Sí, el canal está sonando, este comando atiende a la llamada, caso contrario no hace nada. Si "delay" está especificado, el servidor espera ese valor en milisegundos después de contestar la llamada.

1.6.9.2. Hangup

Cuelga la llamada.

Descripción:

exten => s,n,Hangup(<causecode>)

Este comando cuelga la llamada y devuelve -1 al servidor en la cabecera del protocolo SIP, en caso de usar el causecode, al colgar se devuelve este valor al servidor.

1.6.9.3. Festival

Dice un texto determinado al llamante.

Descripción:

exten => s,n,FESTIVAL("Hola UPS")

Es un comando de sonido, usa un sintetizador de voz de código abierto, se lo usa para generar el texto especificado como un flujo de sonido. Antes de utilizar este comando, siempre se debe usar el comando "Answer".

Este sintetizador de voz debe estar previamente instalado, la versión de Elastix 2.5.0 ya incluye este en su paquete de instalación.

1.6.9.4. Wait

Espera por un periodo determinado de tiempo.

Descripción:

exten => s,n,Wait(seconds)

Este comando se usa para esperar un periodo de tiempo, su argumento puede estar en fracción. Al esperar este tiempo, todos los tonos incluidos los tonos DTMF son silenciosamente ignorados.

1.6.9.5. AGI

Con este comando podemos entrar en la interface de programación de Asterisk.

Descripción:

exten => s,n,AGI(ejemplo_agi.agi)

En donde el archivo "ejemplo_agi.agi" debe estar ubicado en /var/lib/asterisk/agi-bin y debe ser ejecutable y legible por el usuario que emplea Asterisk.

Este archivo puede ser una de las varias diferentes interfaces que existen con diferentes lenguajes de programación, como lo son: PHP, Java, Perl, Python, Ruby, C, C# y bash.

Ayuda:

Si el archivo no es ejecutable, cuando el Dialplan trate de ejecutarlo no contara con los permisos necesarios y devolverá un error, para esto se debe dar los permisos correspondientes a los archivos que se desee ejecutar desde el Dialplan. Se puede dar los permisos agregando el siguiente código (se debe estar en el directorio correspondiente):

```
sudo chmod 755 ejemplo_agi.agi
```

CAPITULO 2. ANÁLISIS Y DISEÑO DEL SISTEMA

2.1. Introducción

En la actualidad los dispositivos que permiten una comunicación y trasferencia de datos vía IP se han desarrollado con mejores prestaciones y cada vez más servicios.

Si se necesita enviar información ya sea datos, audio o vídeo con tecnología IP, en el mercado actual se encuentran varios dispositivos que pueden satisfacer las necesidades, con distintas características y ventajas.

Considerando la versatilidad de los servicios IP y su alto impacto en los sistemas de vigilancia tal como se indicó en el capítulo anterior y debido a que existe una amplia gama de dispositivos para la trasferencia de datos y comunicación usando IP, es necesario que se defina el problema que se quiere resolver, y por supuesto, cuáles van a ser las necesidades para esta comunicación, para así poder escoger que dispositivos existentes en el mercado pueden servir, aprovechando todas sus funciones y los recursos.

Entonces, para el diseño y la fabricación de un "Punto Seguro" es necesario considerar las necesidades dependiendo de los problemas que éste intenta resolver.

2.2. Diseño y Solución del Sistema

2.2.1. Definición del escenario

El dispositivo a diseñar debe ser considerado para el siguiente escenario: ambiente exterior de la Ciudad de Cuenca, en el cual exista afluencia masiva de personas que pueden llegar a encontrarse en riesgo. El dispositivo estará a la intemperie, expuesto a factores ambientales (lluvia, polvo, calor, ruido), podría ser mal utilizado y ser objeto de actos vandálicos. El dispositivo va a ser adaptado a un poste por lo que su diseño deberá ir acorde con este requerimiento.

Por lo tanto, el dispositivo no deberá presentar anomalías en su funcionamiento para lo que se consideran normas constructivas tanto físicas como eléctricas que se adapten a un entorno exterior y expuesto a factores climáticos.

2.2.2. Análisis de dispositivos necesarios

De acuerdo a la definición del escenario se requiere que el sistema a diseñar posea ciertas características. A continuación se presenta un análisis de los requerimientos técnicos para el funcionamiento del sistema.

Al momento de presentarse una emergencia, el solicitante debe ser observado y escuchado por parte de la central de auxilio. Además, el solicitante debe solo escuchar a la central, para lo cual es necesario una cámara que pueda transmitir vídeo en una vía y audio en dos vías es decir full dúplex entre el solicitante y la central de auxilio a través de la red. Por esto se considera la necesidad adicional de un vídeo teléfono IP localizado en la central para cumplir con lo mencionado.

Para poder dar una respuesta inmediata a la emergencia desde la central, será necesaria la activación de dispositivos de alerta. Por lo cual, se ha visto pertinente la utilización de un altavoz y una luz estroboscópica los mismos que tendrán la función de disuadir a posibles agresores en primera instancia.

Para el manejo de los dispositivos mencionados por parte de la central a través de la red se hace evidente la necesidad de un switch dentro de la red para conectar los diferentes dispositivos IP. El mismo que tendrá la función de separar los segmentos de red de cada dispositivo para ser operados individualmente según se requiera.

El dispositivo presenta la necesidad de mantener un funcionamiento continuo sin interferencias, por lo que será necesario que la cámara tenga la opción de alimentación mediante PoE. Esto genera un ahorro en cableado y reducción del consumo de energía, usando para la alimentación el mismo cable que se utiliza para datos. Además se empleará un sistema de respaldo de energía para garantizar el funcionamiento continuo del dispositivo.

Para gestionar el funcionamiento de los elementos que conformarán el sistema desde la central, será necesario un servidor el mismo que deberá ser montado en una PC adecuada para este fin y tarjetas electrónicas para formar el sistema de control.

2.2.3. Elección de dispositivos

2.2.3.1. Cámara IP

Como se analizó en el capítulo anterior, las cámaras IP se desarrollaron con el crecimiento de la vídeo-vigilancia y la necesidad de mejoras en los sistemas analógicos con respecto a la implementación y gestión de la seguridad a través de redes IP.

En el mercado existen muchos tipos de cámaras IP con diversas funcionalidades, de las cuales se debe escoger la que más se ajuste a las necesidades y al entorno de operación.

Necesidad

Basado en la definición del escenario y de los requerimientos del sistema, la cámara IP necesaria debe contar con las siguientes características:

- Ángulo de visión mínimo para captar el rostro del usuario es de 60 – 80 grados.
- Alimentación PoE para garantizar un funcionamiento continuo incluso en presencia de cortes de energía.
- Transmisión de audio en dos vías.

Selección del Dispositivo

Como se mencionó en el capítulo 1, existen cámaras IP fijas, IP de domo, IP PTZ, y combinadas, de las cuales la más óptima para el sistema son las cámaras IP fijas, ya

que en el sistemas no será necesaria la movilidad de la misma pero si un ángulo de visión suficiente.

Dentro de las cámaras IP fijas encontramos un sin número de modelos y funciones de las cuales se ha escogido la cámara GRANDSTREAM GXV3615WP-HD ya que reúne las características necesarias que debe tener el dispositivo. Las mismas que se detallan a continuación.

La cámara IP GRANDSTREAM GXV3615WP-HD de alta definición posee compresión de vídeo H.264 en tiempo real, calidad de imagen de 720p, cuenta con audio en dos vías, altavoz integrado y transmisión de vídeo a teléfonos móviles y vídeo teléfonos. Entre otras características están[33]:

- Cámara de 2 Mega pixeles con sensor CMOS y lente de alta calidad para gran nitidez de imagen.
- Avanzada velocidad de multi-transmisión (velocidad de bits y de cuadros variable).
- Su buffer soporta 24MB de grabación pre-/post-evento.
- Altavoz y micrófono incorporados con calidad SIP/VoIP y capacidad para transmisión audio en dos-vías, y vídeo a teléfonos móviles y vídeo teléfonos.
- Soporta detección de movimiento, notificaciones de alarmas (vía Correo Electrónico o llamada SIP, etc.) almacenamiento local de alarmas y grabaciones de vídeo (requiere tarjeta microSDHC), zoom electrónico.
- Servidor de alto rendimiento de transmisión para permitir 6 espectadores simultáneos en HD.
- Compatible con el HTTP API/SDK de Grandstream para una integración avanzada y mayor desarrollo.
- Alimentación sobre Ethernet PoE (802.3.af) y WI-FI (802.11b/g/n) integrados.

Figura 2.1. *Cámara Grandstream GXV3615WP-HD*[33]

2.2.3.2. Videoteléfono IP

La telefonía IP transmite comunicaciones de voz a través de la red mediante la utilización de IP. Entonces al usar la red como plataforma se consigue mayor seguridad, resistencia, flexibilidad y escalabilidad.

De acuerdo a lo mencionado y considerando que la telefonía IP no representa un porcentaje considerable en el volumen del tráfico en el mundo, se está expandiendo debido a que en las redes basadas en IP pueden aprovechar las mismas facilidades del transporte usando diferentes medios de transmisión, ya sea guiado o no guiado. Esto representa una ventaja muy importante para poder ofrecer el acceso masivo a internet con fines comerciales gracias a la disponibilidad y ubicuidad de esas facilidades de transporte[34].

Necesidad.

El videoteléfono IP deberá tener las siguientes características.

- Calidad de la imagen para poder observar al solicitante.
- Audio en dos vías.

- Grabación de la conversación.
- Activación de procesos remotos.

Selección del Dispositivo.

Para la determinación del teléfono IP a utilizar, se debe considerar la necesidad de poder observar y escuchar al solicitante de forma clara y definida, características que deben estar presentes en el dispositivo a utilizar.

El teléfono IP debe manejar protocolos compatibles con la cámara para realizar la comunicación entre el dispositivo de seguridad y el teléfono IP; entre los teléfonos IP disponibles en el mercado se escogerá un modelo moderno y escalable para posibles cambios.

Para el caso, se ha determinado el uso del teléfono Grandstream modelo GXV3175v2 que es un teléfono multimedia de vídeo IP con una pantalla táctil LCD de 7 pulgadas, usado para vídeo llamadas y de costo asequible. Posee las siguientes características[35]:

- Audio de alta definición y una cámara que permite realizar llamadas de alta calidad y servicio de videoconferencia.
- Conmutación dual 10M/100M, puertos Ethernet con PoE integrado, WiFi integrado.
- Altavoz full dúplex con alto rendimiento además de poseer un cancelador de eco acústico.
- Cuenta con registros de vídeo mail.

- Protocolos de red: SIP RFC3261, TCP/UDP/IP, PPPoE, RTP/RTCP, TLS/SRTP, HTTP/HTTPS, ICMP, ARP/RARP, DNS, DHCP (cliente), NTP/SNTP, Telnet, UPnP.
- Protección de seguridad: HTTPS, SIPS/TLS/SRTP, AES.
- Capacidad de Vídeo: H.264, 30fps, velocidad de bits de 32Kbps 1.5 Mbps.
- Códec de voz: G.711, G.722 (banda ancha), G.723.1, G.729AB, GSM-FR, G.726-32, L16-256.
- Códec de audio: ACC, MP3,WMA, Real, Ogg-Vorbis.

Figura 2.2. *Vídeo teléfono IP GXV3175v2*[35]

2.2.3.3. Luz estroboscópica

Dentro de los sistemas de alerta visual de seguridad se encuentran las luces estroboscópicas, las mismas que generan destellos luminosos a alta velocidad, a la vez que gira de forma rápida y periódica.

Los destellos producidos por la rotación son una manera de alertar una emergencia y disuadir personas que signifiquen un peligro.

Necesidad.

Los requerimientos que deberá cumplir son:

- Emitir una señal de alerta visual para disuadir a posibles agresores.

Selección del Dispositivo.

En el mercado comercial existe una gran variedad de luces estroboscópicas, lo importante para seleccionar la misma es que esta pueda tener fácil visibilidad desde una distancia considerable al momento de su activación y que pueda estar expuesta al medio.

Por lo que se escogerá una luz estroboscópica que posea un alcance de visión que no se vea afectado por la noche o malas condiciones climatológicas.

La luz estroboscópica seleccionada presenta las siguientes características:[36]

- Está diseñado con base de perno fijo para empotrar.
- 4 colores diferentes: rojo, azul, verde y amarillo.
- Potencia: 35W.
- Voltaje: AC 120V.
- Grado de protección IP55.
- No genera calor.
- Servicio de más de 100.000 horas y ahorro de energía.
- Estado de trabajo estable

Figura 2.3. *Luz Estroboscópica*[37]

2.2.3.4. Altavoz

Un altavoz también conocido como altoparlante, es un transductor que transforma la energía eléctrica en energía acústica. Está constituido por las siguientes partes:

- ***Parte electromagnética:*** la energía eléctrica llega a la bobina móvil que se encuentra dentro de un campo magnético generado por un imán ocasionando el movimiento de la bobina móvil.
- ***Parte mecánica:*** está formado por un cono sobre el cual se encuentra la bobina móvil.
- ***Parte acústica:*** transmite las ondas acústicas generadas por el cono.

Necesidad.

El altavoz o altoparlante deberá considerar las siguientes características:

- Emitir una señal de voz para la disuasión de agresores.
- Emitir una señal de alerta sonora (sirena) como indicador de emergencia.

Estas señales deben ser audibles en su entorno de operación.

Selección del Dispositivo.

Al seleccionar el altavoz adecuado para el sistema se debe tener presente el entorno en el cual va a operar el mismo que se considera como ruidoso y expuesto a un medio exterior, por lo que este debe tener la capacidad de emitir una señal sonora audible dentro de ese entorno.

Para dicho fin se ha seleccionado el PHSP4 Pyle Horn Speaker, un altavoz que posee las siguientes características[38].

Figura 2.4. *Altavoz PHSP4*

- Potencia / Capacidad de carga: 50 Watts.
- Impedancia nominal: 8 ohmios
- Rango de frecuencia: 500 Hz - 5 kHz
- Dimensiones: 6 "H x 4" W x 8 " D
- Peso: 1,78 libras.

Para proteger y obtener mayores prestaciones en audio se ha considerado la utilización del amplificador LP-2020A+ Lepai Tripath Class que resulta de la combinación de un

amplificador AB que ofrece fidelidad de audio y un amplificador clase D que otorgan eficiencia energética y al cual debemos el tamaño reducido del amplificador Lepai[39].

Figura 2.5. *Amplificador Lepai LP-2020A+*[39]

Entre otras características tenemos[39]:

- Entrada estéreo de 3,5 mm para conectar casi cualquier fuente de música, tales como iPods, teléfonos celulares o reproductores de MP3.
- El amplificador Lepai Mini tiene una carcasa de aluminio que es ligera, pero resistente, y actúa como disipador de calor.
- Incluye una fuente de 12V, 2A.
- Potencia de salida: 2 x 20 vatios RMS.
- Impedancia de entrada: 47k ohmios.
- Respuesta de frecuencia: 20 Hz - 20 kHz.
- Sensibilidad de entrada: 200 mV.
- THD mínima: <0,05%.

Para poder emitir sonidos pregrabados con alta calidad se hará uso de una tarjeta de sonido. La tarjeta de sonido Creative Sound Blaster X-Fi GO! Pro presenta considerables mejoras de audio 3D. Con cualquier auricular accede a Sorround 3D en películas, juegos y mejora todo el audio en línea y en la PC. Diseñado para máxima portabilidad.

Figura 2.6. *Tarjeta de sonido X-Fi Go! Pro*

Especificaciones[40]:

- Salida estéreo.
- Procesador de audio: X-Fi.
- Opciones de conectividad (principal):
    - Auriculares / Salida de altavoz: 1 conector de 3,5mm.
    - Entrada de micrófono: 1 conector de 3,5 mm
- Salida de Canal max: estéreo.
- Tecnologías de audio: X-Fi, SBX Pro Studio

2.2.3.5. Switch (conmutador)

El switch es un dispositivo similar a un HUB que sirve para interconectar dos o más segmentos de red, trasmite la información solo al puerto indicado, además mejoran el rendimiento y la seguridad de las redes de área local[41]. Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola.

Un switch posee la capacidad de aprender y almacenar las direcciones de red (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos.

Necesidad

El switch será usado para interconectar los segmentos de red de la cámara y el teléfono IP con la centralita, desde la cual se accionaran dichas funciones.

El switch presentará principalmente la siguiente característica:

- Disponibilidad de al menos 4 puertos.

Selección del Dispositivo.

El disposito elegido es el switch D-Link DES-1008D que posee las siguientes características[42]:

Figura 2.7. *Switch D-Link*[42]

- Auto-sensing 10/100 puertos: detecta la velocidad de la red y la negociación automática entre 10BASE-T y 100BASE-TX, así como entre el full y half-duplex, que le permite obtener la máxima velocidad posible para cada dispositivo conectado a la red.
- Auto MDI/MDIX CrossOver: Todos los puertos soportan el cable cruzado automático MDI / MDIX, eliminando la necesidad de cables cruzados o puertos

de enlace ascendente. Cada puerto puede ser conectado directamente a un servidor, hub, enrutador o conmutador mediante cables directos regulares Ethernet de par trenzado.

- Control de flujo para la transmisión segura: Control de flujo 802.3x en cada puerto, minimiza paquetes perdidos cuando el búfer de recepción del puerto está lleno. Esto le da una conexión más fiable para todos los dispositivos conectados.

2.2.3.6. Sistema de control

El diseño de un sistema de control es considerado como una etapa importante dentro de cualquier proceso. Este sirve para comandar todas las funciones utilizadas y a su vez monitorear todas las fases del sistema.

Necesidad

El sistema de control del dispositivo debe cumplir con lo siguiente:

- Accionar todos los elementos que constituyen el sistema.
- Monitorear el funcionamiento del dispositivo.

Selección del Dispositivo

El sistema de control del dispositivo es la etapa encargada de accionar los diferentes elementos del sistema así como de monitorear el funcionamiento de los mismos. Para lo cual se ha determinado el uso de las siguientes tarjetas:

- Arduino Yun
- Arduino UNO + Shield Ethernet

Arduino Yún. El Arduino Yún es una placa electrónica basada en el ATmega32u4 y el Atheros AR9331. El procesador Atheros es compatible con una distribución Linux basada en OpenWrt llamado OpenWrt -Yún.

Figura 2.8. *Arduino Yún*

- Se ha incorporado Ethernet y soporte WiFi.
- Puerto USB-A.
- Ranura para tarjeta micro-SD.
- 20 entradas/salidas digitales (de los cuales 7 se pueden utilizar como salidas PWM y 12 como entradas analógicas).
- Cristal de 16 MHz.
- Conexión micro USB.
- Circuito de Programación Serial ICSP.
- 3 botones de reinicio.

El Arduino Yún se distingue de otras placas Arduino en que se puede comunicar con Linux, ofrece un sistema de red de gran alcance. Además de los comandos de Linux como cURL, se puede escribir scripts de Shell y Python para las interacciones robustas[43].

Esta tarjeta fue seleccionada por incorporar Ethernet, además que se puede manejar de una manera óptima el audio desde una tarjeta micro-SD.

OpenWrt.

OpenWrt es una distribución de GNU/Linux altamente extensible para dispositivos embebidos (típicamente routers inalámbricos). A diferencia de muchas otras distribuciones, OpenWrt es un sistema operativo con todas las funciones, fácilmente modificable que hace del Arduino Yún una tarjeta que puede operar tanto en Windows como en Linux [44].

Arduino UNO + Shield Ethernet. El Arduino Uno es una placa electrónica basada en el microcontrolador ATmega328. Cuenta con catorce pines digitales de entrada/salida (seis pines pueden utilizarse para salidas PWM), seis entradas analógicas, oscilador cerámico de 16MHz, conexión USB, ICSP[45].

La tarjeta Arduino Uno fue seleccionada por la cantidad de pines digitales que se pueden manejar, si bien no se utilizarán todos, le brindan al proyecto la posibilidad de escalar en servicios.

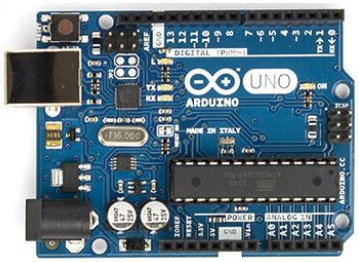


Figura 2.9. *Arduino UNO*[45]

Características:

- Microcontrolador: ATmega328.
- Tensión de funcionamiento: 5V.
- Voltaje de entrada (recomendado): 7-12V.
- Voltaje de entrada (límites): 6-20V.
- Digital pines I / O: 14 (6 pines proporcionan salida PWM).
- Pines de entrada analógica: 6.
- Corriente DC por Pin I / O: 40 mA.
- Corriente DC de 3.3V Pin: 50 mA.
- Memoria Flash 32 KB (ATmega328) de los cuales 0,5 KB utilizado por el gestor de arranque.
- SRAM2 KB (ATmega328).
- EEPROM: 1 KB (ATmega328).
- Velocidad del reloj: 16 MHz.

Ethernet Shield. El Arduino Ethernet Shield, permite que una placa Arduino se conecte a internet, como un servidor para aceptar conexiones entrantes o un cliente que realiza las salientes. Admite hasta cuatro conexiones simultáneas. (Revisar referencia[46]).

La selección de este shield se debe a la necesidad de Ethernet en la tarjeta Arduino UNO, así se puede ampliar la funcionalidad de esta.

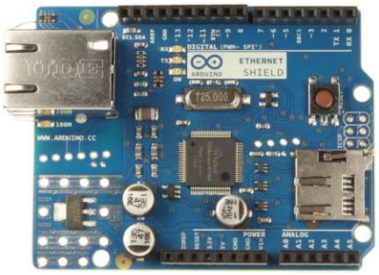


Figura 2.10. *Arduino Ethernet Shield*[46]

Características:

- Requiere una placa Arduino (no incluido).
- 5V Tensión de funcionamiento (suministrado por la Junta Arduino).
- Ethernet Controller: W5100 con buffer interno de 16K.
- La velocidad de conexión: 10 / 100Mb.
- Conexión con Arduino en el puerto SPI.

2.2.3.7. Sistema de iluminación nocturna

Debido a la necesidad de poder observar al solicitante durante la noche se pretende diseñar un sistema que constará de un reloj de tiempo real RTC y un sensor de ultrasonido. El sensor de ultrasonido será programado para detectar la existencia de un usuario y mediante la hora establecida por el reloj de tiempo real accionar o no la iluminación. El rango que se establecerá será de 18:00 a 06:00.

Reloj de Tiempo Real RTC[47]

El módulo RTC DS 1307 es un reloj de tiempo real de bajo consumo que cuenta segundos, minutos, horas, día del mes, mes, día de la semana y año con año bisiesto, compensación válida hasta 2100.

DS1307 tiene un circuito de detección de potencia incorporado que detecta fallas de energía y cambia automáticamente a la fuente de la batería.

Característica:

- Módulo respaldado con batería, 56 bytes, no volátil.
- RAM para el almacenamiento de datos.
- Interfaz serie de dos hilos.
- Señal de salida de onda cuadrada programable.
- Detección automática de falla eléctrica y conmutación de circuitos.
- Consume menos de 500 nA en modo respaldo de batería con el oscilador en funcionamiento.
- Rango de temperatura industrial -40°C a +85°C.

Figura 2.11. *RTC DS 1307*[47]

Sensor de Ultrasonido[48].

El sensor de ultrasonido HC-SR04 ofrece un rango de detección de 2cm-400cm sin contacto, con una precisión de 3mm. El módulo incluye transmisores ultrasónicos, el receptor y el circuito de control.

El principio de funcionamiento es el siguiente:

Usando la IO trigger una señal de nivel alto de al menos 10μs.

El módulo automáticamente envía 8 pulsos de 40kHz y detecta si existe una señal de pulso de vuelta. Si existe un pulso en alto de vuelta, el tiempo de salida de nivel alto IO es el tiempo desde el envío de ultrasonidos hasta el retorno.

$$Prueba\ de\ distancia = \frac{tiempo\ de\ alto\ nivel \times velocidad\ del\ sonido\left(\frac{340m}{s}\right)}{2} \qquad (2.1)$$

La conexión de los cables es la siguiente:

- Alimentación de 5V.
- Ingreso del pulso trigger.
- Salida del pulso de eco.
- 0V tierra.

Figura 2.12. *Sensor de Ultrasonido*[48]

El dispositivo necesita de un pulso de 10µs a la entrada del trigger para iniciar el proceso de detección donde el módulo enviará una ráfaga 8 ciclos de ultrasonido a 40 kHz y eleva su eco para la detección. El eco es la distancia al objeto que se manifiesta en un ancho de pulso y depende de un rango en proporción.

Se puede calcular el rango a través del intervalo de tiempo entre el envío de la señal de trigger y la recepción de señal de eco tal como aparece en (2.2). El diagrama de tiempo de esta explicación se muestra en la figura 2.13.

$$centímetros = \frac{\mu Seg}{58} \tag{2.2}$$

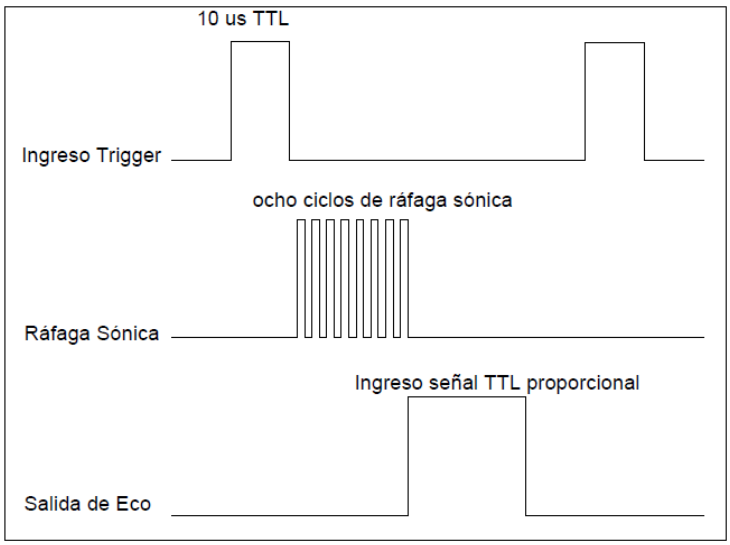


Figura 2.13. *Diagrama de tiempo*[48]

2.2.3.8. Sistema de energía

Los sistemas de respaldo de energía son considerados para situaciones en las cuales la operación continua de dispositivos es de vital importancia. Para lo cual se debe considerar los elementos permitentes para este fin.

Necesidad.

El sistema de respaldo de energía debe considerar lo siguiente:

- Alimentación continua para los dispositivos.
- Protección frente a descargas eléctricas.

Selección de Dispositivos.

Para la selección de dispositivos para el sistema de respaldo de energía se supone las necesidades que presentadas y se ha considerado la utilización de un cargador de baterías automático, una batería y un inversor.

Cargador Automático de Baterías. Es un dispositivo que tiene la función de cargar una batería cuando detecta un determinado nivel de voltaje (inferior) y a su vez la desconecta cuando esté a su máxima carga.

Este elemento es importante ya que al existir energía permite el paso de esta hacia el dispositivo y mantiene la carga de la batería, al no existir energía conmuta un contactor que puede ser utilizado para alertar de la no existencia de energía.

Figura 2.14. *Cargador Automático de Baterías*[49]

Batería. Consiste de un conjunto de celdas electroquímicas que tienen la capacidad de convertir energía química almacenada en electricidad. Las baterías vienen de diferentes tamaños según sea la carga a la cual van a alimentar y el tiempo de respaldo que se tendría.

Figura 2.15. *Batería PS7.5-12*[50]

Características[50]:

- Tensión nominal: 12V.
- Capacidad: 7.5Ah.
- Aplicaciones: sistema de iluminación de emergencia, herramientas eléctricas, aparatos geodésicos, alarma contra incendios, de seguridad y del sistema UPS.
- Característica: placa de aleación especial de calcio de plomo, de alta capacidad de adsorción, configuración sellada, operación libre de mantenimiento, baja auto-descarga.

Inversor. Un inversor es un dispositivo que cambia el voltaje de ingreso de corriente continua a un voltaje de salida de corriente alterna. Este dispositivo es necesario en el sistema ya que la batería entregará un voltaje de 12VDC y los elementos que se necesitan accionar trabajan con 110VAC.

Figura 2.16. *Inversor 100W/500W*[51]

Características[51]:

- Máxima potencia continua de 500 W.
- Capacidad contra sobretensiones (potencia máxima) 1.000 W.
- Entrada de voltaje de 12.8 V.
- Fusible de 30 Amps.
- Salida de voltaje de 120 V.
- Forma de onda de salida: Onda de seno modificada
- Potencias de hasta 4,17 amperios.

2.3. Análisis del sistema a implementar

Para poder obtener el máximo beneficio en un sistema de vigilancia basado en IP se debe evaluar todas las necesidades que se requieren. Se busca utilizar los recursos de manera óptima y aprovechar cada servicio que brindan los dispositivos IP.

Entonces, se analiza factores como el ancho de banda necesario para transmitir vídeo, capacidad de memoria para almacenar este vídeo, capacidad del sistema para ampliar sus servicios o actualizarlos y puertos necesarios para el control de dispositivos. Todos estos serán analizados a continuación.

2.3.1. Ancho de banda

Para poder definir cuanto ancho de banda se considera necesario para el dispositivo de seguridad, se utiliza la información que suministran los fabricantes acerca del consumo de los dispositivos y de ciertos factores característicos del sistema, como son:

- El tamaño de la imagen que se pretende grabar.
- La compresión del vídeo.
- La frecuencia de la imagen por segundo que se pretende transmitir.
- El ancho de banda disponible en la red.

El ancho de banda (BW) está estrechamente ligado con la capacidad del disco duro necesario para almacenar su información. Por tanto, el ancho de banda se mide en bits por segundo (bps), mientras que la capacidad de disco duro se mide en Bytes.

Hay que recordar que el ancho de banda representa la cantidad de información que se puede transmitir en un segundo por un medio de comunicación. Así, se puede definir dos tipos de velocidades en los canales de transmisión de datos:

Velocidad nominal de Transmisión: Determina la máxima velocidad a la que puede transmitir la información. La velocidad nominal mantiene asociados caracteres de control que no aportan nada real para el mensaje pero son necesarios para dar seguridad y confiabilidad al canal. Esta velocidad es siempre mayor que la velocidad efectiva.

Velocidad efectiva de Transmisión: Ésta determina la cantidad real de datos que el canal trasmite. Se debe tomar en cuenta las posibles colisiones, fallas, errores y perdidas en el canal que podrían reducir la velocidad efectiva en un canal de comunicación.

No hay una fórmula definida para determinar la velocidad efectiva de la velocidad nominal, sin embargo, en este caso la mayor parte del ancho de banda la ocupa la transmisión de vídeo por lo que se puede asumir que la velocidad efectiva será del 60% de la velocidad nominal.

Entonces, para calcular el ancho de banda necesario para una cámara IP expresado en bps se debe utilizar la siguiente formula:

BW = (Velocidad de la imagen) x (Tamaño de cada imagen en promedio) x (% de actividad) x (8) (2.3)

Velocidad de la imagen: Cantidad de tramas que se trasmiten por segundo (FPS). Entre menos FPS se trasmita menor información se envía y menor resolución dinámica se obtiene, se corre el riesgo de perder el instante preciso que se necesita.

El estándar americano de la Comisión Nacional de Sistema de Televisión (NTSC) definió que este valor debe ser de 30 FPS, sin embargo el ojo humano puede ver fácilmente a una velocidad de 24 FPS.

Tamaño de cada imagen en promedio: Se expresa en Bytes y depende del fabricante del dispositivo que envía las señales de red. Depende del algoritmo de compresión que

se esté usando, de la resolución estática de la imagen de vídeo que se desee enviar y de la escena que se esté observando. Como estos factores siempre están cambiando se considera un tamaño promedio que viene a ser un dato que el fabricante proporciona.

% de actividad: Es necesario que esté en notación decimal, es decir si es 50% el valor a poner en la formula será 0.5. El porcentaje de la actividad de la escena determina que tanto cambian las imágenes de un cuadro (o frame) a otro, y que tanto movimiento existe en la escena.

Por lo cual debido a que la cámara filmará únicamente al solicitante de la emergencia los cambios en la escena serán casi nulos, por lo que se toma un 10% por motivos de confiabilidad.

Cálculo del Ancho de Banda

Para el dispositivo de seguridad se tomarán en cuenta los momentos críticos, como una transmisión en la noche en donde se necesite más resolución, por lo tanto la cámara tendrá que transmitir a 30 FPS, en promedio cada frame consume 24KB por la noche, la actividad de la escena debido a que no existen mayores cambios se considera en un 10%, entonces en base a la ecuación 2.3, tenemos:

$$BW = 30FPSx24Kbps * 10\% * 8 \quad (2.4)$$

$$BW = 30x24 * 1024 * 0.1 * 8 \quad (2.5)$$

$$BW = 589.824\ Kbps \quad (2.6)$$

Este valor al pasar a la velocidad nominal que requiere seria:

$$VelNominal = \frac{589.824}{0.6} = 983.040\ Kbps \quad (2.7)$$

Para obtener todo el ancho de banda necesario para el sistema se suma al consumo de la cámara el ancho de banda por el audio transmitido.

Debido a que la voz necesita de 4 KHz para ser comprensible por el oído humano, para transmitir se necesita como mínimo el doble de esta frecuencia, que vendrían a ser 8 Kbps según Nyquist. La cámara permite transmisiones a 8 y 16 Kbps y para este análisis se tomará en cuenta el caso crítico que sería con 16 Kbps; por lo tanto:

$$BW_{audio} = 16Kbps \quad (2.8)$$

$$VelNominal = \frac{16}{0.6} = 26.667\ Kbps \quad (2.9)$$

En el caso del ancho de banda consumido por el servidor, es necesario calcular la transferencia que este debe brindar. Debido a que es un servicio exclusivo y va a ser utilizado únicamente por el "ECU 911", el ancho de banda vendría a ser únicamente la trasferencia de la información serial que este va a transmitir por dos (porque son 2 terminales de operación). Tomando en cuenta que el valor promedio de una trasferencia de datos serial es de 9.6 Kbps, el valor para la transferencia de datos es entonces:

$$BW_{servidor} = 9.6\ Kpbs * 2 \quad (2.10)$$

$$VelNominal = \frac{19.2}{0.6} = 32Kbps \quad (2.11)$$

Finalmente sumamos todas las velocidades necesarias para obtener su valor final:

$$BW_{total\_nominal} = 983.040Kbps + 26.667Kbps + 32Kbps \quad (2.12)$$

$$\boldsymbol{BW_{total\_nominal} = 1.041707Kbps \approx 1Mbps} \quad (2.13)$$

Cabe recalcar que este valor esta dimensionado en un caso crítico en donde se utilicen todos los recursos.

Entonces, la red que se necesite para el uso de estos dispositivos dependerá del número de ellos, si se van a instalar 5 dispositivos por ejemplo, se necesitaran 5 Mbps de la red.

2.3.2. Almacenamiento

En caso de que se desee almacenar el vídeo de la cámara es necesario dimensionar la capacidad necesaria de un disco duro que se necesitara dependiendo de varias variables, estas son las siguientes:

- Número de canales o cámaras.
- Resolución a la que se desea grabar.
- Velocidad a la que se desea grabar cada señal de vídeo.
- Algoritmo de Compresión.
- Calidad que se desea en las señales de vídeo almacenadas.
- Tipo de complejidad en cada imagen.
- Tamaño promedio de cada imagen almacenada.
- Tiempo de grabación diario.
- Actividad de la escena que deseo grabar, de acuerdo a la operación y horarios del sitio.
- Forma de grabación (continua, por eventos, por lapso de tiempo)
- Cantidad de información que se desea almacenar

- Importancia que desea dar a cada escena.

Se deben analizar todos estos factores para poder realizar un cálculo final.

Cálculo de la capacidad de un Disco Duro:

En base a los cálculos del ancho de banda obtenido anteriormente, para calcular la capacidad de disco duro se debe seguir la siguiente metodología:

- Calcular cuánto se necesita para almacenar un segundo de vídeo.
- Multiplicar este número por el número de segundos que se desee almacenar.
- Multiplicar este número por el número de cámaras (en este caso será solamente una).

Debido a que en la sección anterior se calculó el ancho de banda necesario para transmitir vídeo y audio desde el dispositivo, se tomarán estos datos que son los siguientes:

$$BW_{video} = 589.824\ Kbps \tag{2.14}$$

$$BW_{audio} = 16Kbps \tag{2.15}$$

$$BW = 589.824\ Kbps + 16Kbps = 605.824\ Kbps \tag{2.16}$$

Para obtener la capacidad del disco duro se multiplica este ancho de banda usado en un segundo por el número de segundos que en promedio se va a utilizar el dispositivo en un mes y este valor por el número de dispositivos que en nuestro caso es uno.

$$CapacidadDisco = BW * SegundosMes * 1 \quad (2.17)$$

La "Unidad de Estadística y Evaluación ECU-911" lleva nóminas de las llamadas de emergencia por día y por tipo, sin embargo no se puede utilizar estos datos debido a que este dispositivo es nuevo. Es decir que no existe registro de estadísticas para este tipo de dispositivo. Este estará en un lugar público en donde cualquier persona pueda acceder. Las video-llamadas de emergencia que se realizaran serán de sucesos que ocurran solo en esta zona, por esto se ha decidido tomar en cuenta un escenario crítico en el cual cada llamada de emergencia duraría 90 segundos y se darían 3 llamadas de emergencia por día. Entonces el tiempo de video-llamada en un mes seria:

$$SegundosMes = 90 * 3 * 31 = 8371 \text{ s} \quad (2.18)$$

Finalmente se calcula la capacidad necesaria del Disco Duro:

$$CapacidadDisco = 605.824 \text{ Kbps} * 8371 \text{ s} * 1 = 5071352.704 \text{ Kb} \quad (2.19)$$

$$CapacidadDisco = 5.1[Gbytes] \quad (2.20)$$

Hay que tomar en cuenta que este valor esta dimensionado para un solo dispositivo, con el que se podrá grabar las video-llamadas en un mes.

2.3.3. Escalabilidad

Se podrá agregar a la red varios dispositivos de seguridad siempre que esté disponible ancho de banda en la red, entonces su escalabilidad estará en función de la capacidad de la red que pueda brindar el proveedor al "ECU 911".

La escalabilidad del dispositivo en cambio estará en función de los puertos disponibles por la cámara, los puertos y servicios disponibles por el sistema de control y por la capacidad de reprogramación del sistema de control.

- El sistema de control del dispositivo se dará por un Arduino UNO, que cuenta con: 10 Pines digitales, que pueden ser usados para entrada como salida, 6 canales de ingreso analógicos, 6 canales de salida analógica (PWM), lo que permite incrementar características de operación al sistema final.
- La programación del servidor que estará alojado en el "Arduino Ethernet Shield" es sencilla, sin embargo se requiere conocer el lenguaje de programación de Arduino, html y php para poder modificarlo sin mayores inconvenientes y ampliar las características de funcionamiento.

Hay que tomar en cuenta que toda la transmisión utiliza IP, que al ser un estándar internacional permite una fácil adaptación con otros dispositivos y servicios que manejen el mismo protocolo.

2.3.4. Gestión de vídeo

La gestión de vídeo se lo realiza basado en la norma H.264 conocido también como MPEG-4 parte 10, que define un códec de vídeo de alta compresión. La intención del proyecto H.264/AVC fue la de crear un estándar capaz de proporcionar una buena calidad de imagen con tasas binarias inferiores a los estándares previos[52].

Dicho codificador presenta mejoras en el ancho de banda con respecto a sus predecesores en un 50%.

El codificador H.264 fue diseñado para aplicaciones de bajo costo y es usado en aplicaciones móviles y servicios de vídeo conferencias ya que brinda mayor robustez frente a la pérdida de información. La tabla 2.1 resume las características del codificador H.264.

Característica	**H.264/MPEG-4 Part 10/AVC**
Tamaño del macro bloque	16x16
Tamaño del bloque	8x8, 16x8, 8x16, 16x16, 4x8, 8x4, 4x4
Codificación	VLC, CAVLC, CABAC
Perfiles	3 perfiles, varios niveles en cada perfil
Tipo de Cuadros	I, P, B, SI, SP
Ancho de Banda	64 kbps a 150 Mbps
Compatibilidad con estándares previos	No

Tabla 2.1. *Características del estándar de vídeo*[53]

2.3.5. Gestión de audio

Para la gestión del audio se manejará el estándar de la ITU-T G.711 el mismo que es usado principalmente en telefonía, implementando las leyes de cuantificación "ley A" y "ley μ[8]".

El estándar de codificación digital G.711, permite representar una señal de audio en frecuencias de la voz humana, mediante palabras de 8 bits de resolución, con tasa de 8000 muestras por lo que proporciona un flujo de datos de 64 kbit/s.

La primera implementación del estándar G.711 minimiza el uso de la memoria, y la segunda utiliza paralelismo de datos para reducir al mínimo la carga de procesamiento del núcleo.

2.3.6. Entradas y salidas digitales del sistema a implementar

Para el diseño del sistema se pretende manejar distintos elementos remotamente para lo cual se requieren las siguientes entradas y salidas mostradas en la tabla 2.2.

Elemento	**Tipo de Señal**	**Uso**	**E/S**
Luz estroboscópica	Digital	Encendido - Apagado	Salida
Alto parlante	Digital	Encendido Apagado	Salida

[8] Estas "leyes de cuantificación" estandarizan en 256 niveles no lineales la cuantificación y codificación de la voz en telefonía.

	Analógica Analógica	Ganancia amplificador Señal de Voz	Salida Salida
Iluminación led	Digital	Encendido Apagado	Salida
Sensor de movimiento	Digital	Detección	Entrada
Cámara	Digital --------	Encendido Apagado Transmisión Audio-Vídeo	Salida --------
Pulsante	Digital	Estado	Entrada

Tabla 2.2. *Entradas y Salidas digitales y analógicas*

RESUMEN

Salidas Digitales.	4
Salidas Analógicas.	2
Entradas Digitales	2
Entradas Analógicas.	-

Tabla 2.3. *Total de Entradas y Salidas digitales y analógicas*

CAPITULO 3. IMPLEMENTACIÓN DEL DISPOSITIVO

3.1. Introducción

En este capítulo se muestra una clara y breve explicación de cómo se realizó el diseño, interconexión y códigos de este proyecto.

Primero se describe el diseño de hardware en donde se expone la conexión de todos los elementos involucrados, tanto de manejo y administración como de energía.

Luego se describe todos los procesos para el diseño de software, desde configurar los videoteléfonos, hasta cargar los códigos de funcionamiento al servidor Elastix y a los microcontroladores de Arduino.

3.2. Diseño de hardware

El diseño de hardware consta de dos partes, la primera tiene que ver con la forma de interconexión de los elementos y dispositivos que van a utilizarse, mientras que la segunda tiene que ver con el respaldo de energía.

Los dispositivos que van a ser utilizados así como su funcionamiento y descripción se las puede ver en el capítulo 2, por este motivo en esta sección únicamente se muestra su interconexión.

Conocidos todos los dispositivos a utilizarse, su interconexión se debe realizar de la siguiente forma: (Ver figuras 3.1 a 3.2).

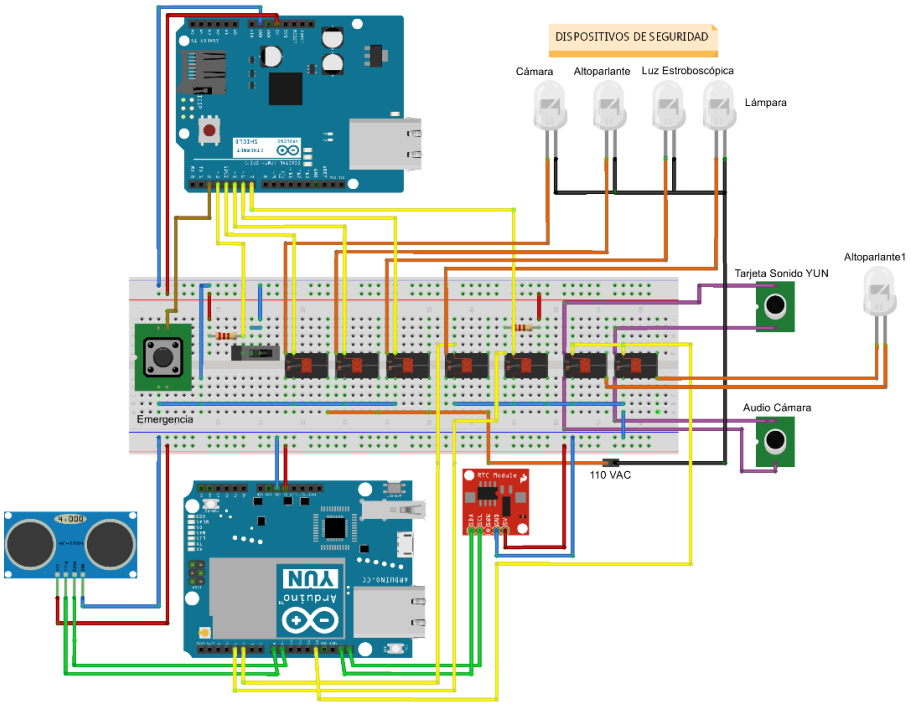


Figura 3.1. *Esquema de Conexiones*

En la figura 3.2 se muestra el esquema de la circuitería realizada.

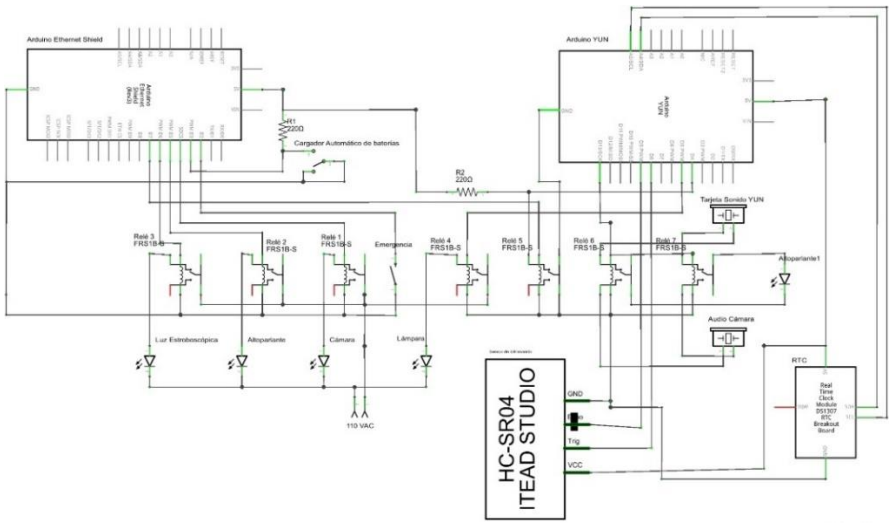


Figura 3.2. *Esquema del circuito*

En la figura 3.3 se muestra el diagrama operacional del sistema.

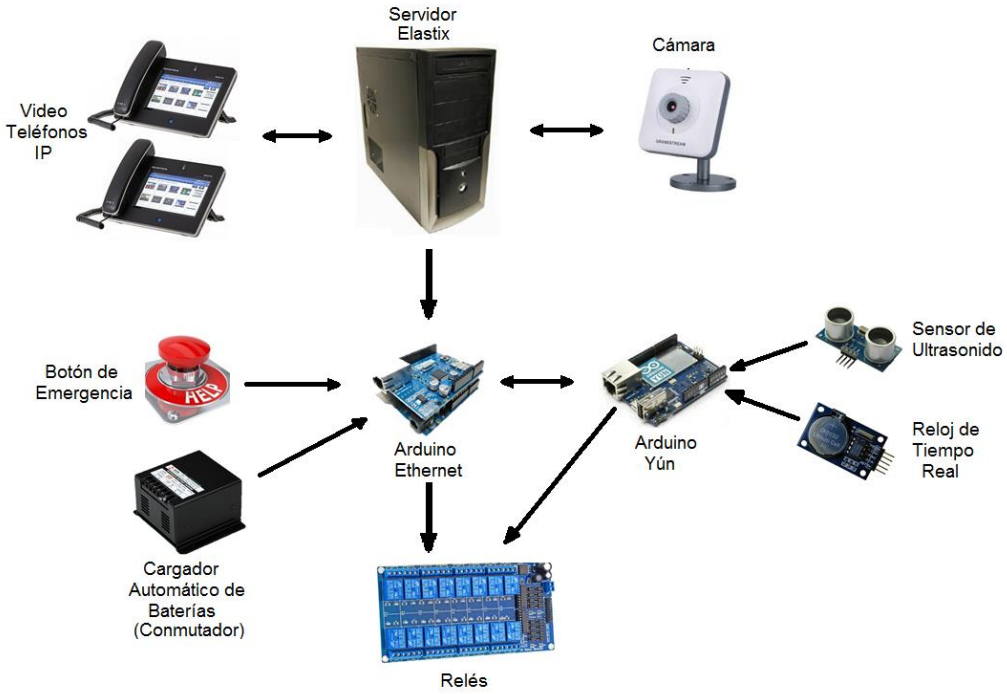


Figura 3.3. *Diagrama de Bloques Operacional*

3.2.1. Respaldo de energía

Para realizar un respaldo de energía eficiente se han utilizado tres elementos:

- Cargador automático de baterías: carga la batería cuando existe alimentación.
- Batería 12V/7Ah: Batería de siete amperios hora de doce voltios.
- Inversor: Trasforma la corriente directa de 12V (DC) a alterna de 110V (AC).

Su conexión se representa en la figura 3.4.

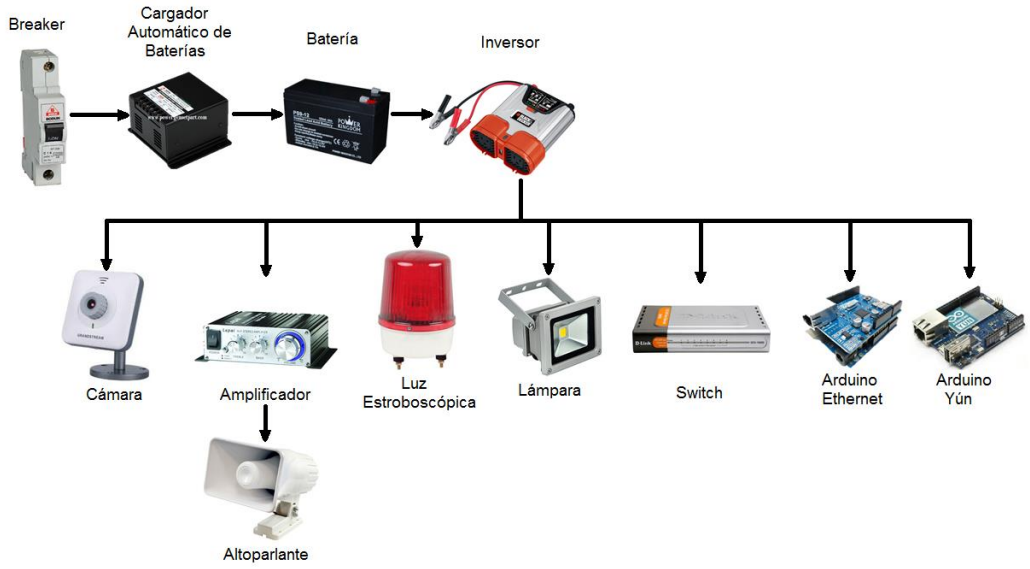


Figura 3.4. *Diagrama de Bloques Alimentación*

El cargador automático de baterías está conectado a la corriente eléctrica, este a su vez mantiene cargada la batería que está alimentando al inversor.

El inversor energiza a todos los dispositivos de tal manera que si se va la energía, el cargador deja de funcionar pero la batería provee la alimentación para que el inversor funcione correctamente.

En caso de existir un corte de energía los dispositivos no sufren ningún problema o pico de energía ya que el cargador se encarga de regular este voltaje en caso de corte. Además, el cargador proporciona un conmutador que se activa en caso de que no exista energía, el mismo que se usa para enviar un aviso a un puerto del Arduino.

También es necesario determinar cuánto tiempo puede la batería mantener energizado al sistema antes de descargarse se procede en primer lugar a determinar el consumo máximo de los dispositivos conectados, este consumo se lo puede ver en el tabla 3.1.

Elemento	**Amperaje (A)**
Cámara	0.05
Luz Estroboscópica	0.33
Tarjetas	0.03
Switch	0.02
Cargador Automático de Baterías	0.1
Amplificador	0.14
Total	**0.67A**

Tabla 3.1. *Consumo de amperaje del sistema*

Como el consumo máximo es de $0.67A$ y la batería utilizada es de 7Ah, simplemente se divide el amperaje por hora de la batería del amperaje total del sistema para obtener el tiempo que la batería podrá mantener energizados a los elementos antes de descargarse.

$$tiempo[H] = \frac{7AH}{0.67A} = 10{,}44 \approx 10\ Horas \qquad (3.1)$$

Por tanto, la batería podrá mantener a los equipos energizados hasta 10 horas luego de un corte de energía. Se debe indicar que si la energía retorno, el cargador recarga completamente la batería y esta podrá nuevamente mantener a los dispositivos energizados por otras 10 horas.

3.3. Diseño de software

Para presentar cómo se realizó el diseño de software, se ha dividido la configuración y programación del proyecto en partes, para así comprender la función que cumple cada sección y su código, mostrando diagramas de flujo que contienen el código completo.

El diseño de software empieza por mostrar cómo se configuran extensiones en Elastix, pasando por la configuración de la cámara y los videoteléfonos IP hasta el código utilizado en el servidor de Elastix y Arduino[54].

Se ha dividido este diseño de la siguiente forma:

1. Configuración de extensiones en Elastix.
2. Configuración de la cámara IP.
3. Configuración de los videoteléfonos IP.
4. Llamadas salientes a través de Elastix mediante Arduino.
5. Control de puertos de Arduino mediante Elastix.
6. Control de luz nocturna y activación de alarma.
7. Diagramas de flujo de los códigos.

3.3.1. CONFIGURACIÓN DE EXTENSIONES EN ELASTIX

Para poder comunicar los videoteléfonos, cámaras o cualquier otro dispositivo que permita la transmisión por el protocolo SIP es necesario crear extensiones en Elastix. Para realizar esto se deben seguir las siguientes instrucciones:

Ingresar a un navegador que este en la misma red que el servidor e ingresar la URL del servidor.

Para este ejemplo se tiene:

- IP servidor: 192.168.10.170
- Usuario: ***Root***, Password: ***passcsc***
- Usuario: ***Admin***, Password: ***adminups***

Cuando se ingrese por primera vez se solicita la contraseña, en esta interfaz se debe utilizar el usuario admin con su respectiva contraseña.

En la pantalla inicial se puede ver la consola de administración Web, aquí se gestiona todo el servidor Elastix, por defecto aparece la pantalla de información del sistema que se muestra en la figura 3.5.

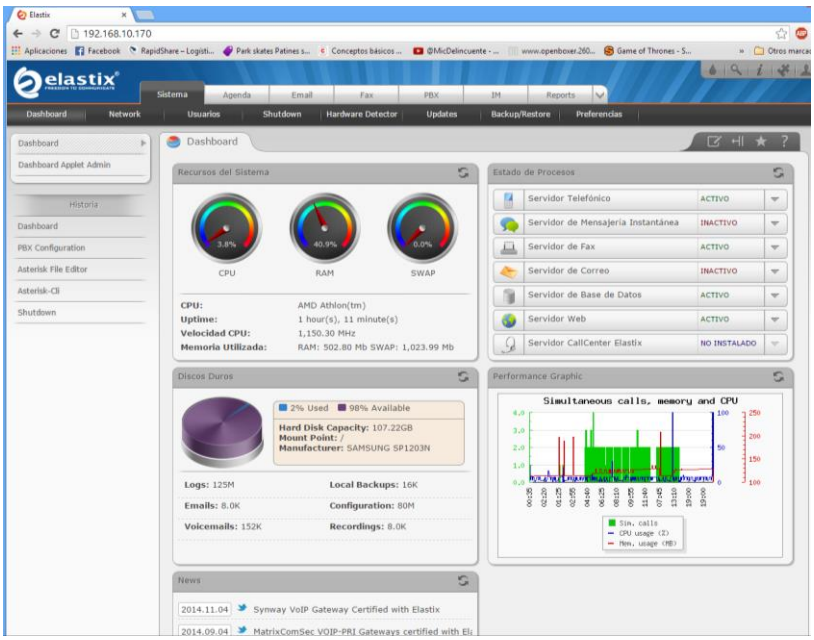


Figura 3.5. *Consola web de Elastix*

Para el ingreso de una extensión se debe tener en cuenta cuatro parámetros para su configuración básica, estos son:

- Tipo de extensión (en nuestro caso únicamente se usara la extensión SIP).
- Número de extensión.
- Nombre de la extensión.
- Clave de la extensión.

Cada extensión debe tener un número único, para que no existan conflictos en el plan de marcado.

En la interfaz de administración Web se debe ingresar en PBX->Extensiones.

Aquí seleccionamos el Device: "Generic SIP Device" y damos click en Submit, este será el primer parámetro de ingreso como se muestra en la figura 3.6.

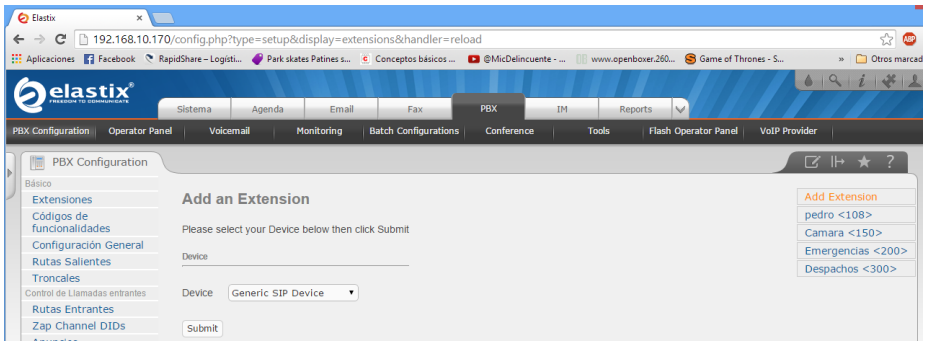


Figura 3.6. *Configuración PBX*

Se nos abrirá una nueva página: "*Add SIP Extension*", en donde colocaremos los tres parámetros restantes de la siguiente manera:

- User Extension: *200*
- Display Name: *Emergencias*
- Secret: *prueba200*

Como se puede observar en la figura 3.7.

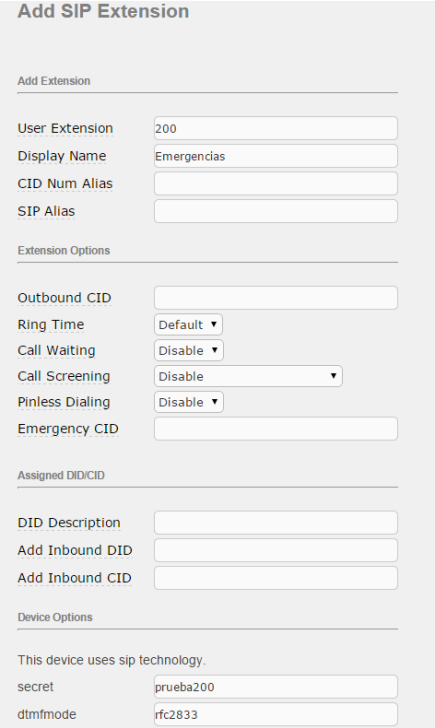


Figura 3.7. *Adición de extensión SIP*

Finalmente se aplica la configuración dando click en la región rosada como se observa en la figura 3.8.

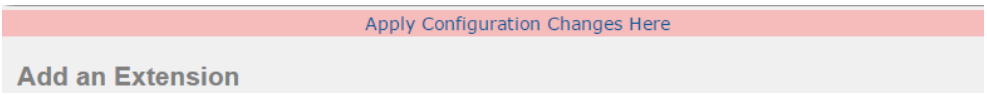


Figura 3.8. *Aplicar configuración de extensión SIP*

Se realiza el mismo procedimiento para todas las extensiones que se requiera, en este caso se necesita 3 extensiones (2 videoteléfonos, 1 cámara) y además se agregará una cuenta más para pruebas. Deberemos tener entonces 4 extensiones creadas como se muestra en la figura 3.9.

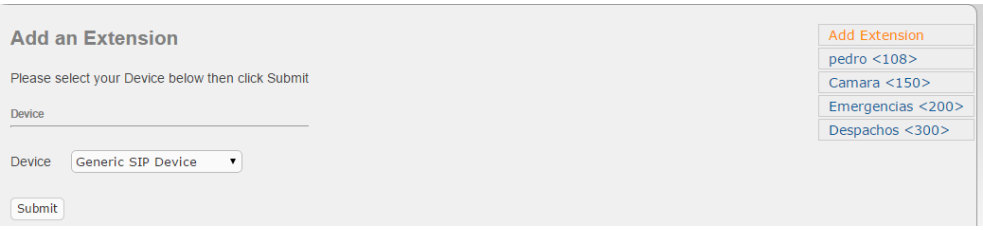


Figura 3.9. *Extensiones creadas*

Grupos de Timbrado.

En ocasiones se requiere que al marcar un número específico, se llamen simultáneamente a varias extensiones; para esto se usan los grupos de timbrado.

Para configurar un grupo de timbrado se debe acceder a ***PBX->Grupos De Timbrado***

Aquí debemos dar cuatro parámetros para su configuración:

- Número del grupo: Número del grupo.
- Descripción: Nombre del grupo.
- Lista de extensiones: Extensiones a las que se requiere llamar.
- Destino: Lugar de dirección de llamada en caso de no respuesta.

Se ha realizado un grupo de llamada para las extensiones 200 y 300, se puede ver en la figura 3.10.

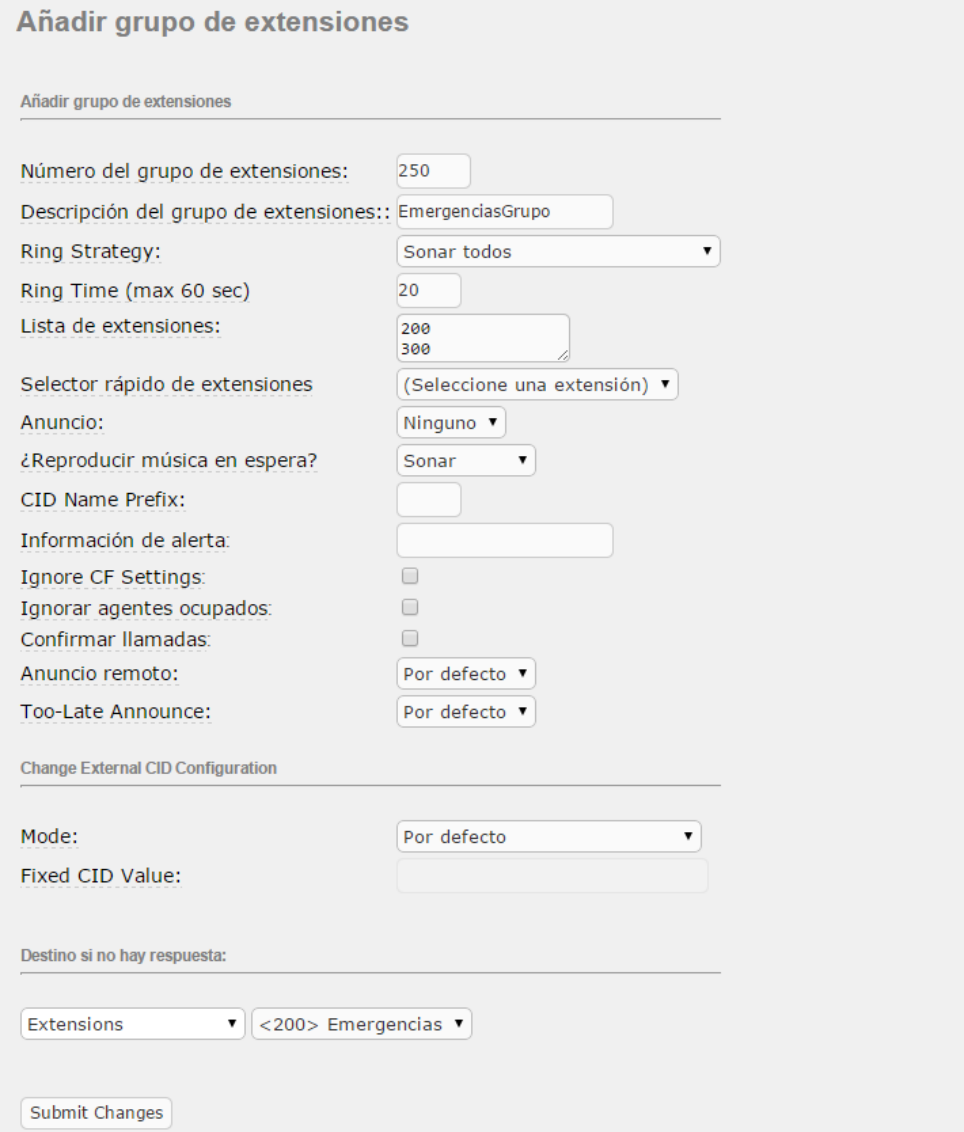


Figura 3.10. *Añadir grupo de extensiones*

3.3.2. Configuración de la cámara IP

Para poder configurar la cámara IP (GXV3615WP_HD) se debe colocar la URL de la cámara desde un navegador que este en la misma red que esta.

Si no se conoce cuál es la IP de la cámara, se debe acceder a “Mis Sitios De Red”, en donde aparece el dispositivo y en sus propiedades se puede ver su IP, este proceso se puede ver en la figura 3.11.

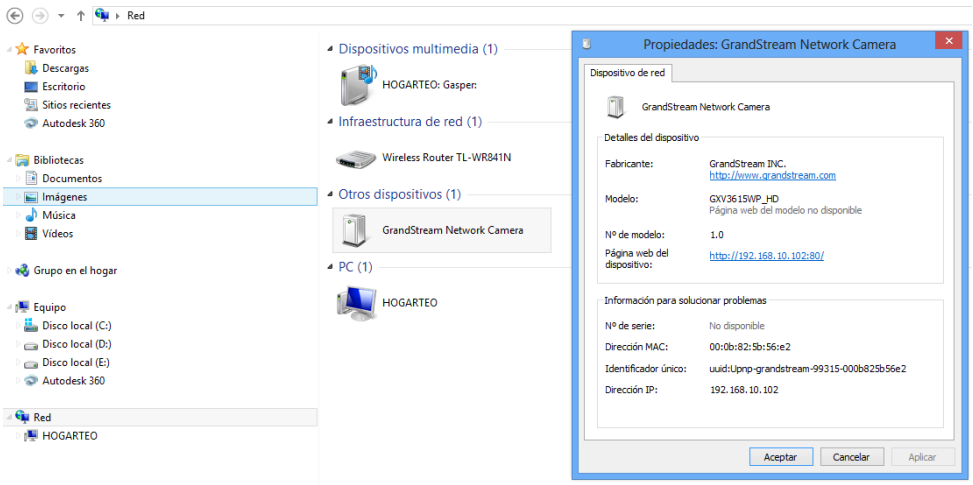


Figura 3.11. *Obtener IP de la cámara*

Una vez conocida la IP de la cámara, se accede mediante el navegador, la primera vez nos pedirá un nombre de usuario y contraseña que por defecto es:

- Nombre de Usuario: admin
- Contraseña: admin

Una vez en la página de administración de la cámara podemos acceder a la configuración de esta, existen varias pestañas de configuración como se puede observar en la figura 3.12, sin embargo se dará a conocer únicamente la configuración pertinente, en este caso:

- Vídeo & Audio
- SIP

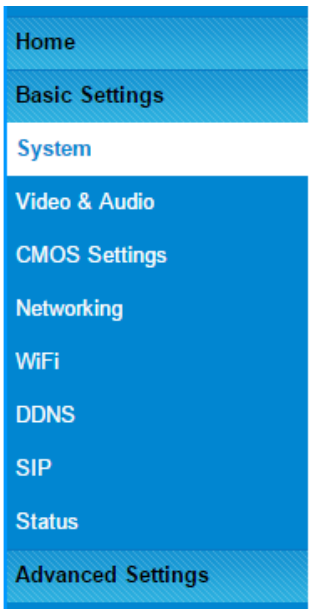


Figura 3.12. *Configuración de la cámara*

3.3.2.1. Vídeo & Audio

Para la configuración de vídeo, se debe utilizar un protocolo que permita manejar tanto en la cámara, en el videoteléfono y a través del servidor, en este caso se usara el códec de vídeo "H264".

En "Video Settings" se puede cambiar la resolución, Bit Rate, Calidad de Imagen entre otras, esto se configura a preferencia del usuario.

También hay que tener en cuenta que existen dos configuraciones para el stream de vídeo, las cuales podrán ser asignadas ya sea para la transmisión SIP o Web, esto se puede cambiar en la configuración "SIP".

Además, para la configuración de audio se puede usar los códecs PCMU o PCMA que son exclusivamente para VoIP, y el volumen del micrófono como del altavoz ya dependerá del usuario. Las configuraciones asignadas para el proyecto se las puede ver en la figura 3.13.

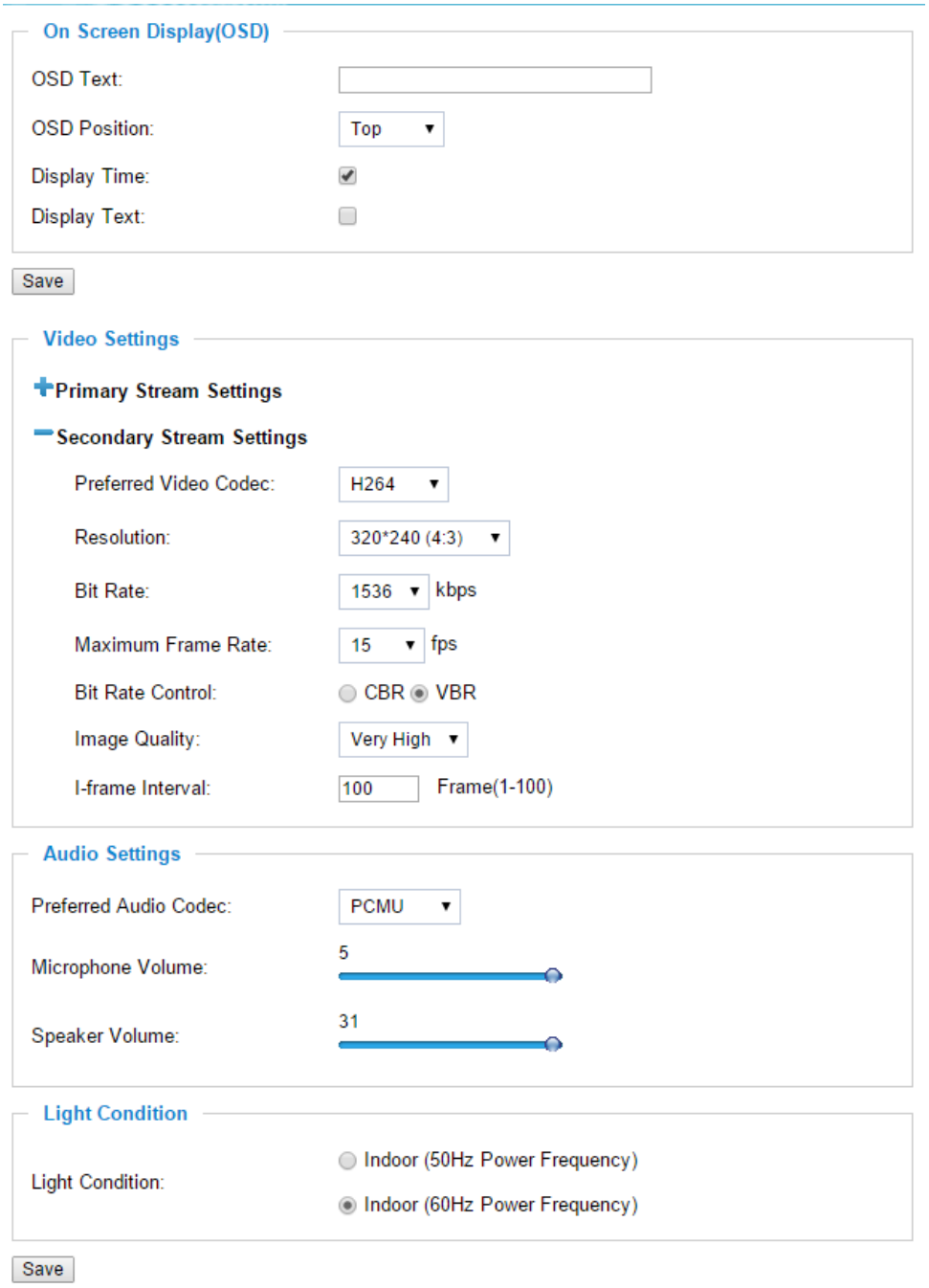


Figura 3.13. *Parámetros de configuración de la cámara*

3.3.2.2. SIP

Para configurar una cuenta SIP en la cámara, se deberá dirigir hacia la configuración SIP en la parte izquierda de la página, a continuación asignar los siguientes campos:

- Account Name: Nombre de la cuenta.
- SIP Server: Dirección IP del servidor VoIp en este caso Elastix.
- SIP User ID: Numero de la extensión.
- Authenticate ID: Numero de extensión.
- Authenticate Password: Contraseña de la extensión.

Una vez guardados los cambios la cámara se pondrá online, esto se puede verificar al inicio de la página en letras verdes. Estas configuraciones se observan en la figura 3.14.

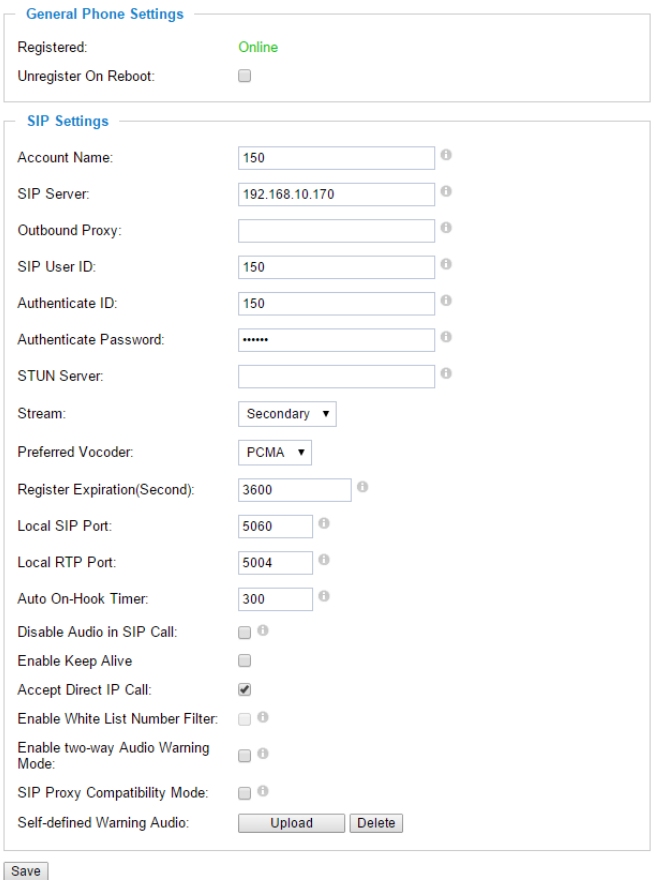


Figura 3.14. *Configuración SIP*

Para acceder a la cámara, únicamente se debe llamar a la extensión de la cámara y se podrá interactuar con la misma.

3.3.3. Configuración de los videoteléfonos IP

Los videoteléfonos IP usados para el proyecto (GRANDSTREAM GXV3175) cuentan con una variedad de servicios multimedia como redes sociales, pantalla táctil, cámara, navegador web, música, entre otras cosas para el proyecto, sin embargo únicamente se dará a conocer como se configuran las cuentas SIP.

Estos teléfonos permiten tener hasta 3 cuentas SIP que pueden estar habilitadas simultáneamente.

Para configurar la cuenta SIP se debe acceder a **Menu->Configuracion->Cuentas**

Aquí se podrán configurar las tres cuentas, para esto debemos llenar los siguientes campos:

- Nombre de cuenta: Se asigna el nombre de quien va a utilizar la cuenta.
- Servidor SIP: Se asigna la dirección IP del servidor (Elastix).
- ID usuario SIP: Numero de extensión.
- ID autentificación SIP: Numero de extensión.
- Contraseña autentificación SIP: Contraseña de la extensión.

Para nuestro caso, en la figura 3.15 se han realizado las siguientes configuraciones para el primer teléfono:

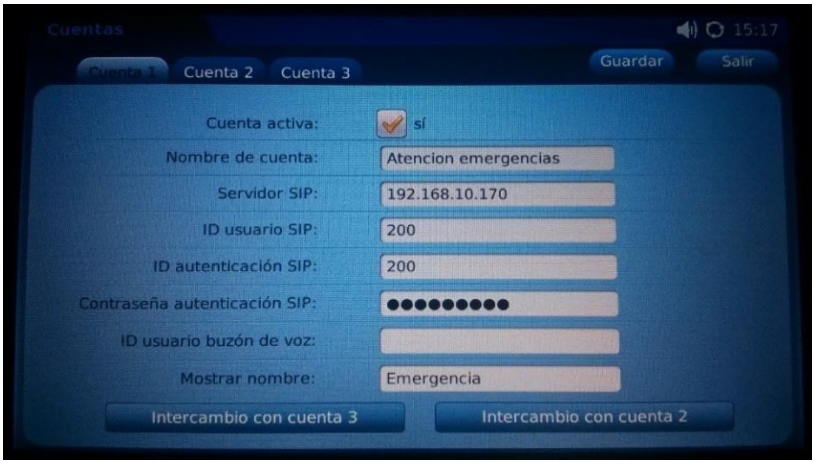


Figura 3.15. *Configuración de cuenta SIP en teléfono*

3.3.4. Llamadas salientes a través de Elastix implementando Arduino

El objetivo de generar llamadas salientes es, que en caso de que suceda un evento como pulsar un botón, activación de sensor, entre otros, se genere una llamada hacia un destino predeterminado y genere un aviso.

3.3.4.1. Funcionamiento de llamadas Elastix-Arduino

En el servidor Elastix está alojado un script: ***.php***, en el cual se verifica si el cliente que está accediendo tiene una dirección IP igual a una pre-definida en el script. Si estas direcciones son iguales se genera un archivo de llamada (call file), en este podemos configurar a que número deseamos llamar; este archivo es enviado al directorio de cola de salida de Elastix para que genere la llamada.

Arduino debe funcionar como un cliente Web, esto se puede lograr gracias a su Shield: "Ethernet" y este debe tener asignado una dirección IP que sea la misma que la predefinida en el script de Elastix.

En el archivo de extensions.conf de Elastix se debe asignar un Dialplan para que la llamada que Elastix debe generar tenga su plan de marcado respectivo.

3.3.4.2. Incidencia en el proyecto

Para este proyecto se necesita generar una llamada en caso de que sucedan 3 posibles eventos:

1. Cuando se pulsa un botón (Para la llamada de emergencia).
2. Cuando exista un fallo de energía, el cargador automático de baterías acciona a un switch y este debe generar una llamada de advertencia.
3. Cuando se llamada a la extensión del Arduino, podemos realizar una petición del estado del cargador automático de baterías (comprobar si hay energía o no).

Todas las llamadas se realizan hacia la extensión 200, desde un mismo dispositivo en este caso un Arduino Uno + Ethernet Shield.

3.3.4.3. Pasos para la configuración

Para hacer esto posible se debe seguir los siguientes pasos:

1. Copiar los archivos*: "arduino_call.php", "arduino_call_energia.php", "arduino_call_energia_0.php", "arduino_call_energia_1.php"* en el directorio web de Elastix, en este caso se ha usado la versión 2.5.0 y su directorio se encuentra en: ***/var/www/html.***

Estos cuatro archivos deben generarse considerando que:

- Deben tener asignados una IP específica.
- Sus variables deben estar debidamente declaradas: Archivos temporales, dirección de salida para archivo temporal, contexto, identificador de llamada.
- Deben tener una condición de sincronización entre las IPs de Arduino y Elastix para su funcionamiento (podría cambiarse la condición, depende del requerimiento).
- Se deben generar archivos temporales para realizar una llamada.
- Dar permisos de ejecución de los archivos.
- Se debe mover los archivos temporales al directorio de salida del servidor Elastix para el marcado.

La única deferencia entre estos es que el ID de marcado es diferente para poder diferenciar entre distintos eventos. Se recomienda ver los diagramas de flujo (Apédice A) para entender su funcionamiento.

Cabe recalcar que el nombre del archivo, así como sus parámetros pueden ser modificados en caso de que se requiera adaptar a otras necesidades, solo hay que asegurarse que estas configuraciones sean las mismas para todos los archivos.

2. En el archivo ***/etc/asterisk/extensions.conf*** (se puede acceder también desde la IP de Elastix en la pestaña de herramientas), se deben agregar las siguientes líneas al final.

```
[arduino_call]
exten => s,1,Answer
exten => s,n,Wait(1)
exten => s,n,Festival(Emergencia parque ECU)
exten => s,n,Hangup
```

```
[arduino_call_energia]
exten => s,1,Answer
exten => s,n,Wait(2)
exten => s,n,Hangup

[arduino_call_energia_1]
exten => s,1,Answer
exten => s,n,Wait(2)
exten => s,n,Hangup

[aarduino_call_energia_0]
exten => s,1,Answer
exten => s,n,Wait(2)
exten => s,n,Hangup
```

Dialplan1. *extensions.conf*

Este Dialplan puede ser modificado al igual que el código para adaptarlo a otras necesidades; para ver que otros comandos se pueden utilizar la información de www.voip_info.org [9]

3. Subir el sketch *"Llamadas.ino"* al Arduino, en este caso como se dijo, se utiliza un Arduino Uno + Ethernet Shield:

```
//************************************************************
// LLamado a librerías
//************************************************************
#include <SPI.h>
#include <Ethernet.h>
```

[9] http://www.voip-info.org/wiki/view/Asterisk+-+documentation+of+application+commands

```
//************************************************************
// Declaración De Variables
//************************************************************
byte mac[] = { 0xDE, 0xAD, 0xBE, 0xEF, 0xFE, 0xED };
IPAddress ipArduino(192, 168, 10, 172); // IP asignada al Arduino
EthernetServer server(23);
EthernetClient client;

byte serverName[] = { 192, 168, 10, 170 }; // Asterisk PBX
const int buttonPin = 2;  // Pin para botón de emergencia
int buttonState = 0;      // variable para leer el estado del botonton

int estadoAnteriorEnergia = 0;
int estadoActualEnergia;
int contadorEnergia = 0;
int pinEnergia = 3;; // aquí el pin digital que se quiere leer
int c=0;
//************************************************************
// Funcion Void Setup
//************************************************************
void setup() {
  Ethernet.begin(mac, ipArduino);
  server.begin();
  Serial.begin(9600);   // PARA DEPURACIÖN
  pinMode(buttonPin, INPUT);
  pinMode(pinEnergia, INPUT);

  delay(1000);
}// FIn void setup

//************************************************************
// Función Void Loop
//************************************************************
```

```
void loop () {
  buttonState = digitalRead(buttonPin);
  estadoActualEnergia = digitalRead(pinEnergia);

  EthernetClient client = server.available();//cliente se conecta al servidor
  // Si se presiona boton de emergencia ==================
  if (buttonState == LOW) {
    sendllamadaarduino(); // cliente envia get funcion
  }
  // Si se activa switch de fallo energia ==================
  if (estadoAnteriorEnergia != estadoActualEnergia)  // ha habido un cambio de estado
  {
    contadorEnergia++;            // cuenta los cambios de estado
    int validarParEnergia = contadorEnergia % 2;      // solo queremos los cambios pares
    if (validarParEnergia != 1)    // si el cambio es par
    {
      sendllamadacorteenergia(); // cliente envia get funcion
    }
    estadoAnteriorEnergia = estadoActualEnergia;
  }
//=================================================
}// FIn void loop
//*********************************************************
// Función sendllamadaarduino
//*********************************************************
void sendllamadaarduino() {
  Serial.println(Ethernet.localIP()); // PARA DEPURACIÖN
  delay(1000); //Evita que se cuelgue la llamada
  if (client.connect(serverName, 80)) {
    Serial.println("Conectado"); // PARA DEPURACIÖN
    client.println("GET /arduino_call.php HTTP/1.0");
```

```
    client.println();
    client.stop();
  } // Fin if client
  else {
    Serial.println("Connection failed"); // PARA DEPURACIÖN
    client.stop();
  } // Fin else
}// Fin sendllamadaarduino

//*********************************************************
// Función sendllamadaarduino
//*********************************************************
void sendllamadacorteenergia() {

  delay(1000); //Evita que se cuelgue la llamada
  if (client.connect(serverName, 80)) {
    Serial.println("Conectado"); // PARA DEPURACIÖN
    client.println("GET /arduino_call_energia.php HTTP/1.0");
    client.println();
    client.stop();
  } // Fin if client
  else {
    Serial.println("Connection failed"); // PARA DEPURACIÖN
    client.stop();
  } // Fin else
}// fin sendllamadacorteenergia
```

Sketch 1. *Llamadas.ino*

3.3.4.4. Consideraciones para configurar el Dialplan

Para configurar el Dialplan, lo óptimo es acceder al menú herramientas de Elastix desde un navegador web con la dirección de Elastix.

El Dialplan se puede modificar agregando otros números de extensión u otros comandos, estos están bien documentados en la web y se debe conocer que hace cada uno para poder darle un uso óptimo.

Para el aviso generado en el DialPlan: "Emergencia Parque ECU", se ha utilizado el comando: "Festival", este puede ser activado o desactivado en Elastix ya que este paquete viene incorporado en la versión 2.5.0 de Elastix.

Es importante que los archivos *.php* ubicados en el servidor de Elastix tengan los permisos necesarios, caso contrario estos no podrán ser ejecutados y quedaran inservibles. Para realizar un archivo ejecutable se debe utilizar el siguiente comando (en su directorio):

sudo chmod 755 arduino_call.php

Existe más información acerca de este procedimiento en www.Nerdybynature.com[10]

3.3.5. Control de puertos de arduino mediante Elastix

El objetivo de manejar puertos del Arduino a través Elastix es poder activar o desactivar dispositivos conmutando relés mediante una llamada a determinada extensión.

[10] http://www.nerdybynature.com/2010/09/01/br-r-r-r-r-ing-its-your-arduino/

3.3.5.1. Funcionamiento de puertos

En Elastix, en el directorio donde se encuentran los archivos AGI, se debe agregar un archivo en cualquier lenguaje de programación soportado por Elastix (véase 1.6.9), este archivo permitirá establecer una comunicación serial con el Arduino, pudiendo enviar información desde una llamada mediante Elastix y usándola con condiciones para manejar puertos analógicos o digitales mediante Arduino.

Al llamar a determinada extensión en el Dialplan (véase sección 1.6.9) se debe agregar el comando AGI para ejecutar el código *.php* (en este caso el *.php* puede estar en otro lenguaje), para enviar la información del marcado hacia Arduino.

El Arduino en este caso debe funcionar como un servidor web, recibiendo la información del marcado cuando exista una conexión y utilizando esta para comandar los puertos del microcontrolador.

3.3.5.2. Incidencia en el proyecto

Para este proyecto se necesita que al llamar a determinada extensión (100 por ejemplo), se pueda establecer una comunicación serial con el Arduino y al pulsar los dígitos del teléfono cada uno de estos active o desactive relés, para que enciendan dispositivos y/o conmuten una señal de audio.

Los dígitos del teléfono deben funcionar de la siguiente manera:

1. Enciende la luz estroboscópica.
2. Apaga la luz estroboscópica.

3. Enciende el altoparlante.
4. Apaga al altoparlante.
5. Enciende la cámara IP.
6. Apaga la cámara IP.
7. Conmuta la señal de audio desde la tarjeta de sonido hacia el altoparlante.
8. Conmuta la señal de audio desde la cámara hacia el altoparlante y reinicia petición de estado de energía.
9. Realiza una petición del estado de energía.

El número de extensión puede cambiar al igual que las condiciones de marcado a disposición.

3.3.5.3. Pasos para establecer la comunicación entre Elastix y Arduino

Para hacer esto posible se deben aplicar los siguientes pasos:

1. Copiar el archivo*: "codigo_arduino.php"* en el directorio donde se encuentran los archivos AGI, para la versión 2.5.0 de Elastix, este se encuentra en: **/var/lib/asterisk/agi-bin/.**

Este archivo debe generarse considerando que:

- Debe tener asignado una IP específica.
- Se debe incluir la librería *"PHPAGI",* incluida en el paquete de Elastix.
- Sus variables deben estar debidamente declaradas: Direcciones IP, Puertos de Acceso.

- Se debe establecer una conexión con una IP y puerto especifico, en este caso del Arduino (con la función "fsockopen" por ejemplo).
- Si se desea se pueden restringir condiciones de salida, antes del envió de datos.
- El archivo debe enviar los datos.

Se recomienda ver los diagramas de flujo (Apéndice A) para entender su funcionamiento.

Al igual que el resto de códigos, estos pueden ser modificados para poder ser adaptados a necesidades específicas.

2. En el archivo ***/etc/asterisk/extensions_custom.conf***, se deben agregar las siguientes líneas al final.

```
;[codigo_arduino]
exten => 100,1,Answer
exten => 100,2,AGI(codigo_arduino.php)
exten => 100,3,Hangup
```

Dialplan2. *extensions_custom.conf*

Con este, se habilita el archivo "codigo_arduino.php" para establecer la comunicación con el Arduino.

3. Finalmente se carga el sketch *"ClienteYServidor.ino"* al Arduino para que funcione como servidor web y pueda comandar los puertos deseados. Para la realización de este sketch, se ha utilizado el código anterior: "Llamadas.ino" para que el Arduino Uno + Ethernet Shield pueda funcionar como servidor web

y al mismo tiempo como cliente web (realizando llamadas); este sería el código final que se deberá cargar para que funcione de ambas maneras.

```
/*
      Universidad Politécnica Salesiana
            Sede Cuenca

 Código #1 para proyecto de grado:
  "Dispositivo de seguridad que permite la intercomunicación entre dos puntos y activación remota de elementos de seguridad "

Realizado por:
     Mateo Santiago Rengel Rivera
     Mariela Alexandra Jimbo Jerez

  El código es de uso libre, este se lo ha realizado con la ayuda de toda la información disponible en la web, adaptandolo a nuestras necesidades.
*/
//*********************************************************
// LLamado a librerías
//*********************************************************
#include <SPI.h>
#include <Ethernet.h>

//*********************************************************
// Declaración De Variables
//*********************************************************
int PinesDeSalida[] = {5, 6, 7, 4};                    //LED set to pin 4
int x;

byte mac[] = { 0xDE, 0xAD, 0xBE, 0xEF, 0xFE, 0xED };
IPAddress ipArduino(192, 168, 10, 172); // Ip asignada al arduino
EthernetServer server(23);
```

```
EthernetClient client;

byte serverName[] = { 192, 168, 10, 170 }; // Asterisk PBX
const int buttonPin = 2;  // Pin para boton de emergencia
int buttonState = 0;      // variable para leer el estado del botonton

int estadoAnteriorEnergia = 0;
int estadoActualEnergia;
int contadorEnergia = 0;
int pinEnergia = 3;; // aquí el pin digital que se quiere leer

int c=0;
//volatile int state = LOW;

//*********************************************************
// Funcion Void Setup
//*********************************************************
void setup() {
  Ethernet.begin(mac, ipArduino);
  server.begin();
  Serial.begin(9600);   // PARA DEPURACIÖN

  pinMode(buttonPin, INPUT);
  pinMode(pinEnergia, INPUT);

  digitalWrite(buttonPin, HIGH);  // acti0va la resistencia pull-up

  //digitalWrite(pinEnergia, HIGH); // activa la resistencia pull-up

  pinMode(PinesDeSalida[0], OUTPUT);
  pinMode(PinesDeSalida[1], OUTPUT);
  pinMode(PinesDeSalida[2], OUTPUT);
  pinMode(PinesDeSalida[3], OUTPUT);
```

```
  digitalWrite(PinesDeSalida[0], HIGH);
  digitalWrite(PinesDeSalida[1], HIGH);
  digitalWrite(PinesDeSalida[2], HIGH);
  digitalWrite(PinesDeSalida[3], HIGH);

  //attachInterrupt(1, sendllamadacorteenergia, FALLING);

  delay(1000);
}// FIn void setup

//*********************************************************
// Función Void Loop
//*********************************************************
void loop () {
  buttonState = digitalRead(buttonPin);
  estadoActualEnergia = digitalRead(pinEnergia);

  EthernetClient client = server.available();//cliente se conecta al servidor
  // Si se presiona boton de emergencia ==================
  if (buttonState == HIGH) {
    sendllamadaarduino(); // cliente envia get funcion
  }// fin if button/*+-
 //   if (estadoActualEnergia == LOW) {
 //   estadoActualEnergia(); // cliente envia get funcion
 // }// fin if button
//=================================================
=====// Si se activa switch de fallo energia ==================
  if (estadoAnteriorEnergia != estadoActualEnergia)  // ha habido un
cambio de estado
  {
    contadorEnergia++;                    // cuenta los cambios de estado
```

```
  int validarParEnergia = contadorEnergia % 2;      // solo queremos los
cambios pares
  if (validarParEnergia != 1)               // si el cambio es par
  {
    sendllamadacorteenergia(); // cliente envia get funcion
  }
  estadoAnteriorEnergia = estadoActualEnergia;
 }
//=================================================
 if (client) {
  //if connection present
  x = client.read();
  //read information coming from server
  Serial.println(x); // PARA DEPURACIÖN
 } // Finalización de datos del cliente

 switch (x) {
  case 1:
   digitalWrite(PinesDeSalida[0], LOW);
   break;
  case 2:
   digitalWrite(PinesDeSalida[0], HIGH);
   break;
  case 3:
   digitalWrite(PinesDeSalida[1], LOW);
   break;
  case 4:
   digitalWrite(PinesDeSalida[1], HIGH);
   break;
  case 5:
   digitalWrite(PinesDeSalida[2], LOW);
   break;
  case 6:
```

```
      digitalWrite(PinesDeSalida[2], HIGH);
      break;
    case 7:
      digitalWrite(PinesDeSalida[3], LOW);
      break;
    case 8:
      digitalWrite(PinesDeSalida[3], HIGH);
      c=0;
      break;

    case 9:
    c=c+1;
    if(c==1){
// Comprobación de fallo de energia==================
      if (estadoActualEnergia == LOW) {

        energiafallo(); // Sin fallo de energia
      }//fin if button
      else {
        energiacorreto(); // fallo de energia
      }// fin else

//================================================
    }
      break;
    default:
      // si nada encaja, realiza default
      break;
  }// FIn switch case
}// FIn void loop

//*********************************************************//
Función sendllamadaarduino
```

```
//*************************************************************
void sendllamadaarduino() {
  Serial.println(Ethernet.localIP()); // PARA DEPURACIÖN
  delay(1000); //Evita que se cuelgue la llamada
  if (client.connect(serverName, 80)) {
    Serial.println("Conectado"); // PARA DEPURACIÖN
    client.println("GET /arduino_call.php HTTP/1.0");
    client.println();
    client.stop();
  } // Fin if client
  else {
    Serial.println("Connection failed"); // PARA DEPURACIÖN
    client.stop();
  } // Fin else
}// Fin sendllamadaarduino
//*************************************************************
// Función sendllamadaarduino
//*************************************************************
void sendllamadacorteenergia() {

  delay(1000); //Evita que se cuelgue la llamada
  if (client.connect(serverName, 80)) {
    Serial.println("Conectado"); // PARA DEPURACIÖN
    client.println("GET /arduino_call_energia.php HTTP/1.0");
    client.println();
    client.stop();
  } // Fin if client
  else {
    Serial.println("Connection failed"); // PARA DEPURACIÖN
    client.stop();
  } // Fin else

}// fin sendllamadacorteenergia
```

```
//*************************************************************
// Función energiacorreto
//*************************************************************
void energiacorreto() { // Sin fallo de energia
  delay(1000); //Evita que se cuelgue la llamada
  if (client.connect(serverName, 80)) {
    Serial.println("Conectado"); // PARA DEPURACIÖN
    client.println("GET /arduino_call_energia_1.php HTTP/1.0");
    client.println();
    client.stop();
  } // Fin if client
  else {
    client.stop();
  } // Fin else
}
//*************************************************************
// Función energiafallo
//*************************************************************
void energiafallo() { // fallo de energia
  delay(1000); //Evita que se cuelgue la llamada
  if (client.connect(serverName, 80)) {
    client.println("GET /arduino_call_energia_0.php HTTP/1.0");
    client.println();
    client.stop();
  } // Fin if client
  else {
    client.stop();
  } // Fin else
}
```

Sketch 2. *ClienteYServidor.ino*

3.3.5.4. Consideraciones para establecer la comunicación Elastix-Arduino

En el script codigo_arduino.php se pueden asignar diferentes condiciones, avisos de voz, advertencias en caso de error, entre otros; esto ya dependerá que se requiera para el proyecto. En este caso se trata de optimizar el tiempo para que los comandos y avisos se ejecuten en el menor tiempo posible debido a que el proyecto es dedicado para casos de emergencia.

El script también debe contar con los permisos necesarios para que pueda funcionar (chmod 755).

Existen varias maneras de comandar al Arduino. Ya que la comunicación serial nos permite una amplia gama de opciones para generar condiciones, en este caso el uso de un solo número se ha visto conveniente por motivos de optimización de tiempo.

3.3.5. Control de iluminación nocturna y activación de alarma

Para el proyecto se requiere que en las noches, cuando alguien se acerque a la cámara se active una lámpara para que ilumine al solicitante.

3.3.6.1. Funcionamiento

Con la ayuda del RTC indicado en el capítulo 2 se puede tener almacenada la hora y fecha actual sin importar la desconexión de la red eléctrica principal, ya que este se energiza con una pila (tiene una duración aproximada de 5 años). Esta información se usa para condicionar cuando vaya a funcionar un puerto digital. Además para saber si

una persona está cerca o no, se utiliza un sensor de proximidad que nos permite saber la distancia a la que se encuentra algún objeto o persona.

Para enviar sonidos ya sea de alarma o cualquier otro sonido pregrabado, almacenado en una micro SD, se utiliza una tarjeta de sonido que gracias al sistema operativo "OpenWrt" que maneja el Arduino Yún, permite administrar esta tarjeta de Audio con comandos en lenguaje Python.

3.3.6.2. Incidencia en el proyecto

Se requiere que por las noches, cuando un solicitante se acerque a la cámara para presionar el botón de emergencia, una lámpara ilumine automáticamente a este.

Para la cuidad de Cuenca la noche se ha definido entre las 18h00 a las 06h00, en estas horas se debe encender una luminaria en caso de que se acerque un solicitante.

Para determinar si un solicitante está cerca se utiliza un sensor de proximidad que nos permite saber si existe algo a menos de 20 centímetros (distancia configurable).

La reproducción de estos archivos solamente se dará cuando se active un switch.

3.3.6.3. Pasos para la configuración

Para hacer esto posible se deben seguir los siguientes pasos:

- Guardar sonidos de sirena en la tarjeta micro SD.
- Realizar las conexiones correspondientes al Arduino Yún (tarjeta de sonido, micro SD)
- Conectar el RTC y el sensor correctamente, su esquema de conexión se puede ver en la figura 3.1.
- Cargar el sketch "LuminariaYAlarma.ino" al Arduino, sketch que se encuentra mostrado a continuación:

```
/*
      Universidad Politécnica Salesiana
            Sede Cuenca
 Código .ino #2 para proyecto de grado:
  "Dispositivo de seguridad que permite la intercomunicación entre dos puntos y activación remota de elementos de seguridad "
  Realizado por:
     Mateo Santiago Rengel Rivera
     Mariela Alexandra Jimbo Jerez

  El código es de uso libre, este se lo ha realizado con la ayuda de toda la información disponible en la web, adaptandolo a nuestras necesidades.
*/
//*********************************************************
// LLamado a librerías
//*********************************************************
#include <Wire.h> //librería para control de peurtos analogicos
#include "RTClib.h" //librería DS1307
#include <Ultrasonic.h> // libreria para sensor ultrasonico
#include <Process.h>
#include <Bridge.h>
//*********************************************************
// Declaración De Variables
//*********************************************************
```

```
RTC_DS1307 RTC; // asignacion de registro para el RTC
Ultrasonic ultrasonic(9,8); // (Trig PIN,Echo PIN)
float distancia_ultrasonido=0;
double hora_actual=0;
int pin_LuzCamara=5; // pin para luminaria
int UmbralhoraIN=6; // Activación luego de
int UmbralhoraFIN=19;// Activacion Antes de
double Umbraldistancia=10; // Activación Luego de (En centímetros)
int pin_audio=4; // Para activacion de alarma

int buttonState = 0;
Process p;
//************************************************************
// Funcion Void Setup
//************************************************************
void setup() {
  Serial.begin(9600);

  Bridge.begin();
  Wire.begin();
  RTC.begin();

  pinMode(13, OUTPUT);
  pinMode(pin_audio, INPUT);
  Serial.begin(57600);

  Serial.println("Inicio de lectura");

  pinMode(pin_LuzCamara, OUTPUT);
  digitalWrite(pin_audio, HIGH); // activa la resistencia pull-up

}// FIn Void Setup
```

```
//************************************************************
// Función Void Loop
//************************************************************
void loop() {

  // Comprobacion de Switch rele, para activar audio
  buttonState = digitalRead(pin_audio);
  if (buttonState == LOW) {
    digitalWrite(13, HIGH);
    p.runShellCommand("madplay /mnt/sda1/Alarma1.mp3");
    while(p.running());
    Serial.println("it works!");
  }
  else {
    digitalWrite(13, LOW);
  }// fin else
// ==== Fin comprobacion para audio

// Extraccion de hora y distancia
   hora_actual=reloj(); //para comparar, usar hora decimal ->6h30=6.5<-
   distancia_ultrasonido=distancia();



//=================================================
   // Comparaci{on para encendido de luz en caso nocturno
    if(hora_actual<=UmbralhoraFIN    &&  hora_actual>=UmbralhoraIN
){
   // /* // en el dia
    // */
    }else{

      if(distancia_ultrasonido<Umbraldistancia){
           digitalWrite(pin_LuzCamara,LOW);
```

```
                        delay(1000);

                    // digitalWrite(13,HIGH);
        }else{
          digitalWrite(pin_LuzCamara,HIGH);
                        delay(1000);

     }// fin if proximidad
   }// FIN if, else
//================================================
}// FIn void loop

//*********************************************************
// Función Test Reloj
//*********************************************************
 double reloj(){
   double horaact;
   int hora=0; // hora del reloj
   double minutos =0; // ;minutos del reloj

   DateTime now = RTC.now(); // Obtener los datos del reloj
   hora = (now.hour());
   minutos = (now.minute());
   horaact=hora+(minutos/60);//(minutos/60);
    return horaact;
 }// Fin reloj

//*********************************************************
// Función Distancia para el sensor ultrasonido
//*********************************************************
 float distancia(){
    float cmMsec;
    long microsec = ultrasonic.timing();
```

```
  cmMsec = ultrasonic.convert(microsec, Ultrasonic::CM); //
Conversion tiempo a distancia
  return cmMsec;
 }// Fin distancia
```

Sketch 3. *LuminariaYAlarma.ino*

3.3.6.4. Consideraciones para la configuración

Para administrar la tarjeta de sonido, dependiendo de qué tarjeta se esté manejando, se necesita actualizar el sistema operativo así como agregar librerías; un buen ejemplo de cómo hacerlo podemos encontrar en la web: http://dev.mikamai.com[11]

La hora considerada como noche y la distancia para que el sensor de proximidad encuentre al solicitante son configurables.

Se pueden grabar varios archivos de audio e incluso archivos de larga duración, ya es cuestión de en donde y de que maneras se los podría usar; es decir dependen de la aplicación.

3.3.7. Diagramas de flujo de los códigos

Para entender el funcionamiento de cada código de una manera más generalizada, se muestran a continuación sus diagramas de flujo respectivos.

[11] http://dev.mikamai.com/post/69775973742/arduino-yun-with-sound-the-supereasy-way

3.3.7.1. Diagrama de flujo para "Código .php 1: Arduino_call.php"

Los archivos:

- "arduino_call.php",
- "arduino_call_energia.php",
- "arduino_call_energia_0.php",
- "arduino_call_energia_1.php".

Tienen la misma estructura, a diferencia que su contexto para llamar en diferentes ocasiones cambia (se puede observar en el código: "*ClienteYServidor*.ino"), por este motivo se pondrá un solo diagrama de flujo para mostrar el funcionamiento de estos cuatro códigos. (Ver Diagramas de Flujo Apéndice A).

Dado que la configuración y funcionamiento de cada parte se ha explicado minuciosamente a lo largo de este capítulo, si algún operario desea solo utilizar los videoteléfonos para atender una emergencia, necesitará saber únicamente que hace cada comando y los números de extensiones de los dispositivos y esto se encuentra expuesto en el Apéndice B.

Considere que el manual del Apéndice B es válido si es que el código implementado es igual al expuesto a lo largo del capítulo y no ha sido modificado.

CAPITULO 4. ANÁLISIS DE RESULTADOS

Considerando que el Consejo de Seguridad Ciudadana (CSC), presentó la necesidad de disponer de un dispositivo que pueda brindar asistencia inmediata a usuarios que se encuentren en espacios donde exista afluencia masiva de personas, y considerando que estas puedan necesitar de ayuda para poder comunicarse en tiempo real con el ECU-911.

El servicio que debe brindar el dispositivo mencionado es tratar de prevenir posibles hurtos, persuadir delincuentes, monitorear eventos y dar ayuda inmediata desde las instituciones de seguridad.

Por lo cual, mediante el presente proyecto, nombrando como "**Ward System v1.1**" al prototipo inicial, se ha desarrollado un dispositivo que permita cumplir con las especificaciones citadas por parte del Consejo de Seguridad Ciudadana de la ciudad de Cuenca. Dicho dispositivo integra el uso de software libre, un diseño personalizado y ajustado a necesidades de la ciudad, la intercomunicación de tarjetas electrónicas, y la implementación de un servidor telefónico de VoIP. Así, se permite realizar llamadas hacia una central de auxilio, como el ECU-911.

De esta manera se alcanza con el cumplimento del objetivo principal: "diseñar, construir e implementar un dispositivo de seguridad que permite la intercomunicación con audio y vídeo entre dos puntos y la activación remota de elementos de seguridad". Este objetivo se ha logrado por fases, cada una de estas tiene su objetivo específico y método de elaboración, los mismos que se mostrarán a continuación.

Entonces, el primer objetivo específico del proyecto "analizar la problemática de seguridad actual en el cantón Cuenca para las respectivas consideraciones en diseño

del sistema", fue planteado con el fin de considerar el medio en el cual van a operar el dispositivo y así determinar qué elementos podrían ayudar a evitar la inseguridad.

Hay que considerar que el prototipo diseñado se implementó en un lugar donde no exista riesgo de hurto o daño por motivos de pruebas de validación funcional del mismo. Sin embargo, el diseño toma en cuenta una estructura anti vandalismo y resistente a la intemperie.

Figura 4.1. *Instalación de red para pruebas*

El segundo objetivo específico fue: "Determinar los elementos a utilizar (cámaras IP, videoteléfonos IP, altoparlantes, switchs, estructuras, etc.) en el sistema". Esto busca identificar los equipos adecuados para el desarrollo de la aplicación. De esta manera, en el capítulo 2 sección 2.2.3, se puede observar el análisis de cada elemento, su funcionamiento y razón de selección del mismo. Cabe mencionar que estos elementos

han sido elegidos en base a las necesidades planteadas por el CSC, tomando en cuenta la calidad que ofrecen y sus precios.

Es decir que la elección de los elementos y dispositivos implementados en el desarrollo de este proyecto es consecuencia del análisis del lugar a implementar y los recursos disponibles para obtener un balance entre calidad y precio.

Durante el desarrollo del proyecto se determinó la necesidad de implementar una estructura resistente a efectos rigurosos del clima que puedan deteriorar los equipos y muy probablemente de actos vandálicos o intentos de hurto. Esto último considerando que la estructura contiene elementos de un sistema que busca disminuir la delincuencia en las calles.

De esta manera se desarrollaron dos estructuras que contienen a los elementos de seguridad. La primera alberga todos los elementos de interconexión, la luz estroboscópica, el altoparlante y todo el sistema de energía. La segunda estructura contiene la cámara IP, el botón de emergencia y su sensor de proximidad. Ambas estructuras fueron realizadas con metal para ser resistentes a golpes o agresiones.

Entonces, la primera estructura está ubicada a siete metros del piso (distancia específica para el poste de prueba en este caso) lugar inaccesible para personas no autorizadas y la segunda estructura a 1.5 metros del piso, estas estructuras han sido fijadas al poste con cinta "eriband[12]" para poder realizar un fácil desmonte del poste por motivos de pruebas. Por supuesto se recomienda que estas estructuras se suelden al poste y así tener una mejor protección para el dispositivo. El montaje de dichas estructuras se pueden apreciar en la figura 4.3, donde se muestra el montaje de las dos estructuras sobre el poste para pruebas y en la figura 4.4 se aprecia de forma más clara el montaje de la estructura número dos que es el gabinete de la cámara IP.

[12] http://www.comtelec.com/productos/flejes.htm

Las dimensiones de las cajas o estructuras descritas están adaptadas para albergar los elementos de seguridad dándoles espacio suficiente para trabajar con ventilación y evitar el calentamiento, la primera estructura mide 65x60x20cm y la segunda 15x15x14cm.

Conociendo ya los elementos a utilizar se generó un esquema de conexión para todos los dispositivos de manera que puedan comunicar entre sí y tengan su respectiva alimentación. El diseño y construcción del hardware del prototipo desarrollado en este proyecto ha sido consecuencia de la implementación de estos esquemas electrónicos.

Este diseño se puede observar en el capítulo 3 sección 3.2. Este dispositivo puede estar sujeto a cambios y ampliaciones mientras las tarjetas electrónicas lo permitan, para esto se necesitan realizar cambios en el software.

El desarrollo del software ha buscado realizar la intercomunicación entre todos los elementos con la central telefónica (cámara IP, videoteléfonos IP, Alertas visuales, Alertas Sonoras) y así poder enviar y recibir información en tiempo real para la atención de emergencias.

El sistema se ha ajustado a las necesidades del CSC, sin embargo esta central tiene muchas más prestaciones para las llamadas que podrían ser útiles en otros tipos de proyectos, por lo que se recomienda conocer la potencialidad que esta central es capaz de brindar, además los microcontroladores utilizados no están al 100% de su capacidad lo que permite una ampliación de servicios, procesar información más “pesada” o compleja, además para que la central pueda comunicarse con los elementos en cualquier momento solo es necesario que el servidor de la central telefónica se encuentre activo.

Prestaciones que ofrece la Central
• Crear conferencias. • Contadores de llamadas, facturadores. • Usar distintos canales VoIP. • Transferencia de llamadas. • Grabaciones. • Permite incluye hardware para poder comunicar con teléfonos convencionales y hacer llamadas a operadoras. • Sistemas de fax, email.

Tabla 4.1. *Prestaciones de una central*

Las pruebas de validación funcional del dispositivo para comprobar el funcionamiento del mismo y verificar si todas las necesidades impuestas por el CSC han sido logradas de forma satisfactoria.

Las pruebas de funcionalidad se realizaron en el ambiente en donde va a funcionar (montado en un poste, en un lugar público) para comprobar que opera correctamente. Este dispositivo por disposición del CSC se lo montó en la "plaza del ECU-911", en un poste destinado para pruebas, en donde se pudo comprobar toda la funcionalidad que el dispositivo tiene en una exposición de la explicación y funcionamiento del mismo a todas las autoridades del CSC, incluyendo el encargado del proyecto, el director del CSC y varios analistas del CSC y del ECU-911.

A continuación se presenta el dispositivo final durante las pruebas de validación.

Figura 4.2. *Interior del gabinete principal (estructura 1).*

Figura 4.3. *Montaje del dispositivo en poste*

Se puede apreciar en la figura 4.3 las dos estructuras del proyecto, la primera se encuentra en la parte superior del poste por encima de la protección y la segunda estructura se ubica en la parte inferior a una distancia prudente para la utilización de cualquier usuario (figura 4.4).

Figura 4.4. *Gabinete de cámara (estructura 2)*

El presente proyecto mantiene mejoras sustanciales frente a dispositivos existentes, considerando el ajuste realizado a las necesidades del cantón", (ver capítulo 5) para poder corroborar que se obtuvo como resultado un dispositivo que puede competir en el mercado.

En la parte funcional y servicios el producto resultante del proyecto fue comparado con dos dispositivos los mismos que poseen características similares en funcionalidad y algunas en servicios pudiendo afirmar que cumple con los requerimientos de una competencia internacional.

En la sección de costos se realiza una comparación económica de los beneficios frente a otros dispositivos y se observa la conveniencia de costos y la competitividad en el mercado que manifiesta un ahorro considerable para las empresas que adquieran el producto resultante de este proyecto, todo esto sin minimizar la calidad (ver capítulo 5).

CAPITULO 5. ANÁLISIS ECONÓMICO

5.1. Introducción

El objetivo de la realización de un análisis económico es demostrar que se puede ejecutar el proyecto con los recursos financieros disponibles y obtener réditos económicos.

Primero se realiza una comparación de funcionalidad y servicios frente a dos dispositivos similares y existentes en el mercado para luego presentar el estudio financiero del proyecto en el cual se mostrará el costo-beneficio que se obtiene en la adquisición de este dispositivo.

5.2. Análisis comparativo entre productos

Para la evaluación se consideran cuatro elementos: funcionalidad, tecnología, aspectos comerciales y aspectos estéticos[48]. A continuación se presenta un breve análisis de cada una de las características del producto elaborado en este trabajo.

5.2.1. Función

Aspectos relacionados con el trabajo que va a desempeñar el dispositivo y a la relación con el ser humano.

- Ergonomía. Facilidad de uso del dispositivo.
- Mecanismos. Eficiencia con la que el dispositivo realiza su trabajo.

5.2.2. Tecnología

Se consideran los elementos que posibilitan la realización del dispositivo.

- Materiales. Los materiales utilizados responden a las necesidades de uso, ambientales y productivas.
- Producción. Procesos utilizados en la trasformación de los materiales
- Costos. El aspecto financiero posibilita el lanzamiento de un nuevo producto.

5.2.3. Estética

Se consideran las características formales que comunican tanto el modo de uso como aspectos de índole estrictamente cultural.

- Perceptual. Características formales del dispositivo (color, textura, forma).
- Cultural. Aspectos connotativos de la forma (juvenil, moderno, agresivo).

5.2.4. Comercial

Características que posibilitan o facilitan la venta de un producto.

- Expectativas del usuario. Depende del contexto de uso y de las necesidades del usuario
- Ventas/Distribución. Aspectos del dispositivo que influyen en este proceso (modulación para ahorrar, espacio de transporte, si es desarmable o apilable).

5.2.5. Principales competidores

Los dispositivos a continuación han sido considerados debido a que poseen características similares al prototipo diseñado, los mismos que son:

- Estaciones de Emergencia de la empresa Aiphone Co. (ver capítulo 1 sección 1.5.2)
- 2N Helios IP Force de la empresa 2N Telecommunications.

El dispositivo 2N Helios Force fue considerado por el CSC.

5.2.6. Cuadro comparativo entre productos

	Ward System v1.1 (Prototipo Actual)	**Emergency Station (Aiphone Co)**	**2N Helios Force (2N Telecommunications)**
Función	• El dispositivo realiza con eficiencia el trabajo para el cual fue diseñado. • El dispositivo es de fácil uso. • Escalable en servicios.	• El dispositivo es una estación de emergencia. • No presenta altoparlante. • Dispositivo integrado en una torre.	• Intercomunicador diseñado para abrir cerraduras y accionar conmutadores. • La facilidad de uso de un intercomunicador cualquiera.

	• Alerta Visual y Sonora. • Respaldo de Energía. • Aviso de estado de la energía. • Recepción de una cola de hasta tres llamadas en videoteléfono.	• Limitación de hasta 2 servicios.	• Limitación de hasta 4 conmutadores (4 servicios).
Tecnología	• Los materiales con los que se realizó el dispositivo son de calidad, no contaminan el medio ambiente y de fácil adquisición. • El diseño del dispositivo fue realizado bajo normas de seguridad constructivas y eléctricas.	• Tecnología japonesa de la empresa Aiphone Co. • Cumple con las normas de seguridad funcionales y constructivas.	• Tecnología europea de la empresa 2N Telecommunicatinos expertos en el diseño de intercomunicadores. • Cumple con las normas de seguridad funcionales y constructivas.
Estética	• La construcción e implementación del	• La integración del dispositivo	• Impacto visual reducido del intercomunicador.

	dispositivo en el poste cumple con las normas de protección para los equipos con un mínimo de impacto visual. • El diseño constructivo del mismo es moderno.	en una torre lo hace fácilmente perceptible. • Diseño moderno. • Colores azul, rojo, amarillo, blanco y negro.	• Material anti vandálico. • Diseño moderno.
Comercial	• El dispositivo surge de una respuesta a una necesidad social. • Es fácilmente transportable y montable.	• Dispositivo desarmable. • Fácil transporte.	• Dispositivo de pequeñas dimensiones. • Fácil tranporte.

Tabla 5.1. *Cuadro comparativo entre productos*

5.3. Análisis financiero

Para realizar el análisis financiero primero se considera el sistema divido en dos partes: una acerca del "dispositivo" que se monta en el poste y otra que considera el servidor y los teléfonos IP es decir "la central".

Primero se presentan los costos de los materiales utilizados para la construcción del sistema, es decir el dispositivo más la central, tabla 5.2.

DISPOSITIVO IMPLEMENTADO			
ELEMENTO	**CANTIDAD**	**COSTO UNITARIO**	**COSTO TOTAL**
Altoparlante tipo corneta	1	$ 54,00	$ 54,00
Cámara IP	1	$ 182,00	$ 182,00
Arduino UNO	1	$ 30,00	$ 30,00
Arduino Yún	1	$ 115,00	$ 115,00
Arduino Ethernet Shield	1	$ 30,00	$ 30,00
Inversor	1	$ 66,00	$ 66,00
Cargador Automático de Baterías	1	$ 70,00	$ 70,00
Batería	1	$ 30,00	$ 30,00
Amplificador 20W Lepai	1	$ 56,00	$ 56,00
Luz Estroboscópica	1	$ 25,00	$ 25,00
Lámpara	1	$ 13,00	$ 13,00
Swicth D-Link 5 puertos	1	$ 16,00	$ 16,00
Sensor de Ultrasonido	1	$ 10,00	$ 10,00
RTC DS 1307	1	$ 11,00	$ 11,00
Placa de Relés	1	$ 32,00	$ 32,00
Pulsante industrial	1	$ 5,00	$ 5,00
Caja para poste	1	$ 150,00	$ 150,00
Otros		$ 200,00	$ 200,00
Video Teléfono IP	2	$ 320,00	$ 640,00
Servidor	1	$ 130,00	$ 130,00
TOTAL			**$ 1,865,00**

Tabla 5.2. *Costos dispositivo prototipo*

Para realizar la venta del dispositivo y determinar si es rentable o no como negocio se utilizarán los indicadores de rentabilidad: Tasa Mínima Aceptable de Retorno (TMAR), Tasa Interna de Retorno (TIR) y Valor Actual neto (VAN), para lo cual se

ha realizado una proyección de ventas en un período de tres años, en la tabla 5.3 se puede observar los dispositivos que se esperan vender en el período establecido. Se ha considerado este periodo debido a que el nicho de mercado es reducido y de acuerdo a la zonificación que maneja el CSC. Esta información aún es considerada como reservada, por lo que no se especifica en este trabajo.

Se ha establecido este número de dispositivos ya que el plan piloto del CSC inicia con cinco dispositivos, posteriormente se implementarán diez quedando una totalidad de quince dispositivos en la ciudad, y el análisis ha considerado que se coloquen quince dispositivos en el tercer año en otra ciudad o provincia.

AÑO	NÚMERO DE DISPOSITIVOS
1	5
2	10
3	15

Tabla 5.3. *Proyección de ventas*

La inversión inicial realizada fue para el diseño del software del dispositivo prototipo, es decir la mano de obra, dicha inversión se muestra en la tabla 5.4.

MANO DE OBRA PROTOTIPO	
horas al mes	80
personas	2
meses	3
horas totales	480
costo por hora	$ 5,00

Total	**$ 2,400,00**
COSTOS DE DISEÑO DE PROTOTIPO	
Mano de obra	$ 2,400,00
Equipos	$ 300,00
Total	**$ 2,700,00**

Tabla 5.4. *Costos del diseño del software prototipo*

En la tabla 5.4 se considera el trabajo de dos personas durante tres meses para desarrollar el software del prototipo, además se adiciona el costo de la utilización de equipos en este caso computadores, resultando un total de $2700,00 dólares.

El enfoque de las ganancias se orientará a la venta de la licencia del software. Considerando que la seguridad de la ciudadanía es una obligación del Estado, solo a éste le interesaría este dispositivo, resultando un nicho de mercado reducido y por consiguiente la venta de dispositivos (hardware) no resultaría rentable.

Por esto, se ha considerado tres escenarios con tres precios de venta y así analizar cada uno en busca del más conveniente (ver tabla 5.5).

En este sentido, se estableció que una licencia de software se venda para cinco dispositivos por implementar, es decir en caso de querer implementarse un sexto la empresa debería adquirir nuevamente la licencia.

	DISPOSITIVOS	COSTO 1	COSTO 2	COSTO 3
Licencia de programa	1-5	$ 600,00	$900,00	$1,200,00
	6-10	$ 1,200,00	$1,800,00	$2,400,00
	11-15	$ 1,800,00	$2,700,00	$3,600,00

Tabla 5.5. *Costos de licencia de software*

También se tendrá como ingreso adicional la instalación y mantenimiento del dispositivo, considerando el pago a una tercera persona por el trabajo de instalación, se tendrá (ver tabla 5.6.):

	COSTO	PAGO	SALDO
Mantenimiento por dispositivo	$ 100	$ 80	$ 20
Instalación por dispositivo	$ 70	$ 50	$ 20

Tabla 5.6. *Costos de instalación y mantenimiento*

El primer año el servicio de instalación y mantenimiento no tendrá costo.

En caso de existir la necesidad de reemplazo de equipos adicionales, el respectivo valor se factura a la empresa dueña del equipo.

5.3.1. Indicadores de rentabilidad

Es necesario establecer un parámetro mínimo para definir si la rentabilidad en la posible implementación del proyecto es la adecuada. Así, está la **TMAR (Tasa Mínima Aceptable de Retorno)**.

Inflación anual[13] = 3,67%

Riesgo País[11] = 569,00=5,69%

Tasa de interés pasiva = 5,22%

$$TMAR = i + t + pr \quad (5.1)$$

Donde:

$i = Tasa\ de\ Interés\ pasiva$
$t = Inflación\ anual$
$pr = premio\ al\ riesgo$

$$TMAR = 5{,}22\% + 3{,}67\% + 5{,}69\%$$

$$TMAR = 14{,}58\%$$

Como ya se mencionó, el análisis a realizar considera tres escenarios: Costo1, Costo2 y Costo3 de licencia de software (ver tabla 5.5). A continuación se presenta el análisis de cada escenario.

5.3.1.1. Escenario 1: Costo de Licencia 1

En la tabla 5.7 se observa el cálculo de TIR y VAN para un costo de licencia de $600,00 dólares por cada cinco dispositivos.

Al iniciar el proyecto existe un egreso único considerado como la inversión para diseño del prototipo (tabla 5.4).

[13] A Enero 2014. A la fecha de esta edición, este parámetro aún no fue actualizado por el Banco Central del Ecuador. http://www.bce.fin.ec/index.php/indicadores-economicos

	AÑOS			
INGRESOS	**0**	**1**	**2**	**3**
Ventas dispositivo		$ 5,475.00	$ 10,950.00	$ 16,425.00
Licencia		$ 600.00	$ 1,200.00	$ 1,800.00
Servidor		$ 770.00		
Instalación		$ 0.00	$ 700.00	$ 1,050.00
Mantenimiento		$ 0.00	$ 1,000.00	$ 1,500.00
Total		$ 6,845.00	$ 13,850.00	$ 20,775.00
EGRESOS				
Materia Prima dispositivo		$ 5,475.00	$ 10,950.00	$ 16,425.00
Diseño Prototipo	$ 2,700.00			
Gastos instalación y mantenimiento		$ 650.00	$ 1,300.00	$ 1,950.00
Total	$ 2,700.00	$ 6,125.00	$ 12,250.00	$ 18,375.00
UTILIDAD NETA	-$ 2,700.00	$ 720.00	$ 1,600.00	$ 2,400.00
Tasa de descuento	**10%**			
VAN	**$ 981.83**			
TIR	**28%**			

Tabla 5.7. *Cálculo de TIR y VAN para licencia Costo1*

El ítem considerado como "ventas dispositivo" contiene solo el valor del "dispositivo" ya que también se considera como un ítem llamado "servidor" a los equipos de "la central" (teléfonos IP y servidor). Esto debido a que los dispositivos abarcados en la central se adquieren solo una vez al principio ya que el servidor tiene la capacidad de operar tantos dispositivos como el procesador lo permita[14], es decir se necesita una única central.

[14] http://www.voip-info.org/wiki/view/Asterisk+dimensioning

En la parte de egresos, en materia prima del dispositivo se considera el mismo valor del ítem "venta dispositivo" ya que representa solo el costo de los materiales utilizados.

En el ítem de "Gastos instalación y mantenimiento" se consideran los valores establecidos como "Pago" en la tabla 5.6.

Por tanto, se puede observar el VAN y TIR en la tabla 5.7, que es mayor a cero requisito necesario para que el negocio sea rentable con un costo de licencia de $600,00 dólares.

5.3.1.2. Escenario 2: Costo de Licencia 2

En la tabla 5.8 se considera para el cálculo de VAN y TIR un Costo2 de licencia de $900,00 dólares cada cinco dispositivos.

Se observa que el VAN y TIR presentan una tendencia incremental casi al doble del caso presentado en el Escenario 1 (tabla 5.7).

	AÑOS			
INGRESOS	**0**	**1**	**2**	**3**
Ventas dispositivo		$ 5,475.00	$ 10,950.00	$ 16,425.00
Licencia		$ 900.00	$ 1,800.00	$ 2,700.00
Servidor		$ 770.00		
Instalación		$ 0.00	$ 700.00	$ 1,050.00
Mantenimiento		$ 0.00	$ 1,000.00	$ 1,500.00
Total		$ 7,145.00	$ 14,450.00	$ 21,675.00
EGRESOS				

Materia Prima dispositivo		$ 5,475.00	$ 10,950.00	$ 16,425.00
Diseño Prototipo	$ 2,700.00			
Gastos instalación y mantenimiento		$ 650.00	$ 1,300.00	$ 1,950.00
Total	**$ 2,700.00**	**$ 6,125.00**	**$ 12,250.00**	**$ 18,375.00**
UTILIDAD NETA	-$ 2,700.00	$ 1,020.00	$ 2,200.00	$ 3,300.00
Tasa de descuento	**10%**			
VAN	**$ 2,295.27**			
TIR	**48%**			

Tabla 5.8. *Cálculo de TIR y VAN para licencia Costo2*

5.3.1.3. Escenario 3: Costo de Licencia 3

En la tabla 5.9 se considera para el cálculo de VAN y TIR un Costo3 de licencia de $1200,00 dólares para la operación de cinco dispositivos.

Se observa que el VAN y TIR presentan una tendencia incremental del caso presentado en el Escenario 2 (tabla 5.8).

	AÑOS			
INGRESOS	**0**	**1**	**2**	**3**
Ventas dispositivo		$ 5,475.00	$ 10,950.00	$ 16,425.00
Licencia		$ 1,200.00	$ 2,400.00	$ 3,600.00
Servidor		$ 770.00		
Instalación		$ 0.00	$ 700.00	$ 1,050.00
Mantenimiento		$ 0.00	$ 1,000.00	$ 1,500.00
Total		$ 7,445.00	$ 15,050.00	$ 22,575.00

EGRESOS				
Materia Prima dispositivo		$ 5,475.00	$ 10,950.00	$ 16,425.00
Diseño Prototipo	$ 2,700.00			
Gastos instalación y mantenimiento		$ 650.00	$ 1,300.00	$ 1,950.00
Total	$ 2,700.00	$ 6,125.00	$ 12,250.00	$ 18,375.00
UTILIDAD NETA	-$ 2,700.00	$ 1,320.00	$ 2,800.00	$ 4,200.00
Tasa de descuento	**10%**			
VAN	**$ 3,608.70**			
TIR	**67%**			

Tabla 5.9. *Cálculo de TIR y VAN para licencia Costo3*

Como se puede observar en los tres escenarios el VAN es mayor a cero requisito necesario para que el negocio sea rentable. El TIR obtenido es considerado como la tasa de interés máxima a la que se puede endeudar para financiar el proyecto obteniendo para cada caso un TIR de 28%, 48% y 67% respectivamente que igual al VAN manifiesta rentabilidad.

Además, para que un proyecto sea aceptado se debe satisfacer la siguiente desigualdad.

$$TIR \geq TMAR$$

TMAR=14,58%

TIR 1= 28%

TIR 2= 48%

TIR 3= 67%

Por lo que el proyecto puede ser aceptado sin problema alguno.

5.3.2. Análisis de ganancias

Para determinar cuánto de ganancia se obtiene, primero se necesita conocer el valor de la licencia por dispositivo para lo cual se realiza lo siguiente:

$$\frac{\$2{,}700{,}00}{30\ dispositivos} = \$90{,}00 \tag{5.2}$$

Los $2,700,00 dólares es el valor del diseño del software y se consideran 30 dispositivos que es la totalidad a vender en los tres años, obteniendo un costo de diseño de software por dispositivo de $90,00 dólares.

Dispositivos	Costo de Diseño	Costo de Licencia	Ganancia	Porcentaje de Ganancia
5	$ 450.00	$ 600.00	$ 150.00	33%
		$ 900.00	$ 450.00	100%
		$ 1,200.00	$ 750.00	167%

Tabla 5.10. *Porcentaje de Ganancia*

En la tabla 5.10 se presenta el porcentaje de ganancia considerando los tres escenarios de venta del software ($600,00; $900,00 y $1200,00 dólares).

Primero se determina que los cinco dispositivos tienen un valor de diseño de software de $450,00 dólares. En el escenario 1 ($600,00 dólares) se obtiene un porcentaje de ganancia de 33%. En el escenario 2 ($900,00 dólares) se obtiene un porcentaje de ganancia de 100%. En el escenario 3 ($1200,00 dólares) se obtiene un porcentaje de

ganancia de 167%, determinando que en los tres escenarios resultaría rentable la ejecución de este proyecto.

Como se pudo ver en la tabla 5.6 las ganancias obtenidas por la instalación, el mantenimiento y la venta del dispositivo no representan mayor ganancia por lo que es importante establecer un costo a la licencia de software para obtener réditos económicos.

La rentabilidad de la venta de estos dispositivos radica en la demanda que exista de los mismos, para este caso hemos considerado los dispositivos que el CSC pretende implementar en la ciudad y la posible ejecución de este proyecto en otras ciudades en un período de tres años.

5.3.3. Comparación financiera entre dispositivos

Esta subsección pretende establecer y mostrar que la implementación de este sistema (WARD SYSTEM) puede competir en el mercado internacional.

Para realizar esta comparación primero se presentan en la tabla 5.11 y 5.12 los costos de cada dispositivo.

DISPOSITIVO 2 (2N Helios Force)			
ELEMENTO	**CANTIDAD**	**COSTO UNITARIO**	**COSTO TOTAL**
Intercomunicador	1	$ 1470,00	$ 1470,00
Video Teléfono IP	2	$ 320,00	$ 640,00
Altoparlante tipo corneta	1	$ 54,00	$ 54,00
Amplificador 20W Lepai	1	$ 56,00	$ 56,00

Inversor	1	$ 66,00	$ 66,00
Cargador Automático de Baterías	1	$ 70,00	$ 70,00
Batería	1	$ 30,00	$ 30,00
Luz Estroboscópica	1	$ 25,00	$ 25,00
Lámpara	1	$ 13,00	$ 13,00
Sensor de Ultrasonido	1	$ 10,00	$ 10,00
RTC DS 1307	1	$ 11,00	$ 11,00
Swicth D-Link 5 puertos	1	$ 16,00	$ 16,00
Placa de Relés	1	$ 32,00	$ 32,00
Caja para poste	1	$ 150,00	$ 150,00
Otros		$ 200,00	$ 200,00
		TOTAL	**$ 2,843,00**

Tabla 5.11. *Costo dispositivo 2N Helios Force (2N Telecommunications)*

DISPOSITIVO 3 (Emergency Station)			
ELEMENTO	**CANTIDAD**	**COSTO UNITARIO**	**COSTO TOTAL**
Intercomunicador	1	$ 920,00	$ 920,00
Video Teléfono IP	2	$ 725,00	$ 1,450,00
Altoparlante tipo corneta	1	$ 54,00	$ 54,00
Amplificador 20W Lepai	1	$ 56,00	$ 56,00
Inversor	1	$ 66,00	$ 66,00
Cargador Automático de Baterías	1	$ 70,00	$ 70,00
Batería	1	$ 30,00	$ 30,00
Luz Estroboscópica	1	$ 25,00	$ 25,00
Lámpara	1	$ 13,00	$ 13,00
Sensor de Ultrasonido	1	$ 10,00	$ 10,00
RTC DS 1307	1	$ 11,00	$ 11,00
Swicth D-Link 5 puertos	1	$ 16,00	$ 16,00

Placa de Relés	1	$ 32,00	$ 32,00
Caja para poste	1	$ 150,00	$ 150,00
Otros		$ 200,00	$ 200,00
TOTAL			**$ 3,103,00**

Tabla 5.12. *Costo dispositivo Emergency Station (Aiphone Co)*

A continuación se presenta tres cuadros comparativos de los costos del dispositivo diseñado frente a los dos dispositivos similares ya existentes en el mercado, se considerará los tres escenarios para la venta de la licencia de software establecidos: Costo1 ($600,00), Costo2 ($900,00) y Costo3 ($1200,00).

Se puede observar la diferencia de costos y el ahorro que le representaría al CSC el adquirir uno, cinco o quince dispositivos.

	Ahorro de la Empresa (Costo1)		
	Costo de 1 dispositivo	**Costo de 5 dispositivos**	**Costo de 15 dispositivos**
Dispositivo 1	$ 2,465,00	$ 6,845,00	$ 18,995,00
Dispositivo 2	$ 2,843,00	$ 14,215,00	$ 42,645,00
Dispositivo 3	$ 3,103,00	$ 15,515,00	$ 46,545,00
Ahorro con respecto al dispositivo 2	$ 378,00	$ 7,370,00	$ 23,650,00
Ahorro con respecto al dispositivo 3	$ 638,00	$ 8,670,00	$ 27,550,00

Tabla 5.13. *Cuadro comparativo de costos entre dispositivos Escenario 1*

	Ahorro de la Empresa (Costo2)		
	Costo de 1 dispositivo	**Costo de 5 dispositivos**	**Costo de 15 dispositivos**
Dispositivo 1	$ 2,765,00	$ 7,145,00	$ 19,895,00
Dispositivo 2	$ 2,843,00	$ 14,215,00	$ 42,645,00
Dispositivo 3	$ 3,103,00	$ 15,515,00	$ 46,545,00
Ahorro con respecto al dispositivo 2	$ 78,00	$ 7,070,00	$ 22,750,00
Ahorro con respecto al dispositivo 3	$ 338,00	$ 8,370,00	$ 26,650,00

Tabla 5.14. *Cuadro comparativo de costos entre dispositivos Escenario 2*

	Ahorro de la Empresa (Costo3)		
	Costo de 1 dispositivo	**Costo de 5 dispositivos**	**Costo de 15 dispositivos**
Dispositivo 1	$ 3,065,00	$ 7,445,00	$ 20,795,00
Dispositivo 2	$ 2,843,00	$ 14,215,00	$ 42,645,00
Dispositivo 3	$ 3,103,00	$ 15,515,00	$ 46,545,00
Ahorro con respecto al dispositivo 2	-$ 222,00	$ 6,770,00	$ 21,850,00
Ahorro con respecto al dispositivo 3	$ 38,00	$ 8,070,00	$ 25,750,00

Tabla 5.15. *Cuadro comparativo de costos entre dispositivos Escenario 3*

Como se puede observar en las tablas 13, 14 y 15 el ahorro que le significa a la Institución en este caso el Consejo de Seguridad Ciudadana CSC es considerable al adquirir de cinco a quince dispositivos frente a la utilización de otras tecnologías.

En cualquiera de los casos el ahorro se ve, por lo que se podría establecer un costo de licencia de hasta $1,200,00 pero por ser un proyecto social se ha considerado como el costo más óptimo para la licencia de software de $900,00 dólares.

Se considera $900,00 dólares de la licencia de software ya que es el único ítem considerado que representa una ganancia, esta no está ni en la venta del dispositivo ni en la instalación y mantenimiento.

CAPITULO 6. CONCLUSIONES Y RECOMENDACIONES

El proyecto planteado propone colaborar con la seguridad de las personas en lugares públicos que es uno de los grandes problemas en la ciudad. Al tener botones de auxilio o de "pánico", a los que la gente puede acudir en caso de emergencia se ganara una respuesta inmediata de las autoridades e instituciones de auxilio en lugares en donde no se tenía fácil acceso a este como son los parques; sin embargo no se puede cuantificar la ayuda que este dispositivo puede brindar ya que estos dispositivos están por ser probados para la ciudadanía.

Al momento de elegir los elementos a utilizar, se debe tener en cuenta que en el mercado existen muchos dispositivos que realizan funciones complejas a bajo costo como el "Arduino Ethernet Shield" que nos permite la administración de los puertos de su microcontrolador vía IP. Esto simplifica la implementación pues así no se programa todo el protocolo, ahorrando tiempo y costos en el desarrollo.

La selección de los diferentes dispositivos a implementar en el proyecto depende de factores externos al proyecto además de que cumplan con las necesidades del mismo. En este sentido, los factores externos como su existencia en stock en el país o la diferencia de calidad entre una marca u otra, etc. pueden inferir de forma directa en los costos del proyecto, siendo esto en muchos casos determinante para la producción en serie, claro está luego del respectivo análisis económico y operativo.

Como el dispositivo tiene que estar expuesto a la intemperie, este debe tener protecciones contra factores climáticos y vandalismo. La estructura que aloja el sistema debe mantener la robustez necesaria que demande el medio ambiente en el que se emplee, sin embargo como el poste de prueba donde fue montado el dispositivo no puede ser dañado, es decir no puede tener perforaciones ni sueldas, la protección se limita bastante y se ha decidido utilizar solo cintas "Eriband" para el montaje.

Con investigación se ha logrado conseguir dispositivos que pueden intercomunicarse entre sí de manera sencilla, por esto es importante que se tenga claras todas las necesidades del proyecto antes de diseñar el hardware y poder optimizar este diseño con los dispositivos correctos para el fin pertinente.

En lo que respecta a la programación de los microcontroladores usada, existen muchas y diversas maneras de hacerlo y así alcanzar un objetivo específico. Sin embargo para este proyecto la mejor vía resulto establecer qué fines específicos se requieren y buscar ejemplos realizados ya que existe gran cantidad de información en la red, y alguna esta simplificada y en librerías; al usar este apoyo el trabajo se puede simplificar considerablemente.

Cuando se comunica el Arduino con los archivos AGI del servidor de Elastix, estos necesitan los permisos necesarios, si un archivo AGI no tiene permisos de ejecución para el usuario administrador de la centralita, estos archivos nunca funcionan y no se van a comunicar con el Arduino.

Al llevar a la práctica una simulación no todos los servicios funcionan a la perfección debido a que los dispositivos en ocasiones no soportan protocolos que los simuladores sí. Por ejemplo el videoteléfono trasmite correctamente el protocolo de vídeo H.264 pero tiene problemas con el MJPEG, error que en las simulaciones no ocurrió. Lo que indica que es necesario asegurarse de los formatos que soporta cada dispositivo en la práctica y bajo que modos de funcionamiento lo hacen.

Para interconectar teléfonos IP, cámaras y otros dispositivos IP con un servidor se debe tener en cuenta que utilicen los mismos protocolos de voz o vídeo, caso contrario no se podría transmitir la información deseada.

Existe una variedad de posibles configuraciones y servicios que el servidor de Elastix nos brinda para telefonía IP, para poder obtener el mayor provecho es recomendable que se tengan en cuenta los servicios que tiene, como grabador de voz, facturador, estadísticas, fax, email, entre otros.

A pesar de que los elementos que energizan a los dispositivos permiten el flujo de la suficiente corriente, estos se calientan considerablemente por lo que se recomienda el uso de ventiladores para evitar cualquier inconveniente. Es decir que es necesario analizar y considerar los rangos máximos de operación de cada dispositivo a usar, así como las condiciones ambientales para conseguir un óptimo funcionamiento.

Existe una amplia variedad de cámaras disponibles en el mercado que tienen varias funcionalidades extras en diferentes marcas, dependiendo de estas se puede mejorar el desempeño del dispositivo, por esto se recomienda el uso de cámaras que permitan accionar señales de alarma mediante un puerto de entrada, ya que gracias a esto se podrían realizar llamadas por medio del protocolo SIP, y así al presionar el pulsante de emergencia se llamaría directamente a la central de emergencias sin necesidad de hacer un llamada de vuelta como está realizado en este proyecto, minimizando algunos segundos vitales para establecer la comunicación.

Al montar los dispositivos al poste, por más que esté protegido con cintas o soldados, estos quedan relativamente inseguros ya que la cámara que se instala es costosa y puede convertirse en un objetivo para delincuentes, por esto se recomienda que se cree una estructura propia para los dispositivos en donde su base nazca desde la acera y la estructura encierre a todo el dispositivo y así además de proteger a todos los elementos se tendrá una zona exclusiva para esta atención de emergencias denominada “punto seguro”.

Toda la gestión que se está realizando desde un videoteléfono IP para controlar a los dispositivos remotamente mediante la central telefónica Elastix, podría ser

reemplazada por un servidor Web, en donde desde un navegador web, se gestione el dispositivo y la cámara. Este es otro método de realizar el mismo tipo de control y comunicación que se requiere, sin embargo cada uno presenta ventajas y desventajas, por ejemplo en el caso de usar un servidor web necesariamente se requiere tener una PC para administrar los dispositivos no así directamente con teléfonos IP pero la interfaz de administración puede ser más cómoda, amigable y tener control sobre varios puntos, además de permitir el uso de mejores códecs de vídeo que se encarga de resolver el problema para diversos tipos de cámaras IP. Esta puede ser una buena opción en caso de tener más elementos para administrar y si se dispone de un computador para este fin.

En lo que respecta al análisis económico, se recomienda a futuro realizar una reinversión para mejoras tanto del dispositivo como del software y ofrecer mayor calidad y eficiencia al sistema. En este mismo campo es necesario recordar que análisis de diversos escenarios permite mejorar el proceso de la toma de decisiones para establecer un negocio adecuado.

Finalmente, se recomienda ampliar los conocimientos exclusivos a la parte ingenieril como tal, ya que para lograr un proyecto con calidad y eficiencia no se puede basar tan solo en la parte técnica, sino se debe conocer, para este proyecto por ejemplo, de economía, mercadeo, publicidad, sociología, seguridad, mecánica, entre otros, es decir, un proyecto multidisciplinario. Así, con conocimiento de diversos temas como los mencionados, se puede generar un trabajo mucho más consistente y elaborado con una base sólida en cada parámetro que se podría necesitar. Como éste es multidisciplinario, en caso de implementarlo a gran escala sería necesario contratar a gente especializada en cada tema, sin embargo como administradores del mismo es pertinente conocer de qué se trata cada tema y así estar al tanto de todo su proceso, independiente de no ser puramente temas de ingeniería.

APÉNDICES

APÉNDICE A

En está apéndice que muestran los diagramas de flujo de los programas requeridos en este proyecto.

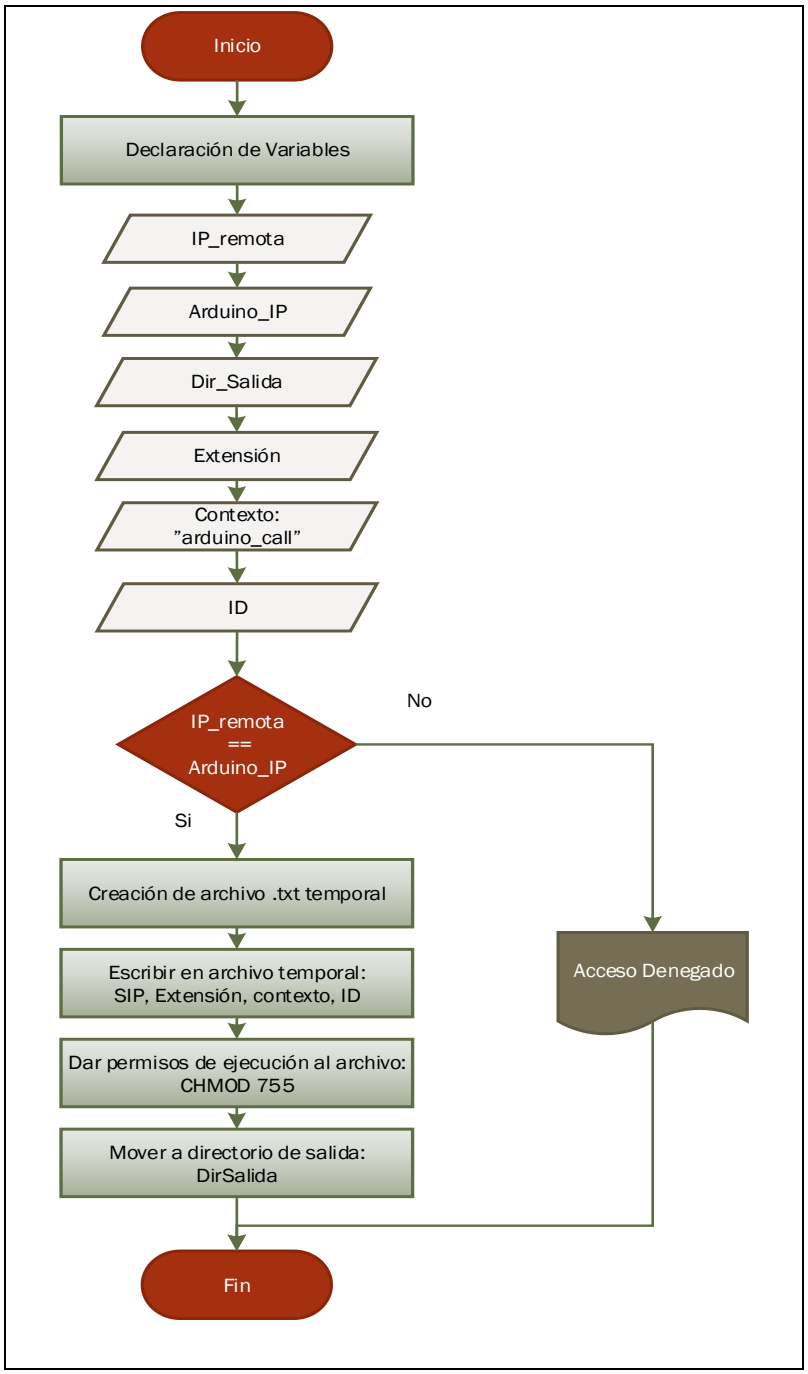


Diagrama de Flujo 1. *"arduino_call.php"*

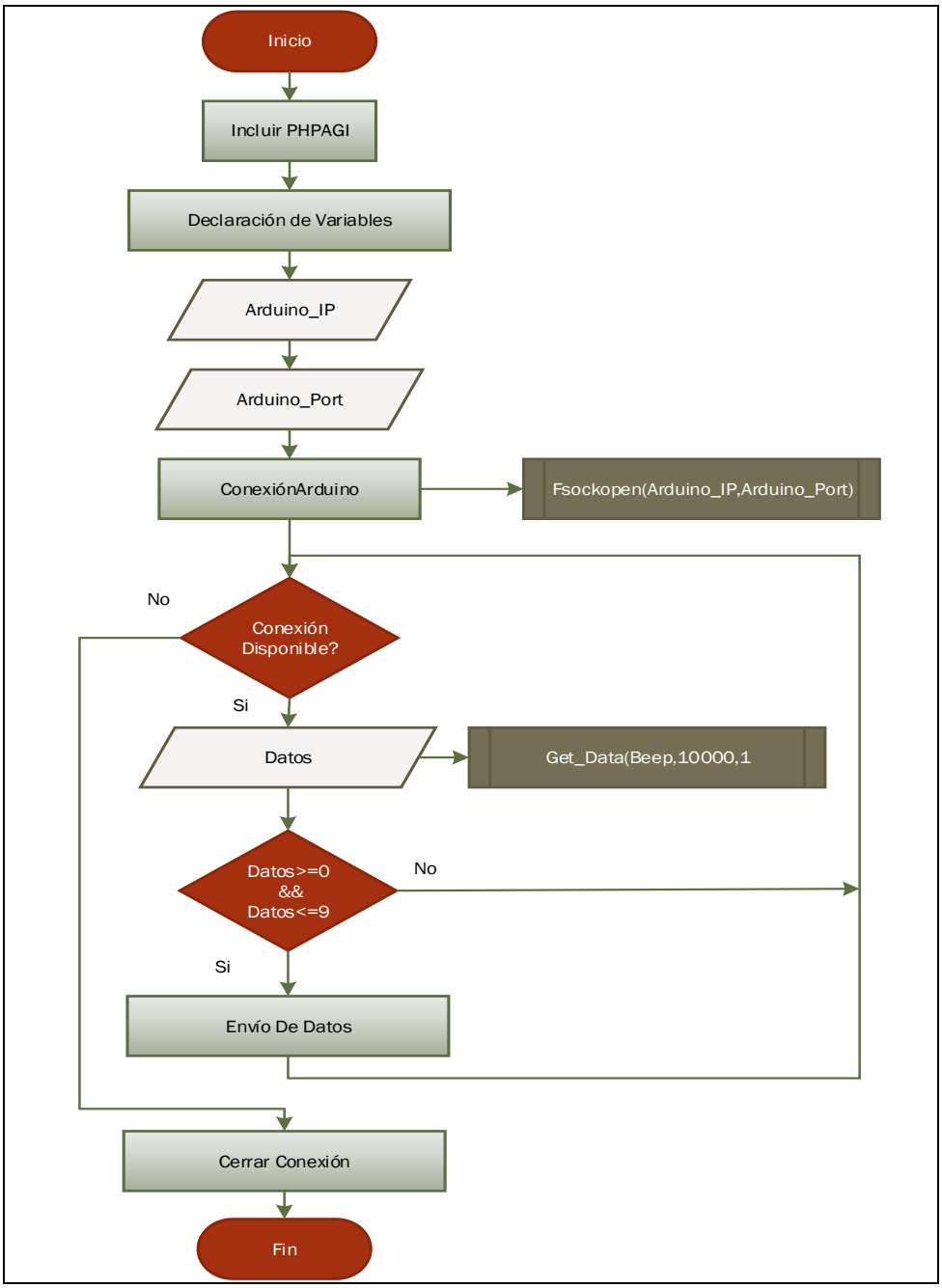
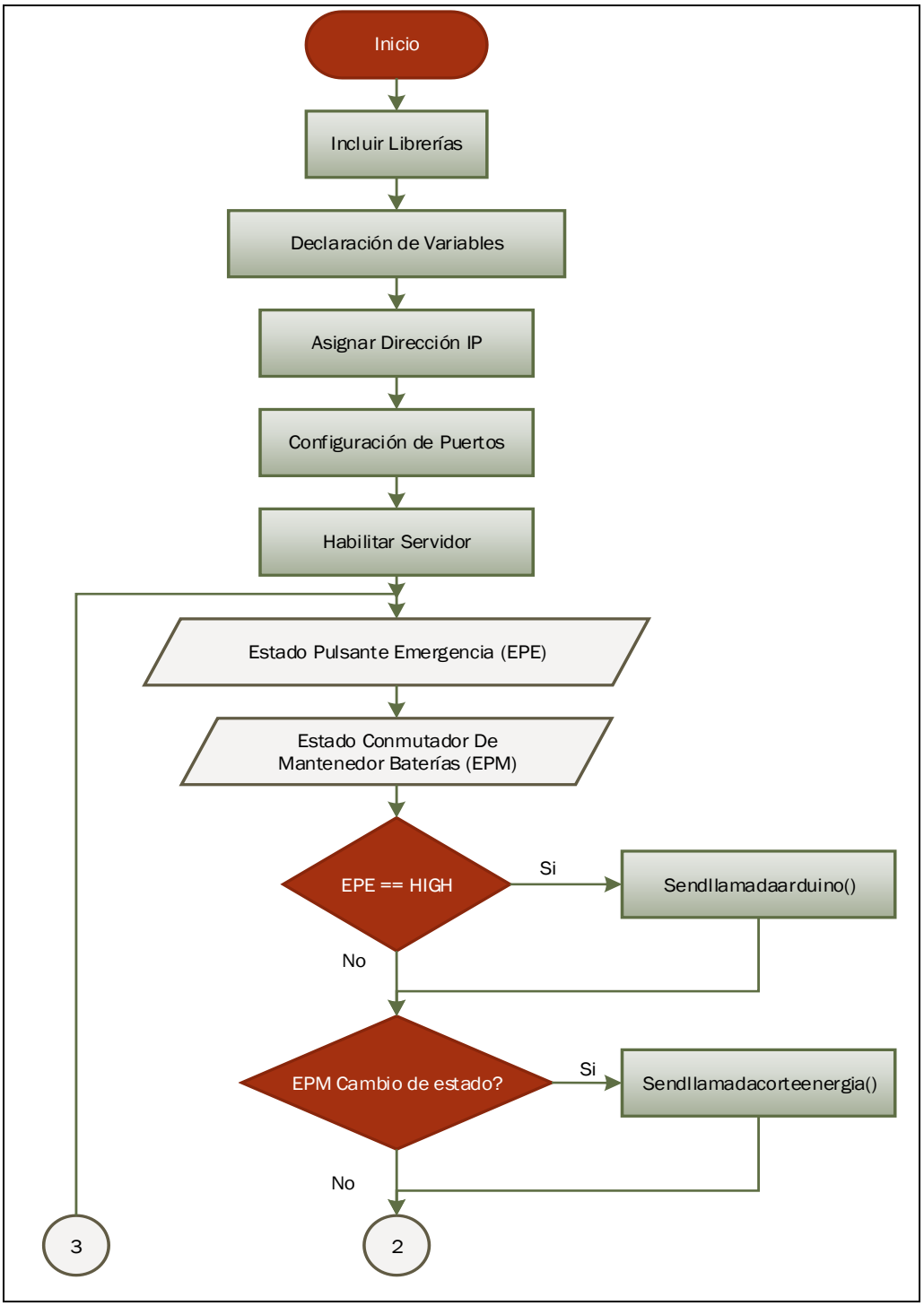


Diagrama de Flujo 2. *"codigo_arduino.php"*


Inicio
Incluir Librerías
Declaración de Variables
Asignar Dirección IP
Configuración de Puertos
Habilitar Servidor
Estado Pulsante Emergencia (EPE)
Estado Conmutador De Mantenedor Baterías (EPM)
EPE == HIGH
Si
SendllamadaarduinO()
No
EPM Cambio de estado?
Si
SendllamadacorteenergiA()
No
3
2

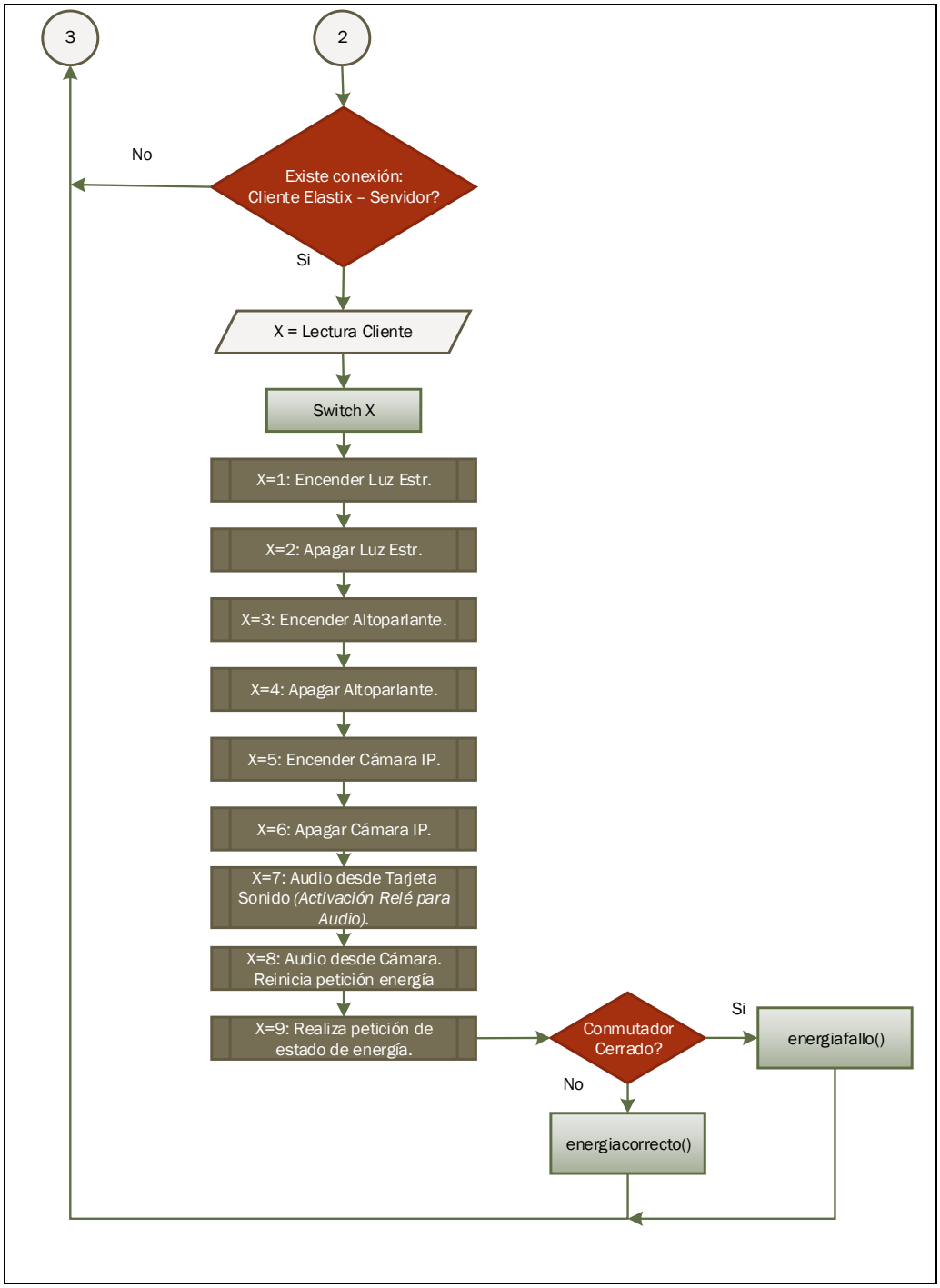
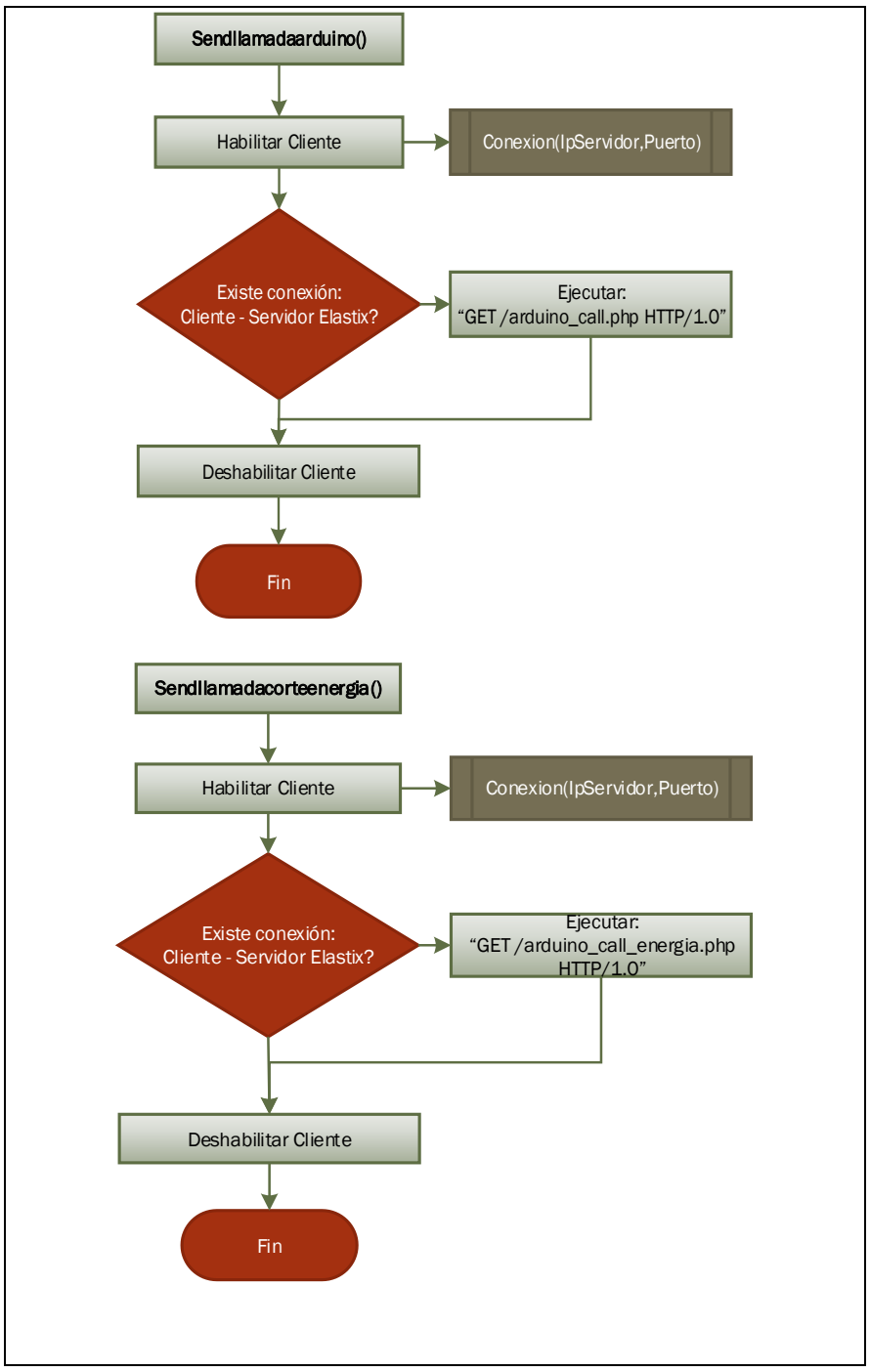


Diagrama de Flujo 3. *"ClienteYServidor.ino"*


SendllamadaarduinO()
Habilitar Cliente
Conexion(IpServidor,Puerto)
Existe conexión:
Cliente - Servidor Elastix?
Ejecutar:
“GET /arduino_call.php HTTP/1.0”
Deshabilitar Cliente
Fin
SendllamadacorteenergiA()
Habilitar Cliente
Conexion(IpServidor,Puerto)
Existe conexión:
Cliente - Servidor Elastix?
Ejecutar:
“GET /arduino_call_energia.php
HTTP/1.0”
Deshabilitar Cliente
Fin

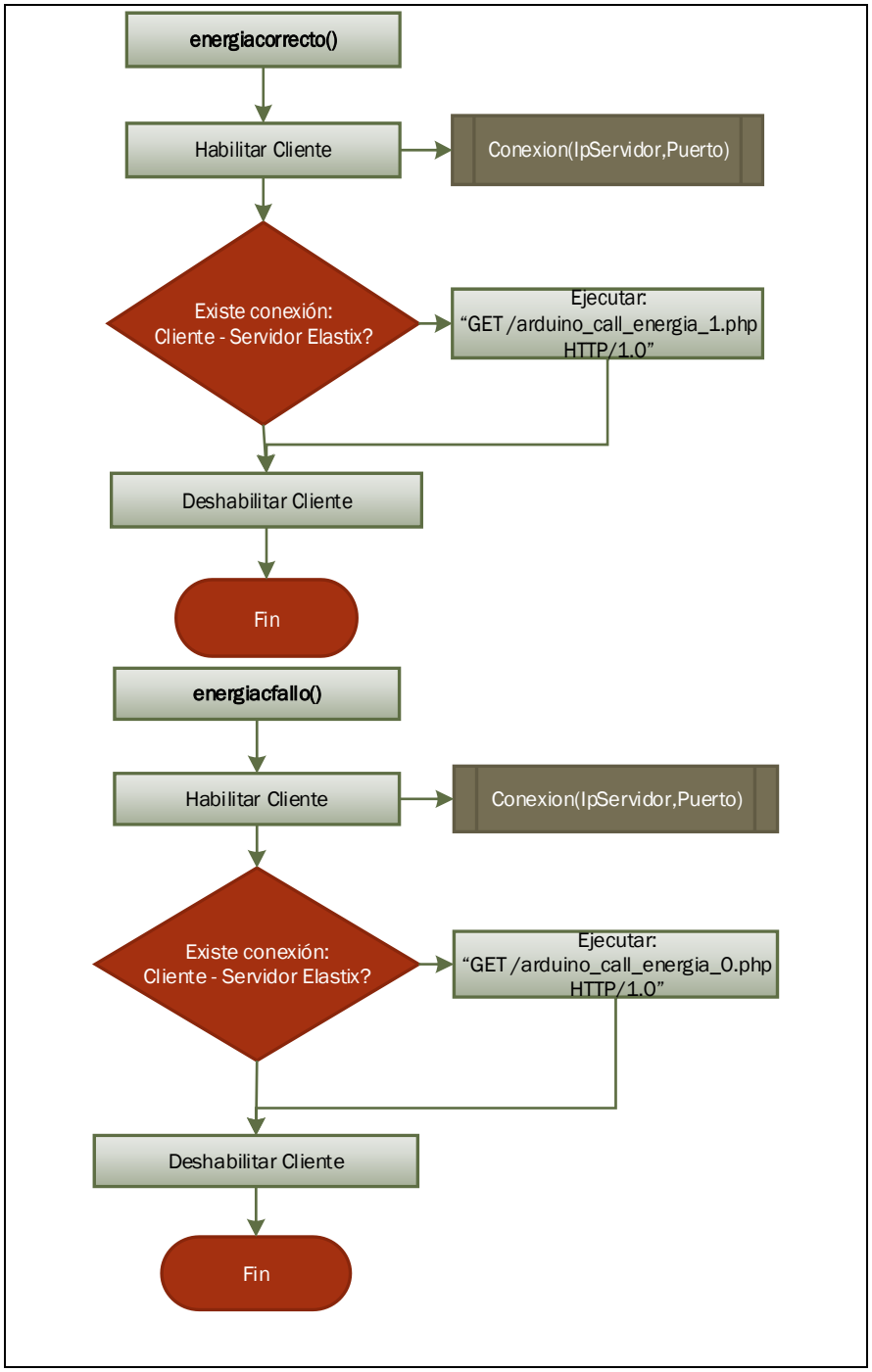


Diagrama de Flujo 4. *“ClienteYServidor.ino”*

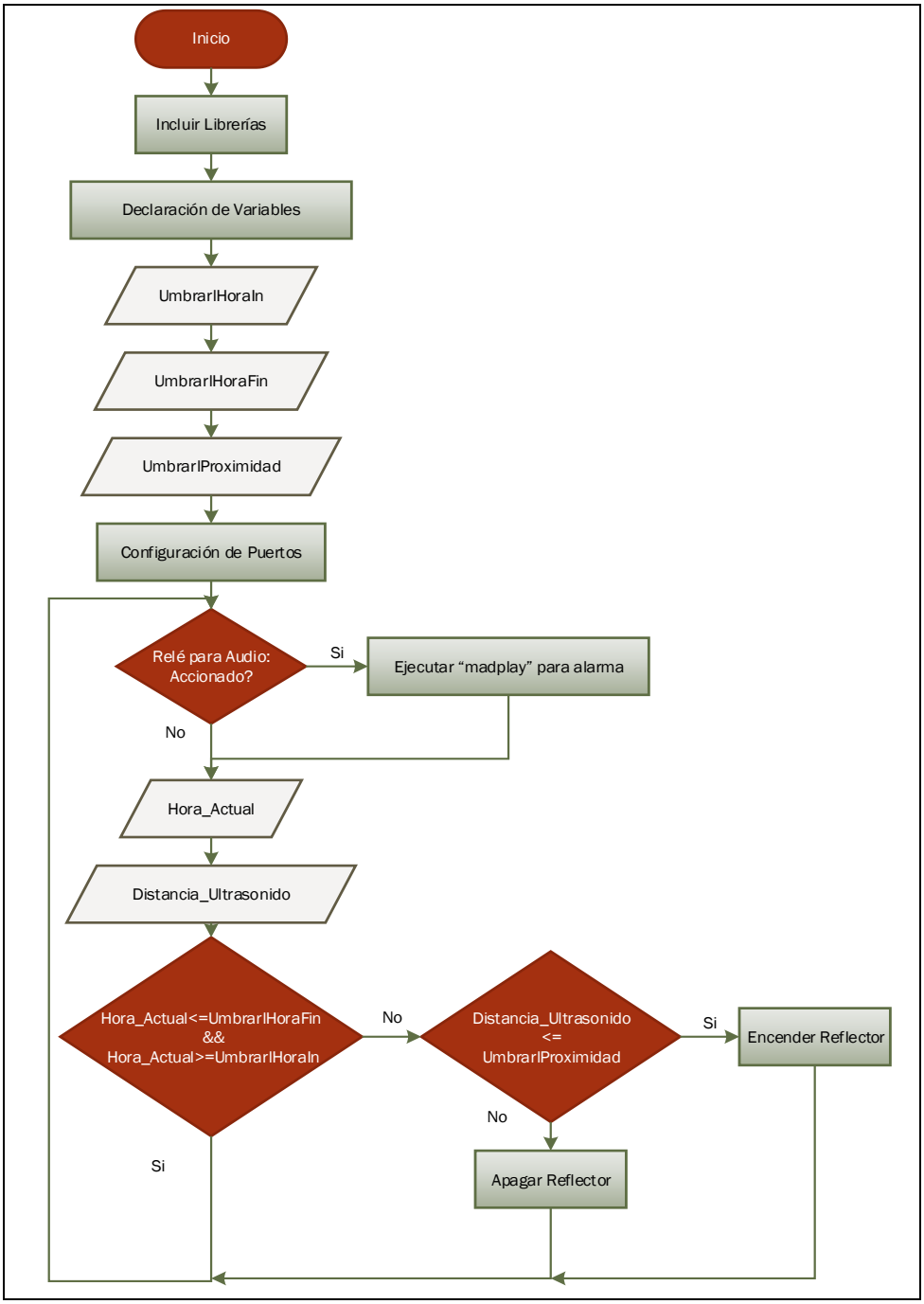


Diagrama de Flujo 5. *"LuminariaYAlarma.ino"*

APÉNDICE B

En el presente apéndice que muestra el manual para el operario del sistema.

MANUAL DE OPERARIO.

Para la atención de emergencias se cuenta con dos videoteléfonos IP:

- Videoteléfono 1: Extensión “200”.
- Videoteléfono 2: Extensión “300”.
- Grupo de llamadas (Extensión 200 y 300): Extensión “250”.

En caso de desear llamar a la cámara IP para intercomunicarse con el solicitante o con el administrador de dispositivos, únicamente marcar sus números de extensión:

- Administrador de dispositivos (Arduino): Extensión “100”.
- Cámara IP: Extensión “150”.

Cuando se desea administrar los dispositivos, al marcar su extensión (100 en este caso), se abrirá una comunicación entre el teléfono y el administrador, permitiéndonos marcar cualquier número del uno al nueve. A continuación la lista de que maneja cada número:

1. Enciende la luz estroboscópica.
2. Apaga la luz estroboscópica.
3. Enciende el altoparlante.
4. Apaga al altoparlante.
5. Enciende la cámara IP.
6. Apaga la cámara IP.
7. Conmuta la señal de audio desde la tarjeta de sonido hacia el altoparlante.
8. Conmuta la señal de audio desde la cámara hacia el altoparlante y reinicia petición de estado de energía.
9. Realiza una petición del estado de energía.

BIBLIOGRAFIA

[1] C. Pérez, “Redes de Telecomunicaciones y de Datos.”

[2] AXIS Communications, “Las redes IP : Conceptos básicos,” 2002.

[3] E. Taylor, *The McGraw-Hill Internetworking Handbook*, 2nd ed. New York, NY, USA.

[4] A. Amaguaña and F. Cardenas, “Estudio y Diseño del sistema de seguridad por videovigilancia IP para el Hospital de Brigada No. 11 Galápagos.,” 2009.

[5] AXIS Communications, “Guía técnica de vídeo IP,” .

[6] R. Gould, “Comparative Power-Over-Ethernet (PoE) Testing Between Category 6A and Category 5e Cables,” pp. 1–6.

[7] Texas Instruments, “LM5072 Integrated 100V Power Over Ethernet PD Interface and PWM Controller with Aux Support,” no. March 2006, 2013.

[8] A. D. Nogueiras, “Apéndice A Clasificación y Análisis de los Convertidores Conmutados PWM,” 2003.

[9] T. Matínez, “Redes GPON, las nuevas redes de operador,” 2013. [Online]. Available: http://www.telequismo.com/2013/02/gpon-operador.html.

[10] Union International Telecommunication, “Gigabit-capable passive optical networks (GPON): General characterisitcs,” 2008.

[11] CTDI, “U9264H GPON/GEPON OLT,” pp. 1–4, 2011.

[12] Huawei, “HG8447 Home Gateway,” 2011.

[13] Ericsson, “T720G MDU ONU,” 2010.

[14] FOS Series, “Versatile optical splitters for a wide range of fiber-based applications,” p. 185.

[15] N. J. Lippis, “GPON vs. Gigabit Ethernet in Campus Networking,” 2012.

[16] M. Paz and A. Erazo, “DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD POR VIDEOVIGILANCIA IP Y CONTROL DEL SISTEMA DE ILUMINACIÓN PARA LA JEFATURA DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD - UNIDAD DE POSGRADOS DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO EXTENSIÓN LATACUN,” 2011.

[17] AXIS Communications, “Cámaras de Red,” 2013. [Online]. Available: http://www.axis.com/es/products/video/camera/index.htm.

[18] O. I. Ogunyinka, “Security Surveillance Architecture : The Wireless Mesh Network Approach,” *Mediterr. J. Soc. Sci.*, vol. 2, no. November, pp. 59–66, 2011.

[19] Real Academia Española, “videovigilancia.” [Online]. Available: http://buscon.rae.es/drae/?type=3&val=videovigilancia&val_aux=&origen=REDRAE.

[20] C. Nicolás Fraile, “Adiós a los Postes SOS,” *Tráfico y Segur. Vial*, vol. 205, pp. 21–22, 2011.

[21] 2N Telecommunications, “2N Helios IP Safety,” 2012. [Online]. Available: http://www.2n.cz/es/productos/sistemas-de-intercomunicacion/intercomunicadores-ip/helios-ip-safety/por-proyectante/#product-content.

[22] Aiphone, “Rescue Assistance,” 2012. [Online]. Available: http://www.aiphone.com/home/products/rescue-assistance/.

[23] Ermes Freedom to communicate, “CityHELP.” [Online]. Available: http://www.ermes-cctv.com/CityHELP-it.htm.

[24] Maitrise Technologique, “MT A89,” 2012. [Online]. Available: http://www.maitrise-technologique.com/actualites/mt-realise-le-reseau-dappel-durgence-de-lautoroute-a89-2/.

[25] S. Osorio Herrera, “DISEÑO E IMPLEMENTACIÓN DEL SISTEMA VOIP DE LA EMPRESA CMSA Y SUS SEDES,” UNIVERSIDAD DEL SINU. ESPECIALIZACION DE REDES Y TELECOMUNICACIONES., 2012.

[26] AECT Association for Educational Communications and Technology, “Protocolo SIP Session Initiation Protocol,” 2013.

[27] Quarea Voz Datos IP, “¿Que es una Centralita IP? - Central Telefónica VoIP - IP-PBX,” 2014. [Online]. Available: http://www.quarea.com/es/que_es_una_centralita_ip_central_telefonica_voip_ip_pbx. [Accessed: 03-Oct-2014].

[28] E. Landívar, “Comunicaciones Unificadas con Elastix,” vol. 1, 2008.

[29] Digium The Asterisk Company, “About Digium,” 2014. [Online]. Available: http://www.digium.com/en/company.

[30] elastix Freedom to Communicate, “Elastix Overview,” 2014. [Online]. Available: http://elastix.org/index.php/en/product-information/elastix-info.html.

[31] C. Cabrera, “Asterisk vs Elastix vs Trixbox vs AsteriskNow vs FreePBX: Explicando la diferencia,” 2013. [Online]. Available: Asterisk vs Elastix vs Trixbox vs AsteriskNow vs FreePBX: Explicando la diferencia. [Accessed: 13-Oct-2014].

[32] Voip-Info.org, “Asterisk Dialplan Commands,” 2014. [Online]. Available: http://www.voip-info.org/wiki/view/Asterisk+-+documentation+of+application+commands.

[33] Grandstream, “GXV3615WP _ HD Especificaciones Técnicas.”

[34] ITU, “Informe esencial sobre telefonía por el protocolo Internet (IP).”

[35] Grandstream, “GXV3175v2 Teléfono IP Multimedia,” 2013.

[36] People Electric, “Lightings.”

[37] VANTO Industrial Electric, “Rotator Warning Light,” 2014. [Online]. Available: http://www.vantoele.com/products/Rotator-Warning-Light-460.html.

[38] Pyle, “6'' Indoor / Outdoor 50 Watts PA Horn Speaker,” 2014. [Online]. Available: http://www.pyleaudio.com/sku/PHSP4/6-Indoor--Outdoor-50-Watts-PA-Horn-Speaker.

[39] Lepai, “LP-2020A+ Lepai Tripath Class.” [Online]. Available: http://www.lepai.us/amplifier-lepai-lp-2020a.html.

[40] Creative, “Sound Blaster X-Fi Go! Pro,” 2014. [Online]. Available: http://us.creative.com/p/sound-blaster/sound-blaster-x-fi-go-pro. [Accessed: 28-Oct-2014].

[41] Cybercursos, “Switches y Ruteadores.” [Online]. Available: http://www.redes-linux.com/manuales/Tecnologia_redes/switchesyruteadores.pdf. [Accessed: 17-Sep-2014].

[42] D-Link, “8-Port 10/100 Switch,” 2010.

[43] Arduino, “Arduino Yún,” 2014.

[44] OpenWrt, “OpenWrt Wireless Freedom,” 2014. [Online]. Available: https://openwrt.org/.

[45] Arduino, “Arduino Uno,” 2014. [Online]. Available: http://arduino.cc/en/pmwiki.php?n=Main/ArduinoBoardUno.

[46] Arduino, “Arduino Ethernet Shield,” 2014. [Online]. Available: http://arduino.cc/en/Main/ArduinoEthernetShield.

[47] Dallas Semiconductor, “DS1307 64 x 8 Serial Real-Time Clock.”

[48] ELEC Freaks, “Ultrasonic Ranging Module HC - SR04.”

[49] Kutai, “Cargador de Batería Automático.” [Online]. Available: http://es.powergensetpart.com/buy_2.5-Kutai-AVR-EA63.

[50] Power Kingdom, “PS Series,” 2014. [Online]. Available: http://www.powerkingdom.com.cn/power/product_view.asp.

[51] Black+Decker, “2-IN-1 AUTOMOTIVE POWER SUPPLY,” 2014. [Online]. Available: http://www.blackanddecker.com/power-tools/PI500BB.aspx.

[52] digiMAD, “Servicios.” [Online]. Available: http://www.digimad.es/h261-h263-h264-codecs-video.html.

[53] J. Joskowicz, “CODIFICACION DE VOZ Y VIDEO,” pp. 1–39, 2013.

[54] P. A. Gómez Espinoza and P. A. Salamea Cordero, “Estudio y simulación de la implementación de un operador móvil virtual (OMV),” Universidad Politécnica Salesiana, 2013.