UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERIA
POSTGRADO EN INGENIERÍA DE TELECOMUNICACIONES

Trabajo Especial de Grado

PROPUESTA PARA LA MEJORA DE LOS SISTEMAS DE SEGURIDAD Y TELECOMUNICACIONES DE UNA ORGANIZACIÓN DE TRANSPORTE MARITIMO.

Presentado por:

Sanabria Cancino, Iván Darío

Para optar al título de Especialista en

Ingeniería de Telecomunicaciones

Asesor:

Di Attanasio, Berardo

Caracas, Junio de 2013

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERIA
POSTGRADO EN INGENIERÍA DE TELECOMUNICACIONES

Trabajo Especial de Grado

PROPUESTA PARA LA MEJORA DE LOS SISTEMAS DE SEGURIDAD Y TELECOMUNICACIONES DE UNA ORGANIZACIÓN DE TRANSPORTE MARITIMO.

Presentado por:

Sanabria Cancino, Iván Darío

Para optar al título de Especialista en

Ingeniería de Telecomunicaciones

Asesor:

Di Attanasio, Berardo

Caracas, Junio de 2013

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERIA
POSTGRADO EN INGENIERÍA DE TELECOMUNICACIONES

ACEPTACIÓN DEL ASESOR

Por la presente hago constar que he leído y analizado el Trabajo Especial de Grado presentado por el (la) ciudadano (a) Iván Darío Sanabria Cancino, titular de la C.I. 15.182.222, para optar por el título de Especialista en Ingeniería de Telecomunicaciones, cuyo título es **"PROPUESTA PARA LA MEJORA DE LOS SISTEMAS DE SEGURIDAD Y TELECOMUNICACIONES DE UNA ORGANIZACIÓN DE TRANSPORTE MARITIMO"** y que acepto asesorar al estudiante durante la etapa de desarrollo del trabajo, hasta su presentación y evaluación final.

En la ciudad de Caracas a los 19 días del mes de febrero de 2013,

_____

Prof. Berardo Di Attanasio

C.I: 5.418.846

Dedicatoria

A MI PAPA Y MAMA…
POR SU CONSTANTE APOYO
EN LAS METAS QUE ME ESTABLEZCO
Y AYUDARME A MATERIALIZAR ESTE SUEÑO…

Iván Darío Sanabria Cancino.

Agradecimientos

Primeramente agradecerle a Dios, por darme la paciencia, sabiduría y entendimiento necesarios para afrontar esta etapa de mi vida.

A mi Papá y Mamá por ser mi ejemplo a seguir y estar allí, siempre presente en los momentos más importantes para mi. Gracias por ese gran apoyo desde el primer día que les comenté sobre esta meta a cumplir.

A Maria Cecilia, mí novia, quien constantemente me da animos para afrontar los retos que se me presentan en el camino y, más allá de la distancia que puede haber (vive fuera de Caracas), es la persona que más cerca está de mi, y a la cual acudo en todo momento.

A mis compañeros de clase del Post-Grado, empezamos juntos y terminamos juntos. Siempre solidarios entre nosotros cuando se presentaba alguna dificultad. Siendo lo más importante, la amistad que empieza de aquí en adelante.

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERIA
POSTGRADO EN INGENIERÍA DE TELECOMUNICACIONES

PROPUESTA PARA LA MEJORA DE LOS SISTEMAS DE SEGURIDAD Y TELECOMUNICACIONES DE CORPORACION FEARNLEYS DE VENEZUELA.

AUTOR: ING. IVÁN DARÍO SANABRIA CANCINO.
ASESOR: BERARDO DI ATTANASIO.
AÑO: 2013

Resumen

Las empresas de transporte marítimo hoy en día cuentan con sistemas de seguridad y telecomunicaciones de última tecnología, los cuales les permiten tener plena confianza que los canales de comunicación con clientes y proveedores estarán en pleno funcionamiento, y la información que se maneja, envía y recibe llegará a su destino sin problema alguno en los tiempos pautados. La empresa a la cual va dirigido el presente trabajo, no presenta un sistema de seguridad muy robusto, que pueda resguardar la información que se maneja y los activos de la misma. Cuentan solamente con un sistema de cámaras que vigila en ciertas zonas claves para el acceso a la oficina. En cuanto a las telecomunicaciones, Internet y telefonía presentan varios fallas e inconvenientes, que afectan constantemente las tareas diarias de la empresa. En este sentido se realizaron varios análisis sobre la situación actual de estas áreas y en busca de dar solución a dichos inconvenientes, se presentan tres propuestas para mejorar los sistemas de seguridad y telecomunicaciones, en donde la principal innovación es la migración hacia Telefonía IP (VoIP). En esta tecnología pueden converger en una misma red voz, datos y video, también se puede manejar un sistema de seguridad robusto que proteja la información. La migración hacia esta nueva tecnología, traerá beneficios a la empresa como la reducción de la facturación telefónica, incorporar nuevos servicios a la red, estar a la par con otras oficinas a nivel mundial.

Palabras clave: transporte marítimo, mejora, sistemas, seguridad, canales de comunicación, telecomunicaciones.

Línea de trabajo: redes de próxima generación, gestión de redes.

Lista de Acrónimos y Siglas

3CX: marca comercial de centrales telefónicas.

AMFE: Análisis Modal de Fallos y efectos, procedimiento de análisis de fallos potenciales en un sistema de clasificación determinado por la gravedad o por el efecto de los fallos en el sistema.

Ancho de Banda: es la cantidad de datos que puede ser transportados por algún medio en un determinado periodo de tiempo.

ANSI: American National Standards Institute.

Asterisk: software libre diseñado para la integración y unificación de los sistemas de comunicación conocidos.

ATA: Advanced Technology Attachment, es una interfaz de transferencia de datos entre la placa base y algunos dispositivos de almacenamiento.

Broker: Un broker es una persona física o una firma que actúa de intermediario entre un comprador y un vendedor y que normalmente cobra una comisión de la operación.

Codecs: algoritmo que traduce la señal analógica en señal digital.

CPU: Central Processing Unit, parte fundamental o cerebro de la computadora.

DVR: Digital Video Recorder, dispositivo que almacena video en un disco duro proveniente de una o varias cámaras de video.

E1: Equivalencia europea del T1, excepto que su capacidad es 2.048 Mbps.

Escala MOS: Mean Opinion Score.

Ethernet: Protocolo de red definido por la IEEE. Define como los datos son transmitidos y recibidos en la red.

FXS: Foreing Exchange Station, conector de una central telefónica o de pared, que permite conectar un teléfono analógico estándar.

FXO: Foreing Exchange Office, dispositivo de la computadora que permite conectarse con el RTC, y mediante un software, recibe y realiza llamadas telefónicas.

H.323: Protocolo o estándar en la transmisión de audio, video y datos en redes IP, sin garantía de QoS.

Hacker: persona que entra de manera desautorizada a computadoras y redes de computadoras.

Hardware: termino en ingles que se refiere a cualquier componente físico tecnológico, que trabajo o interactúa con la computadora.

IAX: protocolo diseñado para trabajar con Asterisk.

IEEE: Institute of Electrical and Electronics Engineers, asociación que investiga en el campo aeroespacial, computacional, comunicacional, etc.

IETF: Internet Engineering Task Force, organización de técnicos que administran tareas en ingeniería de telecomunicaciones, principalmente de Internet.

IP: Internet Protocol, es un protocolo para la comunicación en una red a través de paquetes conmutados.

IP-PBX: central encargada de conmutar las llamadas de voz en una red de datos a través del protocolo IP e interoperar con la PSTN.

ISO: International Organization for Standardization.

Jitter: Se refiere a la variación que puede tener el retardo en una transmisión de datos.

SDP: Session Descripcion Protocol.

LAN: Local Area Network.

Latencia: tiempo necesario para que un paquete de información se transfiera de un lugar a otro.

MAN: Metropolitan Area Network.

MMSC: Multimedia Session Control, grupo desarrollador del protocolo SIP.

Modelo OSI: es un modelos creado por ISO, para la interconexión de sistemas abiertos.

PBX: Private Branch Exchange, central telefónica conectada a la red pública de telefonía, a través de líneas troncales.

PC: Personal Computer.

PDA: Personal Digital Assistant, es un dispositivo de pequeño tamaño que combina un ordenador, teléfono/fax, Internet y conexiones de red.

Proxy: es un servidor que sirve de intermediario entre un cliente y otro servidor.

PSTN: Public Switched Telephone Network.

QoS: Quality of Service.

Red: Una red es un sistema de objetos o personas conectados entre sí. Ejemplo: Sistema Nervioso, Red de Transporte urbano, Red de datos.

RTC: reloj de computadora que mantiene la hora actual.

RTP: Real Time Protocol, protocolo empleado para la transmisión de información en tiempo real, como audio y video para teleconferencias.

RTCP: Real Time Control Protocol.

RTSP: Real Time Streaming Protocol.

Sesión multimedia: aplicación de mensajería instantánea, aplicaciones de video, de audio, conferencias y aplicaciones similares.

Shipping: embarque, envío, transporte marítimo.

SIP: Session Initiation Protocol.

Softphone: software que se emplea para realizar llamadas a otros softphones o a otros teléfonos convencionales usando VoIP.

Software: todo programa o aplicación programada para realizar tareas específicas.

SPAM: es todo tipo de método de publicidad engañosa, no solicitada u oculta.

T1: Canal de comunicaciones de datos con un ancho de banda de 1.544 Mbps, disponible en varias versiones. Estándar Estadounidense y Japonés.

TCP: Transmission Control Protocol.

Token Ring: es una arquitectura de red desarrollada por IBM en los años 1970 con topología física en anillo y técnica de acceso de paso de testigo, usando un frame de 3 bytes llamado Token que viaja alrededor del anillo.

UDP: User Datagram Protocol.

UPS: Uninterruptible Power Supply.

Virus: pequeño software que infecta a las computadoras y tiene como propósito dañar la información, robarla, modificarla, etc.

VoIP, Voz sobre IP: Término utilizado en la Telefonía IP para un conjunto de facilidades para administrar la dotación de voz utilizando el protocolo Internet (IP).

WAN: Wide Area Network.

Índice

Lista de Figuras 10

Lista de Tablas..... 11

Introducción 13

Capitulo I. Tema de Investigación..... 15

I.1 Planteamiento del Problema 15

I.2 Interrogantes 16

I.3 Objetivo General 17

I.4 Objetivos Específicos 17

I.5 Justificación..... 17

I.6 Alcance..... 18

Capitulo II. Marco Teórico 19

II.1 Antecedentes 19

II.2 Seguridad de la Información..... 23

II.2.1 Definición 23

II.2.2 Elementos de Seguridad de la Información 23

II.2.3 Tipos de ataques 24

II.2.4 Vulnerabilidad de la Información..... 25

II.2.5 Amenazas de la Información 25

II.2.6 Riesgos de la Información 27

II.2.7 Clasificación de la Seguridad..... 27

II.3 Redes de Datos..... 32

II.3.1 Tipos de Redes de Datos 34

II.3.2 Componentes de una Red..... 39

II.4 VoIP 42

II.4.1 Definición de VoIP 42
II.4.2 Arquitectura 43
II.4.3 Señalización y Audio..... 46
II.5 Seguridad en VoIP 53
II.5.1 Clasificación de los Ataques 56
II.6 Herramientas para el desarrollo de las actividades 61
Capitulo III. Marco Metodológico..... 64
III.1 Disposiciones Generales..... 64
III.2 Tipo de Investigación..... 64
III.3 Diseño del Estudio 65
III.4 Etapas de la Investigación..... 67
III.5 Unidad de Análisis..... 68
III.6 Cronograma 69
III.7 Consideraciones Éticas 70
Capitulo IV. Marco Referencial 74
IV.1 Información de una empresa de transporte marítimo 74
IV.2 Organización de la Empresa..... 75
IV.3 Situación Actual 76
Equipos actuales 77
Capítulo V. Análisis de Resultados 82
V.1 Calidad de Servicio (QoS)..... 82
V.1.1 Cableado 83
V.1.2 Ancho de banda 84
V.1.3 Perdida de paquetes 87
V.1.4 Retardos..... 88

V.1.5 Evolución y modificación de la red 88
V.2 Aspectos económicos de la solución VoIP..... 89
V.3 Aplicaciones y Equipos en VoIP 90
V.3.1 Servidores de Telefonía IP y PBXs 90
V.3.2 Softphone 92
V4. Fallas en los Sistemas Actuales 94
V.5 Propuestas o Alternativas al problema planteado..... 95
V.5.1 Primera Alternativa 96
V.5.2 Segunda Alternativa 103
V.5.3 Tercera Alternativa 105
V.6 Sistema de Seguridad..... 109
V.7. Selección de la Alternativa..... 114
Capítulo VI. Conclusiones y Recomendaciones 121
VI.1 Conclusiones 121
VI.2 Recomendaciones 124
Referencia Bibliografía..... 126
Anexos..... 133
Anexo 1. Normas para Cableado Estructurado. 133
Anexo 2. Cuadro comparativo del software IP PBX Asterisk y el software IP PBX 3CX..... 134
Anexo 3. Cuadro comparativo entre la IP PBX Asterisk Appliance 50 (AA50) y la IP PBX 3CXPSENT. 134
Anexo 4. Teléfono IP Digium D40. 135
Anexo 5. Teléfono IP Digium D50 136
Anexo 6. Cámara Domo 1/3 Cmos Sony Color 136

Anexo 7. DVR Stand Alone Hikvision 8 canales..... 137

Lista de Figuras

FIGURA 1. DÍAGRAMACIÓN DE LA LLAMADA TELEFÓNICA. 15
FIGURA 2. AMENAZAS PARA LA SEGURIDAD. 26
FIGURA 3. PIRÁMIDE DE LA SEGURIDAD. 28
FIGURA 4. DÍAGRAMA DE UNA RED. 33
FIGURA 5. RED LAN. 35
FIGURA 6. RED WAN. 36
FIGURA 7. RED MAN. 36
FIGURA 8. TOPOLOGÍA EN LÍNEA. 37
FIGURA 9. TOPOLOGÍA DE ESTRELLA. 38
FIGURA 10. TOPOLOGÍA DE ANILLO. 39
FIGURA 11. ARQUITECTURA VOIP. 44
FIGURA 12. TELÉFONO IP CISCO SMALL BUSINESS SPA303 3 LÍNEAS. 45
FIGURA 13. PROTOCOLO H.323. 51
FIGURA 14. PIRAMIDE DE SEGURIDAD EN VOIP. 54
FIGURA 15. DÍAGRAMA DE FLUJO AMFE. 63
FIGURA 16. ORGANIGRAMA DE LA EMPRESA. 75
FIGURA 17. CENTRAL PANASONIC KX-TDA30. 77
FIGURA 18. TELÉFONO PANASONIC KX-T7633X. 77
FIGURA 19. TELÉFONO PANASONIC KX-TG2810LA. 78
FIGURA 20. TELÉFONO PANASONIC KX-TG2820LA. 78
FIGURA 21. SWITCH TP-LINK TL-SF1024. 78
FIGURA 22. PATCH PANEL LANPRO CAT 5E. 79
FIGURA 23. ROUTER LINKSYS WRT54G2 V1. 79
FIGURA 24. CÁMARA DE PUERTA KOCOM KC-60C. 80
FIGURA 25. TARJETA PCI. 80
FIGURA 26. CAMARA DE SEGURIDAD TIPO DOMO. 81
FIGURA 27. ANCHO DE BANDA ANTES DE LA APERTURA DEL CENTRO COMERCIAL. 85
FIGURA 28. ANCHO DE BANDA DESPUÉS DE LA APERTURA DEL CENTRO COMERCIAL. 86

FIGURA 29. VISTA DEL SOFTWARE DE LINPHONE. 93
FIGURA 30. VISTA DEL SOFTWARE ZOIPER..... 94
FIGURA 31. ASTERISK APPLIANCE 50 (AA50). 98
FIGURA 32. SOLUCIÓN A LA RED DE LA EMPRESA DE TRANSPORTE MARÍTIMO. ... 116

Lista de Tablas

TABLA 1. ANTECEDENTES 21
TABLA 2. NIVELES DE SEGURIDAD..... 27
TABLA 3. CARACTERÍSTICAS DEL PROTOCOLO SIP. 47
TABLA 4. SOLICITUDES SIP. 49
TABLA 5. RESPUESTA SIP..... 49
TABLA 6. ATAQUES Y AMENAZAS A LAS CAPAS DE LA PIRÁMIDE DE SEGURIDAD DE VOIP..... 55
TABLA 7. PLAN DE TAREAS..... 69
TABLA 8. CRONOGRAMA DE ACTIVIDADES..... 70
TABLA 9. ESCALA MOS PARA MEDIR LA CALIDAD DE LA VOZ 83
TABLA 10. ESCALA MOS PARA MEDIR EL ESFUERZO DE INTERPRETACIÓN DEL MENSAJE 83
TABLA 11. DIFERENCIA ENTRE CABLE UTP CAT 5E Y CAT 6 84
TABLA 12. COSTOS RELACIONADOS A LA IP PBX 98
TABLA 13. CARACTERÍSTICAS DE LOS TELÉFONOS IP D40 Y D50. 100
TABLA 14. COSTOS RELACIONADOS A TELÉFONOS IP 101
TABLA 15. COSTO TOTAL PRIMERA ALTERNATIVA..... 103
TABLA 16. COSTO MENSUAL NUEVO PROVEEDOR DE TELECOMUNICACIONES. 105
TABLA 17. COMPARACIÓN DE COSTOS ALQUILAR O COMPRAR LOS EQUIPOS PARA VOIP CON BANTEL. 108
TABLA 18. COSTOS ASOCIADOS A LA TERCERA ALTERNATIVA 109
TABLA 19. COMPARACIÓN ENTRE SISTEMAS ANALÓGICOS Y SISTEMAS DIGITALES.111
TABLA 20. COSTOS SISTEMA DE CÁMARAS DE SEGURIDAD. 112
TABLA 21. COSTO ANTIVIRUS. 114

TABLA 22. COSTOS SISTEMAS DE SEGURIDAD 114
TABLA 23. ESCALA VALORACIÓN PARA LA MATRIZ DÍAGNOSTICO..... 117
TABLA 24. MATRIZ DE DÍAGNOSTICO ELECCIÓN SOLUCIÓN IDEAL 117

Introducción

Las comunicaciones se han convertido en parte integral de las sociedades modernas y ha puesto al usuario final en la vanguardia de la telecomunicación. Cualquier tipo de información está disponible y además en numerosos formatos. Siguiendo esta idea, las empresas actualmente tratan de poseer sistemas revolucionarios en sus áreas de trabajo que las coloque a la vanguardia en cuanto a tecnología. Sistemas de seguridad y sistemas de telecomunicaciones que cubran sus necesidades y puedan aportar grandes beneficios son los principales focos de las empresas hoy día.

Durante los últimos años, los servicios de voz por protocolo de Internet (VoIP), impulsados por el crecimiento de las redes de banda ancha y las reducciones de costos, han sido tan convulsivos que han transformado el mundo de las telecomunicaciones. VoIP ha sido aceptado generalmente por los proveedores de servicios, consumidores y empresas, ya que es una manera más económica de comunicar porque, en lugar de utilizar líneas terrestres convencionales, las llamadas telefónicas viajan por Internet y los propios operadores ahorran dinero utilizando las redes basadas en el IP.

Es el caso de las empresas de transporte marítimo, están obligadas a mantener una comunicación constante con clientes, proveedores y principalmente, con sus embarcaciones que pueden estar en alta mar o cualquier puerto del mundo. Estas empresas al migrar a una tecnología como ésta, VoIP, pueden manejar voz, datos y video a través de una misma red, de manera constante cuando se requiera a costos menores a los sistemas que se usan en la actualidad y más aún, implementando sistemas de seguridad que puedan salvaguardar la información que se maneja.

El presente trabajo va dirigido a una empresa del ramo, la cual presenta inconvenientes en estas áreas específicas y busca mejorarlas lo antes posible. Se presentan alternativas de solución, las cuales se sustentan con la investigación realizada para que a corto o mediano plazo pueda ser

implementada la que mejor se adapta a las condiciones de la empresa en cuestión.

Para dar solución a la problemática que presenta la compañía de Trasporte Marítimo, se ha desarrollado el presente trabajo, organizado de la siguiente manera:

Capítulo I. Tema de Investigación, se presenta el planteamiento del problema, los objetivos propuestos y la justificación y alcance del mismo.

Capítulo II. Marco Teórico, se muestran las bases teóricas que sustentan el presente trabajo. Aquí se plasman todos los conceptos y conocimientos necesarios para el desarrollo y comprensión de proyecto.

Capítulo III. Marco Metodológico, se plasma la metodología a través de la cual se desarrolla el presente trabajo.

Capítulo IV. Marco Referencial, breve reseña de la empresa a la cual va dirigido el presente trabajo.

Capitulo V. Análisis de Resultados, se presenta los resultados obtenidos de la investigación. Se mencionan varias alternativas que ayudarán a solucionar los problemas actuales de la empresa en el área de seguridad y telecomunicaciones, y de las cuales, se selecciona la alternativa ideal.

Capítulo VI. Conclusiones y Recomendaciones, se muestran las conclusiones que se obtienen de esta nueva tecnología y las recomendaciones necesarias para poder migrar hacia la misma.

Referencias Bibliográficas: toda la bibliografía consultada para el desarrollo del trabajo.

Capitulo I. Tema de Investigación

I.1 Planteamiento del Problema

Actualmente los servicios de telecomunicaciones (telefonía e Internet) que recibe la organización en estudio son a través de un proveedor que ofrece el condominio del centro comercial donde se encuentra la oficina. Estos servicios presentan muchas fallas, generando problemas en los sistemas de seguridad y telecomunicaciones de la empresa. En la parte de telefonía el principal problema es el número telefónico con las llamadas salientes, ya que éste no concuerda con los números de la empresa y al devolver la llamada, esta no cae en la empresa de transporte marítimo, sino en otra oficina o local del centro comercial.

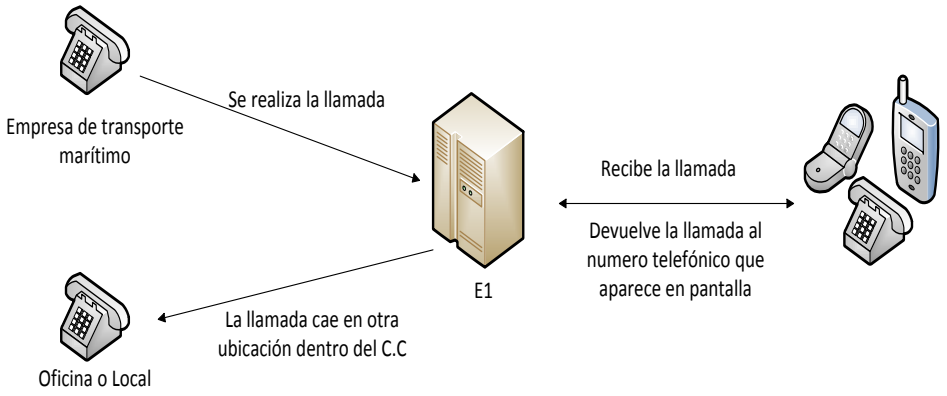

Figura 1. Diagramación de la llamada telefónica.
Fuente: Elaboración Propia.

Para la conexión a Internet o datos, el servicio que ofrecen es muy lento y se cae constantemente alterando el funcionamiento normal de las actividades de la empresa. También es imposible monitorear vía Internet, las cámaras de seguridad, limitando su verdadera función. Esta imposibilidad se presenta al conectarse a Internet fuera de la oficina.

El problema que se presenta con la telefonía y las cámaras de seguridad es constante, mientras que Internet presenta fallas ocasionalmente.

Para poder solucionar estos problemas anteriormente planteados y estar a la par de otras sedes en cuanto a tecnología, la empresa de transporte marítimo debe contar con sistemas de seguridad y telecomunicaciones que garanticen la comunicación a distancia, manteniendo la integridad de la información en todo momento. Partiendo de esta premisa, se presentan varias alternativas las cuales ayudarán a solventar los inconvenientes que tiene actualmente la organización en estudio. Adquirir equipos nuevos y de última tecnología en la parte de telefonía y redes de datos que permitan migrar a VoIP. Analizar y consultar las consecuencias de adquirir un nuevo proveedor de servicios de telecomunicaciones. Este último puede presentar la opción de prestar el servicio de VoIP directamente.

Al migrar a Telefonía IP (VoIP), la seguridad en las llamadas telefónicas es alta y constante. Esto se debe a que las mismas salen es a través de la red interna (Internet) y no por el proveedor CANTV, evitando que puedan ser interceptadas o pinchadas. Para darle más robustez a esta red en la parte de seguridad, se evaluarán distintos dispositivos, como: firewalls, switches; que protegen a la misma de ataques. También por medio de la red, se pueden integrar los sistemas de seguridad física y control de acceso a la oficina.

I.2 Interrogantes

¿Es importante para la empresa en cuestión migrar hacia VoIP? ¿Gestionar una red que integre voz, datos y video presenta grandes beneficios a una empresa de transporte marítimo? ¿Son necesarios mecanismos de control de acceso a la oficina? ¿De qué manera un nuevo o actualizado sistema de seguridad protegerá la información que se trasmite y recibe?

I.3 Objetivo General

Analizar alternativas de mejoras en los sistemas de seguridad y telecomunicaciones de una organización de transporte marítimo.

I.4 Objetivos Específicos

- Identificar fallas y vulnerabilidades en los actuales sistemas de seguridad en las redes de información.
- Identificar fallas y vulnerabilidades en los actuales sistemas de telecomunicaciones.
- Evaluación de la tecnología a un nuevo sistema de seguridad y de telecomunicaciones.
- Proponer la solución técnica idónea para el sistema de seguridad y de telecomunicaciones.

I.5 Justificación

Con este trabajo se busca que al migrar hacia una nueva tecnología, específicamente Telefonía IP (VoIP), la compañía en cuestión quiere integrar en una misma red voz, datos y video; cumpliendo los procesos de transmisión en su tiempo determinado, con la certeza que la información no presentará inconvenientes, ataques o robos.

Con este proyecto de investigación se da a conocer toda la información necesaria sobre Telefonía IP (VoIP) que darán sustento a la propuesta de migrar hacia esta nueva tecnología. Esta permite converger en una misma red voz, datos y video; la cual se puede integrar con equipos y software de última tecnología, agilizando las actividades diarias de la empresa y dando solución a los problemas presentes en cuanto a telecomunicaciones.

I.6 Alcance

El presente trabajo tiene como alcance presentar una propuesta para migrar hacia una tecnología donde puedan converger en una misma red voz, datos y video. También se proponen mecanismos de seguridad de datos y seguridad física que tienen como finalidad la protección de la información. Con estas propuestas se busca mejorar los sistemas de seguridad y telecomunicaciones de una empresa de transporte marítimo. Queda a criterio de la empresa su aprobación y posterior ejecución e implementación.

Capitulo II. Marco Teórico

II.1 Antecedentes

Para el desarrollo del presente trabajo es importante tener referencia de trabajos de investigación que se han realizado con anterioridad.

Algunos trabajos de investigación que se han realizado previos a este trabajo son:

Guitan (2010), realizó un trabajo de grado, en el cual el objetivo principal es "*Diseñar y planificar la infraestructura tecnológica requerida para prestar los servicios de voz, datos y video en los nuevos edificios de CVG EDELCA ubicados en el complejo hidroeléctrico Antonio José De Sucre en Macagua".* El desarrollo de este trabajo sirvió como punto de partida a EDELCA para modernizar y renovar el sistema de telefonía. Al migrar a tecnología VoIP, generó una reducción en los costos de telefonía y permite el uso de aplicaciones más avanzadas de telecomunicaciones.

Con este trabajo se obtuvo información relacionada con VoIP, que ayuda a fortalecer los conocimientos que se poseen en el área y sustentan el planteamiento que se hace en el presente trabajo. Las palabras claves en este trabajo son: Red de Voz, Red de Datos, Voz sobre IP, Telefonía IP.

Wasylkowski (2007), realizó un trabajo de grado cuyo objetivo principal es "*Implementar una red telefónica IP para la sede de Fe y Alegría en Caracas basada en software de fuente libre".* Con la elaboración de este trabajo se logró la reducción notoria en la facturación de la telefonía. También al realizar los manuales correspondientes, el personal de la institución tiene la capacidad para manejar dicha tecnología. Las palabras claves en este proyecto son: IP PBX, Telefonía IP, protocolos de señalización, códec, Asterisk.

Este trabajo aporta conocimientos en la parte de VoIP. Menciona los protocolos de señalización más usados en cuanto a Telefonía IP, destacando el protocolo SIP. Hace mención a los códec que se emplean para convertir la señal de analógica a digital. Refuerza la información obtenida sobre el tema.

Velásquez (2010), presentó un trabajo de grado, en el cual su objetivo es "*Desarrollar una propuesta de diseño de una red VoIP sobre una plataforma IP-PBX, tomando en cuenta el factor económico, técnico y operativo necesario al evaluar las características de las diversas soluciones comerciales de sistemas telefónicos disponibles, dirigida a satisfacer las necesidades de comunicación actuales y futuras de la empresa Neoprana Technologies C.A.*". Desarrollar este proyecto generó la reducción de costos en telefonía, la integración de los servicios de voz y datos. También proporcionó la independencia de la red de telefonía y capacidad de crear nuevas aplicaciones.

El desarrollo de este trabajo refuerza los conocimientos adquiridos sobre implementación de VoIP en organizaciones. Destaca la necesidad de hacer un estudio de la situación actual de la empresa y si cuenta con las condiciones mínimas para poder migrar hacia esta tecnología.

Hernández (2004), desarrollo un trabajo de grado que tiene como objetivo: "*Evaluación de los mecanismos de seguridad en los sistemas de notificación y registro de eventos para la gestión de redes*.". El desarrollo de este proyecto muestra lo importante de tener mecanismos que protejan las redes de datos frente a la gran cantidad de amenazas que se presentan hoy día en Internet. Estos sistemas pueden integrarse en una sola red, lo que hace más segura la misma. Implementar políticas de seguridad es un aspecto relevante en la seguridad de la red.

Este trabajo tiene como aportes la manera de gestionar los sistemas de seguridad en las redes de datos. Funcionamiento de los protocolos Syslog y SNMP. Presenta varias alternativas en cuanto a sistemas de seguridad.

Tabla 1. Antecedentes

Tesis	Objetivos	Resultados	Aportes	Bases Teóricas
Propuesta para implementar redes de voz y datos. Caso EDELCA	- Recopilar información sobre las soluciones existentes en el mercado en lo referente a redes de datos que soporten voz sobre IP (VoIP) y redes de voz que operen bajo IP (Telefonía IP). - Proponer las diferentes alternativas de redes de voz que operen bajo IP. - Definir las normas de operación y gestión de la red. - Validar la solución propuesta para el caso EDELCA.	Se reducen los costos en cuanto a telefonía. Aunque es un proyecto factible, representa una alta inversión. Integración de los servicios de voz, datos y video en una misma red.	Realizar este proyecto le sirve a EDELCA como punto de partida para modernizar y renovar la red de telemática. Al migrar a tecnología VoIP, los costos se reducen en cuanto a telefonía. También permite el uso de aplicaciones más avanzadas de comunicaciones, trayendo beneficios a la compañía.	Investigación documental y técnica de los conceptos básicos utilizados en las áreas de redes de datos y redes de voz
Implementación de una red de Telefonía IP en la sede de Fe y Alegría en Caracas	- Estudio teórico sobre los protocolos por los cuales se lleva a cabo la comunicación en la red. - Plan de procura del hardware necesario para la implementación de una red telefónica IP. - Instalar el hardware necesario para la implementación de la red según los servicios adecuados a la red de Fe y Alegría especialmente en la sede nacional en Caracas. - Realizar un manual de instalación y un manual de operación del sistema instalado. - Implementar un plan de entrenamiento para el personal.	Previa investigación sobre sobre la tecnología IP, se obtienen conocimientos sobre protocolos y servicios PBX. Luego se seleccionan los dispositivos a implementar. Posterior a esto se realizan las pruebas, instalación y manuales que dan como resultado la red de Telefonía IP que se desea implementar.	Reducción notoria en la facturación de la telefonía. Con la realización de los manuales, el personal está en la capacidad de instalar ciertos equipos previamente haber leído el o los manuales.	Investigación sobre voz IP, transporte de voz sobre redes de conmutación de paquetes. Investigación sobre protocolos de señalización y los códec.
Implementación de una solución de VoIP: caso de estudio NEOPRANA TECHNOLOGIES C.A.	- Analizar la plataforma de comunicaciones existente en Neoprana Techonologies, y la nueva plataforma de VoIP, a fin de identificar los cambios necesarios en las características y funcionalidades a tomar en cuenta en el desarrollo de la nueva solución. - Identificar la mejor solución de un grupo de soluciones de VoIP que maneja la empresa, mediante la evaluación desde un punto de vista tecnológico, económico y organizacional con el fin de satisfacer las necesidades de comunicación de la organización. - Proponer la implementación de una solución de	Luego de estudiar la situación actual, se presenta la propuesta para la implementación, la cual fue aprobada por la Gerencia de TI según sus requerimientos.	Reducción de costos, integración de los servicios de voz y datos, facilidad de implementación escalabilidad, independencia de la red telefónica tradicional y capacidad de crear nuevas aplicaciones.	Estudio del estado actual de la plataforma de comunicación de la empresa Neoprana Technologies. Investigación sobre Voz IP, factores técnicos y económicos para escoger la propuesta más adecuada.

	un sistema VoIP sobre una plataforma IP-PBX, basado en el marco metodológico del autor Khaled Salah (2009) que cubre los parámetros de diseño y de ingeniería solicitados por la empresa.			
Evaluación de los mecanismos de seguridad en los sistemas de notificación y registro de eventos para la gestión de redes	- Estudiar el funcionamiento de los protocolos Syslog y SNMP tal como se usan actualmente. - Realizar pruebas en una red experimental para determinar las debilidades de dichos protocolos en lo que a seguridad de refiere - Implantar y probar los protocolos Syslog seguros y SNMP en una red experimental para evaluar sus características de seguridad y desempeño. - Comparar las distintas alternativas y recomendar la mejor solución	El desarrollo de este proyecto muestra lo importante de tener mecanismos que protejan las redes de datos frente a la gran cantidad de amenazas que se presentan hoy día en Internet. Estos sistemas pueden integrarse en una sola red, lo que hace más segura la misma. Implementar políticas de seguridad es un aspecto relevante en la seguridad de la red.	Presenta como se gestiona los sistemas de seguridad en las redes de datos. Funcionamiento de los protocolos Syslog y SNMP. Presenta varias alternativas en cuanto a sistemas de seguridad.	Análisis y estudio de los sistemas de seguridad en las redes. Protocolos de gestión de redes. Syslog. Analizadores de la red.

Fuente: Elaboración Propia.

II.2 Seguridad de la Información

II.2.1 Definición

La seguridad de la información es fundamental, ya que se puede divulgar información cuando los empleados publican datos en sus cuentas de redes sociales, o por accidente dejan al descubierto información confidencial. Estas faltas a la seguridad generan costos monetarios o de credibilidad muy altos a las empresas.

Areitio, (2008), menciona que “la seguridad es un proceso continuo multidimensional, que debe tenerse en cuenta en la definición, en la gestión y en la reingeniería de empresas y procesos de negocios. La seguridad puede verse en distintos planos de la sociedad, como una comunidad, una organización, en un sistema embebido, en un producto, o en un servicio.”

Calle (1997), define seguridad como “el conjunto de principios, normas y prácticas que regulan como deben ser gestionados, protegidos y distribuidos los activos, en cuanto a información se refiere, de una compañía.”

Las tecnologías de seguridad de redes protegen las redes contra robos y el uso incorrecto de la información confidencial de la empresa y ofrecen protección contra ataques maliciosos de virus y gusanos de Internet. Si la empresa no cuenta con seguridad de la red, puede ser blanco de ataques por parte de intrusos (hackers) que pueden robar, modificar, manipular información importante. También se pueden presentar interrupciones del servicio, inactividad de la red y hasta acciones legales.

II.2.2 Elementos de Seguridad de la Información

Mendillo (2012 a), expone sobre los elementos de seguridad de la información:

Integridad: controla quien tiene acceso a la información impidiendo que ésta sea manipulada por personas sin el debido permiso.

Disponibilidad: asegura un buen desempeño, garantizando protección y recuperación del sistema si se presenta algún inconveniente.

Integridad: asegura que la información entregada sea la misma que se ha enviado; sin que la misma no sufra modificaciones, daños o errores en su proceso de transmisión.

Autenticidad: garantiza que la información es genuina y no es réplica de información vieja.

Identificación y control de acceso: es la que identifica y da acceso a los datos.

Toda información es importante y por ende debe ser resguardada, sin embargo, para lograr esto existen pautas que se deben cumplir. Para Borghello (2001), existen tres aspectos básicos que se deben proteger:

Hardware: son todos los sistemas físicos como CPU, cableados, impresoras entre varios más.

Software: son los elementos lógicos que hacen funcionar al hardware como sistemas operativos, aplicaciones, utilidades.

Datos: información lógica que manejan tanto el hardware como el software, bases de datos, archivos, documentos.

II.2.3 Tipos de ataques

Borghello (2001), menciona que existen dos tipos de ataques, Activos y Pasivos.

Ataques Activos: este ataque implica modificación del flujo de la información o la creación de un falso flujo de datos. Estos ataques son realizados por hackers o piratas informáticos.

Ataques Pasivos: el atacante no altera la comunicación. Por lo general la intercepta, escucha para saber que se transmite. Sus objetivos son la intercepción de datos y el análisis de tráfico.

II.2.4 Vulnerabilidad de la Información

Los principales ataques que se presentan en los sistemas de seguridad en las redes son consecuencia de personas que han violado los códigos de cifrado, han intervenido líneas de comunicación, han burlado controles de acceso y han creado programas malintencionados.

No solo las personas son las principales fuentes en cuento a los problemas de seguridad. Existen otros factores como accidentes naturales que pueden malograr la información y hasta en ocasiones, perderla en su totalidad. Estos aspectos se relacionan directamente con la vulnerabilidad física de la información.

Areitio (2008), expone “una vulnerabilidad, por si misma, no causa daño alguno; es, simplemente, una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo.”

II.2.5 Amenazas de la Información

Stallings (2004), se refiere a las amenazas como “una posibilidad de violación a la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera traspasar la seguridad y causar

perjuicio. Es decir, una amenaza es un peligro posible que podría aprovecharse de una vulnerabilidad."

Borghello (2001), define amenaza "como cualquier elemento que comprometa al sistema."

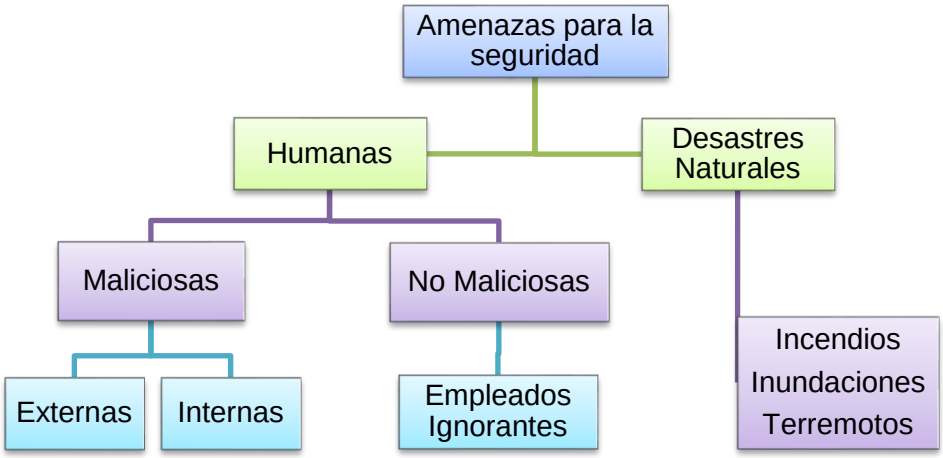

Figura 2. Amenazas para la Seguridad.
Fuente: Borghello (2001).

Se pueden analizar las amenazas en tres momentos:

Prevención (antes): es un mecanismo que aumenta la seguridad del sistema durante su normal funcionamiento.

Detección (durante): mecanismo el cual revela violaciones a la seguridad.

Recuperación (después): se procede con este mecanismo cuando la violación ha sido detectada y así, retornar el sistema a su funcionamiento normal.

Tabla 2. Niveles de Seguridad.

Nivel	Especificación
Aplicación	• Es lo que ve el usuario. • Es el nivel más complejo y menos fiable. • La mayor parte de los fraudes ocurren aquí.
Middieware	• Implicados los sistemas de gestión BD y la manipulación del software.
Sistema Operativo	• Se trata de la gestión de archivos y comunicaciones.
Hardware	• Es el nivel menos complejo y más fiable. • Características de seguridad en el CPU y en el hardware de gestión de memoria.

Fuente: Areitio (2008).

II.2.6 Riesgos de la Información

Según Areitio (2008), riesgo "es la posibilidad que se produzca un impacto determinado en un activo, en un dominio (o conjunto de activos) o en toda la organización." Este impacto se produce por las vulnerabilidades que explota una amenaza, causando pérdidas o daños.

A demás menciona, "el riesgo se caracteriza por dos factores: la *probabilidad* de que ocurra el incidente no deseado y su *impacto*."

II.2.7 Clasificación de la Seguridad

Seguridad Lógica (técnica): se encarga de la protección del software y los datos.

Seguridad Administrativa: se relaciona con las normas, política y procedimientos.

Seguridad Física: se enfoca en los riesgos relacionados con hurtos, daños, fallas, etc.; de los equipos, sistemas o redes. Igualmente llevan el control de acceso a las instalaciones.

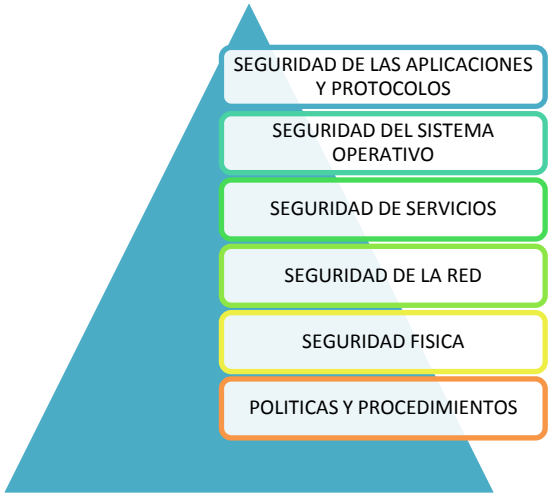

Figura 3. Pirámide de la Seguridad.
Fuente: Mendillo (2012 b).

Seguridad Lógica (técnica)

Borghello (2001), define la Seguridad Lógica como "la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlos."

García y Alegre (2011), menciona "la seguridad lógica se encarga de asegurar la parte software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y los datos."

Control de Acceso: Comenta Borghello (2001), "estos controles pueden implementarse en el Sistema Operativo de aplicación, bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario."

También menciona que Identificación y Autentificación, "es la primera línea de defensa para la mayorías de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor

parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.”

Roles: Los roles también pueden controlar el acceso a la información, ya que según sea el cargo en la empresa, el usuario tiene acceso a dicha información.

Transacciones: Cuando se desea realizar una transacción determinada, se solicita un clave que permite dicha transacción.

Modalidad de Acceso: Borghello (2001), describe las modalidades de acceso a la información de la siguiente manera:

- Lectura: el usuario solo puede leer o visualizar la información, aunque puede ser copiada o impresa.
- Escritura: permite realizar modificaciones a la información, bien sea agregando o eliminando información.
- Ejecución: otorga el privilegio a los usuarios de ejecutar programas.

Un ejemplo de estas modalidades son las cuentas de usuarios en los computadores; si es administrador, tiene la posibilidad de manejar toda la información, realizar modificaciones y ejecutar programas, en cambio un usuario estándar, solo podrá realizar ciertas funciones que se le permitan.

Seguridad Administrativa

GC Alarmas y Monitoreo (2012), empresa de seguridad y vigilancia privada, menciona “la seguridad administrativa es la política de trabajo, que se fundamenta en la filosofía y política que tiene establecida la empresa a resguardar y se debe seguir.”

Seguridad Física

Protege los sistemas informáticos a través de barreras para físicas y mecanismos de control. Se emplea para proteger físicamente el sistema informático.

Según Borghello (2001), seguridad física “se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo así como también los medios de acceso remoto al y desde el mismo; implementados para proteger al hardware y medios de almacenamiento de datos.”

Mendillo (2012 b), menciona sobre la seguridad física: “es muy importante tener en cuenta que por más que se hayan implementado medidas de protección adecuadas contra ataques externos, hackers, virus, etc., la seguridad de un sistema será pobre si no se ha previsto como combatir un incendio o una inundación.”

Los desastres que pueden afectar la información son varios, y de los cuales se deben tener conocimiento para prevenir riesgos de perder la información. Los tipos de desastres son:

Incendios: son producto del uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y mal almacenamiento y traslado de sustancias peligrosas.

Borghello (2001), destaca “el fuego es una de las principales amenazas contra la seguridad.es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.”

Inundaciones: son una de las causas de mayores desastres en centros de cómputo. Las inundaciones se pueden originar por acumulación de agua en terrenos planos, mal drenaje que puede ser por causa natural o artificial.

También, las inundaciones pueden ser a causa del agua que se acumula por la necesidad de apagar un incendio.

Condiciones Climatológicas: estas se asocian a tempestades, tormentas, tifones y catástrofes sísmicas, las cuales están documentadas para su prevención y actuación ante eventos como estos. Igualmente existen servicios que identifican estos sucesos con antelación, dando tiempo a que se pueda proceder a la logística para prevenir accidentes relacionados con la información.

Otra manera de verse afectada la información es a través de las acciones hostiles. Sobre las acciones hostiles, Borghello (2001) expone:

Robo: las computadoras contienen mucha información valiosa la cual puede ser sustraída de las mismas por los trabajadores sin ningún problema, esto es posible ya que muchas veces la seguridad para las computadoras es muy precaria.

El software, es una propiedad muy fácilmente sustraible y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

Fraude: cada año millones de dólares son sustraídos en empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumentos para dichos fines.

Sabotaje: es el peligro al cual más le temen los centros de datos. Estos sabotajes pueden ser a través de empleados de la empresa o personas ajenas a ella.

Físicamente, los imanes son empleados para realizar estas acciones, ya que al pasar un imán por una cinta magnética, este puede borra la información que en ella se guarda.

El control de acceso es un aspecto importante en la seguridad, ya que de esta manera se tiene controlado el acceso de personas a las instalaciones de la compañía.

Borghello (2001), comenta sobre el control de acceso, “no solo requiere la capacidad de identificación, sino asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.”

También menciona que para el control de acceso se pueden emplear varias técnicas:

Utilización de guardias: controla el acceso a las instalaciones de las personas, sean peatones o a través de vehículos. Son ubicados en sitios estratégicos para cumplir con el control de acceso del personal.

Detectores de metal: es un elemento práctico para la revisión de personas. La sensibilidad de estos detectores se puede graduar, así se puede activar con un mínimo de volumen metálico.

Sistemas biométricos: la Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. Los detectores biométricos pueden ser de manos, ojos, huellas digitales y voz.

II.3 Redes de Datos

Una red de datos es un sistema en el cual se enlazan dos o más puntos (terminales) a través de un medio físico por donde se puede enviar o transmitir un determinado flujo de información.

Las redes datos nacen por una necesidad empresarial de transmitir información, modificarla y actualizarla de manera rápida y eficaz. Antes de que existieran las redes de datos los usuarios tenían que utilizar medios

rígidos de almacenamiento de información; precisamente el desplazamiento de este medio lo hacía complejo.

Por estos inconvenientes se desarrollaron estándares para las tecnologías networking, siendo sus soluciones principales:

1. Compartir información.
2. Compartir hardware y software.
3. Centralizado administración y el soporte.

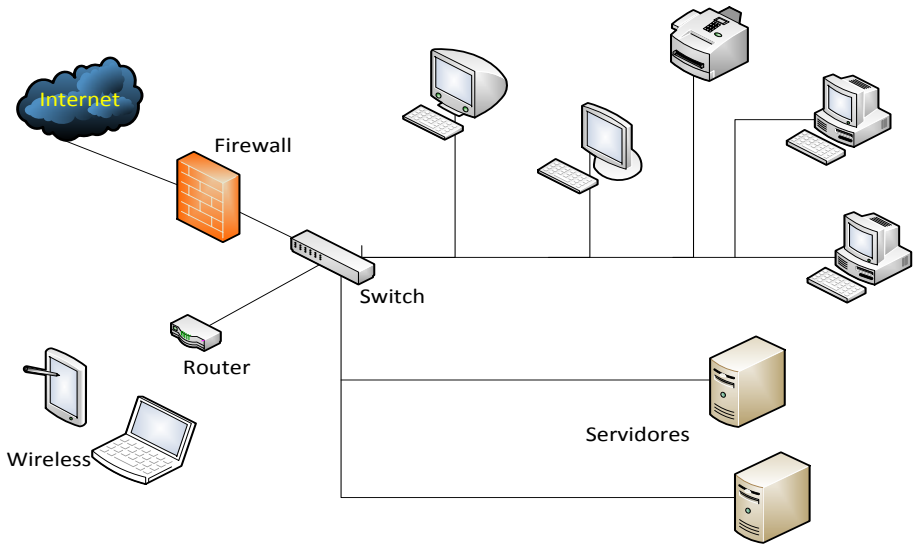

Figura 4. Diagrama de una red.
Fuente: Elaboración Propia.

Una definición de Redes de datos según Gil et al (2010), es “como un conjunto de dos o más dispositivos autónomos con la capacidad de interconectarse mediante un enlace de medio físico.”

También menciona, un enlace es “el medio físico que transfiere los datos de un dispositivo a otro.”

Gil et al (2010), clasifica las redes según el tipo de conexión:

Redes de difusión o multipunto: es cuando más de dos dispositivos comparten el mismo enlace. Se puede enviar un mismo mensaje desde un dispositivo a varios equipos.

Redes punto a punto: es cuando dos dispositivos tienen un enlace directo entre ellos. Conectar varios equipos equivale a varias conexiones punto a punto y, para que un mensaje llegue a destino, debe visitar varias máquinas primero.

II.3.1 Tipos de Redes de Datos

Las redes lógicas se clasifican según su tamaño y distribución lógica:

Clasificación según su tamaño

Redes de Área Local (LAN): son redes privadas y se usan para la conexión de computadores personales y estaciones de trabajo de una oficina, fábrica o empresa; con el fin de intercambiar información entre ellas. Estas redes tienen un tamaño restringido, teniendo como beneficio una alta velocidad de transmisión si se compara con otros tipos de redes. El material que se emplea para la conexión de este tipo de red es cable coaxial, fibra óptica o cable UTP. Las redes LAN emplean reglas o protocolos de transmisión como Ethernet.

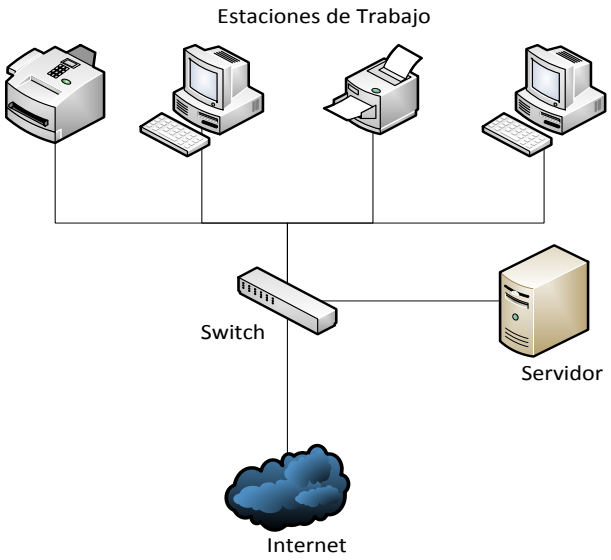

Figura 5. Red LAN.
Fuente: Elaboración Propia.

Redes de Área Amplia (WAN): estas redes son extensas geográficamente, interconecta zonas distantes como ciudades, estados, países. Su velocidad de conexión es menor debido a su largo recorrido pero son capaces de transportar altos volúmenes de datos. Estas redes están interconectadas por varias máquinas (host) conectadas por una subred de comunicaciones para conducir mensajes de un host a otro. En redes amplias, la subred tiene dos componentes, las líneas de transmisión y los elementos de conmutación que son computadoras especializadas que conectan dos o más líneas de transmisión.

Las redes LAN comúnmente, se conectan a las redes WAN, con el objetivo de tener otros servicios, como por ejemplo Internet. Estas redes son más complejas, deben enrutar de manera correcta toda la información proveniente de las redes que están conectadas a ésta.

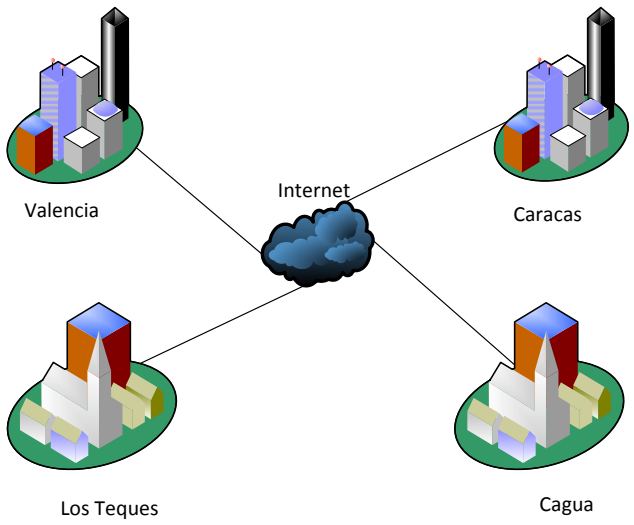

Figura 6. Red WAN.
Fuente: Elaboración Propia.

Redes de Área Metropolitana (MAN): estas redes se pueden conectar a lo largo de una ciudad, un municipio; teniendo un rango de cobertura mayor a una red LAN pero menor a una red WAN. Las redes MAN tienen el control de la transmisión de datos, a diferencia de las redes WAN, donde la transmisión de datos depende mucho del proveedor de servicios.

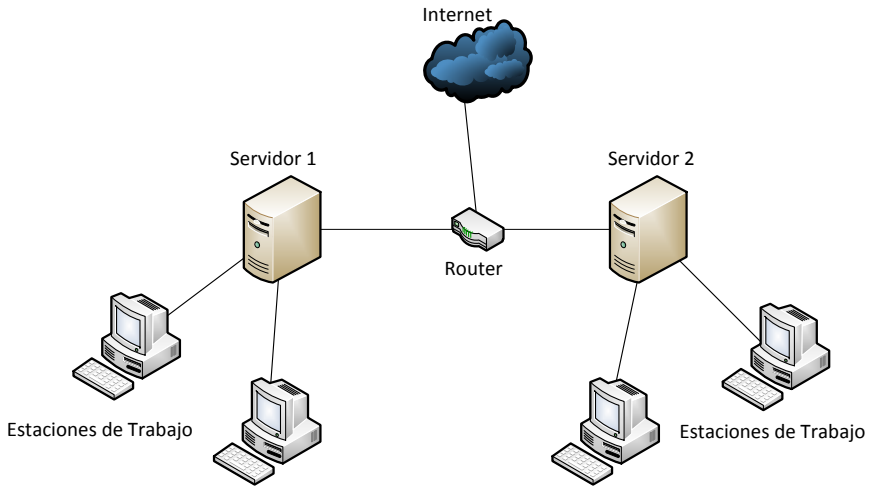

Figura 7. Red MAN.
Fuente: Elaboración Propia.

Clasificación según su topología

Topología lineal (Bus): todas las estaciones de trabajo se conectan se conectan a un canal de comunicación único llamado *bus*, por el cual fluye toda la información, entregando la información que transmite a quien le corresponde. Es una red sencilla y fácil de instalar permitiendo el aumento o disminución de equipos que la conforman. La cantidad de cable que se emplea para su configuración es menor en comparación con otras topologías, esto se debe a que el cable no va desde el servidor hasta cada equipo o estación de trabajo.

Tiene la ventaja que si falla en alguno de los equipos, no afecta a la red entera.

Su principal desventaja es el control de flujo. Al estar conformada por una sola línea, se requiere control de acceso al medio para evitar colisiones.

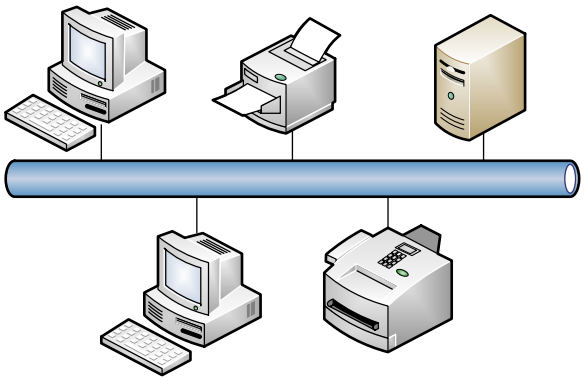

Figura 8. Topología en Línea.
Fuente: Elaboración Propia.

Topología de estrella: consiste en conectar todas las computadoras o estaciones de trabajo a un computador principal o servidor. A través de este servidor, es que se realizan todas las comunicaciones entre los computadores.

Esta topología, tiene una buena flexibilidad para incrementar o disminuir el número de estaciones de trabajo; una falla en algún equipo periférico, no represente gran problema para la red. Sin embargo, la falla es en el servidor, si afectará a todos los equipos conectados. Esta topología requiere de gran cantidad de cable para las conexiones. La comunicación de un computador con el servidor es rápida, pero la comunicación entre computadoras, es lenta. La velocidad de la red es alta si el flujo de información es entre las computadoras y el servidor.

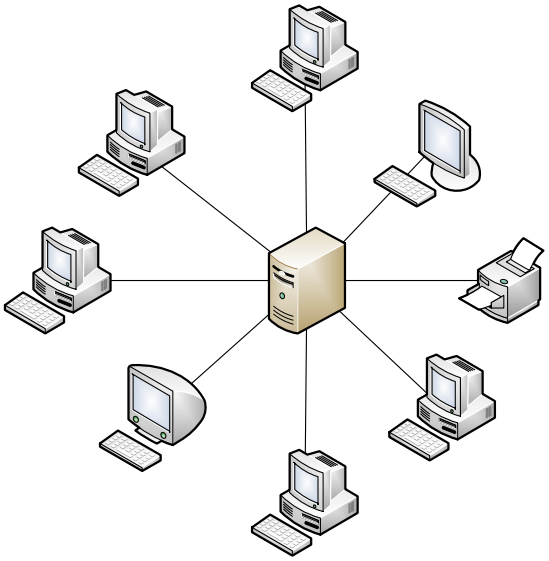

Figura 9. Topología de Estrella.
Fuente: Elaboración Propia.

Topología de anillo: en esta topología, todas las computadoras o estaciones de trabajo están conectadas entre sí formando un anillo, lo que significa que cada estación tiene conexión con otras dos. Los datos viajan de estación en estación en una sola dirección, es decir, que los mensajes pasan por todas las computadoras hasta llegar a su destino final. Sin embargo cada estación recibe el mensaje que va dirigido a ella y retransmite los mensajes que tienen otra dirección.

Este tipo de red permite aumentar o disminuir el número de equipos que conforman la red. Su velocidad de respuesta decrece si el flujo de información aumenta, lo que significa que entre más computadoras usen la red, más lenta se volverá. Es un tipo de red apropiada para el sector industrial. Una falla en el servidor, afecta toda la red; pero una falla en una computadora no afecta a la red.

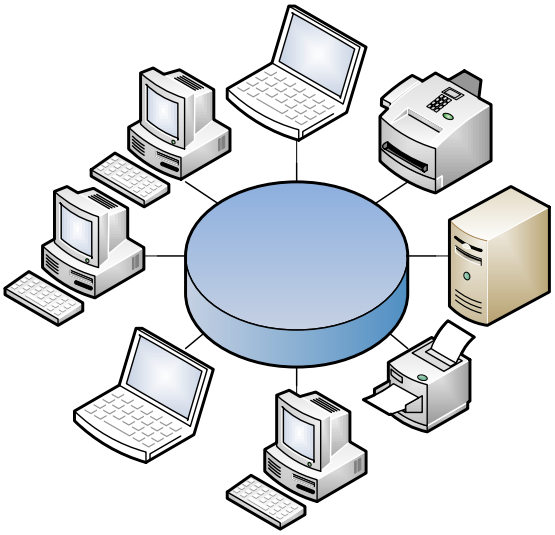

Figura 10. Topología de anillo.
Fuente: Elaboración Propia.

II.3.2 Componentes de una Red

Según Herrera (2003), son los elementos de cómputo que integran cualquier tipo de red.

Elementos básicos de una red

Servidor: es el sistema de cómputo central, el cual posee un software especializado que otorga el acceso a los usuarios de la red. El servidor debe tener un disco duro lo suficientemente grande para guardar el sistema operativo de la red, las aplicaciones y archivos de los usuarios.

Los servidores pueden ser de varios tipos: el *servidor de archivos* mantiene a estos en subdirectorios privados que se pueden compartir con los usuarios de la red; el *servidor de impresoras* al cual se le conectan las impresoras que comparte en la red y el *servidor de comunicaciones* el cual permite la comunicación entre usuarios de la red.

Estaciones de trabajo (ET) o computadoras: constituidas por los sistemas de cómputo de los usuarios que comparten los recursos del servidor. Los sistemas de cómputo que se utilizan en las ET dependen de las aplicaciones que se ejecuten en la red.

Tarjeta de interfaz de red (NIC): para poder conectar la red con el servidor y las ET deben de disponer de una tarjeta NIC. Esta tarjeta debe ser la apropiada para la tecnología que se va a utilizar.

La NIC actúa como interfaz entre la res y las computadoras, que deben cumplir los protocolos apropiados para no generar conflicto entre los nodos y oros dispositivos conectados a la red.

Cableado: es el medio físico a través del cual se realizan las conexiones de cada ET y el servidor. Los cables pueden ser coaxial grueso y delgado, par torcido no blindado y la fibra óptica. Actualmente se habla de cableado estructurado, el cual está formado no solo por el cable sino también por los distintos equipos que se conectan en la red.

Sistema operativo de red: es el conjunto de programas y aplicaciones que permite comunicarse entre sí a las distintas computadoras de una red, y compartir información de manera eficaz y transparente.

Dispositivos de conectividad de una red LAN

Son los dispositivos que permiten la interconexión de distintas redes que se encuentran en una misma estructura o con medios externos de transmisión.

Repetidor: es el dispositivo de conectividad más sencillo. Se encarga de aumentar el alcance de la red, alargando la longitud física del enlace. Es un amplificador y no un enrutador, ya que no posee inteligencia alguna. Opera en la capa física del modelo OSI.

Puente: sistema conformado por hardware y software que permite la conexión de dos LAN distintas. Se encarga de la transferencia de datos entre las redes con bases en direcciones físicas. Este puente trabaja en capa física y de enlace en el modelo OSI. El puente revisa la direcciona asociado a los paquetes y los transfiere al segmento de red que corresponden. Estos puentes ayudan a reducir el tráfico de la red lo que genera un aumento en su rendimiento.

Enrutador: permite conectar redes con distintas topologías, como lo pueden ser Ethernet y Token Ring. Este dispositivo traduce la información de una red a otra. La información es transmitida mediante direcciones lógicas por lo que funciona en la capa de red del modelo OSI. Pueden interconectar redes con diferentes protocolos físicos y de enlaces de datos, ya que la dirección de origen y destino es tomada de la capa de red.

Compuerta (Gateway): puede interconectar varias redes de distintas topologías, protocolos y arquitecturas, ya que puede manejar las siete capas del modelo OSI. La compuerta de emplea en varia aplicaciones, donde las computadoras de distintas marcas y tecnologías deben comunicarse.

Dispositivos de conectividad de una red WAN

Modem: es un dispositivo periférico de computadora el cual la auxilia en sus comunicaciones. Emplea una línea telefónica pública o privada y un software que permite que el modem marque el número telefónico del otro punto de conexión y maneje información para transmitir o recibir datos de otra computadora.

Multiplexor: es un equipo que permite mantener más de una comunicación por una misma línea. Cada comunicación opera como si tuviera una línea exclusiva y puede emplear diferentes protocolos y velocidades.

Concentrador (Hub): es un equipo que permite compartir el uso de una línea entre varias computadoras. Las computadoras conectadas al concentrador pueden utilizar la línea pero no pueden tener diferentes protocolos ni velocidades de transmisión.

II.4 VoIP

II.4.1 Definición de VoIP

La voz sobre IP (VoIP) también es conocida como *Voz Sobre Protocolo Internet,* es una tecnología que permite comunicar señal de voz a través de la red.

Anderrunthy (2007), define VoIP como "es una tecnología que sirve para comunicarse por voz a través de toda red que acepte el protocolo IP utilizado en Internet."

Otra definición de VoIP por Ross (2007) es: VoIP consiste en el uso de redes de datos que utilizan un conjunto de protocolos TCP/UDP/IP para la trasmisión de señales de voz en tiempo real en forma de paquetes.

VoIP convierte la señal de voz analógica a voz digital y comprime la señal a protocolo de Internet (IP) para su transmisión. En la parte de la recepción de llamadas, se realiza el proceso inverso para la conversión de la señal de voz digital a analógica. Al realizar una llamadas, la voz se digitaliza, se comprime y se envía en forma de paquetes de datos IP. Cuando estos paquetes llegan a su destino, son ordenados, descomprimidos y llevados a la señal de voz original.

Las llamadas en VoIP pueden ser:

- PC a PC. Llamadas gratis.
- PC a Teléfono. Llamadas económicas.
- Teléfono a Teléfono. Buena calidad a un buen precio.

El uso de VoIP tiene algunas ventajas, como:

- Con esta tecnología se puede hablar a través de la computadora con otras personas que se encuentren en otra localidad en cualquier parte del mundo, teniendo la llamada, un costo menor al de una llamada local.
- Reduce gastos de desplazamiento, esto a través de videoconferencias y conferencia en línea.
- Actualiza los sistemas telefónicos de acuerdo a las necesidades de la empresa.
- Reduce gastos telefónicos.
- Emplea una sola red para voz y datos, lo que simplifica la gestión.

II.4.2 Arquitectura

La arquitectura en VoIP, desde el punto de vista de su distribución, puede ser centralizada o distribuida. La distribución centralizada es criticada porque al estar todo localizado en un mismo punto, las innovaciones que se quieran realizar se verán entorpecidas; por el contrario, la arquitectura distribuida es más complicada. Sin importar cuál sea la elección de la arquitectura, VoIP permite una gran flexibilidad.

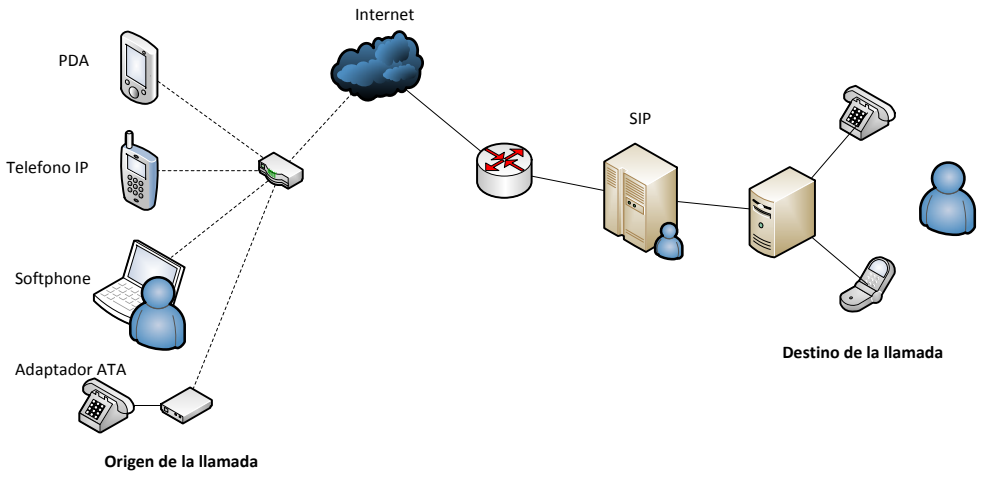

Figura 11. Arquitectura VoIP.
Fuente: Gómez y Gil (2008).

La arquitectura VoIP está compuesta por varios dispositivos, como se muestran a continuación:

Teléfonos IP: son teléfonos similares a los teléfonos tradicionales, con la salvedad que tienen la capacidad de usarse en entornos IP, y son muy importantes en la arquitectura de la VoIP.

Los aspectos que diferencian un teléfono IP de un teléfono tradicional son:

- Al menos poseen un puerto RJ-45[1] a diferencia del RJ-11[2].
- Disponen de una pantalla donde se muestra cierta información.
- Variedad de botones programables.
- Conector de auriculares.

[1] RJ-45: puerto que poseen las computadoras/equipos telefónicos para conectarlos a una red LAN e Internet.
[2] RJ-11: puerto que poseen los equipos telefónicos para su conexión.

Figura 12. Teléfono IP Cisco Small Business SPA303 3 líneas.
Fuente: 2GC S.H. (2012).

A través del puerto RJ-45 los teléfonos IP se conectan a la red (Internet) y se comunican con otros dispositivos basados en IP que se encuentren en la red, como proxy o router VoIP, otro teléfono IP, entre otros más.

Gateway y Adaptadores Analógicos: el adaptador analógico (ATA), convierte la señal analógica empleada en conversaciones, en un protocolo IP. Igualmente puede hacer la conversión inversa de señal digital a señal analógica.

Gómez y Gil (2008), comenta: “estos adaptadores podrían ser descritos como *Gateway*, ya que su función la de pasarela entre el mundo analógico y el IP.”

Dispositivos GSM/UMTS: los teléfonos móviles son empleados para realizar una comunicación de voz o datos conectándose a una radio base de una determinada red de telefonía móvil. Para VoIP, existen gran cantidad de equipos que pueden integrar varias tecnologías, teniendo como ejemplo SIP y GSM. A través de estos dispositivos es posible enviar toda la señalización existente en una red de manera transparente y fiable, aspecto que no se cumplía en la tecnología analógica.

Softphone: son teléfonos implementados por software, permitiendo a computadoras o PDA´s funciones de teléfonos VoIP. Simplemente se

necesita un equipo que posea audio y conexión a una red TCP/IP. Los softphone trabajan bajo diferentes protocolos, como SIP. Presentan una ventaja respecto a los teléfonos IP, es el costo. Esto se debe a que los softphone es un hardware que se instala en las computadoras y así, se evita el gasto de adquirir equipos de teléfonos físicos.

Proxy y Enrutadores: trabajan tal cual como un router con el enrutamiento de datos normales; se en cargan de enrutar la señalización según sea la indicación dada por el protocolo que se emplea.

II.4.3 Señalización y Audio

Protocolos de Señalización

Para garantizar la comunicación entre dos equipos se realice de manera adecuada, es necesario una serie de reglas o normas las cuales se conocen con el nombre de protocolo de señalización.

Para conmutación de paquetes, se tienen varios tipos de protocolos de señalización, entre los cuales se tiene:

SIP (Session Initiation Protocol): es un protocolo de señalización a nivel de aplicación que se encarga del inicio, de la modificación y terminar las sesiones multimedia que se llevan de manera interactiva. En marzo de 1999, SIP se definió en el RFC-2543 por el grupo de MMSC pertenecientes a IETF. Luego, en junio del 2002, el IETF publica una nueva revisión de SIP con el RFC-3261.

Las características del protocolo SIP, se observan en el siguiente cuadro:

Tabla 3. Características del protocolo SIP.

Características	Descripción
Localización del usuario	SIP posee la capacidad de conocer en todo momento la localización de los usuarios. De esta manera no importa en qué lugar se encuentre un determinado usuario. La movilidad de los usuarios no se ve limitada.
Negociación de los parámetros	Posibilidad de negociar los parámetros necesarios para la comunicación: puertos para el tráfico SIP, así como el trafico Medía, direcciones IP para el tráfico Medía, códec, etc.
Disponibilidad de los usuarios	SIP permite determinar si un determinado usuario está disponible o no para establecer una comunicación.
Gestión de la comunicación	Permite la modificación, trasferencia, finalización de la sesión activa. A demás informa del estado de la comunicación que se encuentra en progreso.

Fuente: Gómez y Gil (2008)**.**

Menciona Gómez y Gil (2008), acerca de SIP: “El protocolo SIP es una parte de una arquitectura multimedia, ya que la única finalidad es la de gestionar las sesiones multimedia: iniciarlas, modificarlas, finalizarlas, etc. Sin embargo, se integra perfectamente con otros protocolos como RVSP, RTP o RTSP. Gracias al protocolo SDP se puede formar una completa arquitectura multimedia.”

Las siguientes funcionalidades son soportadas por el protocolo SIP:

- Movilidad de usuarios y terminales.
- Identificaciones de usuarios.
- Se puede utilizar al mismo tiempo con otros protocolos de señalización.
- Llamadas con múltiples interlocutores.
- Servicios suplementarios.

Guitian (2010), menciona que para implementar estas funcionalidades el protocolo SIP tiene varios componentes, entre los cuales están:

Agentes de usuarios (User Agent, AU): son las aplicaciones establecidas en las estaciones terminales SIP. Constan de dos partes distintas, los agentes de usuarios cliente (UAC) y los agentes de usuarios servidores (UAS). Las unidades UAC, son entidades lógicas que generan y reciben solicitudes SIP asociadas al extremo que origina la llamada y las unidades UAS, se encargan de responder las solicitudes y están asociadas al extremo receptor de la llamada.

Servidores de red: los agentes de usuarios pueden establecer la comunicación básica, pero sin los servidores de red, no pueden aprovechar al máximo el protocolo SIP. Estos servidores de red se clasifican en servidores de redirección, de proxy y de registro. Los servidores de redirección procesan las solicitudes SIP y le envían al solicitante la dirección de la parte llamada; los servidores de proxy actúan de intermediarios, respecto al llamante actúa como servidor y respecto al llamado actúa como cliente. Este atiende las solicitudes y las redirige. Finalmente, los servidores de registro son los encargados de registrar las direcciones SIP y sus direcciones IP asociadas.

Los mensajes que se intercambian durante una comunicación SIP son, las solicitudes (métodos) y las respuestas (códigos de estado). En las siguientes tablas se muestran las solicitudes y respuestas que genera SIP.

Tabla 4. Solicitudes SIP.

Solicitudes	Descripción
INVITE	Invita a un usuario a participar en una sesión, iniciar una conversación.
ACK	Confirma el establecimiento de la conversación.
BYE	Finaliza la conexión o comunicación entre dos usuarios.
CANCEL	Cancela peticiones pendientes.
OPTIONS	Solicita información sobre la capacidad de los servidores.
REGISTER	Los usan los clientes para registrar una dirección en el servidor SIP.

Fuente: Guitian (2010)**.**

Tabla 5. Respuesta SIP.

Función	Descripción	Ejemplo
1xx	Informativo. Solicitud recibida, se continua para procesar la solicitud.	180 Repicando
2xx	Solicitud exitosa. La solicitud fue recibida en forma adecuada, comprendida y aceptada.	200 OK
3xx	Redireccionado. Más acciones deben ser consideradas para completar la solicitud.	300 Múltiples Opciones
4xx	Error de cliente. La solicitud contiene mala sintaxis o no puede ser resuelta en este servidor.	403 Prohibido 404 No encontrado
5xx	Error de servidor. El servidor ha errado en una solicitud aparentemente válida	501 No implementado
6xx	Falla global. La solicitud no puede ser resuelta en servidor alguno.	600 Todos ocupados

Fuente: Guitian (2010)**.**

Guitian (2010), habla de las cabeceras como: Las cabeceras (campos) SIP especifican aspectos referentes a los participantes, trayectos, etc. El número

total de cabeceras SIP definidas es de 46, entre las cuales, las más significativas son las siguientes:

- Call-ID: identifica unívocamente una llamada. Esta cabecera es utilizada para varios propósitos como detectar duplicados de solicitud INVITE o cambiar dinámicamente parámetros de una sesión.
- Cseq: identifica cada solicitud.
- From: identifica el origen de la solicitud. Contiene la dirección de origen y posiblemente el nombre de éste.
- To: identifica el destino de cada solicitud. Debe estar presente en todos los mensajes de solicitudes y respuestas.
- Vía: se emplea para registrar la ruta de la solicitud.

H.323: este protocolo fue diseñado por la ITU en 1996. Es un estándar en la transmisión de audio, video y datos en las redes IP que no cuentan con garantía en la calidad del servicio. Este estándar ofrece control y señalización de la llamada, control y transporte multimedia, control del ancho de banda punto a punto y conferencias.

La señalización de este protocolo es muy rápida, esto es porque el formato de los mensajes en H.323 es binario. El diseño sigue mucho la filosofía que sigue el diseño de la PSTN, simplicidad y alta disponibilidad.

El protocolo H.323 incluye el protocolo H.225 para empaquetar, sincronizar e iniciar llamadas mediante la señalización Q.931. H.245 se usa para la negociación como para el manejo de los canales lógicos y, T.120 y T.38 son utilizados para datos y fax.

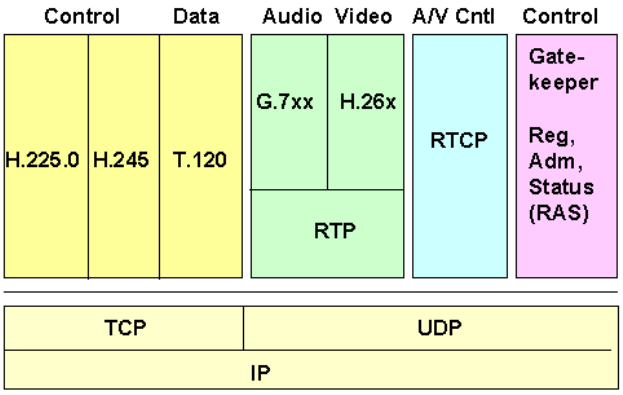

Figura 13. Protocolo H.323.
Fuente: Pouseele (2002).

Protocolos de Audio

Para el establecimiento de una comunicación es necesario un protocolo que transporte la información entre un origen y su destino y proveer las técnicas necesarias que se presentan durante el intercambio, como retardos, jitter y otros más.

Los protocolos más empleados para el transporte de audio y video son:

Real Time Protocol (RTP): definido en el RFC3550 y transporta el audio y video en tiempo real. Emplea UDP como protocolo de transporte y no TCP, ya que su control de flujo y congestión generarían retardo durante la comunicación.

RTP hace uso de un número de secuencia, marcas de tiempo, envío de paquetes sin retransmisión, identificación del origen, identificación del contenido, sincronización, etc., lo que le permite en presencia de pérdidas, jitter o retardo poder continuar con la reproducción del flujo de paquetes. Esto no garantiza que la entrega de tráfico se haga en tiempo real, aunque sí garantiza al menos que lo hará de forma sincronizada.

Real Time Control Protocol (RTCP): es el protocolo compañero de RTP y se encarga de monitorizar el flujo de los paquetes RTP. Se relaciona con la

calidad de servicio, monitoreando la calidad de servicio RTP pero no posee mecanismo de reserva de ancho de banda o control de congestión para paliar una situación en la que la calidad de servicio no es suficiente.

Codecs

Un codificado - decodificador, es un algoritmo que traduce la señal analógica a señal digital, siendo un aspecto importante cuando se elige un códec el tamaño al codificar la onda analógica. Después de finalizar la codificación, si el tamaño es grande la compresión del codec será baja, presentando una buena fidelidad en sonido digital pero requiriendo un anche de banda mayor para la transmisión. Ahora bien, si el tamaño es pequeño al finalizar la codificación, la razón de compresión es alta, lo que implica que la fidelidad del sonido analógico no es buena y no se requiere un ancho de banda tan grande como en el caso anterior.

Para Gómez y Gil (2008), los codecs de audio para la telefonía se dividen en: "basados en *pulse code modulation* (PCM) y los que reestructuran la representación digital de PCM en formatos más livianos."

Según Guitian (2010), los codec de audio se caracterizan por los siguientes parámetros:

Número de canales: un flujo de datos codificados puede contener una o más señales de audio. Para el caso de la telefonía la voz se transmite por un único canal, es decir, se trata de una audición "mono".

Frecuencia de muestreo: se refiere al criterio de Nyquist, que determina la frecuencia máxima que se puede codificar. Por lo tanto, cuanto mayor sea la frecuencia de muestreo, mayor será la fidelidad del sonido obtenido respecto a la señal de audio original.

Número de bits por muestra: determina la precisión con la que se reproduce la señal original.

MOS: Indica la calidad general del codec. Es una medida subjetiva comprendida entre 1 y 5, siendo 5 la mejor calidad. Es determinado estadísticamente basándose en las opiniones de un gran número de personas escuchando la misma llamada.

II.5 Seguridad en VoIP

La Telefonía IP ha venido incrementando su uso y comercialización mucho en los últimos años, abarcando gran parte del mercado en las telecomunicaciones a nivel mundial. Junto a este crecimiento, aumentan las preocupaciones por la seguridad de las telecomunicaciones y la Telefonía IP. VoIP se apoya en capas y protocolas ya existentes de las redes de datos, por lo que heredan los problemas que estos contienen.

Estas redes IP, poseen una arquitectura abierta con lo cual le dan paso o acceso a las vulnerabilidades, amenazas y riesgos; en especial a los hackers. Al hacer uso de una red, la cual es compartida por más usuarios y millones de aplicaciones, hace que la Telefonía IP se vuelva vulnerable.

Figura 14. Piramide de Seguridad en VoIP.
Fuente: Guitierrez Gil (2013).

Otro aspecto importante y el cual es amenazado, son los datos que se transmiten en las llamadas. Estos datos pueden ser interceptados, robados o modificados con el fin de alterar las llamadas que se realizan o reciben, modificar las llamadas o manipular los datos de la misma para realizar acciones hostiles e ilegales.

En la siguiente tabla, Gutiérrez Gil (2013) destaca algunos de los puntos débiles y ataques que afectan a cada una de las capas:

Tabla 6. Ataques y amenazas a las capas de la Pirámide de Seguridad de VoIP.

Capa	Ataques y Vulnerabilidades
Políticas y Procedimientos	Contraseñas débiles. Ej: Contraseña del VoiceMail. Mala política de privilegios. Accesos permisivos a datos comprometidos.
Seguridad Física	Acceso físico a dispositivos sensibles. Ej: Acceso físico a un gatekeeper. Reinicio de máquinas. Denegación de servicios.
Seguridad de Red	DDoS. ICMP unreachable. SYN floods. Gran variedad de floods.
Seguridad en los Servicios	SQL injections. Denegación de DHCP. DoS.
Seguridad en el S.O	Buffer overflows. Gusanos y virus. Mala configuración.
Seguridad en la Aplicaciones y protocolos de VoIP	Fraudes. SPIT (SPAM). Vishing (Phising). Fuzzing. Floods (INVITE, REGISTER, etc). Secuestro de sesiones (hijacking). Intercepción (Eavesdroping). Redirección de llamadas (CALL redirection). Reproducción de llamadas (CALL replay).

Fuente: Gutiérrez Gil (2013)

Para el atacante, no solo es importante la llamada telefónica, sino también los datos que van en ella, los cuales puede interceptar, modificar, reenviar en forma de SPAM, robar la identidad, reproducir conversaciones, entre otros más; en otras palabras, degradar o anular la calidad de servicio (QoS).

Para Mendillo (2013 c), “la seguridad VoIP entonces no consiste sólo en proteger la confidencialidad, sino también la integridad, autenticidad y disponibilidad”.

Confidencialidad: la información no puede ser manipulada por personas extrañas.

Integridad: la información llegue a su destino sin ser alterada o modificada de manera intencional.

Autenticidad: la información provenga de una fuente genuina, y no pasar por nueva, una información vieja.

Disponibilidad: las personas autorizadas puedan manejar la información y recursos y que los equipos y redes trabajen eficientemente para evitar grandes congestiones.

II.5.1 Clasificación de los Ataques

La gran mayoría de los riesgos y ataques son en las capas en que se maneja la tecnología IP. Gutiérrez Gil (2013), clasifica las amenazas de las redes de Telefonía IP de la siguiente manera:

Accesos desautorizados y fraudes

Una de las amenazas más significativa, es el fraude debido a accesos desautorizados en redes VoIP. Los usuarios que llevan a cabo estas acciones, por lo general realizan llamadas ilegales y a larga distancia, destacando las llamadas internacionales. Estas acciones se practican en su mayoría en las empresas.

Explotando la red subyacente

Una de las principales debilidades de la tecnología VoIP, es que se apoyan en las redes IP, las cuales sufren de muchos ataques. Los ataques son denegación de servicios, inundación de paquetes u otros que afectan la disponibilidad de la red.

La intercepción o *eavesdropping*, es la captura por parte del intruso de información (cifrada o no) que no va dirigida a él. En VoIP, es la intercepción de las conversaciones al cual no va dirigida. Para la intercepción de datos, eavesdropping presenta diferencias ante redes tradicionales. En VoIP puede diferenciar entre la señalización y el flujo de datos. En señalización, se centra en el protocolo SIP, mientras en el flujo de datos se utiliza el protocolo RTP sobre UDP.

Ataques de denegación de servicios

Estos ataques buscan degradar el rendimiento de la red o sistema, impidiendo en algunos casos, que usuarios legítimos puedan utilizar los mismos. Los ataques se realizan a través del envío de paquetes construidos para explotar algunas de las vulnerabilidades del software o hardware del sistema, sobrecargar los procesos en los dispositivos o saturar el flujo de datos.

Los DDoS o ataques de denegación distribuidos, son muy dañinos y se realizan desde múltiples computadoras de una manera organizada. La principal razón, es la dependencia y necesidad de garantías en la calidad de servicios. La existencia de dispositivos que presentan funciones específicas, se ven afectados cuando cualquier dispositivo de la red es atacado.

Como las aplicaciones y dispositivos de Telefonía IP trabajan sobre ciertos puertos específicos, bombardear estos puertos con tráfico innecesario, puede causar denegación de servicios originando que usuarios legítimos no puedan hacer uso del servicio. En redes VoIP basadas en protocolo SIP, se

pueden enviar mensaje como CANCEL, GOODBYE o ICMP Port Unreacheable, con el fin de desconectar usuarios de las llamadas o evitar que la misma se realice. Se destaca también, que en ocasiones VoIP es vulnerable a ataque de fragmentación IP o envío de resets TCP, lo que origina el fin de la llamada antes de lo debido.

Ataques a los dispositivos

Actualmente mucho de los ataques que realizan los hackers y crackers van dirigidos al hardware y software de los dispositivos, por lo que los Gateway, call manager, proxy servers y teléfonos IP son potencialmente objetivos de ataques.

Un ataque muy común es *fuzzing,* el cual es un paquete mal formado que provoca cuelgues y reboots cuando este paquete es recibido. Otro ataque de denegación de servicios es *flooders* sus objetivo son los puertos de servicios y puertos abiertos de dispositivos VoIP. Una mala configuración también es un punto débil dentro de las redes. Al trabajar con la configuración por defecto, los dispositivos presentan gran cantidad de puertos abiertos en los cuales corren los servicios por defectos y son vulnerables a ataques de DoS u otros ataques que comprometan a los dispositivos VoIP. Por esto a la hora del ataque, el intruso se concentra en los puertos y servicios innecesarios, passwords comunes o los que tiene por defecto el dispositivo.

Descubriendo objetivos

Cuando el hacker selecciona su objetivo, se encarga de obtener la mayor información posible de la víctima. Al poseer ya la información, elige el método de ataque.

Algunos de los métodos de obtención de información son los siguientes:

- *Footprintng*. Es el proceso de acumulación de la información de un entorno de red específico, con el fin de buscar como entrar en el entorno. A través de Google, los hackers pueden obtener mucha

información sobre las víctimas, perfiles y direcciones de contacto, correos electrónicos y teléfonos.

- *Escaneado*. Obteniendo la dirección IP de la víctima, se puede tener acceso a la información de la misma. Una herramienta que puede escanear la red es NMAP. Esta herramienta tiene una función que le permite identificar el sistema operativo de la máquina escaneada mediante la información que obtiene de los puertos abiertos, tipos de servicios y huellas identificativas de la pila TCP/IP.
- *Enumeración*. Es una técnica empleada para obtener información sensible que el hacker puede usar para sus ataques posteriores. Primero debe obtener la información del servicio que corre por un puerto determinado. NMAP es una herramienta que puede realizar esta función. Para la realización de los ataques, el intruso debe conocer nombre de usuario y extensiones telefónicas correctas. Un protocolo que se encuentra en los dispositivos VoIP y es vulnerable a ataques, es el protocolo SNMP.

Explotando el nivel de aplicación

Uno de los niveles más atacados en la red IP, es el nivel de aplicación. Esto se debe a que VoIP engloba gran cantidad de protocolos y estándares, los cuales tienen su propio riesgo. Ejemplos de ataques son secuestros de sesión, desconexiones ilegales, generación de paquetes malformados, falsificación de llamadas entre varios más.

- *Autenticación en VoIP.* En VoIP la autenticación es necesario que los dispositivos que van a estar comunicados se autentiquen uno al lado del otro antes de realizar cualquier intercambio de información. Este proceso de autenticación se conoce como priori por los dos.
- *Manipulación de la señalización.* Algunos de los ataques que se pueden producir al capturar y manipular las llamadas son los siguientes: **Suplantación de identidad en el registro**, el registro de

usuario es la primera acción que se realiza entre el usuario y el servidor de registro. Esta comunicación se debe realizar de manera segura y tener garantía que el usuario es quien dice ser por el resto de la sesión. Si un servidor no autentica las peticiones de un usuario, cualquiera intruso puede registrarse como cualquier usuario y secuestrar las llamadas y su identidad. **Desregistrar usuarios,** es una necesidad para conseguir suplantar la identidad de usuarios. Para lograr esto, el intruso debe realizar un ataque de DoS al usuario. Generar constantes peticiones REGISTER que se sobrepongan por las que el usuario legítimo realiza. Desregistrando al usuario con mensajes REGISTER. **Desconexión de usuarios,** el intruso puede desconectar a los usuarios de las llamadas enviando mensajes BYE con la identidad falsificada, simulando ser el usuario del otro lado de la línea. **Redirección de llamadas,** es uno de los ataques más comunes en las redes VoIP. Existen varios métodos que van desde comprometer los servidores y redirigir la llamada a donde la desee el intruso, hasta la suplantación de identidad en el registro.

- *Manipulación de la transmisión.* A través de la técnica de comunicación o eavesdropping se puede manipular la información de los usuarios. **Inserción de audio,** la transmisión del flujo de datos en las llamadas VoIP se realizan sobre el protocolo UDP, debido a su eficiencia y sencillez. Sin embargo, este protocolo no da garantía en la entrega de sus mensajes y no tiene información de estado o conexión. Por esto la inserción de paquetes UDP extraños dentro de un flujo legítimo puede llegar a ser trivial. El protocolo RTP es el que transporta los datos de voz, y se encuentra encapsulado dentro de UDP. Este último, tampoco tiene un control exhaustivo sobre el flujo de datos por lo que le otorga las funciones de recuento de paquetes y calidad de servicio al protocolo RTCP.
- *Fuzzing.* También conocido como testeo funcional del protocolo, es de los mejores métodos para la identificación de errores y agujeros de

seguridad. Crea paquetes mal formados para ir más allá de las especificaciones del protocolo. Su función, comprobar como manejan los dispositivos, la aplicaciones o el propio sistema operativo que implementa el protocolo, situaciones que terminan por lo general en un error, denegación de servicio o una vulnerabilidad más grave.

Ingeniería social

- *SPIT: Spam over Internet Telephony.* El spam también es un problema que afecta a la Telefonía IP, y el cual se conoce como SPIT. Es una técnica poco empleada pero las redes VoIP son vulnerables al envío de mensajes de voz basura, teniendo un impacto mayor que el spam tradicional.
- *Vishing: VoIP Phishing:* esta técnica también afecta a la Telefonía IP. El intruso puede realizar llamadas desde cualquier parte del mundo a teléfonos IP y con las técnicas de ingeniería social y suplantando la identidad, puede obtener información de cualquier tipo. Al igual que SPIT, posiblemente el número de incidentes de este tipo aumente en años venideros.

II.6 Herramientas para el desarrollo de las actividades

Existen gran cantidad de herramientas con las cuales se pueden llevar a cabo las actividades u objetivos que se plantean los trabajos de investigación. Estas herramientas tienen su alcance y objetivo específico para la cual pueden ser empleados.

Análisis Modal de Fallos y Efectos (AMFE): FUNDIBEQ (2010), define AMFE como: “es una herramienta de análisis identificación, evaluación y prevención de los posibles fallos y efectos que pueden aparecer en un producto/servicio o un proceso.”

Es de carácter preventivo porque se anticipa a los posibles fallos, previniendo problemas que se presenten. El enfoque estructurado que se le da asegura considerar todos los posibles fallos, lo que le da un carácter sistemático. Finalmente, es participativo porque requiere del aporte de todos los conocimientos de las áreas afectadas.

Para FUNDIBEQ (2010), los tipos de AMFE son:

Un producto o servicio (AMFE de producto). Sirve como herramienta de optimización para su diseño.

El proceso que permite la obtención del producto o prestación del servicio (AMFE de proceso). Sirve como herramienta de optimización antes de su traspaso a operaciones.

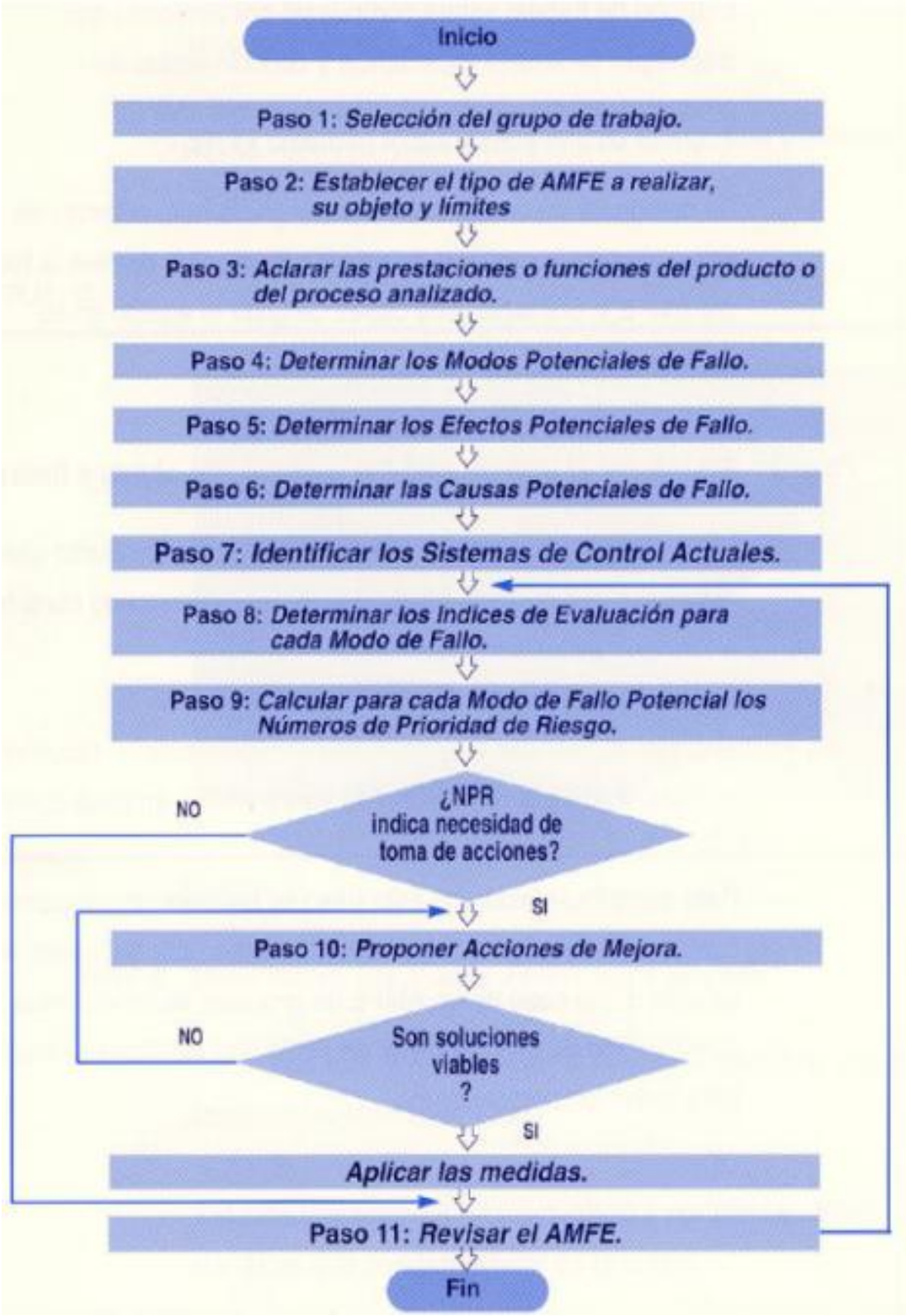

Figura 15. Diagrama de flujo AMFE.
Fuente: FUNDIBEQ (2010).

Capitulo III. Marco Metodológico

A continuación se presenta la metodología de investigación para el desarrollo del presente trabajo. A demás, se puede encontrar el tipo de investigación que se está realizando, el diseño del estudio, las etapas de la investigación, la unidad de análisis, el cronograma y las consideraciones éticas.

III.1 Disposiciones Generales

Referente a las Disposiciones Generales Campagnaro y Sandoval (2010), comenta: “El trabajo especial de grado se concibe dentro de la modalidad de investigación cuyo objetivo fundamental es el de aportar soluciones a problemas y satisfacer necesidades teóricas o prácticas, ya sean profesionales, de una institución o de un grupo social. Se pretende que el alumno demuestre el dominio instrumental de los conocimientos aprendidos en la especialización, para lo cual el tema elegido por el estudiante deberá insertarse en una de las materias del plan de estudios correspondientes.”

III.2 Tipo de Investigación

El tipo de investigación en la cual se desarrolla el presente trabajo es *investigación aplicada.* Pertenece a este tipo de investigación ya que se busca materializar los conocimientos adquiridos en el área, con los cuales se analizan y generan diagnósticos sobre la situación tecnológica de la empresa en cuestión, y que buscan ser mejorados a través de alternativas que den solución a los problemas presentes.

La investigación aplicada se fundamenta en aportes específicos, en la investigación científica que cuentan con teoría y antecedentes que sustentan el desarrollo del presente trabajo.

“La investigación aplicada, además de generar conocimiento, busca soluciones aceptables y pertinentes a un fenómeno social determinado.” Valarino et al (2010).

Este tipo de investigación cuenta con una tipología según sea su propósito: investigación y desarrollo, investigación evaluativa e investigación y acción.

El presente trabajo pertenece investigación y acción. Valarino et al (2010), la define como:

“Su propósito es investigar la condición actual y condición deseada de un grupo, equipo, proyectos, programas, unidades o la organización en su conjunto, para luego realizar intervenciones que conduzcan al mejoramiento de gestión para lograr la condición deseada.”

III.3 Diseño del Estudio

El diseño es tipo documental, porque los datos e información con que se trabaja proviene de documentos (revistas, libros, trabajos de grados, publicaciones) que son materiales impresos.

De igual manera el trabajo se centra en un estudio de campo, ya que se realizaron consultas y entrevistas a una selección de expertos en el área de Seguridad de la Información y Telecomunicaciones.

La investigación de campo es “la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna”. Arias (2006).

El diseño se realizara en las siguientes fases p procedimientos por objetivos:

Identificar fallas y vulnerabilidades en los actuales sistemas de seguridad en las redes de información: primeramente se identificaran los sistemas de seguridad informática y física con que cuenta la compañía en

cuestión, luego a través de la herramienta AMFE, se realiza un estudio en el cual se identificaran las fallas y/o vulnerabilidades, los puntos críticos, las probabilidades de ocurrencia de una falla que presenten estos sistemas.

Identificar fallas y vulnerabilidades en los actuales sistemas de telecomunicaciones: primeramente se identificaran los sistemas de telecomunicaciones con que cuenta la compañía en cuestión, luego a través de la herramienta AMFE, se realiza un estudio en el cual se identificaran las fallas y/o vulnerabilidades, los puntos críticos, las probabilidades de ocurrencia de una falla que presenten estos sistemas.

Evaluación de la tecnología a un nuevo sistema de seguridad y de telecomunicaciones: Migrar hacia una nueva tecnología en la cual pueda subsistir en un mismo sistema voz, datos y video representa un gran avance tecnología para la empresa a la cual se está desarrollando el presente proyecto. Para destacar los aspectos positivos, en especial las ventajas de migrar hacia una nueva tecnología "Telefonía IP (VoIP)", se harán cuadros comparativos entre las características de la tecnología actual con la nueva tecnología a implementar, donde se destacarán las ventajas de esta última y darán sustento al desarrollo del presente proyecto.

Proponer la solución técnica idónea para el sistema de seguridad y de telecomunicaciones: Para poder seleccionar la opción más adecuada primero se deben estudiar cada una de las alternativas, destacando los aspectos positivos y negativos de cada una. Estas comparaciones se pueden realizar a través de cuadros comparativos donde se mencionan los aspectos que se deseen destacar. Es importante que también analizar otros aspectos externos que pueden influir en la selección de la propuesta. Estos aspectos externos son las condiciones que plantea el centro comercial para la ejecución de las propuestas.

III.4 Etapas de la Investigación

Como se mencionó con anterioridad, el presente trabajo pertenece a un tipo de investigación-acción; ofreciendo alternativas, propuestas, soluciones a situaciones irregulares dentro de la empresa a la cual va dirigido el presente trabajo.

Las etapas que se sugieren para este tipo de investigación son cuatro, la cuales son:

Investigación. Primeramente se estudia y analiza la situación actual de los sistemas de seguridad y telecomunicaciones que posee la empresa de transporte marítimo. El estudio de esta situación se hace de manera exhaustiva y detallada para poder obtener la mayor información posible. Los sistemas actuales, configuración de los mismos, protocolos empleados, equipos empleados que integrarán un diagnóstico inicial de la empresa.

Visualización. Se tiene una visión sobre que se quiere modelar, a donde se quiere llegar, cual es la condición final e idónea a lograr. Se presentan las características, equipos, protocolos, sistemas, reglas, normas que mejor se adapten a la condición final. Para llegar a este punto, se debe trabajar en conjunto todos los aspectos y áreas comprometidas, y así entre ellas, ir armando la condición final deseada.

Suposición. Se presentan una serie de alternativas, propuestas, soluciones a los problemas existentes dentro de la empresa. Se debe tomar en cuenta que para lograr cada alternativa, propuesta o solución, se deben cumplir con normas y lineamientos que pueden ser puntos de traba a la hora de realizar la elección. Estas trabas no solo son de carácter físico, administrativo, económico, sino también legal, ya que se debe regir bajo las condiciones que propone el condominio del centro comercial donde se ubica la oficina de la empresa en cuestión. Para lograr presentar la propuesta final, se debe pasar por cada fase de diseño de la investigación.

Acción o Diseño. Diseño e implementación de la solución. Se destacan los cambios que se efectuaron y cuáles son sus posibles consecuencias, de esta manera se evaluará el cumplimiento de la situación deseada. Para el presente trabajo, aparte de implementación se realizará en un futuro, ya que el alcance del mismo no contempla implementarlo.

III.5 Unidad de Análisis

Para el desarrollo del presente trabajo participan varios recursos que son los que dan vida a la ejecución del mismo. Cuando se habla de recurso, se refiere recursos humanos, recursos tecnológicos y materiales, recursos financieros; que son los principales actores dentro del presente trabajo.

Estos recursos deben estar bien identificados porque algunos de ellos son limitantes a la hora de la ejecución del proyecto.

Los costos financieros para realizar el presente trabajo son:

Costo Unidad por Crédito	600 Bs.
Unidades de Crédito	12 Cr.
Sub-Total	*7200 Bs.*
% a cancelar	40%.
Total	*2880 Bs.*

Otro recurso que maneja es el tiempo u horas, el cual es empleado en investigación, recolectar información, analizar la situación de la empresa, reuniones con el asesor/tutor.

Lograr el cumplimiento de estas tareas, llevando un control de las horas empleadas para cada una de ellas, se realiza una tabla de plan de tareas que ayuda a la planificación y organización del presente trabajo. Esta tabla se elabora en función a doce (12) semanas. El cumplimiento de las tareas va

relacionada con la tabla 6, según la semana que le corresponda. Las horas empleadas son semanales.

Tabla 7. Plan de Tareas

Tareas	Tiempo estimado (horas x semana)	Producto
Investigar sobre tema a realizar	6	Obtener tema a desarrollar
Investigación bibliográfica	6	Información sobre el tema de investigación
Planteamiento del problema	4	Se define el problema a solventar
Marco Teórico	6	Se plasma la teoría que sustenta la investigación
Marco Metodológico	4	La metodología a través de la cual se desarrollará el proyecto
Desarrollo	8	La ejecución del proyecto
Conclusiones/Recomendaciones	4	Resultados
Revisión	4	Acomodar posibles fallas en el desarrollo
Presentación	2	Entrega proyecto

Fuente: Elaboración Propia.

III.6 Cronograma

Se presenta el cronograma de ejecución de la presente propuesta de investigación que se seguirá para culminar con éxito el resto de los capítulos en base a la metodología planteada y lograr así el objetivo central de la investigación.

Tabla 8. Cronograma de Actividades.

Semanas/Tareas	1	2	3	4	5	6	7	8	9	10	11	12
Investigar sobre tema a desarrollar												
Buscar información bibliográfica												
Planteamiento del problema												
Marco Teórico												
Marco Metodológico												
Desarrollo												
Conclusiones/Recomendaciones												
Revisión												
Presentación												

Fuente: Elaboración Propia.

III.7 Consideraciones Éticas

Colegio de Ingenieros de Venezuela (2012), en el Código de Ética Profesional del Colegio de Ingenieros (CIV), considera contrario a la ética profesional lo siguiente:

1ro. (virtudes): Actuar en cualquier forma que tienda a menoscabar el honor, la responsabilidad y aquellas virtudes de honestidad, integridad y veracidad que deben servir de base a un ejercicio cabal de la profesión.

2do. (ilegalidad): Violar o permitir que se violen las leyes, ordenanzas y reglamentaciones relacionadas con el cabal ejercicio profesional.

3ro. (conocimiento): Descuidar el mantenimiento y mejora de sus conocimientos técnicos, desmereciendo así la confianza que al ejercicio profesional concede la sociedad.

4to. (seriedad): Ofrecerse para el desempeño de especialidades y funciones para las cuales no tengan capacidad, preparación y experiencias razonables.

5to. (dispensa): Dispensar, por amistad, conveniencia o coacción, el cumplimiento de disposiciones obligatorias, cuando la misión de su cargo sea de hacerlas respetar y cumplir.

6to. (remuneración): Ofrecer, solicitar o prestar servicios profesionales por remuneraciones inferiores a las establecidas como mínimas, por el Colegio de Ingeniero de Venezuela.

7mo. (remuneración): Elaborar proyectos o preparar informes, con negligencia o ligereza manifiestas, o con criterio indebidamente optimista.

8vo. (firma): Firmar inconsultamente planos elaborados por otros y hacerse responsable de proyectos o trabajos que no están bajo su inmediata dirección, revisión o supervisión.

9no. (obras): Encargase de obras, sin que se hayan efectuado todos los estudios técnicos indispensables para su correcta ejecución, o cuando para la realización de las mismas se hayan señalado plazos incompatibles con la buena práctica profesional.

10mo. (licitaciones): Concurrir deliberadamente o invitar, a licitaciones de Estudio y/o proyectos de obras.

11ro. (influencia): Ofrecer, dar o recibir comisiones o remuneraciones indebidas y, solicitar influencias o usa de ellas para la obtención u otorgamiento de trabajos profesionales, o para crear situaciones de privilegio en su actuación.

12do (ventajas): Usar de las ventajas inherentes a un cargo remunerado para competir con la práctica independiente de otros profesionales.

13ro. (reputación): Atentar contra la reputación o los legítimos intereses de otros profesionales, o intentar atribuir injustificadamente la comisión de errores profesionales a otros colegas.

14to. (intereses): Adquirir intereses que, directa o indirectamente colindan con los de la empresa o cliente que emplea sus servicios o encargases sin conocimiento de los interesados de trabajos en los cuales existan intereses antagónicos.

15to. (justicia): Contravenir deliberadamente a los principios de justicia y lealtad en sus relaciones con clientes, personal subalterno y obreros, de manera especial, con relación a estos últimos, en lo referente al mantenimiento de condiciones equitativas de trabajo y a su justa participación en las ganancias.

16to (el ambiente): Intervenir directa o indirectamente en la destrucción de los recursos naturales u omitir la acción correspondiente para evitar la producción de hechos que contribuyen al deterioro ambiental.

17mo. (extranjeros): Actuar en cualquier forma que permita o facilite la contratación con profesionales o empresas extranjeras, de estudios o proyectos, construcción, inspección y supervisión de obras, cuando a juicio del Colegio de Ingenieros, exista en Venezuela la capacidad para realizarlos.

18vo. (autoría): Utilizar estudios, proyectos, planos, informes u otros documentos, que no sean el dominio público, sin la autorización de sus autores y/o propietarios.

19no. (secreto): Revelar datos reservados de índole técnico, financiero o profesionales, así como divulgar sin la debida autorización, procedimientos, procesos o características de equipos protegido por patentes o contratos que establezcan las obligaciones de guardas de secreto profesional. Así como utilizar programas, discos, cintas u otros medios de información, que no sea de dominio público, sin la debida autorización de sus autores y/o propietarios,

o utilizar sin autorización de códigos de acceso de otras personas, en provecho propio.

20mo. (experimentación y servicios no necesarios): Someter a su cliente o a su empleador a la aplicación de materiales o métodos en experimentación, sin su previo y total conocimiento y aprobación o recomendarle servicios no necesarios.

21ro. (publicidad indebida): Hacer o permitir cualquier publicidad no institucional, dirigida a atraer al público hacia la acción profesional, personal o participar en programas de televisión, radio u otros medios, que no tengan carácter divulgativo profesional, o que en cualquier forma, ateten contra la dignidad y seriedad de la profesión. Así como, valerse de posición para proferir declaraciones en los medios o hacer propaganda de materiales, equipos y tecnologías.

22do. (actuación gremial): Incumplir con lo dispuesto en las “Normas de Actuación Gremial del CIV”.

Capitulo IV. Marco Referencial

IV.1 Información de una empresa de transporte marítimo

La empresa de transporte marítimo a la cual va dirigido el presente proyecto, es la representante en Venezuela de una empresa multinacional con varias oficinas a nivel mundial. Es una sociedad mercantil que representa, promueve y mercadea bienes y servicios relativos al transporte marítimo y de manera especial todo lo relativo a las actividades de fletamento marítimo de hidrocarburos y minerales. Su actividad económica es el shipping o servicio de transporte marítimo, trabajando principalmente con el flete de petróleo, gas y minerales. Cuenta con una nutrida cartera de clientes nacionales e internacionales. En Venezuela, el mayor cliente es una empresa del estado, con el cual se mantiene una estrecha relación de trabajo. Actualmente la oficina se encuentra ubicada en un reconocido centro comercial, en la ciudad de Caracas.

Es una empresa que cumple la función de *Broker*. Son los intermediarios entre el cliente que necesita del producto y el que suministra. El cliente en base a sus requerimientos de transporte o fletamento marítimo, solicita en comunicación vía correo electrónico y/o telefónicamente los servicios. Y es un mercadeo en base a las características de la unidad marítima que se requiera para el transporte de los hidrocarburos o minerales.

Una definición de Broker, es: “El papel de la empresa cuando actúa como agente para un cliente y cobra al cliente una comisión por sus servicios. ” Investopedia (2012).

La comunicación entre las distintas partes que actúan en la negociación debe ser lo más clara y precisa, y sobre todo, de una manera rápida y eficiente y así, poder finiquitar la transacción a realizar. Para cumplir estos aspectos los canales o vías de comunicación, sean equipos telefónicos, sistemas de comunicación e infraestructura, deben estar actualizados,

equipos de última generación que soporten altas cargas de transferencia de datos y presten una comunicación acorde a la necesidad.

Dentro de la oficina, las actividades que constantemente se están realizando son: llamadas telefónicas nacionales e internacionales, tanto a equipos fijos como móviles, video conferencias, teleconferencias y reuniones presenciales, envío y recepción de faxes, navegación en la web. Muchas de estas actividades son con otras sedes a nivel mundial o con clientes/proveedores, lo que amerita que los canales de comunicación estén funcionando óptimamente. También se maneja en gran parte el contacto con público, ya que se recibe la facturación de los distintos proveedores y clientes como también personas que van reunirse con un empleado, jefe y/o director.

IV.2 Organización de la Empresa

El organigrama de la empresa de conformidad con el acta constitutiva y sus reformas está integrado de la siguiente manera:

Presidente – Vicepresidente – Director - que son integrantes de la junta directiva. Un administrador, una gerencia de fletamento.

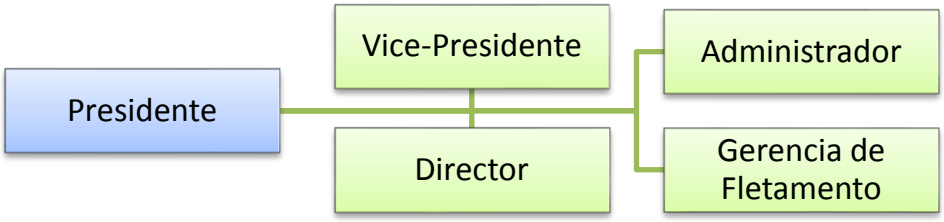

Figura 16. Organigrama de la Empresa.
Fuente: Empresa de Transporte Marítimo.

Luego del Administrador y Gerencia de Fletamento, se encuentra el Departamento Legal, Departamento de Informática y Departamento de Tesorería.

IV.3 Situación Actual

Como se menciona en el Capítulo I, los servicios de telecomunicaciones que posee la empresa de transporte marítimo en cuestión son ofertados a través de un proveedor que no cumple con las expectativas de la empresa, ocasionando problemas en sus labores diarias. En pro de solucionar estos inconvenientes, se han hecho averiguaciones con otros proveedores en telecomunicaciones para adquirir sus servicios, pero los mismos por aspectos, legales, administrativos o burocráticos han sido rechazados o imponiendo reglas o normas que salen de contexto. En vista de esta situación, y en busca de dar solución a estos inconvenientes, se desarrolla el presente trabajo.

Los problemas puntuales que presenta la empresa en cuestión son:

- Los números telefónicos de salida, no concuerdan con los números telefónicos asignados por el proveedor.
- El ancho de banda es poco, por lo que navegar en Internet en ocasiones es lento.
- El acceso a las cámaras de seguridad de manera remota está restringido, porque la dirección IP que otorgan, no permite dicha función.

El costo mensual en servicios de telecomunicaciones (telefonía e Internet) es de aproximadamente 3.300,00 Bs mensuales, lo que no representan un gasto elevado, sin embargo, la empresa en cuestión, busca optimizar sus servicios antes mencionados y está en la disposición de realizar un gasto económico en equipos y servicios, si estos cumplen con sus requerimientos.

La velocidad del enlace de conexión a Internet es de 2048 Kbps, la cual es adecuada para las actividades que se realizan en la empresa, pero al ser compartida con el resto del centro comercial desde su hora de apertura hasta su hora de clausura, hace que la conexión sea muy lenta.

Equipos actuales

Central Telefónica Panasonic KX-TDA30

Figura 17. Central Panasonic KX-TDA30.
Fuente: telavip.com.ve (2013)

Teléfono Panasonic KX-T7633X

Figura 18. Teléfono Panasonic KX-T7633X.
Fuente: Panasonic, S.L (2013)

Teléfono Panasonic KX-TG2810LA y KX-TG2820LA

Figura 19. Teléfono Panasonic KX-TG2810LA.
Fuente: Inversiones Teleiva.com19, C.A (2013)

Figura 20. Teléfono Panasonic KX-TG2820LA.
Fuente: Inversiones Teleiva.com19, C.A (2013)

Switch TP-Link TL-SF1024

Figura 21. Switch TP-Link TL-SF1024.
Fuente: TP-LINK Technologies Co., Ltd (2013)

Patch Panel LANPRO Cat 5e

Figura 22. Patch Panel LANPRO Cat 5e.
Fuente: LanPro (2013)

Router Linksys wrt54g2 v1

Figura 23. Router Linksys wrt54g2 v1.
Fuente: Linksys (2013)

Sistema de Seguridad KOCOM KC-60C

Figura 24. Cámara de Puerta KOCOM KC-60C.
Fuente: KOCOM (2013)

Tarjeta Geovision GV-800

Figura 25. Tarjeta PCI.
Fuente: CompuResale (2013)

Cámaras tipo Domo

Figura 26. Cámara de seguridad tipo domo.
Fuente: CompuResale (2013)

Capítulo V. Análisis de Resultados

Al implementar un nuevo servicio de red, como lo es VoIP, se debe tomar en cuenta muchas características y aspectos técnicos que son esenciales para el buen funcionamiento y calidad de la red. A su vez, estas características y aspectos técnicos deben ajustarse a los requerimientos y necesidades del cliente, por lo que es necesario proponer la arquitectura óptima para la solución.

A continuación se mencionan y describen estas características y aspectos técnicos que pertenece a la solución VoIP.

V.1 Calidad de Servicio (QoS)

La calidad de servicio en VoIP está relacionada con la percepción que tienen los usuarios finales en una conversación telefónica. Cuando el grado de satisfacción no sea el adecuado, es porque existen deficiencias que no permiten las cargas de tráfico de manera puntual o permanente.

Para determinar la calidad de servicios en la red VoIP, se hará uso de la escala MOS (Mean Opinion Score). Consiste en someter a varios individuos a conversaciones, en las cuales evaluarán la claridad con que perciben la conversación.

Las siguientes tablas muestran la evaluación que se la hace a la calidad de voz y el esfuerzo que se realiza para entender el mensaje final.

Tabla 9. Escala MOS para medir la calidad de la voz

Puntuación	Calidad
5	Excelente
4	Buena
3	Aceptable
2	Pobre
1	Mala

Fuente: Elaboración Propia

Tabla 10. Escala MOS para medir el esfuerzo de interpretación del mensaje

Puntuación	Esfuerzo
5	Relajación completa: no se necesita ningún esfuerzo
4	Necesario prestar atención: no se requiere esfuerzo aceptable
3	Esfuerzo moderado
2	Esfuerzo considerable
1	Imposible de entender

Fuente. Elaboración Propia

Factores que intervienen en la calidad de servicio QoS:

V.1.1 Cableado

El cableado que posee la oficina de Transporte Marítimo, se realizó bajo las normas establecidas para *Cableado Estructurado*, ver anexos. Su estructura dentro de la oficina es un cableado horizontal, porque va desde el punto de distribución hasta las distintas estaciones de trabajo. Se respetaron las normas que rigen esta estructura de cableado, como son: ANSI, EIA, TIA, ISO, IEEE.

Se crearon 19 puntos, los cuales cuentan con un punto de conexión a Internet (RJ 45) y otro punto de conexión telefónica (RJ 11) respectivamente. Actualmente se encuentran en uso 16 puntos de datos y telefónicos.

El cable empleado es UTP categoría 5e. Es un cable que puede soportar la tecnología a la cual se desea migrar y posiblemente, no necesita de modificaciones. Sin embargo, es importante un análisis y supervisión del mismo para corroborar su buen funcionamiento y posibles fallas, las cuales deberán ser corregidas para su óptimo funcionamiento.

Otra opción es el cable UTP categoría 6, el cual soporta transmisiones de voz y datos a una velocidad de 1 Gbps. Según como sea la escalabilidad de la red VoIP, el cableado estructurado debería cambiar a categoría 6.

Tabla 11. Diferencia entre cable UTP cat 5e y cat 6

Características	Cable UTP 5e	Cable UTP 6
Frecuencia	100 MHz	250 MHz
Capacitancia	14 pF máxima	14 pF máxima
Impedancia	100 ± 15 Ohms	100 ± 15 Ohms
Diámetro Exterior	5 mm	5,4 mm
Retardo	45 ns	45 ns
Perdida en Retorno	19 db	19db@100MHz15.6db@250MHz

Fuente: Elaboración Propia

V.1.2 Ancho de banda

El ancho de banda establece la velocidad máxima de transferencia de datos entre dos extremos de la red. Este ancho de banda es repartido entre las aplicaciones que hay en la red.

El ancho de banda actual con que cuenta la empresa en cuestión, es de 2048 kbps, perteneciente a un enlace que se comparte con el resto del centro comercial donde se encuentra la oficina, es decir, que en el momento en que los comercios del centro comercial empiezas a trabajar (10 am), la velocidad de navegación en Internet disminuye notoriamente, en comparación a la velocidad que se experimenta cuando el mismo no ha abierto sus puertas al público.

A continuación se muestra las velocidades de navegación en Internet antes de la apertura del centro comercial y luego de su apertura.

A través de la página web http://speedtest.cnt-grms.com.ec/ se puede realizar una prueba que mide el ancho de banda con el cual se cuenta. Los resultados se muestran en las siguientes figuras:

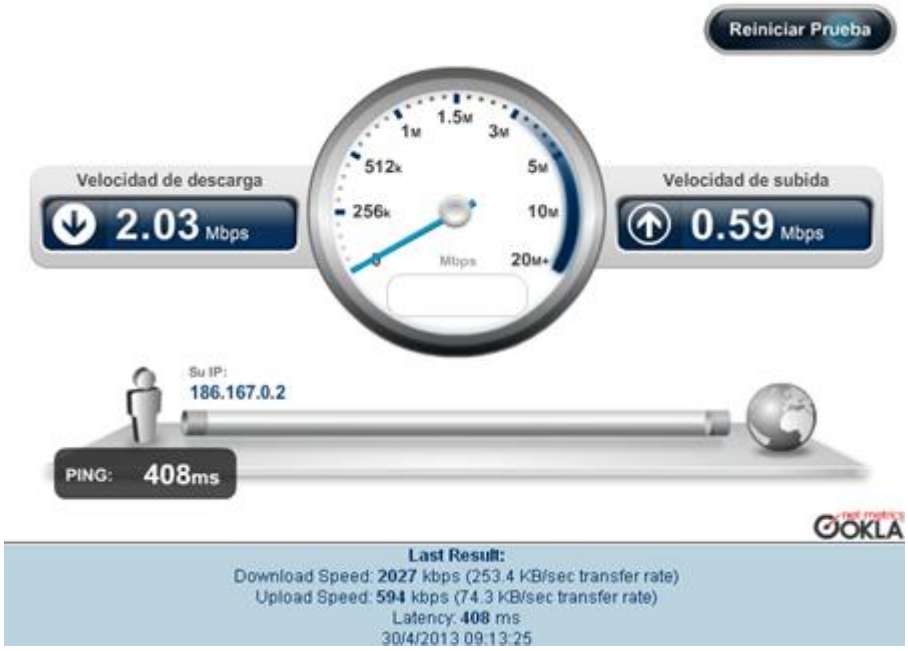

Figura 27. Ancho de banda antes de la apertura del Centro Comercial.
Fuente: CNT (2013)

En la figura 27, se observa que la velocidad de bajada (download speed) 2027 kbps y la velocidad de subida (upload speed) 594 kbps. También se

muestra un retardo (latencia) de 408 ms, el cual es alto. Esta medición se realzó a las 9:13 am, antes de la apertura comercial del centro comercial. Se observa que la velocidad de navegación en Internet es lo suficientemente rápida, sin afectar el desempeño de las actividades de la empresa.

En la figura 28, se observa que la velocidad de bajada (download speed) 287 kbps y la velocidad de subida (upload speed) 373 kbps. También se muestra un retardo (latencia) de 418 ms. Esta medición se realzó a las 5:10 pm, horario en el cual el tráfico en la red es elevado. Se puede observar que el ancho de banda ha disminuido a menos de la mitad, por lo que la navegación en Internet es más lenta.

Figura 28. Ancho de banda después de la apertura del centro comercial.
Fuente: CNT (2013)

Se destaca también la existencia de perdida de paquetes

El ancho de banda a emplear va sujeto a la elección del códec con el cual se va a trabajar. Según el códec que se emplee en la transmisión de datos, se utilizará más o menos ancho de banda. La elección del códec, va muy

relacionada con las actividades y requerimientos de la empresa, si el flujo de transmisión de datos es alto, es necesario un códec que maneje un ancho de banda alto, que permita la transmisión de la información sin retardo alguno.

La recomendación G.711 comenta que necesita un ancho de banda por canal de 64 kbps en una dirección. Es un códec empleado comúnmente para comunicaciones VoIP. Con este códec, la voz codificada se encuentra en el formato correcto para la entrega digital de voz en la PSTN o a través de una PBX. Mejora la calidad de ruido, sin aumentar la cantidad de datos. Esta recomendación muestrea 20 ms o 30 ms de voz por paquete, y se deben transmitir 50 paquetes por segundo. PCM no se creó para redes paquetizadas, sino para redes de conmutación de circuitos, se muestrea cada 125 ms, luego se paquetiza cada 160 muestras de voz o cada 240 muestras. Los paquetes se envían en tramas por la red de transporte, como puede ser ATM, Ethernet o Frame Relay. Los encabezados de las capas de los protocolos adicionales son incorporados con cada paquete, 160 bytes de carga. Las cabeceras incluyen RTP + UDP + IP + Ethernet, con un preámbulo de tamaños, 12 + 8 + 20 + 26 respectivamente. Por lo que un total de 226 bytes o 1808 bits, deben ser transmitidos 50 veces por segundo, o 90,4 kbps en una dirección. Para ambas direcciones el ancho de banda para una llamada es de 100 pps (paquetes por segundo) o 180,8 kbps para un flujo simétrico.

V.1.3 Perdida de paquetes

La pérdida de paquete es un aspecto común de las redes conmutadas de paquetes. La información fragmentada viaja por la red pero puede no llegar a su destino, sino a otro equipo. En este caso el router se congestiona y produce las perdidas. Para solucionar esto se puede cambiar el router o el ancho de banda de la red se puede aumentar.

Para evitar las pérdidas de datos, el ancho de banda elegido debe ser el idóneo por lo que resalta la elección del códec a utilizar. Al tener el ancho de banda ideal, se evita la pérdida o reenvío de paquetes que pueden originar retardos en la red.

V.1.4 Retardos

El retardo de extremo a extremo es un factor crítico en las redes de transporte VoIP. La calidad de voz empieza a degradarse a partir de retardos superiores a 150ms, aunque en algunos casos extremos, se pueden soportar hasta 400 ms. Estos retardos pueden ser a causa de *ECO* (consecuencia de las reflexiones de la señal) y *TALKER OVERLAP* (solapamiento de la voz de los interlocutores).

Para evitar retardos en la red, se cumplirá con la norma de un máximo de 150 ms de latencia por paquete en una dirección de extremo a extremo.

V.1.5 Evolución y modificación de la red

Es necesaria una evaluación de la infraestructura existente, tanto de la red, como de los equipos con que cuenta la empresa y, a partir de ello, realizar los requerimientos de la nueva tecnología. En caso de sufrir alguna modificación, normalmente son equipos que se incorporan a la red ya existente, mejora de las computadoras y al enlace que se posee. El cableado y topología de red, poco es modificado y más bien, la nueva tecnología se adapta a la ya existente.

Hay que tener en cuenta que es una tecnología que puede evolucionar, por lo cual, es conveniente trabajar con equipos que acepten mejoras en un futuro, que puedan integrarse a otras marcas sin ninguna complejidad y lo más importante, que la estructura de la red, no sufra cambios importantes.

V.2 Aspectos económicos de la solución VoIP

Para la empresa de Transporte Marítimo a la cual va dirigido el presente trabajo, cambiar su red telefónica y de datos a una red VoIP, va generar grandes beneficios en su facturación telefónica, llevándola a nuevos estándares de calidad, promoviendo su desarrollo en el mercado que se desempeñen.

El principal atractivo de las redes VoIP es el costo de las llamadas, el cual es más económico en comparación a las llamadas normales a través de una PSTN. Por el contrario, migrar a esta tecnología tiene un alto costo, por lo que es necesario un análisis exacto de la necesidad de la empresa en migrar a VoIP.

Otro aspecto interesante para la Telefonía VoIP, es que por el mismo cableado pasa voz y datos, ahorrando tanto costos a la empresa, como economizando espacio en la infraestructura de la red.

Teniendo en una misma red voz y datos, es más fácil su administración y no es necesario personal para cada área específica, sino que una persona puede administrar la red. Aspecto que también se puede ver como un beneficio y ahorro a la empresa.

En la parte de seguridad física y de la red, a través de la red VoIP se pueden integrar los distintos sistemas de protección que ayudan al resguardo de la información. Se incorporan firewalls que protege de ataques externos a la red. También un sistema de acceso y control de personal a las instalaciones, el sistema de cámaras de vigilancia se puede controlar a través de esta misma red. Es decir, que es una red bastante robusta que permite la manipulación de varias aplicaciones al mismo tiempo sin que se vean afectados sus tiempos de respuesta.

Para la empresa a la cual va dirigido el presente trabajo, la parte más importante, más allá que genere un beneficio económico, es que puede solucionar el problema que presentan con los números telefónicos, sumándose a este aspecto un ancho de banda mayor a través del cual la navegación en Internet es más rápida, una red segura y un avance en cuanto a tecnología se refiere.

V.3 Aplicaciones y Equipos en VoIP

V.3.1 Servidores de Telefonía IP y PBXs

La central PBX es la encargada de conmutar las llamadas de voz en una red de datos a través del protocolo IP e interoperando con la PSTN. Esta central puede ser implementada tanto en hardware como en software.

La IP PBX se puede instalar sobre una plataforma tipo servidor, funcionando como un servidor dedicado, realizando las mismas funciones que una PBX convencional y manejar las comunicaciones por medio del protocolo IP. También cumple funciones de Gateway a la red PSTN por medio del hardware. Si se implementa como software, es fácil y económico añadir nuevas funciones o módulos que le dan valor agregado. Estos pueden ser: buzón de voz, música en llamadas de espera, llamadas en conferencias, entre muchas más.

Algunas plataformas de software que permite la instalación e implementación de Servidores de Telefonía IP y PBX, son:

Asterisk

Es una PBX completa en software que se puede ejecutar en varios Sistemas Operativos (Linux, BSD, Windows y OS X) generando todas las características referidas a una PBX.

Entre los servicios que ofrece Asterisk se tiene correo de voz con directorio, llamada en conferencia, respuesta interactiva de voz (IVR), cola de llamadas, soporte de tres en llamada de conferencia, identificador de llamadas, ADSI, IAX, SIP, H.323 (como cliente y puerta de enlace), MGCP (administrador único de llamada) y SCCP.

Asterisk no necesita de hardware adicional para Voz sobre IP. Se pueden utilizar uno o varios proveedores para las llamadas entrantes y salientes. Estas llamadas pueden manejarse bajo proveedores independientes.

Para conectarse con equipos de telefonía analógica y digital, Asterisk soporta varios tipos de dispositivos de hardware, en especial, los dispositivos fabricados por Digium. Entre los equipos que poseen se mencionan interfaces T1 y E1 para la conexión a líneas PRI y bancos de canal, tarjetas analógicas de cuatro (4) puertos FXS y FXO. Soporta tarjetas de otros proveedores.

3CX

La central telefónica 3CX, está orientada para el Sistema Operativo Windows, la cual reemplaza en su totalidad los sistemas telefónicos tradicionales. Soporta teléfonos SIP estándar, servicios VoIP y líneas telefónicas tradicionales.

Al trabajar con pasarelas (Gateway) VoIP, permite usar líneas PSTN con la central telefónica. No existe la necesidad de un proveedor de VoIP, con el proveedor de líneas PSTN, se puede proporcionar un servicio fiable. 3CX trabaja con una amplia gama de puertas de enlace, también puede trabajar con pasarelas que soporten el estándar SIP.

Las características que presentan son: llamadas de extensión a extensión, buzón de voz, menús de respuestas interactivos de voz. Mensaje de voz a correo electrónico, música o melodías de espera, conectar aplicaciones directas de una computadora, como registros de llamadas.

V.3.2 Softphone

Es una aplicación que se ejecuta en una computadora y funciona como un teléfono a través de voz sobre IP, utilizando la red de datos como medio de transmisión telefónica. Esta aplicación presenta todas las funciones y características de un teléfono convencional; emplea la tarjeta de sonido, altavoces y micrófono para la comunicación, a través del teclado se realiza la marcación del número telefónico.

El emplear este tipo de telefonía, ayuda a reducir costos y espacio, ya que no es necesario otro equipo o hardware, sino que la función del teléfono se realiza a través del software instalado en la computadora, el cual permite tener todas las funciones y otras más de un teléfono convencional.

Linphone

Softphone SIP, con soporte para varios codecs, es bastante amigable y sencillo de manejar, tiene una interfaz sencilla, y es compatible con Asterisk. Se puede ejecutar en Linux, Mac OS X y Windows. Algunas de sus características son:

- Soporta voz, video y mensajería de texto.
- Emplea el protocolo SIP, el cual es soportado por la mayoría de los proxys y teléfonos.
- Compatible con varios Sistemas Operativos. (Windows para el desarrollo del presente trabajo).
- Algunos de los codecs que soporta: G.711, G.722, GSM, Speex.

- Empleo de plugins. Añadir nuevos codecs o funciones básicas.
- Soporta tonos DTMF.
- Soporta IPv6.

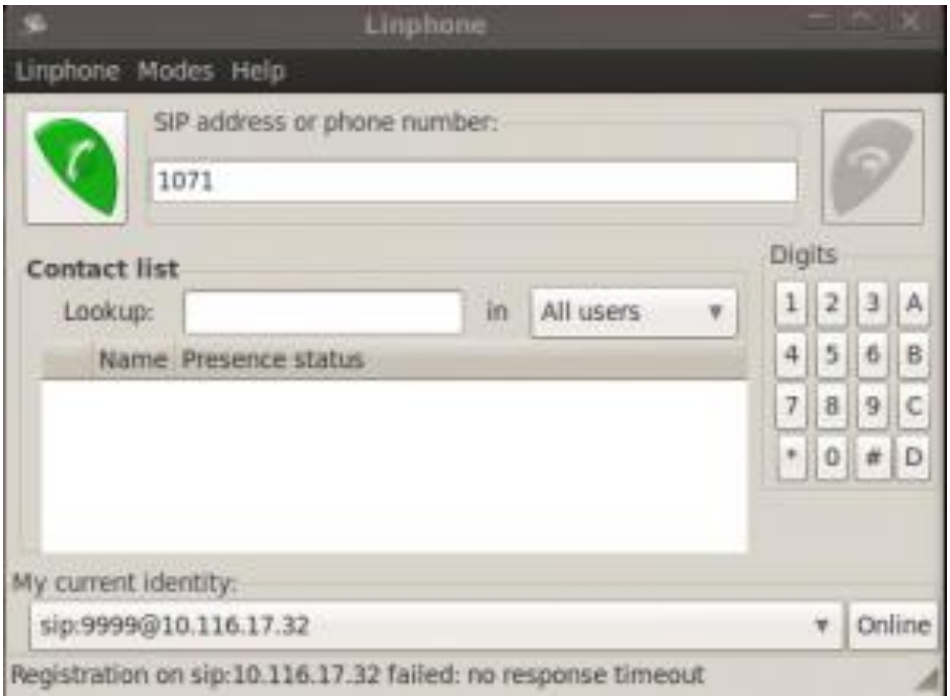

Figura 29. Vista del software de Linphone.
Fuente: Hotfixed (2013)

Zoiper

Es un softphone que soporta SIP y IAX, funciona para las plataformas Windows, Linux y Mac OS X. trabaja con cualquier sistema o infraestructura IP. Es una herramienta con software de comunicación multiprotocolo HD que combina las características de softphone, mensajería y medios de comunicación comerciales.

Ofrece llamadas de voz de alta calidad, teleconferencias, envío y recepción de fax. Iniciar llamadas directamente desde el administrador de correos (Outlook, Thunderbird), grabación de llamadas. Es un software bastante amigable y de fácil manejo.

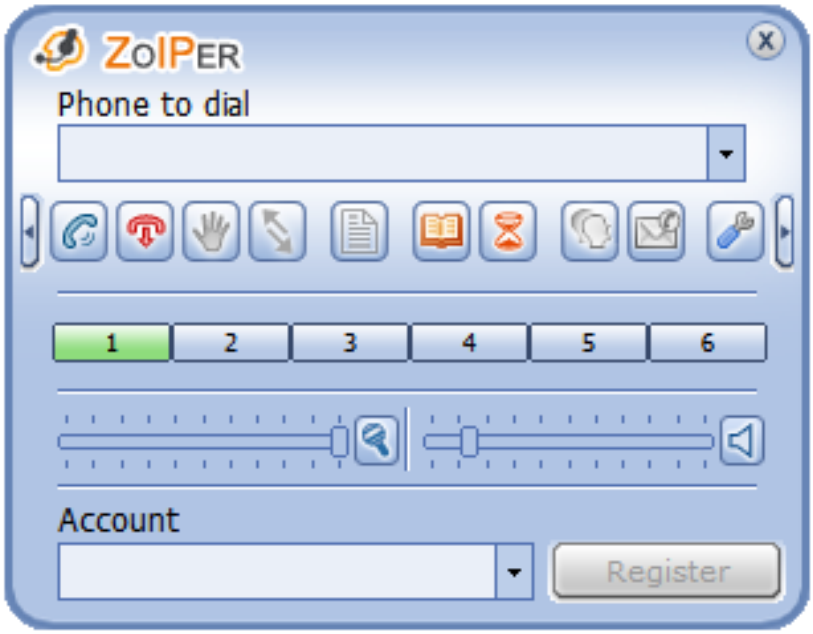

Figura 30. Vista del software Zoiper.
Fuente: ZoIPer (2012)

V4. Fallas en los Sistemas Actuales

A lo largo del desarrollo del presente trabajo se han ido mencionando las fallas que la empresa de Transporte Marítimo presenta en los servicios de seguridad y telecomunicaciones. Fallas que en ocasiones, han presentado grandes inconvenientes en las labores diarias de la empresa.

Los sistemas de seguridad son pocos, un sistema de 4 cámaras que vigilan ciertas áreas de la oficina conectadas a una tarjeta PCI instalada en una computadora, que hace la función de servidor y es allí, donde se almacenan los archivos guardados de las grabaciones. Este sistema de cámaras se administra a través del software que trae la misma tarjeta. La computadora

donde está instalada esta tarjeta, es un equipo de uso diario y por lo que en ocasiones al haber un alto número de recursos en funcionamiento, la computadora empieza a fallar y por ende, el sistema de cámaras de seguridad.

Otro sistema de seguridad, es un intercomunicador o portero que cuenta con una cámara integrada y un alta voz, que permiten ver y escuchar a la persona que desea entrar a la oficina, para posteriormente darle acceso a la misma. Para el resguardo de la información que está en las computadoras, se posee un antivirus en cada computadora; el mismo se está actualizando constantemente para tener las últimas bases de datos de los programas maliciosos que puedan dañar la información.

En los servicios de telecomunicaciones, voz y datos, las fallas son mayores. En la parte de telefonía el principal problema es el número telefónico de salida, el cual no coincide con los números telefónicos de la empresa. Otro problema es que en ocasiones las líneas telefónicas aparecen ocupadas, cuando en realidad no se está hablando por teléfono. En la parte de datos, el principal problema es lo lento de la velocidad de conexión, ya que el enlace al que se pertenece, comparte el ancho de banda con el centro comercial, aspecto que desmejora notablemente la velocidad de navegación en Internet.

V.5 Propuestas o Alternativas al problema planteado

En vista de la situación a la que se hace referencia en el punto anterior y en el desarrollo del presente trabajo, se plantea la posibilidad de migrar hacia una nueva y mejor tecnología, VoIP.

Para poder migrar hacia VoIP, se presentan tres alternativas, cada una con sus aspectos positivos y negativos pero con un fin en común, buscar solución a la situación actual. Es muy importante que cada alternativa sea analizada y estudiada a la hora de tomar decisiones ya que las mismas generan gastos

que pueden ser muy significativos. Tomando en cuenta las características de la red actual, los equipos, topología y red; se plantean las siguientes alternativas:

V.5.1 Primera Alternativa

La empresa continúa obteniendo los servicios de telecomunicaciones con su actual proveedor, manteniendo las mismas características de la red de datos, ancho de banda, topología, distribución de las estaciones de trabajo. Por otra parte, invierte en la adquisición de equipos nuevos en la parte de telefonía y red de datos, para así, poder migrar hacia una red VoIP.

Ventajas

- Se adquieren equipos de última tecnología en la parte de telefonía.
- Los equipos no necesariamente tienen que ser de una marca específica, sólo que sean compatibles entre ellos.
- Migrar a Telefonía IP, generará un ahorro económico en telefonía.
- La escalabilidad de esta tecnología, los impulsa a estar a la par con otras empresas o sedes del ramo.

Desventajas

- Quedarse con el actual servicio de telecomunicaciones, puede presentar muchos problemas para el funcionamiento de la red IP.
- Realizar mejoras en la red IP, se pueden ver obstaculizadas por la tecnología y las características de la red.
- No poder realizar mejoras en su red interna, se ve reflejado en un atraso en tecnología e igualmente con otras sedes y empresas del ramo.

- Es un gasto significativo, en especial con la adquisición de equipos nuevos, sin embargo ese aspecto se compensa con los beneficios que se obtienen al migrar a VoIP.

Al seguir las indicaciones de esta alternativa, adquirir nuevos equipos para la implementación de VoIP implica obtener una IP PBX, un softphone, teléfonos IP, router entre otros.

Para la selección del software de la IP PBX, se analizaron y compararon par de aplicaciones, las cuales dieron como resultado la escogencia de Asterisk.

La tabla comparativa entre las dos opciones se puede observar en los anexos.

La elección de Asterisk se debe principalmente a que es un software libre, ampliamente usado y probado. También por el hecho que se ejecuta en ambiente Windows, aspecto importante ya que las computadoras de la empresa trabajan con el Sistema Operativo Windows. Permite la instalación de una central IP PBX con todas sus funciones. Posee una amplia comunidad de desarrolladores de habla hispana y documentación en español. Es compatible con los equipos y appliance que fabrica la empresa Digium.

Aspectos como ser un software libre y trabajar en Windows, fueron factores determinantes en la elección de Asterisk. De esta manera las modificaciones o adquisición de equipos nuevos se disminuyen notoriamente.

La IP PBX a emplear es la Asterisk Appliance 50 (AA50), la cual es una PBX independiente, creada para trabajar con Asterisk. Va dirigida a pequeñas y medianas empresas. Ofrece una solución hibrida (combina aplicaciones VoIP con equipamiento de telefonía tradicional), esto es para el caso de empresas que no migran por completo a Telefonía IP. Su licencia comercial Asterisk Business Edition, es open source. Posee la capacidad de integrarse a la red existente y comenzar a trabajar de manera inmediata.

En los anexos se puede observar un cuadro comparativo entre IP PBX que originaron en la elección de la Asterisk Appliance 50.

Figura 31. Asterisk Appliance 50 (AA50).
Fuente: Digium, Inc. (2013)

En la siguiente tabla se observa los costos asociados a la adquisición de esta IP PBX Asterisk Appliance 50.

Tabla 12. Costos relacionados a la IP PBX

Hardware/Software	Cantidad	Costos
Asterisk Appliance 50	1	$ 1.399,00
Tarjeta FXS[3]/FXO[4] DigiumTDM2411B	1	$ 715,00
Asterisk Buisness Edition Software	1	$ 889,95
	Total a Pagar	**$ 3.003,95**

Fuente: Elaboración Propia.

[3] FXS: puerto en la central telefónica, que permite conectar un teléfono analógico estándar.
[4] FXO: puerto que permite conectar líneas telefónicas analógicas con extensiones de una centralita IP.

También se selecciona el softphone, el cual es un software que se instalará en las distintas computadoras y funcionará como un teléfono sobre voz IP.

Linphone, es un softphone de fácil manejo e instalación, el cual funciona con Asterisk, adaptándose a esa condición. Se pude descargar directamente de la página web del mismo, y presenta varias versiones, tanto para computadoras como equipos móviles. Es de software libre, por lo que no es necesario pagar para adquirirlo. Posee ayuda y soporte técnico, lo que es importante a la hora de presentarse algún inconveniente.

Lo ideal es instalarlo en las estaciones de trabajo que lo ameriten, de esta manera permite la flexibilidad y un mejor alcance de la Telefonía IP en la empresa. Inclusive, se puede instalar en dispositivos móviles, originando que las llamadas que se realicen a los mismos o desde los mismos dispositivos, sean sin costo alguno.

Al combinar llamadas de voz, video llamadas y mensajería instantánea, junto a una interfaz sencilla, ayudan a la transición de telefonía tradicional a la telefonía sobre voz IP.

Los equipos restantes que conforman la red IP, se muestran de manera referencial en los anexos.

Los teléfonos IP a utilizar son los modelos D40 y D50 de la marca Digium. Son equipos diseñados para uso exclusivo con Asterisk, software que será el empleado en nuestra solución. Son equipos altamente avanzados, con implementación de voz en alta definición (HDVoice) y con instalación automático plug-and-play. Presentan aplicaciones preinstaladas, que muestran datos que se manejan constantemente de una manera fácil y sencilla y, siempre a la mano.

Tabla 13. Características de los teléfonos IP D40 y D50.

Características	D40	D50
HDVoice	4	4
Teclas de línea	2	4
Teclas de función	4	6
Teclas de marcación rápida	------	10
Conexión LAN	100 Mbps w/ Switch	100 Mbps w/ Switch
Pantalla Principal	3.5 pulgadas	3.5 pulgadas
Poder sobre Ethernet (PoE)	4	4
Conectores	RJ-9	RJ-9
Aplicaciones del teléfono	Correo de voz, contactos, registro de llamadas, llamadas en espera, varias mas	Correo de voz, contactos, registro de llamadas, llamadas en espera, varias mas
Funciones del teléfono	Respuesta automática, tonos de timbre personalizados, llamada en espera, desvío de llamadas, 3 formas de conferencia, identificador de llamadas, entre otros.	Respuesta automática, tonos de timbre personalizados, llamada en espera, desvío de llamadas, 3 formas de conferencia, identificador de llamadas, entre otros.
Funciones de audio	Modos de teléfono altavoz y mudo, altavoz HD, micrófono HD con aislamiento acústico, tonos de llamadas (CNG),supresión de ruido de trasfondo, entre varios más.	Modos de teléfono altavoz y mudo, altavoz HD, micrófono HD con aislamiento acústico, tonos de llamadas (CNG),supresión de ruido de trasfondo, entre varios más.
Soporte de red	Asignación de dirección IP DHCP o estática, sincronización de tiempo SNTP, recorrido VLAN, LLDP, NAT; QoS.	Asignación de dirección IP DHCP o estática, sincronización de tiempo SNTP, recorrido VLAN, LLDP, NAT; QoS.

Fuente: Elaboración Propia.

Tabla 14. Costos relacionados a teléfonos IP

	Cantidad	Costo Unitario	Costo
Teléfono IP D40	6	$ 141,90	$ 851,40
Adaptador de corriente internacional	6	$ 27,50	$ 165,00
Teléfono IP D50	4	$ 207,90	$ 831,60
Adaptador de corriente internacional	4	$ 27,50	$ 110,00
		Total a Pagar	**$ 1.958,00**

Fuente: Elaboración Propia.

Los servicios de telecomunicaciones que ofrece el actual proveedor se seguirán usando, en especial la red de datos ya que a través de ella se va levantar e integrar esta nueva tecnología voz, datos y videos. Por medio de la red, trabajará la Telefonía IP, los sistemas de seguridad y la transmisión de datos. También las líneas telefónicas que se poseen en la actualidad seguirán operando, esto debido a que la central IP que se adquiere, tiene la característica de aceptar la conexión de PSTN y tener al mismo tiempo telefonía tradicional y Telefonía IP. Por estos servicios se seguirá cancelando un estimado de Bs. 2.300,00 mensuales.

Los sistemas de seguridad son de gran importancia para el resguardo tanto de la información como del personal que labora dentro de la oficina. Para mantener controlada esta situación, se necesitan de sistemas que puedan controlar los accesos a la oficina. Así mismo mecanismos de defensa que puedan detectar ataques a la información y poder neutralizarlos. En el punto V.6 de este capítulo, se explica de manera más detalla los sistemas de seguridad a emplear, y también los costos asociados a los mismos.

El servicio post-venta es muy importante, con ello se busca el buen funcionamiento y durabilidad del software y hardware que se adquiera. Estos equipos requieren de un mantenimiento o servicio, actualizaciones de software que en muchas ocasiones se puede realizar de manera on-line en la página web del proveedor. Algunos servicios son de manera gratuita, otros necesariamente tiene un costo. El personal de la empresa de Transporte Marítimo, está en la capacidad de prestar cierto tipo de servicio técnico a los equipos y asesorías a otros empleados en cuanto al manejo del software y hardware adquiridos.

Esta alternativa presenta una serie de equipos que se adquieren en moneda extranjera (Dólares), por lo que es necesario llevarlos a la moneda local (Bolívares) para tener una referencia del costo de migrar a VoIP. La tasa de cambio a usar es de Bs. 6,3 por dólar. A ello también se debe agregar el costo de importación lo que incrementa en alrededor de un 25% el total a pagar.

Tabla 15. Costo total Primera Alternativa

Descripción	Costo
Costo total relacionado IP PBX	$ 3.003,95
Costo total relacionado con teléfono IP	$ 1.958,00
Sub Total ($)	$ 4.961,95
Costo importar equipos	$ 1.240,49
Total ($)	**$ 5.932,44**
Sub Total (Bs.)	**Bs. 37.374,36**
Costo total Sistemas de Seguridad[5][6]	Bs. 24.887,37
Total a pagar (Bs.)	**Bs. 62.262,73**

Fuente: Elaboración Propia.

V.5.2 Segunda Alternativa

Como segunda alternativa, la empresa adquiere los servicios de un nuevo proveedor en el área de telecomunicaciones. Al mismo tiempo, se adquieren equipos nuevos en la parte de telefonía y redes de datos, que puedan acoplarse con las características que ofrece el nuevo proveedor con la cual se puedan realizar todas las mejoras que se propongan y así, migrar hacia la tecnología IP. De esta manera en una misma red pueden converger de manera óptima voz, datos y video.

Ventajas

- Se adquieren equipos de última tecnología en la parte de telefonía.

[5] La descripción detallada de los seguridad se puede en el punto V.6 del presente Capitulo.
[6] El antivirus o firewall, debe actualizar su licencia nuevamente, por lo que se cancela el costo asociado a la actualización de la licencia del mismo.

- Los equipos no tienen que ser de una marca específica, solo que sean compatibles entre ellos.
- Migrar a Telefonía IP, generará un ahorro económico en telefonía.
- La escalabilidad de esta tecnología, los impulsa a estar a la par con otras empresas o sedes del ramo.
- Al obtener un nuevo ancho de banda, la red IP, funcionará de manera adecuada.

Desventajas

- El gasto es doble, por lo que puede ser una opción costosa en comparación a las otras dos.
- Los servicios post-venta del nuevo proveedor en telecomunicaciones, se pueden ver afectados si es un proveedor con mucha demanda.

Esta alternativa presenta dos partes, la primera conformada por el hardware y software necesarios para migrar hacia VoIP. La segunda parte, el proveedor de los servicios de telecomunicaciones.

Para la primera parte, la opción del software IP PBX, la central IP PBX y el softphone; son los mismos seleccionados en la primera alternativa. Entonces el costo asociado a esta primera parte, es el mismo que se muestra en la tabla 15.

En la segunda parte, el nuevo proveedor de los servicios de telecomunicaciones, se encargará de aportar exclusivamente los servicios relacionados con la red de datos.

Se solicitaron presupuestos a dos empresas del área de telecomunicaciones y en el cual se requería el mismo servicio, un Internet dedicado de 2048 kbps. Inicialmente se va a trabajar con este ancho de banda, y dependiendo de los resultados que se obtengan, se propondrá mejorar el mismo. De esta manera mensualmente se debe cancelar el monto que se indica en la tabla 16, según sea la elección del proveedor.

Tabla 16. Costo mensual nuevo proveedor de telecomunicaciones.

	CCOM	BANTEL
Acceso a Internet 2048 kbps (simétrico)	Bs. 11.660,00	Bs. 11.660,00
Conectividad dedicada Última Milla	----------	Bs. 9.965,00
Total a pagar	**Bs. 11.660,00**	**Bs. 22.625,00**

Fuente: Empresa de Transporte Marítimo.

Los sistemas de seguridad a emplear (portero, sistema de cámaras y antivirus) se describen en el punto V.6 del presente capitulo. Allí se destacan cada uno de los sistemas, mencionando sus características y costos.

El servicio post-venta del software y hardware es igual que en la primera alternativa, a través del sitio web del proveedor y con el personal del departamento de informática de la empresa. El nuevo proveedor de los servicios de telecomunicaciones, posee un departamento especializado en recibir y canalizar todos los problemas o inconvenientes que se puedan presentar en la parte de la red y están en la obligación de solucionar dichos inconvenientes. Estas soluciones se pueden dar de igual manera a través de su sitio web o con personal físico que se dirija a la oficina de la empresa de Transporte Marítimo.

V.5.3 Tercera Alternativa

En esta alternativa, la empresa adquiere los servicios de un nuevo proveedor en el área de telecomunicaciones, el cual debe ofrecer un servicio de alta calidad, ofrecer los requerimientos necesarios para migrar hacia VoIP. El proveedor al mismo tiempo, suministra el servicio de Telefonía IP (VoIP), los equipos necesarios para la introducción de VoIP en la empresa y la

restructuración de la red interna (de ser necesario), convergiendo en la misma red voz, datos y video.

En la actualidad existen muchas compañías que ofrecen los servicio de Telefonía IP, algunas de gran renombre nacional e internacional; las cuales trabajan con distintos software y hardware que se van ajustar a la necesidad del cliente. Al adquirir un nuevo proveedor en los servicios de telecomunicaciones, en cierta medida la empresa en cuestión se está "casada" con el proveedor, ya que se firma un contrato en el cual se deben cumplir las pautas allí especificadas que pueden tener sus aspectos positivos y negativos.

Ventajas

- La tecnología que se instala, es de última generación, con equipos de punta.
- La red que ofrecen es robusta, en la cual convergen voz, datos y videos sin problema alguno.
- Esta red permite que los sistemas de seguridad se puedan canalizar por la misma red.
- Velocidad de banda ancha acorde a la necesidad del cliente.
- Posibilidad de escalabilidad de la red. Mejoras internas y externas.

Desventajas

- Los costos pueden ser muy elevados.
- Se deben cumplir las pautas planteadas en el contrato sin restricción.
- Incumplir una pauta, puede significar la ruptura del contrato.
- El proveedor es el que impone la pauta en cuanto a la tecnología, marca de los equipos, modelos, etc.
- La evolución tecnológica, depende de la evolución de la marca de los equipos con la cual se trabaja.

- El servicio técnico lo ofrece el proveedor y por lo general, son demorados en dar respuesta a las solicitudes por su alta demanda de los servicios.

Una empresa que puede prestar este servicio, es BANTEL. La misma tiene experiencia en redes privadas para el servicio de transporte satelital y terrestre de voz, video y datos. Por estas características se consideró como una opción entre las empresas de servicio de telecomunicaciones a la cual se le solicitó un presupuesto en la segunda alternativa.

Como lo indica en su página web, Telecomunicaciones Bantel, (2013), "**Servicio de Voz y Datos** está apoyado en la más moderna tecnología, con la calidad y respuesta inmediata que nos caracteriza: Banda Ancha Satelital (BAS), Enlaces Dedicados y Canales Internacionales. El servicio de transmisión de **VOZ, VIDEO Y DATOS** a nivel nacional e internacional se realiza **vía microondas, vía satélite o vía fibra óptica** con QoS y SLA, garantizando la calidad del servicio independientemente del medio."

Lo descrito anteriormente, muestra que es una empresa que puede cumplir con las exigencias de la empresa de Transporte Marítimo.

En el presupuesto entregado por esta empresa, muestra una primera parte relacionada con la red de transmisión de datos. Ofrecen la misma características y condiciones que se muestran en la tabla 16, por lo que mensualmente se debe cancelar por la red de datos el monto reflejado en esta tabla, siendo la opción a elegir BANTEL.

La segunda parte es la relacionada con la Telefonía IP. BANTEL, da a sus clientes la posibilidad de alquilar o comprar el software y hardware para implementar VoIP. Según sea la opción a elegir, existen pautas y normas que limitan al cliente a estar vinculados, lo que puede verse como una desventaja.

Este proveedor trabaja con Asterisk, aspecto positivo a la hora de tomar la decisión en cuanto a la adquisición de los servicios de telecomunicaciones con un nuevo proveedor.

Los equipos que presupuesta este proveedor para la Telefonía IP son de una marca muy reconocida, son de alta calidad, genuinos y de última generación; beneficiando a la empresa de Trasporte Marítimo en cuanto a su tecnología. Sin embargo por ser ellos los que suministran estos equipos, el cliente se debe atener a las recomendaciones de este proveedor, dejando poco margen para variar los equipos en marca y modelo al momento de una actualización o sustitución del hardware.

Tabla 17. Comparación de costos alquilar o comprar los equipos para VoIP con BANTEL.

Equipo	Cantidad	Costo Alquilando los equipos	Costo Comprando los equipos
Central Telefónica IP PBX Zycoo	1	Bs. 19.000,00	Bs. 26.500,00
Teléfono IP Cisco 7962	4	Bs. 3.900,00	Bs. 6.700,00
Teléfono IP Cisco SPA502G	6	Bs. 1.700,00	Bs. 2.500,00
Softphone EyeBeam 1.5[7]	6	Bs. 1.500,00	Bs. 1.900,00
Router Cisco E3200 N600 Mbps	1	Bs. 3.500,00	Bs. 5.000,00
	Total a Pagar	**Bs. 29.600,00**	**Bs. 42.600,00**

Fuente: Empresa de Transporte Marítimo.

La instalación del hardware y software la realiza el mismo proveedor, trabajando con la infraestructura ya existente, y si es necesario la modifica, la

[7] Sólo SO Windows 32 bits.

mejora o la cambia para que se pueda adaptar a la nueva tecnología. El servicio de post-venta es directamente con ellos, a través de su portal web o vía telefónica, y de persistir la falla, personal especializado visita la oficina para dar solución a los requerimientos del cliente.

Los sistemas de seguridad a emplear (portero, sistema de cámaras y antivirus) se describen en el punto V.6 del presente capitulo. Allí se destacan cada uno de los sistemas, mencionando sus características y costos.

Tabla 18. Costos Asociados a la Tercera Alternativa

Descripción	Alquilando los equipos VoIP	Comprando los equipos VoIP
Costos equipos VoIP	Bs. 29.600,00	Bs. 42.600,00
Instalación de los equipos	Bs. 6.000,00	Bs. 6.000,00
Costos Sistemas de seguridad[8][9]	Bs. 24.887,37	Bs. 24.887,37
Total a pagar Tercera Alternativa	**Bs. 60.487,37**	**Bs.73.487,37**

Fuente: Elaboración Propia

V.6 Sistema de Seguridad

Los sistemas de seguridad son de suma importancia en las empresas para el resguardo de las instalaciones, el resguardo de la información y el resguardo del personal; ahorrándole a las empresas grandes cantidades de dinero en equipos e información valiosa para la organización. Actualmente en el mercado, existen gran cantidad de sistemas de seguridad, que son empleados según la necesidad del cliente. Empresas dedicadas a proveer dichos servicios o sistemas, y equipos que se pueden adquirir de manera

[8] La descripción detallada de los sistemas de seguridad se puede ver en el punto V.6 del presente Capitulo.

[9] El antivirus o firewall, debe actualizar su licencia nuevamente, por lo que se cancela el costo asociado a la actualización de la licencia del mismo.

independiente. Algunos de los sistemas de seguridad son: circuito cerrado de video vigilancia, controles de acceso por tarjetas magnéticas, lectores de huellas y retinas; detectores de metal.

La empresa de transporte marítimo a la cual va dirigido este trabajo, busca mejorar los sistemas de seguridad con que cuenta e implementar nuevas pautas y técnicas que le ayuden a resguardar la información que manejan y sus instalaciones.

En el punto anterior del presente capítulo, se presentaron tres (3) alternativas para la red IP, a través de la cual, los equipos y sistemas de seguridad se van a manejar. Independientemente de la alternativa que se elija, los sistemas de seguridad van a trabajar directamente con ella, por lo que es importante tener en cuenta este aspecto en la decisión de la alternativa, y en especial, el ancho de banda que se necesita para cumplir las exigencias de la empresa en cuestión.

Un sistema de circuito cerrado de videocámaras o DVR, es ideal para la seguridad de la empresa. Este da la opción que puede ser monitoreado vía web o mejor aún, a través de dispositivos móviles, lo que permite la vigilancia a grandes distancias. El DVR, al ser un grabador digita de video, procesa el video de manera digital permitiendo grabación continua y presentando imágenes claras.

Actualmente existen todavía equipos de grabación analógicos, pero los mismos están siendo desplazados por los sistemas de grabación digital. En la siguiente tabla se observan la diferencia entre los sistemas.

Tabla 19. Comparación entre sistemas analógicos y sistemas digitales.

Características	Sistema Analógico	Sistema Digital
Grabación	Imagen analógica (pobre)	Imagen de alta resolución
Medio de grabación	Casette de VHS	Disco duros de alta capacidad
Grabación continua	La calidad de imagen empeora con el tiempo y al verse varias veces	Uso ilimitado
Búsqueda de imágenes	Toma mucho tiempo, información no organizada	Búsqueda en segundos
Calidad de imagen	Baja calidad	Alta calidad
Mantenimiento del sistema	Necesario espacio para guardar casettes	No es necesario mantenimiento
Función de transmisión de imágenes	No posee función	Transmisión posible
Costo de mantenimiento	Alto costo	Sin costo
Área de detección	Hasta lo que llega el cable	Sin límite de distancia
Impresión	Requiere equipo separado	Impresión de alta calidad de imagen en pantalla, impresión remota interna
Grabación	Grabación simple sin opciones	Grabación de movimientos o sensor

Fuente: Voxdata Comunicaciones IP (2010)

El sistema de cámara de seguridad estará conformado por cámaras digitales y un DVR, teniendo acceso a las cámaras a través de Internet. Es una solución bastante atractiva, la cual ahorra en espacio, ya que las cámaras no necesitan de cables para su instalación y con el DVR, se tiene un equipo exclusivo para las cámaras de seguridad. En los anexos se puede observar las características de las cámaras y del DVR.

Tabla 20. Costos Sistema de Cámaras de Seguridad.

Articulo	Cantidad	Costo Unitario	Costo
Cámara Seguridad Domo 1/3 Cmos	4	Bs. 380,00	Bs. 1.520,00
DVR Stand Alone Hikvision 8 canales	1	Bs. 4.599,00	Bs. 4.599,00
Video Balun (Par)	2	Bs. 100,00	Bs. 400,00
Monitor LED LG 21,5 pulgadas	1	Bs. 3.249,00	Bs. 3.249,00
		Total a pagar	**Bs. 9.768,00**

Fuente: Elaboración Propia.

Para el control de acceso, el sistema de portero o intercomunicador que posee la empresa, es adecuado y se mantendrá el mismo. Este sistema presenta la opción de intercomunicador, apertura de puerta y video, permitiendo tener conocimiento sobre la persona que desea entrar a las instalaciones.

El resguardo de la información que se contiene en las computadoras, como la información física en papel, es más compleja, debido a que en gran parte se basa en el uso y manera de trabajarla por parte del empleado.

El personal del área de sistemas, deberá redactar un informe en el cual se establezcan pautas sobre la manipulación de la información, formas de guardarla o almacenarla, sitios en los cuales se puede navegar en Internet y en cuáles no; administración de claves, manejos de las estaciones de trabajo, entre varias más.

Una herramienta que ayuda a la protección de la información es el Firewall. Este puede ser un software, el cual se instala en la computadora y se manipula a través de su interfaz gráfica, o un hardware, el cual se coloca entre en la red física, entre el switch y las estaciones de trabajo.

Como menciona Microsoft (2013), firewall “es un software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de esta a la información, en función de la configuración del firewall”.

En la actualidad existe una gran cantidad de software que protegen a los sistemas de ataques malintencionados, hackers, malware, etc. Los antivirus son un ejemplo de ello, los cuales cuentan con varias funciones, en la que destaca el firewall, que ayuda a una mayor protección de la red y del equipo donde se instala. Estos sistemas de seguridad, nunca deben faltar en una empresa, principalmente en las estaciones de trabajo, ya que en ellas es donde se guarda la mayoría de la información y la necesidad de navegar en Internet, muchas amenazas se pueden recibir a través de la web.

Kaspersky Total Security for Business

Esta es una herramienta que va dirigida a las empresas y en la cual se integran varios módulos que ayudan a la seguridad de la información. Además de antimalware para estaciones de trabajo y dispositivos móviles, más tecnologías de cifrado especializadas, controles flexibles de endpoint y herramientas de administración de sistemas de aumento de la eficacia, Kaspersky TOTAL Security for Business entrega una confiable protección para servidores de correo electrónico, servidores de colaboración y flujo de tráfico por puertas de enlace de Internet.

Algunas de sus funcionalidades son:

- Antimalware, controles, cifrado de datos y seguridad móvil.
- Administración de parches y escaneo automático de vulnerabilidades.
- Herramientas de administración de sistemas de aumento de eficacia.
- Seguridad de correos electrónicos, Internet Gateway y servidores de colaboración.

En la siguiente tabla se puede observar el costo anual para adquirir el antivirus. Pasado el año, la licencia caduca y es necesaria una renovación o actualización a un costo menor que adquirirlo por primera vez. Es necesario llevar a moneda local el costo de adquirir este software. La conversión se realiza con la tasa de 6,3 Bolívares por Dólar.

Tabla 21. Costo Antivirus.

Descripción	Cantidad	Costo Unitario	Costo
Kaspersky Total Security for Business (1 Año de protección, 10 Pc`s)	2	$ 1.199,95	$ 2.399,90
		Total a Pagar ($)	**$ 2.399,90**
		Total a Pagar (Bs.)	**Bs. 15.119,37**

Fuente: Kaspersky Lab ZAO (2013)

Tabla 22. Costos Sistemas de Seguridad

Descripción	Costos
Sistema Cámaras de Seguridad	Bs. 9.768,00
Antivirus	Bs. 15.119,37
Total a Pagar Sistemas de Seguridad	**Bs. 24.887,37**

Fuente: Elaboración Propia

V.7. Selección de la Alternativa

Luego de recopilar toda la información en las distintas etapas y capítulos del presente trabajo, se plasmaron en las tres alternativas que presentan para dar solución al problema existente en la empresa de Transporte Marítimo con los sistemas de telecomunicaciones y sistemas de seguridad. Estas

alternativas dan a conocer distintas opciones con las cuales se pueden trabajar y llegar a la parte central del trabajo. Cada alternativa tiene sus aspectos positivos y negativos, sus propias características.

La solución que se busca es que en la misma red de datos, se puedan integrar voz, datos y video, de esta manera se obtienen grandes beneficios para la empresa a la cual va dirigido el presente trabajo. Una red de datos con un ancho de banda adecuado para la tecnología que se propone, en la cual la latencia, perdida de paquetes y retardos se reduzcan a lo mínimo y más bien, la trasmisión de datos e información fluya lo mejor posible en ambos sentidos. A través de esta misma red de datos (LAN), va a funcionar la Telefonía IP, usando equipos nuevos y especializados en esta tecnología. Algunos de estos equipos permiten el uso de video, conferencias o teleconferencia que absorben gran cantidad de recursos en la red.

Una novedad en esta solución, son los sistemas de seguridad, los cuales se integrarán y funcionarán a través esta red. Estos sistemas tienen características que les permiten ser manejados a través de Internet, accediendo a ellos desde distintas computadoras, laptops, celulares o tabletas; en cualquier parte del mundo.

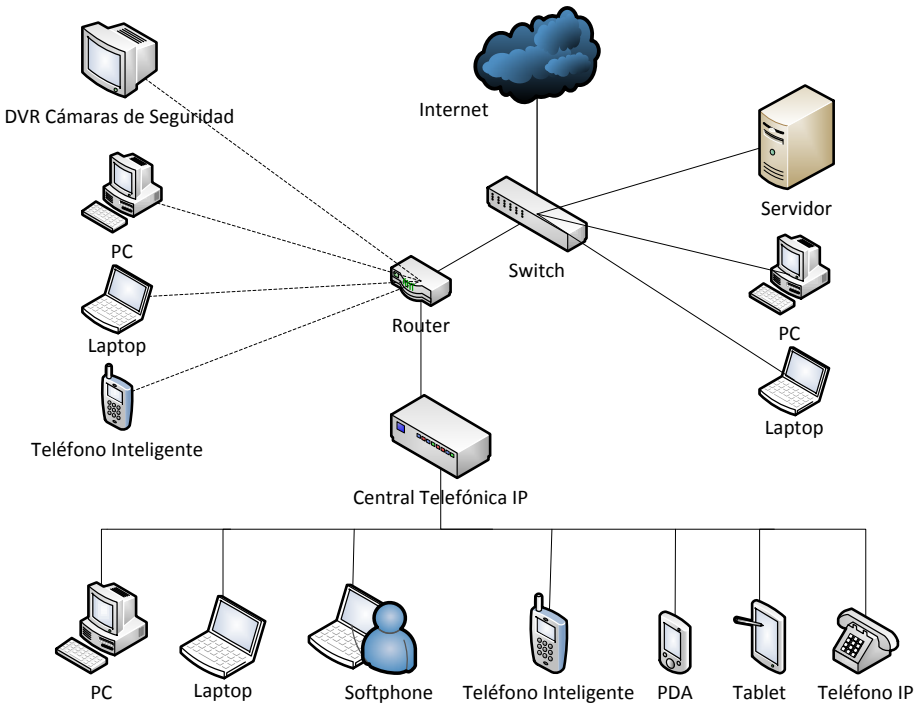

Figura 32. Solución a la red de la Empresa de Transporte Marítimo.
Fuente: Elaboración Propia

Luego de presentarse las tres alternativas, estudiarlas y analizarlas; se dispone a seleccionar la alternativa que más se ajuste a las necesidades da la empresa de Transporte Marítimo. Cada alternativa presenta sus ventajas y desventajas, desde el punto de vista económico, estructural, informativo, escalabilidad, topológico y otros más; factores que ayudaron a tomar la decisión final. La empresa en cuestión, debe tener muy claro que esta solución arrojará los beneficios tiempo después de poner en marcha el proyecto.

Para sustentar esta elección, se muestra una matriz diagnostico basada en ciertos factores y parámetros que se evalúan para la toma de decisión. También se especifica una tabla de ponderación, donde se le coloca un valor al factor o parámetro que se está evaluando para la solución ideal. La tabla de ponderación se muestra a continuación.

Tabla 23. Escala Valoración para la Matriz Diagnóstico

Valor	Descripción
1	Mínima/Mala/Sencilla/Bajo
2	Medía/Regular/Complicada/Moderado
3	Alta/Buena/Difícil/Elevado

Fuente: Elaboración Propia.

Matriz con parámetros a evaluar para la elección de la solución ideal.

Tabla 24. Matriz de Diagnóstico elección solución ideal

Parámetro	Primera Alternativa	Segunda Alternativa	Tercera Alternativa
Ventajas	3	3	3
Desventajas	2	1	2
Seguridad	3	3	3
Telefonía	2	3	3
Conexión a Internet	1	3	3
Instalación	1	1	1
Escalabilidad	2	3	2
Topología	1	1	1
Tecnología	3	3	3
Servicio Post Venta	2	3	2
Costo	1	2	3

Fuente: Elaboración Propia.

Al comparar las tres alternativas en cada uno de los parámetros que se muestran en la matriz de diagnóstico, junto con los requerimientos que

planteados por la empresa en cuestión, se obtiene que la solución ideal es la segunda alternativa.

Económicamente cualquiera de las tres alternativas representa una fuerte inversión. En el caso de la segunda alternativa se invierten en la adquisición de nuevos equipos, software y hardware; los cuales son exportados en su mayoría, buscando minimizar en lo posible el gasto a realizar. También se adquieren los servicios de un nuevo proveedor telecomunicaciones, específicamente en la parte de red de datos. Este nuevo proveedor ofrece grandes cambios y beneficios en comparación con el actual proveedor, otorgando la posibilidad de migrar hacia VoIP. El costo de la adquisición del software y hardware, es uno solo; sin embargo, mensualmente hay que cancelar lo correspondiente a la red de datos.

Técnicamente, esta alternativa tiene varias características que ayudaron a tomarla como la solución ideal. De esta manera la parte económica no es el aspecto fundamental en la decisión, ya que en este caso se busca la relación costo/beneficio, y sobre todas las cosas, dar solución a los problemas que se han venido planteando.

Adquirir un nuevo proveedor de telecomunicaciones, implica la mejora en la transmisión de datos. Este nuevo proveedor entrega un ancho de banda dedicado de 2048 Kbps simétrico. Con este ancho de banda, se empezará a trabajar y se verá el comportamiento de voz, datos y videos en la misma red. Para poder llegar a la oficina de la empresa en cuestión, deben hacer uso de la infraestructura existente en el edificio donde se ubica la oficina, acatando las normas que existan para no presentar inconvenientes. Una vez que llegan a la oficina de la empresa en cuestión, usan el cableado estructurado que existe para llegar al cuarto principal donde se encuentra el rack, switch y Gateway que distribuyen la red interna.

La central IP Asterisk Appliance 50, es ideal para pequeñas o medianas empresas, soportando 16 líneas telefónicas en este caso. Es una solución

hibrida, por la capacidad que posee de trabajar con aplicaciones VoIP usando los equipos de telefonía tradicional. Este aspecto es beneficioso para empresas que no quieren migrar a Telefonía IP por completo sino ir haciéndolo de manera escalonada.

Esta central es de fácil instalación y se acopla de una vez a la red telefónica existente. Además funciona como servidor de correo electrónico, servidor de conferencia y VoIP Gateway. Su configuración es fácil y sencilla, disminuyendo los costos soporte.

Los teléfonos IP D40 y D50 de Digium, son equipos de última generación; trabajan específicamente con Asterisk. Incluyen audio de alta definición e implementación plug-and-play, con solo conectar el teléfono ubica y configura el sistema Asterisk que se encuentra en la red. Luego selecciona el usuario que va asignar al teléfono y lo configura al instante. Tienen aplicaciones de teléfonos nativos como correo de voz, directorio, grabación de llamadas, llamadas en espera, entre varias características más.

Incluye un aplicación llamada App Engine Digium, es una característica innovadora que permite al usuario construir y desplegar aplicaciones personalizadas. Las aplicaciones suministradas en los teléfonos IP Digium, están desarrolladas con la API de JavaScript. La interfaz gráfica, permite entrar a las aplicaciones de manera rápida y sencilla.

Otro tipo de teléfonos que se propone son los softphone. Son emuladores de teléfonos físicos pero que se instalan en las computadoras y se manejan a través de su interfaz gráfica. Linphone, es un softphone de software libre, que se descarga directamente de su sitio web. De fácil instalación y funcionamiento, que se puede instalar tanto en computadoras como equipos móviles, permitiendo la comunicación a grandes distancias sin costos adicionales. Es compatible con Asterisk, y funciona con el SO Windows, que es el instalado en las computadoras de la empresa en cuestión.

Los sistemas de seguridad son muy necesarios para el resguardo principalmente de la información. A esto también se le suma el hecho que ayudan resguardan la integridad física de los empleados y de las instalaciones. Dependiendo de las dimensiones de la oficina, como la carga de información existente, se incorporan más sistemas de seguridad o se mejoran los existentes.

Para el acceso a la oficina, el portero o timbre es el mismo que está en uso. Permite tener conocimiento de la persona que desea entrar a la oficina, a través de una cámara y de un intercomunicador, así se tiene contacto con esa persona antes de entrar a la oficina. Su instalación es pequeña y sencilla ya que va desde la puerta principal hasta la recepción.

Un DVR y cuatro cámaras IP, integran el sistema de cámaras de seguridad, que ubicadas en puntos importantes de la empresa, dan visión del área que se desea resguardar. El software de seguridad se encuentra instalado en el DVR y desde allí se manejan las cámaras de seguridad. Puede ser configurado de tal manera, tener acceso a las cámaras a través de Internet. De esta manera este sistema se integra a la red IP junto a voz, datos y videos. Las cámaras al ser IP, reducen espacio y costo en instalación, ya que no es necesaria la utilización de cables para su conexión al DVR.

Para el resguardo de información se implementaran varias normas que indiquen el manejo y como guardar de manera segura la información física que se encuentra en la oficina. En cuanto a la información que está en las computadoras, se contará con un software (antivirus), que protege la información, evitando las amenazas tan comunes que en la actualidad se encuentran en Internet. Hackers, robos de identidad, software malicioso son algunos de los ataques que puede sufrir la información. Este antivirus se instala en cada una de las estaciones de trabajo y se configura para que periódicamente este analizando el equipo sobre ataques y se actualice. La licencia de este software se renueva anualmente.

Capítulo VI. Conclusiones y Recomendaciones

VI.1 Conclusiones

Al estudiar la situación actual de los sistemas de seguridad y sistemas de telecomunicaciones, se detectan las fallas y vulnerabilidades (problemas con las líneas telefónicas, lo lenta que es la conexión a Internet y sus constantes interrupciones, la falta de seguridad y resguardo de la información), las cuales son las que se desean corregir con el presente trabajo. En cuanto a los sistemas de seguridad, se realizó un estudio detallado de los riesgos a los que se encuentra expuesta la información, junto con los servicios y equipos. La información física está mal organizada y guardada, estando a disponibilidad de cualquier persona ajena a la empresa. No existen normas para el uso de Internet, permitiendo navegar en cualquier página web y descargar programas o archivos que resultan potencialmente peligrosos para la información, dejando en riesgo la información que se encuentra en las estaciones de trabajo.

Igualmente para los sistemas de telecomunicaciones se analizó el funcionamiento actual de sus servicios, los beneficios y ganancias que están aportando a la empresa. Tanto la telefonía como Internet, son parte fundamental en las labores diarias de la empresa. A través de ellas se mantiene contacto con clientes y proveedores a nivel nacional e internacional (mediante su sitio web o llamadas telefónicas), permitiendo concretar transacciones a grandes distancias sin la necesidad de estar físicamente en el sitio.

De estos estudios se obtuvo también información sobre las características de la red interna, la infraestructura, topología; aspectos a través de los cuales se va a desplegar el desarrollo de la solución que se plantee.

Migrar hacia la telefonía VoIP, será la punta de lanza para el crecimiento tecnológico en el área de telecomunicaciones de la empresa en cuestión.

Con ella no solo se logra corregir el grave problema con las líneas telefónicas, sino también permite iniciarse en nuevas prácticas laborales, como lo son la videoconferencia y teleconferencia.

Para la solución de Telefonía IP, se propone la aplicación Asterisk, ya que esta permitirá trabajar con líneas analógicas, VoIP, terminales analógicos y digitales, SIP, softphone entre otras. La IP-PBX, los teléfonos IP y el softphone seleccionados trabajan exclusivamente con Asterisk, además de sus características y bondades que ofrecen.

Los sistemas de seguridad no van a eliminar por completo los ataques a la información o impedir el acceso de personas no deseadas a la empresa, pero si son mecanismos que van ayudar a mantener controlada la manipulación de la misma, autorizar la descarga de software que no afecten la integridad de las computadoras y por ende, la información allí almacenada. Guardar de manera adecuada la información escrita, manteniéndola a la mano y con fácil acceso pero restringida para personas ajenas a la misma. Estos sistemas de seguridad, deben ser actualizados constantemente para su buen funcionamiento.

Instalar software en las computadoras (antivirus, firewall) que protejan la información de spyware, malware, ataques, robos. El sistema de cámaras de seguridad será a través de un DVR. Este es un equipo estrictamente para las cámaras de seguridad y no de uso diario como lo es en la actualidad la computadora donde se encuentran instalados el hardware y software de las cámaras de seguridad.

Para el ancho de banda se decide empezar con un enlace dedicado de 2048 kbps, aunque éste no es el ideal porque el video consume gran parte del ancho de la red cuando se hace uso del mismo. Por lo que una videoconferencia entre un cierto número de personas, disminuiría notoriamente la calidad de la red. Se toma esta decisión principalmente para reducir el gasto que genera la incursión de la empresa en la tecnología VoIP.

No obstante, se llevará un control del desempeño de la red IP con este ancho de banda y de allí, se obtendrán nuevas conclusiones en pro de la convergencia de voz, datos y video en la misma red.

Como el actual proveedor de los servicios de Internet no cumple con los requerimientos de la empresa, es imperante contactar otro proveedor que pueda garantizar las condiciones necesarias e ideales para el buen funcionamiento de las actividades diarias de la empresa. La velocidad de conexión a Internet permita acceder a los sitios web rápidamente a cualquier hora del día; las interrupciones del servicio sean mínimas y en el momento de presentarse alguna, sea por fallas ajenas al nuevo proveedor.

Como resultado de la comparación de las tres alternativas plateadas a través de la Matriz de Diagnóstico, se puedo seleccionar la segunda alternativa como la solución técnica ideal. Se llegó a este resultado después de comparar los siguientes parámetros entre sí: ventajas, desventajas, seguridad, telefonía, Internet, escalabilidad, costos, entre varios más. De esta forma, la segunda alternativa resultó la más atractiva desde el punto de vista técnico y económico.

La integración de voz, datos y video en la misma red, junto con los sistemas de seguridad, constituye un avance fundamental en la convergencia del área de las telecomunicaciones para la empresa de Transporte Marítimo.

VI.2 Recomendaciones

Para disminuir los costos asociados a la Telefonía VoIP, se puede migrar a la misma por etapas, es decir, adquirir primero la central IP, luego los teléfonos IP y así sucesivamente, para que al final en un período de tiempo no muy largo, se tenga la infraestructura completa de la Telefonía IP. De esta manera, la adaptación de la empresa a esta nueva tecnología es mejor, ya que se va corroborando el buen funcionamiento de cada etapa que se realiza. también se adapta mejor al presupuesto de la empresa, aunque en general es un gasto fuerte, al ser por etapas, el gasto es fraccionado, dejando tiempo para que la empresa pueda recuperar la inversión hecha.

Constantemente los ataques y amenazas a la información se actualizan y mejorando, por lo que es importante tener actualizados los sistemas de seguridad. Si se observa que estos sistemas son insuficientes, se pueden incorporar nuevos software o hardware que van a fortalecer la seguridad. Un ejemplo, conectar las estaciones de trabajo a un UPS. Son equipos que cuentan con una batería que almacena energía, siendo capaz de proporcionar energía eléctrica por un tiempo determinado a la hora de un apagón. De esta manera se puede guardar correctamente la información que se está trabajado, evitando daños en la misma.

El departamento de sistemas deberá redactar un informe en el cual muestre las pautas y condiciones para el manejo y resguardo de la información, tanto digital como física. Igualmente se debe incluir normas para navegar en Internet, ya que muchos sitios web o archivos descargables, son potencialmente perjudiciales para la el equipo donde se guarda la información. No todo el personal puede manejar toda la información que se posee, por lo que se tiene que sectorizar y señalar el campo de trabajo de cada uno de los empleados.

Es importante que las estaciones de trabajo dentro de la empresa cumplan con las condiciones tanto técnicas (S.O, memoria, capacidad en disco) como

de ambiente (temperatura controlada, cableado estructurado, puesta a tierra, eliminación del polvo) necesarias para la instalación del hardware y software adquirido. De no cumplir estas características, se recomienda primero actualizar y/o mejorar las mismas.

Promover la formación de personal especializado en Redes y Telefonía VoIP, por medio de cursos dirigidos específicamente a estas áreas, los cuales posteriormente, serán los encargados de prestar el servicio técnico necesario para estas tecnologías.

Es de gran importancia mantener un plan de contingencia vigente para el resguardo de la información, que permite a la empresa adaptarse a cualquier situación de riesgo que se pueda presentar, tanto natural como provocada.

Se recomienda que el ancho de banda ideal para que converjan voz, datos y videos adecuadamente en la misma red, sea un enlace dedicado entre 8 y 10 Megas; aunque no siempre se utilice este ancho de banda. De esta manera se garantiza la calidad de la red cuando se haga uso de voz y video al mismo tiempo. Sin embargo, dependiendo del uso de voz y video en la red, se debe aumentar a mediano o largo plazo el ancho de banda por el ideal. Esta situación debe estar clara entre el cliente y el proveedor, especialmente este último, quien debe contar con la capacidad de incrementar la velocidad de ser requerida.

Tener un segundo proveedor de los servicios de red de datos aunque parezca redundante, es importante ya que este sirve como back-up al momento de presentarse algún inconveniente con el proveedor principal. Este debe ofrecer las mínimas condiciones necesarias para que la red IP se mantenga operativa mientras se solventa el inconveniente presentado con la red principal.

Referencia Bibliografía

2GC S.H. (2012). *http://www.ciscocignal.com/*. Recuperado el 26 de 10 de 2012, de http://www.ciscocignal.com/products/view/16-telefono-ip-cisco-small-business-spa303-3-lineas.html

3CX 2013. (2013). *3CX*. Recuperado el 2013 de 05 de 01, de http://www.3cx.es/

Anderruthy, J.-N. (2007). *Skype y Telefonía IP.* Barcelona: Ediciones ENI.

Areitio, J. (2008). *Seguridad de la Informacion, Redes, Informatica y Sistemas de informacion.* Madrid: Paraninfo.

Borghello, C. (2001). *Segu-Info.* Recuperado el 27 de septiembre de 2012, de http://www.segu-info.com.ar/tesis/

Calle, J. (1997). *Reingenieria y Seguridad en el Ciberespacio.* España: Díaz de Santos, S.A.

Campagnaro, S., & Sandoval Lozano, Z. (2010). Disposiciones generales sobre el trabajo de grado especial. *Disposiciones generales sobre el trabajo de grado especial*, (pág. 1). Caracas.

Cisco Systems, Inc. (2010 a). *Cisco*. Recuperado el 2012 de septiembre de 27, de Lo que usted necesita saber sobre seguridad de la red: http://www.cisco.com/web/LA/soluciones/la/information_security/index.html

Cisco Systems, Inc. (2010 b). *Cisco*. Recuperado el 2012 de septiembre de 27, de Seguridad de Informacion: http://www.cisco.com/web/LA/soluciones/la/information_security/index.html

CNT. (2013). Recuperado el 2013 de 04 de 29, de http://speedtest.cnt-grms.com.ec/

CompuResale. (2013). *CompuResale*. Recuperado el 2013 de 05 de 04, de http://www.compuresale.com/index.php

Cisco. (2010). Recuperado el 2012 de septiembre de 27, de Lo que usted necesita saber sobre seguridad de la red: http://www.cisco.com/web/LA/soluciones/la/information_security/index.html

Cisco. (2010). Recuperado el 2012 de septiembre de 27, de Seguridad de Informacion: http://www.cisco.com/web/LA/soluciones/la/information_security/index.html

Dictionarist.com. (2011). *Dictionarist*. Recuperado el 11 de 30 de 2012, de http://definicion.dictionarist.com/shipping

Digium, Inc. (2013 b). *Digium*. Recuperado el 01 de 05 de 2013, de http://www.digium.com/en/products/asterisk/phones

Digium, Inc. (2013). *Digium*. Recuperado el 24 de 03 de 2013, de http://www.asterisk.org/get-started

EFXTO comunidad forex. (2012). *EFXTO Comunidad Forex*. Recuperado el 30 de 11 de 2012, de http://www.efxto.com/diccionario/b/3432-broker

FONDONORMA. (2005). Sistema de Cableado Estructurado para Servicios de Telecomunicaciones en Edificios Comerciales. Diseño e Instalacion. Caracas.

FUNDIBEQ. (2010). *FUNDIBEQ Fundacion Iberoamericana para la Gestion de la Calidad*. Recuperado el 09 de 11 de 2012, de http://www.fundibeq.org/opencms/export/sites/default/PWF/downloads/gallery/methodology/tools/amfe.pdf

Garcia-Cervigón, A., & Alegre, M. (2011). *Seguridad Informatica.* Madrid: Paraninfo.

Garía-Cervigón Hurtado, A., & Alegre Ramos, M. D. (2011). *Seguridad Informatica.* Madrid: Paraninfo.

GC Alarmas y Monitoreo. (2012). *GC Alarmas Y Monitoreo S.A.C.* Recuperado el 04 de octubre de 2012, de http://www.gcalarmasymonitoreo.com/productos-y-servicios/seguridad-administrativa/

GC Alarmas Y Monitoreo S.A.C. (2012). Recuperado el 04 de octubre de 2012, de http://www.gcalarmasymonitoreo.com/productos-y-servicios/seguridad-administrativa/

Gil , P., Pomares , J., & Candelas, F. (2010). *Redes y Transmision de Datos.* Alicante: Publicaciones Universidad de Alicante.

Gómez López, J., & Gil Montoya, F. (2008). *VoIP y Asterik.* Almeria: Alfaomega.

Guitian, J. (2010). *PROPUESTA PARA IMPLEMENTAR REDES DE VOZ Y DATOS. CASO EDELCA.* Tesis Especialización, Universidad Metropolitana, Caracas.

Gutiérrez Gil, R. (2013). *http://issuu.com.* Recuperado el 22 de 02 de 2013, de http://issuu.com/dragonjar/docs/seguridad-voip

Hernández, M. J. (2004). *Evaluación de los mecanismos de seguridad en los sistemas de notificación y registro de eventos para la gestión de redes.* Tesis Especialización, Caracas.

Herrera. (2003). *Tecnologia de redes y Transmision de Datos.* Mexico, D.F.: Limusa.

Herrera, E. (2003). *Tecnologia de redes y Transmision de Datos.* Mexico, D.F.: Limusa.

Hotfixed / Comunidad de Software Libre. (2013). *http://hotfixed.net/*. Recuperado el 24 de 03 de 2013, de http://hotfixed.net/2011/05/21/top-5-softphones-gratuitos/

Inversiones Teleiva.com19, C.A. (2013). *Teleiva*. Recuperado el 23 de 01 de 2013, de http://teleiva.com.ve/telefonos-panasonic-analogicos-digitales/telefonos-inalambricos-panasonic.html

Investopedía EE.UU. (2012). *Investopedía*. Recuperado el 14 de 11 de 2012, de http://www.investopedía.com/terms/b/broker.asp#axzz2CGAgRKSn

Kaspersky Lab ZAO. (2013). *Kaspersky*. Recuperado el 04 de 04 de 2013, de http://latam.kaspersky.com/productos-para-empresas/total

KOCOM. (2013). *Kocom*. Recuperado el 23 de 01 de 2013, de http://www.kocom.com/?construct=productContent&fz=kocom&productCategory=66&productMiddle=13&productDetail=97&pNo=588

LanPro. (2013). *LANPRO*. Recuperado el 22 de 01 de 2013, de http://www.lanpro.com/documents/sp/cablingsys/LPPATCHPANELCAT5E_SS_SPB01W.pdf

Linksys. (2013). *http://www.linksys.com/en-us/home*. Recuperado el 2013 de 03 de 22, de http://support.linksys.com/en-us/support/routers/WRT54G2

Linphone. (2010). *http://www.linphone.org/*. Recuperado el 24 de 03 de 2013, de http://www.linphone.org/eng/features/

Mendillo, V. (2012 a). Introduccion a la Seguridad informatica. Caracas, Venezuela.

Mendillo, V. (2012 b). Seguridad Fisica y Ambiental. Caracas, Venezuela.

Mendillo, V. (2012). Introduccion a la Seguridad informatica. Caracas, Venezuela.

Mendillo, V. (2012). Seguridad Fisica y Ambiental. Caracas, Venezuela.

Mendillo, V. (2012). Vulnerabilidades y Riesgos 1. Caracas, Venezuela.

Mendillo, V. (2013 c). Seguridad en VoIP.

MercadoLibre Venezuela S.R.L. (2013). *Mercado Libre*. Recuperado el 10 de 05 de 2013, de http://articulo.mercadolibre.com.ve/MLV-407809802-camara-seguridad-domo-13-cmos-sony-color-audio-380-lineas-_JM

MercadoLibre Venezuela S.R.L. (2013). *Mercado Libre*. Recuperado el 10 de 05 de 2013, de http://articulo.mercadolibre.com.ve/MLV-408830538-dvr-stand-alone-hikvision-8ch-1aud-240fps-ds-7208hvi-stsn-_JM

Microsoft. (2013). *Windows Microsoft*. Recuperado el 03 de 04 de 2013, de http://windows.microsoft.com/es-419/windows-vista/what-is-a-firewall

Navarro, H. (2012). *Angelfire.com*. Recuperado el 10 de octubre de 2012, de http://www.angelfire.com/biz/HUMBERTOLOTNAVARRO/glosario.html#K

Panafonic, S.L. (2013). *Panafonic*. Recuperado el 22 de 01 de 2013, de http://www.panafonic.com/pbx/kxt7633.htm

Pouseele, S. (2002). *ISAserver.org*. Recuperado el 26 de 10 de 2012, de http://www.isaserver.org/articles/Using_NetMeeting_and_the_H323_Gatekeeper_as_a_HelpDesk_tool.html

Promigas Telecomunicaciones, S. (2012). *Promigastel.com*. Recuperado el 10 de octubre de 2012, de http://www.promitel.com/glosario.htm

QuinStreet Inc. (2012). *Webopedía*. Recuperado el 08 de 11 de 2012, de http://www.webopedía.com/TERM/R/RJ_45.html

redesdedatosinfo.galeon.com. (2012). Recuperado el 04 de octubre de 2012, de http://redesdedatosinfo.galeon.com/enlaces2128619.html

Ross, J. (2007). *VoIP voz sobre IP.* Rio de Janeiro: Antenna Edicoes Tecnicas.

Soler Palacín, E. (2013). *http://upcommons.upc.edu/.* Recuperado el 2013 de 03 de 05, de http://upcommons.upc.edu/pfc/bitstream/2099.1/8373/1/Memoria%20PFC%20-%20Erika%20Soler.pdf

Stallings, W. (2004). *Fundamentos de Seguridad en Redes.* Madrid: Pearson Prentice Hall.

Telecomunicaciones Bantel C.A. (2013). *Bantel Telecomunicaciones*. Recuperado el 2013 de 05 de 03, de http://www.bantel.com.ve/productos/conectividad.htm

TP-LINK Technologies Co., Ltd. (2013). *TP-LINK*. Recuperado el 23 de 01 de 2013, de http://www.tp-link.com/ve/products/details/?model=TL-SF1024

Valarino, E., Yáber, G., & Cemborain, M. S. (2010). *Metodología de la Investigación. Paso a Paso.* México D.F.: Trillas.

Velásquez, J. (2010). *Implementacion de una solución VoIP: Caso de estudio NEOPRANA TECHNOLOGIES C.A.* Tesis Especialización, Caracas.

Voxdata Comunicaciones IP. (2010). *Voxdata Comunicaciones IP*. Recuperado el 02 de 04 de 2013, de http://www.voxdata.com.ar/dvr.html

Wasylkowski, K. (2007). *Implementacion de una red de telefonia IP en la sede de Fe y Alegria en Caracas.* Tesis Especialización, Caracas.

www.civ.net.ve. (2012). *Colegio de Ingenieros de Venezuela*. Recuperado el 11 de octubre de 2012, de http://www.civ.net.ve/uploaded_pdf/cep.pdf

www.telavip.com.ve. (2013). *telavip.com.ve*. Recuperado el 23 de 01 de 2013, de http://www.telavip.com.ve/centrales_telefonicas/centrales_telefonicas_con_tecnologia_ip/kx-tda30/kx-tda30.html

ZoIPer.com. (2012). *ZoIPer*. Recuperado el 2013 de 05 de 01, de http://www.zoiper.com/softphone/classic/

Anexos

Anexo 1. Normas para Cableado Estructurado.

Algunas de las normas más importantes para el cableado estructurado son:

Normas
Estándar ANSI/TIA/EIA.
Normas Venezolanas
COVENIN 398: 1984 Símbolos gráficos para instalaciones eléctricas.
COVENIN 2730: 1990 Nomenclatura en relación con centrales privadas automáticas.
FONDONORMA 200: 2004 Código Eléctrico Nacional.
Elementos principales del cableado estructurado
Cableado Horizontal.
Cableado de Backbone.
Cuarto de Telecomunicaciones.
Cuarto de Equipos.
Cuarto de Entrada de Servicios.
Sistema de Puesta a Tierra.

Fuente: FONDONORMA (2005)

Anexo 2. Cuadro comparativo del software IP PBX Asterisk y el software IP PBX 3CX.

Asterisk	3CX
• Es un open source bajo la licencia GNU General Public License (GPL). • Software altamente usado, probado y recomendado • Software completo, que dispone de todas las funciones de una PBX. • Amplia documentación, manuales y libros en español. • Soporta los protocolos SIP, H.323 IAX. • Posee una amplia comunidad de desarrolladores de habla hispana. • Se ejecuta en los Sistemas Operativos Linux, Windows, OS X. • Compatible con los equipos y appliance desarrollados por Gigium.	• Es un software propietario, aunque se puede descargar de manera gratuita en Internet. • Corre solamente en el Sistema Operativo Windows. • Permite la instalación de una central telefónica o PBX basada en una computadora. • Puede configurarse como servidor SIP. • Permite conexión de softphone, teléfonos físicos y líneas telefónicas tradicionales. • Posee funciones tradicionales de una PBX. • Existe un foro en español donde prestan ayuda y asistencia técnica.

Fuente: Elaboración Propia

Anexo 3. Cuadro comparativo entre la IP PBX Asterisk Appliance 50 (AA50) y la IP PBX 3CXPSENT.

Asterisk Appliance 50 (AA50)	3CXPSENT
• Su tipo de licencia es código abierto. • Soporta los protocolos SIP, H.323, IAX. • Servidor Asterisk completo con AsteriskGUI. • Asterisk Business Edition Embadded con licencia comercial. • Funciona como router para pequeñas empresas. • Tarjeta Compact Flash de 1GB.	• Sistema telefónico completo, proporciona conmutación de llamadas, enrutamiento y colas. • Su configuración se puede realizar a través de la web. • Elimina el cableado telefónico. • Permite 32 llamadas simultáneas. • Hace uso del estándar SIP. • Correo de voz, correo electrónico de voz, operadora automática. • Tiene un costo de 1.995,00 dólares americanos.

• 8 MB de memoria flash. • 64 MB de memoria RAM. • 5 puertos Ethernet (4 LAN, 1 WAN). • Tiene un costo de 1.399,00 dólares americanos.	

Fuente: Elaboración Propia

Anexo 4. Teléfono IP Digium D40.

Fuente: Digium, Inc. (2013 b)

Anexo 5. Teléfono IP Digium D50

Fuente: Digium, Inc. (2013 b)

Anexo 6. Cámara Domo 1/3 Cmos Sony Color

Fuente: MercadoLibre Venezuela S.R.L (2013)

Anexo 7. DVR Stand Alone Hikvision 8 canales

DS-7208HVI-ST/SN

Video/Audio Input	Video Compression:	H.264
	Analog Video Input:	8-ch
	PAL/NTSC Adaptive:	Support
	Video Input Interface:	BNC (1.0 Vp-p, 75Ω)
	Audio Compression:	G.711
	Audio Input:	1-ch
	Audio Input Interface:	RCA (2.0 Vp-p, 1 kΩ)
	Two-way Audio:	1-ch RCA(2.0Vp-p, 1kΩ)
Video/Audio Output	VGA Output:	1-ch, resolution: 1280×1024/60Hz, 1024×768/60Hz
	CVBS Output:	1-ch, BNC connector (1.0 Vp-p, 75 Ω); Resolution: PAL: 704 × 576, NTSC: 704 × 480
	Recording resolution:	4CIF/2CIF/CIF
	Frame Rate:	Main stream: 4CIF / 2CIF @ 8 fps Sub stream: CIF / QCIF
	Video Bit Rate:	32Kbps~2048Kbps, or user-defined (Max.3Mbps)
	Stream Type:	Video/Video&Audio
	Audio Output:	1-ch RCA(Linear, 1kΩ)
	Audio Bit Rate:	64kbps
	Dual Stream:	Support
	Synchronous Playback:	8-ch
Hard Disk Driver	Interface Type:	1 SATA Interface
	Capacity:	Up to 2TB capacity for each disk
External Interface	Network Interface:	1 RJ45 10M/100M adaptive Ethernet Interface
	USB Interface:	2 USB 2.0 Interfaces
	Serial Interface:	1 RS-485 interface
General	Power Supply:	12 VDC
	Consumption:	≤10W (without hard disk or DVD-R/W)
	Working Temperature:	-10 °C ~ +55 °C
	Working Humidity:	10% ~ 90%
	Chassis:	Standalone 1U chassis
	Dimensions:	315 (W)× 230(D) × 45 (H)mm
	Weight:	≤ 2kg (without hard disk or DVD-R/W)

Fuente: MercadoLIbre Venezuela S.R.L (2013)