UNIVERSIDAD NACIONAL DE LOJA

PFC-CIS-002

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Implementación de protocolos de seguridad para la red VoIP del Hospital Isidro Ayora de Loja"

Tesis previa a la obtención del título de Ingeniero en Sistemas

AUTOR:

- ***Cristian Leonardo Calderón Ordoñez***

DIRECTOR:

- ***Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.***

LOJA- ECUADOR

2015

CERTIFICACIÓN

Ing. Carlos Miguel Jaramillo Castro, Mg. Sc

DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS DEL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES Y DIRECTOR DE TESIS.

CERTIFICA:

Haber dirigido, revisado y corregido en todas sus partes el desarrollo de la tesis denominada **"IMPLEMENTACIÓN DE PROTOCOLOS DE SEGURIDAD EN LA RED DE VOIP DEL HOSPITAL ISIDRO AYORA DE LOJA"**, con autoría del egresado **Cristian Leonardo Calderón Ordoñez.**

En razón de que la misma reúne los requisitos de fondo y forma, exigidos para la investigación de este nivel, por ello autorizo su presentación sustentación y defensa ate el tribunal designad para el efecto.

Loja 06 de Octubre del 2015

……..

Ing. Carlos Miguel Jaramillo Castro, Mg. Sc

DIRECTOR DEL TRABAJO DE TITULACIÓN

AUTORÍA

Yo **CRISTIAN LEONARDO CALDERÓN ORDOÑEZ,** declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional – Biblioteca Virtual.

Firma: 

Cédula: 1104617053

Fecha: 14-XII-2015

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo **CRISTIAN LEONARDO CALDERÓN ORDOÑEZ**, declaro ser autor de la tesis titulada: **IMPLEMENTACIÓN DE PROTOCOLOS DE SEGURIDAD PARA LA RED VOIP DEL HOSPITAL ISIDRO AYORA DE LOJA,** como requisito para optar al grado de: **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 14 días del mes de Diciembre del dos mil quince.

Firma: 

Autor: Cristian Leonardo Calderón Ordoñez

Cédula: 1104617053

Dirección: Loja, San José Alto (Francisco Arias y Francisco Cumbicus)

Correo Electrónico: clcalderono@unl.edu.ec

Teléfono: 072- 561-336 **Celular:** 0994910707

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Carlos miguel Jaramillo Castro, Mg.Sc.

Tribunal de Grado: Ing. Mario Enrrique Cueva Hurtado Mg.Sc.

Ing. Pablo Fernando Ordóñez Ordóñez, Mg.Sc

Ing. Waldemar Victorino Espinoza Tituano, Mg.Sc

DEDICATORIA

A ti mi Dios, que me has concedido la oportunidad de vivir y de regalarme una familia maravillosa, a mi padre que ha sido el eje fundamental en mi diario vivir, a mi madre que hizo y dio todo para que pudiera lograr mis sueños, a mi esposa que ha sido la incansable compañera en las noches de desvelo, gracias por motivarme y darme la mano, cuando sentía que el camino se terminaba, a mi hija, quien ha sido fuente de inspiración, para poder alcanzar mi anhelado sueño, y convertirme en un ejemplo para ella, gracias a cada uno de ustedes y a todos quienes estuvieron a mi lado, brindándome su paciencia y comprensión para cumplir con la meta propuesta.

Cristian Leonardo Calderón Ordoñez.

AGRADECIMIENTO

Mi agradecimiento profundo primeramente a mi Dios, quien ha sido mi guía por los senderos de la vida, a mis padres, mi esposa y familiares quienes con sus palabras de aliento, y sabios consejos han contribuido en la formación de mi carácter, para convertirme en persona de bien y un servidor de nuestra sociedad.

Al Ing. Carlos Miguel Jaramillo Castro, Mg.Sc. Director del presente trabajo de fin de carrera y amigo incondicional, le estoy eternamente agradecido por el apoyo absoluto y entusiasmo, por ser, quien me motivó para seguir adelante, a través de sus directrices, consejos y enseñanzas.

Expreso mis más sinceros agradecimientos, a las autoridades de la Universidad Nacional de Loja, al Director del Área de Energía, las Industrias y los Recursos Naturales no Renovables, al Coordinador de Carrera de Ingeniería en Sistemas y a todo el personal administrativo, que labora en esta prestigiosa institución.

A todos los docentes, de la Carrera de Ingeniería en Sistemas, quienes compartieron sus conocimientos intelectuales, los mismos que sirvieron de base para mi formación académica, laboral y profesional; gracias por todos sus consejos que ayudan y seguirán ayudando en el desempeño social.

Así mismo, mil gracias al personal técnico y administrativo que labora en el Hospital Isidro Ayora de Loja, por confiar en mi capacidad y abrirme las puertas para obtener información afines a la investigación, gracias por facilitar el uso de equipos y espacio físico, porque a través de estos se llegó a una exitosa culminación del presente trabajo investigativo.

Para todos solo me queda decir

“MIL GRACIAS”

El Autor….

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS.

GLOSARIO DE TÉRMINOS.

A
ACK ACKNOWLEDGEMENT.
ACL Access Control List.
AH Authentication Header.
ARP Address Resolution Protocol.
B
BPDU Bridge Protocol Data Units.
BW Bandwidth.
C
CAM Content Addressable Memory.
CIA Confidentiality, Integrity, Availability.
CPU Central Processing Unit.
CRC Cyclic Redundancy Check.
CUCM Cisco Unified Communications Manager.
CUPS Cisco Unified Presence Server.
D
DDoS Distributed Denial of Service.
DES Data Encryption Standard.
DH Diffie Hellman.
DHCP Dynamic Host Configuration Protocol.
DMZ Demilitarized Zone.
DoS Denial of Service.
DTP Dynamic Trunk Protocol.
E
ESP Encapsulating Security Payload.
F
FXO Foreign Exchange Office.
FXS Foreign Exchange Station.
H
H323 Recommendation Del ITU-T.
HIPS Host-based Intrusion prevention system.
HMAC Hash-based Message Authentication Code.
HTTP Hypertext Transfer Protocol.
I
IAX2 Inter-Asterisk eXchange protocol v2.
ICMP Internet Control Message Protocol.
IDS Intrusion Detection System.
IETF Internet Engineering Task Force.
IKE Internet Key Exchange.
IOS Internetwork Operating System.
IP Internet Protocol.
IPS Intrusion Prevention System.
IPsec Internet Protocol Security.
ISL Inter-Switch Link.
ITU International Telecommunication Union.
L
LAN Local Area Network.
M
MAC Media Access Control.
Megaco Media Gateway Control Protocol o H248.
MG Media Gateway.
MGC Media Gateway Controller.
MGCP Media Gateway Control Protocol.
MIKEY Multimedia Internet KEYing.
MITME Multipurpose Internet Mail Extensions.

MKI Master Key Identifier.
MPLS Multi-protocol Label Switching.
N
NAT Network Address Translation.
NDP Neighbor Discovery Protocol
NBIPX NetBIOS sobre IPX

P
PBX Private Branch Exchange.
PKE Performance Key Engineering.
PKI Public Key Infrastructure.
PPTP Point to Point Tunneling Protocol.
PSK Phase Shift Keying.
Q
QoS Quality of Service.
R
RAM Random Access Memory.
RAS Registration Admission Status.
RFC Request for Comments.
RSA Rivest, Shamir y Adleman.
RTCP Real-time Transport Control Protocol.
RTP Real-time Transport Protocol.
S
SAS Short Authentication String.
SCCP Skinny Client Control Protocol.
SDES Security Descriptions for Media Streams.
SDP Session Description Protocol.
SER SIP Express Router.
SG Signaling Gateway.
SHA1 Secure Hash Algorithm 1.
SIP Session Initiation Protocol.
SMS Short Message Service.
SMTP Simple Mail Transfer Protocol.
SNMP Simple Network Management Protocol.
SPAM Correo no deseado.
SPIT Spam Over Internet Telephony.
SRTP Secure Real-time Transport Protocol.
SS7 Signaling System No 7.
SSH Secure Shell.
SSL Secure Sockets Layer.
STP Spanning tree Protocol.
T
TCP Transmission Control Protocol.
TFN Tribe Flood Network.
TFTP Trivial File Transfer Protocol.
TLS Transport Layer Security.
U
UDP User Datagram Protocol.
UMTS Universal Mobile Telecommunications System.
URL Uniform Resource Locator.
V
VLAN Virtual Local Area Network.
VLT Virtual LAN Trunk.
VoIP Voice over IP.
VPN Virtual Private Network.
Z
ZRTP Media Path Key Agreement for Unicast Secure RTP.

1. TÍTULO.

“IMPLEMENTACIÓN DE PROTOCOLOS DE SEGURIDAD PARA LA RED VOIP DEL HOSPITAL ISIDRO AYORA DE LOJA”

2. RESUMEN.

El presente trabajo de fin de carrera, está orientado a realizar un análisis de las amenazas que afectan a las redes de *(VoIP),* aprovechando cualquier debilidad de la red, para ello se realizó un escáner, con la finalidad de encontrar los equipos que la conforman, así como las extensiones, que dispone la *(PBX),* utilizando herramientas informáticas, denominados (*sniffers*), las cuales determinan qué debilidades existen actualmente en la red, para lograr este objetivo, se trabajó sobre un escenario de pruebas, donde dos máquinas conectadas a la *(PBX),* se comunican entre sí y una tercera máquina intrusa, que ha logrado ingresar a la red, captura la comunicación establecida entre los atacados, logrando así grabar las llamadas, que se establecen entre las dos víctimas, utilizando la técnica de *eavesdropping*, la cual tiene como objetivo, interceptar datos en una transmisión de manera no autorizada.

Para el desarrollo del presente proyecto, se utilizaron las siguientes metodologías: ***OSSTMM***, por ser una de las más utilizadas, para la búsqueda y verificación de vulnerabilidades, en redes que disponen de una conexión a Internet, junto con la distribución *Kali Linux* , por ser un sistema operativo, que cuenta con un sinnúmero de herramientas, especializadas para pruebas de seguridad o lo que se conoce como *ethical hacking***,** así mismo, para el análisis y gestión de riesgos, se utilizó la metodología ***OCTAVE***, con el fin de clasificar el nivel de riesgos, según las vulnerabilidades encontradas en la red de telefonía *(IP),* del Hospital Isidro Ayora de Loja.

Para contrarrestar las vulnerabilidades de mayor riesgo, encontradas en la red de *(VoIP),* se realizó un análisis de los diferentes protocolos de seguridad, como son *(SSL/TLS)* e *(IPSec),* con el fin de escoger el protocolo con las mejores características y que se adapten a la configuración de la red *(VoIP),* para encubrir las vulnerabilidades encontradas, finalmente se puso en funcionamiento el protocolo de seguridad *(SSL/TLS),* por ser el que mejor se adapta a la funcionalidad de la red y es soportado por el servidor de *(VoIP),* finalmente, se realizaron las pruebas de la configuración, resultando exitosa porque se cubrió todas las vulnerabilidades clasificadas con el riesgo más alto.

2.1. SUMMARY

The present work of career end, it is guided to carry out an analysis of the threats that affect to the nets taking advantage of any weakness of the net, *(VoIP),* for to do this carried out it a scanner, with the purpose of finding the teams that conform it, as well as the extensions that supports *(PBX),* using computer, denominated *(sniffers)* tools, which determine what weaknesses they exist at the moment in the net, to achieve this objective, one worked on a scenario of tests, where two connected machines to the *(PBX),* communicate to each other and a third intruding machine that has been able to enter to the net it captures the established communication among those attacked, being able this way to record the calls that settle down among the two victims, using the eavesdropping technique, which has as objective, to intercept data in a transmission in a not authorized way.

For the development of the present project, the following methodologies were used: ***(OSSTMM),*** to be one of those most used ones, for the search and verification of vulnerabilities, in nets that have an Internet connection, together with the distribution Kali Linux, to be an operating system that has a lot of tools, specialized for tests of security or what is known as ethical hacking, likewise, for the analysis and management of risks, the methodology ***(OCTAVE)*** was used, with the purpose of classifying the level of risks, according to the vulnerabilities found in the telephony net, *(IP),*of Isidro Agora's Hospital of Loja city.

To counteract the vulnerabilities of more risk, found in the net of *(VoIP),* it was carried out an analysis of the different protocols of security, like they are *(SSL / TLS)* and *(IPsec),* with the purpose of choosing the protocol with the best characteristics and that they adapt to the configuration of the net *(VoIP),* to hide the opposing vulnerabilities, Finally it put into operation the protocol of security *(SSL / TLS),* to be the one that better it adapts to the functionality of the net and it is supported by the servant of *(VoIP),* in conclusion, they were carried out the tests of the configuration, being successful because the covered all the vulnerabilities classified with the highest risk.

3. INTRODUCCIÓN.

Hoy en día, Internet es la herramienta más utilizada a nivel mundial y el aumento de aplicaciones a través de la *web*, como el envío de voz, video y datos han ayudado en el desarrollo de las telecomunicaciones, como la voz sobre el protocolo de Internet *(VoIP),* siendo un conjunto de normas, dispositivos y protocolos, que permiten transportar la voz en forma digital, de manera correcta y eficiente utilizando el protocolo *(IP). (VoIP),* es sinónimo de la telefonía *(IP). (VoIP),* es una tecnología, que entrega más funcionalidades que solamente telefonía, además de permitir las llamadas telefónicas, a través de todo Internet, *(VoIP),* permite controlar el ancho de banda utilizado para la voz, definir horarios para las llamadas, marcar paquetes provenientes de redes específicas y darles prioridad, poner en funcionamiento aplicaciones que mejoran los servicios de los teléfonos *(IP).* Con la tecnología se unifican servicios, por lo que se aprovechan los recursos y se disminuye costos, que se pueden generar gracias a los servicios de Internet, frente a la telefonía tradicional.

Sin embargo, a medida que aumenta la utilización de esta tecnología, se hacen más evidentes las vulnerabilidades de la *(VoIP),* debido a que se transmiten por Internet o por redes potencialmente inseguras, la *(VoIP),* hereda las vulnerabilidades que suelen darse en una red de datos, razón por la cual, es importante tener una buena seguridad en la red y adicionalmente establecer políticas de seguridad, única y exclusivamente para la transmisión de la voz, por el protocolo *(IP),* debido a esto resulta preocupante porque cualquier intruso o atacante, puede escuchar y espiar los paquetes de voz, que circulan a través en la red, cuando no se toman las medidas necesarias para protegerla.

Estas vulnerabilidades conllevan mucho más que el simple hecho de que las llamadas sean escuchadas ilegítimamente, esto implica que los sistemas telefónicos, puedan ser utilizados fraudulentamente para llamadas de larga distancia, a través de la red telefónica tradicional y generar altos costos a las víctimas. Además, para las casas de salud se deben tomar en consideración estas medidas, porque además de obtener los datos sanitarios, también existe información personal y detallada que puede ser utilizada por los ciberdelincuentes.

Un caso emblemático de explotación de vulnerabilidades de sistemas *(VoIP),* es el de Telecom Junkies. Telecom Junkies era una empresa proveedora de *(VoIP)* que vendía minutos que robaba a otras empresas. *Robert Moore*, un joven empleado de 23 años, fue sentenciado a 2 años de presión y una multa de 150.000 dólares por robar más de 10.000.000 minutos a 15 proveedores *(VoIP).* Esto significó un robo de más de 1.000.000 de dólares, por el cual el Sr. Moore recibió sólo 23.000 dólares de Edwin Pena, el propietario de Telecom Junkies, ya sentenciado el año del 2009.

Moore y Pena escanearon direcciones *(IP),* corporativas en busca de sistemas *(VoIP).* En particular, se trataba de sistemas *(VoIP)* que utilizaban routers *Cisco XM* y *gateways* Quintum Tenor que usaban contraseñas fáciles de adivinar y que permitían traspasar minutos a los usuarios de Telecom Junkies.

Para resolver o aminorar los problemas de seguridad de *(VoIP),* se pueden implementar diversos protocolos y medidas de seguridad a nivel de capa de enlace y red. Actualmente existen protocolos para mejorar la seguridad de la información que se transmite usando cualquier red de datos, como *(TLS)* e *(IPsec).* Estos permiten encriptar el tráfico de establecimiento de llamadas, para que no sea revelado a los atacantes. Sin embargo, *(IPsec),* en particular requiere un gran ancho de banda y gran procesamiento debido al incremento del tamaño del encabezado, que produce cerca de un 19,47% de sobrecarga, además del incremento en la carga útil de los paquetes.

Si bien los protocolos de seguridad autentican y encriptan los flujos de información, no son suficientes para asegurar la red *(VoIP).* Algunos protocolos de seguridad también exhiben vulnerabilidades y no necesariamente todos los proveedores los han implementado. Por otra parte, en redes *(VoIP),* también aparecen vulnerabilidades existentes en las redes de datos que se deben tener en cuenta *(Virus, Gusanos, Ataques en capa de red y enlace, DoS, etc.).*

Razón por la cual, surge la iniciativa de este proyecto, donde se analizará las vulnerabilidades, que se encuentran en la red de *(VoIP),* del Hospital Isidro Ayora de Loja, a través de herramientas informáticas y finalmente se implementa medidas de seguridad lógica, con el fin de cifrar la voz y evitar que entes malintencionados tengan accesos a la misma.

4. REVISIÓN LITERARIA.

En esta sección se detallan conceptos referentes a la arquitectura, protocolos y estándares de *(VoIP),* los componentes principales en la digitalización de la voz, como son los códec de voz, centrales telefónicas, así mismo, se hace hincapié de los conceptos relacionados con la seguridad física y lógica en las redes, además se describen las herramientas con las que se pueden identificar vulnerabilidades en las redes de *(VoIP),* los ataques que se pueden realizar a las mismas, y finalmente qué mecanismos de seguridad, se puede implementar para evitar o contrarrestar este tipo de incidentes.

4.1. VOZ IP.

(VoIP), es el acrónimo de *"Voice Over Internet Protocol"*, que hace referencia a la emisión de voz en paquetes *Internet Protocol (IP),* sobre redes de datos como Internet; en este punto se unen dos mundos que hasta entonces habían convivido separados, la transmisión de voz y la de datos. La tecnología *(VoIP),* trata de transportar la voz previamente procesada, y encapsulada en paquetes, para poder ser transportada sobre la red de datos, sin necesidad de disponer de una infraestructura telefónica convencional, con lo que se consigue desarrollar una única red homogénea, en la que se envía todo tipo de información ya sea voz, video o datos. [1] [2]

Es evidente que la utilización de una única red, para la transmisión de voz y datos presenta gran cantidad de ventajas, una llamada telefónica requiere una gran red de centralitas conectadas entre sí, ya sea por cableado, fibra óptica, satélites de telecomunicación o cualquier otro medio, que equivale a una enorme inversión para crear y mantener cualesquiera de esta infraestructura. En cambio, una llamada telefónica, sobre el paquete *(IP)*, comprime la voz y la envía por la red de datos, o por una línea en la que pueden viajar diferentes llamadas, e incluso diferentes datos, sin necesidad de líneas dedicadas ni desaprovechamiento del ancho de banda. [1] [2]

Por otro lado, existen también ciertos inconvenientes para el desarrollo de la telefonía sobre *(IP)*, que se resume en los siguientes tres conceptos: **seguridad, fiabilidad y calidad de servicio**. La *(VoIP),* al basarse sobre el protocolo *(IP),* y en muchos casos usando *User Datagram Protocol (UDP)*, en la capa de transporte, asume la posibilidad

de que los paquetes se pierdan, otro problema es que no hay una garantía absoluta, del tiempo en que tardan, en llegar los paquetes al otro extremo de la comunicación, aunque se utilicen técnicas de priorización de servicio. *(VoIP)*, es vulnerable en muchos otros puntos, ya sea en los protocolos utilizados, dispositivos que intervienen o debilidades en la red por la que se transmite. Pero es evidente que poco a poco dichos problemas se van solucionando, con la evolución de las tecnologías involucradas. [1] [2]

4.1.1. Historia de VoIP.

Sin duda, la invención que hoy se conoce como telefonía, debió ser un acto asombroso en su tiempo, se diría que fue mágico, al oír la voz de alguien remoto, saliendo de una misteriosa caja en tiempo real, en una época, en que esto era solo posible en la ciencia ficción, debió haber sido una experiencia única y casi fantástica, pero, con el pasar de los años, la telefonía ha tenido grandes avances, gracias a experimentos de *telegrafía* de hombres como Guglielmo Marconi (1874-1937), luego con la aparición de la informática y los avances tecnológicos, hicieron posible la comunicación por Internet y el envío de paquetes de voz a través de las redes de datos, que es lo que llamamos hoy en día, voz sobre *(IP)*. [2]

4.2. ARQUITECTURA DE LA RED VOIP.

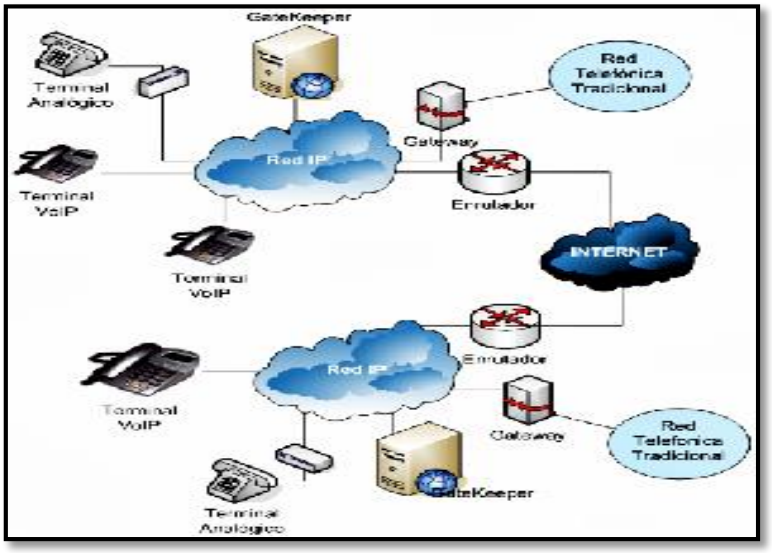


Ilustración 1: Topología de la infraestructura básica de red (VoIP).
Fuente: Sistema Telefónico (VOIP). Rogelio Rodríguez Martínez (2010)

En la imagen anterior, se puede ver una estructura básica de una red *(VoIP)*, donde dos organizaciones, realizan la transmisión de voz por medio del Internet.

Dentro de la estructura básica de una red *(VoIP),* hay que diferenciar tres elementos fundamentales:

- **Terminales:** Son los dispositivos que usan los usuarios para comunicarse, implementados tanto en *hardware* como en *software*, las funciones de los teléfonos tradicionales.
- **Gateway:** De forma transparente se encargan de conectar las redes *(VoIP),* con las redes de telefonía tradicional.
- **Gatekeepers:** Son el centro neurálgico de las redes *(VoIP),* por ser los encargados de realizar tareas de autenticación de usuarios, control de admisión, control de ancho de banda, encaminamiento, servicios de facturación y temporización, entre otros. [2]

4.2.1. Códec de voz.

Códec, es una abreviatura de *compresor-descompresor*, que convierte las señales análogas a señales digitales, y otro códec idéntico en el final de la comunicación, que convierte las señales digitales nuevamente en una señal análoga. La voz o el video para ser transmitidos por la red de datos tienen que codificarse, para ello se hace uso de un códec, que garantice la comprensión y codificación de audio y video, para su posterior descodificación y descompresión, antes de poder generar un sonido o una imagen utilizable. [2]

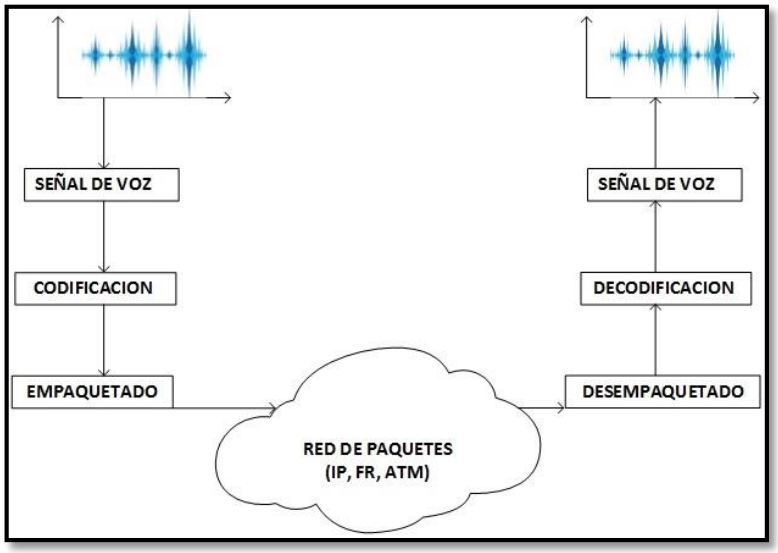


Ilustración 2: Transporte de la voz en redes de paquetes.
Fuente: El Autor (2015).

4.3. PROTOCOLOS VOIP.

Los protocolos son el lenguaje que utilizan los distintos dispositivos *(VoIP),* para su conexión, esta parte es importante, porque de ella dependerá la eficacia y la complejidad de la comunicación. Los protocolos hacen posible que la señal de voz viaje a través de Internet, en forma digital o en paquetes de datos, en lugar de enviarla de forma analógica, a través de circuitos utilizables sólo por telefonía convencional. [2]

4.3.1. Protocolos de Transporte VoIP.

En la aplicación de la tecnología de *(VoIP),* se dispone de estándares y protocolos, que son utilizados por las aplicaciones de tiempo real y multiusuario, además ofrecen facilidades de interconexión, entre las distintas tecnologías de transporte. En la siguiente figura, se muestra las diferencias entre los protocolos de señalización *(H.323 y SIP),* y los protocolos de transporte *(RTCP, RTP, RTSP).* [2]

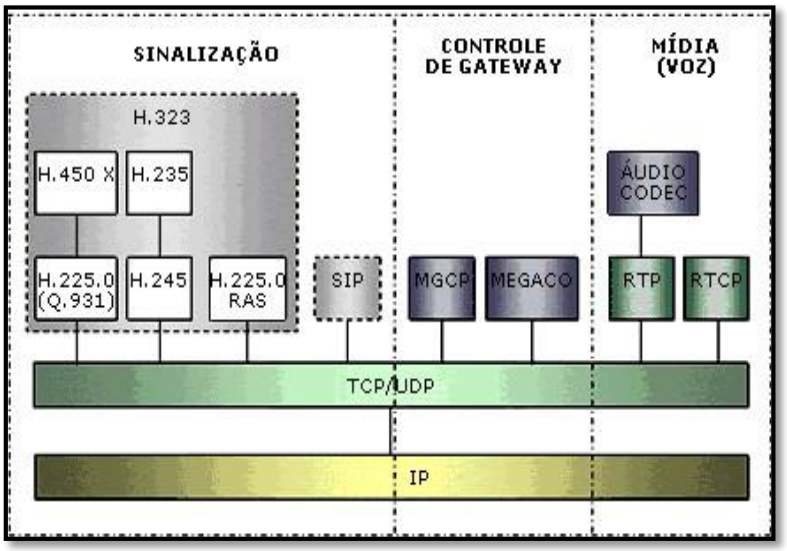


Ilustración 3: Protocolos de Transporte y Señalización de (VoIP).
Fuente: (TELECO) Inteligencia en Telecomunicaciones, Jessica Vanessa Gaibor Ortega (2010)

- **Protocolo de Transporte en Tiempo Real (RTP).**

Real-Time Transport Protocol (RTP), es el estándar para el transporte de tráfico (audio o video), en tiempo real sobre Internet. Cada paquete *(RTP),* contiene una muestra pequeña de la conversación, el tamaño del paquete y el tamaño de la muestra de voz dentro de dicho paquete, depende del códec utilizado.

- **Protocolo de Control de Transporte en Tiempo Real (RTCP).**

Real-Time Transport Control Protocol (RTCP), regula el intercambio de mensajes de control, entre los participantes de una sesión multimedia, es decir regula la calidad de servicio, con que se está desarrollando la comunicación: retardo *(jitter),* tasa de paquetes recibidos y perdidos, entre otros. [2]

- **Protocolo de Transmisión en Tiempo Real (RTSP).**

Real-Time Streaming Protocol (RTSP), está inmerso en la capa de aplicación, además, es un protocolo no orientado a la conexión, en la mayoría de los casos *(RTSP),* usa *Transmisión Control Protocol (TCP),* para el envío de datos del reproductor (*mensajes "out of band"),* y *(UDP),* para los datos de audio y vídeo *(mensajes "in band"),* el concepto de *"in band" y "out of band"*, se refiere, a que el protocolo es capaz de enviar distintos tipos de información, por distintos puertos. [2]

- **Protocolo de Reservación de Recursos (RSVP).**

Resource Reservation Protocol (RSVP), permite que las aplicaciones de Internet o una red local, obtengan diferente *Quality of Service (QoS),* para su flujo de datos.

4.3.2. Protocolos de señalización.

Se denomina señalización, a la información relacionada con una llamada, que se transmite entre dos equipos.

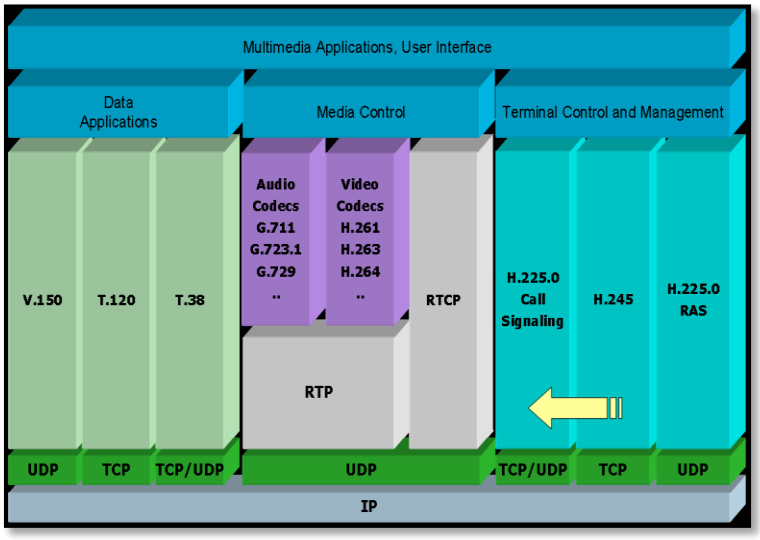


Ilustración 4: Protocolos de señalización de (VoIP).
Fuente: Servicio de tecnología de voz IP VoIP. Vicente Sánchez Patón (2010).

A través de la señalización, la central puede ubicar a la otra central, con la que debe establecer una comunicación, algunas de las funciones principales que realizan los protocolos de señalización son las siguientes:

- Localización de usuarios.
- Establecimiento de sesión.
- Negociación de sesión.
- Gestión de los participantes en la llamada.

- **H. 323.**

La *International Union Telecommunications (ITU),* ha combinado varios estándares de bajo nivel en estándares de protección, incluido *(H.323),* para multimedia sobre *Local Area Network (LAN),* con calidad de servicio no garantizada cuya arquitectura se muestra en la figura anterior. [2] [3]

- **Protocolo de Control de Media Gateway (MGCP).**

Media Gateway Controller Protocol (MGCP), tiene su origen en *Skinny Gateway Control-Protocol (SGCP),* de Cisco y Bellcore, es un protocolo de control de dispositivos. (*MGCP),* soporta un control de señalización de llamada escalable, integrando el control de *(QoS),* en el *gateway*, su compatibilidad con normas de *Internet Engineering Task Force (IETF),* y con *(H.323)* lo hace ideal para aplicaciones de multimedia sobre redes (*IP).* [2] [3]

- **Protocolo IAX (Intercambio entre Asterisk).**

Inter Asterisk eXchange (IAX), es uno de los protocolos utilizado por *Asterisk*, para manejar conexiones *(VoIP),* entre servidores *Asterisk*, ofrece ventajas frente a *Session Initiation Protocol (SIP),* las cuales resultan perfectas en la troncalizacion *(Trunking),* entre dos servidores *Elastix*. Hoy en día existe *(IAX2),* la segunda versión del protocolo *(IAX),* mismo que tiene ventajas frente al anterior, como transportar virtualmente cualquier tipo de dato, es un protocolo casi transparente a los cortafuegos, es eficaz para trabajar dentro de redes internas, es extremadamente flexible y puede ser utilizado con cualquier tipo de dato, incluido video y provee soporte para ser transparente a *(NAT).* [2] [3]

- **Protocolo de Inicio de Sesión (SIP).**

Es un protocolo simple de señalización y control, generalmente usado para telefonía y videoconferencias sobre las redes *(IP),* su estructura está basada en otros protocolos, como *Simple Mail Transfer Protocol (*SMTP*),* y *Hypertext Transfer Protocol* (HTTP), con los que guarda cierta similitud. *(SIP),* soporta cinco elementos funcionales.

- Localización de usuarios.
- Intercambio / negociación de capacidades de los terminales.
- Disponibilidad de usuarios.
- Establecimiento de llamada.
- Gestión de llamada.

Utiliza el puerto *(UDP 5060),* para el establecimiento, negociación y fin de la comunicación, la arquitectura *(SIP),* define cuatro tipos de servidores:

- **Servidor proxy.**

Encamina peticiones/respuestas hacia el destino final, esto lo realiza a través de saltos de un servidor a otro, hasta alcanzar el destino final, esto evita bucles y forzar que las respuestas sigan el mismo camino que las peticiones. [2] [3]

- **Servidor de redirección.**

Realiza una función equivalente a una llamada, con la diferencia que contesta a un (*INVITE),* con un mensaje de redirección, indicando en el mismo, como contactar con el destino. [2] [3]

- **Servidor de registro.**

Utilizado para que los terminales, registren la ubicación en la que se encuentra el usuario, este facilita la movilidad de usuarios, al actualizarse dinámicamente.

4.4. ESTÁNDARES VOIP.

Los principales grupos de estandarización, se encargan de facilitar la comunicación y la interoperabilidad, entre dispositivos de diferentes fabricantes, los más comunes son:

- **IEEE 802.1P.**

El estándar *Institute of Electrical and Electronics Engineers (IEEE 802.1p),* define el método de etiquetar los paquetes y por medio de este, los conmutadores de nivel 2 pueden darles prioridad *(Impide que se creen bucles),* el estándar *(802.1p),* prioriza el tráfico de red, en la subcapa de vínculo de datos/*MAC.* [3]

- **IEEE 802.1Q**

El estándar *(IEEE 802.1p),* define el funcionamiento de los puentes, es decir, este permite definir y administrar las *Virtual Local Area Network (VLAN),* dentro de las infraestructuras de *Local Area Network (LAN)* con un switch. [3]

4.5. CENTRAL TELEFÓNICA DIGITAL (PBX).

La *Prívate Branch Exchange (PBX),* es la red privada de telefonía que se utiliza dentro de una empresa, es decir, se refiere al dispositivo que actúa como una ramificación de la red primaria pública de teléfonos, por lo que los usuarios de una *(PBX),* no están asociados con la central de telefonía pública, es la misma *(PBX),* que actúa como tal. Una *(IP-PBX),* al ser totalmente digital, no sólo puede trabajar con voz, sino también con video, se pueden realizar videoconferencias sin ningún tipo de problema, siempre y cuando se disponga de una cámara. Además, al trabajar por *(IP),* es aún más económica que una *(PBX),* convencional, dado que a través de Internet, no hay distancias y necesita solamente la conexión a la red y por supuesto, las llamadas internas son gratuitas. La *Network Exchanged Telefonica (*RTC*),* es quien en ruta las llamadas a otro destino, mediante líneas troncales, la *(PBX),* se encarga de redirigir y gestionar las llamadas entrantes, a uno o varios teléfonos de una empresa o red. [3]

Ventajas:

- Te ayuda a configurar *Asterisk* más rápidamente.
- Todas las distribuciones open source disponibles hacen uso de esta interfaz.

Desventajas:

- No todos los módulos están soportados.

Resumiendo una *(PBX)*, es una computadora centralizada, en la que el usuario configura los parámetros de las llamadas entrantes y salientes, según las necesidades de la red, a continuación se detallan algunas de las *(PBX)*, más conocidas:

4.5.1. Asterisk.

Asterisk, es una *(PBX)*, completa para múltiples plataformas, bajo los sistemas operativos *(Linux, BSD, MacOSX)*, y otros donde las llamadas en el sistema, disparan funciones a través de patrones de dígitos *(mejor conocidos como extensiones)*, ofreciendo un completo control sobre el enrutamiento de las mismas con relativa facilidad. Incluye funcionalidades encontradas en los sistemas de comunicación más recientes tales como correo de voz, colas de llamadas, conferencias, audio respuesta, música en espera y otras funcionalidades más avanzadas que permiten la interconexión con sistemas de telefonía externos a través de troncales análogas, digitales o las más avanzadas opciones del estado del-arte con interfaces para *(VoIP)*, tales como *(SIP), (H.323), (IAX)* y otros más no sólo para comunicaciones de voz sino incluso para video. Esta poderosa combinación de funcionalidades permite construir aplicaciones tan complejas o avanzadas como se desee, sin incurrir en altos costos es más flexibilidad que en cualquier sistema de telefonía existente. [3]

Ventajas:

- Al compilar, tu conmutador se ajustará a la arquitectura de tu *(PC)*.
- Puedes elegir que módulos quieres compilar y cuáles no.

Desventajas:

- Tienes que hacer todo a mano.
- Toma un mayor tiempo de implementación.

4.5.2. Elastix.

Elastix es una distribución creada por *Palosanto Solutions*, cuya base de operaciones está en Guayaquil, Ecuador. *Elastix* surgió en el 2006 como una interfaz de tarificación de llamadas para *Asterisk (una herramienta para interpretar los registros de llamadas que Asterisk genera)*, pero rápidamente se convirtió en una suite de comunicaciones que

integra varios productos en uno, porque en un solo (*CD),* es posible instalar *(en un solo paso)* no solamente *Asterisk,* sino una interfaz web de configuración como *(FreePBX),* un sistema de base de datos *(MySQL),* un sistema de mensajería instantánea *(OpenFire),* soporte para fax *(Hylafax),* entre otras aplicaciones más que incluye, al igual que *Asterisk, Elastix* es un proyecto open source, por lo que es libre y gratuito. Según el roadmap de *Elastix* con su próxima versión 3.0, se abandonará el uso de (*FreePBX),* para usar su propia interfaz de configuración. En las versiones 2.x e inferiores, la interfaz gráfica está "amarrada" con el uso de *(FreePBX 2.9),* o inferiores, *Elastix* usa un *wrapper (para personalizarlo con su interfaz)* y no soporta versiones posteriores para la *Users Graphical Interface (GUI).* [3]

Ventajas:

- Sistema todo en uno.
- Soporte incluido para señalizaciones de América Latina.
- Amplia comunidad de apoyo.

Desventajas:

- Instala muchos componentes por default, los quieras usar o no.
- Su interfaz gráfica es muy lenta y pesada *(comparada con FreePBX puro).*
- Algunos componentes no han sido actualizados en mucho tiempo por romper la arquitectura propia de Elastix *(FreePBX 2.8, Vtiger 5.2.1).*
- Al tener muchos componentes "extras", también ha sido víctima de errores de seguridad de los mismos.

4.5.3. Trixbox.

En sus inicios fue conocida como *Asterisk@Home,* y fue la primera distribución todo en uno que hacía uso de: *(FreePBX + MySQL + PHP + CentOS + Asterisk),* para levantar un conmutador *(IP),* de manera rápida. En el 2006 cambia su nombre a *(Trixbox)* y se separa en las versiones *Community Edition (CE)* y Pro, que es el servicio de paga proporcionado por Fonality (la empresa que compró su desarrollo). *(Trixbox),* es más usada en el mercado norteamericano al estar creada originalmente en inglés y tener su base de operaciones en *(EUA).* Sin embargo, al utilizar la misma interfaz de *(FreePBX),*

las funcionalidades que ofrece esta plataforma son casi las mismas que el resto de las distribuciones que se basan en ella. *(Trixbox),* hace uso de un (*fork),* muy viejo de *(FreePBX),* por lo que muchas de sus funcionalidades están atrasadas, comparadas con el resto de las distribuciones. [2] [3]

Ventajas:

- Mucho tiempo en el mercado.
- La versión *Pro*, permite administrar tú *(PBX),* desde la nube.

Desventajas:

- Sus componentes son muy viejos.
- Sin soporte para el mercado de América Latina.
- Poco desarrollo a la plataforma.

4.5.4. Asterisknow.

Es la distribución oficial de *(Digium),* y al igual que las anteriores permite instalar *(CentOS + Asterisk)* en un solo paso, la diferencia primordial con las 2 anteriores es que esta es la distribución más ligera de todas, por lo que no se instalan extras (*como Hud en Trixbox u OpenFire, Vtiger e Hylafax en Elastix*). El *(FreePBX),* viene puro, por lo que puede utilizar la versión más reciente y no estar amarrado a limitantes del desarrollador de la distribución. También es la distribución que más rápidamente ofrece las nuevas actualizaciones para *Asterisk*. Un inconveniente quizá es que al ser mantenida por *Digium*, no se ofrece el soporte precargado para las tarjetas de *Public Switched Telephone Network (PSTN)* de sus competidores *(como Sangoma),* por lo que si necesita estos drivers tendrá que instalarlos por aparte. [2] [3]

Ventajas:

- Ligero.
- Apoyado por *Digium*.

Desventajas:

- Todos los extras deben ser instalados a mano.

4.5.5. Avaya IP office.

Es una central telefónica híbrida modular, diseñada para combinar telefonía analógica, digital e *(IP)*. Las funciones de telefonía de *(Avaya IP Office)*, son muy completas y configurables, permitiendo crear prácticamente ilimitados grupos, rutas de entrada de llamadas y funciones de *Automatic Call Distributor* (*ACD)* con sencillez. [2] [3]

4.6. SOFTPHONES.

Es un software que emula un teléfono en un computador y permite hacer llamadas de *(VoIP)*, es decir convierte un *(PC)*, en un teléfono *(IP)*, para hacer llamadas a otros softphone de modo gratis en general, o a otros teléfonos convencionales usando un operador de telefonía *(IP)*, poseen una interfaz intuitiva, tienen un teclado virtual parecido a los teléfonos convencionales. [2] [3]

4.7. CONCEPTOS Y AMENAZAS DE SEGURIDAD EN REDES VOIP.

En este apartado se describen los principales conceptos de seguridad y las diferentes amenazas que pueden aparecer en un sistema *(VoIP).* A continuación se describe los conceptos de seguridad como son: la **confidencialidad**, **integridad** y **disponibilidad**, conceptos que la seguridad pretende resguardar, también conocidos como tríada ***CIA*** *(por las iniciales de las palabras en idioma Inglés:* ***confidenciality***, ***integrity***, ***availability****).*

4.7.1. Confidencialidad.

La norma *International Organization of Normalization* (ISO *27001*), define la confidencialidad como*: "El acceso a la información, por parte únicamente de quienes estén autorizados*" por lo tanto, la información transmitida entre, el emisor y uno o más destinatarios, ha de ser preservada frente a terceros, para evitar vulnerabilidades de confidencialidad, se utilizan contraseñas de seguridad y técnicas de encriptación. [4]

4.7.2. Integridad.

La norma (*ISO 27001)*, interpreta el principio de integridad como: *"El mantenimiento de la exactitud y completitud de la información y sus métodos de proceso"*, la integridad vela para que no se realicen modificaciones de la información. En el caso de existir alguna modificación no autorizada, debe alertarse, para evitar vulneraciones de la integridad de un mensaje, para ello se adjunta un conjunto de datos, que permiten comprobar que el

mensaje, no ha sido modificado por terceros, un ejemplo de este conjunto de datos son los bits de paridad. [4]

4.7.3. Disponibilidad.

La norma (*ISO 27001)*, interpreta el principio de disponibilidad como*: "Acceso a la información y los sistemas de tratamiento de la misma, por parte de los usuarios autorizados cuando lo requieran"*, es decir, los recursos deben estar disponibles, cada vez que un usuario los requiera. Para disminuir las vulneraciones de la disponibilidad de un sistema, se utiliza redundancia *(por ejemplo, de hardware, de software y de suministro eléctrico)*, de tal modo que se pueda disminuir la probabilidad de que el sistema no pueda operar, debido a fallas del sistema. Garantizar la disponibilidad, implica también la prevención de ataques que tienen por objetivo, inhabilitar el sistema. [4]

4.7.4. Resumen.

Tabla 1: Resumen de los conceptos de seguridad.

CONCEPTO	DEFINICIÓN	MECANISMO DE RESGUARDO
Confidencialidad	Acceso a la información por parte únicamente de quienes estén autorizados.	Contraseñas y Encriptación
Integridad	El mantenimiento de la exactitud y completitud de la información y sus procesos.	Paridad
Disponibilidad	Acceso a la información y los sistemas de tratamiento de la misma, por parte de los usuarios autorizados cuando lo requieran.	Redundancia

Fuente: Seguridad en voz sobre (IP), María José Liberona (2010)

4.8. AMENAZAS DE SEGURIDAD DE UN SISTEMA VOIP.

La norma (*ISO 27001)*, define amenaza como: *"Una causa potencial de un incidente indeseado, que puede dar lugar a daños a un sistema o a una organización"*. Las amenazas de seguridad, son incidentes que pueden provocar que menos un concepto de seguridad sea vulnerado, las amenazas de seguridad de un sistema *(VoIP)*, descritas a continuación incluyen la denegación de servicio *Distributed Denial of Service (DoS), accesos no autorizados, fraudes telefónicos, interceptación y Vishing.* [4]

4.8.1. Denegación de Servicio (DoS).

Las amenazas *(DoS)*, son intentos maliciosos para degradar o inhabilitar el funcionamiento del sistema, afectando la disponibilidad del mismo. El objetivo de una amenaza de denegación de servicio en *(VoIP)*, es colapsar los dispositivos de red, a través

de llamadas falsas que generan tráfico excesivo, de esta manera, las llamadas legítimas no pueden realizarse o se interrumpen. En el caso de *(VoIP)*, algunos ataques pueden resultar en un *(DoS)*, para muchos equipos de telefonía *(IP)*, por ejemplo, los terminales pueden dejar de operar cuando intentan procesar una alta tasa de paquetes; los servidores también pueden experimentar fallas y discrepancias de registro, con un ataque de señalización especificó de menos de *1Mb/segundo*. *(VoIP)*, está expuesto a 3 tipos de amenazas de *(DoS)*, que se describen a continuación. [4]

4.8.2. Denegación de Servicio Distribuido (DDoS).

Las amenazas *Distributed Denial-of-Service (DDoS)*, son ataques de *(DoS)*, desde múltiples sistemas, todos coordinados para invalidar un sistema de red *(VoIP)*. Para realizar el ataque se insertan programas dentro de los computadores de las víctimas, sin ser detectados, logrando así crear miles de robots listos para realizar sus ataques de *(DDoS)*, en *(VoIP)*, estos ataques distribuidos tienen como objetivo causar *(DoS)*, en varios puntos de la red, de manera simultánea, colapsando el sistema por completo. [4]

4.8.3. Fuzzing.

También conocido como testeo funcional, es un ataque que hace uso de paquetes malformados, causando el desbordamiento de *buffer*, cuelgues o reinicios en los dispositivos que provocan un mal funcionamiento del sistema, en *(VoIP)*, en particular el protocolo (*SIP)*, envía mensajes en texto plano, por lo tanto, es muy fácil realizar el cambio de los campos del mensaje. En cambio protocolos, como *(H.323)* e *(IAX2)*, los mensajes son binarios, así hace más difícil la realización de este tipo de ataques. [4]

4.8.4. Inundaciones (Flooders).

Un *flood*, consiste en mandar mucha información en poco tiempo a un dispositivo para intentar que se sature, en *(VoIP)*, los inundadores *(flooders)*, tienen como objetivo los servicios y puertos de telefonía *(IP)*, una inundación puede causar mayor daño, en una red *(VoIP)*, que en una red de datos. La utilización de calidad de servicio *(QoS)*, provee que los mensajes de telefonía sean transmitidos con prioridad a través de la red, por ello, cuando se realiza una inundación en la red, el ancho de banda es afectado dificultando la transmisión de voz y datos por la red. [4]

4.8.5. Accesos no autorizados.

Los accesos no autorizados, son ataques que se enfocan en los sistemas de control de llamadas, administración, facturación, y otras funciones de telefonía que requieren autentificación. A través de sistemas de administración remota como *Secure Shell (SSH),* y contraseñas débiles los atacantes provocan accesos no autorizados en los equipos. [4]

4.8.6. Fraude telefónico (Toll Fraud).

Los fraudes telefónicos son frecuentes en los sistemas telefónicos tradicionales, se trata de ataques que pretenden recaudar dinero a costa del servicio telefónico, realizando llamadas de larga distancia o robos de minutos de llamadas. [4]

4.8.7. Interceptación (Eavesdropping).

Eavesdropping, es el término con el que se conoce al ataque de interceptación, en términos de telefonía *(VoIP),* se trata de la interceptación de las conversaciones telefónicas, por parte de individuos que no participan en la conversación y la interceptación de los mensajes utilizados en el sistema. En telefonía *(IP),* la interceptación presenta pequeñas diferencias, con la interceptación de paquetes en redes tradicionales. En *(VoIP),* se diferencian básicamente dos partes dentro de la comunicación: la señalización y los paquetes de voz, la señalización, a más que revela información de las víctimas que realizan y reciben la llamada, revelan la configuración de la red y la localización de los dispositivos. La interceptación de paquetes de voz revela el contenido de las conversaciones telefónicas. [4]

4.8.8. Spam Over Internet Telephony (SPIT).

El *(SPIT),* es el *(SPAM),* de la telefonía *(IP).* El atacante puede usar paquetes de datos o de voz, ya sea enviando *Short Message Service (SMS),* promocionando productos en los diferentes terminales, o enviando grabaciones promocionales a los buzones de voz.

4.8.9. Vishing.

Vishing, es el término usado para referirse al *phishing* de *(VoIP),* mediante la combinación de ingeniería social y tecnologías de *(VoIP),* permite al criminal engañar a personas para obtener datos delicados como pueden ser datos de tarjetas de crédito o

cuentas bancarias El atacante además, mediante técnicas de *"Caller-Id spoofing",* puede suplantar la identidad *(número de teléfono)* de una entidad bancaria o una compañía legitima, para no levantar sospechas por parte de la persona atacada. [4]

4.8.10. Resumen.

Para el buen funcionamiento de las redes *(VoIP)*, es necesario reforzar la seguridad de la digitalización de la voz, de manera independiente de la establecida en la red. Estos inconvenientes no significan, que la tecnología *(VoIP)*, tenga mayores problemas que beneficios, gracias a ella se reducen los costos administrativos y el consumo de recursos, provee de gran movilidad y privilegios para todos los usuarios. [4]

Tabla 2: Amenazas de seguridad en (VoIP).

ATAQUE	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Denegación de Servicio			x
Accesos no Autorizados	x	x	
Fraudes Telefónicos		x	
Interceptación	x		
SPIT		x	
Vishing	x	x	

Fuente: Seguridad en voz sobre (IP) María José Liberona (2010)

4.9. VULNERABILIDADES DE LA VOIP EN LA CAPA DE APLICACIÓN.

A continuación, se estudian las vulnerabilidades, en los diferentes dispositivos *(VoIP)*, que se utilizan la capa de aplicación para su comunicación, porque no todos los dispositivos se relacionan con esta capa. La mayor parte de los ataques y vulnerabilidades del *software* en los dispositivos *(VoIP)*, son los mismos que se generan en los dispositivos de una red de datos. Esto se debe a que ambas redes comparten muchas aplicaciones como: *(HTTP, e-mail, base de datos, entre otros)*, que funcionan sobre el mismo protocolo *(IP)*. Los ataques y vulnerabilidades de las redes de datos en la capa de aplicación, han sido estudiados y se puede encontrar información detallada en Internet, de los cuales los más comunes son los siguientes:

- Contraseñas débiles
- Falta de actualizaciones de *firmware*
- Accesos remotos
- Servicios innecesarios
- Malas configuraciones

Las vulnerabilidades de la capa de aplicación, en las redes de datos, que fueron listadas previamente, también forman parte del conjunto de vulnerabilidades de las redes *(VoIP)*, pero no serán descritas en este apartado, pues en esta sección serán expuestas las vulnerabilidades explotadas comúnmente en la capa de aplicación de la red *(VoIP)*. [4]

4.9.1. Terminales.

En general, los teléfonos *(IP)* y *softphone*, son herramientas utilizadas por los atacantes para tener acceso a las redes *(VoIP)*, los terminales son los dispositivos menos críticos, es decir es un dispositivo, que si se ve vulnerado no produce que la red *(VoIP)*, deje de funcionar. Por otro lado, son los dispositivos más comunes y menos controlables, a través de ellos los atacantes pueden conocer la configuración de la red *(VoIP)*, debido que cuenta con información en sus configuraciones dirección *(IP)*, de la central y datos de usuario. Los *softphones*, se localizan en un computador, lo que significa que cuentan con las mismas vulnerabilidades y se encuentran en la misma red de datos, por lo tanto, obligan a dar acceso a los terminales, a la red de datos y a la red de voz. Los *softphones* no permiten separar la red de voz con la de datos.

Esto permite que cualquier ataque realizado en la red de datos afecte directamente a la red de voz, es por esta razón que *National Institute of Science and Technology (NIST)*, recomienda que los *softphones* no se utilicen en la red *(VoIP)*, a continuación, se describirán problemas de seguridad ocasionados cuando los dispositivos *(VoIP)*, utilizan los protocolos de la capa de aplicación. [4]

4.9.2. Inserción de servidor (TFTP).

Trivial File Transfer Protocol (TFTP), es un protocolo utilizado por los terminales, para descargar archivos que permiten configurar y actualizar *software*. Un servidor *(TFTP)*, debe tener acceso a la mayor parte de la red, para distribuir los archivos de configuración, por lo tanto, se debe mantener bajo estricta seguridad. [4]

4.9.3. TELecommunication NETwork (TELNET).

Es un protocolo de red que sirve para acceder desde la red a una máquina, para manejarla remotamente. Algunos de los teléfonos *(IP)*, soportan el servicio *telnet* y poder ser configurados remotamente. El atacante debe configurar manualmente la dirección *(IP)*,

en los teléfonos de las víctimas, para poder acceder a través de la dirección *(IP),* con el servicio *telnet*. Una vez dentro de la configuración del terminal, los atacantes pueden obtener parámetros como: modelo del teléfono, servidor *Dynamic Host Configuration Protocol (DHCP),* dirección *(IP)* y máscara de red y router de salida *default gateway.* Estos parámetros son utilizados para conocer la configuración de la red *(VoIP),* este ataque es pasivo, por permitir al atacante obtener información que le será de utilidad para realizar un ataque activo. [4]

4.9.4. Hyper Text Transfer Protocol (HTTP).

Es el protocolo usado en cada transacción de la *World Wide Web (www).* En *(VoIP),* el protocolo *(HTTP),* se utiliza para la configuración remota de la mayoría de los dispositivos *(VoIP),* incluso los terminales cuentan con su servidor *(HTTP),* para la configuración, con las limitaciones que el dispositivo conlleva. [4]

El protocolo *(HTTP),* ha sido ampliamente vulnerado, estas vulnerabilidades pueden ser transmitidas a los dispositivos *(VoIP),* mediante su interfaz *web*, de configuración remota, los atacantes pueden lograr ataques de denegación de servicio, accesos no autorizados o fraudes telefónicos. [4]

4.9.5. Gateways VoIP.

Un *gateway*, se considera un dispositivo crítico dentro de una red *(VoIP),* el *gateway* provee una salida hacia la red telefónica tradicional, lo que permite a los atacantes que logren tener acceso al dispositivo, pueden salir directamente a la red de telefonía tradicional e instalar llamadas. Las vulnerabilidades de un *gateway*, dependen de los servicios que provee y de su configuración. Entre los servicios o especificaciones que se pueden encontrar en un *gateway* están: soporte para *Simple Network Management Protocol (SNMP),* administración *(Web)* o *(HTTP), (DHCP)* y *(TFTP).* Todos estos protocolos usualmente encontrados en las redes de datos, tienen sus problemas de seguridad ya comentados anteriormente, una vulnerabilidad de configuración depende del plan de discado que se utilice. Por ejemplo, comúnmente se antepone un número predefinido para poder llamar a celulares. Se utiliza en algunos *gateways*, pero se encuentra en casi todas las *(IP-PBX).* [4]

4.9.6. Central telefónica o (PBX IP).

Una *(IP-PBX)*, o central telefónica *(IP)*, es el dispositivo más crítico dentro de los sistemas *(VoIP)*, porque a través de este dispositivo los atacantes pueden tomar el control de la red *(VoIP)*. Las *(IP-PBX)* además cuentan con otros servicios en la capa de aplicación, los cuales traen problemas de seguridad a la red *(VoIP)*, las bases de datos, y los servicios de correo, tienen vulnerabilidades ya conocidas que se las mencionadas al comienzo de este punto. Estas afectan comúnmente al sistema operativo, en el cual reside la *(IP-PBX)*, además comparte la vulnerabilidad de las configuraciones del plan de discado con los *gateways* y tienen servicios que proveen facilidades de configuración, como lo son las interfaces *web* que proveen accesos extras a los atacantes. [4]

4.9.7. Resumen.

La capa de aplicación depende de los servicios que se deseen implementar en la red *(VoIP)*, con estos servicios aumentan las vulnerabilidades del sistema, se debe tomar medidas para evitar las vulnerabilidades, propias de cada aplicación.

Tabla 3: Vulnerabilidades en la capa de Aplicación.

PROTOCOLO	ATAQUE	C	I	D
TFTP	Inserción de servidor *(TFTP)*		✓	
Telnet	Acceso telnet	✓		
HTTP	*(HTTP, DoS)*			✓
	Interceptación de configuración *(HTTP)*	✓		
	Acceso no autorizado *(HTTP)*	✓	✓	✓

Fuente: Seguridad en voz sobre (IP) María José Liberona (2010).

4.10. PROTOCOLOS VOIP Y SUS VULNERABILIDADES (CAPA DE SESIÓN Y TRANSPORTE).

En este punto, se ahondará en los protocolos más utilizados en las redes *(VoIP)*, como son: *(H.323)*, *(SIP)* y *(MGCP)* que se ubican en la capa de sesión del modelo *(OSI)*, *y (RTP)* que se ubica en la capa de transporte, con el fin de comprender las vulnerabilidades y ataques de cada uno de ellos. Estos ya fueron descritos en el apartado de protocolos para *(VoIP)*. Las secciones son: señalización, transporte, codificación, y control de medios, adicionalmente, debido a que los proveedores de dispositivos *(IP)*, añaden e implementan protocolos propios, para facilitar la interacción entre sus dispositivos, se

agrega a las secciones anteriores el estudio de protocolos propietarios. En particular, se describirán los protocolos *(IAX2)* y *Skinny Call Control Protocol (SCCP),* utilizados por el proveedor *Cisco* y la central telefónica *Asterisk*. [4]

4.10.1. Señalización.

Los protocolos de señalización que se estudian en esta sección son *(H.323)* y *(SIP).*

- **H.323.**

  De los protocolos que pertenecen a *(H.323),* se originan variados ataques:

- **Ataque H.225.**

  Este ataque es una amenaza de *(DoS),* particularmente *fuzzing*, para generar el ataque, se utiliza una vulnerabilidad en los mensajes de instalación de *(H.225).* El ataque funciona haciendo que los mensajes de instalación *(H.225),* de gran tamaño sean procesados completamente por la víctima, los mensajes de instalación *(H.225),* son de diferente tipo y tamaño, permitiendo que los atacantes asignen un tamaño determinado a los mensajes. Los paquetes *(H.225),* cuentan con un límite de tamaño, pero al procesar los paquetes con un tamaño excesivo, cercano al límite, los sistemas experimentan *(DoS),* o un 100% del uso de la *(CPU).* [4]

- **Ataque H.245.**

  Al igual que el ataque *(H.225),* es una amenaza de *(DoS),* pero explota una vulnerabilidad del mensaje que describe el *Terminal Capability Set (TCS)*. Este ataque funciona a través de la captura del mensaje *(TCS),* o alteración, su captura produce que múltiples sistemas fallen y dejen de funcionar, cuando se altera el mensaje *(TCS),* que es enviado a un terminal, por ejemplo, cuando se cambia la dirección *(IP),* del destino por la de la víctima, deja en un bucle al mensaje *(TCS),* esto hace que la víctima se envíe así mismo el mensaje *(TCS).* [4]

4.10.2. Protocolo de Inicio de Sesión (SIP).

A continuación, se describen los ataques *(SIP),* basadas en las referencias

- **Ataque a hashes digest.**

El ataque a *hashes digest*, es una amenaza de acceso no autorizado, se trata de un mecanismo basado en *hashes* que evita el envío de la contraseña de los usuarios en texto plano. Los *hashes digest* se encargan de proteger solamente la contraseña del usuario y no el mensaje enviado, una vez capturado el paquete *(SIP),* se obtiene el *hash* de la contraseña, del usuario y se puede vulnerar de dos modos: por fuerza bruta o utilizando un diccionario. Un ataque de fuerza bruta, permite recuperar una clave, probando todas las combinaciones posibles, hasta encontrar aquella que permite el acceso; en cambio, el método de diccionario consiste en intentar averiguar una contraseña, probando todas las palabras del diccionario creado por el atacante. [4]

- **Suplantación de identidad (Registration Hijacking).**

La suplantación de identidad, es una amenaza del tipo fraude telefónico, utiliza una vulnerabilidad en el mensaje (*REGISTER),* este ataque utiliza el registro de usuario, que es la primera comunicación que se establece en el entorno (*VoIP).* La comunicación se realiza entre el usuario y el servidor, debe ser realizado de forma segura, caso contrario, no se puede asegurar que el usuario registrado sea el auténtico.

- **Desconexión de usuarios.**

Este ataque es una amenaza de *(DoS),* esta vulnerabilidad, hace uso de la posibilidad de alterar los mensajes (*BYE)* y (*CANCEL),* por lo tanto, es una amenaza de *fuzzing*. La desconexión de usuarios, funciona debido a que muchos de los protocolos de (*VoIP),* se utilizan sin encriptación alguna; por lo tanto, es sencillo interceptar mensajes y obtener la información de la identidad del usuario, y los datos de la llamada. De esta manera, para un intruso resulta fácil desconectar las llamadas utilizando el mensaje *(BYE),* y simulando ser él usuario, al otro lado de la línea. Por otro lado, el mensaje *(CANCEL),* alterado se debe enviar al momento de establecerse la llamada, es decir, antes que el usuario recepte la llamada, a diferencia del mensaje *(BYE)* que se envía cuando la llamada está establecida. [4]

4.10.3. Protocolo de Descripción de Sesión (SDP).

Session Description Protocol (SDP), utiliza la codificación de texto, un mensaje *(SDP),* se compone de una serie de líneas, denominadas campos, donde los nombres son

abreviados por una sola letra. La interceptación de los mensajes *(SDP),* permite, que el atacante conozca muchas características de los terminales, como *códec* y puertos utilizados, número de teléfono, el protocolo utilizado para transportar la voz e información de conexión. [4]

4.10.4. Transporte y codificación.

En esta sección se estudia las vulnerabilidades del protocolo *(RTP),* encargado de transportar los datos de audio y video.

- **Protocolo de Transporte de Tiempo Real (RTP).**

  A continuación se describen los ataques realizados comúnmente al protocolo *(RTP).*

- **Captura e inserción de Audio.**

  La captura e inserción de audio, puede ser una amenaza tanto de *(DoS),* como de interceptación *(eavesdropping).* Este ataque funciona debido a que en las llamadas *(VoIP),* se realiza por el protocolo (*UDP*), el cual no da garantías en la entrega de sus mensajes y no mantiene ningún tipo de información de estado o conexión. Cuando el propósito del atacante es lograr que un usuario no pueda realizar correctamente una llamada, es decir, realizar una denegación de servicio, puede agregar ruido o incluso su propio mensaje y así degradar o alterar drásticamente la conversación. Por otra parte, cuando un atacante quiere escuchar llamadas en curso, donde se esté transmitiendo información importante, el atacante solo debe capturar los mensajes y después decodificar los paquetes capturados. [4]

- **Saturación mediante paquetes (RTP).**

  Es una amenaza del tipo *(DoS),* específicamente una inundación *(flood).* Se realiza durante el establecimiento de la sesión, al se intercambia información relativa al protocolo de transporte. [4]

4.10.5. Protocolo de Control de Transporte de Tiempo Real (RTCP).

Se encarga de transportar los datos del monitoreo de la calidad del servicio que el protocolo *(RTP),* proporciona. *(RTCP),* no transporta información por sí mismo, para esto

utiliza *(RTP),* que se encarga de transmitir periódicamente paquetes de control *(RTCP),* a todos los participantes de una sesión. [4]

4.10.6. Control de medios.

En esta sección, se describen los protocolos de control de medios *(MGCP)* y *(MEGACO) o (H.248)* por ser los más utilizados, para realizar este proceso en redes *(VoIP).* [4]

- **Media Gateway Control Protocol (MGCP).**

  Los ataques a *(MGCP),* son poco comunes, debido a que *(MGCP),* es un protocolo utilizado en grandes redes *(VoIP),* donde existen gran cantidad de usuarios y varios *gateways* por ende, más de una salida, hacia la red telefónica tradicional. [4]

- **Suplantación (MGCP)**

  El ataque de suplantación es una amenaza de interceptación *eavesdropping*, el cual elige una conexión activa y solicita al dispositivo *(MGCP),* ciertos detalles de la conexión elegida, como por ejemplo, el identificador de llamadas; después de que el *gateway* atacado responde estos mensajes, el atacante vuelve enviar un mensaje, con todos los datos obtenidos, para dirigir el tráfico *(RTP),* hacia él y escuchar la llamada.

4.10.7. Protocolos propietarios.

En esta sección, se describen dos protocolos propietarios, *Skinny Client Control Protocol (SCCP) y (IAX2),* que se utilizan para proveedores de *(VoIP),* específicos, pero son ampliamente utilizados en redes (*VoIP).* [4]

- **Skinny Client Control Protocol (SCCP).**

  La documentación de *(SCCP),* es muy escasa y difícil de conseguir, porque Cisco mantiene documentación sólo para sus afiliados, esto hace más difícil la tarea de los atacantes, sin embargo las vulnerabilidades igualmente existen. [4]

- **Vulnerabilidades en el call manager.**

  El *call manager*, que es una central telefónica que sirven para indicar el estado de un usuario, son atacados remotamente e inundados con tipos específicos de tráfico, con la intención de hacerlos colapsar.

4.10.8. Inter Asterisk Exchange v.2 (IAX2).

- **Ataque Poke.**

Este ataque es una amenaza de *(DoS)* y utiliza la vulnerabilidad del mensaje *(POKE)*, del protocolo *(IAX2).* Por medio del envío masivo de peticiones *(POKE)*, a un sistema vulnerable, un atacante podría acaparar todos los números de las llamadas *(líneas)* asociados con el protocolo *(IAX2)*, impidiendo el procesamiento del resto de llamadas o peticiones. [4]

- **Inundación con (IAX).**

Este ataque es una amenaza de *(DoS)*, puede utilizar una gran gama de mensajes pertenecientes al protocolo *(IAX2).* Este ataque envía mensajes *(IAX2)*, en grandes cantidades para hacer colapsar al dispositivo *(IAX)*, receptor, esto es posible debido a que el protocolo (IAX2), no auténtica todos sus mensajes. [4]

- **Ataque de enumeración con (IAX).**

Este ataque es una amenaza de acceso no autorizado, que utiliza herramientas que enumeran usuarios de *(IAX2), (utilizando fuerza bruta)*. Para conseguir este objetivo, se envían peticiones *(IAX2)*, válidas y se monitorea la respuesta. [4]

- **Ataque hangup**

Este ataque es una amenaza de *(DoS)*, que utiliza una vulnerabilidad del mensaje (*HANGUP)*, que permite cancelar las llamadas. Este ataque funciona capturando paquetes del tipo *(PING)*, *(PONG)* o *(ANSWER)* y se reemplazan los campos incluyendo el número de secuencia correspondiente, de allí se envía el mensaje de *(HANGUP)*, si este mensaje llega antes que el mensaje correspondiente enviado por el servidor la llamada se cancela. [4]

4.10.9. Resumen de vulnerabilidades capa de sesión y transporte.

A continuación, se define una matriz que resume los atributos de seguridad que afectan los ataques antes vistos. Se clasifican de acuerdo al protocolo vulnerado y permite establecer las contramedidas, que se puede usar para estos, en la sección de resultados.

Tabla 4: Vulnerabilidades en la capa de Sesión y Transporte.

PROTOCOLO	ATAQUE	C	I	D
H.323	Ataque *(H.225)*			✓
	Ataque *(H.245)*			✓
	Malformación de mensajes *(RAS)*		✓	✓
SIP	Ataque a hashes digest	✓	✓	
	Suplantación de identidad *(Registration hijacking)*		✓	
	Desregistro de usuarios			✓
	Desconexión de usuarios			✓
	Malformación en mensajes *(INVITE)*			✓
	Inundación en mensajes *(INVITE)*			✓
	Ataque de falsa respuesta *(Faked Response)*			✓
	Ataque de *(Re-INVITE)*		✓	
RTP	Captura e inserción de Audio			✓
	Manipulación *(RTP tampering)*			✓
	Saturación mediante paquetes *(RTP)*			✓
MGCP	Suplantación (hijacking)	✓		
	Creación de llamadas		✓	
	Cancelación de conexión			✓
IAX2	Ataque *(POKE)*			✓
	Inundación con *(IAX)*			✓
	Ataque de enumeración con *(IAX)*	✓	✓	✓
	Ataque *(HANGUP)*			✓

Fuente: Seguridad en voz sobre (IP) María José Liberona (2010)

4.11. VULNERABILIDADES DE LA VOIP EN LA CAPA DE RED.

Las vulnerabilidades de *(VoIP)*, en la capa de red, son comunes a las vulnerabilidades de las redes de datos, por lo tanto, no se estudiarán en detalle ***(para más información respecto de las vulnerabilidades de la capa de red, de una red de datos, revisar aquí).***

4.11.1. Vulnerabilidades del protocolo IP.

Los ataques comúnmente realizados en la capa de red, utilizan el protocolo *(IP)* y los protocolos descritos en la tabla anterior, además los protocolos de *(VoIP)*, utilizan protocolos para transportar sus mensajes, por ello se considera a *(UDP)*, y *(TCP)*. [4] [5]

Tabla 5: Ataques en el protocolo (IP).

ATAQUE IP	AMENAZA	DESCRIPCIÓN
Suplantar *(IP) (IP spoofing)*	*(DoS)*, acceso no autorizado	Consiste en la generación de paquetes *(IP)*, con direcciones *(IP)* de orígenes falsificados. Este ataque da lugar a muchos otros.
Inundación*(IP) (IP flooding)*	*(DoS)*, inundación	Consiste en la generación de tráfico *(IP)* basura, con el objetivo de conseguir la degradación del servicio, un ejemplo de esto son los ataques *(UDP/flood)* o *(ICMP/flood).*
Smurf	*(DoS)*, inundación	Se envían mensajes *(ICMP)*, broadcast a la red, solicitando respuesta, pero con la dirección de origen falsificada. Esto provoca una inundación de respuestas *(ICMP)*, hacia la dirección falsificada, cuyo dueño es la víctima del ataque.

Inundación *(TCP/SYN)*	*(DoS)*, inundación	El atacante genera un gran número de paquetes, con diferentes direcciones *(IP)* y establece conexiones (*TCP)*, inundando el buffer de la víctima, esto se realiza para los servidores de diversos servicios de (*TCP)*, como: *(telnet, FTP, HTTP, SMTP).*
Teardrop	*(DoS)*, fuzzing	El ataque teardrop realiza una utilización fraudulenta de la fragmentación *(IP)*, para poder confundir al sistema operativo, en la reconstrucción del paquete original y colapsar así el sistema.
Ping de la muerte *(Ping of deah)*	*(DoS)*, fuzzing	El ataque ping de la muerte, se basa en la posibilidad de construir, mediante el comando ping, un paquete *(IP)*, superior a los 65535 bytes, fragmentado en ***N*** trozos, con el objetivo de provocar incoherencias en el proceso de re-ensamblado en el receptor y hacer que el receptor no pueda comunicarse.
Land	*(DoS)*, fuzzing	Este ataque permite bloquear un sistema, mediante un paquete cuya dirección de origen y destino son las mismas. También se utiliza con el mismo puerto de origen y destino.
TRIN00	*(DDoS).*	*(TRIN00)*, es un conjunto de herramientas *maestro-esclavo* utilizadas para sincronizar distintos equipos que cooperan, de forma distribuida, en la realización de *(DoS)*. Existe una versión para *Windows*, *Wintrin00*.
. *(Tribe Flood Network)*	*(DDoS).*	*(TFN)*, es otra de las herramientas existentes, para realizar ataques de denegación de servicio distribuidos que utiliza un esquema *maestro-esclavo*, para coordinar ataques de denegación tradicionales *(ICMP Flooding, SYN Flooding, UDP Flooding.*
Inanición (DHCP)	*(DoS).*	Los atacantes pueden hacer peticiones masivas al *(DHCP)*, para agotar las direcciones *(IP)*, disponibles en el servidor *(DHCP)*. Con esto logran evitar que las direcciones *(IP)*, sean asignadas a los teléfonos *(IP)*, causando una denegación de servicio.
Suplantación *(DHCP).*	Acceso no Autorizado	En un ataque de suplantación *(DHCP)*, el atacante se hace pasar por un servidor *(DHCP)*, y obtiene el control de la asignación de direcciones *(IP)*.

Fuente: Seguridad en voz sobre IP María José Liberona (2010)

4.11.2. Resumen.

En este punto se hizo un análisis de las vulnerabilidades en la capa de red, con énfasis en los ataques más conocidos que utilizan las vulnerabilidades del protocolo *(IP).*

Tabla 6: Vulnerabilidades en la capa de Red.

PROTOCOLO	ATAQUE	C	I	D
IP	Suplantación de dirección *(IP) (IP spoofing)*		✓	✓
	Inundación *(IP) (IP flooding)*		✓	✓
	Teardrop		✓	✓
	Loki	✓	✓	✓
	Land		✓	✓
	Tribu red de inundación *(Tribe Flood Network)*			✓
	Eje *(Shaft)*			✓
ICMP	Smurf		✓	✓
	Ping de la muerte (Ping of death)		✓	✓
TCP/IP	Inundación *(TCP/SYN)*		✓	✓
DHCP	Inanición *(DHCP)*			✓
	Ataque de suplantación *(DHCP)*		✓	

Fuente: Seguridad en voz sobre (IP) María José Liberona (2010)

4.12. VULNERABILIDADES DE LA VOIP EN CAPA DE ENLACE.

A continuación, se describen brevemente cada uno de los ataques de la capa de enlace, estos ataques no son propios de las redes de *(VoIP),* sino que, se heredan de las redes de datos.

4.12.1. Ataque de salto de VLAN (VLAN Hopping).

El ataque de salto de *(VLAN),* consiste en que el atacante se hace pasar por una troncal utilizando un switch y así gana acceso a todas las *(VLAN),* en la red. Actualmente este ataque ha sido mitigado, por los proveedores de dispositivos de red. Este ataque permite que los atacantes puedan tener acceso a todas las redes lógicas disponibles y a los datos que por ellas son transmitidos. [4] [5]

4.12.2. Ataque de inundación MAC (MAC flood).

Un ataque de inundación por *(MAC),* ocurre cuando un atacante envía direcciones *(MAC),* no validas a la tabla *(CAM 3),* haciendo que se agote el espacio de almacenamiento de las direcciones *(MAC).* El *switch*, al encontrar la tabla *(CAM),* llena, no reconoce la dirección del receptor como entrada valida y envía el paquete recibido por todos sus puertos. [5]

4.12.3. Ataque de suplantación ARP (ARP Spoofing).

El ataque de suplantación *Address Resolution Protocol (ARP),* es un ataque que funciona reemplazando la *(MAC),* del atacante por una *(MAC),* de un usuario válido, capturando la identidad del usuario y por ende su tráfico. [5]

4.12.4. Resumen.

Aquí se analizó las vulnerabilidades de la capa de enlace, con énfasis en los ataques más conocidos que utilizan las vulnerabilidades de los *switch Cisco*.

Tabla 7: Vulnerabilidades la capa de Enlace.

PROTOCOLO	ATAQUE	C	I	D
802.1Q	Salto de *(VLAN), (VLAN hopping)*	✓	✓	
(ARP)	Inundación *(MAC), (MAC flood)*	✓	✓	✓
	Suplantación *(ARP), (ARP spoofing)*	✓	✓	

Fuente: Seguridad en voz sobre (IP) María José Liberona (2010)

4.13. EXPLORACIÓN DE PUERTOS.

Las vulnerabilidades en el modelo *(TCP/IP),* están asociados a los protocolos que utilizan las aplicaciones o servicios, para establecer la comunicación según la numeración, los puertos se pueden clasificar en:

- **Puerto con números inferiores a 1024**:

  Denominados puertos bien conocidos, reservados para servicios muy definidos como: telnet, *Simple Network Management Protocol (SMTP), Post Office Protocol (POP3),* etc. Son asignaciones fijas que no pueden ser utilizadas por otros servicios. [6]

- **Puertos numerados entre 1024 y 49151:**

  Son los puertos registrados, significa que *(IANA),* intenta ordenar el uso de este rango, pero sin las restricciones que existen para los puertos bien conocidos. [6]

- **Puertos numerados entre 49152 y 65535:**

  Son puertos privados, de los que se puede disponer para cualquier uso. [6]

4.14. TEST DE INTRUSIÓN.

El test de intrusión o pruebas de penetración, permite evaluar vulnerabilidades, por medio de la identificación de debilidades de configuración que pueden ser explotadas, analizadas y categorizadas, estas se basan en el impacto potencial y la posibilidad de concurrencia, por ende, se puede promover recomendaciones priorizadas para mitigar y eliminar las debilidades, para ello generalmente se utilizan dos métodos como: [7]

- **El método de caja negra (white box);** Mismo que consiste en intentar penetrar en la red, sin tener conocimiento del sistema y generar una situación realista. [7]

- **El método de caja banca (black box);** Consiste en intentar penetrar en el sistema por completo, teniendo cierto grado de conocimiento del diseño de la red, para poner a prueba los límites de la seguridad de la red. [7]

El método de caja blanca se utilizó para llevar a cabo esta investigación, debido a que existe el consentimiento, por parte del administrador de la red de datos del Hospital Isidro

Ayora de Loja, para poder extraer información a fines al objeto de estudio y realizar modificaciones, ya sea en la red o el servidor de voz, este acuerdo se lo realizó por medio de una carta de autorización ***(ver anexo. B)***

4.15. METODOLOGÍAS PARA ANÁLISIS DE VULNERABILIDADES EN REDES VOIP.

En el siguiente apartado se realiza la comparación de tres metodologías de auditorías y *pentesting***,** mediante este análisis se podrá definir cuál será la mejor metodología, que se acople al proyecto de investigación, *pentest* es un método de evaluación y seguridad de un sistema, simulando un ataque, tal y como lo llevaría a cabo cualquier hacker que pretendiera hacerse con el control del sistema, manipular la información o robarla, sobre todo, aquella que se define como sensible y crítica. Las metodologías que van a ser detalladas, están al alcance de cualquier persona; es decir, son de libre uso, por ende, al hacer uso de estas, se debe contar con preparación precisa, madurez, rigor ético y prudencia moral, para garantizar su objetividad. Todas estas metodologías contienen pruebas de *(white box)* y *(black box),* cuya definición se la describe en el punto de (test de instrucción), pero curiosamente una de ellas es la excepción por ejemplo: (*OWASP)* la cual solo usa *(black box).*

- ***(OWASP)***. Método de test para aplicaciones web, basado en dos fases: pasiva y activa, enfocada en *"black box"*, se sabe poco de la aplicación que va ser probada, incluso del contexto que se van a hacer las pruebas. [8] [9]

- ***(ISSAF).*** Es una metodología diseñada para evaluar una red, los sistemas y la aplicación de controles según la *web, Open Information Systems Security Group (OISSG),* cabe mencionar que no está actualizada desde el año 2006. Utiliza un enfoque que se lleva a la práctica en tres fases y se evalúa en 9 pasos. [8] [10]

- ***(OSSTMM)***. Es una metodología que reúne las diversas pruebas y métricas de seguridad, utilizadas por los profesionales durante las auditorías de seguridad, esta se centra en los detalles técnicos de los elementos que deben ser probados. ¿**Qué** hacer antes, durante y después de una prueba de seguridad? y ¿**Cómo** medir los resultados? [8] [11]

4.15.1. Comparativa de las metodologías en cuestión.

En la siguiente tabla, se realiza un análisis de las características más relevantes de las metodologías enunciadas anteriormente, cabe señalar que en el estudio realizado, no podemos extraer sabias conclusiones que reflejen gran profundidad de lectura y análisis, para un mejor detalle de la comparación realizada ***(ver anexo F).*** [8]

Tabla 8: Comparativa entre las metodologías más usadas en seguridad de redes.

PATRONES	ISSAF	OWASP	OSSTMM
Rigor de la metodología	Alta. Desactualizada. Año 2006.	Muy Alta. Solo centrada en la web, pero muy didáctica e instructiva.	Muy Alta. Actualizada y en constante revisión
Niveles de detalle	Muy detallada, pero sencilla. Faltan elementos de cloud computing y Protección datos.	Muy detallada. Su enfoque web no le resta ni un ápice de meticulosidad. Orienta perfectamente el trabajo del auditor.	Parece como si la experiencia de uso de anteriores versiones diera lugar a crear la necesidad de formación previa.
Facilidad de uso	Muy Alta. Se puede usar con conocimientos medios.	Alta. Muy técnico, aunque muestra uso de herramientas, sugiere usos y muestra ejemplos.	Media. Muy técnico. Requiere entrenamiento y práctica. Certificaciones.
Entornos de aplicabilidad	Todos. Genérico para auditorías de todo tipo. *¿Servidores IBM únicamente?*	Solo web y aplicaciones enfocadas a la web. Servidores.	Todos. Incluso los que todavía no se han implementado. Es dinámica y potente en su diseño.
Uso por los auditores	Fácil. Es lineal y cubre las etapas típicas de una auditoría con test de intrusión. Ampliamente usado ya que respeta los modelos *NIST (que se tienen muy en cuenta en USA)*	Muy usado también en combinación con el resto de metodologías por su precisión y nivel de detalle. Detrás hay muy importantes empresas e instituciones que quieren que esta metodología se desarrolle plenamente	El más usado por lo que he podido averiguar en Internet, aunque la tendencia es simplificar *(tipo ISSAF)*, su uso supone un conocimiento y experiencia alto.
Ventajas	Fase de evaluación conocida. Uso frecuente del método. Pasos más desgranados en el pentest. Facilita el informe en función de los pasos seguidos y los resultados obtenidos. Recomienda herramientas para la evaluación.	Facilidad de uso de los controles más conocidos Top Ten". Novedoso y bien estructurado. Se preocupa de las auditorías de la web = elemento centrado en el Marketing y el negocio. Propone hasta las herramientas de uso.	Ampliamente documentada, soporte de la Comunidad. Pone a punto plantillas de uso y medidas. Se integra y tiene en cuenta todos los estándares de seguridad de la información.

Inconvenientes	Falta concretar acuerdos, no señala límites en el uso de los tests. Menos rigurosa que el resto. Podría escaparse de las manos el uso de los tests de intrusión. Inmaduro en cuanto a desarrollo.	Habría que combinar con otras herramientas y metodologías para que la auditoría fuera más completa. No olvidemos que la infraestructura de la web y los servidores no son auditados.	No se hace referencia a qué tipo de objetivos para cada tipo de test. Se basa más en la creatividad del auditor y también en su experiencia.
Comentario y valoración personal	Un poco desactualizada. Al ser una metodología lineal *(aunque se señala como cíclica)*, es de fácil uso y la práctica puede aplicarla auditor sin experiencia.	Menos agresiva e intrusiva, fácilmente se pueden borrar las huellas de paso.	Al igual que *ISSAF* es agresiva y muy intrusiva, pero deja muy clara su postura en cuanto a los límites en los acuerdos con el cliente *(objetivo)*

Fuente: Comparativa de metodologías de auditorías y pentesting. Maximiliano Camilo Pérez Fernández (2012).

Luego de haber analizado y comparado las diferentes metodologías, se determina que la metodología que mejor se acopla al tema de investigación es ***(OSSTMM),*** por contar con secciones que se desarrollan de forma individual, es decir, es muy versátil y flexible, la cual encaja perfecto en el estudio que se lleva a cabo; de las seis secciones que contiene dicha metodología, se escogen dos secciones denominadas:

- **Seguridad en las Tecnologías de Internet.**
- **Seguridad en las Comunicaciones.**

Estas dos secciones son necesarias para poder llevar a cabo la presente tesis, sobre todo la sección de **seguridad en comunicaciones,** por ser la parte medular del estudio, para un detalle completo de la metodología en cuestión ***(ver anexo D).*** [11]

4.16. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES EN VOIP.

Aquí se detalla, las herramientas de seguridad y *hacking*, para la explotación de redes y sistemas de información, mismas que son utilizadas por los piratas informáticos y analistas de seguridad, es decir, se utilizan con fines legales como ilegales.

- **KALI LINUX.** Es una distribución de *Linux*, para pruebas de penetración y auditorías de seguridad, cuenta con más de 300 herramientas para pruebas de penetración de forma gratuita. Esta herramienta puede descargarse desde aquí: https://www.kali.org/downloads/.

- **NMAP.** Permite descubrir qué puertos están abiertos en el *host* de destino, se suele realizar en la fase inicial de una prueba de penetración, para descubrir todos los puntos de entrada de red. Esta herramienta puede descargarse desde aquí: https://nmap.org/download.html.

- **ICMQUERY.** Esta herramienta nos permite tener información del sistema, como la máscara de red mediante paquetes *(ICMP)*. Esta herramienta puede descargarse desde aquí: http://www.gegereka.com/?&tg=P22G18

- **SIPSCAN.** Es una herramienta que trabaja sobre *Windows*, cuya utilidad es obtener extensiones *(SIP)*, de una *(PBX)*, tan solo conociendo la dirección *(IP)*, del Servidor. Esta herramienta puede descargarse desde aquí: http://sipscan.software.informer.com/1.0/

- **ENUN IAX.** Es una herramienta que trabaja sobre *Linux*, y que sirve para la obtención de extensiones *(IAX)*, de una *(PBX)*. Esta herramienta puede descargarse desde aquí: http://sourceforge.net/projects/enumiax/.

- **ICMPENUM.** Permite la enumeración de host y determinar la dirección *(IP)*, es ideal para la suplantación de identidad y la escucha promiscua de paquetes de respuesta. Esta herramienta puede descargarse desde aquí: http://linux.softpedia.com/get/System/Networking/Icmpenum-26927.shtml.

- **ETTERCAP.** Es un sniffer potente y flexible para los ataques *(MitM)*, es compatible con muchos protocolos *(incluso algunos cifrados)*, e incluye muchas características para el análisis de la red y de *host (como huellas digitales OS)*. Esta herramienta puede descargarse desde aquí: http://ettercap.source.net/downloads.html

- **TCPDUMP.** Trabaja bajo *Linux y Unix*, analiza e intercepta el tráfico entrante y saliente de las redes hacia el equipo, por medio de librerías *libpcaps*. Puede leer y escribir el contenido de un fichero capturado. Esta herramienta puede descargarse desde aquí: http://tcpdump_for_windows.es.downloadastro.com/

- **WIRESHARK.** Es un analizador de protocolos, utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, porque permite ver todo el

tráfico que pasa a través de una red, este incluye un completo lenguaje, para filtrar lo que quiere ver y la habilidad de mostrar el flujo reconstruido de una sesión. Esta herramienta puede descargarse desde aquí: https://www.wireshark.org/download.html

- **NESSUS.** Es un programa de escaneo de vulnerabilidades, consiste en dos partes *(nessusd)*, que es el encargado de realizar un escáner en el sistema objetivo, y *(nessus)*, que es el cliente *(basado en consola o gráfico*), que muestra el avance y resultados de los escáner. Desde la consola nessus puede ser programado con Chrome para hacer escáner o actualizar la base de datos de *plugins*. En operación normal, nessus comienza escaneando los puertos con *(Nmap)*, o con su propio escaneador de puertos, para buscar puertos abiertos y después intenta usar varios *exploits* para atacar. Esta herramienta puede descargarse desde aquí: http://www.tenable.com/products/nessus-system

4.17. METODOLOGÍAS PARA ANÁLISIS DE RIESGOS.

El estudio de las metodologías de análisis de riesgo, permite seleccionar aquella que mejor se ajuste a los objetivos del proyecto, se describen tres de las metodologías más utilizadas, a través del siguiente cuadro comparativo. Las vulnerabilidades tecnológicas aportan el mayor porcentaje en el riesgo de seguridad de una organización, lo que conlleva a profundizar este tema con datos de investigaciones reales. [8] [12]

Tabla 9: Cuadro comparativo de las metodologías de análisis de riesgos.

CARACTERÍSTICAS	MAGERIT	OCTAVE	CRAMM
País de creación	España	Estados Unidos	Reino Unido
Herramientas para aplicar la metodología	Herramientas: *PILAR CHINCHON*	Según lo investigado la norma no especifica un producto en concreto para el análisis Vulnerability, Evaluation & Tools.	Un gran número de herramientas de análisis y gestión de la información ejemplo *(CRAMM Express)*
	Planificación del proyecto de riesgos: *(como consideraciones iniciales para arrancar el*	**Construcción de las vulnerabilidades basadas en activos** *(visión organizacional).*	**Identificación y valoración de activos** *(Se identifican los activos físicos y los activos, software, y los*

Fases	*proyecto de análisis y gestión de riesgos.)* **Análisis de riesgo:** *(Se identifican y valoran las diversas entidades, obteniendo una valoración del riesgo, así como, una estimación del umbral de riesgo deseable)* **Gestión de riesgo** *(se identifican las funciones y servicios de salvaguarda reductoras del riesgo).* **Selección de salvaguarda** *(plan de implantación de los mecanismos de salvaguardas elegidos).*	**Identificación de las vulnerabilidades de la infraestructura** *(visión tecnológica)* **Desarrollo de la estrategia de seguridad y planes de mitigación de las vulnerabilidades** *(estrategia y plan de desarrollo).*	*activos de datos que conforman los sistemas de información).* **Valoración de las amenazas y vulnerabilidades** *(determinar cuál es la probabilidad de que esos problemas).* **Selección y recomendación de contramedidas** *(CRAMM contiene una gran librería de más de 3.000 contramedidas organizadas en 70 grupos).*
Principales características	Habla de análisis algorítmico con 3 modelos: cualitativo cuantitativo y escalonado. En la versión 2 posee 3 documentos: Catálogo Metódico y Técnicas	Posee Self- Direction un pequeño equipo de personal de la misma organización, es involucrado en los procesos de implementación de la metodología *(personal de IT y de otros departamentos).* Creación de un grupo pequeño interdisciplinario de análisis de la información.	400 tipos de activos. 38 tipos de amenaza. 25 tipos de impactos. 7 medidas de riesgo 3500 control
Costo	No tiene costo ya que es una normativa libre de libre aplicación Plantea un análisis de costo beneficio, expresa una fórmula del ROI	Usó internet gratuita Uso externo se debe comprar la licencia y si se quiere implementar la metodología a un tercero	La versión 4 para una compañía comercial € 3550. Para agencias y departamentos € 2450.
Resultado de análisis	Resultados ordinales y cardinales	Fase 1 activos críticos requerimientos críticos para activos críticos vulnerabilidades de los activos críticos lista de prácticas de seguridad actuales lista de vulnerabilidades actuales de la organización fase 2 componentes claves vulnerabilidades tecnológicas actuales base 3 riesgo de los activos críticos métricas del riesgo estrategia de protección planes de mitigación de riesgo	Tabla de valoración de riesgo sobre los activos en escala de uno a diez

Análisis	Soporta un análisis completo cualitativo y cuantitativo, pero no la combinación de los dos.	El análisis cualitativo y cuantitativo no es completo pero es satisfactorio, porque permite la combinación de las dos.	Soporta un análisis completo cualitativo y cuantitativo pero no la combinación de los dos
Inventarios	Permite el análisis de todos los tipos de recursos, amenazas y salvaguardas no incluye vulnerabilidades.	Permite determinar para todos los recursos amenazas, vulnera bilidades y salvaguardas.	Permite el análisis de todos los tipos de recursos, amenazas, v ulnerabilidades y salvaguardas.
Aplicación	Análisis de riesgo Gestión del riesgo Plan de seguridad	Análisis de riesgo Gestión del riesgo Plan de seguridad	Análisis de riesgo Gestión del riesgo Plan de seguridad
Otras	Tiene una herramienta de soporte que la hace más efectiva proporciona inventarios predefinidos	Permite el uso de herramientas externas para la identificación de vulnerabilidades.	Dispone de una herramienta con una extensa base de datos de activos salvaguardas

Fuente: Análisis Comparativo: Metodologías de análisis de Riesgos Abraham Mogollón (2011)

Luego de haber realizado una comparación, de las diferentes características de las metodologías para el análisis de los riesgos se determina que ***(OCTAVE),*** es la que mejor se perfila para llevar a cabo esta investigación, debido a la siguientes características: es gratuita, se la utiliza para pequeñas empresas y cuenta con pasos cortos y ofrece flexibilidad en cada uno de ellos, cuyas característica permiten dar cumplimiento a los objetivos planteados. Para mejor detalle de esta metodología ir al (**Anexo E).**

4.17.1. Análisis y gestión de riesgo.

El primer paso de la gestión de riesgo, es el análisis de un proceso que comprende la identificación de activos informáticos, así como las vulnerabilidades y amenazas a los que están expuestos, además se analiza la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. Conceptos que intervienen en el control de riesgo. [13]

- **Amenaza.** Es la posibilidad de ocurrencia de cualquier tipo de evento, o acción que produce un daño *(material o inmaterial)*, sobre los elementos de un sistema.

- **Vulnerabilidad.** Es la exposición latente a un riesgo, debido al grado de susceptibilidad ante alguna amenaza.

- **Impacto.** Consecuencia de que la amenaza ocurra.

En la figura 5, se detallan directrices para la gestión de riesgos de seguridad que proporciona la norma *(ISO 27001),* mas no proporciona ninguna metodología específica para el análisis y la gestión del riesgo. [12] [13]

4.17.2. Valoración del riesgo.

Se basa en la fórmula matemática: $Riesgo = PA * MD$ *donde, (PA = Probabilidad de Amenaza. Md Magnitud de Daño).*

Grado de Clasificación del Riesgo		Consecuencias		
		Ligeramente dañino	Dañino	Extremadamente dañino
Probabilidad	Baja	Riesgo trivial	Riesgo tolerable	Riesgo moderado
	Media	Riesgo tolerable	Riesgo moderado	Riesgo importante
	Alta	Riesgo moderado	Riesgo importante	Riesgo intolerable

Ilustración 5: Probabilidad de amenazas y magnitud de daños.
Fuente: Fabián Leonardo Cortés Torres 2012

Mediante la fórmula descrita se pueden calcular valores entre **(1** y **2)** = Bajo, **(3** y **4)**,= Medio, **(6** y **9)** = Alto, mientras más alta sea la probabilidad de amenaza y la magnitud del daño, más grande es el riesgo y el peligro al sistema, por ello hay que implementar medidas de protección. Se habla de un ataque cuando una amenaza se convirtió en realidad, se habla de un impacto cuando un ataque fue exitoso y perjudica a la confidencialidad, integridad, disponibilidad, y autenticidad de la información. [12] [13]

4.18. SEGURIDAD EN REDES.

Las necesidades de seguridad de la información han ido evolucionando, con la aparición del Internet, la seguridad de un sistema generalmente es "asimétrica" *(diferente),* el pirata informático debe encontrar sólo una vulnerabilidad, para poner en peligro el sistema, mientras que él administrador debe corregir todas sus fallas. Es erróneo pensar que una filosofía de seguridad tradicional, basada en passwords y protección de ficheros, es

suficiente para protegerse en una red o en Internet, porque la seguridad como tal, implica a más de un elemento, por ende, la seguridad en redes debe garantizar el funcionamiento de todos los equipos conectados a la misma, la confidencialidad, integridad y disponibilidad, debe ser accesible únicamente al autorizado, si se manejan estos parámetros de seguridad se podría evitar lo siguiente: [14] [15]

- Que personas no autorizadas intervengan en el sistema, con el fin de modificar o robar la información.
- Que los usuarios realicen operaciones involuntarias que puedan dañar el sistema.
- Asegurar los datos mediante la previsión de fallas.
- Garantizar que no se interrumpan los servicios.

4.18.1. Seguridad física.

La seguridad física *"Es la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas hacia las amenazas que perjudican ya sea a los* activos *o la información confidencial de una organización"*. Estos mecanismos, son implementados para proteger el *hardware* y medios de almacenamiento de datos, por ende todos los *(servidores, centros de cómputo o data center),* deben contar con parámetros de seguridad física, así mismo, deben ubicarse en sitio adecuado y solo tener acceso el personal autorizado, ya sea a través de lectores de tarjetas, controles biométricos e incluso cajas acorazadas y cámaras de seguridad, dependiendo de la importancia de los datos almacenados. Si se cuenta con estas medidas de seguridad, se puede cubrir amenazas ocasionadas tanto por el hombre, como por la naturaleza, las principales amenazas que se prevén en la seguridad física son: [14] [15]

- **Desastres naturales:**
    - **Incendios accidentales:** Son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas o defectuosas, inadecuado almacenamiento y traslado de sustancias peligrosas.
    - **Tormentas e inundaciones.** Se las define como la invasión de agua, por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.

- **Amenazas por el hombre:**

    - **Robo.** Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero, el *software* es una propiedad muy fácil de sustraer, las cintas y discos son fácilmente copiados sin dejar rastro alguno.

    - **Fraude.** Cada año, millones de dólares son sustraídos de empresas u organizaciones financieras y en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

    - **Sabotaje interno y externo.** El peligro más temido en los centros de procesamiento de datos, es el sabotaje; las empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros, estos sujetos pueden ser empleados de la misma organización o ajenos a la ella.

En conclusión, la seguridad física de la entidad es la base para comenzar a integrar la seguridad, como una función primordial dentro de cualquier organismo tener controlado el ambiente y acceso físico permite: [14] [15]

- Disminuir siniestros.
- Trabajar mejor manteniendo la sensación de seguridad.

4.18.2. Seguridad lógica.

Se refiere al uso de herramientas para la protección de la información, en el mismo medio en el que se genera o se transmite; para ello, debe contar con protocolos de autenticación entre cliente y servidor, además se debe contar con reglas de seguridad en las aplicaciones para, garantizar la austeridad, así mismo, deben incluirse medidas de prevención de riesgos y la instauración de políticas, normativas y planes de contingencia, para la recuperación en caso de que exista cierto incidente o desastre, es decir, la seguridad lógica consiste en *"Aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita el acceso a personas autorizadas"*. Los principales objetivos que se plantean dentro de la seguridad lógica son los siguientes: [14] [15]

- Asegurar que los operadores trabajen sin una supervisión minuciosa y no puedan modificar los programas, ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas por el procedimiento correcto.
- Que la información transmitida, sea recibida sólo por el destinatario, al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que no existan sistemas alternativos o secundarios, para la transmisión de datos entre los diferentes puntos de conexión.
- Que se disponga de pasos alternativos en caso de emergencia, para la transmisión de información. [14] [15]

4.18.3. Seguridad en la red de VoIP.

Comúnmente los administradores de redes, cometen el error de pensar que al de digitalizar la voz, y enviarle por la red de datos, con las medidas de seguridad que esta tiene, ya se le ha transferido a la voz dicha seguridad, cosa que no es tan cierta porque es necesario reforzar la seguridad de la digitalización de la voz, de manera independiente de la establecida en la red. El hecho de que la voz esté en un medio compartido que comunica servicios y/o recursos, resulta problemático ofrecer las bases de la seguridad que son: confidencialidad, integridad, autenticidad y disponibilidad, por ser la base del diseño del protocolo *(IP),* no se diseñó para brindar seguridad por sí misma. Por esto es muy importante considerar las implicaciones de seguridad para la *(VoIP),* la cual puede ser implementada muy fácilmente en las centrales telefónicas *(VoIP)* y de esta forma evitar ataques indiscriminados. Para redactar una guía de creación de una infraestructuras segura de *(VoIP),* es necesario listar más de un tema y mucho más extenso que el actual, por lo que me limitaré, a señalar qué controles de seguridad deben ser imprescindibles en el entorno *(VoIP)* y explicar las medidas necesarias, para aplacar la mayoría de riesgos y ataques comentados en los apartados anteriores; para mantener segura la tecnología de *(VoIP),* es necesario tener en cuenta lo siguiente: [5] [14] [15]

- Mantener los sistemas y antivirus actualizados.
- La red de *(VoIP),* debe estar sobre una infraestructura de red segura.

- Se debe contar con *Intrusion Detection System (IDS)* o *Intrusion Prevention System (IPS),* porque estos, detectan y previenen ataques contra los protocolos, (*fuzzing*) ataca contra los servicios, *(exploits y vulnerabilidades)*, escaneos y ciertos tipos de ataques *(DoS).*
- Configurar protocolos y dispositivos para que utilicen autenticación y/o cifrado. Este punto se especifica con mayor descripción, por ser la parte medular del tema de investigación:

Todos los mensajes que se intercambia deben tener una autenticación o un cifrado, cada dispositivo debe de tener limitado los grupos de elementos o direcciones *(IP),* de los que pueden recibir tráfico; con una correcta configuración, es posible limitar muchos de los ataques de denegación de servicio, el cifrado es quizás una de las principales medidas que se deben adoptar en una infraestructura *(VoIP).* El uso de *Internet Protocol security (IPsec),* proporciona servicios de seguridad para el tráfico *(IP),* lo que permite configurar un canal *(IP),* seguro, el anfitrión puede elegir los diferentes servicios, en función del nivel de seguridad requerido, los servicios proporcionados por *(IPsec),* se basan en dos sub-protocolos: un sub-protocolo de *Authentication Header (AH)* y un combinado de cifrado y el sub-protocolo de autenticación *Encapsulating Security Payload (ESP).* [14]
El primero ofrece servicios tales como integridad sin conexión y autenticación del remitente, mientras que el segundo es en encargado de garantizar la confidencialidad entre otros servicios. El uso de *Secure Sockets Layer/Transport Layer Security (SSL/TLS),* para establecer canales de comunicación seguros, resolverá la mayoría de problemas de *eavesdropping*, manipulación y reproducción de los mensajes que se intercambian. Los teléfonos *(VoIP),* pueden cifrar el audio con el protocolo *Secure Real-Time Transport Protocol (SRTP)* que es una réplica del *(RTP),* pero ofrece confidencialidad, autenticación de mensajes y protección, evitando los ataques de interceptación e inserción de audio entre otros y no afecta a la *(QoS),* porque es evidente que el canal de señalización también debe ir completamente cifrado. Se debe utilizar *(VLAN),* para priorizar y proteger el tráfico *(VoIP),* separándolo en canales lógicos de las redes de datos. Con esto se protege y se limita el acceso a la red *(VoIP),* sobre todo desde el exterior, limitar los volúmenes de datos y ráfagas de paquetes, en puntos estratégicos de la red, para evitar gran cantidad de ataques *(DoS).* Y finalmente algunos consejos para protegerse de ataques de enumeración: [1] [14]

- Configurar correctamente los servicios, para que no muestren más información de la necesaria.
- No usar nombres por defecto en los archivos de configuración.
- No usar *(TFTP), (FTP),* porque tampoco son canales seguros. La mejor solución es usar un canal cifrado.
- Desactivar puertos de administración como *(HTTP)* y *(SNMP),* por citar los más comunes.
- Cambiar el password por defecto, de todos los lugares y realizar un cambio cada cierto periodo.

4.19. PROTOCOLOS DE SEGURIDAD.

Los protocolos de seguridad, definen las reglas que gobiernan las comunicaciones, diseñadas para que el sistema pueda soportar ataques de carácter malicioso, protegerse contra todos los ataques posibles, es generalmente muy costoso, por lo cual los protocolos son diseñados bajo ciertas premisas, con respecto a los riesgos a los cuales el sistema está expuesto. [16]

Seguridad de Nivel de	Ventajas	Desventajas	Ejemplos de protocolos
Aplicación	- Se puede extender la aplicación para brindar servicios de seguridad sin tener que depender del SO - Facilita el servicio de no repudio	- Los mecanismos de seguridad deben ser diseñados de forma independiente para cada aplicación - Mayores probabilidades de cometer errores	Kerberos PGP SSH S/MIME SET IPSec (ISAKMP) RADIUS TACACS
Transporte	- En teoría, no se requieren modificaciones por aplicación	- Mantener el contexto del usuario es complicado - TLS requiere que las aplicaciones sean modificadas	SSL (Netscape Corp.) TLS (IETF)
Red	- Disminuye el flujo excesivo de negociación de claves - Las aplicaciones no requieren modificación alguna - Permite crear VPNs e Intranets	- Difícil manejar el no repudio	IPSec (AH, ESP)(IETF) NLSP (ISO) Protocolos de tunneling: PPTP, L2TP
Enlace de datos	- Más rápido	- No son soluciones estables y funcionan bien sólo para enlaces dedicados - Los dispositivos deben estar físicamente conectados	ATMs (IEEE) SILS (IEEE) CHAP PAP MS-CHAP, EAP, LEAP, PEAP

Ilustración 6: Ventajas y Desventajas de los protocolos de seguridad.
Fuente: Antonio Izquierdo Manzanares (2009)

Como un protocolo es el conjunto de programas y actividades programadas, que cumplen con un objetivo específico, el cual es cifrar o encriptar la información, para ello crean túneles entre origen y destino, por donde viaja la información, en la figura 6, se detalla qué tipo de protocolos se puede implementar, en cada capa del modelo *(TCP/IP).* Para

corregir las vulnerabilidades de *(VoIP),* es necesario centrándose únicamente en la capa de transporte y de red, donde se puede manejar mejor la seguridad según las vulnerabilidades enunciadas anteriormente. En los siguientes apartados se llevará a cabo un análisis sobre el protocolo *(SSL/TLS)* e *(IPSec),* debido a la amplia aceptación de ambos por parte de la comunidad científica, y su amplia adopción de ambos, para la protección de los servicios de Internet, como lo es la *(VoIP).* La aprobación de ambos ha sido tal, que la aparición de nuevos dispositivos y sistemas de comunicación, que no podían implementar estos protocolos, ha llevado a la par, el desarrollo de nuevos protocolos que sustituyan a *(SSL/TLS)* o *(IPSec).* [16]

4.19.1. Internet Protocol Security (IPSEC).

La arquitectura de seguridad *(IP), (IPsec),* es una propuesta de *Internet Engineering Task Force (IETF),* para dotar de protección basada en criptografía con alto nivel de seguridad, a la capa de red *(IP),* manteniendo la interoperabilidad entre los dispositivos o equipos que implementen esta arquitectura de seguridad. Al ser una arquitectura de seguridad, está compuesta por múltiples protocolos internos, las especificaciones *(IPSec),* han sido definidas para trabajar en la capa inferior de la pila *(stack),* del protocolo *(TCP/IP),* por lo tanto, funciona a nivel de datagrama, es independiente del resto de protocolos que se encuentran en las capas superiores a *(TCP, UDP...). (IPSec),* es en realidad, un conjunto de estándares para integrar en *(IP),* funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas *(IP),* combinando tecnologías de clave pública *(RSA),* algoritmos de cifrado *(DES, 3DES, IDEA, Blowfish),* algoritmos de hash *(MD5, SHA-1)* y certificados digitales *(X509v3).* Dentro de *(IPSec),* se distinguen los siguientes componentes: [16] [17]

- Authentication Header *(AH).*
- Encapsulating Security Payload *(ESP).*

Proporcionan mecanismos de seguridad para proteger tráfico *(IP).*

- Protocolo de gestión de claves *Internet Key Exchange (IKE)*

Permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión *(AH)* o *(ESP).*

- **Protocolo AH:**

Garantizar la integridad y autenticación de los datagramas *(IP)*.

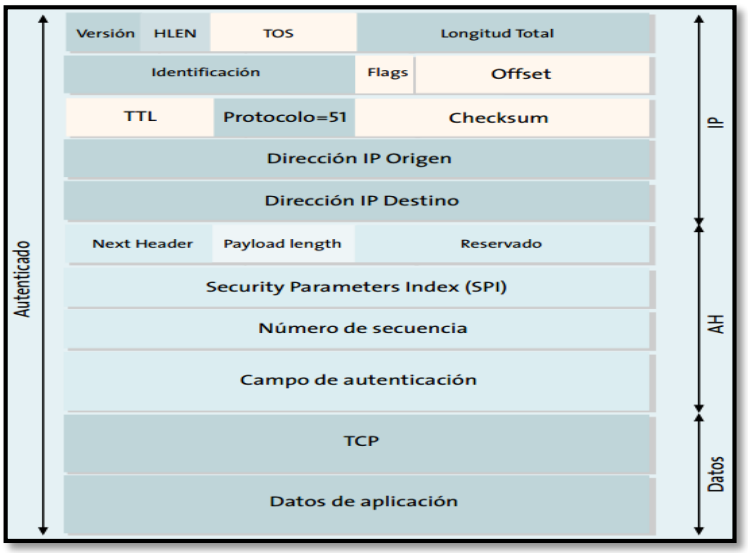


Ilustración 7: Estructura del datagrama (AH).
Fuente: Seguridad en la capa de Red. – IPSec Luis Müller (2011)

Sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros, *(AH)*, es una cabecera de autenticación que se inserta entre la cabecera *(IP)* estándar y los datos transportados, que pueden ser un mensaje *(TCP, UDP o ICMP)*, o incluso un datagrama *(IP)* completo, es importante destacar que *(AH)*, asegura la integridad y autenticidad de los datos transportados y de la cabecera *(IP)*, excepto los campos variables: *(TOS, TTL, flags, offset y checksum).* [16]

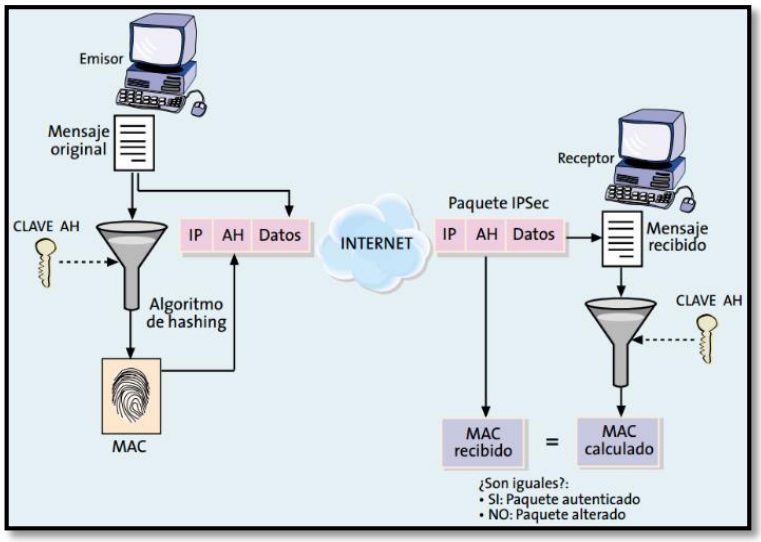


Ilustración 8: Funcionamiento del protocolo (AH).
Fuente: Seguridad en la capa de Red. – IPSec Luis Müller (2011)

El funcionamiento de *(AH)*, se basa en un algoritmo *(HMAC)*, esto es, un código de autenticación de mensajes. En la figura 8 se muestra el modo en que funciona el protocolo *(AH)*. [16] [17]

- **Protocolo ESP**:

  Proporciona confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama *(IP)*.

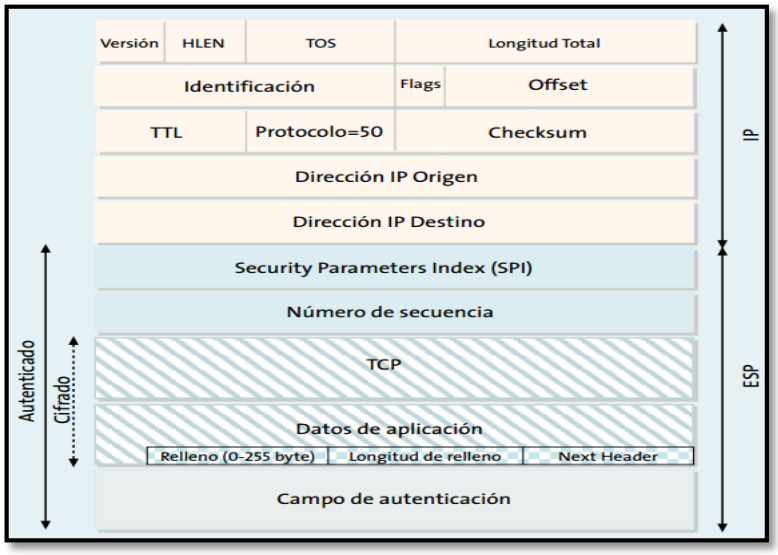


Ilustración 9: Estructura de un datagrama (ESP).
Fuente: Seguridad en la capa de Red. – IPSec Luis Müller (2011)

Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de *(AH)*. Dado que *(ESP)*, proporciona más funciones que *(AH)*, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo *(IP): (TCP, UDP o ICMP, o incluso un paquete IP completo)*. [16] [17]

- **Funcionamiento:** Antes de entrar en los detalles del protocolo *(IKE)*, es necesario explicar los dos modos de funcionamiento que permite *(IPSec)*. Tanto *(ESP)*, como *(AH)*, proporcionan dos modos de uso:

  - **El modo transporte.** En este modo el contenido transportado dentro del datagrama *(AH)* o *(ESP)*, son datos de la capa de transporte *(por ejemplo, datos TCP o UDP)*. Por tanto, la cabecera *(IPSec)*, se inserta inmediatamente a continuación de la cabecera *(IP)* y antes de los datos de los niveles

superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo *(IPSec)*. [16] [17]

- **El modo túnel.** En éste el contenido del datagrama *(AH)* o *(ESP)*, es un datagrama *(IP)* completo, incluida la cabecera *(IP)* original. Así, se toma un datagrama *(IP)*, al cual se añade inicialmente una cabecera *(AH)* o *(ESP)*, posteriormente se añade una nueva cabecera *(IP)* que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones *(IPSec)*. [16] [17]

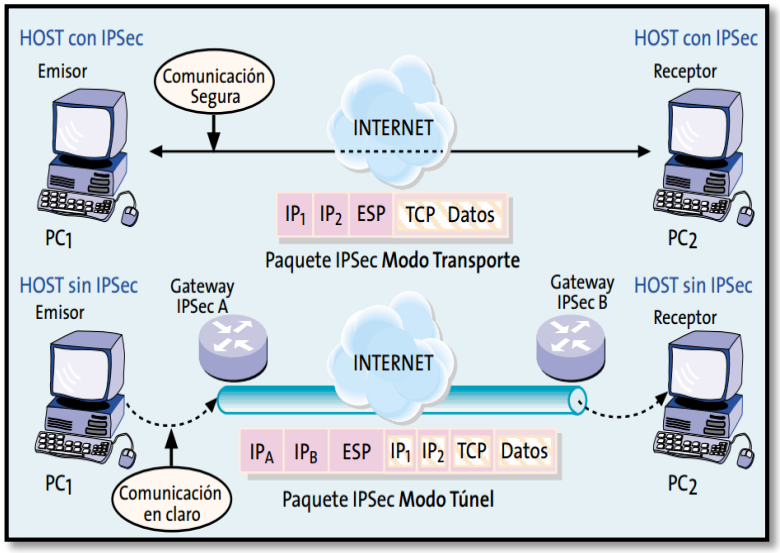


Ilustración 10: Los modos de funcionamiento transporte y túnel de (IPSec).
Seguridad en la capa de Red. – IPSec Luis Müller (2011).

- **Protocolo de control IKE**:

Un concepto esencial en *(IPSec)*, es el de asociación de seguridad *(SA):* es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de *(SA)*. El objetivo principal de *(IKE)*, es de establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad *(IPSec)*. Dicha negociación se lleva a cabo en dos fases:

- La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo *(HMAC)*. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves *Diffie-Hellman*. [16] [17]

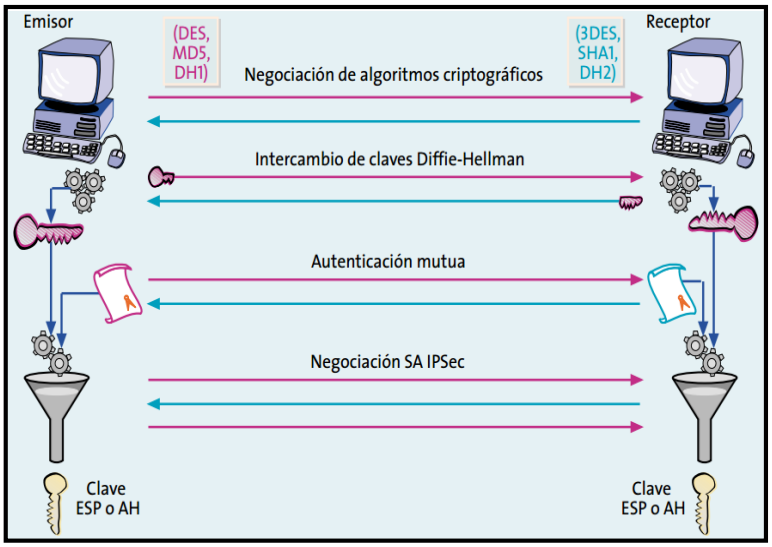


Ilustración 11: Funcionamiento del protocolo (IKE).
Fuente: Seguridad en la capa de Red. – IPSec Luis Müller (2011).

- En la segunda fase el canal seguro *(IKE)*, es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso *(IPSec)*. Durante esta fase se negocian las características de la conexión *(ESP)* o *(AH)* y todos los parámetros necesarios. [16] [17]

4.19.2. Protocolo SSL/TLS.

El protocolo *(SSL)*, fue desarrollado por la compañía *(Netscape Communications)*, luego pasó a encontrarse bajo el control de *(IETF)*, que es el responsable de la evolución del mismo, en la actualidad, se lo ha renombrado como protocolo *(TLS)*, y en el mundo de las telecomunicaciones se lo describe de la siguiente manera *(SSL/TLS)*, se sitúa sobre la capa de transporte de la pila de comunicaciones, más concretamente sobre el protocolo *(TCP)*. Una de sus características principales es que al introducirse en la pila de protocolos, lo hace de forma transparente, a las capas inmediatamente superior e inferior, de forma que no es necesario realizar ninguna modificación al protocolo *(TCP)*, porque utiliza los mecanismos de comunicación que ofrece *(TCP)*, en concreto, los *sockets*, tampoco realiza modificaciones a la capa de aplicación, porque esta podría hacer uso de

los *sockets* seguros de *(SSL/TLS)*, prácticamente de igual forma que utilizaba los *sockets* de *(TCP)*. *(SSL/TLS)*, crea una capa adicional en la pila de comunicaciones que permite a las aplicaciones supervisen sus comunicaciones, sin tener que realizar modificaciones importantes en su código. *(SSL/TLS)*, Está compuesto por dos capas: [16] [17]

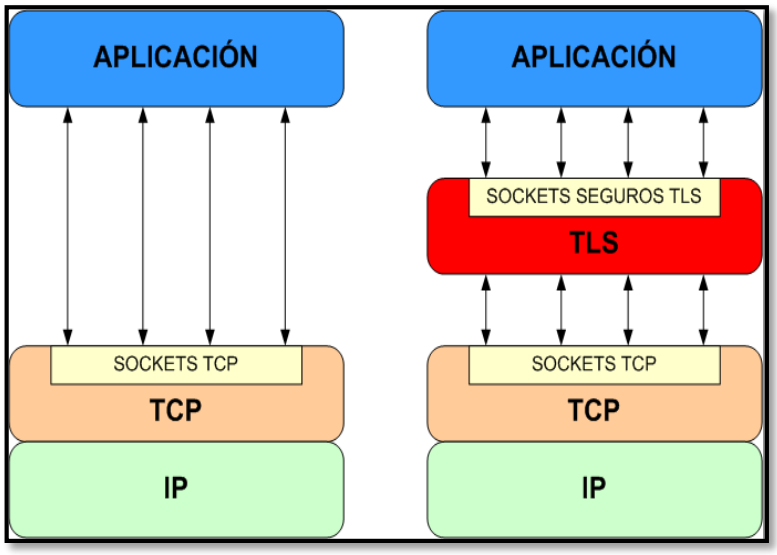


Ilustración 12: Aplicación del protocolo (TLS), en la pila (TCP/IP).
Fuente: Antonio Izquierdo Manzanares (2009).

- **Capa 1. Protocolo de registro (Record Protocol).**

Toma los mensajes en las capas superiores a *(SSL/TLS)*, o la capa de aplicación de *(TCP)*, que desean enviar y los fragmenta en bloques del tamaño adecuado, comprimiendo los mecanismos de confidencialidad y autenticidad necesarios, finalmente los transmite a las capas inferiores de la pila de comunicaciones, es decir, encapsula los protocolos de nivel más alto y construye el canal de comunicaciones seguro, tal como se muestra en la siguiente imagen: [16] [17]

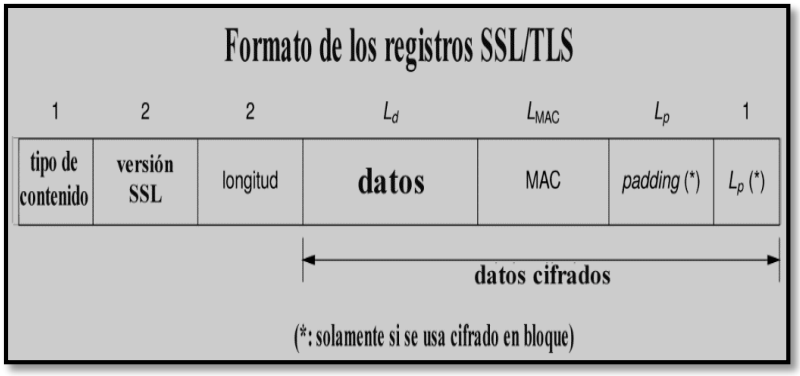


Ilustración 13: Estructura del datagrama de registro (SSL/TLS).
Fuente: Protección del nivel de transporte: SSL/TLS/WTLS José María Morales Vázquez (2011).

- El primer campo indica cual es el tipo de contenido de los datos.
    - Un mensaje del protocolo de negociación,
    - Una notificación de cambio de cifrado,
    - Un mensaje de error, o datos de aplicación.
- El segundo campo son dos bytes que indican la versión del protocolo: si son iguales a 3 y 0 el protocolo es *(SSL 3.0)* y si son iguales a *3* y *1* el protocolo es *(TLS 1.0).*
- El tercer campo indica la longitud del resto del registro, por tanto, es igual a la suma de *(Ld)* y *(LMAC)* y, si los datos están cifrados con un algoritmo en bloque, *(Lp +1).*
- El cuarto campo son los datos, comprimidos si se ha acordado algún algoritmo de compresión.
- El quinto campo es el código de autenticación *(MAC),* en el cálculo de este *(MAC),* intervienen la clave *(MAC),* un número de secuencia implícito de 64 bits *(que se incrementa en cada registro pero no se incluye en ningún campo)* y, naturalmente, el contenido del registro. La longitud de este campo depende del algoritmo de *(MAC)* que se haya acordado utilizar.

- **Capa 2. Protocolo de negociación: (*handshake protocols*).**

También llamado protocolo de encajada de manos, tiene por finalidad autenticar el cliente y/o el servidor, y acordar los algoritmos y claves que se utilizaran de forma segura, garantizando la confidencialidad y la integridad de la negociación, está compuesto los protocolos utilizados en esta fase son los siguientes: [16] [17]

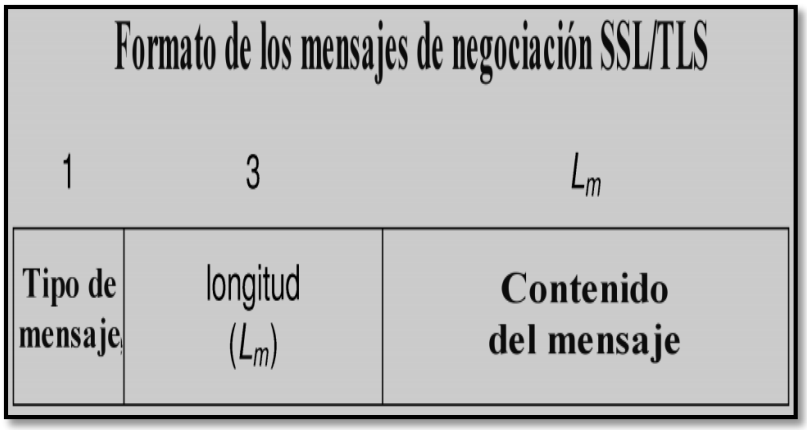


Ilustración 14: Estructura de un datagrama de Handshake protocol (SSL/TLS).
Fuente: Protección del nivel de transporte: SSL/TLS/WTLS José María Morales Vázquez (2011).

- *Handshake protocol* se encarga de gestionar la negociación de los algoritmos de cifrado, y la autenticación entre el cliente y el servidor.

- *Assert Protocol* señaliza errores y problemas en la sesión establecida.

- *Change Cipher Espec Protocol* consiste en un solo mensaje de *1* byte que sirve para notificar cambios en la estrategia de cifrado

- **Funcionamiento**

  - El cliente al hacer la conexión informa sobre los sistemas criptográficos que tiene disponibles, y el servidor responde con un identificador de la conexión, su clave certificada e información sobre los sistemas criptográficos que soporta.

Ilustración 15: Estructura de negociación entre cliente y servidor del protocolo (SSL/TLS).
Fuente: Protección del nivel de transporte: SSL/TLS/WTLS José María Morales Vázquez (2011).

  - El cliente deberá elegir un sistema criptográfico, verificará la clave pública del servidor. Entonces se genera una clave cifrada con la clave del servidor.

- Este es uno de los puntos importantes del protocolo SSL, porque si alguien pudiese descifrar la información, sólo conseguiría romper esa conexión, y una conexión posterior requeriría una clave criptográfica diferente.

- Una vez finalizado este proceso, los protocolos toman el control de nivel de aplicación, de modo que *(SSL)* nos asegura que:

    - Los mensajes que enviamos o recibimos no han sido modificados.
    - Efectivamente recibe la información quien debe recibirla.
    - Ninguna persona sin autorización puede leer la información transmitida.

Cuando existe autenticación de al menos una de las partes, el túnel criptográfico es resistente a ataques de *man-in-the-middle (MitM),* porque para autenticarse, cada entidad debe presentar una cadena de certificados, que conduzca a una *Certification Authority (AC),* aceptada por la otra parte, utiliza los servicios de una infraestructura de clave pública; mediante el uso de las suites criptográficas que se negocian. [16] [17]

5. MATERIALES Y MÉTODOS.

En esta sección, se da a conocer los métodos, técnicas y metodologías necesarios para la construcción de esta investigación, porque a través de ellas, se recolectó información relevante para realizar un proceso investigativo fructífero y eficiente, y de esta forma cumplir con éxito los objetivos planteados al comienzo de esta investigación.

5.1.MÉTODOS DE INVESTIGACIÓN.

En este apartado, se describe los métodos teóricos-practicos que se utiliza en la investigación, los cuales ayudan a obtener información teórica y deducir la misma:

- **Científico:** Este método permite buscar información en libros, revistas, artículos científicos e Internet, lo que da lugar a detectar los problemas fundamentales, para lograr esta investigación, porque a través de estos se transmite las posibles soluciones del caso.

- **Analítico:** Este método es aplicado durante la etapa de análisis donde se recopiló la información necesaria, para tener una idea clara, de lo que se va a realizar durante la investigación, es decir, se puntualiza que es lo que se debe hacer y cómo se debe hacerlo.

- **Experimental:** Este método consiste en provocar voluntariamente una situación que se requiere estudiar, para modificar o alterna, es decir, se realiza ambientes de simulación, para realizar los test necesarios, para determinar vulnerabilidades y los ataques a la que está expuesta la red de *(VoIP),* del Hospital Isidro Ayora de Loja.

5.2. TÉCNICAS DE INVESTIGACIÓN.

Para efectuar una investigación eficiente, se requiere de una selección adecuada del tema u objeto de estudio, sumado a esto se requiere de técnicas y herramientas que auxilien al investigador, en la realización de su estudio, a continuación se detalla cada una de las técnicas utilizadas, para acceder a información real y necesaria, para la construcción del presente proyecto de investigación:

- **Entrevista:** A través de ellas se realizan diálogos con el administrador de la Gestión Informática del Hospital, con la finalidad de obtener la información de la problemática actual, así como la de la administración de la red de datos, la cual involucra la red de *(VoIP),* y la seguridad de la misma ***(ver anexo A).***

- **Observación Directa:** Por medio de esta se puede conocer de forma real, las instalaciones e infraestructura, es decir, se conoce el equipo que se utiliza para brindar los servicios de voz, además se conoce como está la distribución y topología de la red de *(VoIP),* existente en el Hospital Isidro Ayora de Loja, de la misma forma, se constata procedimientos y normas de seguridad que se aplican en la dicha institución.

- **Consulta a Expertos:** Como el objetivo de esta investigación, es implementar un servicio eficiente en la seguridad de la red *(VoIP),* con el fin de salvaguardar los datos que se genera dentro del Hospital, se busca información valedera de entes confiables y conocedoras de esta tecnología, con la vasta experiencia en el área laboral, cuyas referencias dan un plus de calidad a la presente investigación**.**

5.3. METODOLOGÍAS

En todo proceso investigativo, es necesario apoyarse en metodologías que guíen y respalden los procesos que se llevan a cabo, razón por la cual, se detallan las metodologías idóneas para esta investigación, por ser las más acordes y que cubren los puntos necesarios para dar cumplimiento a los objetivos de la investigación.

5.3.1. Metodología OSSTMM.

Es uno de los estándares profesionales, más completos y comúnmente utilizados en auditorías de seguridad, para revisar la seguridad de los sistemas de Internet, al utilizar esta metodología, el investigador sabe (***Que*** *se debe de probar,* ***Como*** *se puede hacer y* ***Cuando*** *es necesario ejecutarlo). OSSTMM****,*** permiten identificar claramente el alcance de cada una de las siguientes actividades: [11]

- **Búsqueda de Vulnerabilidades:** Orientado principalmente a realizar comprobaciones automáticas, de un sistema o sistemas dentro de una red.

- **Escaneo de la Seguridad:** Orientado a búsquedas de vulnerabilidades en el sistema, identificación de puntos débiles del sistemas y análisis individualizado.

- **Test de Intrusión:** Se plantean test de pruebas que se centran en romper la seguridad de un sistema determinado.

- **Evaluación de Riesgo:** Se refiere a los análisis de seguridad, a través de entrevistas e investigación de nivel.

- **Auditoría de Seguridad:** Continua inspección a los sistemas, por parte de los administradores que controlan, el cumplimiento de las políticas de seguridad definidas.

- **Hacking Ético:** Obtener objetivos complejos, dentro de la red de sistemas, a partir de los test de intrusión.

Mapa de seguridad

La siguiente imagen, está compuesta por seis secciones, las cuales constan de varios módulos y en cada módulo, se indica una serie de tareas o pruebas a realizar, el orden en que se desarrolla cada módulo, dependerá de la visión del autor, debido a que, cada sección es independiente de las otras. Estas secciones están en constante evolución y actualmente se compone de un sinnúmero de fases orientadas a la seguridad, las cuales se prescriben con mayor detalle en el ***(anexo 4).*** [11]

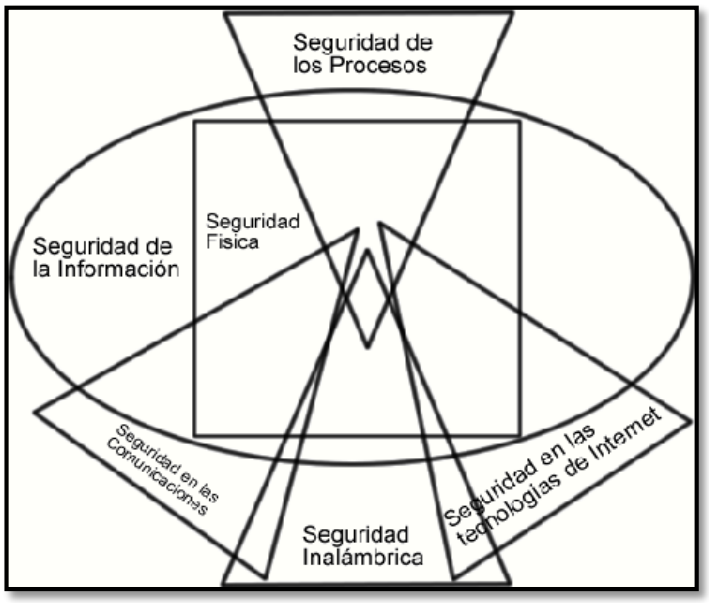


Ilustración 16: Mapa de seguridad de la metodología (OSSTMM).
Fuente: INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES Pete Herzog (2000)

5.3.2. Metodología OCTAVE.

Es una metodología de análisis de riesgos, desarrollada por la Universidad Carnegie Mellon, en el año 2001, está enfocada en tres principios como son: *confidencialidad, integridad y disponibilidad.*

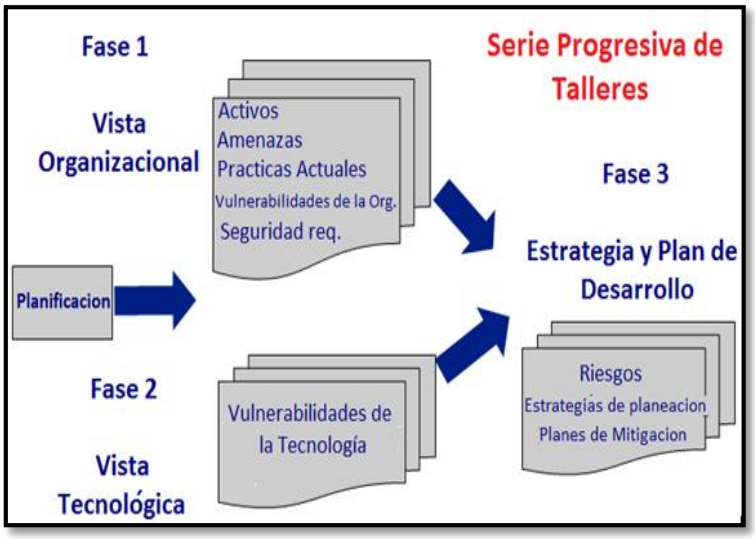


Ilustración 17: Proceso de (OCTAVE).
Fuente: Software Engineers Institute, Carnegie Mellon University (2001)

Para ello utiliza un enfoque de tres fases, para examinar la organización y la tecnología, con el fin de extraer una imagen completa de la información y necesidades de la organización, cada fase consta de varios procesos que se resumen a continuación. [18]

- **Fase 1: Construir los activos basados en perfiles de amenazas.**

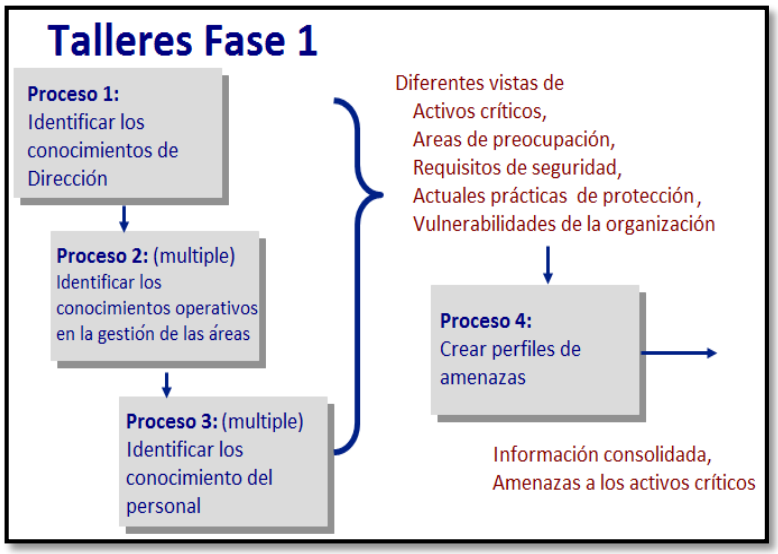


Ilustración 18: Procesos de la Fase 1 de (OCTAVE).
Fuente: Software Engineers Institute, Carnegie Mellon University (2001)

En esta fase, se realiza la recopilación de información de los distintos niveles de la organización, así mismo, se determina que activos, son más importantes para la institución *(activos críticos)* y que se está haciendo actualmente, para proteger esos activos, en la siguiente figura, se detalla cada uno de los procesos pertenecientes a esta fase. [18]

- **Fase 2: Identificar las vulnerabilidades de la infraestructura.**

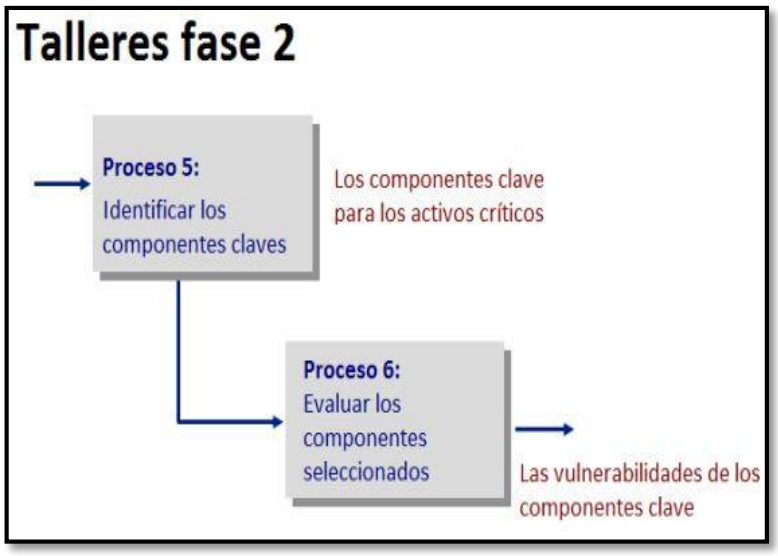


Ilustración 19: Procesos de la Fase 2 de (OCTAVE).
Fuente: Software Engineers Institute, Carnegie Mellon University (2001)

- Se trata de una evaluación, a la infraestructura de información, el equipo de análisis, examina los principales componentes operacionales y sus debilidades *(vulnerabilidades tecnológicas)* que dar lugar a una acción no autorizada contra los activos críticos. [18]

- **Fase 3: Estrategia y plan de desarrollo.**

  Es la planificación, de las medidas y reducción de los riesgos, las cuales se clasifican en los siguientes elementos:

  - Evaluación de los riesgos
  - Estrategia de protección
  - Ponderación de los riesgos

- Plano de reducción de los riesgos.

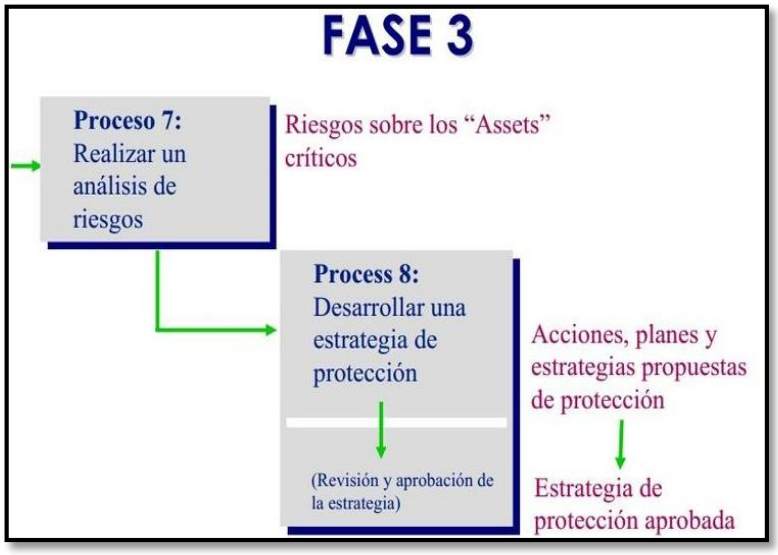


Ilustración 20: Procesos de la Fase 3 de OCTAVE.
Fuente: Software Engineers Institute, Carnegie Mellon University (2001)

5.4. DESARROLLO DE LAS METODOLOGÍAS EN CUESTION.

La Metodología *(OCTAVE)*, ha permitido desarrollar el análisis de riesgo, a través de la identificación de los activos de la infraestructura de red, sus amenazas y el desarrollo del proceso de evaluación de vulnerabilidades, en la estructura tecnológica mediante la metodología *(OSSTMM)*.

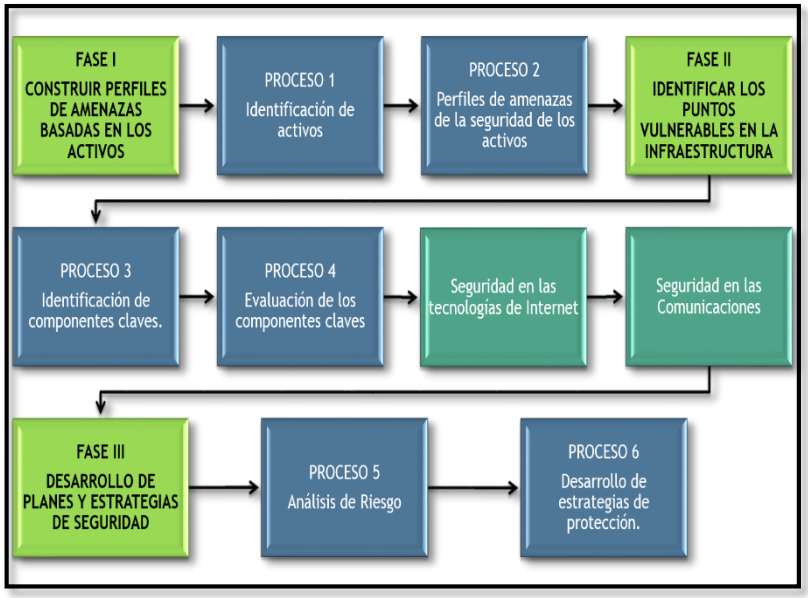


Ilustración 21: Diagrama de procesos seleccionados de (OCTAVE) y (OSSTMM).
Fuente: El Autor (2015).

En la figura 21, se muestran los procesos que se realizaran en base a las dos metodologías, se han omitido los procesos 1 y 2, de la metodología *(OCTAVE),* debido a que la información de los activos es proporcionada por el personal del departamento de *(TIC)* del Hospital, lo cual corresponde al proceso 3 de la metodología. Las secciones de la metodología *(OSSTMM),* seleccionadas no incluyen aquellas para las que no se posee información de entrada, considerando los módulos y pruebas necesarias, para la evaluación de los componentes clave de la red. Las secciones de la metodología *(OSSTMM),* se han unificado como parte del proceso 4, debido a que constituyen las pruebas de seguridad sobre los componentes clave. [11]

Una vez puntualizado, la descripción de las metodologías que se va a utilizar, es necesario señalar que y como, se va a realizar el proceso, para dar cumplimiento a cada una de las fases. A continuación se describe los pasos que se va a llevar a cabo, tanto en la metodología ***(OSSTMM)*** como ***(OCTAVE)****:*

- **La metodología *(OCTAVE)* está diseñada para el análisis y gestión de riesgo lo cual permitió:**
    - Estudiar el perfil actual de la red de Datos, del Hospital Isidro Ayora de Loja.
    - Determinar los activos importantes a evaluar.
    - Determinar los perfiles de amenaza para cada activo.
    - Realizar la valoración de riesgos de las vulnerabilidades encontradas.
    - Desarrollar una estrategia de protección para las vulnerabilidades encontradas.
- **La metodología *(OSSTMM)* está diseñada para el análisis de vulnerabilidades en la red de datos lo cual permitió:**

- Investigar las herramientas necesarias para llevar a cabo los procesos de evaluación definidos.

- Investigar los posibles ataques y vulnerabilidades a los que están expuestos los equipos de red.

- Realizar simulaciones de ataques a la red para determinar las vulnerabilidades de la misma

- Realizar un estudio de protocolos de seguridad que se pueden implementar, para proteger la red de *(VoIP),* frente a las vulnerabilidades encontradas.

- Implementar el o los protocolos de seguridad, idóneos, para cifrar la información, que se transmite por la red de *(VoIP),* de la Institución.

- Realizar una simulación de ataques a la red, con el fin de comprobar que la implementación de la seguridad, sea la correcta, y que no afecte a la operatividad de la red.

6. RESULTADOS.

En la presente sección, se realiza un análisis de la situación actual, de la red de *(VoIP),* del Hospital Isidro Ayora, donde se detalla la estructura organizacional, procesos, políticas, y medidas de seguridad que actualmente se manejan en la Institución, de la misma forma, se da un detalle de toda la infraestructura, es decir, se da a conocer todos los equipos que se encuentran en funcionamiento de la red *(VoIP),* se realiza un detalle de la topología y distribución de la red, donde se expone el direccionamiento de *(VLANs)* y la distribución de usuarios de la *(PBX).*

6.1. ANTECEDENTES DEL HOSPITAL ISIDRO AYORA.

El Hospital Provincial General Isidro Ayora de Loja, es una institución pública, sin fines de lucro, la cual presta sus servicios en el campo de la salud humana, a nivel local, provincial, nacional e internacional. Está ubicado en el casco céntrico de la ciudad de Loja, mismo que fue puesto a beneficio de la comunidad el 2 de Agosto de 1979, lleva su nombre en honor al ilustre Lojano y Ex presidente de la República Dr. Isidro Ramón Ayora Cueva.

Ilustración 22: Hospital Regional Isidro Ayora de Loja
Fuente: Departamento de (TIC), del Hospital Isidro Ayora de Loja (2015).

El Hospital Isidro Ayora, cuenta con los siguientes servicios: cirugía general, gineco obstetricia, medicina interna, pediatría, servicio de emergencia, consulta externa, odontología, fisiatría, además cuenta con dos unidades de hemodiálisis y quemados, así mismo, tiene el servicio de hospitalización y cuidados intensivos, laboratorio,

imagenología, entre otros. Cuenta con el servicios de carácter ambulatorio, para servir a la comunidad en las áreas de consulta externa, urgencias, servicios de diagnóstico y tratamiento, etc.

6.1.1. Estructura organizacional de procesos.

El Hospital Isidro Ayora, cuenta con la siguiente infraestructura organizacional, la cual es establecida por el Ministerio de Salud Pública del Ecuador.

Ilustración 23: Estructura de procesos del Hospital Isidro Ayora.
Fuente: Departamento de (TIC), del Hospital Isidro Ayora de Loja (2015).

En la figura anterior, se muestra como se establece la jerarquía de la institución, cuyo objetivo es brindar servicios de salud, para lo cual requieren el apoyo de actividades principales como:

- **Gestión Hospitalaria:** Contribuye la atención al paciente, en las diferentes áreas del Hospital, apoyándose en sistemas de gestión hospitalaria.

- **Gestión Financiera:** Involucra las actividades económicas de la Institución, apoyándose en sistemas de información, como el sistema de recaudación para la administración de caja.

- **Servicios Técnicos Complementarios:** Comprende el personal y el servicio de mantenimiento que dan soporte a la infraestructura de la Institución.

Estas actividades, se apoyan en tecnologías, tanto de equipos de atención médica, como de los sistemas de información. Los componentes claves de esta estructura, son los recursos humanos que desarrollan las actividades y la infraestructura de las *Information Technology (TI)*, mismas que comprenden lo siguiente: *(PC)*, de usuarios y tecnologías de comunicación, siendo el valor agregado al objetivo de la institución, por ser los medios e instrumentos de comunicación entre los distintos procesos.

6.1.2. Estructura jerárquica del Hospital Isidro Ayora de Loja

En la siguiente imagen, se resume la estructura jerárquica del Hospital Isidro Ayora.

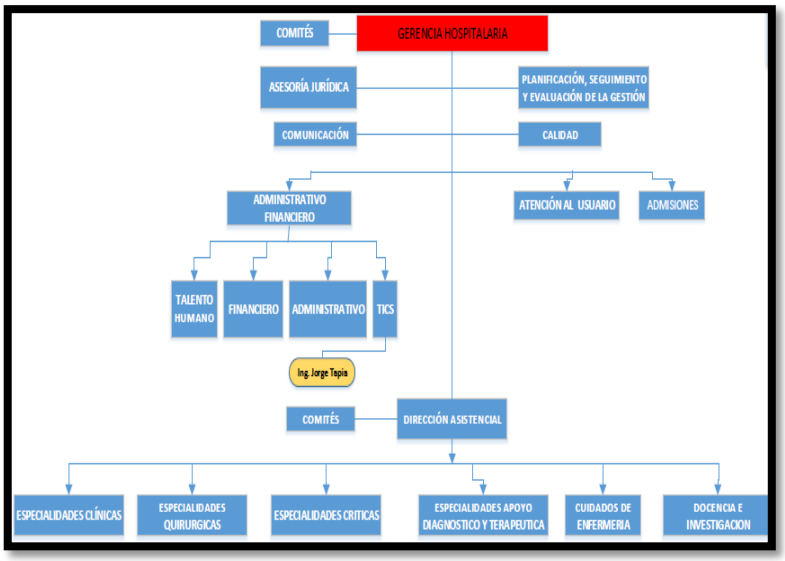


Ilustración 24: Estructura Jerárquica del Hospital Isidro Ayora.
Fuente: Departamento de (TIC), del Hospital Isidro Ayora de Loja (2015).

6.2. DISEÑO ACTUAL DE LA RED DE DATOS.

La descripción del perfil actual, se basa en la esquematización de la información obtenida, mediante la observación directa, la documentación existente del diseño de la red y la configuración de los equipos; la red está conformada por equipos de *networking*, como un *router Internet Service Provider (ISP), firewall, switch* de capa 2 y 3, equipos terminales como *servidores, estaciones de trabajo* y *teléfonos*.

6.2.1. Equipos que se administran en la red de datos.

A continuación, se describen los equipos y dispositivos de *networking*, utilizados, para la administración y comunicación de la red, además se han considerado los equipos que están fuera de uso, porque la red está sujeta a constantes cambios, ya sea por

remodelaciones físicas en la institución o reestructuración del diseño de la red, por ende, estos equipos están a la espera de asignación de algún servicio.

- **Ruteadores y switch.**

  En la siguiente tabla, se muestran las características de los equipos de red.

Tabla 10: Lista de Routers y Switch del Hospital Isidro Ayora de Loja.

#	EQUIPO	CARACTERÍSTICAS	FUNCIÓN
3	Switch	✓ **Comunicación: 3.2** Gbps. ✓ **Ancho de banda: 1.6** Gbps. ✓ **Envió de paquetes:** 3 millones de paquetes por segundo. ✓ **Memoria:** 8mb de dram y 4 Mb de memoria flash. ✓ **Direcciones Mac:** 2048. ✓ **Standard:** dúplex completo IEEE 802.3x en puertos 10baset y 100baset. ✓ **Puertos:** puertos para conectores RJ 45 y un puerto de consola.	Distribución Y acceso.
2.	Switch	✓ **Ancho de banda:** 8.8 Gbps. ✓ **Envío de paquetes: 6.5** millones de paquetes por segundo. ✓ **Direcciones Mac:** 8000. ✓ **Apilamiento:** 8 unidades de switch, o 384 puertos 10/100. ✓ **Estándar:** 802.1x **servidor de aplicaciones**. ✓ **Puertos:** 24 puertos 10base t/100base-tx con auto negociación mdi/mdix 2 pares de puertos gigabit de uso dual: para rj45 ✓ **Seguridad:** Radius rada (acceso a dispositivo autenticado mediante radius) control de puertos ACL soporte de secure shell (sshv2) y snmpv3. ✓ **Capa 2:** VLAN basadas en puertos (802.1q).	Core.
1.	Switch	✓ **Conmutación:** 5.2 Gbps, velocidad hasta 3.9 Mbps. X3430 (2.40 GHz). ✓ **Puertos:** 26 puertos disponibles en total que consisten en: 24 puertos 10base-t/100base-tx, 2 puertos 10/100/1000 o sfp, puerto de consola rj45. ✓ **Capa 2:** soporte de VLAN IEEE 802.1q. ✓ **Seguridad:** login de red IEEE 802.1x autenticación de servidor radius, rada.	Distribución.
1.	Router	✓ **Comunicación:** entre 50 y 70 kbps. X3430 (2.40GHz). ✓ **Memoria flash: 8** Mb ampliables a 32 Mb. ✓ **Memoria del sistema:** 16 Mb dram ampliables a 128 Mb. ✓ **Ranuras para módulos de red:** 4.	De borde *(ISP).*
1.	Switch	✓ **Puertos:** 8 puertos 10/100base- tx. Soporte de auto mdi mdi-x en todos los puertos. ✓ **Control de flujo:** 802.3x en cada puerto. Plug & play no requiere configuración.	Distribución.
1.	Switch.	✓ **Puertos: 24** puertos 10/100 Mbps p/rack. ✓ **Estándares: IEEE** 802.3, 802.3u, 802.3x. ✓ **Velocidad:** 10/100 m (1000m) auto Sensing. ✓ **Memoria:** 1.5mb ✓ **Tipo de procesamiento:** store and forward, full/Half Duplex, non-Blocking Flow control.	Distribución.

Fuente: Departamento de TIC del Hospital Isidro Ayora de Loja (2015).

- **Servidores.**

Los servidores que posee el Hospital Isidro Ayora, corresponden al sistema de información y servicio de *(VoIP),* que se encuentran instaladas, las bases de datos y sistemas de: estadística, recaudación, sistema de recursos humanos, entre otros.
Cabe recalcar que ciertas máquinas, trabajan con sistemas operativos de *Microsoft (Windows),* mismas que carecen de licencias, lo que de antemano se considera una vulnerabilidad, ante la falta de soporte y la correcta utilización del sistema. En la siguiente tabla, se describen las características más relevantes, de los principales servidores de la institución.

Tabla 11: Servidores de la red de datos del Hospital Isidro Ayora de Loja.

SERVIDOR	CARACTERÍSTICAS	FUNCION	LICENCIA
IBM	✓ **MEMORIA:** 785.944KB 4 discos IBM SCSI 10GB Adaptador PCI IBM10/100 Ethernet IBM 10/100 Netfity ✓ **S.O: Windows**	Servidor de seguridad.	**NO**
HP	✓ **PROCESADOR:** Core 2 Quad Intel Xeon 5450 (3.0GHz). ✓ **MEMORIA:** 12 MB. ✓ **ALMACENAMIENTO:** 2 discos 146 GB 10K SAS 2.5. ✓ **RED:** E400/512MB RAID ✓ **S.O:** Windows Server 2008 SPD.	Servidor de Aplicaciones.	**NO**
HP	✓ **PROCESADOR:** Quad Core Intel Xeon X3430 (2.40 GHz). ✓ **MEMORIA:** 2 GB expansible a 8 GB DDR3. ✓ **ALMACENAMIENTO:** Disco de 500 GB SATA. ✓ **RED:** Controladora Ethernet CbE. ✓ **S.O:** Linux.	Servidor de Voz.	**LIBRE**

Fuente: Departamento de TIC del Hospital Isidro Ayora de Loja (2015).

- **Estaciones de trabajo.**

Según el inventario de activos en entidad, actualmente cuenta con 135 computadores hábiles, con arquitecturas diferentes como: *(Pentium, Celeron, Dual Core, Core2 Duo, Core2 Quad, Intel, entre otras).* Así mismo, existen alrededor de 4 impresoras compartidas, en la red de datos, identificadas con una dirección *(IP)* que corresponde a la subred de los equipos, que se encuentran ubicadas en la unidad de gestión informática, gestión financiera, dirección y recursos humanos, respectivamente. Esta información fue proporcionada, por el administrador del departamento de *(TIC).*

- **Teléfonos (VoIP).**

La red cuenta con 91 teléfonos *(IP)*, distribuidos en las distintas dependencias del Hospital y que se asignan a la subred de voz, se debe mencionar que algunos de ellos no están en funcionamiento. De la misma forma, se da a conocer que el departamento de *(TIC)*, carece de documentación detallada, sobre el diseño de la red, políticas de seguridad y planificación de trabajo, así como la configuración de los equipos terminales de la red. En la siguiente tabla, se detalla el número de extensión que le corresponde a cada oficina, donde se encuentra establecido un equipo terminal *(teléfono)* para la comunicación.

Tabla 12: Lista de extensiones de la (IP-PBX) del Hospital.

DEP.	EXT	DEP.	EXT	DEP.	EXT	DEP.	EXT
Activo fijos	7230	Gestión Administrativa Coordinación	7233	Mantenimiento bodega	7250	Consultorio oftalmología 2	7279
Activo fijos delegación	7225	Gestión Administrativa Secretaria	7232	Mantenimiento calderos	7243	Consultorio traumatología	7214
Asesoría jurídica asistencia	7221	Gestión de calidad y acreditación	7284	Mantenimiento coordinación	7216	Compras públicas adquisiciones	7208
Asesoría jurídica coordinación	7217	Gestión Documental	7211	Mantenimiento secretaria	7215	Compras públicas coordinación	7206
Audiometría	7274	Estación de enfermería	7246	Medicina física y rehabilitación (fisiatría)	7271	Compras públicas secretaria	7207
Bodega general de coordinación	7249	Gestión financiera coordinación	7213	Medicina interna estación de enfermería	7265	Dirección administrativa y financiera	7278
Bodega general secretaria	7248	Gestión financiera secretaria	7228	Neonatología estación de enfermería	7256	Dirección secretaría	7210
Caseta principal	7281	Estación social	7226	Nutrición y dietética coordinación	7264	Dispensario anexo al IESS	7222
Central esterilización	7259	Gineco obstétrico estación de enfermería	7234	Odontología	7297	Docencia e Investigación	7292
Central telefónica	7231	Gineco obstétrico secretaria	7238	Operadora	9	Hemodiálisis estación enfermería	7262
Centro obstétrico estación de enfermería	7224	Imagenologica agendamiento de turnos	7269	Ortesis y prótesis coordinación	7219	Unidad de quemados estación de enfermería	7282
Centro quirúrgico	7261	Imagenología sala de ecos	7272	Pediatría estación de enfermería	7258	Unidad de salud mental	7287
Cirugía estación de enfermería	7275	Imagenología secretaria	7270	Sala de primera acogida	7266	Emergencia	7254
Clínica del VIH	7257	Laboratorio clínico exámenes	7283	Salud mental coordinación	7280	Facturación de la RIPS y SOAT	7227
Comunicación imagen y prensa	7235	Laboratorio clínico secretaria	7253	Salud ocupacional	7223	Gerencia secretaria	7204

Consulta externa	7218	Laboratorio clínico SMT	7251	Talento humano asistente	7209	Electroencefalogramas	7277
Consulta externa cardiología	7296	Laboratorio de patología	7240	Talento humano coordinación	7299	Gestión financiera Adm. Caja secretaria	7242
Consulta externa trabajo social	7286	Estadística archivo	7236	Taller de Ortesis y Prótesis	7220	Farmacia coordinación (medican. E Insumos)	7298
Consultorio cardiología	7267	Estadística coordinación	7244	Tics	7200	Emergencia 2	7285
Consultorio oftalmología 1	7273	Estadística datos	7241	Transporte y servicios	7294	Endoscopia	7276
Gestión financiera Administración de caja	7229	Estadística referencia/contra referencia	7237	UCI estación de enfermería	7239		

Fuente: Departamento de TIC del Hospital Isidro Ayora de Loja (2015).

6.2.2. Diseño de la estructura de red.

La red cuenta con un modelo jerárquico, donde se establece las *Access Control List (ACL)*, y las *(VLAN)*, así como los módulos del **core** y los **servidores**, es decir, su núcleo y los principales equipos, están diseñados en una topología en estrella, que posee un cableado estructurado *Unshielded Twisted Pair (UTP)*, categoría 5e, con un aproximado de 200 puntos de red, de los cuales, 106 son destinados a los puntos de la red de datos y 96 para puntos de voz, además, cuenta con cableado *(UTP)*, categoría 6, con 48 puntos de red, en el área de neonatología del Hospital.

6.2.2.1.Bloque de campo.

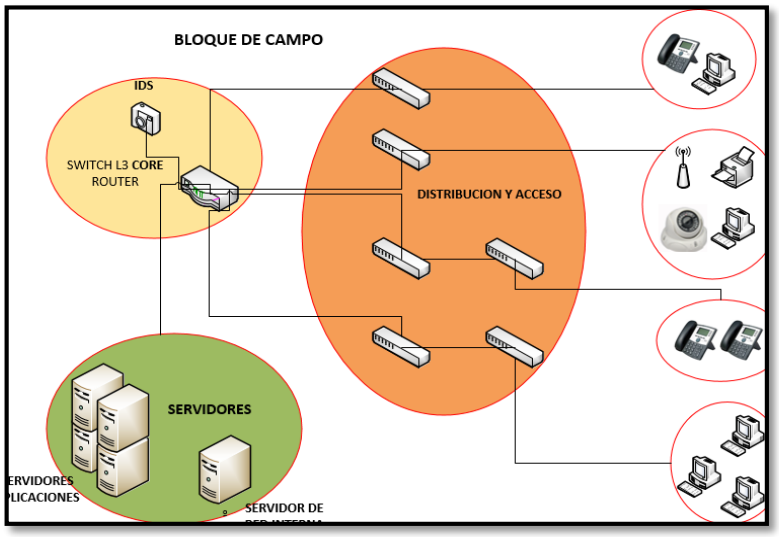


Ilustración 25: Bloque de campo de la red de datos del Hospital Isidro Ayora de Loja
Fuente: El Autor (2015).

En este bloque, se encuentra la infraestructura de la red, distribuida en módulos de manera jerárquica, contiene un switch de capa tres, el cual contiene las interfaces virtuales de las *(VLAN)*, tal como se muestra en la figura anterior:

- **Módulo core.**

El objetivo del módulo core, es enrutar y conmutar el tráfico, lo más rápido posible de una red a otra, es decir conectar el bloque del perímetro con la red de campo.

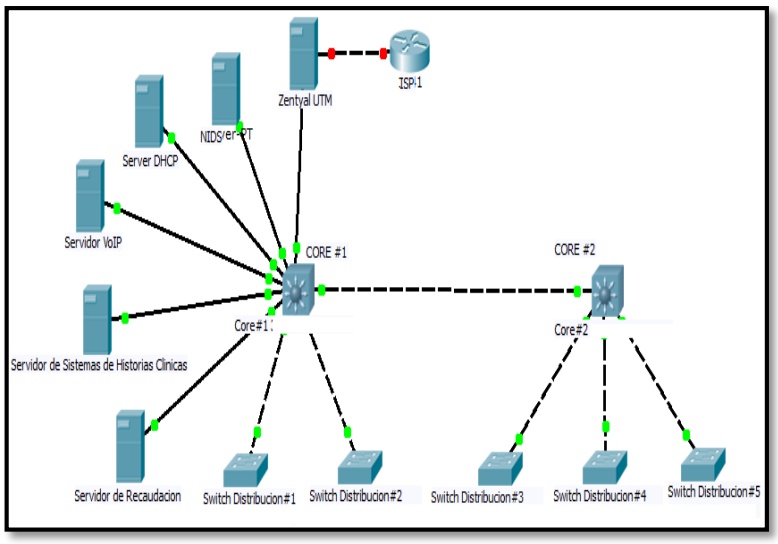


Ilustración 26: Esquema del módulo core de la red de datos del Hospital.
Fuente: El Autor (2015).

En el módulo **core**, se encuentran dos switch de capa 3, los cuales, proporcionan las funcionalidades de acceso y la seguridad necesaria entre las subredes, en estos equipos están instaladas 4 interfaces, donde se alojan los puntos de acceso inalámbrico, mismos que cuentan con *(IP)*, estáticas en la *(VLAN)*, de acuerdo a los usuarios. En la siguiente tabla, se detalla la distribución de *(VLAN)* del *switch core*, cabe mencionar que por cuestiones de seguridad, no se presenta las direcciones *(IP)*, completas.

Tabla 13: Distribución de VLANs en el Switch Core.

DISPOSITIVO	INTERFAZ	DESCRIPCIÓN	RED	DIRECCIÓN IP	MÁSCARA
Switch core1	VLAN xxx	Nativa	--	--	--
	VLAN xxx	Internet	192.x.x.x	192.x.x.x	255.x.x.x
	VLAN xxx	Administrativos	10.x.x.x	10.x.x.x	255.x.x.x
	VLAN xxx	Administración	10.x.x.x	10.x.x.x	255.x.x.x
	VLAN xxx	Servidores	10.x.x.x	10.x.x.x	255.x.x.x
Switch Core2	VLAN xxx	Voz	10.x.x.x	10.x.x.x	255.x.x.x
	VLAN xxx	Médicos	10.x.x.x	10.x.x.x	255.x.x.x
	VLAN xxx	Operativos	10.x.x.x	10.x.x.x	255.x.x.x
	VLAN xxx	Administración	10.x.x.x	10.x.x.x	255.x.x.x

Fuente: Departamento de (TIC), del Hospital Isidro Ayora de Loja (2015).

- **ACL/VLAN.**

Las reglas de control están diseñadas, para permitir o denegar acceso, tal como se muestra a continuación:

- Permite el acceso de la *(VLAN),* Administrativos y Médicos al servidor *(SGH).*
- Permite el acceso de la *(VLAN),* Administrativos al servidor de Recaudación.
- Permite el acceso de la *(VLAN),* Administración a todas las *(VLAN).*
- Permite únicamente la administración de equipos a direcciones IP, de la *(VLAN),* Administración
- Denegar el acceso a las interfaces de las *(VLAN),* para la administración de los equipos y denegar el acceso de *intra-VLAN.*
- Permite el acceso de todas las *(VLAN),* al Internet

- **Módulo de distribución**

EL objetivo de este módulo, es proveer la conectividad de red, en las diferentes estaciones de usuarios finales, a través de los equipos de distribución, como son los *switch* de capa 3, por medio de enlaces, del cableado estructurado y los puntos inalámbricos.

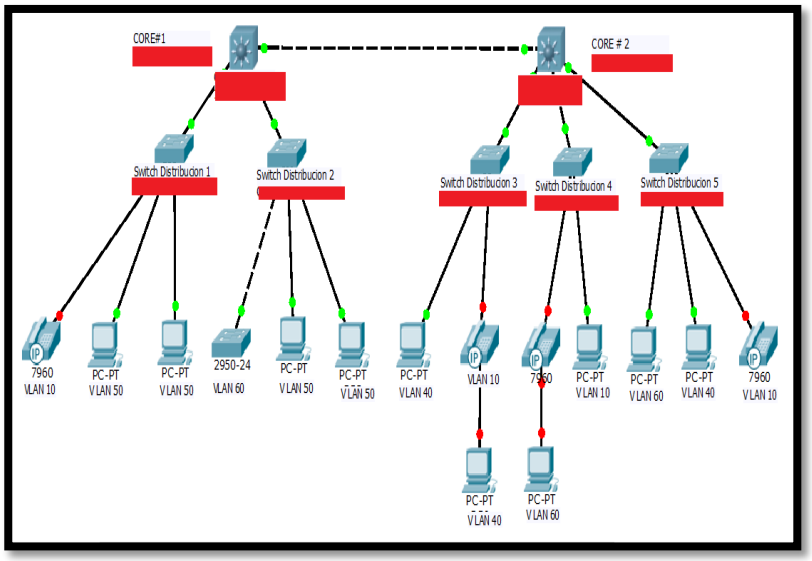


Ilustración 27: Diseño de la configuración del módulo de distribución.
Fuente: El Autor (2015).

En el switch de capa 3, se encuentran las *(VLAN),* previamente mencionadas, en el cual se define una *(VLAN),* por cada puerto, la distribución está realizada, de acuerdo a la cantidad de equipos disponibles y el número de usuarios. Con la finalidad de abastecer, a la cantidad de usuarios, conectados a la red, los *switch* de la capa de distribución, permiten el acceso directo a los clientes, ya sean estos: teléfonos, impresoras, estaciones de trabajo, o puntos de acceso inalámbrico.

En la siguiente tabla, se muestra la distribución de puertos de los equipos de red.

Tabla 14: Configuración de los puertos del Switch Core.

DISPOSITIVO	ASIGNACIÓN	PUERTO
Switch Core 1	VLAN xxx Nativa Modo Trunk	fa0/1, fa0/6, fa0/12, Gi0/27
	VLAN xxx Internet	Gi0/28
	VLAN xxx Servidores	fa0/2, fa0/3
	VLAN xxx Voz	fa0/4
	VLAN xxx Administración	fa0/13, fa0/23
	Monitoreo	fa0/24
Switch Core 2	VLAN xxx Nativa Modo Trunk	Gi0/28, Gi0/25, fa0/1, fa0/2,
Switch Distribución 1	VLAN xxx Nativa Modo Trunk	fa0/1,
	VLAN xxx Administrativa (Nativa) VLAN xxx Voz Modo Trunk	fa0/2 – fa0/24
Switch Distribución 2	VLAN xxx Nativa Modo Trunk	fa0/1
	VLAN xxx Administrativa (Nativa) VLAN xxx Voz Modo Trunk	fa0/2 – fa0/24
Switch Distribución 3	VLAN xxx Nativa Modo Trunk	fa0/1
	VLAN xxx Médicos (Nativa) VLAN xxx Voz Modo Trunk	fa0/2 – fa0/24
Switch Distribución 4	VLAN xxx Nativa Modo Trunk	fa0/1
	VLAN xxx Médicos (Nativa) VLAN xxx Voz Modo Trunk	fa0/2 – fa0/14
	VLAN xxx Voz	fa0/14 – fa0/19
	VLAN xxx Operativos	fa0/20 – fa0/23
Switch Distribución 5	VLAN xxx Nativa Modo Trunk	Gi0/25
	VLAN xxx Voz	fa0/1 – fa0/6
	VLAN xxx Operativos	fa0/7 – fa0/11
	VLAN xxx Médicos	fa0/14 – fa0/24
Switch Acceso 1	VLAN xxx Voz	fa0/1 – fa0/24

Fuente: Departamento de TIC del Hospital Isidro Ayora de Loja (2015).

- **Módulo de servidores.**

Aquí se encuentran, los servidores de la red interna del Hospital, mismos que se conectan directamente al **core** de la red, garantizando que los servicios, sean alcanzados por los usuarios finales. Cabe señalar que aquí se incluye el servidor

(DHCP), de la red, el mismo que contiene las *(VLAN)*, de: Médicos, Administrativos, Operativos y Administración. Los servidores están ubicados en la *(VLAN)* xxx, y tendrán una dirección *(IP)*, estática asignada de la siguiente forma:

Tabla 15: Asignación de dirección IP a los servidores de la Red.

SERVIDOR	DIRECCIÓN IP
Servidor SGH-SGRHIA	10.x.x.x
Servidor de Recaudación Sistema Mónica Active Directory	10.x.x.x
Servidor VoIP	**10.x**.x.x
Servidor DHCP	10.x.x.x

Fuente: Departamento de (TIC), del Hospital Isidro Ayora de Loja (2015).

6.2.2.2.Bloque de perímetro.

En este bloque, se encuentra el módulo de Internet, en donde, se establecen las políticas necesarias, para el acceso a las redes internas de la *Demilitarized Zone (DMZ).*

- **Módulo de Internet.**

  Este es el módulo más crítico de la red, por ser el que provee el servicio de Internet, aquí se aloja el servidor del sitio *web*, cuya base principal es el equipo *firewall*, permitiendo controlar el acceso tanto al servidor *web*, como a la red interna, este cuenta con tres interfaces, en las cuales se encuentra el servidor *proxy*, de la red interna, como también el equipo *(IDS)* y el *System Of Intruders Detection In A Host (HIDS).* El *(IDS)*, en el switch de la *(DMZ)*, es el encargado de realizar el monitoreo, de las peticiones que ingresan a los servidores, para detectar cualquier tipo de ataque.

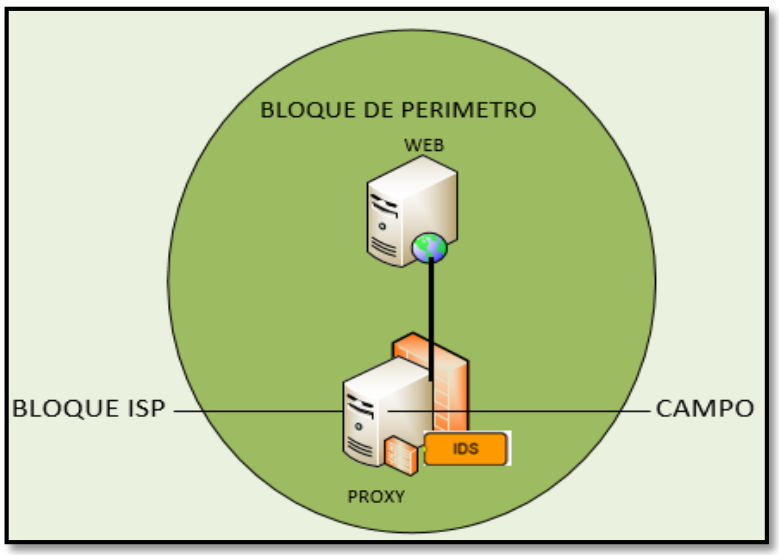


Ilustración 28: Seguridad perimetral firewall con tres interfaces de red
Fuente: El Autor (2015).

- **Firewall**

Por las características planteadas anteriormente, es necesario detallar que el sistema *(IDS),* cuentan con la distribución de ***Linux (Zentyal)***, para la seguridad perimetral, donde están configurados, los servicios de seguridad, cuya infraestructura se describe a continuación: *(IDS, DNS, Antivirus, Firewall, Filtro HTTP*, entre otros).

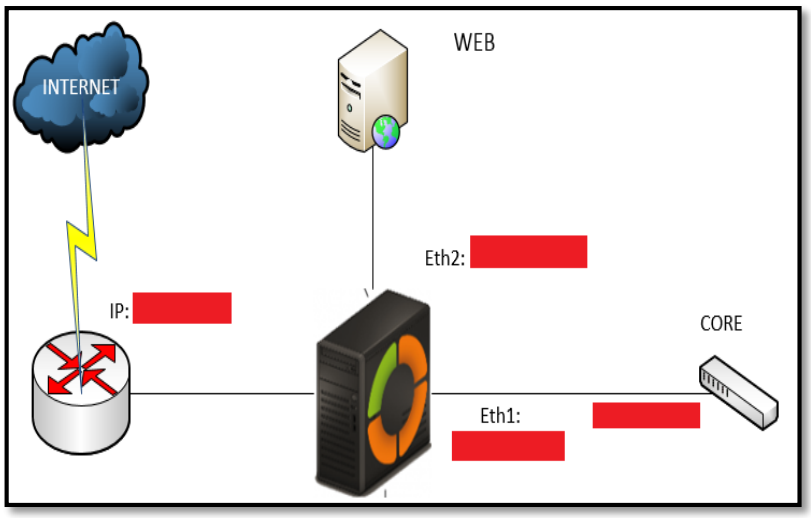


Ilustración 29: Configuración de interfaces Zentyal bloque perímetro.
Fuente: El Autor (2015).

6.2.2.3.Bloque ISP.

Este bloque proporciona el servicio de Internet, con un enlace de 10 *Mbps*, a través de un *router* que administra el enlace *(WAN),* el enrutamiento a Internet, la seguridad y el *(DNS),* el *(ISP),* está configurado con una dirección *(IP),* privada, para el Internet y una *(IP)* pública, para el servidor *web*, tal como se aprecia en la imagen anterior.

6.2.2.4.Esquema de la red de datos del hospital isidro ayora.

En el diagrama anterior, se detalla el modelo de la red de datos, de forma general y como se interconecta, con las demás áreas que trabajan sistemáticamente, para coordinar actividades propias de la institución. Para la obtención, de la información sobre el estado actual, de la red de datos del Hospital Isidro Ayora de Loja, en la cual se encuentra inmersa la red de *(VoIP),* se aplicaron las técnicas de investigación, como la observación directa y entrevistas, estas últimas, están enfocadas al personal técnico del departamento

de *(TIC)*, porque son ellos quienes conocen cómo está la configuración y distribución de la red de datos, gracias a estas entrevistas se pudo investigar, si existen planes de contingencia, políticas de seguridad y mecanismos, para la protección de la red de datos, las cuales se ven reflejadas en la red de *(VoIP)*, de la institución.

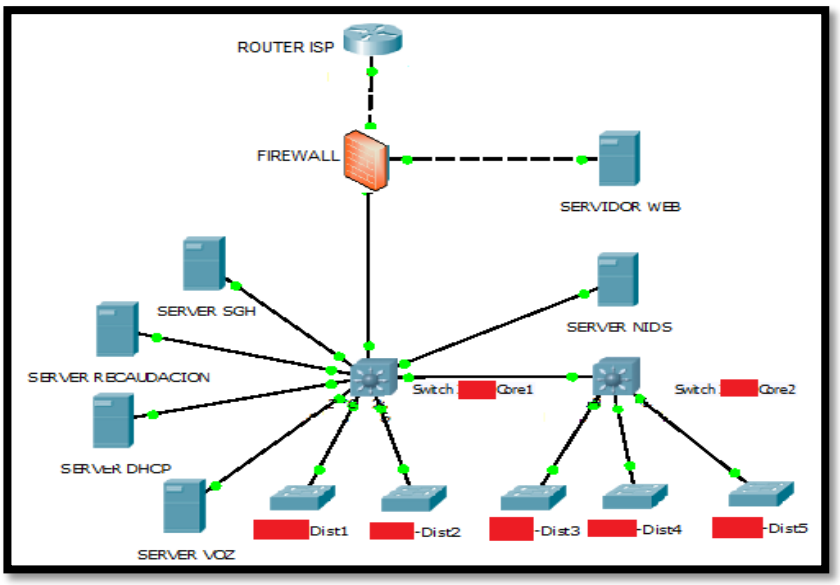


Ilustración 30: Topología de la red de datos del Hospital Isidro Ayora de Loja.
Fuente: El Autor (2015).

Luego de haber analizado y detallado la situación actual, de la red de datos de la Institución, a simple vista se identificó algunas amenazas, a las que está expuesta y el riesgo que implican para la entidad, en la siguiente tabla, se muestra los resultados obtenidos de las entrevistas realizadas, identificando problemas críticos que constituyen una amenaza para la Institución.

Tabla 16: Lista de problemas encontrados en la Institución

PROBLEMA	AMENAZA
✓ Asignación manual de direcciones IP. ✓ Falta de backup de información. ✓ Falta de políticas de acceso a la red. ✓ Falta de control de acceso del contenido de Internet.	Interrupción en la disponibilidad del servicio.
✓ Contraseñas inseguras. ✓ Ausencia de contraseñas. ✓ Pérdida de información. ✓ Falta de control de acceso a las instalaciones del centro de cómputo. ✓ Pérdida de información. ✓ Falta de documentación en la configuración de los equipos de red.	Accesos no autorizados.
✓ No se utiliza mecanismos de protección como: firewall, proxy, autenticación o detección de intrusos. ✓ Carece de email corporativo.	Ataques de (Malware)

Fuente: El Autor (2015).

6.3. FASE 1. REUNIÓN DE ACTIVOS Y PERFILES DE AMENAZA

La primera fase de la metodología ***(OCTAVE)***, describe la reunión de activos de la infraestructura, identificados en la base de información y el perfil de la red, sobre los cuales se realizará los perfiles de vulnerabilidades.

6.3.1. Proceso 1. Identificación de activos.

En base a la infraestructura de la red, se procedió a identificar los activos críticos, los cuales representan los puntos clave, en la comunicación de la red *(VoIP)*, del Hospital Isidro Ayora, se han agrupado los activos críticos de la siguiente manera.

- **Hardware**

Se considera como equipos críticos de hardware**,** a todos los servidores y equipos de red, de acuerdo a la función que desempeñan, su importancia radica en la operatividad de los servicio, de los sistemas de información y comunicaciones que permiten a la institución brindar sus servicios y gestionar sus tareas, tanto en el ámbito administrativo, como en el campo de la salud, por ende, en la siguiente tabla, se detalla los principales servidores, siendo el principal punto de atención, el servidor de comunicaciones *Elastix*.

Tabla 17: Activos críticos de hardware.

HARDWARE	FACTORES DE IMPORTANCIA
IBM	✓ Servidor del software MONICA utilizado por el departamento de recaudación.
HP	✓ Servidor del Sistema de Gestión Hospitalaria *(SGH)*. ✓ Servidor del Sistema de Recursos Humanos *(SGRHIA)*.
HP	✓ **Servidor de Comunicaciones con Elastix para *(VoIP)*.**
SWITCH	✓ **Administración de *(VLAN)* de la red.**
ACCESS POINT	✓ Acceso inalámbrico para el área de dirección.
SWITCH	✓ Acceso de estaciones de trabajo a la red.
ROUTER	✓ Servicio de Internet. *(ISP)*

Fuente: El Autor (2015).

- **Software**

Se los ha denominado activos de *software*, a cada uno de los sistemas operativos y aplicaciones, que están corriendo sobre los servidores y en los equipos administrables de red, mismos que se detallan en la siguiente tabla.

Tabla 18: Activos Críticos de Software.

SOFTWARE	FACTORES DE IMPORTANCIA
Sistemas Operativos de los servidores	✓ Sistema Operativo del Servidor de recaudación. ✓ Sistema Operativo del servidor de los sistemas SGH y SGRHIA. ✓ **Sistema Operativo servidor de Voz**
Sistema Operativo de equipos de red	✓ **Sistema Operativo de equipos administrables de la red.**

Fuente: El Autor (2015).

- **Comunicaciones**

Estos activos se los considera los más importante de todos, por ser el objeto de estudio de nuestra investigación, por contemplarse, la central *(PBX)*, los terminales (*teléfonos*), es decir todo el sistema de *(VoIP)*, la importancia y eficacia de este servicio, radica en la fiabilidad y disponibilidad, por ser el medio utilizado, para realizar la reservación de turnos, de los pacientes del Hospital Isidro Ayora, además, es el medio de comunicación entre todos los departamentos de la institución.

6.3.2. Proceso 2. Perfil de amenazas de seguridad de los activos

Se ha determinado las amenazas de los activos críticos, identificados en el proceso anterior, considerando el perfil actual de la red y los problemas de seguridad, identificados en las entrevistas realizadas.

En la siguiente tabla, se detalla una serie de amenazas, con las cuales se puede llegar a convertirse en problemas para la institución.

Tabla 19: Posibles amenazas en la red de (VoIP), del Hospital Isidro Ayora

ACTIVOS	AMENAZAS
Hardware	Corte de energía Acciones mal intencionadas o por desconocimiento sobrecargas eléctricas Discontinuidad del servicio por diseño inadecuado de infraestructura de red y falta de documentación.
Software	Accesos no autorizado Robo de contraseñas No existen planes de mantenimiento preventivo ni correctivo. Denegación de servicios Destrucción o modificación del sistema operativo o aplicaciones Errores en la manipulación del sistema operativo o aplicaciones Malware
Comunicaciones	Corte de energía Acceso no autorizado Manipulación inadecuada de la infraestructura de comunicación telefónica Denegación de servicios Intercepción de la comunicación.

Fuente: El Autor (2015).

Para calcular, el nivel de riesgos críticos, de los activos se requiere, la probabilidad de ocurrencia de las amenazas y la identificación de las vulnerabilidades que se puedan explotar, cuyo análisis se lo realiza en la última fase de la metodología ***(OCTAVE).***

6.4. FASE 2. IDENTIFICACIÓN DE VULNERABILIDADES EN LA INFRAESTRUCTURA DE LA RED VOIP DEL HOSPITAL.

Esta fase comprende, la evaluación de la infraestructura de la red, donde se evalúa las debilidades, de los componentes claves que pueden llevar a acciones no autorizadas, contra los activos de la red. Para proceder con el análisis de vulnerabilidades, es necesario determinar las herramientas a utilizar, el método de análisis y el tipo de test, con el fin de determinar las tareas que se va a realizar.

- **Elección de herramientas**

  Para poder realizar la búsqueda de vulnerabilidades, es necesario tomar las herramientas adecuadas, por la infinidad que existe, tal como se describe en la revisión literaria apartado, herramientas de análisis de vulnerabilidades en *(VoIP)*. Para ello se ha realizado las siguientes tablas, con las principales características de cada una de estas, y así poder seleccionar las que mejor se acoplen a esta investigación.

  - **Herramientas para escanear la red.**

    En la siguiente tabla, se realiza una comparación de las características y operatividad de las herramientas, especializadas en el escaneo de la red, con el fin de escoger el mejor perfil de la misma, y que sea de utilidad en la investigación.

Tabla 20: Comparación de Herramientas para escaneo de la red.

CARACTERÍSTICAS	FPING	NMAP	ICMPENUM	ICMPQUERI
Paquetes ICMP	x	x	x	x
Bloqueo de Firewall	x	x	x	x
Direcciones IP desde el fichero				
Barridos de Ping		x		x
IP Activas	x	x		
Sistemas Operativos Linux	x	x	x	x
Determinar servicios activos en modo escucha		x		
Detección del sistema operativo		x		

Fuente: El Autor (2015).

- **Herramientas para obtención de extensiones.**

En la siguiente tabla, se realiza una comparativa, entre las características de las herramientas, especializadas en la obtención de extensiones, donde se selecciona, las que mejor se adaptan a las necesidades requeridas.

Tabla 21: Comparación de Herramientas para obtención de extensiones.

CARACTERÍSTICAS	SIPSCAN	ENUMIAX	SIPVICIOS	SHODAN
Sistema operativo Linux		x	x	
Obtención de extensiones *(SIP)*	x	x	x	x
Necesario contar con la dirección del servidor	x	x	x	
Obtención de extensiones de la *(PBX)*		x	x	x
Obtiene contraseñas en caso que las extensiones las soliciten			x	
Encuentra dispositivos conectados a Internet con configuraciones erróneas de seguridad		x		x

Fuente: El Autor.

- **Herramientas para capturar paquetes en la red.**

Para la captura de paquetes también, se realizó una comparación, para seleccionar las mejores características, de la herramienta adecuada para este proceso.

Tabla 22: Comparación de Herramientas para captura de datos.

CARACTERÍSTICAS	ETERCAP	KISMET	TCPDUMP	WIRESHARK
Interceptor registrador para redes *(LAN)*	x			x
Soporta direcciones activas y pasivas de varios protocolos	x			x
Permite identificar ataques de *spoofing*	X		x	x
Husmeador de paquetes		x		
Analiza el tráfico de información de una red	x	x	x	x
Detección de intrusos en redes inalámbricas		x		x
Requiere tarjeta inalámbrica soporte el modo de monitorización *raw*		x		
Captura y muestra los paquetes transmitidos y recibidos en la red			x	x
Plataforma *Linux*	x	x	x	x
Interfaz Gráfica	x			x
Gran capacidad de filtrado				x

Fuente: El Autor (2015).

Finalmente, se realiza una tabla con las herramientas escogidas durante la comparación, con las que se pretende realizar el análisis de las vulnerabilidades de la red.

Tabla 23: Herramientas elegidas para el objeto de estudio.

HERRAMIENTA	OBJETIVO
Nmap	Escaneo de red
EnumIAX	Obtención de extensiones
Wireshark	Captura de llamadas
Hydra	Búsqueda de contraseñas.

Fuente: El Autor (2015).

- **Método de Análisis de vulnerabilidades**

Para poder realizar este análisis, se utilizara el método de caja blanca, porque se cuenta con la información necesaria, así mismo, se conoce ciertas direcciones *(IP)*, de los servidores y las puertas de enlaces de los equipos de red, las cuales se las agrupado en archivos de texto plano, denominados `[IP-Servidores.txt e IP-Equipos-Red.txt]`, con el fin de no revelar las *(IP)*, por motivo de seguridad. Gracias a ello se definió los puntos clave, en los cuales se ve comprometida la seguridad de la red.

- **Tipo de test**

Para la recopilación de información, se ha considerado realizar un test interno, el cual permita determinar el nivel de acceso, de un usuario común, en la red, no se contempla un test externo, debido a que la institución no tiene presencia en Internet, por lo tanto no se puede comprobar el acceso externo.

6.4.1. Proceso 3. Identificación de componentes clave.

En esta actividad, se revisa los activos críticos y amenazas de la *(Fase 1)*, donde se destaca la información contenida en los equipos de red, la asistencia que proporcionan los servidores.

Tabla 24: Componentes claves de la red.

COMPONENTE CLAVE	FACTORES DE IMPORTANCIA
Servidores	Constituyen el componente principal de la Red, por permitir la gestión de la información y la comunicación dentro y fuera del Hospital.
Equipos de comunicación	Son los encargados de establecer la comunicación, entre los diferentes usuarios, es decir, son el medio de transmisión de datos, voz y videos.
Equipos terminales	Son los encargados de recibir y reproducir las señales analógicas y digitales, además son los extremos de la comunicación *(origen destino).*

Fuente: El Autor (2015).

6.4.2. Proceso 4. Evaluación de los componentes claves.

La metodología ***(OSSTMM),*** permite realizar una evaluación a los componentes clave de la red, como ya se mencionó anteriormente en el apartado del método de análisis de vulnerabilidades.

EL software utilizado para el desarrollo del presente proyecto, es la distribución *Kali Linux,* el cual contiene un variedad de herramientas que serán utilizadas en las correspondiente pruebas de cada fase, según la metodología propuesta, para la ejecución de estas herramientas, se lo realiza desde la terminal o consola del sistema operativo, como usuario root.

1. SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET.

En la ejecución de esta fase se identifica el objetivo que va a ser testeado mediante el módulo del sondeo de red.

1.1. SONDEO DE RED

El sondeo de red, es la primera actividad de esta sección, que nos permite explorar el diseño de la red para determinar sus vulnerabilidades. Para la realización del test a través de la herramienta *Kali Linux,* se asignado la *(IP),* `[10.x.x.x]` al equipo de pruebas.

1.1.1. Enumeración de puertos

Esta actividad permite conocer los puertos *(TCP) y (UDP),* que se encuentran abiertos, filtrados o cerrados en el servidor *(VoIP),* para posteriormente descubrir las vulnerabilidades a las que se encuentra expuesto. En la numeración de puertos se hace uso de herramienta *(Nmap),* la cual, contiene una base de conocimiento bastante amplia, para determinar los resultados con la mayor precisión posible. Es necesario conocer los puertos abiertos mayores a `[1024]` que son utilizados por las distintas aplicaciones, y de esta manera descubrir el uso de puertos no registrados por aplicaciones inseguras.

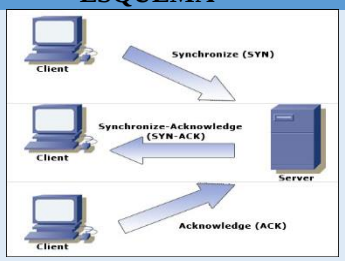
El escáner de los puertos *(UDP),* no es exacto, sin embargo, este protocolo es bastante débil, por lo que es necesario, analizar los puertos que se encuentran abiertos, para

verificar los resultados obtenidos con *(Nmap)*, para ello se realiza conexiones vía *telnet* a los puertos *(TCP)*.

1.1.1.1. Enumeración de puertos en los servidores

Para realizar la enumeración de puertos, se utiliza la técnica de *(SNY flood)*, *Initial Numbers Sequence (SYN)*, es un bit de control dentro del segmento *(TCP)*, que se utiliza para sincronizar los *(ISN)* de una conexión esto se conoce como (TCP 3-Way Handshake Diagrama). En la tabla 25, se muestra un diagrama simple del proceso de apretón de manos de 3 vías *(TCP)*. [19]

Tabla 25: TCP Three Way Handshake (SNY, SNY-ACK, ACK).

EVENTO	ESQUEMA
Host A sends a TCP SYNchronize packet to Host B Host B receives A's SYN Host B sends a SYNchronize-ACKnowledgement Host A receives B's SYN-ACK Host A sends ACKnowledge Host B receives ACK. TCP socket connection is ESTABLISHED.	

Fuente: El Autor (2015).

- **Escaneo *(SNY)*, a los puertos *(TCP)*, por defecto con Nmap).**
  - `[nmap -sS -iL /root/Desktop/IP-Servidores]`

```
Starting Nmap 6.47 ( http://nmap.
Nmap scan report for 10.[redacted]
Host is up (0.0065s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
443/tcp  open  https
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql
4445/tcp open  upnotifyp
```

Ilustración 31: Enumeración de puertos (TCP), de servidores (Escaneo SNY).
Fuente: El Autor (2015).

Para que *(Nmap)*, envíe paquetes *(SNY)* y *(-sS)*, al objetivo, se utiliza lo siguiente:

- *(-sS):* No abre una conexión *(TCP)*, completa, solo se envía un paquete *(SYN)*, si llega un *(SYN | ACK)*, se envía un *(RTS)*, para cerrar la conexión.

- *(-iL) :<archivo>*, identifica el archivo de texto que contiene la lista de *(IP)*, activos seleccionados, para el escáner. [7] [19]

- **Escaneo (*CONNECT)* a los puertos *(TCP)*, mayores que 1024**

`[nmap -sT -p1024 -iL /root/Desktop/IP-Servidores].`

Ilustración 32 : Enumeración de puertos (TCP), de servidores (Escaner Connect).
Fuente: El Autor (2015).

- *(-sT):* Llama al sistema para establecer una conexión con los puertos.

- *(-iL): iL <archivo>:* identifica el archivo de texto, que contiene la lista, de las *(IP)*, activos, seleccionados para el escaneo.

- **Escaneo de puertos *(UDP)*, por defecto con Nmap).**

`[nmap -sU -iL /root/Desktop/IP-Servidores].`

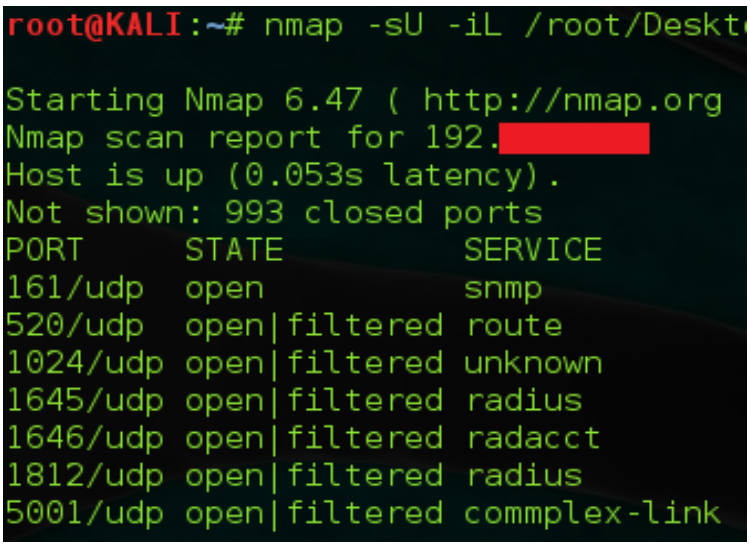


Ilustración 33: Escaneo de puertos (UDP) en los servidores.
Fuente: El Autor (2015).

(Nmap), envía paquetes *(SNY),* al objetivo para evaluar su respuesta y considerar los destinos inalcanzables, como puertos cerrados, los comandos utilizados son los siguientes:

- *(-iL):* <*archivo*> identifica el archivo de texto que contiene la lista de *(IP),* activos, seleccionados para el escaneo.
- *(–sU):* Se usa para saber que puertos *(UDP),* están abiertos.

En la imagen anterior, se muestran ciertos puertos abiertos, pero que están *(filtrados),* por ende, ya no se los considera una vulnerabilidad, porque son hostiles a los ataques, por parte de los piratas informáticos. Cabe mencionar que se realizó un scanner, a todos los servidores que se encuentran en la red, e incluso a los que, no realizan ninguna actividad, pero se encuentran conectados a la red, como el estudio está enfocado solo al servicio de *(VoIP),* razón por la cual en la siguiente tabla, solo se muestra un resumen de los resultados obtenidos del escáner *(SNY), (CONNECT) y (UDP),* realizado al servidor de *(VoIP),* "*por cuestiones de seguridad no se expone el nombre de los puertos y servicios"*.

Tabla 26: Enumeración de puertos en el servidor de Voz.

SERVIDOR DE VOIP 10.104.33.2					
Puerto	**Estado**	**Servicio**	**Puerto**	**Estado**	**Servicio**
22/TCP	Abierto	SSH	2000/TCP	Abierto	Cisco-SCCP
25/TCP	Abierto	SMTP	3306/TCP	Abierto	MySQL
80/TCP	Abierto	HTTP	4445/TCP	Abierto	Upnotifyp
110/TCP	Abierto	POP3	4559/TCP	Abierto	Hylafax
111/TCP	Abierto	Rpcbind	5038/TCP	Abierto	Desconocido
143/TCP	Abierto	IMAP	69/UDP	Abierto	POP3
443/TCP	Abierto	HTTPS	111/UDP	Abierto	Rpcbind
993/TCP	Abierto	IMAPS	123/UDP	Abierto	POP3S
995/TCP	Abierto	POP3S	1019/UDP	Abierto	Desconocido
1022/TCP	Abierto	EXP2	5060/UDP	Abierto	SIP

Fuente: El Autor (2015).

A continuación se realiza un análisis, de los puertos más importantes, encontrados abiertos en el servidor de *(VoIP).* Se encuentran abiertos, debido a que el sistema operativo incluye algunos servicios como*: Internet Message Access Protocol (IMAP), (SMTP), (POP3),* entre otros. Se debe redefinir la configuración del servidor, cerrando los puertos abiertos, para prevenir algún tipo de ataque. En el punto de identificación de servicios, se obtiene los servicios que se ejecutan en dichos puertos, a través de estos, los atacantes pueden realizar inyecciones de virus o troyanos, por ejemplo: en el puerto 25, los troyanos que se pueden ingresar son: *(Ajan, Antigen, Email Password Sender,*

Happy99, Kuang2, Promail, Shtrilistz, Stealth, Tapiras, Terminator, Winpc, WinSpy, entre otros).

1.1.1.2. Enumeración de puertos en los equipos de red.

De la misma forma, se realizó un escáner equipos de red que realizan la función del core, porque en unos de estos equipos se encuentran configurada la *(VLAN),* de transmisión de voz, los resultados obtenidos se los detalla a continuación:

- **Escaneo *(SNY),* a los puertos *(TCP),* por defecto con Nmap**

(Nmap), envía paquetes *SNY (-sS),* al objetivo, las opciones utilizadas son:

  - *(-iL): <archivo>:* identifica el archivo de texto que contiene la lista de *(IP),* activos seleccionados para el escáner.
  - *(-sS):* No abre una conexión *(TCP),* completa, solo envía un paquete.

```
[nmap -sS -iL/root/Desktop/IP-Equipos-Red]
```

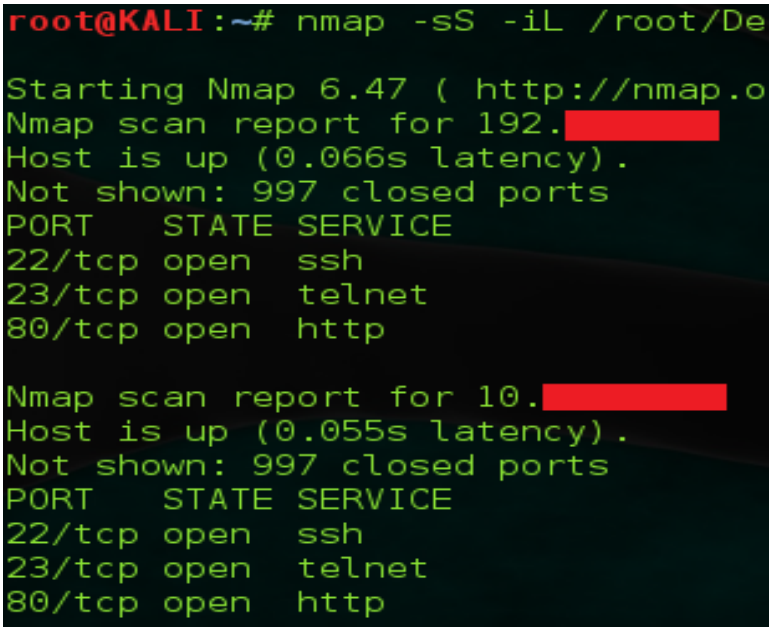


Ilustración 34: Enumeración de puertos (TCP), en los equipos de red.
Fuente: El Autor (2015).

- **Escaneo de puertos *(UDP),* por defecto con Nmap.**

(Nmap), envía paquetes *SNY (-sS),* al objetivo, las opciones utilizadas son:

(–sU): Se usa para saber que puertos *(UDP),* están abiertos.

- *(-iL):* <*archivo*> identifica el archivo de texto que contiene la lista de sistemas activos seleccionados para el escaneo.

```
[Nmap -sU -iL /root/Desktop/IP-Equipos-Red].
```

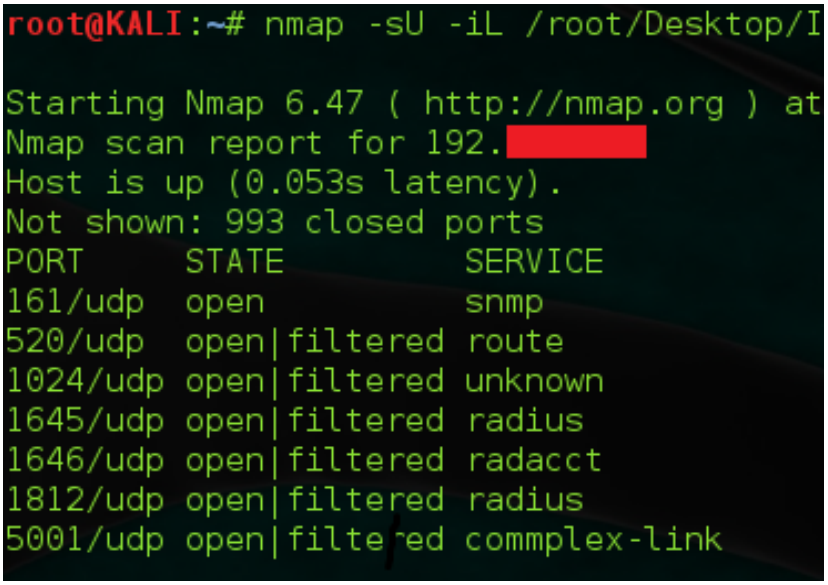


Ilustración 35: Enumeración de puertos (UDP), en los equipos de red.
Fuente: El Autor (2015).

El escáner se realizó a todos los equipos de red y a cada una de las puertas de enlaces o gateways, asignados a las interfaces, donde están configuradas las *(VLAN).* En la siguiente tabla, se muestra un resumen de los puertos que se encuentran abiertos en el *(Switch).*

Tabla 27: Enumeración de puertos TCP y UDP de los equipos de red.

SWITCH 3COM					
PUERTO	**ESTADO**	**SERVICIO**	**PUERTO**	**ESTADO**	**SERVICIO**
22/TCP	Abierto	SSH	1024/UDP	Abierto/filtrado	Desconocido
23/TCP	Abierto	TEINET	1645/UDP	Abierto/filtrado	Radius
80/TCP	Abierto	HTTP	1646/UDP	Abierto/filtrado	Radacct
161/UDP	Abierto/filtrado	SNMP	1812/UDP	Abierto/filtrado	Radius
520/UDP	Abierto/filtrado	ROUTE	5001/UDP	Abierto/filtrado	Complex-link

Fuente: El Autor (2015).

En los equipos de red, se encontró un puerto abierto, el cual puede ser utilizado, para obtener información de los equipos, mediante *software* de enumeración, cuando el servicio, de este puerto no está configurado adecuadamente se pueden modificar los valores por defecto.

1.1.2. Identificar el de uso de protocolos de enrutamiento.

Para identificar los protocolos de enrutamiento, utilizados en la red del Hospital, se utilizó

la herramienta *wireshark*, para la capturar el tráfico.

Ilustración 36: Identificación de protocolo de enrutamiento.
Fuente: El Autor (2015).

Los resultados obtenidos de varias capturas, muestran el uso de *(RIPv2)*, para el enrutamiento de paquetes de voz y datos a sus respectivos servidores.

1.1.3. Identificar el uso de protocolos no estándar

Se ha categorizado como protocolos no estándar, aquellos que no se utilizan, y que pueden consumir recursos de la red. Durante la captura con *wireshark*, se encontró los siguientes protocolos: *(NBIPX)*, *(IPX)*, *(SAP)*, entre otros. Los servicios de la red del Hospital, corresponden al protocolo *(IP)*, los protocolos derivados de *(IPX)*, que es una familia de protocolos de red, que se reemplazó por *(TCP/IP)*. El protocolo (*SEBEK)*, utilizado por la aplicación *groove*, para compartición de recursos y actualizaciones, también se establece como protocolo no estándar.

1.1.4. Identificación de servicios

La mayoría de ataques en los equipos y servidores de la red, se deben a las vulnerabilidades que presentan las aplicaciones o servicios, más no en los puertos como tal, ya sea por defectos en la configuración e implementación, o por las versiones desactualizadas, cuya información suele ser útil, para los atacantes, porque pueden reconocer los exploits, para cada una de las vulnerabilidades encontradas, en las versiones de servicios y/o aplicaciones.

1.1.4.1.Identificación de servicios de los servidores

La identificación de servicios, de los servidores, se lo realizó por cada uno de los puertos, enumerados en el escáner *(SNY).* Se aplicó la herramienta *(Nmap),* para obtener las versiones de las aplicaciones. Esto se lo realizo por consola desde *Kali-Linux.*

Las opciones utilizadas son:

- *v:* Para aumentar el nivel del escaneo.
- *A:* Para identificar el sistema operativo y versión.
- *T4:* Aumentar temporizado, realiza el escaneo más rápido.
- *iL <archivo>:* Identifica el archivo de texto que contiene la lista de sistemas activos seleccionados para el escaneo.

```
[#nmap -v -A -T4 -iL /root/Desktop/IP-Servidores]
```

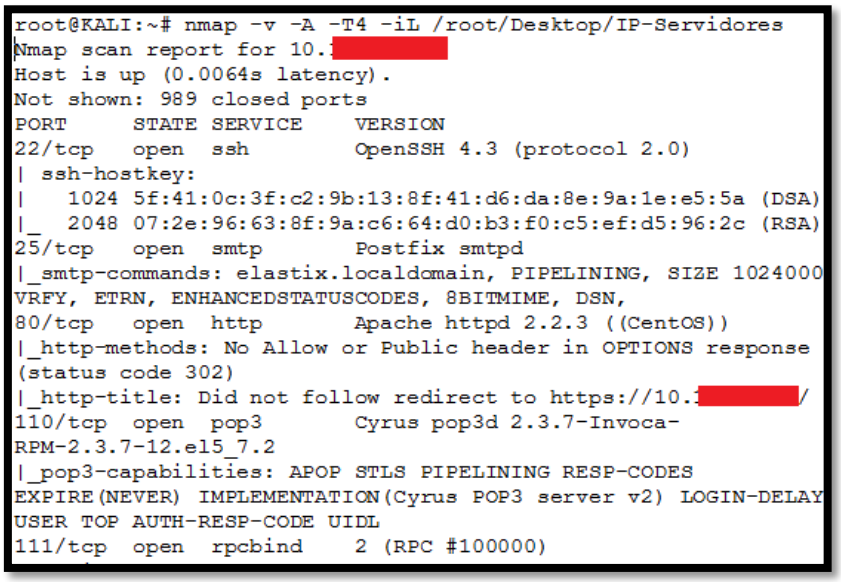


Ilustración 37: Resultado del escáner de la versión del servidor.
Fuente: El Autor (2015).

En la siguiente tabla, se describen los resultados obtenidos, de la ejecución de los servicios, que se encuentran corriendo en los puertos de servidor *(VoIP).*

Tabla 28: Enumeración de servicios en el servidor de voz

SERVIDOR DE VOIP 10.104.33.2		
PUERTO	**SERVICIO**	**APLICACIÓN**
22/TCP	SSH	OpenSSH 4.3 (Protocol 2.0)
25/TCP	SMTP	-
80/TCP	HTTP	Apache HTTPD 2.2.3 (CentOS)

110/TCP	pop3?	-
111/TCP	Rpcbind	-
143/TCP	IMAP	-
443/TCP	HTTPS	apache httpd 2.2.3 ((Red Hat)
993/TCP	IMAPS	-
995/TCP	POP3S	-
1022/TCP	Status	1 (rpc#100024)
2000/TCP	cisco-sccp	-

Fuente: El Autor (2015).

1.1.4.2.Identificación de servicios de los equipos de red.

De la misma forma, se realizó la sentencia por consola desde *Kali Linux*, para el escáner de las versiones de los equipos de red:

Las opciones utilizadas son las siguientes:

- *v:* Para aumentar el nivel del escaneo.
- *A:* Para identificar el sistema operativo y versión.
- *T4:* Aumentar temporizado, realiza el escaneo más rápido.
- *iL <archivo>:* Identifica el archivo de texto que contiene la lista de sistemas activos seleccionados para el escaneo. [7] [19]

```
[#nmap -v -A -T4 -iL /root/Desktop/Equipos-red]
```

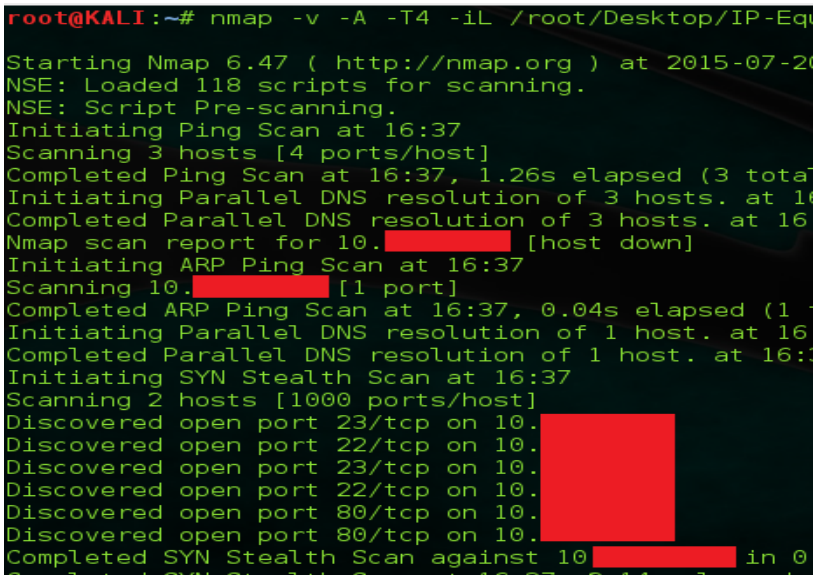


Ilustración 38: Resultados de escáner de versiones en los equipos de red.
Fuente: El Autor (2015).

En la siguiente tabla, se detallan los resultados obtenidos, de la ejecución por consola, para identificar los servicios que se encuentran corriendo, en los puertos de los equipos de red *(core).*

Tabla 29: Enumeración de servicios en servidor de VoIP.

SWITCH 3COM		
PUERTO	**SERVICIO**	**APLICACIÓN**
22/TCP	SSH	HUAWEI VRP SSHD 3.3 (protocol 2.2)
23Telnet	Telnet	3Com 4500 switch TELNET
80/TCP	HTTP	WMI V5 (3Com 5500g-El switch HTTP config)

Fuente: El Autor (2015).

Un atacante, con los conocimientos suficientes en vulnerar sistemas, reconocerá las versiones de las aplicaciones que poseen vulnerabilidades y poder realizar ataques a la red. En el siguiente test, se pretende realizar un reconocimiento, de las vulnerabilidades en las aplicaciones, para lo cual se utilizará el escáner que proporciona el sistema *Kali - Linux.*

1.1.5. Identificación de sistemas operativos.

Los puertos de comunicación, de los equipos en algunos casos proporcionan servicios, de acuerdo al sistema operativo, sin embargo su configuración depende del sistema operativo, por lo que es importante conocerlo y poder determinar la forma de explorar, una aplicación vulnerable o diseñar *exploits*. Los resultados obtenidos con *(Nmap),* en la identificación de los sistemas operativos se muestran con exactitud conforme a la imagen 33, donde un atacante puede hacer uso de esta información, con la finalidad de descubrir las vulnerabilidades de los sistemas, en base a la configuración de los servicios que vienen por defecto, y errores en la programación de las aplicaciones por la versión del *(S.O).*

1.1.5.1.Identificación del sistema operativo de los servidores y equipos de red.

La sentencia por consola desde *Kali Linux,* para el escaneo de las versiones de los servidores y equipos de red, son las que se detallan a continuación, cabe señalar que la misma sentencia se ejecuta para los dos grupos de *(IP),* lo que cambiaría es (*archivo.txt).*

La sentencia, para escanear de las versiones de los equipos de red, son las siguientes:

- *v:* Para aumentar el nivel del escaneo.
- *A:* Para identificar el sistema operativo y versión.
- *T4:* Aumentar temporizado, realiza el escaneo más rápido,
- *iL <archivo>:* Identifica el archivo de texto que contiene la lista de sistemas activos seleccionados para el escaneo. [7] [19]

```
[# Nmap -v -A -T4 iL /root/Desktop/IP-Servidores]
```

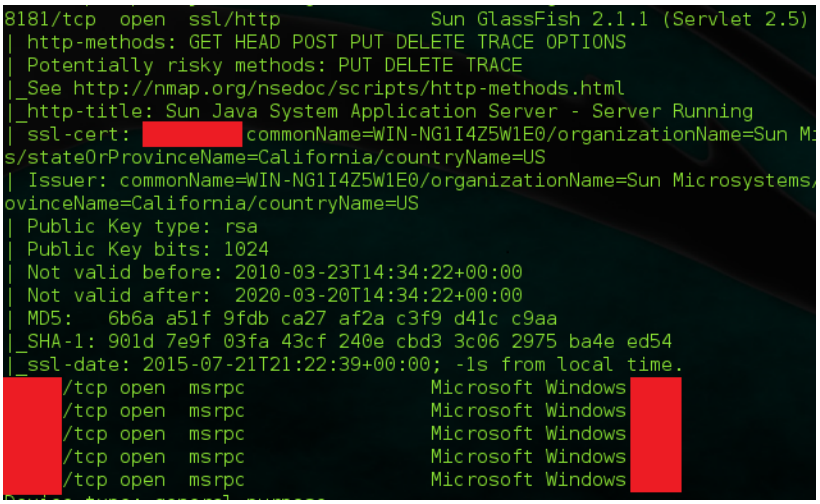


Ilustración 39: Identificación de (S.O) en los servidores y equipos de red.
Fuente: El Autor (2015).

En la siguiente tabla, se describen los sistemas operativos que se están ejecutando en cada uno de los equipos, antes mencionados, siendo de nuestra importancia el servidor de voz, y los equipos de red, junto con la *(IP)*, correspondientes.

Tabla 30: Enumeración de sistemas en equipos de red y servidores.

EQUIPO	IP	SISTEMA OPERATIVO
Router	10.x.x.x	**Cisco IOS 12.X/11.x**
Switch 3Com	**10.x.x.x**	**3Com Europe 4000**
Servidor SGH (HP)	10.x.x.x	Microsoft Windows Vista SP0 - SP2, Server 2008, or Windows 7Ultimate
Servidor Recaudación (IBM)	10.x.x.x	Microsoft Windows 2000 SP4
Servidor de Voz	**10.x.x.x**	**Linux 2.6.9 - 2.6.30**

Fuente: El Autor (2015).

1.2. BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDADES.

En la siguiente sección, se realizará la búsqueda de vulnerabilidades, en los sistemas mencionados, lo que permitirá corroborar la información descrita, para ello se utilizara herramientas de *hacking* y *exploits.*

La identificación de vulnerabilidades, se realizó, a través de la herramienta *(Nessus 6)* que utiliza información basada en *Common Vulnerabilities and Exposures (CVE*) y le asigna un código a una vulnerabilidad que le permite ser identificado de forma unívoca. Estas herramientas, realizan intentos de exploits, para obtener las vulnerabilidades correspondientes, a cada uno de los puertos abiertos en los sistemas.

Se realizó el análisis de las vulnerabilidades encontradas, identificando aquellas correspondientes, al sistema operativo y a las aplicaciones de componentes claves como: servidores y equipos de red. La imagen 41, corresponde a los resultados obtenidos por la herramienta *(Nessus)*, en el escáner realizado al servidor de *(VoIP).*

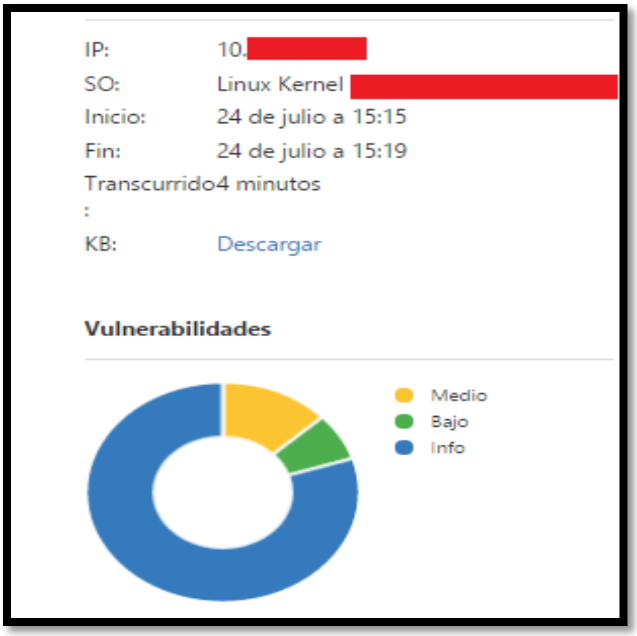


Ilustración 40: Vulnerabilidades en el servidor de (VoIP).
Fuente: El Autor (2015).

1.2.1. Vulnerabilidades en servidor de voz.

A continuación se describen las vulnerabilidades encontradas por puerto y servicio.

Tabla 31: Lista de vulnerabilidades en el servidor de Voz.

PUERTO/ PROTOCOLO	VULNERABILIDAD	IMPACTO	RIESGO	CVE	EXPLOIT
443/TCP	La versión de Apache http (2.2.3) se ve aceptado por una vulnerabilidad de degeneración de servicio.	Aplicación/ Sistema	Alto	2011-3192	49303.c
80/TCP	El servidor Apache 2.0 es vulnerable a ataques de inyección de comandos	Aplicación	Alto	2009-3095	

Fuente: El Autor (2015).

Las vulnerabilidades obtenidas, mediante las herramientas mencionadas, son generalmente conocidas. El escáner *(OpenVas)*, identificó el gusano code red, en el servidor de *(VoIP)*, recomienda actualizar el antivirus, para evitar propagación del mismo.

Los diseñadores de sistemas y aplicaciones, han creado *plugins* de actualización, para cubrir los agujeros de seguridad, descubiertos luego de su publicación. En la *web*, se pueden encontrar exploits con el nombre del *(plugin)* o el código de vulnerabilidad *(CVE)*, tal como se indica en el siguiente punto.

1.2.2. Vulnerabilidades en los equipos de red

Los equipos de red, no presentan vulnerabilidades con riego crítico, en el análisis de puertos y aplicaciones. Los *switch* presentan una vulnerabilidad en el servidor *(SNMP)*, que posee el nombre por defecto de la comunidad *(pública)*, lo que se considera un riesgo si un atacante logra acceder como administrador, podrá conocer toda la información de los dispositivos de la red, tanto de hardware como de la configuración. Sin embargo, proporciona algunas advertencias de seguridad con el puerto, *(telnet)* que es comúnmente vulnerado. El *router* de Internet no presenta vulnerabilidades de alto riesgo, por no encontrar puertos abiertos, a lo que se considera vulnerabilidades de mínimo riesgo.

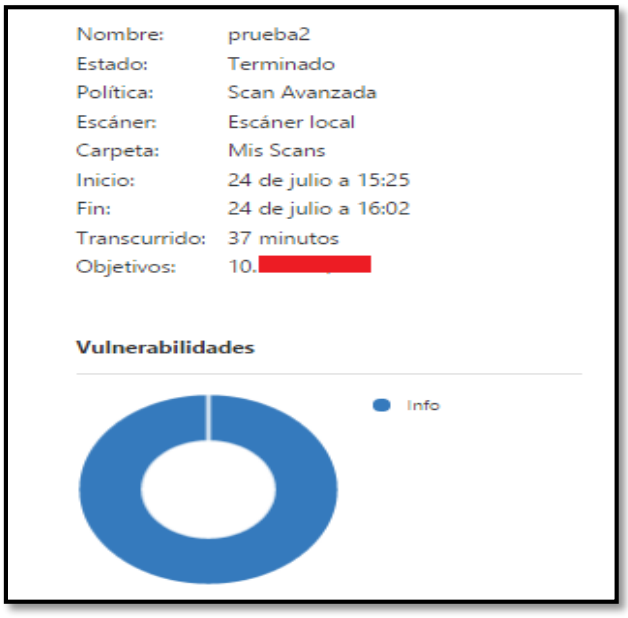


Ilustración 41: Análisis de vulnerabilidades de los equipos de red.
Fuente: El Autor (2015).

1.2.3. Verificación de vulnerabilidades

Con la finalidad, de demostrar cómo un atacante puede ingresar a los servidores, valiéndose de las vulnerabilidades encontradas, se utilizó la herramienta *Metasploit*, muy conocida en el mundo del *hacking*, por la extensa base de datos, de exploits que contiene,

de acuerdo al sistema o aplicación. *Kali Linux*, nos proporciona una base de datos denominada *exploits-db* en donde, se puede realizar la búsqueda de exploits, de acuerdo a la vulnerabilidad de la aplicación o sistema, además de algunos enlaces *web*, para la búsqueda de *exploits*. [7] [19]

Ilustración 42: Búsqueda de exploits mediante el código (CVE) en Security Focus.
Fuente: El Autor (2015).

La búsqueda se realiza mediante el código de vulnerabilidad *(CVE)*, cabe mencionar que esta herramienta es privativa, porque si se quiere solventar las vulnerabilidades que este muestra habría que adquirir la licencia, pero se puede realizar lo siguiente: Los exploits encontrados, se pueden copiar en la base de datos de *Kali Linux*, para hacer uso de ellos y poder generar soluciones a tales vulnerabilidades. *Security Focus* permite, a través de su interfaz web, encontrar información acerca de la vulnerabilidad como: la clase, ejecución remota, la fecha de publicación de la vulnerabilidad y las versiones de sistemas que posee la misma.

1.3. ENRUTAMIENTO.

Para obtener información, del enrutamiento interno de la red, no fue necesario utilizar ninguna herramienta porque el administrador de *(TIC)*, nos proporcionó esta información, así mismo nos advirtió que la red, está sujeta a redistribuciones, por lo cual estas direcciones están sufriendo modificaciones. En el caso de ser necesario, se utilizará la herramienta *(SNMP Chek)*, para vulnerar el puerto *(UDP)* y *(SNMP)*, pudiendo obtener

información sin la necesidad de loguearse. Para realizar el escáner, se indica el sistema objetivo, con la opción *(–t)*, y el comando necesario para realizar este objetivo sería el siguiente:

```
[snmpchek-1.8.pl –t 10.x.x.x]
```

Tabla 32: tabla de enrutamiento Switch 3Com1.

DESTINO	MÁSCARA	SIGUIENTE SALTO	INTERFACE
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-interface1
10.x.x.x	225.x.x.x	127.0.0.1	InLoopback0
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-interface10
10.x.x.x	225.x.x.x	127.0.0.1	InLoopBack0
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-interface20
10.x.x.x	225.x.x.x	127.0.0.1	InLoopback0
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-interface20
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-interface20
127.0.0.0	225.x.x.x	127.0.0.1	InLoopback0
127.0.0.1	225.x.x.x	127.0.0.1	InLoopback0

Fuente: El Autor (2015).

Tabla 33: Tabla de enrutamiento Switch 3Com2.

DESTINO	MÁSCARA	SIGUIENTE SALTO	INTERFACE
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-interface20
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-interface20
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-interface20
10.x.x.x	225.x.x.x	127.0.0.1	InLoopback0
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-nterface1
10.x.x.x	225.x.x.x	127.0.0.1	InLoopback0
10.x.x.x	225.x.x.x	10.x.x.x	Vlan-interface10
10.x.x.x	225.x.x.x	127.0.0.1	InLoopback0
127.0.0.0	225.x.x.x	127.0.0.1	InLoopback0
127.0.0.1	225.x.x.x	127.0.0.1	InLoopback0

Fuente: El Autor (2015).

En el caso del router *(ISP)*, no se proporcionó ninguna información, por motivos de seguridad, las tablas 36 y 37, corresponden a la información de la tabla de enrutamiento, proporcionada por el administrador.

1.4. DESCIFRADO DE CONTRASEÑAS.

En este apartado se intenta buscar contraseñas, a través de ataque de fuerza bruta, hacía las aplicaciones de los equipos de red y servidores.

Para la ejecución de esta técnica, se requiere de una lista de palabras, con el fin de efectuar las combinaciones necesarias, hasta descubrir usuarios y contraseñas correctas, para poder llevar a cabo, este ataque se elaboró un archivo de texto con palabras claves `(diccionario.txt)`. *Kali Linux*, contiene algunas herramientas, para descifrado de

contraseñas mediante fuerza bruta, se han seleccionado dos de las más utilizadas, como son *hydra* y *medusa*.

Los parámetros utilizados en hydra corresponden a la búsqueda de:

- *(–L):* Busca el login.
- *(–P):* Busca el password.
- *(–e):* Añadimos esta opción para que se realice la búsqueda desde un diccionario.
- *(–n):* Para las comprobaciones con password null.
- *(–s):* Para comprobaciones con login y password similares con la opción.
- *(–f):* Indica que se detenga la búsqueda cuando se haya acercado.

Además se debe hace referencia al protocolo y la página que se pretende vulnerar: http-get/en/login.html [7] [19]

```
[hydra 10.x.x.x –L /root/Desktop/diccionario.txt –P /root/Desktop/
         diccionario.txt –e ns –f http-get/en/login.html]
```

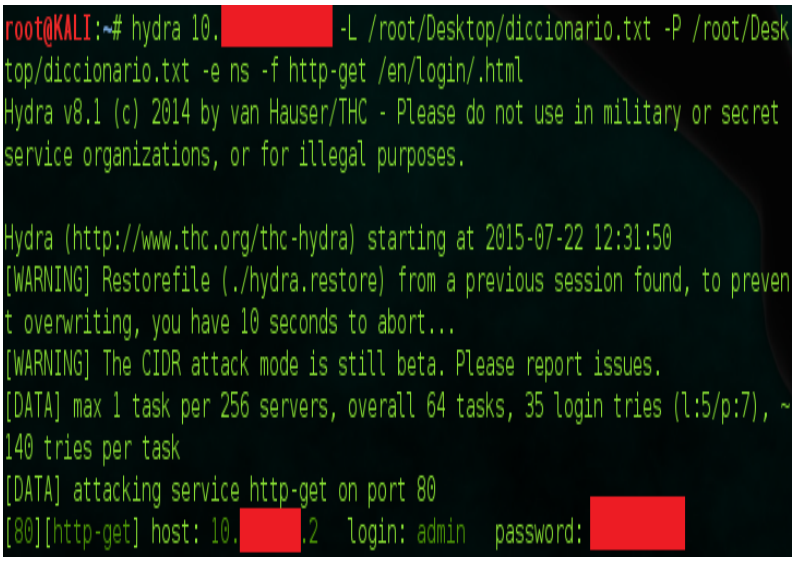


Ilustración 43: Descifrado de contraseñas por fuerza bruta con Hydra.
Fuente: El Autor (2015).

Los parámetros utilizados en medusa corresponden a la búsqueda de:

- *(–h):* Muestra esta página resumen de la ayuda.
- *(–U):* Busca el password.
- *(–P):* Sólo sondear los puertos indicados
- *(–e):* Utilizar la interfaz indicada
- *(–v):* Incrementa / Reduce el detalle (Más / Menos verboso)

- *(–F):* Analizar sólo los puertos listados en el archivo
- *(–M):* Indica que se detenga la búsqueda cuando se haya acercado. [7] [19]

```
[medusa –h 10.x.x.x –U /diccionario.txt –P /diccionario.txt –e ns –v 6
–F –M http-m DIR:GET/en/login.html]
```

Ilustración 44: Descifrado de contraseñas por fuerza bruta con medusa.
Fuente: El Autor (2015).

Las herramientas utilizadas, muestran el usuario y password de la víctima, a partir de las palabras del diccionario, sin embargo, solo se pudo descubrir el password de ciertos equipos, que tienen password muy sencillas o por defecto.

1.4.1. Identificar sistemas vulnerables a ataques de descifrado de contraseñas.

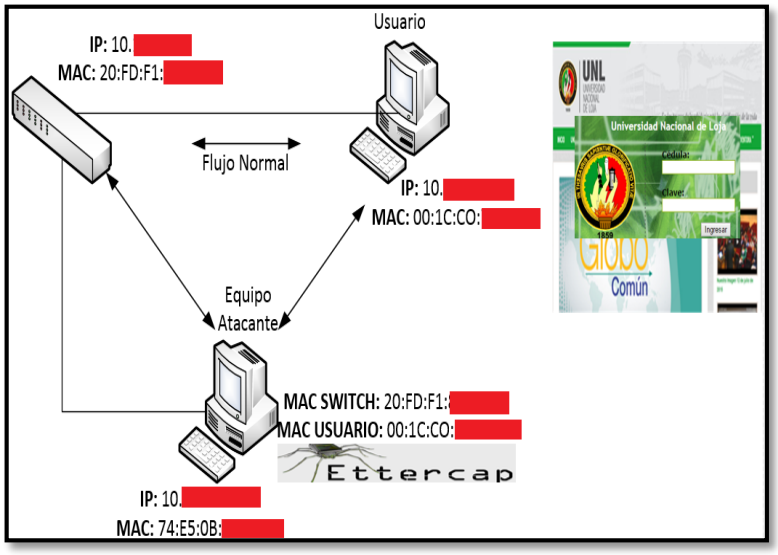


Ilustración 45: Esquema de red de descifrado de contraseñas.
Fuente: El Autor (2015).

Para poder realizar un test y verificar que sistemas son vulnerables, a un descifrado de contraseña se realizó un ataque *(MitM)*, a través de la herramienta *Ettercap***,** este ataque permitió obtener el usuario y password de los equipos de red a través de la conexión *(HTTP)*, desde un equipo del departamento de *(TIC)*. Para realizar el *sniffing* con *Ettercap*, se debe ingresar al menú, opción *Sniff*, ~~> *Unified Sniffing*, ~~> interfaz de red, ~~> modo monitor, a través del cual se captura el tráfico.

Ilustración 46: Activar Sniffing mediante Ettercap.
Fuente: El Autor (2015).

Para seleccionar los equipos fuente y destino de la transmisión que se va a capturar, se obtiene la lista de hosts pertenecientes a la red, se selecciona la *(IP)*, de la víctima, se coloca como destino 2 y el equipo servidor se coloca como destino 1.

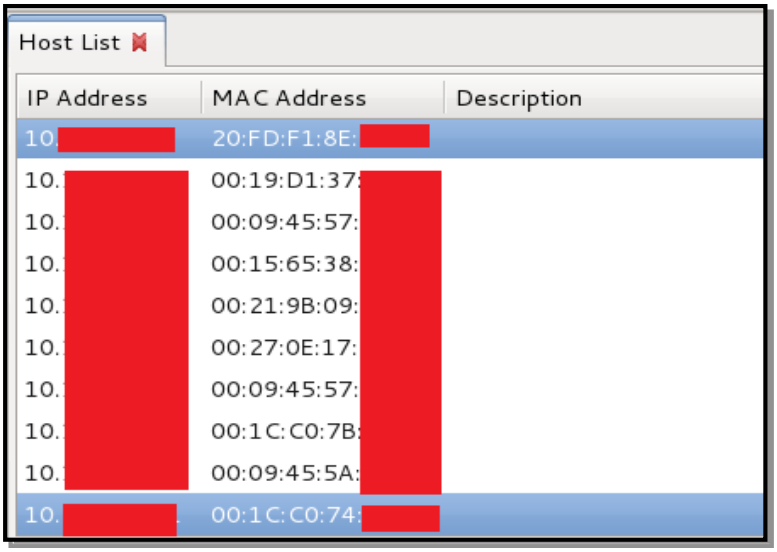


Ilustración 47: Ataque Man in the Middle con Ettercap.
Fuente: El Autor (2015).

En el menú ***(MITM),*** se selecciona la opción del atacante a realizar, en este caso *(ARP Spoofing).* Una vez realizado todo el proceso se debe esperar, hasta que la víctima intenta loguearse al equipo servidor o acceder a algún servicio. En el menú *view* se puede observar las conexiones realizadas así como los datos de cada transmisión y conexión.

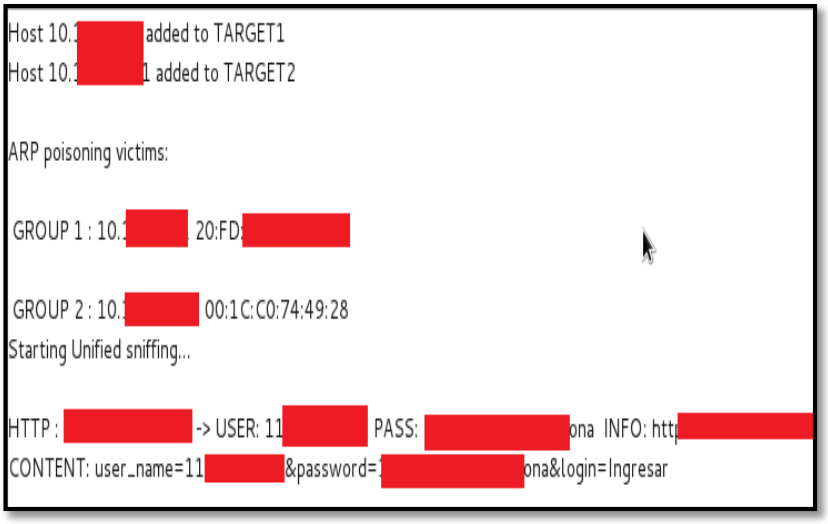


Ilustración 48: Descifrado de contraseñas, mediante ataque (MitM), con Ettercap.
Fuente: El Autor (2015).

Una vez realizado el test, se puede decir que el uso de protocolos, para el acceso a los equipos sin encriptación alguna, es una amenaza para la seguridad de los mismos y más aún cuando su administración se realiza desde la red, desde un usuario final.

1.4.2. Identificar sistemas de usuarios con las mismas contraseñas

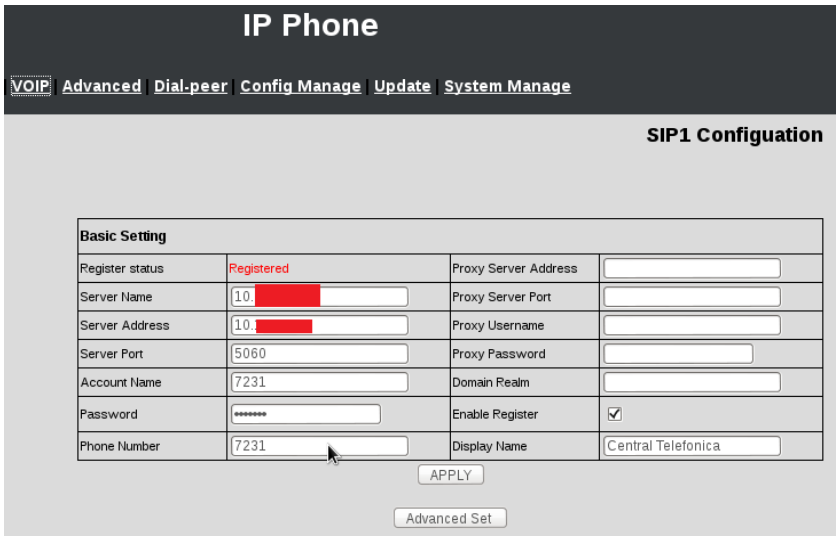


Ilustración 49: Equipos con la misma contraseña.
Fuente: El Autor (2015).

Utilizando el usuario y password descifrados, se obtuvo acceso a los equipos de red, esto permite corroborar la información proporcionada por el administrador de *(TIC)*, en las entrevista, acerca del uso, de la mismas contraseña para la mayoría de los equipos administrables de la red. En la imagen 50, se puede observar la configuración de un teléfono el cual fue encontrado con una contraseña muy básica y esta se repite en varios de ellos, si revisamos la tabla las extensiones de la *(PBX)*, sabremos que pertenece la central telefónica del Hospital, lo cual genera un altísimo riesgo, por lo que, un atacante puede ingresar a este equipo y empezar a sacar información referente al servidor, como: configuración de la red, códec y protocolos, además tendrá acceso al discado en el cual está funcionando el servidor de *(VoIP)*.

1.5. TESTEO DE DENEGACIÓN DE SERVICIOS.

En este apartado se intenta identificar, los sistemas que son vulnerables a ataques de degeneración de servicios, para este testeo se realizó dos tipos de ataques:

1.5.1. Ataque Smurff y SNY-flood, a través de herramienta Hping3.

En la red se puede observar, gran cantidad de tráfico broadcast que no es controlado, por esta razón se realizó el ataque Smurff, al servidor de voz, obteniendo como resultado la inundación de la red, con paquetes broadcast, dejando fuera de servicio al servidor de telefonía de *(VoIP)*.

```
[# hping3 -p 80 -S -flood 10.x.x.x.]
```

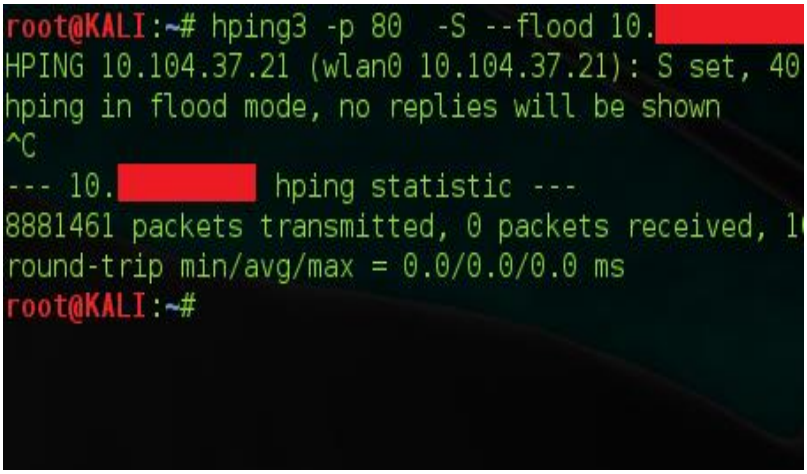


Ilustración 50: Ataque de (DoS) al servidor de (VoIP).
Fuente: El Autor (2015).

Las instrucciones para el ataque (*SNY-FLOOD)* en el router de Internet son las siguientes:

- *(–i) u20* Indica el intervalo de tiempo entre los paquetes enviados.
- *(–S)* El tipo de paquetes *(SNY).*
- *(–p)* Indica el puerto a donde se envía los paquetes.

Las instrucciones para el ataque (*SMURFF),* en el router de Internet son las siguientes:

- *(-1):* Para indicar el uso de protocolo *(ICMP).*
- *(-c):* 8 *(–k)* 0 un paquete tipo 8, código 0 es decir un *echo request* o *ping*.

```
[#hping3 -1 –C 8 –K 0 –spoof 10.x.x.x –flood 10.x.x.x]
```

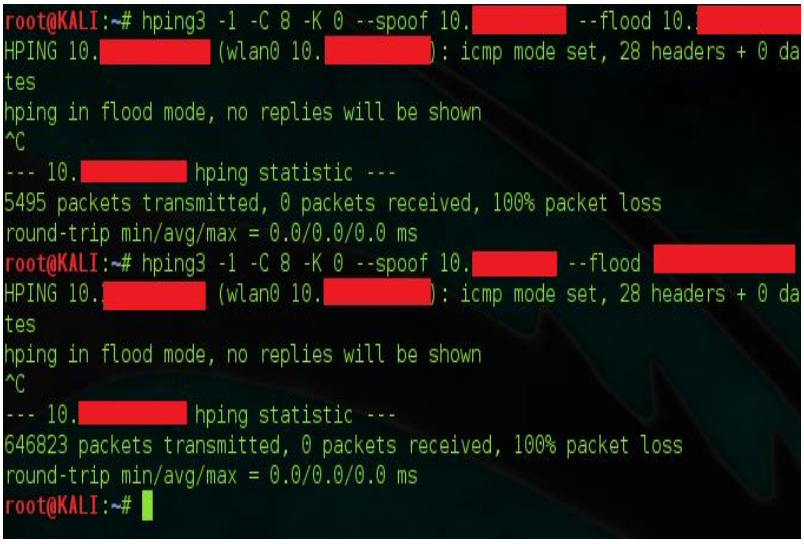


Ilustración 51: Ataque de (DoS) al servidor de (VoIP).
Fuente: El Autor (2015).

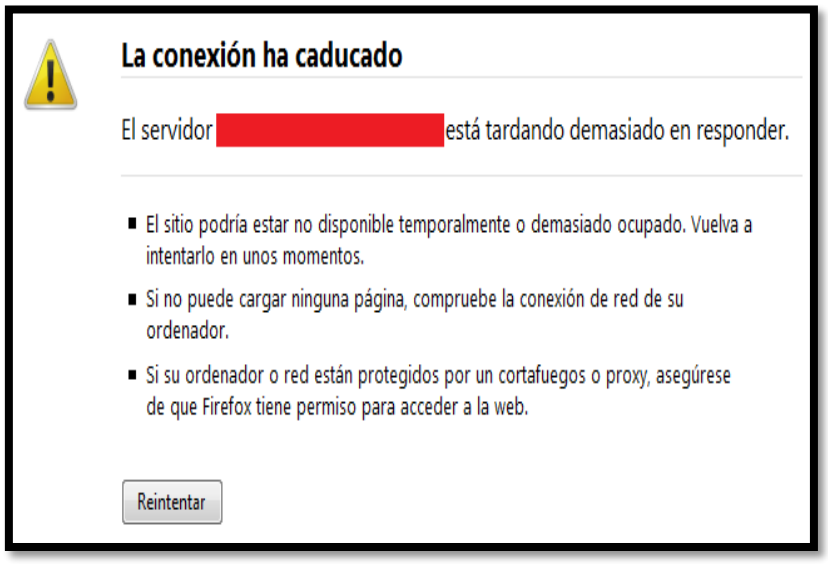


Ilustración 52: Servidor de voz colapsado por ataque (DoS).
Fuente: El Autor (2015).

Con la dirección de origen `10.x.x.x`, y el destino `10.x.x.x`, con la finalidad de que los equipos que reciben el mensaje broadcast respondan al servidor y colapse la red. El ataque culmina cuando suspendemos la instrucción con la combinación de teclas *Ctrl+C.* Los ataques de *(DoS),* utilizando el protocolo *(ICMP),* se puede controlar mediante el uso de una herramienta *(IDS)* que permita detectar en tiempo real, acciones inusuales en la red como el envío masivo de paquetes *echo ping.*

2. SEGURIDAD EN LAS COMUNICACIONES

Luego de haber conocido las vulnerabilidades, en los medios de transmisión, es decir en los equipos de red y en los servidores, en el siguiente apartado, se realiza un test para intentar vulnerar el servicio de *(VoIP),* es decir, veremos si es susceptible a capturas de llamadas en la red, para ello se agregaron dos extensiones en *Elastix,* denominadas prueba1 y prueba2, cuyo número es 3000 y 3001 respectivamente. Con el fin de no impedir la regularidad de las actividades diarias de los usuarios, se implementó el *software softphone,* denominado *zoiper***,** el cual emular un teléfono *(IP),* en un ordenador. El *softphone,* tiene los mismos servicios y vulnerabilidades de un teléfono físico, a través de estos, se procedió a realizar llamadas entre los dos y luego hacia el resto de extensiones del Hospital, con el fin de capturar una llamada y demostrar, si el sistema de *(VoIP),* es vulnerable a algún tipo de ataque o no.

2.1.Testeo de VoIP.

A continuación, se detalla los niveles de control de intercepciones en las comunicaciones, para esto se realizó el testeo de la *(VoIP),* con el uso de la herramienta *wireshark.* El método empleado corresponde a un ataque *(MitM),* el cual permite registrar todas las llamadas identificadas, durante el ataque. La voz transmitida es almacenada en tres archivos con formato *.wav,* tanto de emisor, receptor y la llamada completa. La captura del tráfico con *wireshark* durante el ataque *(MitM),* permite observar las llamadas realizadas a través del servidor de *(VoIP)* `(10.x.x.x)`.

La existencia de teléfonos en la *(VLAN)* de datos, permite fácilmente la intercepción de llamadas, una vez concluido el ataque, *wireshark,* crea un archivo con las direcciones *(IP)* y extensiones respectivas, que se puede utilizar para un ataque *(MitM), target mode,*

capturando llamadas entre dos teléfonos específicos. La transmisión de voz, a través de la red, sin contar con un protocolo de seguridad en el servidor, permite fácilmente la captura de la voz durante las llamadas.

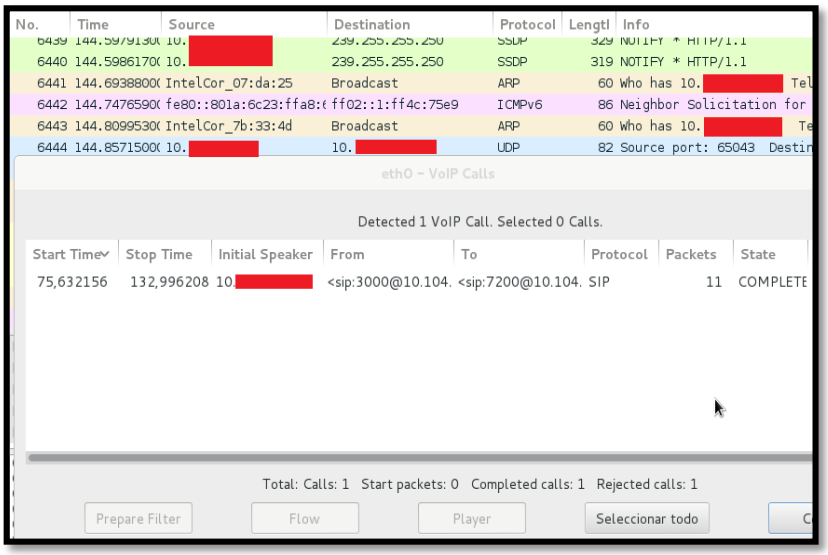


Ilustración 53: Captura de llamada con wireshark.
Fuente: El Autor (2015).

2.2.1. Análisis de los paquetes del protocolo SIP.

En este punto se realizara el análisis de la llamada capturada, entre dos softphones cuyo fin es conocer cómo se transmiten los paquetes por el protocolo *(SIP)* y *(RTP)*, sin encriptación alguna. Los mensajes *(SIP)* se componen de:

- Línea de inicio *(Start line)*
- Cabeceras *(Headers)*
- Cuerpo de mensaje (*Message body*)

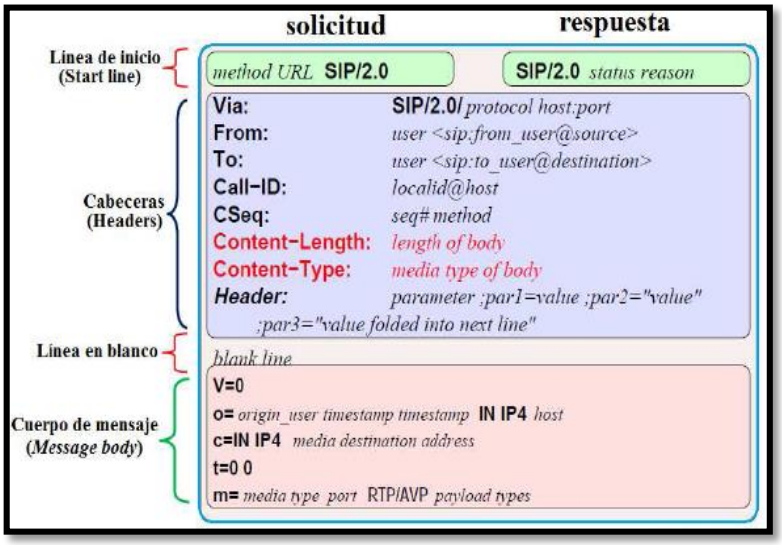


Ilustración 54: Formato del mensaje (SIP).
Fuente: Víctor Hugo López Chalacán (2011).

- **Línea de inicio (Start line)**

Todos los mensajes *(SIP),* comienzan con una línea de inicio. La línea de inicio transmite el tipo de mensaje tipo (*mensaje de solicitud*) / código de estado (*mensaje de respuesta)* y la versión del protocolo. La línea de inicio puede ser una línea de *Solicitud (Request-line, para solicitudes)* o una línea de *Estatus (Status-line, para respuestas),* de la siguiente manera:

  - La línea de *Solicitud* incluye una *(Solicitud-URI),* que indica a que usuario o servicio se está dirigiendo la solicitud, además incluye las direcciones involucradas en la sesión.

  - La línea de Estatus contiene el número del código de estatus (*Status-code*), y su frase textual asociada.

- **Cabeceras (Headers)**

En los campos de la cabecera del mensaje *(SIP),* transportan información necesaria a las entidades *(SIP),* información relacionada con la sesión en forma de texto, como por ejemplo indica las direcciones de origen y destino de la solicitud, identificador de llamada entre otros. También, en las cabeceras se transmiten los atributos del mensaje, que proporcionan información adicional acerca del mensaje. Estos campos son similares en la sintaxis y semántica a los campos de cabecera del mensaje *(HTTP), "de hecho, algunas cabeceras son tomadas del mensaje (HTTP)"* por lo tanto siempre tienen el siguiente formato: *<Nombre>: <Valor>*. Las cabeceras pueden abarcar múltiples líneas. Algunos campos de las cabeceras *(SIP),* son*: Via, From, To, Call-ID, CSeq, Contact, User-Agent, Content-Type, Content-Length* entre otros, a continuación se detallan algunos campos:

  - *Via*: Muestra el transporte utilizado para él envió, también identifica la ruta de solicitud, por lo tanto cada proxy server agrega una línea en este campo.
  - *From*: Indica la dirección del terminal origen de la solicitud.
  - *To*: Indica la dirección del terminal destino de la solicitud.
  - *Call-ID*: Es un identificador único para cada llamada e incluye la dirección del host, este debe ser el mismo para todos los mensajes de una transacción.

- *CSeq*: Es presentado por un número aleatorio, identificando la secuencia de transacciones, o de cada solicitud.
- *Contact*: Indica la o las direcciones que pueden ser utilizadas para contactarse con el usuario.
- *User Agent*: Indica el agente de usuario, cliente que realiza la transacción.

- **Cuerpo de mensaje (Message body)**

El cuerpo del mensaje o carga útil (*Payload*) se utiliza para describir la sesión que iniciará *"por ejemplo, en una sesión multimedia puede incluir los tipos de codecs de audio y video, también frecuencias de muestreo"*, es decir el cuerpo del mensaje que transporta información *(generalmente SDP).* Alternativamente puede ser utilizado para datos textuales o binarios de cualquier tipo, que tengan relación con la sesión. El cuerpo del mensaje puede aparecer tanto en mensajes de solicitud como en mensajes de respuesta. *(SIP)* hace una clara distinción entre la información de señalización, transmitido en la línea inicio y cabeceras del mensaje *(SIP).*

Tabla 34: métodos de solicitudes SIP (Requests).

NOMBRE	DESCRIPCIÓN
INVITE	Inicia una llamada, cambios en los parámetros de la llamada *(re-INVITE)*
ACK	Confirma una respuesta final para *(INVITE)*
BYE	Finaliza una llamada
CANCEL	Cancela las búsquedas y timbrando *(ringing)*
OPTIONS	Consulta parámetros de capacidades de negociación, del otro extremo de la llamada
REGISTER	Registra con el Servicio de la Ubicación
INFO	Envía información media de la sesión que no modifica el estado de la sesión

Fuente: Víctor Hugo López Chalacán (2011).

- **Invite**

El mensaje (*INVITE),* se utiliza para establecer una sesión multimedia entre dos o más agentes de usuario, es decir invita a un usuario *"al que se desea llamar"* para establecer una sesión. Este mensaje se envía desde el usuario llamante *(origen)* hacia el usuario llamado *(destino).*

- **Ack**

El mensaje (*ACK), "Acknowledgement o en español acuse de recibo"*, indica que: si ha llegado el mensaje y además ha llegado correctamente, dicho de otra manera,

confirma una respuesta final *"por ejemplo el mensaje (200 OK)"* para (*INVITE),* es decir para el establecimiento de una sesión, se utiliza el procedimiento llamado *saludo de tres vías* o negociación en tres pasos (*3-way handshake*), debido a la naturaleza asimétrica de la invitación. Se puede tomar un tiempo antes de que el usuario llamado *(destino)* acepta o rechaza la llamada, entonces el Agente de Usuario *(UA)* llamado, periódicamente retransmite una respuesta final positiva hasta que reciba un (*ACK),* enviado usuario llamante *(origen),* indica que el usuario llamante está presente, y listo para comunicarse. Este mensaje (*ACK)* es enviado como respuesta al mensaje (*200 OK).*

- **Bye**

El mensaje *(BYE)* se utiliza para finalizar las sesiones multimedia. El usuario que desee finalizar la sesión, envía un mensaje *(BYE)* al otro usuario integrante de la sesión.

- **Cancel**

El mensaje *(CANCEL)* es utilizado para cancelar una sesión que todavía no está completamente establecida. Este mensaje es aplicado cuando el usuario llamado (*destino*) aún no ha respondido con una respuesta final.
Por lo tanto el mensaje *(CANCEL)* se utiliza cuando el usuario llamante *(origen)* desea anular la llamada, *"típicamente cuando el usuario llamado no responde durante algún tiempo"*.

- **Options**

El mensaje *(OPTIONS)* se utiliza para consultar a un agente de usuario o servidor sobre sus capacidades y descubre su disponibilidad actual. Dicho de otra manera este mensaje solicita información acerca de sus propias capacidades. La respuesta a esta solicitud, lista las capacidades del agente de usuario o servidor.

- **Register**

El propósito del mensaje *(REGISTER)* es de permitir que el *(SIP Registrar Server),* conozca la ubicación actual del usuario. El mensaje *(REGISTER),* lleva información sobre la dirección *(IP)* actual y el puerto en que un usuario puede ser contactado.

En la tabla se detallan los códigos numéricos de respuestas, seguidamente de una pequeña descripción del código correspondiente.

Tabla 35: Códigos de respuestas. (SIP)

NÚMERO	SIGNIFICADO
100	Trying *(Recibí y estoy procesando la llamada)*
180	Ringing (El terminal está timbrando)
200	OK *(Atendí la llamada)*
300	Multiple choices *(Múltiples opciones)*
301	Moved permanently *(Movido permanentemente)*
302	Moved temporarily (Movido temporalmente)
400	Bad request *(Solicitud incorrecta)*
401	Unauthorized *(No autorizado)*
403	Forbidden *(Prohibido)*
408	Request time-out *(Solicitud tiempo de espera)*
480	Temporarily unavailable (Temporalmente no disponible)
481	Call/Transaction does not exist *(La llamada/transacción no existe)*
482	Loop detected *(Bucle o lazo detectado)*
500	Server error *(Error del servidor)*
600	Busy everywhere *(Ocupado en todas partes)*
603	Decline *(Declive o descenso)*
604	Does not exist anywhere *(No existe en ninguna parte)*
606	Not acceptable *(No aceptable)*

Fuente: Víctor Hugo López Chalacán (2011).

2.2.1.1.Análisis de los paquetes trasmitidos por el protocolo (SIP) en una llamada.

Este escenario de prueba se presenta en la figura 55, donde se realiza el siguiente procedimiento:

- Empieza la captura de paquetes mediante *Wireshark.*
- Se realiza una llamada entre dos *Softphone (PhonerLite).*
- Se finaliza la llamada.
- Se detiene la captura de paquetes.

Tabla 36: funcionamiento: Llamada entre dos Softphone

Direcciones IP		**RTP Streams**				
Fuente	Destino	Paquetes	Perdidos	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)
192.168.143	192.128.1.127	4833	0(0,0%)	33,02	2,87	0,73

Fuente: El Autor (2015).

Para obtener gráficamente el flujo de mensajes en una llamada *(VoIP)*, se selecciona *Telephony* en el menú principal de *Wireshark*, posteriormente se selecciona *(VoIP Callsn)*

a continuación se escoge la llamada *(VoIP)* y se selecciona *Graph*, obteniendo como resultado la siguiente ventana:

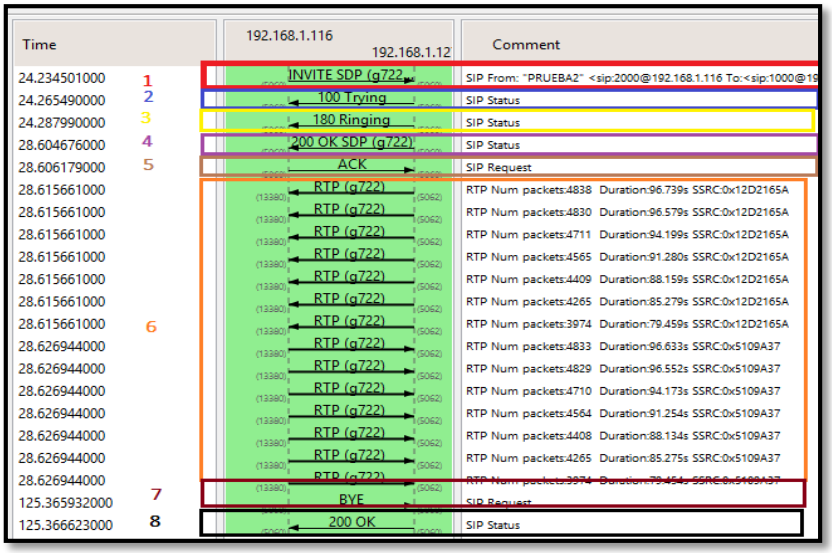


Ilustración 55: Flujo de mensajes en una llamada (VoIP): ventana Graph Analysis.
Fuente: El Autor (2015).

La figura anterior presenta el intercambio teórico de mensajes *(SIP)*, para una mejor explicación se ha señalado en recuadros de colores cada fase del mensaje *(SIP)*.

- El recuadro roja muestra el establecimiento de la llamada, se empieza con un mensaje (*INVITE)* por parte del *Softphone. (SIP)*, para el control de señalización de llamada utiliza *Session Description Protocol (SDP)*, se envía conjuntamente con los mensajes (*INVITE)* y (*200OK)*, cabe aclarar que: el mensaje (*INVITE)* se envía desde el origen hacia el destino, y el mensaje (*200OK)*, se envía desde el destino hacia el origen. Como se mencionó el protocolo *(SDP)* se encuentra embebido en *(SIP)*, donde usualmente los puertos utilizados por *(SIP)* son: el *(5060)*, en texto plano *(UDP* y *TCP)* y el puerto (*5061)*, en el caso de *(TLS)*. Dentro del mensaje *(SDP)*, se envían los parámetros a negociar como por ejemplo el listado de *Codecs* que soporta o está en la capacidad de trabajar tanto el terminal de origen como destino, este códec se envía en orden de prioridad *(g722)*. También se envía la *(IP)*, el puerto que se desea recibir el audio mediante *(RTP)*.

- En el recuadro azul se muestra el mensaje después de recibir la solicitud (*INVITE)*, se envía un mensaje de respuesta (*100 Trying), "recibí y estoy procesando la llamada"*, esto lo realiza para detener las retransmisiones del mensaje (*INVITE)*.

- Luego en el recuadro amarillo donde se señala el mensaje de respuesta (*180 Ringing), "el terminal está timbrando",* esta respuesta es generada cuando el teléfono empieza a timbrar.

- En el recuadro violeta esta la aceptación de la comunicación, se retransmite un mensaje de respuesta (*200OK), "atendí la llamada"*, con un mensaje *(SDP)*, proponiendo el codec a utilizarse (*g722*), hacia el usuario origen.

- En el recuadro café representa al usuario destino reciba un mensaje de confirmación *(ACK), "atendí la llamada"*, enviado por el usuario de origen.

- En el recuadro tomate se establece la conversación mediante el envío de paquetes *(RTP), "audio/video (RTP) streams"*. Adicionalmente, en ciertos casos el terminal de origen confirma la negociación con un mensaje (*ACK).*

- En el recuadro color lila se representa la finalización de la llamada, se lleva a cabo mediante el envío del mensaje de solicitud (*BYE)* dentro del diálogo establecido por (*INVITE).* El mensaje (*BYE)* se envía directamente desde un agente de usuario hacia el otro agente de usuario. El usuario que desea finalizar la sesión, envía la solicitud (*BYE),* directamente al otro usuario involucrado en la sesión.

- Finalmente en el recuadro de color negro se representa al usuario que recibe la solicitud (*BYE),* envía una respuesta *(200OK),* para confirmar la finalización de la sesión *(SIP).*

En el establecimiento de la llamada, es el primer mensaje enviado es (*INVITE),* el cual se lo representa en la imagen 56, el encabezado de la trama *Ethernet* de la capa de Enlace, se resalta en el recuadro superior de color verde, donde se observa que el protocolo utilizado es *Ethernet*. El término "*Ethernet*" se refiere a la familia de implementaciones de *(LAN)* una de las tres principales categorías es: *10 Mbps Ethernet e IEEE 802.3*: especificaciones *(LAN)* que operan a 10 Mbps sobre cable coaxial. En la captura es posible observar los campos de la trama *(MAC)* 802.3: dirección destino (*destination 6 bytes*), dirección de origen (*source 6 bytes*), *Tipo/Longitud, (especifica el protocolo de red que encapsula, la IP).* Dirección *(MAC)* de destino: `74:e5:0b:07: xx: xx`, dirección *(MAC)* de origen: `00:19:21:25: xx: xx`, tipo/longitud: `08 00`.

Los campos del encabezado de *(IP)*, se representan en el recuadro de color amarillo por ejemplo: dirección fuente: `192.168.xxx` *(dirección IP de la computadora, la cual generó el datagrama)*, dirección *(IP)* destino: `192.168.1.xxx` *(servidor VoIP)*, entre otros.

La capa de transporte se encuentra en el recuadro rojo donde se presenta el encabezado con sus respectivos campos del mensaje *(UDP)*, este contiene: el puerto origen: *5060*, puerto destino: *5060*, entre otros.

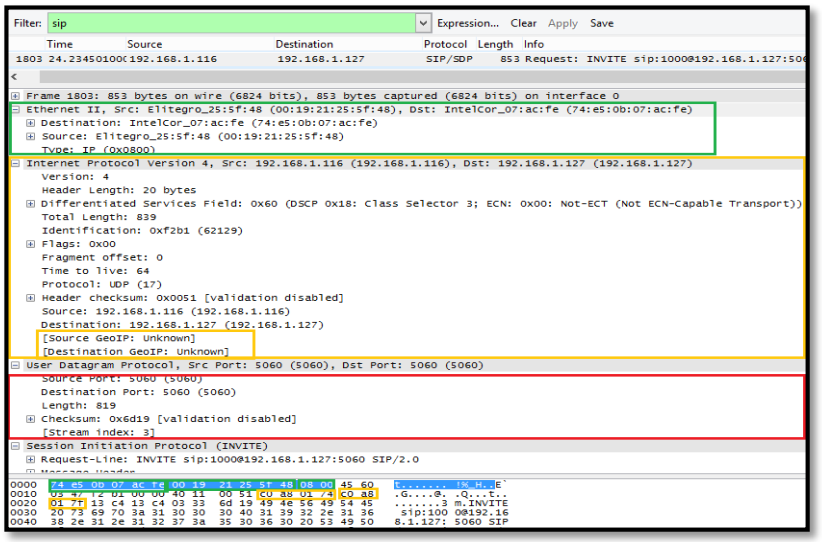


Ilustración 56: Captura del mensaje (INVITE).
Fuente: El Autor (2015).

El siguiente mensaje que se envía como respuesta al mensaje (*INVITE)* anterior, es el mensaje (*TRYING)*, el cual está representado en la captura anterior.

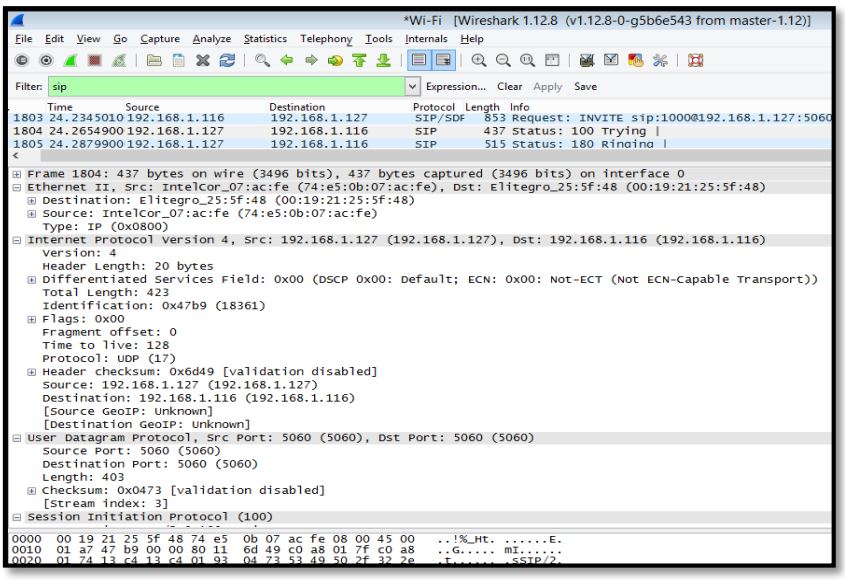


Ilustración 57: Captura del mensaje (TRYING).
Fuente: El Autor (2015).

En el nivel de enlace se observa que los campos de las direcciones *(MAC)* fuente y destino invertidas, puesto que la trama viajan en sentido inverso, desde el servidor *(VoIP)* hacia el *Softphone*. De la misma forma las direcciones *(IP)* y puertos *(UDP)* han sido invertidas. El siguiente mensaje que se envía es el mensaje (*RINGING)*, el sentido de este datagrama es el mismo que el mensaje anterior (*Trying*), a continuación se presenta el mensaje.

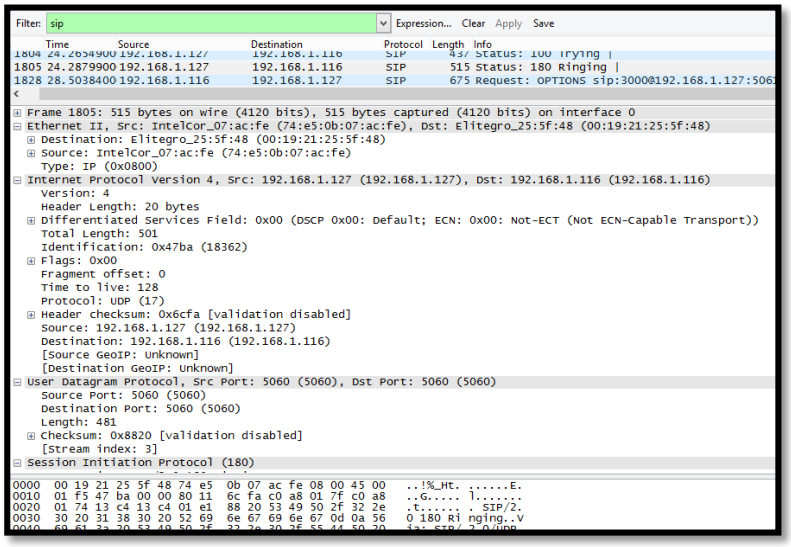


Ilustración 58: Captura del mensaje (RINGING).
Fuente: El Autor (2015).

Los campos de direcciones *(MAC, IP* y puertos *UDP)*, son los mismos que el mensaje anterior (*Trying*), puesto que el mensaje viaja en el mismo sentido, desde el servidor *(VoIP)* hacia el *Softphone*. El siguiente mensaje que se envía es el mensaje (*200OK)*, enviado desde el servidor *(VoIP)*, a continuación se presenta la captura de este mensaje.

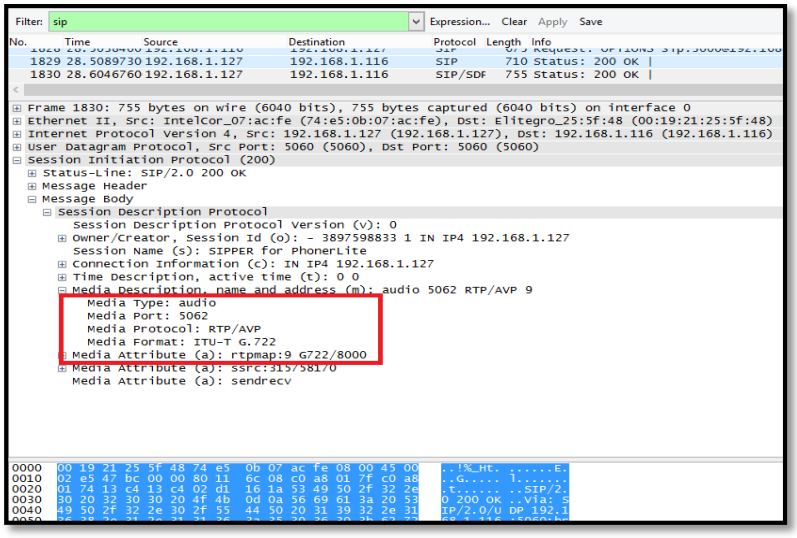


Ilustración 59: Captura del mensaje (200 OK).
Fuente: El Autor (2015).

El mensaje de respuesta (*200 OK) "atendí la llamada"* tiene la función de confirmar que acepta la llamada. Esta respuesta (*200OK),* contiene un mensaje *(SDP),* encapsulado en *(SIP),* con el propósito de confirmar el codec que será utilizado en la comunicación. En este caso el codec se confirma el *(G.722).*

El siguiente mensaje que se envía es *(ACK) (atendí la llamada),* enviado desde el Softphone, con el propósito de confirmar los diferentes valores de los campos enviados en el mensaje *(INVITE).* A continuación se presenta estos campos, los cuales coinciden entre los dos mensajes (*INVITE* y *ACK*) de la misma transacción *(SIP).*

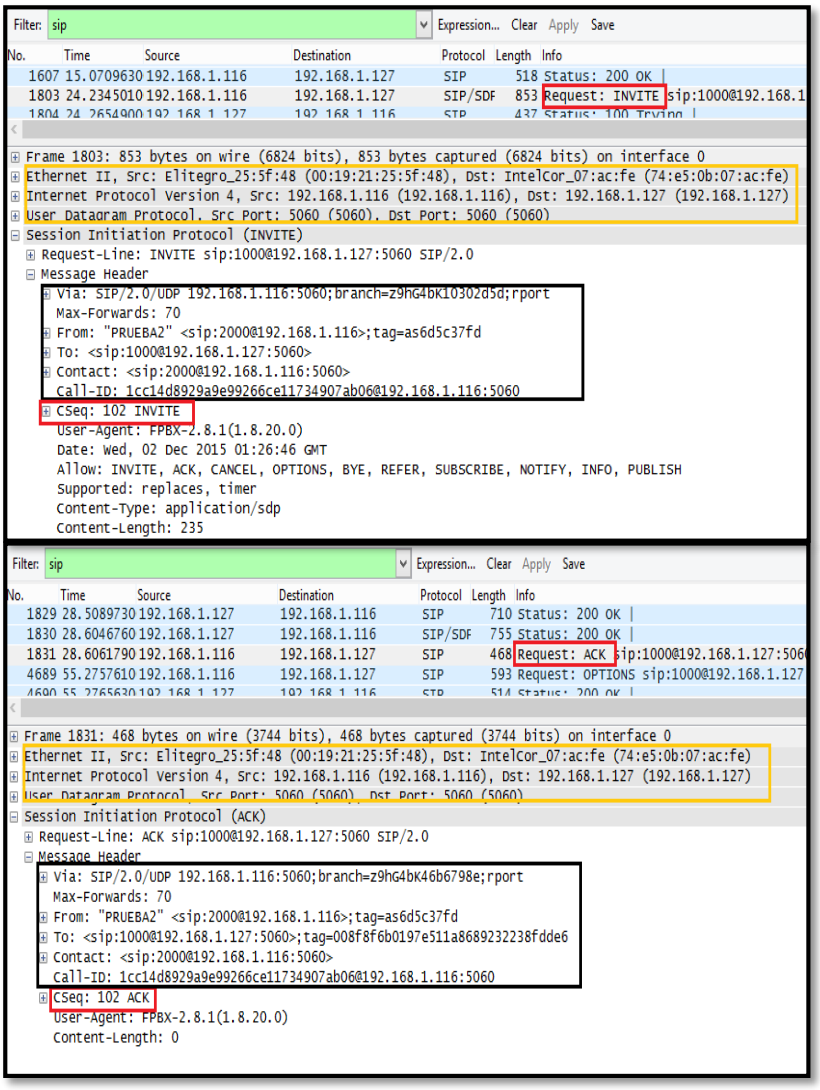


Ilustración 60: Comparación entre los mensajes (INVITE y ACK).
Fuente: El Autor (2015).

En este punto se establece la conversación o el intercambio de audio, mediante el envío de paquetes *(RTP).*

A continuación se presenta el intercambio de paquetes *(RTP),* en los dos sentidos de la conversación.

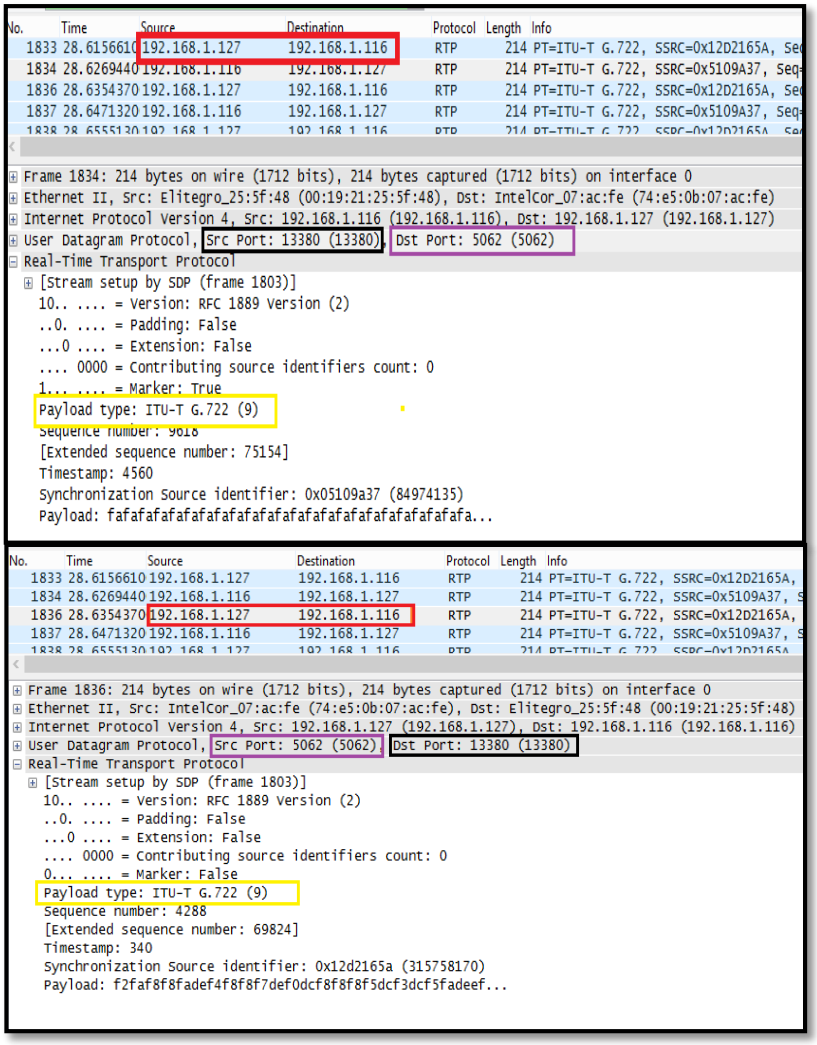


Ilustración 61: Intercambio de paquetes (RTP), en los dos sentidos de la conversación.
Fuente: El Autor (2015).

Para la finalización de la llamada, se lleva a cabo mediante el envío del mensaje de solicitud (*BYE),* en el cual se finalizó la llamada desde el *Softphone,* en la figura 62 se presenta la captura del mensaje (*BYE).*

El usuario que recibe la solicitud (*BYE),* envía una respuesta (*200OK),* para confirmar la finalización de la sesión *(SIP),* como se presenta en la figura 63.

Cabe mencionar que estas capturas de estos paquetes se lo realizo en el servidor de pruebas tal como se puede apreciar las direcciones *(IP)* corresponde a una (LAN)

improvisada con el fin de no interrumpir el funcionamiento del servidor activo en la institución.

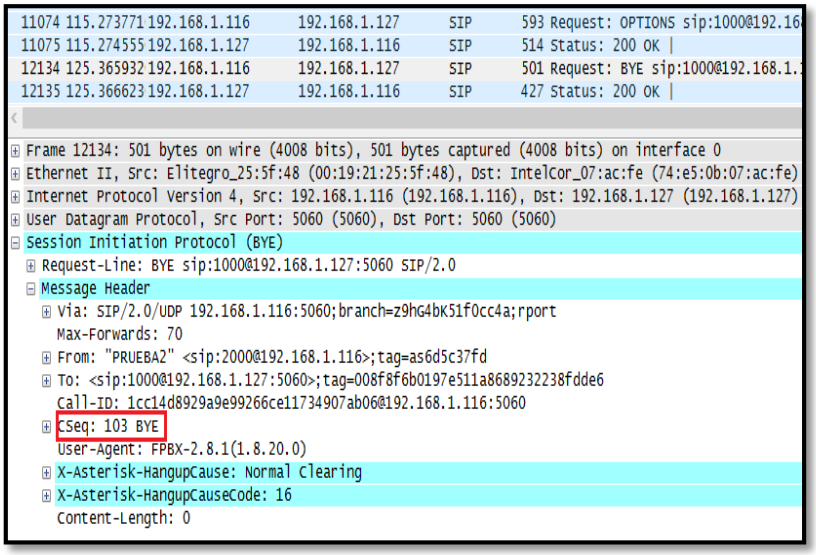


Ilustración 62: Captura del mensaje (BYE).
Fuente: El Autor (2015).

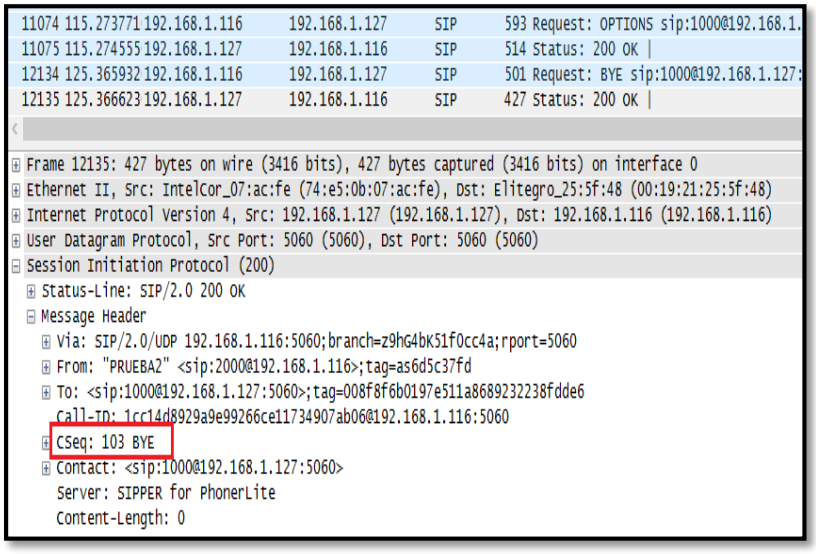


Ilustración 63: Captura del mensaje (200 OK).
Fuente: El Autor (2015).

Luego del análisis realizado finalmente se presenta las vulnerabilidades a las cuales está expuesta la red de *(VoIP)*, del Hospital Isidro Ayora de Loja.

Tabla 37: Resumen de los ataques que está expuesta la red (VoIP), del Hospital.

#	ATAQUE	DESCRIPCIÓN
1	**Puertos innecesarios abiertos.**	El servidor *Asterisk (VoIP)*, cuenta puertos abiertos, los cuales se los una vulnerabilidad, producida por una instalación por defecto.
2	**Descifrado de contraseñas por ataque de fuerza bruta**	La red *(VoIP)* es propensa a un descifrado de contraseñas por contar con contraseñas por defecto o fáciles de descifrar, producidas por la configuración por defecto de la central *Elastix*.

3	**Firewall deshabilitado**	El firewall de *Elastix* se encuentra deshabilitado, por lo que el servidor esta propenso a infinidad de ataques.
4	**Captura de tráfico *(VoIP)***	La red *(VoIP)* actualmente cuenta con el protocolo *(SIP* sin *TLS)* lo que facilita la captura de paquetes, de los cuales se puede obtener los hash *(MD5),* de las contraseñas. Mediante el uso de una de las múltiples herramientas que existen.
5	**Denegación de servicios *(DoS)***	La red *(VoIP),* está expuesta a ataques de *(DoS)* por inundación (flooding), mismos que afectan la operatividad y los servicios, estos ataques incluyen la inundación de dispositivos telefónicos, con una serie de andanadas de paquetes *(TCP), (SNY/UDP).*
6	**Interpretación de la comunicación *(Eavesdropping)***	El servidor de *(VoIP)* del Hospital es propenso a ataques *Eavesdropping* tal como se lo demuestra en la captura de audio de las llamadas a esta técnica también se la denomina *Man-in-the-Middle (MitM).*

Fuente: El Autor (2015).

6.5. FASE 3: DESARROLLO DE ESTRATEGIAS DE SEGURIDAD.

En esta fase, se desarrolla un análisis, para identificar el nivel de riesgos de activos críticos, ante las amenazas identificadas en las fases anteriores, y en base a este, plantear las estrategias eficientes y necesarias para mitigar los riesgos.

6.5.1. Proceso 5. Realizar un análisis de riesgo.

El análisis de riesgos, determina la rigurosidad de las amenazas y su impacto sobre los activos, en base a ciertos criterios de evaluación. Este estudio permite elaborar un plan de seguridad lógica, para la red de datos de la Institución, con el fin de solventar los problemas encontrados en la misma y mejorar sus servicios.

6.5.1.1.Criterios de evaluación.

El criterio de evaluación, se determina para valorar el impacto de la ocurrencia de una posible amenaza, sobre los activos críticos encontrados.

- **Probabilidad**

  La presente tabla, describe los valores de probabilidad, de ocurrencia de una amenaza, sobre los activos críticos.

Tabla 38: Criterios de valoración de probabilidad de amenazas.

VALOR	FRECUENCIA DE OCURRENCIA
Alto (3)	Más de 12 veces por año.
Medio(2)	De 2 a 11 veces por años
Bajo(1)	Una vez por año

Fuente: El Autor (2015).

El valor de la probabilidad asignado en la matriz de riesgos se fija en base al conocimiento del administrador y observación directa.

- **Impacto**

Para determinar el impacto, sobre la ocurrencia de una amenaza se han considerado 3 factores principales: *"revelación, pérdida/destrucción e interrupción"*. Los criterios de la valorización de impacto se describen en la siguiente tabla.

Tabla 39: Matriz de criterios para la evaluación de probabilidades y amenazas.

IMPACTO	CRITERIOS DE VALORACIÓN		
	ALTO = 3	**MEDIO = 2**	**BAJO = 1**
REVELACIÓN	Conocimiento de la información contenida en los activos o su configuración por personas no autorizadas.	Conocimiento del estado de los activos de red. Conocimientos de las características de los activos	No se contabilizan daños físicos ni lógicos en los activos
PÉRDIDA / DESTRUCCIÓN	Puede existir el riesgo de pérdida irrevocable de información que se está transmitiendo en la red en el momento del colapso. Existe un alto riesgo de pérdida de información contenida en los servidores. Pérdida irrevocable de la confianza de autoridades y personal en la funcionalidad de las aplicaciones	Daños reparables a los equipos de red o servidores. El personal al igual que las aplicaciones que dependen del funcionamiento de los servidores pierden productividad por algunas horas hasta solucionar el problema	Daños a los equipos bajos o nulos. Pérdida de productividad de aplicaciones y/o persona en el rango de minutos. Los servicios que dependen del Internet se ven mínimamente afectados
INTERRUPCIÓN	Pérdida completa de la disponibilidad de los equipos de la red y servidores. La mayoría del personal del hospital no puede realizar tareas que dependan de la disponibilidad del activo. Disponibilidad nula del servicio de Internet en la institución. No disponibilidad de servicios que dependan del uso del Internet.	Pérdida de disponibilidad de la red y equipos de conectividad por algunas horas. Servicios que dependen del uso del Internet se ven parcialmente afectados	Pérdida en la disponibilidad de la red por pocos minutos

Fuente: El Autor (2015).

6.5.1.2.Estimación del riesgo

En base a los criterios de evaluación ya definidos, se determina la matriz de riesgo, misma que se construyó a partir de las amenazas identificadas, en los activos críticos de la red. El riesgo obtenido, es el producto de la probabilidad de ocurrencia de la amenaza y la

magnitud del daño o impacto, sobre los activos de las comunicaciones, se ha coloreado el valor de riesgo, para poder clasificar el nivel de riesgo según el impacto. El departamento de *(TIC),* determinará las acciones a tomar: controlar, eliminar, compartir o aceptar el riesgo en base a un plan de estrategias, el nivel de riesgos se presenta en base a los siguientes valores:

Tabla 40: Criterio de valoración de riesgos.

RIESGO	VALOR	ACCIÓN
Alto	6 – 9	Se debe dar tratamiento de vulnerabilidades de forma inmediata.
Medio	3 – 4	El riesgo puede ser controlado.
Bajo	1 – 2	El riesgo puede ser aceptado.

Fuente: El Autor (2015).

La valoración de los activos se la realizó en base a las entrevistas realizadas, a personas conocedoras del tema, personal del departamento de (*TIC)* y en base a la observación directa, para un mejor detalle de la valoración de riesgos de los activos de *software* y *hardware* ***(ver anexo G)***, en los cuales, la mayoría de amenazas presentan un nivel de riesgo medio y bajo, debido a que no se han presentado incidentes de este tipo, aunque no se descarta la posibilidad de ocurrencia de alguna de estas amenazas, por lo que deben ser tratadas en un caso de estudio diferente, debido a que esta investigación está enfocada a la seguridad de las comunicaciones, en la siguiente tabla, se muestra la valoración de los riesgos en la comunicación.

Tabla 41: Matriz de riesgos a los activos de comunicación.

ACTIVOS DE COMUNICACIÓN				
AMENAZAS	**PROBABILIDAD**	**IMPACTO**		**RIESGO**
Puertos innecesarios abiertos	2	Revelación	2	4
		Pérdida –Destrucción	1	2
		Interrupción	2	4
Descifrado de contraseñas por ataque de fuerza bruta	3	Revelación	3	9
		Pérdida –Destrucción	1	3
		Interrupción	2	6
Firewall deshabilitado	2	Revelación	3	6
		Pérdida-Destrucción	2	4
		Interrupción	3	6
Captura de tráfico *(VoIP)*	2	Revelación	2	4
		Pérdida-Destrucción	2	4
		Interrupción	2	4
Denegación de servicio	2	Revelación	1	2
		Pérdida –Destrucción	2	4
		Interrupción	3	6
Interceptación de las comunicaciones *(Eavesdropping)*	3	Revelación	3	9
		Pérdida-Destrucción	2	6
		Interrupción	2	6

Fuente: El Autor (2015).

Los riesgos que predominan, en los activos de comunicación son: ***(descifrado de contraseñas, denegación de servicios e interpretación de la comunicación)***, se los definió como altos, porque todo el personal que se encuentra laborando en la institución, realizan intercomunicaciones con una constancia muy alta, con el fin de agilizar sus tareas, un ejemplo de ello es la funcionalidad de la central telefónica, por ser el medio de transmisión de mensajes al personal médico, administrativo, técnico, entre otros. Así mismo, a través de este servicio, se realiza la recepción de turnos, por parte de los pacientes, por lo que, si se prescinde de este servicio, sería un riesgo muy alto para la entidad.

6.5.1.3.Valoración de riesgos a los ataques más frecuentes en las redes VoIP.

Con el fin de realizar, un trabajo eficiente y fructífero, centrándose en lineamientos comprobados, se realizó una investigación de los ataques con mayor incidencia y los más frecuentes, en la tecnología de *(VoIP)*, se los comparó con los resultados obtenidos en la simulación de ataques en la red de *(VoIP)*, con el fin, de considerar los ataques de más alto riesgo y solucionarlos en el diseño del esquema de seguridad lógica que se va a implantar, cabe señalar que la definición completa de cada ataque, y cómo se da la valoración del impacto, amenaza y riesgo de los ataques *(VoIP)*, se encuentra en el ***(anexo H)***. [8] [11]

Tabla 42: Valoración de riesgo de los ataques con mayor incidencia en las redes (VoIP).

ATAQUE	PROBABILIDAD	IMPACTO	RIESGO	C	I	D
Enumeración *(DNS o Footprinting)*	Alta	Bajo	Medio			x
Indexado de equipos	Alta	Bajo	Medio	x		
"Banner-grabbing" o *(fingerprinting)*	Alta	Bajo	Medio	x	x	x
"Brute-force" de extensiones	Alta	Medio	Alto	x	x	
"Brute-force" de contraseñas	Alta	Alto	Alto	x	x	
Fallas conocidas y "0-days"	Baja	Alto	Medio			x
"Spoofing"	Baja	Bajo	Bajo	x		
(DDoS) por inundación	Media	Alto	Alto			x
Malware	Media	Alto	Alto	x		
Ataque con paquetes *(INVITE)*	Media	Baja	Bajo		x	x
Escuchas ilegales *(eavesdropping)*	Media	Alto	Alto	x		
Cracking de contraseñas	Media	Alto	Alto	x	x	
Manipulación/interrupción de las comunicaciones	Baja	Medio	Medio		x	x
Servidores *(TFTP)*	Media	Alto	Alto		x	
Salto entre *(VLAN)*	Baja	Alto	Media	x	x	

(SPIT)	Media	Bajo	Bajo		x	
Vishing	Media	Alto	Alto	x	x	
Botnet *(SIP)*	Baja	Alto	Media			x
OccupyPhones	Baja	Medio	Medio			x
Ataques *(DTMF)*	Baja	Alto	Medio	x	x	x

Fuente: El Autor (2015).

En la tabla 39, se muestra un resumen, de la valoración de riesgos, con el fin de conocer los ataques con el riesgo más alto y buscar las vulnerabilidades que conlleven a estos incidentes, cuyos ataques que contienen, una incidencia más baja o mediana, se los dará a conocer al administrador de la red, para que sean tomados en cuenta, porque al perpetuarse uno de ellos, puede causar daños similares a los catalogados en la prioridad alta.

6.5.1.4.Valoración de riesgos a los ataques encontrados en la red VoIP del Hospital.

A continuación, se realiza una valoración de los vulnerabilidades encontradas en la red *(VoIP)*, del Hospital Isidro Ayora de Loja, descritos en la tabla # 37, junto con los riesgos más altos, descrito en la tabla anterior, con el fin, de solventar estos incidentes y evitar la interrupción de sus servicios por ende, las actividades propias de la institución, , lo cual significaría una pérdida económica, caos entre los usuarios y desprestigio para la casa de salud, al verse perjudicada por dichos incidentes.

Tabla 43: Comparación de ataques en la redes (VoIP) con la red (VoIP) del Hospital.

ATAQUE	ATAQUE A LA RED VOIP DEL HOSPITAL	PROBABILIDAD	IMPACTO	RIESGO
Enumeración *(DNS).*	NO	Alta	Bajo	Medio
Indexado de equipos	NO	Alta	Bajo	Medio
"Banner-grabbing" o *(fingerprinting)*	SI	Alta	Medio	Alto
"Brute-force" de extensiones	SI	Alta	Medio	Alto
"Brute-force" de contraseñas	SI	Alta	Alto	Alto
Fallas conocidas y "0-days"	NO	Baja	Alto	Medio
"Spoofing"	NO	Baja	Bajo	Bajo
(DDoS) por inundación	SI	Media	Alto	Alto
Malware	NO	Media	Alto	Alto
Ataque de paquetes *(INVITE)*	NO	Media	Baja	Bajo
Eavesdropping	SI	Media	Alto	Alto
Cracking de contraseñas	SI	Media	Alto	Alto
Manipulación/interrupción de las comunicaciones	SI	Baja	Medio	Medio
Servidores *(TFTP)*	NO	Media	Alto	Alto

Salto entre *(VLAN)*	NO	Baja	Alto	Media
(SPIT)	NO	Media	Bajo	Bajo
Vishing	NO	Media	Alto	Alto
Botnet *(SIP)*	NO	Baja	Alto	Media
OccupyPhones	NO	Baja	Medio	Medio
Ataques *(DTMF)*	NO	Baja	Alto	Medio

Fuente: El Autor (2015).

En la siguiente tabla, se realiza un resumen de los ataques que van a ser solucionados, por ser considerados con el riesgo más alto.

Tabla 44: Listado de ataques que se dará seguridad en la red de VoIP.

ATAQUE A LA VOIP	ATAQUE A LA VOIP DEL HOSPITAL	PROBABILIDAD	IMPACTO	RIESGO
"Banner-grabbing" o *(fingerprinting)*	SI	Alta	Medio	Alto
"Brute-force" de contraseñas	SI	Alto	Alto	Alto
(DoS) por inundación	SI	Media	Alto	Alto
Eavesdropping	SI	Media	Alto	Alto
Cracking de contraseñas "Brute-forc"	SI	Media	Alto	Alto
Captura de tráfico	SI	Medio	Alto	Alto
Puertos innecesarios abiertos.	SI	Alto	Bajo	Alto
Firewall deshabilitado	SI	Alto	Alto	Alto

Fuente: El Autor (2015).

Una vez detallado el funcionamiento del protocolo *(SIP)* y *(RTP)*, es decir como es el intercambio de mensajes dentro de un llamada y luego de haber identificado plenamente las vulnerabilidades con el riesgo más crítico *(Alto)* ya sea en el servidor o en la red *(VoIP)*, del Hospital Isidro Ayora es necesario definir las contramedidas que se pueden implementar para dar soluciones definitivas o contrarrestar, este tipo de incidentes que se generan actualmente, para poder mantener el sistema seguro, sin olvidar que ninguno hará que el sistema tenga la seguridad total deseada. En la siguiente tabla, se expone las soluciones para contrarrestar las vulnerabilidades cabe mencionar que el eje fundamental de nuestra investigación es la implementación de protocolos para cifrar la voz razón por la cual se realizara un detalle más excautivo en dicha configuración.

Tabla 45: Listado de ataques que se dará seguridad en la red de (VoIP).

#	ATAQUE	DESCRIPCIÓN
1	**Interpretación de la comunicación (Eavesdropping)**	Para dar solución a este inconveniente se debe implementar protocolos de seguridad *(TLS o IPSec)* los cuales garantizan la integridad de la información debido a que se transmiten por canales cifrados de comunicación.
2	**Descifrado de contraseñas por ataque de fuerza bruta (fáciles o intuitivas).**	Para dar solución a esta vulnerabilidad se debe cambiar los parámetros del archivo de configuración "sip.conf", y se debe establecer contraseñas más robustas con un mínimo de 8 dígitos, combinados entre letras, números y caracteres especiales, así mismo se debe asegurar el protocolo SSH.

3	**Firewall deshabilitado**	Debido a que la central brinda un módulo de seguridad que incluye un Firewall es evidente y lógico que deberíamos usarlo para protegernos de una infinidad de ataques.
4	**Captura de tráfico *(VoIP)***	La solución a esta vulnerabilidad se contrarresta con la implementación de protocolos de seguridad ya que actualmente los paquetes no cuenta con seguridad alguna, es decir, el texto se transmite por el protocolo *(SIP* sin *TLS)* lo que facilita la captura de paquetes, de los cuales se puede obtener los hash *(MD5)*, de las contraseñas, mediante el uso de una de las múltiples herramientas que existen.
5	**Denegación de servicios *(DoS)***	El *(DoS)*, se genera por las vulnerabilidades descritos en los ítems anteriores, debido a ello las soluciones son las mismas que se utilizan para contrarrestar los ataques de los ítems anteriores, además de ellos debe configurar o descargar la herramienta *FAIL2BAN* misma que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por fuerza bruta
6	**Puertos innecesarios abiertos.**	La solución más apropiada en este caso es cerrar los puertos innecesarios, podemos realizarlos a través de la configuración manual de iptables o con la herramienta firewall de Elastix.

Fuente: El Autor (2015).

6.5.2. Proceso 6. Desarrollar estrategias de protección.

Una estrategia de protección involucra las iniciativas que utiliza la Institución, para implementar y mantener la seguridad interna, para establecer una estrategia adecuada es conveniente pensar en políticas de protección, de los distintos niveles: físicos lógicos y humanos, cuya interacción que existe entre estos factores determinaran el grado de seguridad que cuenta dicha organización.

El objetivo de una estrategia es proporcionar una guía a través de un conjunto de pasos para dar solución y elevar los niveles de seguridad de la red, más no para encontrar una solución inmediata a cada vulnerabilidad o preocupación de la seguridad.

6.5.2.1. Elección del protocolo de seguridad para la red de VoIP de Hospital Isidro Ayora de Loja.

Como ya se mencionó el punto neurálgico de esta investigación es implementar protocolos de seguridad para encriptar la voz, razón por la cual, antes de empezar con las medidas de seguridad se debe realizar un análisis de los protocolos idóneos para acoplarlos a las características de la red, por ello en la sección de la revisión literaria ya se describió las características y funcionamiento de los protocolos *(IPSec)* y *(SSL/TLS)*, pues en este apartado se tomará las características más relevantes y se las compara según la necesidad y funcionalidad de la red.

En la tabla se describe un resumen de las características más relevantes, con el fin de elegir el perfil más adecuado y poder cubrir las vulnerabilidades encontradas, cuyo objetivo es *encriptar* las llamadas y proteger la central *(VoIP)*, del Hospital Isidro Ayora, cabe mencionar que la comparación completa de las características de los protocolos se encuentran en el **(Anexo I).**

Tabla 46: Comparativa de los protocolos de seguridad (IPSec) y (TLS).

PROTOCOLO	TLS	IPSEC
Puede transportar *(VoIP).*	x	x
Fácil Implementación	x	
Transporte de mensajes seguros	x	
Encriptar *(VoIP).*		x
Forma un túnel entre los extremos por donde la información viajará de forma segura		x
Diseñado como protocolo de comunicación	x	
Transmitir y recibir llamadas		x
Permite asignaciones seguras entre emisor y receptor		x
Utiliza encriptación para mantener la seguridad		x
Conexiones permanentes		x
Conexiones efímeras o puestos móviles	x	
Todos los usuarios han de tener acceso a todos los recursos de la red		x
Deseamos controlar el acceso a determinadas aplicaciones	x	
Precisamos de un alto nivel de seguridad en el cifrado y autenticación	x	x
La confidencialidad y autenticidad no son especialmente críticas en nuestros sistemas	x	
Tiempo de Handshake	Lento	Rápido
Throughput	Alto	Medio
Interoperabilidad	Alto	Medio
Velocidad de transferencia	Alto	Medio
Vulnerabilidades	Media	Baja

Fuente: El Autor (2015).

De acuerdo a las características analizadas en la tabla anterior, se deduce que el protocolo *(IPSec)*, es el mejor para implementar medidas de seguridad en el las comunicaciones *(VoIP)*, mismo que permite establecer un túnel de encriptación, para él envió de los paquetes *(IP).* [17]

Sin embargo, según la infraestructura de la red analizada, no soporta la configuración de dicho protocolo, así mismo, por el elevado costo que resultaría para la institución adquirir un equipo con las características necesarias para la implementación de este protocolo, razón por la cual, se toma el protocolo *(SSL/TLS)*, para ser implementado y de esta forma poder cifrar la *(VoIP)*, en las comunicaciones, debido a que *(SSL/TLS)*, posee características muy similares *(IPSec)*, las cuales se detalla continuación:

- El protocolo *(SSL/TLS)*, se acopla a las características y funcionalidad de la red, además no requiere realizar ninguna modificación en los equipos de distribución de la red, porque se lo puede configurar directamente en el servidor de *(VoIP).*

- *Elastix* es un sistema operativo basado en *Linux*, es una versión compilada de *Asterisk* y *(FreePBX)*, en el cual ya están generados los *scripts*, para la configuración de *(SSL/TLS)*, que es soportada por teléfonos físicos y *softphones*.

- Establece un canal seguro de comunicación, antes que este empiece la transmisión de los datos, formando así, un túnel entre los dos extremos de la comunicación, por ende el emisor y receptor, mantiene integra la información.

- Permite que los paquetes sean cifrados y no estén en texto plano, con lo cual se previene que las conversaciones telefónicas, no puedan ser escuchadas, por personas ajenas a la misma.

- Con la correcta configuración del protocolo *(TLS)* y en el servidor asterisk se previene ataques como y análisis de trafico debido que los paquetes se trasmiten encriptados, es decir, El protocolo *(SIP)*, se transmite cifrado el objetivo principal de *(TLS)* es contrarrestar uno de los ataques más comunes dentro de *(VoIP):*

    - *Eavesdropping. (Hombre en el medio (MitM))*

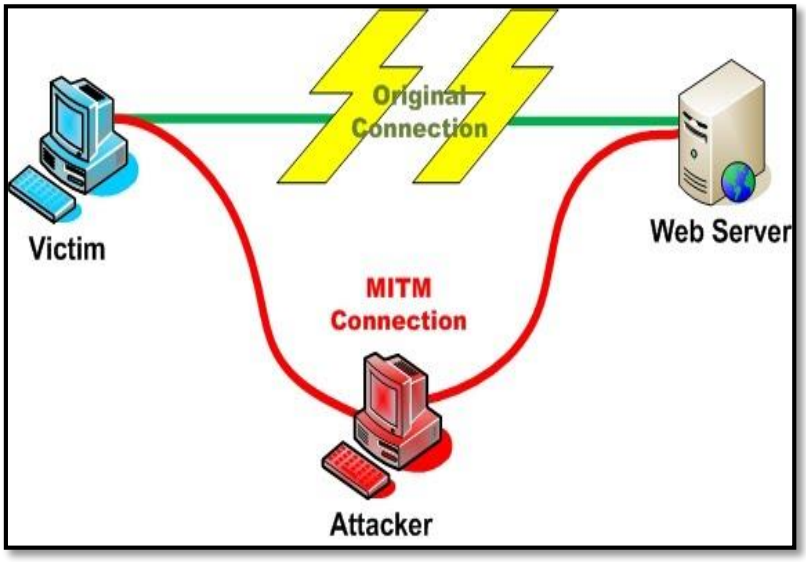


Ilustración 64: Ataque de hombre en el medio (MitM)
Fuente: El Autor (2015).

1. IMPLEMENTACIÓN LAS MEDIDAS DE SEGURIDAD

Una vez conocida la situación actual de la red *(VoIP)*, del Hospital Isidro Ayora de Loja, haber conocido las vulnerabilidades y haber definido las medidas de seguridad, para contrarrestarlas, en el siguiente apartado se procede con la implementación del protocolo de seguridad *(SSL/TLS)*, para cifrar las comunicaciones en el servidor *Asterisk*, con lo cual se pretende contrarrestar las escuchas en la red o el eavesdropping

1.1. CONFIGURACIÓN DEL ESCENARIO DE PRUEBAS (PROTOTIPO)

Para no interrumpir el servicio de las telecomunicaciones *(VoIP)*, en el Hospital Isidro Ayora, ya que la configuración es de prueba/error por ciertas descargas y actualizaciones de librerías y *script* se realizó la implementación de las medidas de seguridad en un escenario de pruebas, simulando un área de trabajo, en caso de que alguna configuración no funcionara de acuerdo con lo esperado. El material necesario, para la implementación es el siguiente:

- Un servidor con la misma versión del sistema operativo del servidor *(VoIP)*, que está siendo utilizada actualmente en el Hospital Isidro Ayora de Loja.
- Dos computadores para que sirvan como clientes.
- Dos teléfonos *(IP)* que soporten *(SSL/TLS)*.
- Una computadora para acceso al servidor
- Un router para crear una red LAN.

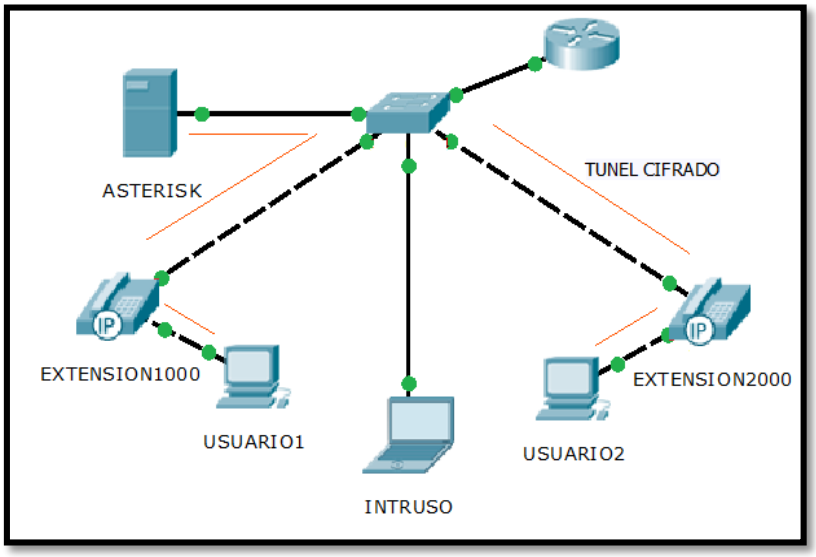


Ilustración 65: Prototipo del escenario de pruebas.
Fuente: El Autor (2015).

1.2. CONFIGURACIÓN DE (SSL/TL) EN ASTERISK.

Para contar con las mismas configuraciones, se realizó un *backup* del servidor *(VoIP)* que está en funcionamiento, para implementarlo en el servidor de pruebas, se ingresa a *Elastix*, en la pestaña *Sistema*, opción *Backup/Restore*, *Desarrollar un respaldo*, tal como se muestra en la siguiente imagen.

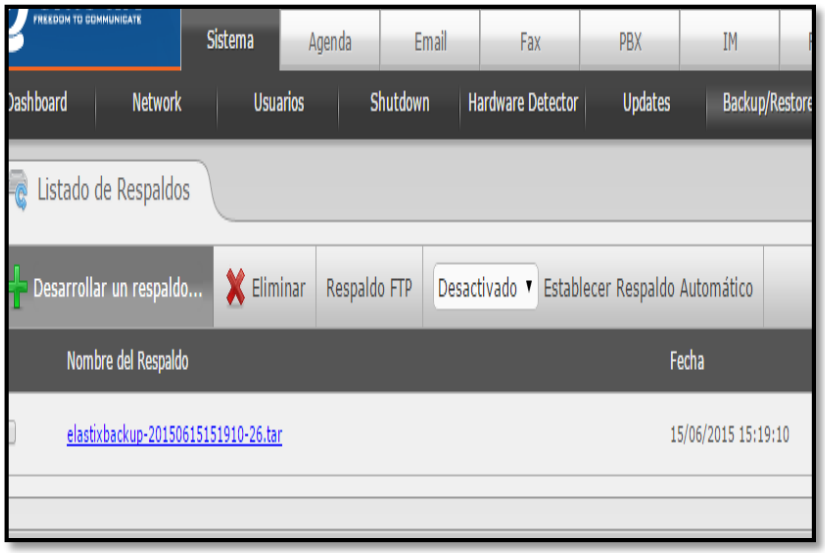


Ilustración 66: Realizar un backup del servidor Elastix
Fuente: El Autor (2015).

Para extraer el *backup* del servidor, se lo hace mediante el programa *WinSCP*, tal como se muestra en la imagen, en el cual hay que configurar la *(IP)*, del dominio, el usuario y clave root.

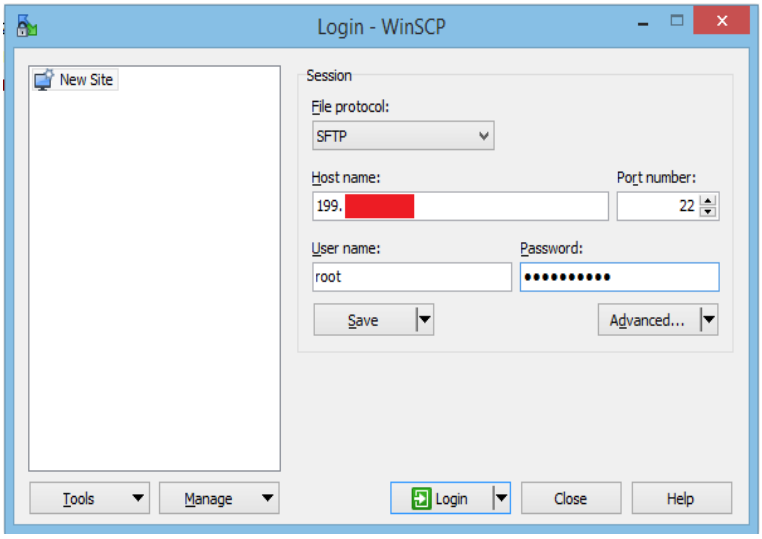


Ilustración 67: Interfaz de WinSCP para el ingreso al servidor.
Fuente: El Autor (2015).

WinSCP, posee una interfaz muy intuitiva, en la parte derecha se busca el *backup* generado que se encuentra en: *etc/www/html/backup*, mientras que en la parte izquierda, se guarda el archivo presionando *(F5)*, tal como se muestra en pantalla.

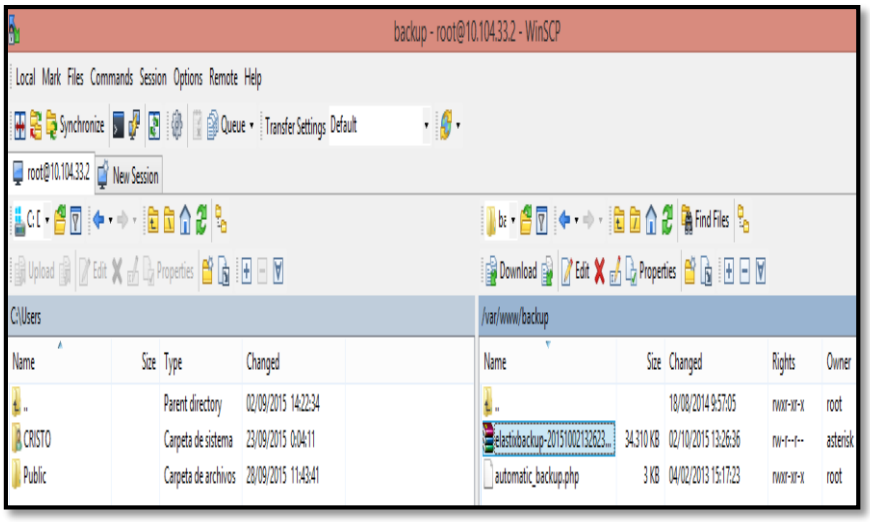


Ilustración 68: Traslado del backup del servidor al ordenador.
Fuente: El Autor (2015).

Para subir el *backup* al servidor de pruebas, se realiza el mismo proceso, se ingresa con *WinSCP* a la dirección: *etc/www/html/backup* y se presiona *(F5)*, luego se ingresa a *Elastix*, en la pestaña *Sistema*, opción *Backup/Restore*, debe aparecer el archivo con una *extencion.rar*, seleccionar y presionar *Restore*, con eso se tiene la misma configuración en los dos servidores, para un detalle más completo de cómo realizar un *backup* en *Elastix* ir a la siguiente dirección electrónica: [http://elastixtech.com/como-clonar-un-servidor-elastix/.](http://elastixtech.com/como-clonar-un-servidor-elastix/)

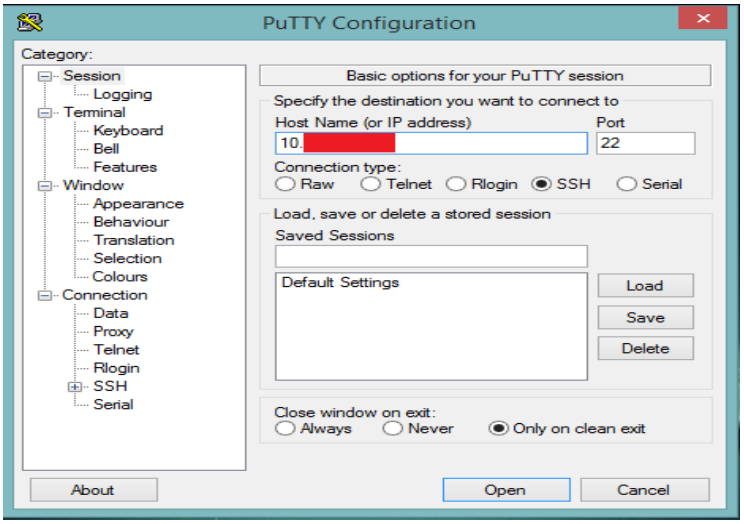


Ilustración 69: Interfaz de PuTTy para el acceso al servidor.
Fuente: El Autor (2015).

Antes de empezar con la configuración es aconsejable utilizar el *software PuTTy*, el cual, permite ingresar de forma remota al servidor *Asterisk*, facilitando el ingreso de comandos, para arrancar *PuTTy*, es necesario colocar la *(IP)*, del servidor, accediendo por el puerto 22 *(SSH)* y loguearse como usuario root, tal como se muestra en la siguiente imagen:

1.2.1. Configuración del protocolo (SSL/TLS) en la plataforma (Asterisk).

Una vez listo el escenario de pruebas se procede con la configuración de *(SSL/TLS)*, en *Asterisk*. Para ello se debe realizar lo siguiente:

- Modificar el fichero `functions.inc.php`.
- Configuración del cifrado en el servidor Asterisk.
- Configuración del protocolo *(SSL/TLS)*, en Elastix.
- Configurar la encriptación para clientes locales.
- Configurar la encriptación para clientes locales.

1.2.1.1.Modificación del script functions.inc.php

Por defecto en *Elastix*, no se presentan los campos *(encryption y transport)* que son campos fundamentales, para la encriptación en las extensiones. Para visualizar estos campos, se lo hace asignando parámetros adicionales de programación, para que acepte la configuración y no altere la funcionalidad de *Asterisk*, esta modificación se realiza en el *script* `functions.inc.php` que se encuentra en el siguiente path:

```
#vim /var/www/ html/admin/modules/core/functions.inc.php
```

Se recomienda hacer una copia del archivo antes de editarlo, si algo sale mal durante la configuración, se puede volver a copiarlo y restaurar de nuevo el sistema. Una vez abierto este archivo, aproximadamente en la línea 3800, se tiene los siguientes parámetros de programación:

```
array($account,'deny',$db>escapeSimple((isset($_REQUEST['deny']))?$_RE
QUEST['deny']:''),$flag++),
array($account,'permit'$db>escapeSimple((isset($_REQUEST['permit']))?$
_REQUEST['permit']:'')$flag++),
array($account,'disallow',$db>escapeSimple(sset($_REQUEST['disallow'])
?$_REQUEST['disallow'],$flag++),
array($account,'allow',$db>escapeSimple((isset($_REQUEST['allow']))?$_
REQUEST['allow']:''),$flag++),
```

A continuación de estas líneas se debe ingresar el siguiente código:

```
array($account,'encryption',$db>escapeSimple((isset($_REQUEST['allow']
))?$_REQUEST['allow'])$flag++),
array($account,'transport',$db>escapeSimple((isset($_REQUEST['allow'])
)?$_REQUEST['allow']:'')$flag++),
```

La inserción de estas líneas de código, sirven para poder cifrar la información y que se transporte por una línea segura, es decir, se establece un canal cifrado para la comunicación, una vez realizado estos cambios, se debe ubicar aproximadamente en la línea 6014, del mismo archivo donde se tiene: [20]

```
$tmparr['deny'] = array('value' => '0.0.0.0/0.0.0.0','level' => 1);
$tmparr['permit'] = array('value' =>'0.0.0.0/0.0.0.0','level'=> 1);
```

A continuación de estas líneas se agrega el siguiente código:

```
$tmparr['encryption'] = array('value' => 'no', 'level' => 1);
$tmparr['transport'] = array('value' => 'udp', 'level' => 1);
```

El cual permite realizar la encriptación y el modo de transporte que se verá reflejado en Elastix, al momento de crear una extensión, una vez hecho estas modificaciones se guardan los cambios para continuar con la configuración. En resumen, lo que se ha establecido con esas dos modificaciones, es agregar dentro del formulario *(HTML)* y del archivo `sip_additional`, los campos *encryption y transport* que son utilizados para la configuración de extensiones. [20]

1.2.1.2.Configuración del cifrado en el servidor Asterisk.

El siguiente paso, es la creación de una autoridad de certificación, tanto para el servidor como para el cliente. *Asterisk*, cuenta con los *scripts* necesarios para compilar los certificados de seguridad, haciendo una autenticación de quienes se afilian a estos certificados firmados y codificados según la configuración de *Asterisk*, para el cifrado de *(SIP)* y *(RTP)*, los *scripts* están dentro de la documentación de *Asterisk*, cuyo path es:

```
"cd /usr/share/doc/asterisk-1.8.20.0/contrib/scripts"
```

Para guardar la (*CA)*, en el servidor se crea una carpeta denominada `"certs"`, *(dentro de la dirección antes mencionada)*, sin salir de esta dirección se debe ejecutar lo siguiente:

```
. /ast_tls_cert –d certs –C tesis.hial.com –o tesis.hial.com
```

Donde:

- `-C`: Es el nombre *(DNS)* o dirección *(IP)*, de la organización Matriz.
- `-O`: Nombre del objetivo, similar al objetivo al redactar un correo en *Outlook.*
- `-d`: Nombre de salida hacia un directorio especificado.

Con esto se genera el certificado de autorización, en la siguiente imagen, se muestra todos los pasos realizados hasta ahora.

```
[root@tesis ~]#
[root@tesis ~]# cd /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/
[root@tesis scripts]# ./ast_tls_cert -d certs -C tesis.hial.com -o tesis.hial.com

No config file specified, creating 'certs/tmp.cfg'
You can use this config file to create additional certs without
re-entering the information for the fields in the certificate
Creating CA key certs/ca.key
Generating RSA private key, 4096 bit long modulus
.....................................................................++
.................++
e is 65537 (0x10001)
Enter pass phrase for certs/ca.key:
Verifying - Enter pass phrase for certs/ca.key:
Creating CA certificate certs/ca.crt
Enter pass phrase for certs/ca.key:
Creating certificate certs/tesis.hial.com.key
Generating RSA private key, 1024 bit long modulus
......++++++
..++++++
e is 65537 (0x10001)
Creating signing request certs/tesis.hial.com.csr
Creating certificate certs/tesis.hial.com.crt
Signature ok
subject=/CN=tesis.hial.com/O=Asterisk
Getting CA Private Key
Enter pass phrase for certs/ca.key:
Combining key and crt into certs/tesis.hial.com.pem
[root@tesis scripts]#
```

Ilustración 70: Código para la creación de los certificados.
Fuente: El Autor (2015).

Una vez, que empiece a crear el certificado de autorización, se debe ingresar una clave para cada uno de los siguientes archivos.

- `ca.key`.
- `ca.crt`.
- `tesis.hial.com.pem`.
- `tesis.hial.com.crt`

Cabe mencionar que el archivo `tesis.hial.com.pem`, es combinado con el archivo `tesis.hial.com.crt`, en la imagen anterior, se puede apreciar los archivos creados para la certificación. El contenido de cada archivo se lo detalla a continuación:

`.pem` = La extensión `pem` se utiliza para diferentes tipos de archivos que contienen `ASCII` *(Base64)* datos blindados prefijo a - línea "*BEGIN...*".

`.crt` = La extensión `crt` se utiliza para los certificados. Los certificados pueden ser codificados como `der` binario o como `ASCII pem`. Las extensiones `cer` y `crt` son casi sinónimos. Lo más común entre los sistemas Unix. [21]

.key = La extensión key se utiliza tanto para PKCS pública y privada. Las claves pueden ser codificados como der binario o como ASCII pem.

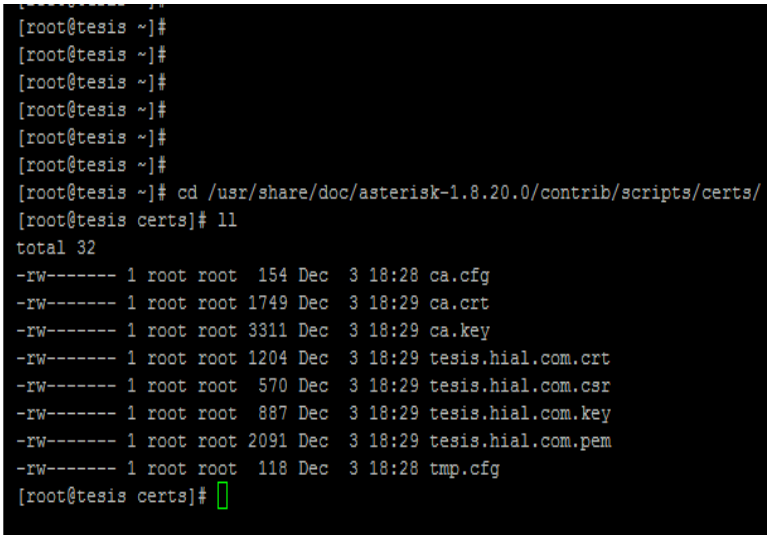


Ilustración 71: Archivos generados por las certificaciones
Fuente: El Autor (2015).

Si, se desea copiar estos archivos, se lo realiza con el programa *WinSCP* o montando una *(USB)*, en el servidor, para este último proceso se tiene un detalle completo en la siguiente dirección electrónica https://www.voztovoice.org/?q=node/103.

Una vez creado el certificado de autorización, se debe setear el *(fqdn)*, en servidor, para ello se modifica el archivo "/etc/hosts", este archivo contiene la configuración por defecto, por lo que se debe agregar la dirección *(IP)*, del servidor y el nombre del dominio.

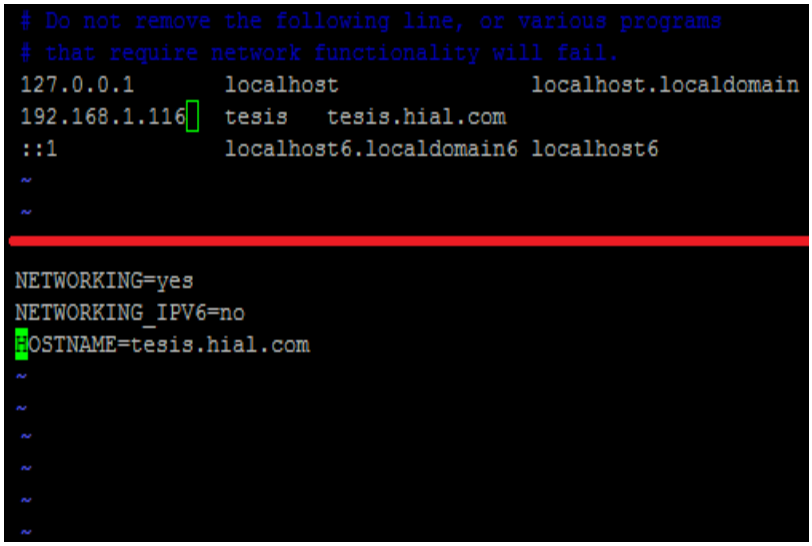


Ilustración 72: Modificación del archivo Host y Network indicando la dirección o dominio del servidor.
Fuente: El Autor (2015).

Así mismo, se debe modificar el archivo "`/etc/sysconfig/network`", en el cual se cambia el campo **NETWORKING = *no***, por **NETWORKING = *yes***, finalmente en el **HOSTNAME**, se debe ingresar la *(IP)* o dominio tal como se indica en la figura 71 y se guardan los cambios.

Una vez generados los certificados tanto para la autoridad de certificación, como para el servidor, el siguiente paso que se debe hacer es, copiar los archivos generados a la carpeta *keys* de *Asterisk*. Una vez copiados estos archivos, se debe dar los permisos de lectura y escritura *(cambiar de propietario),* para que *Asterisk* los pueda cargar; esto se realiza con el siguiente código.

```
#cp certs/ca.crt /var/lib/asterisk/keys
#cp certs/tesis.hial.com.pem /var/lib/asterisk/keys
#chown –R asterisk:asterisk /var/lib/asterisk/keys/*
```

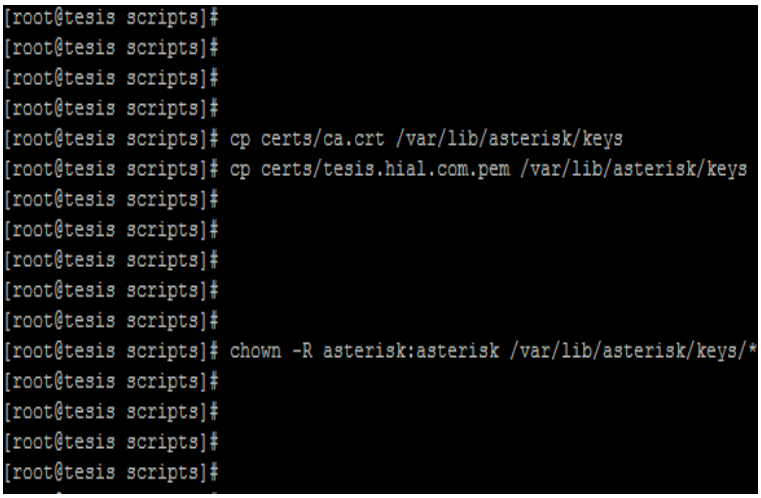


Ilustración 73: Copiar y dar permisos de lectura y escritura los certificados de autorización.
Fuente: El Autor (2015).

Con esto termina la configuración de *(SSL/TLS),* desde *Asterisk*, ahora se debe aplicar y activar los cambios en Elastix, para ello hay que hacer lo siguiente:

1.2.1.3.Configuración del protocolo (SSL/TLS) en Elastix.

Para aplicar las modificaciones realizadas, se ingresa a *Elastix* y se habilita el acceso al *(FreePBX),* no embebido, esto se hace en la pestaña *Security -> Advanced Options -> Enable access to FreePBX -> ON,* para habilitar este campo se requiere de una autenticación, la cual es necesaria para loguearse en la *FreePBX*.

Para ingresar en la *(FreePBX)*, se lo hace desde una nueva pestaña del navegador, agregando siguiente comando: ***https://10.x.x.x/admin***

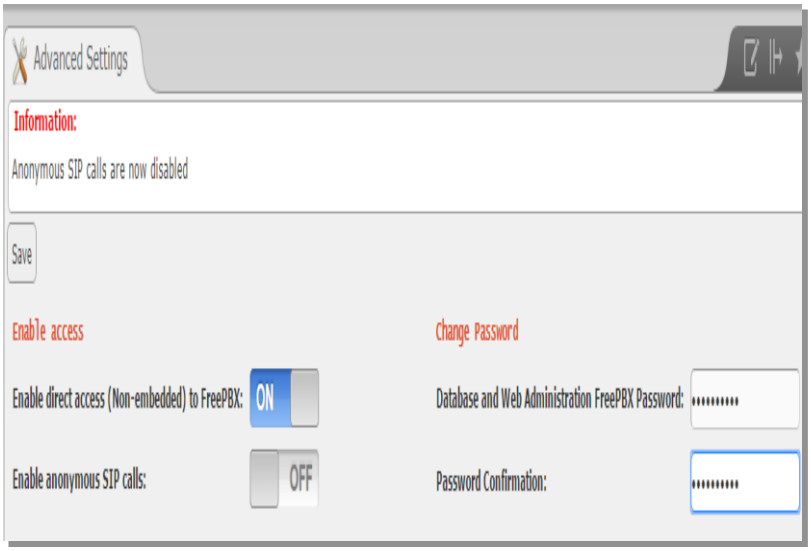


Ilustración 74: Activación de la (FreePBX).
Fuente: El Autor (2015).

Una vez dentro, se debe ir a la sección de *Tools* (*ubicada en la esquina superior izquierda*) -> *Asterisk SIP Settings*, desde aquí, se pueden editar las configuraciones generales para *SIP*, tal como se muestra en la siguiente imagen.

Ilustración 75: Activación de Asterisk SIP.
Fuente: El Autor.

Una vez hecho esto, aparece la siguiente ventana, donde se debe configurar la *(IP)*, de salida, *(IP pública)*, se debe configurar la máscara y la red a la cual se está conectado, cabe mencionar que esta configuración de la *(IP)* publica se debe realizar si se requiere

de salida a internet por medio de *(NAT)*, caso contrario se debe desactiva y continuar con la configuración tal como se muestra a continuación:

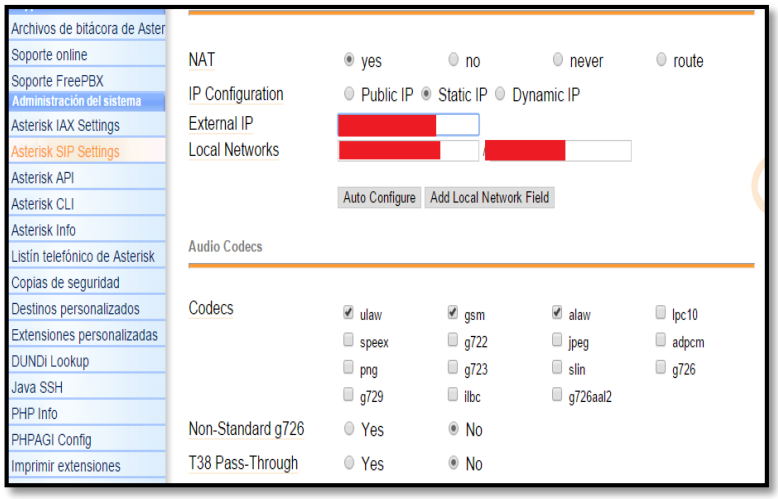


Ilustración 76: Configuración de la red en la (FreePBX).
Fuente: El Autor (2015).

En la parte final de esta ventana, se encuentra el campo denominado *Other SIP Settings*, en el cual se agregan los parámetros descritos a continuación:

```
tlsenable=yes
tlsbindaddr=0.0.0.0
tlsdontverifyserver=yes
tlscertfile=/var/lib/asterisk/keys/tesis.hial.com.pem
tlscafile=/var/lib/asterisk/keys/ca.crt
```

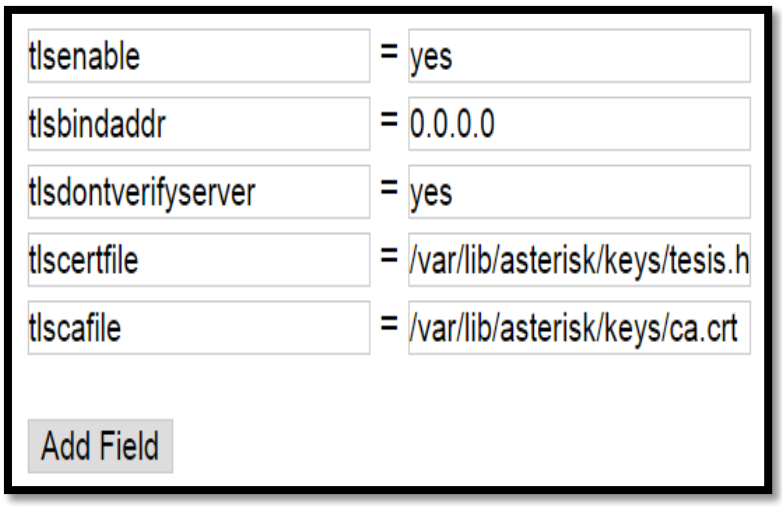


Ilustración 77: Parámetros de configuración de (TLS).
Fuente: El Autor (2015).

Luego de haber realizado todas estas modificaciones, se guardan los cambios y se reinicia el servidor *Asterisk*, quedando listo, para poder establecer las comunicaciones de manera segura. Para saber si los cambios se aplicaron correctamente, se puede ver que *Asterisk*, ahora también escucha el puerto *(TCP-5061),* con el siguiente código:

```
#netstat –atunp | grep asterisk.
```

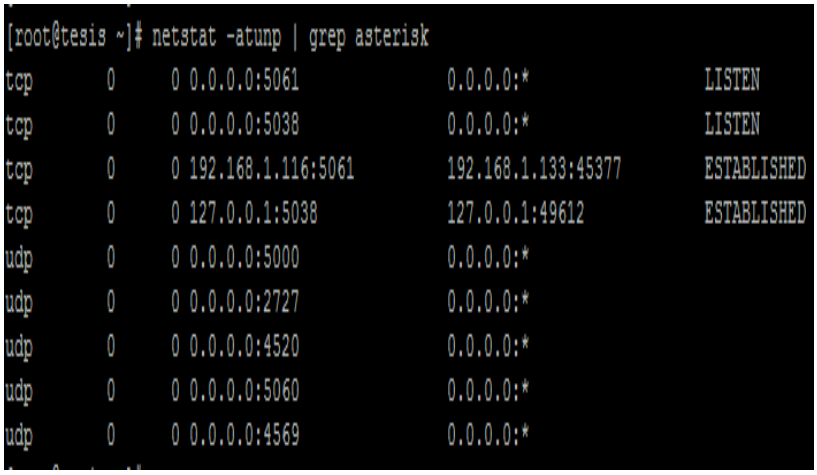


Ilustración 78: Escucha del puerto 5061 en el servidor Asterisk.
Fuente: El Autor (2015).

Así mismo para poder determinar que los certificados se han creado correctamente para el cifrado de la voz se utiliza el siguiente comando de ejecución: `sip reload` el cual devuelve lo siguiente: `SSL certificate ok`, tal como se muestra en la siguiente imagen:

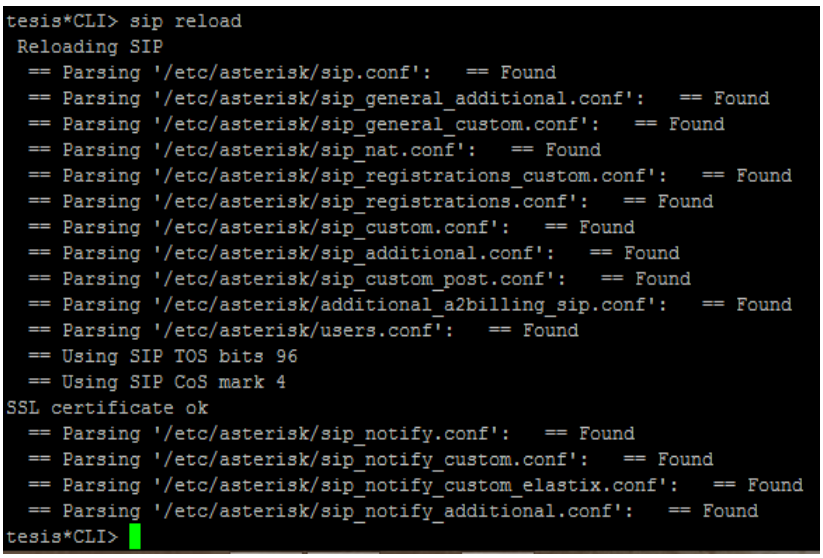


Ilustración 79: Verificación de la creación de los certificados utilizados por (TLS).
Fuente: El Autor (2015).

Para habilitar el soporte *(SSL/TLS),* en una extensión, el campo *transport* se debe cambiar "*UDP*" por "*TLS*", en el campo *encriptación* se debe cambiar *"no"* por *"yes"*, tal como se muestra a continuación:

disallow	all
allow	g722
dial	SIP/1000
accountcode	
mailbox	1000@device
vmexten	
deny	0.0.0.0/0.0.0.0
permit	0.0.0.0/0.0.0.0
encryption	yes
transport	tls

Ilustración 80: Configuración de la encriptación y del protocolo (TLS), en la (PBX).
Fuente: El Autor (2015).

1.2.1.4.Creación de certificados para clientes.

Para crear certificados, de las extensiones locales se hace lo siguiente:

```
#sh /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/ast_tls_cert –m
client –c /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/ca.crt –k
/usr/share/doc/asterisk-1.8.20.0/contrib/scripts/ca.key –C 1000.tesis.
hial.com. –O "tesis.hial.com" –d /etc/asterisk/claves/ -o 1000
```

```
[root@tesis ~]# sh /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/ast_tls_cert -
m client -c /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/certs/ca.crt -k /usr/
share/doc/asterisk-1.8.20.0/contrib/scripts/certs/ca.key -C 1000.tesis.hial.com -O
 "tesis.hial.com" -d /etc/asterisk/claves -o 1000

No config file specified, creating '/etc/asterisk/claves/tmp.cfg'
You can use this config file to create additional certs without
re-entering the information for the fields in the certificate
Creating certificate /etc/asterisk/claves/1000.key
Generating RSA private key, 1024 bit long modulus
.............++++++
.....................................................++++++
e is 65537 (0x10001)
Creating signing request /etc/asterisk/claves/1000.csr
Creating certificate /etc/asterisk/claves/1000.crt
Signature ok
subject=/CN=1000.tesis.hial.com/O=tesis.hial.com
Getting CA Private Key
Enter pass phrase for /usr/share/doc/asterisk-1.8.20.0/contrib/scripts/certs/ca.ke
y:
Combining key and crt into /etc/asterisk/claves/1000.pem
[root@tesis ~]#
```

Ilustración 81: Creación de los certificados para las extensiones.
Fuente: El Autor (2015).

- `-m client`: Utilizado para crear certificados de extensiones locales.
- `-c`: Certificado de autenticación cliente-servidor.
- `-k`: Llaves de autenticación cliente-servidor.
- `-C`: Extensión a registrarse.
- `-O`: Nombre objetivo.
- `-d`: Directorio de almacenamiento de certificados.
- `-o`: Nombre de la extensión.

1.2.1.5.Implementación del protocolo (SSL/TLS) en los terminales.

Para realizar la configuración en los terminales, se debe realizar lo siguiente: en el caso de los teléfonos *Yealink*, se ingresa *Account -> Cuenta 1 -> Basic -> Transport -> TLS*, tal como se muestra en la siguiente imagen.

Ilustración 82: Configuración de (TLS) en el teléfono Yealink.
Fuente: El Autor (2015).

Una vez configurado este parámetro se procede con la activación de *(SRTP)*, en *Account -> Cuenta 1 -> Advanced -> Voice Encryption (SRTP) -> ON.*

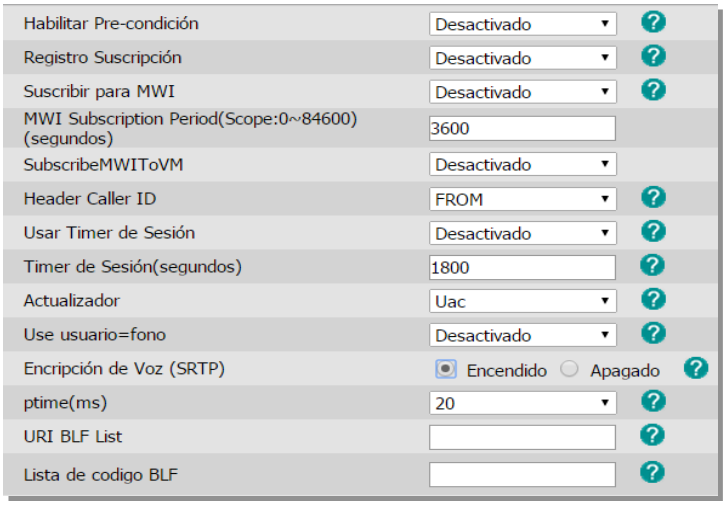


Ilustración 83: Activación del SRTP en el teléfono Yealink.
Fuente: El Autor (2015).

Así mismo, se debe cambiar el puerto de registro, en lugar del 5060, se debe colocar el 5061, luego se debe ubicar en la pestaña seguridad -> *certificados confiados* -> *seleccionar archivo* -> *cargar el certificado (extensión) 1000.key* -> tal como se muestra en la siguiente imagen y se debe aplicar los cambios, con ello se termina la configuración del cifrado de la voz en el servidor *Asterisk*.[21]

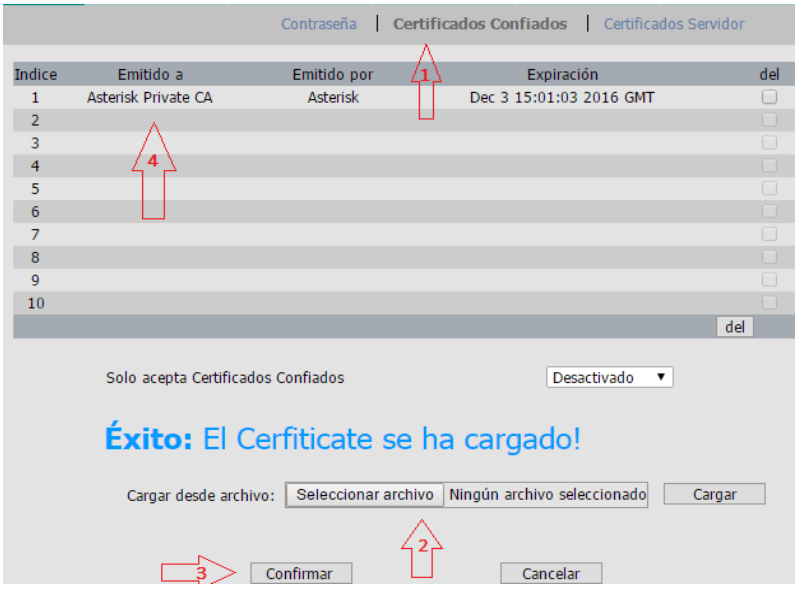


Ilustración 84: Cargar el certificado para la certificación
Fuente: El Autor (2015).

Los teléfonos *Grandstream* soportan *(TLS)* y funcionan correctamente, pero existen ciertos inconvenientes con *(SRTP)*, para solucionar este problema se descarga un parche y se instala en *Asterisk*, luego se re-compila el servidor, cabe mencionar que este parche está diseñado para *Asterisk* 2.1.8.4. El *link* para el repositorio de descarga es el siguiente:

```
#wget'https://issues.asterisk.org/file_download.php?file_id=29497&type
=' -O - |patch -p0
```

Para el caso de los *softphones*, la configuración es similar, en la mayoría de casos se debe especificar el puerto para el registro, que es el *5061*. Para mejor indicación de la configuración de los softphone ver ***(anexo I).***

Cabe mencionar que los puertos 5060 y 5061, tanto en *(TCP)* y *(UDP)*, se asocian con el *(SIP)*, en particular, el puerto *5060*, se asigna a *(SIP texto)*, y el puerto 5061, se asigna a *(SIP cifrada)*, también conocido como *(SIP-TLS)*, es decir, *(SIP a través de una capa de seguridad o canal cifrado)*. [21]

1.3. ASEGURANDO EL PROTOCOLO SSH

SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, *(SSH)* ya de por si es un protocolo seguro, pero podemos afinar más los parámetros para que sea aún más seguro con lo cual estaríamos resolviendo las vulnerabilidades de cracking de contraseñas por fuerza bruta que actualmente se dan el servidor *(VoIP)* del Hospital Isidro Ayora de Loja, para ello se va a realizar lo siguiente:

- Deshabilitar *(SSH)* 1
- Autenticación basada en clave
- No permitir autenticación por p*assword*
- Cambiar el puerto por Defecto
- No Permitir logeo como root
- Banear *(IPs)* tras 5 login erróneos

1.3.1. Deshabilitar SSH 1

Puesto que la versión del protocolo *(SSH)* 1, hay algunas inseguridades, que mejor manera que usar el protocolo *(SSH)* 2 que es mucho más seguro. Para esto editaremos el fichero de configuración de *(SSH)* en que se encuentra en los directorios de *Asterisk* cuyo path es el siguiente: `/etc/ssh/sshd_config`. La opción del protocolo la dejaremos de esta forma: `Protocolo 2`, guardar los cambios realizados y reiniciar el `sshd_config`, con el siguiente comando `# /etc/init.d/sshd restart`.

```
[root@tesis ~]#
[root@tesis ~]#
[root@tesis ~]#
[root@tesis ~]# vim /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.73 2005/12/06 22:38:28 reyk Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#Protocol 2,1
Protocol 2
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

[root@tesis ~]# /etc/init.d/sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[root@tesis ~]#
[root@tesis ~]#
```

Ilustración 85: Modificación del archivo sshd_config para cambiar la versión del protocolo.
Fuente: El Autor (2015).

1.3.2. Autenticación basada en clave:

Entrar con usuario y password está bien, pero podemos tener más seguridad usando un par de claves pública y privada, es decir, podemos crear nuestra clave pública para acceder desde la maquina cliente, esto se realiza con el código: `ssh-keygen`:

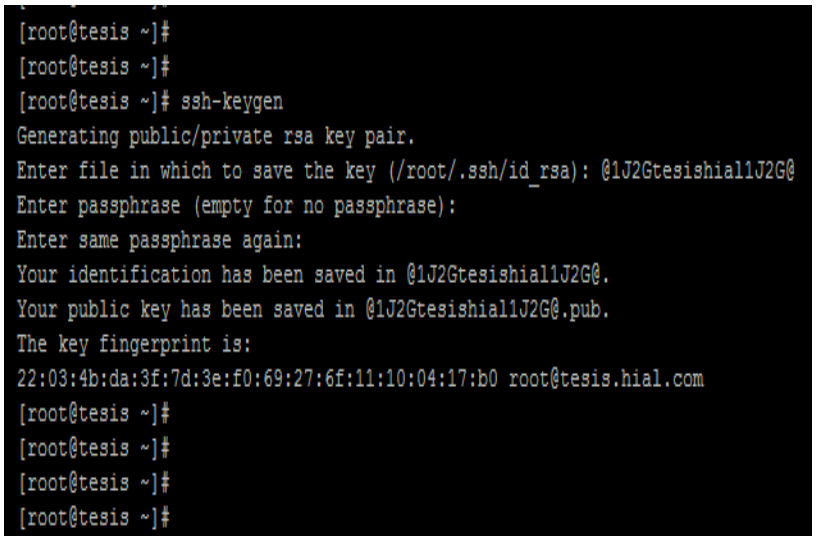


Ilustración 86: Creación de la clave privada para el acceso al servidor
Fuente: El Autor (2015).

Al ejecutar este comando se debe asignar una clave al terminar generara dos archivos, una de ellos con una extensión `.pub` que vendría siendo la clave privada que acabamos de generar, misma que se debe copiar a la maquina remota, luego se habilita la autenticación por clave en el servidor, configurando el archivo `/etc/ssh/sshd_config`, donde se habilita la autenticación con las claves anteriormente añadidas al archivo `.ssh/authorized_keys` del servidor `ssh`. El archivo debe quedar así:

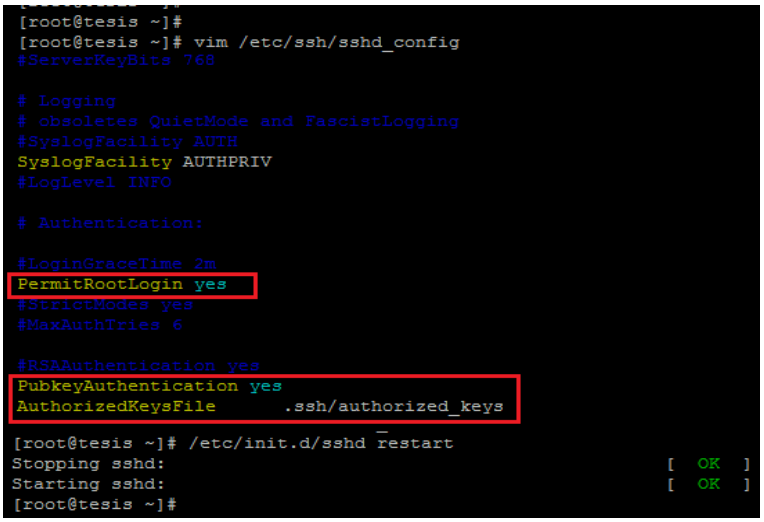


Ilustración 87: Activación de la autenticación por clave.
Fuente: El Autor (2015).

1.3.3. Deshabilitar la autenticación por password

Para poder hacer útil lo anteriormente mencionado dejaremos solo la autenticación por clave eliminando la autenticación por password para esto editaremos de nuevo `/etc/ssh/sshd_config` tal como se muestra en la siguiente imagen:

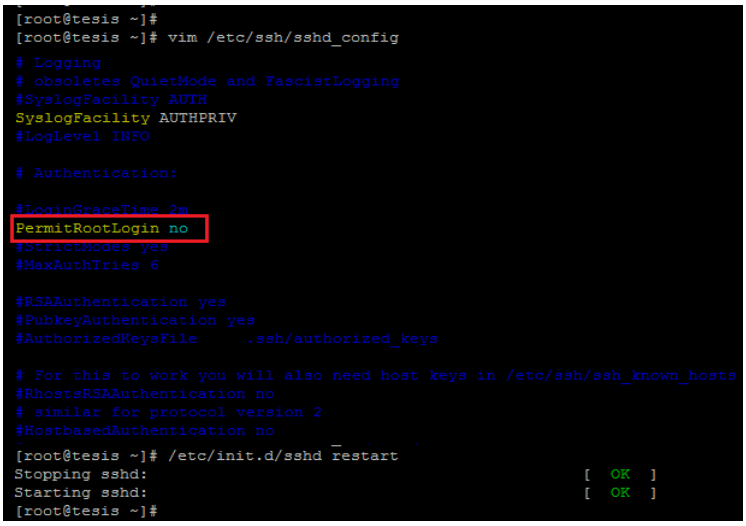


Ilustración 88: Deshabilitar autenticación por password.
Fuente: El Autor (2015).

De esta forma se reduce drásticamente el impacto de ataques por fuerza bruta, debido a que se dificultara el descifrado de claves, ya que no se puede ingresar, al sistema sin la clave que tendrá únicamente el administrador de la red, para el ingreso con acceso remoto. Para acceder remotamente con algún *software* como por ejemplo *PuTTy*, se debe cargar la clave que fue generada y descargada en la maquina cliente tal como se muestra en la siguiente imagen:

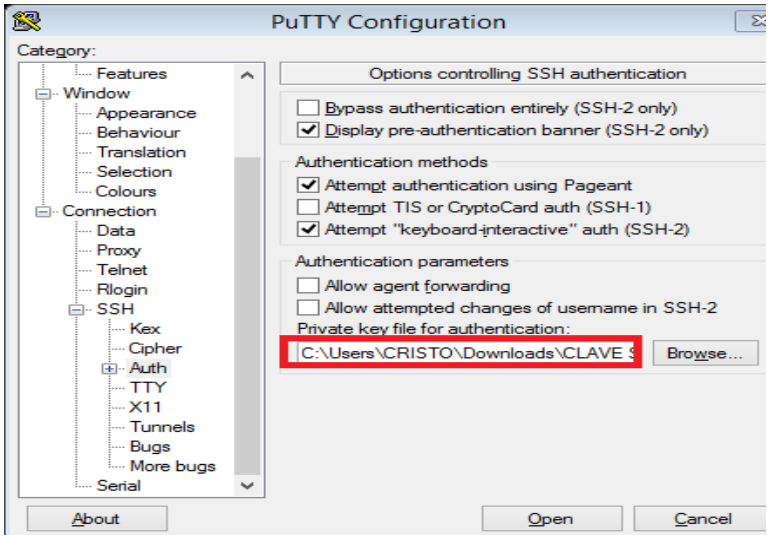


Ilustración 89: Cargar la clave a PuTTy para acceder al servidor
Fuente: El Autor (2015).

En caso de no cargar la clave e insertar acceder con la password de usuario, no se establecerá la sección, tal como se muestra en la siguiente imagen:

Ilustración 90: Acceso denegado al sistema por no contar con l clave privada
Fuente: El Autor (2015).

1.3.4. Cambiar el puerto por defecto

En vista de que hay forma muy conocidas para realizar accesos rotamente como es el puerto 22 el cual trabaja *(SSH)*, se debe realizar ciertas modificaciones con el fin de dificultar la tarea de las personas que rastrean los servicios de *(VoIP)*, debido a ello se debe cambiar el acceso del puerto por defecto, con lo que evitaríamos exploits típicos de Script Kidies. Para ello se debe modificar el archivo: `/etc/ssh/sshd_config` en el cual se debe remplazar el Port *(22)*; *(25141);* donde *(25141)* puede ser otro puerto.

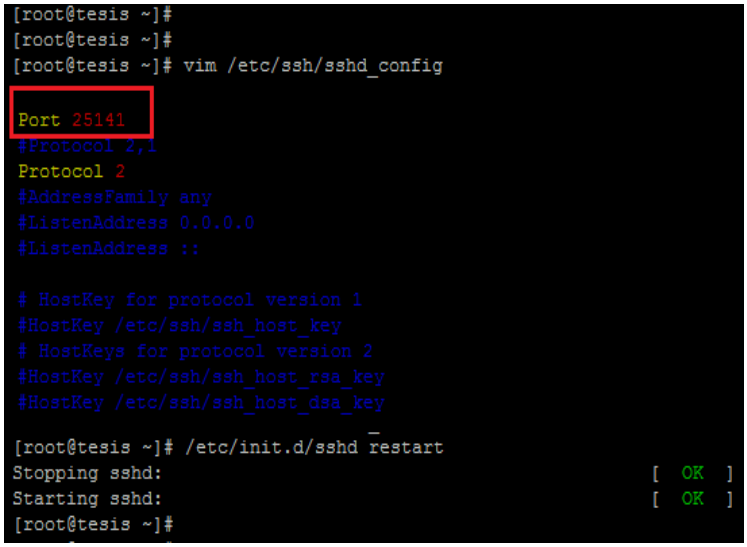


Ilustración 91: Cambio del puerto por defecto (SSH)
Fuente: El Autor (2015).

Para acceder con *PuTTy* se debe cambiar el puerto 22 por el que fue asignado en el archivo `sshd_config`, tal como se muestra en la siguiente imagen:

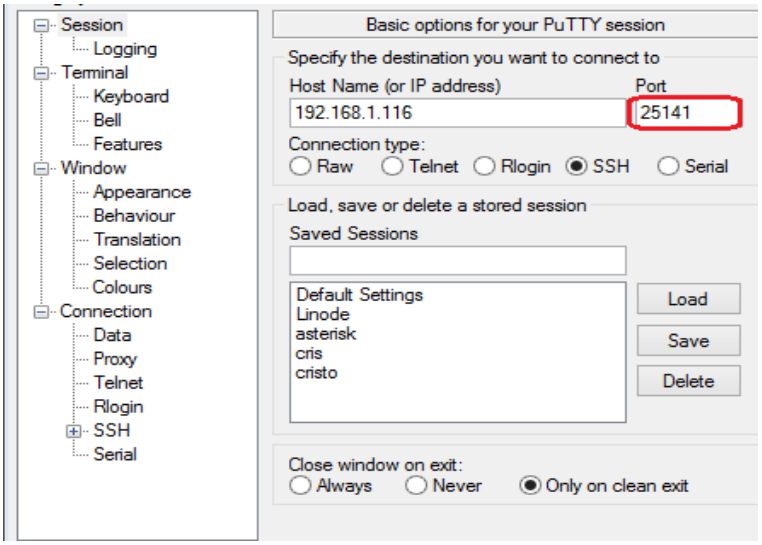


Ilustración 92: Cambio de puerto en el software PuTTy.
Fuente: El Autor (2015).

1.4. BLOQUEAR A LAS IPS QUE HACEN MÁS DE 5 LOGEOS ERRONEOS:

Lo que se va a configurar en este punto, requiere la instalación de una herramienta denominada *(fail2ban)*, esta sirve para evitar posibles ataques hacia un equipo, específicamente para los ataques de fraudes telefónicos, funciona como una especie de sistema de protección de intrusos. *Fail2ban* deniega el registro de un cliente si ha intentado loguearse cierta cantidad de veces con datos erróneos, es decir, bloquea las *(IP)*, de donde se han originados los intentos, interactuando con *iptables (cortafuegos).* [22]

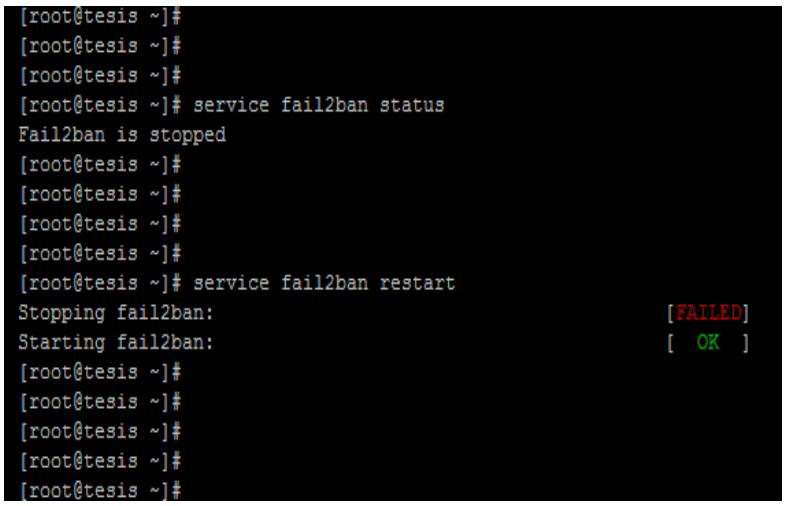


Ilustración 93: Activación de la herramienta Fail2ban.
Fuente: El Autor (2015).

Fail2ban está escrito en *Python* y para que funcione tenemos que instalar este lenguaje de programación, pero en las distribuciones de *GNU/Linux* con *Asterisk (por ejemplo en Elastix)* viene preinstalado, lo que se debería hacer es activarlo y configurarlo, para comprobar se ejecuta el siguiente comando `service fail2ban status`, si se tiene la respuesta similar a la que se muestra en la imagen anterior, es que la que la herramienta si está instalada pero no está en funcionamiento, si la respuesta es: `service fail2ban unrecognized` es que se requiere la instalación de *fail2ban* para ello se ejecuta el siguiente comando: `yum -y install fail2ban.`

Para levantar el servicio se ejecuta el siguiente comando `service fail2ban restart`, quedando listo para realizar las configuraciones, lo que primero se debe hacer es, crear un archivo denominado `jail.local` dentro de los repositorios de fail2ban con el siguiente comando:

```
# vi /etc/fail2ban/jail.local
```

En él se debe añadir la siguiente directiva tal como se muestra en la siguiente imagen:

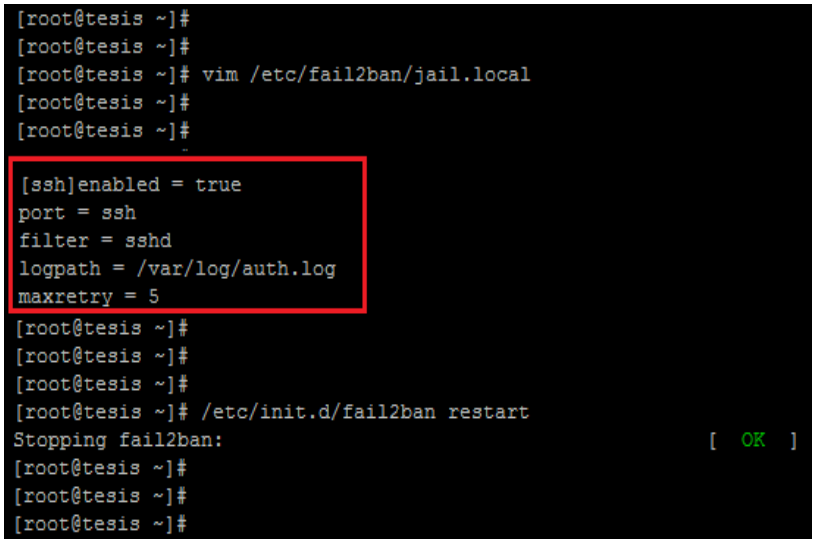


Ilustración 94: Configuración del archivo jail.local
Fuente: El Autor (2015).

Nota: Cada vez que se hace un cambio en los archivos se debe reiniciar para que se apliquen los cambios con el siguiente comando `/etc/init.d/archivo restart.`

Finalmente reiniciamos *fail2ban* para que se ejecuten los cambios realizados y se intenta ingresar al sistema remotamente luego de cinco accesos denegados en el terminal saldrá un error de conexión

1.5. ACTIVACIÓN DEL FIREWALL DE ELASTIX

En esta sección se da a conocer el *Firewall* de *Elastix*, con el fin de configurar algunas reglas de seguridad, Elastix incorpora un módulo de seguridad, basado en el *Firewall* de *Linux (IPTABLES)*, que sin bien es cierto es bastante básico, permite configurar lo necesario para minimizar el riesgo de accesos indebidos al servidor, así como restringir las redes IP que tendrán acceso a los servicios de telefonía que el servidor *Elastix* provee por defecto el *Firewall* viene desactivado en *Elastix*, para ingresar damos clic en la pestaña -> *Security*, luego aparece la pantalla del *Firewall*, damos clic en la opción -> *Activate Firewall*, luego -> *Actívate Firewall*, con estos pasos activaríamos el *Firewall* tal como se muestra en la siguiente imagen:

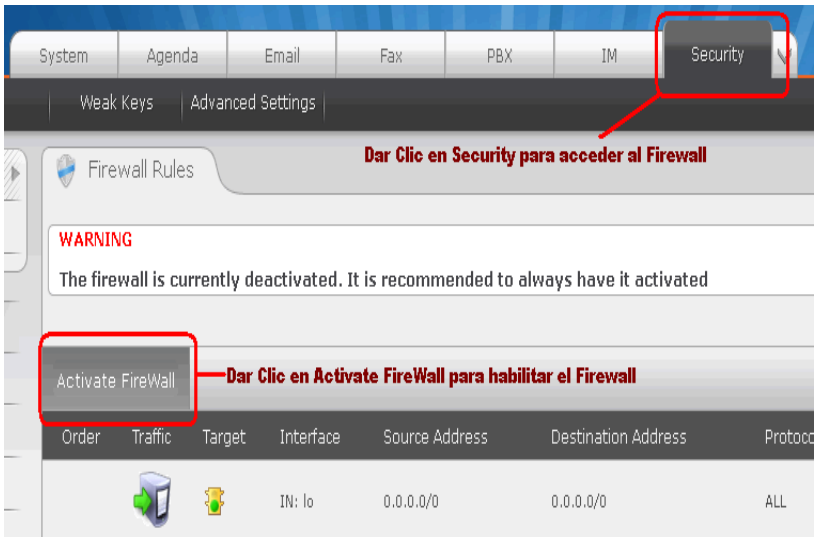


Ilustración 95: Activación de firewall de en Elastix
Fuente: El Autor (2015).

Inmediatamente que se activa el *Firewall* aparece la pantalla similar a la siguiente, con las opciones por defecto numeradas, todas las reglas están activas para permitir todo. Para activar las reglas de filtrado de *(HTTP), (HTTPS)* y *(SSH):* cuyos servicios corresponden al acceso *(Web)* y *(SSH),* mismas que están asignadas por números: *10 (SSH), 12 (HTTP)* y *15 (HTTPS).*

Editamos las opciones para cada una de las reglas a modificar, para acceder lo hacemos dando clic sobre el icono azul, lado derecho de la pantalla. Lo que se pretende con esta configuración es permitir el acceso únicamente desde la dirección IP: `192.168.xxx` *(IP del administrador),* para hacerlo se ingresa la dirección *(IP)* y la máscara de subred, en

este caso al tratarse de una sola dirección *(IP)*, se debe colocar un valor de /32 en la máscara *(Equivalente a: 255.255.255.255)*, tal como se muestra en la siguiente imagen:

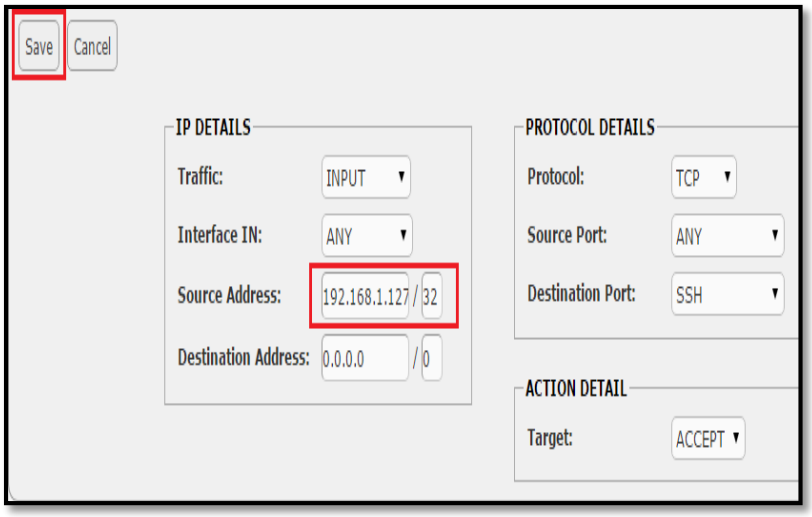


Ilustración 96: Configuración de la regla 10 del firewall de Elastix
Fuente: El Autor (2015).

Es recomendable colocar primero la regla para *(SSH)* tal como se muestra en la imagen anterior, se debe comprobar luego de su configuración, si todo sale de acuerdo a lo planeado se proceder con la configuración de las otras dos reglas.

Cabe mencionar que esta configuración se la realiza en caso de que no se haya realizado la configuración del puerto *(SSH)* que se detalló en los puntos anteriores, finalmente se guarda los cambios y lo que se obtiene es lo siguiente:

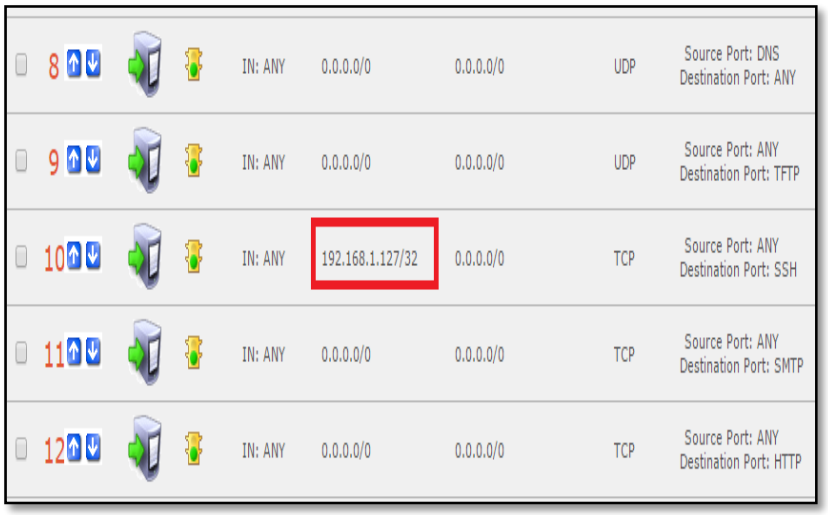


Ilustración 97: Cambios realizados en el firewall de Elastix
Fuente: El Autor (2015).

Para las otras dos reglas se debe realizar el mismo procedimiento con la excepción de la 15 donde se debe elegir el protocolo *(HTTPS)* en el parámetro Destination Port, finalmente se guardan los cambios realizados y se obtiene la siguiente imagen:

Ilustración 98: Modificación de las tres reglas del firewall de Elastix
Fuente: El Autor (2015).

De esta manera hemos configurado el Firewall de Elastix, para restringir el acceso a las sesiones de administración del servidor *(SSH, HTTP, HTTPS)* y de esta forma tener ingreso desde una sola dirección *(IP).*

Nota: El uso erróneo de la siguiente configuración **puede dejarlos sin acceso completo al entorno de administración**, si no se aplican bien las instrucciones. En caso de eso sucediera o en el caso hipotético que no desee tener el muro de fuego o firewall activado debido a que solamente se está ejecutando un servicio público http (puerto 80). Para ello c se debe seguir el siguiente procedimiento:

```
#service iptables save
#service iptables stop
#chkconfig iptables off
```

`Iptables`: Es una herramienta de administración /comando para el filtrado de los paquetes *(IPv4)* y *(NAT).*

`Service`: Es un comando de ejecución `script init V`. Este se usa para detener `/ iniciar / el servicio del firewall.`

`Chkconfig`: Es un comando usado para actualizar y consultar los niveles de ejecución para los servicios del sistema. Se trata de una herramienta del sistema para mantener la jerarquía de `/etc/rc*.d`. Utilice está herramienta para deshabilitar el servicio de cortafuegos *(firewall)* en el arranque del sistema.

1.6. CERRAR PUERTOS INNECESARIOS ABIERTOS

Para cerrar los puertos se debe trabajar con iptables para para proteger el servidor de accesos no autorizados y abrir los puertos que necesita el servidor asterisk.

Nota también se puede realizar esta configuración con la herramienta fail2ban que se la describió en los puntos anteriores.

Para instalar iptables: En *Fedora, Centos, RedHat*: `sudo yum install iptables`
El firewall iptables se encarga de gestionar los paquetes que entran y salen del servidor. Iptables utiliza 3 tipos de reglas:

- Filter: donde pasan todos los paquetes en entrada y salida. La regla filter acepta tres tipos de opciones (cadenas):
  - INPUT para los paquetes en entrada
  - OUTPUT para los paquetes en salida
  - FORWARD para redireccionar los paquetes.

- NAT: se utiliza para redirigir el tráfico o los puertos de los paquetes *(IP)*.
- MANGLE: se utiliza para modificar algunos parámetros de los paquetes (un ejemplo es marcar los paquetes para que sean procesados y enviados con una prioridad más alta).

Las reglas hay que definirlas una por línea y serán procesadas por iptables siguiendo la misma secuencia. Por defecto cuando no se especifica una regla, se aplica a la regla filter.

A continuación las reglas a definir en iptables:

- Regla para aceptar todo el tráfico en entrada con destino a la interfaz local *(lookpack):*

  ```
  iptables -A INPUT -i lo -j ACCEPT
  ```

- Se rechaza *(REJECT)* todo el tráfico entrante destinado a las *(IP)* `127.0.0.0/127.255.255.255` menos los paquetes para la interfaz local *(lookpack):*

  ```
  iptables -A INPUT ! -i lo -d 127.0.0.0/8 -j REJECT
  ```

- Se aceptan todos los paquetes en entrada de conexiones ya establecidas, o relacionados con conexiones establecidas:

  ```
  iptables -A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT
  ```

- Se dejan pasar todos los paquetes salientes:

  ```
  iptables -A OUTPUT -j ACCEPT
  ```

- Se deja pasar todo el tráfico en entrada para el protocolo *(SSH)*:

  ```
  iptables -A INPUT -p tcp -m state –state NEW -m tcp –dport 22 -j ACCEPT
  ```

- Se deja pasar todo el tráfico en entrada destinado al puerto udp 4569 *(protocolo IAX2):*

  ```
  iptables -A INPUT -p udp –dport 4569 -j ACCEPT
  ```

- Se deja pasar todo el tráfico en entrada destinado al puerto udp 5060 *(protocolo SIP):*

  ```
  iptables -A INPUT -p udp –dport 5060 -j ACCEPT
  ```

- Se deja pasar todo el tráfico en entrada destinado al puerto tcp *5060 (protocolo SIP sobre TCP):*

  ```
  iptables -A INPUT -p tcp -m state –state NEW -m tcp –dport 5060 -j ACCEPT
  ```

- Se deja pasar todo el tráfico en entrada destinado a los puertos *(UDP)* que van de `10000` a `20000`, tráfico *(RTP):*

  ```
  iptables -A INPUT -p udp –dport 10000:20000 -j ACCEPT
  ```

- Se dejan pasar las solicitudes de ping:

  ```
  iptables -A INPUT -p icmp -m icmp –icmp-type 8 -j ACCEPT
  ```

Una vez establecidos todos los puertos necesarios para *Asterisk*, se rechaza el resto de tráfico:

```
iptables -A INPUT -j REJECT
iptables -A FORWARD -j REJECT
```

Comprobamos las reglas que acabamos de definir y las guardamos:

```
iptables -L
service iptables save
service iptables start
```

Para terminar hay que configurar Asterisk para que use los puertos *(UDP)* desde `10000` hasta `20000` para el protocolo *(RTP)*: Se modifica el archivo de configuración del *(RTP):*

```
sudo vim /etc/asterisk/rtp.conf
```

```
[general]          // Etiqueta inicial del archivo de configuración.
Rtpstart=10000     // Puerto inicial para el tráfico (RTP).
rtpend=20000       // Puerto final para el tráfico (RTP).
rtpchecksums=no    // Activar o no la suma de verificación en los paquetes (RTP).
```

`dtmftimeout=3000` // La cantidad de tiempo *(en ms)* del tono *(DTMF)* sin marcar el fin.

`rtcpinterval=5000` // Milisegundos entre cada reporte del protocolo *(RTCP)*.

`strictrtp=yes` // Lo paquetes que no proceden del mismo flujo RTP utilizado en la conexión serán eliminados.

Se guardan los cambios efectuados y se recarga la configuración de *Asterisk* tal como se muestra en la siguiente imagen: `sudo /etc/init.d/asterisk reload`

```
[root@tesis ~]#
[root@tesis ~]# sudo vim /etc/asterisk/rtp.conf
[root@tesis ~]#
[root@tesis ~]#
;
; RTP Configuration
;
[general]
;
; RTP start and RTP end configure start and end addresses
; These are the addresses where your system will RECEIVE audio an
; If you have connections across a firewall, make sure that these
;
rtpstart=10000
rtpend=20000
rtpchecksums=no
dtmftimeout=3000
rtcpinterval=5000
strictrtp=yes

[root@tesis ~]#
[root@tesis ~]# sudo /etc/init.d/asterisk reload
[root@tesis ~]#
```

Ilustración 99: Modificación del archivo rtp.conf
Fuente: El Autor (2015).

Con las configuraciones realizadas ese ha contrastados las vulnerabilidades encontradas en el servidor de *(VoIP)*, es decir, se ha reducidos al minino los ataques con el índice de riesgo más alto, como *(DoS)*, *eavesdropping*, *cracking de contraseñas accesos no autorizados y cerrar puertos innecesarios abiertos*, los cuales se clasificaron en la tabla 41 de la sección valoración de riesgos

1.7. COMPROBACIÓN DE LA IMPLEMENTACIÓN DE PROPUESTA DE SEGURIDAD.

Una vez realizada la configuración de la seguridad, para establecer un canal cifrado de comunicaciones, bloquear intentos de *(DoS)*, evitar cracking de contraseñas y haber creado reglas para permitir el ingreso solo por los puertos adecuados, es necesario comprobar que dicha seguridad, está cumpliendo de forma eficiente con su trabajo, cuyo fin es evitar ataques que se puedan generar en la red y sobre todo que la integridad de la información sea fiable, es decir, cuando se realice comunicaciones entre dos o más usuarios de la institución, estas no sea interceptada por terceras personas.

Para poder comprobar la configuración del protocolo *(TLS)*, se realiza llamadas telefónicas y se tratara de capturar los paquetes *(SIP* y *RTP)*, para ello hay que realizar configuraciones en el analizador de paquetes wireshark porque con la configuración habitual no se logra capturar ningún paquete, en el menú principal de wireshark en la pestaña *Edit --> Preferences… --> la pestaña --> Protocols --> SSL*, luego aparecerá una nueva ventana en la cual se elige *--> Edit --> New* en esta nueva ventana se configura la *(IP)*, del servidor el puerto en este caso el 5060 y finalmente se cargara la clave del servidor que previamente descargada sin ella, no podremos realizar ningún tipo de posibilidad de ver el tráfico *(SIP)* en texto claro, como se muestra en la siguiente imagen:

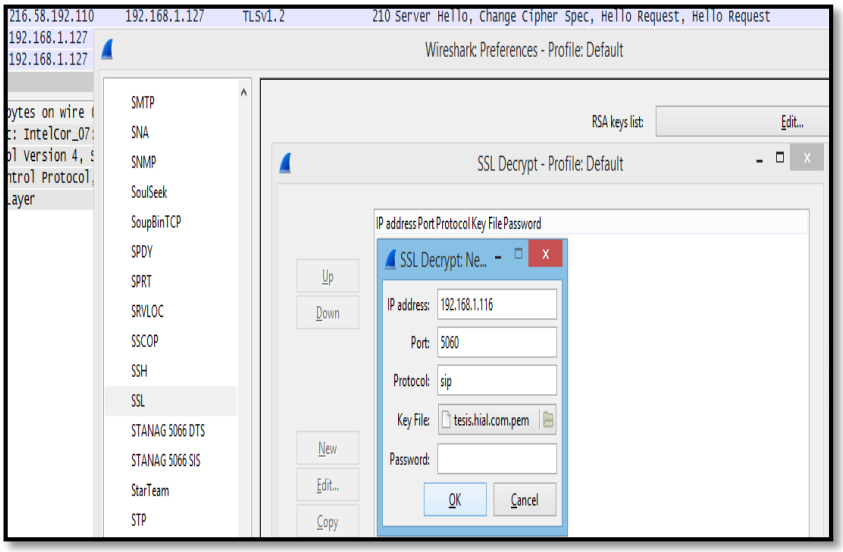


Ilustración 100: Configuración de wireshark para capturar (TLS).
Fuente: El Autor (2015).

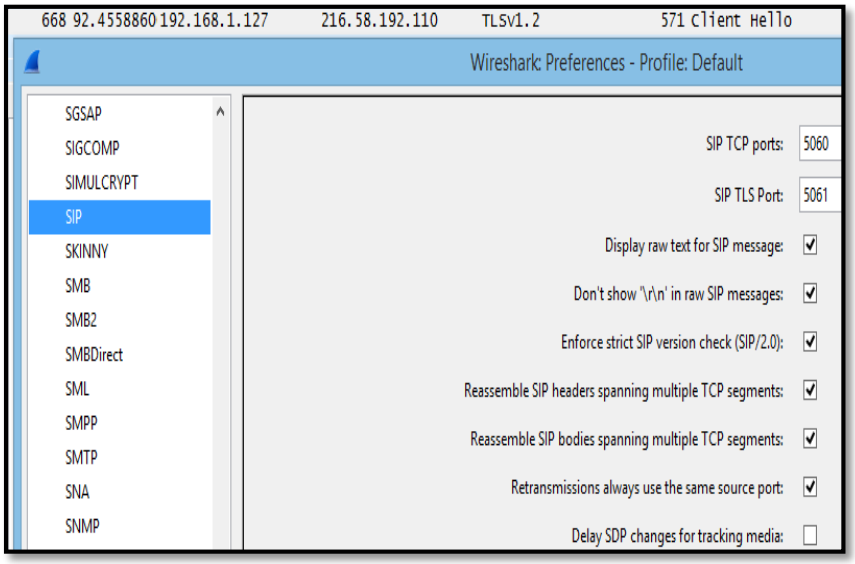


Ilustración 101: Configuración del puerto para interceptar tráfico (TLS).
Fuente: El Autor (2015).

Luego se debe indicar el puerto *(TLS)* que utilizamos para nuestras comunicaciones *(SIP),* tal como se muestra en la imagen 101 una vez terminado se procede con la captura de *(TLS)* y poder visualizar el intercambio de mensajes entre el cliente y el servidor. Cabe mencionar que estas llamadas se realiza desde teléfonos físicos *(IP)* con lo cual no se puede capturar las llamadas debido a que los paquetes *(RTP)* van encapsulados dentro de *(TLS)*

1.8.ANÁLISIS DELAS TRAMAS DEL PAQUETE TLS EN UNA LLAMADA VOIP.

Una vez implementadas las soluciones se realiza un análisis de las tramas de los paquetes que viajan mediante el protocolo *(TLS),* es necesario aclarar que el protocolo *(SIP)* se encripta nativamente, es decir, la señalización *(y sólo la señalización, no RTP)* se encripta por defecto a través de *(TLS).* Como siempre, hemos de destacar que el audio y la señalización van por separado. Recordemos que *(SIP)* significa "*Session Initation Protocol"*. En realidad no es *(SIP)* sobre *(TLS),* sino yo lo llamaría *(SIP)* dentro de *(TLS),* porque en realidad lo que se hace es generar una sesión *(TLS),* y en el campo de datos pasamos los mensajes *(SIP),* es decir, se ha añadido una capa de seguridad a nuestras comunicaciones, dado que ya no se sabe tan fácilmente qué se está transmitiendo tráfico de voz. Por otro lado, sólo el servidor y el cliente pueden saber a qué números se está llamando. Es importante mencionar también que se ocultan las extensiones que se registran, y/o emiten llamadas, siempre y cuando tengamos configurada una (*CA),* para nuestros certificados, con lo que mitigamos el efecto de *(Man In The Middle).*

Protocolo handshake (TLS)

El protocolo de Handshake es el que permite a ambas partes autenticarse mutuamente y negociar el cifrado antes de intercambiar datos, para posteriormente establecer la conexión.

- **Client Hello:** El cliente envía un mensaje al servidor para dar inicio a una conexión cifrada, especificando una lista de conjuntos de cifrados, métodos de compresión soportados, la versión del protocolo *(SSL/TSL)* Además, se envía una cadena de 32 bytes aleatorios que sirven para generar la clave simétrica (más adelante en el protocolo). También, se incluye un identificador de sesión *(ID),* en caso de intentar "retomar" una sesión establecida con anterioridad y hacer un handshaking más corto *Server Hello*: El servidor contesta al cliente escogiendo un cifrado, enviando *(ID)* de sesión correspondiente, la versión de *(TLS)* a utilizar en la conexión, el tipo de compresión de datos y otra cadena de 32 bytes aleatorios

- **Server Key Exchange:** Con este mensaje el servidor ofrece para el cifrado asimétrico entre cliente y servidor la clave pública firmada con la clave del certificado.
- **Client Key Exchange:** El cliente, tras haber comprobado y validado el certificado, genera el premaster secret *(48 bytes)* cifrado con la clave pública del servidor y se lo envía. Luego, cliente y servidor pueden generar el master secret aplicando funciones hash a la cadena random de 32 bytes y al premaster secret, usado para el cifrado simétrico de datos.
- **Change Cipher Spec:** Con este mensaje el cliente informa que sus mensajes sucesivos estarán cifrados con el cifrado simétrico acordado.
- **Finished:** El cliente da por finalizada su fase de negociación asimétrica, garantizando la integridad de la comunicación.
- **Change Cipher Spec:** El servidor descifra con su clave privada el premaster secret enviado por el cliente y genera por su cuenta el master secret. Desde este momento, cliente y servidor han logrado establecer una clave simétrica.
- **Finished:** El servidor finaliza su fase de negociación asimétrica, con este protocolo de negociación finalizado, se logra crear un canal bajo el protocolo *(TLS)* que garantiza que todos los datos enviados por el protocolo de aplicación serán cifrados

Protocolo de registro TLS

Mientras el protocolo de handshake se encarga de negociar los parámetros de seguridad, es en la capa de registro donde se realizan las operaciones de formación de cada registro con sus campos correspondientes, fragmentado, compresión y cifrado. Todo el trabajo que está a cargo del registro *(TLS)* es totalmente transparente para la mayoría de aplicaciones. Este protocolo también es responsable de identificar los diferentes tipos de mensajes *(handshake, alert, cambio de cifrado o datos),* así como la obtención y verificación de la integridad de cada mensaje. Los datos son encriptados usando el cifrado negociado. Una vez completados estos pasos, los datos cifrados se transmiten a la capa transporte mediante *(TCP).* En el extremo receptor, se aplican los mismos pasos pero a la inversa; descifrar datos utilizando el cifrado negociado.

Detalle del proceso de negociación TLS

En la siguiente figura se muestra el detalle del handshake en una sesión *(TLS)* nueva, desde la petición del cliente para iniciar una conexión, además, el tipo de mensaje *Client Hello* corresponde a 1 y de los 32 bytes aleatorios, hay 4 que corresponden a la hora exacta de la solicitud, esto cuenta como un sello de tiempo por motivos de seguridad.

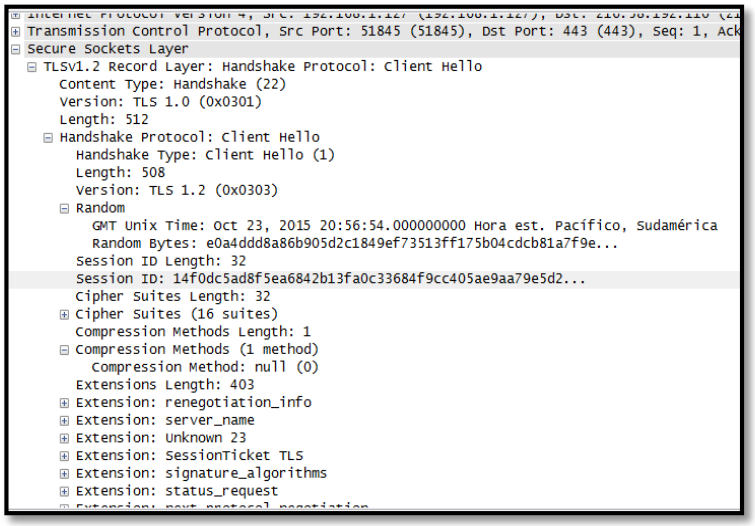


Ilustración 102: Mensaje (ClientHello)
Fuente el Autor (2015)

El identificador de sesión corresponde al cero y se ofrecen 16 suites de cifrados distintas a elección del servidor. Finalmente, ofrece solo un tipo de método de compresión, el nulo. El servidor contesta estos requerimientos con el tipo de versión 1.2 de *(TLS)*, a utilizar, la cadena aleatoria de 32 bytes de respuesta, que incluye otra vez el sello de tiempo, y la elección de la suite de cifrado (0xcc14); el tipo de mensaje *Server Hello* corresponde al 2

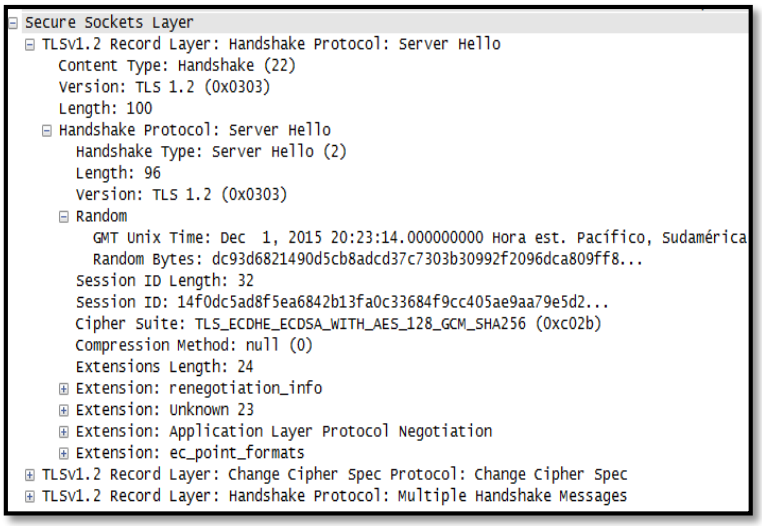


Ilustración 103: Mensaje (ServerHello)
Fuente el Autor (2015)

El servidor prosigue con el protocolo enviando su certificado de autenticidad, el envío de su clave pública y la finalización por parte suya del protocolo, con un *Server Hello Done* de 4 byte de longitud. Los valores de tipo de mensaje que identifican esta secuencia son 11, 12 y 14 respectivamente.

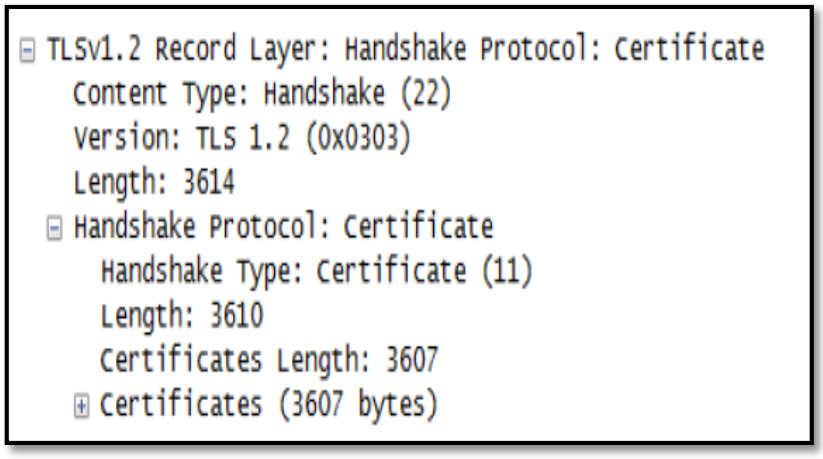


Ilustración 104: Envió de certificado por parte del servidor
Fuente el Autor (2015)

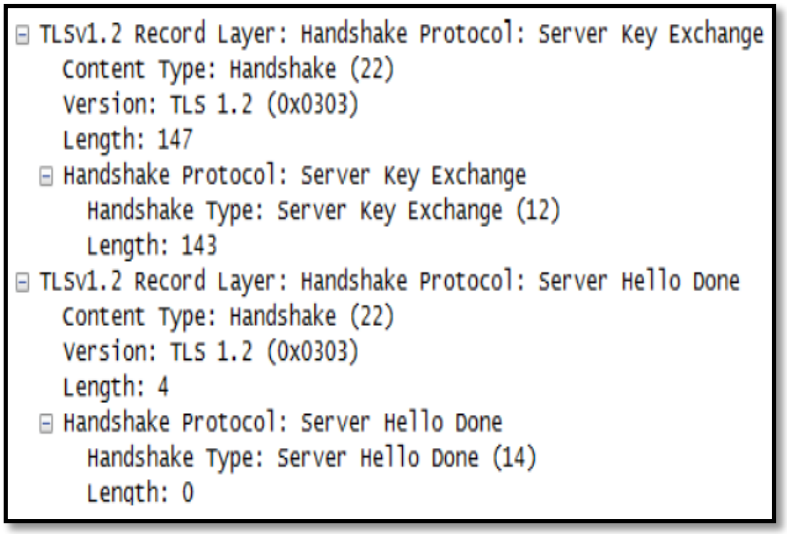


Ilustración 105: Server Key Exchange y Server Hello Dome
Fuente el Autor (2015)

En las figura 105, 106 se observa por parte del cliente y servidor el intercambio de claves, con lo cual se pasa de un cifrado asimétrico a simétrico de datos.

Notar que este cambio se identifica con el mensaje *Change Cipher Spec* de apenas 1 byte de longitud. El mensaje *New Session Ticket* es una extensión de *(TLS)* que le permite al

cliente volver a iniciar una conexión *(TLS)*, sin necesidad de rehacer el handshake completo nuevamente, con ello el servidor guarda una copia del estado de la sesión *(TLS)* en proxy.

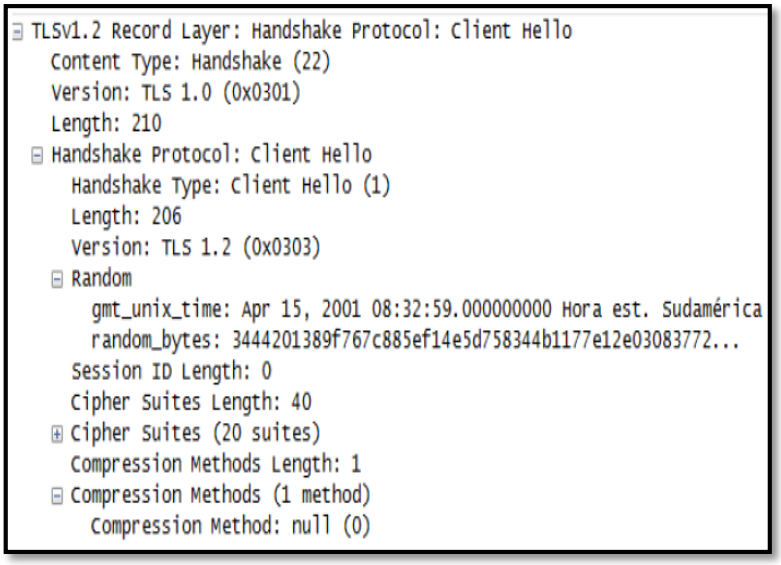


Ilustración 106: Client Key Exchange y envió de premaster secret
Fuente el Autor (2015)

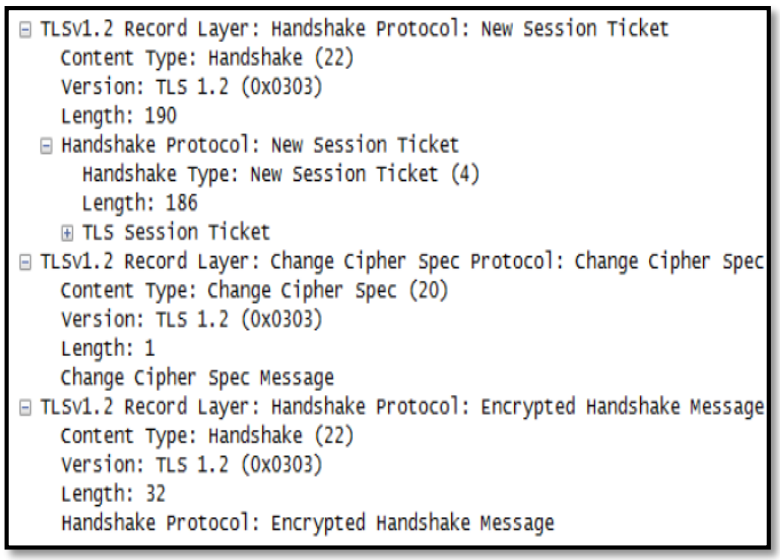


Ilustración 107: New Session Ticket y cambio del servidor
Fuente el Autor (2015)

Las únicas llamadas que se pudieron interceptar es realizando desde un softphone y desde la misma máquina que se está realizando el *sniffer* la red en el cual se la asigna las extensiones 3000 y 4000, y se realizan las llamadas respectivas en el cual paquetes pueden ser capturados y escuchados, los paquetes pero no se puede escuchar nada no se captura ningún audio, debido a que está protegido con el protocolo *(TLS)*, por lo que

únicamente puede ser decodificado por la extensión de la dirección de destino cuyo certificado de seguridad es asignado desde el servidor al cliente. Tal como se muestra en la siguiente imagen:

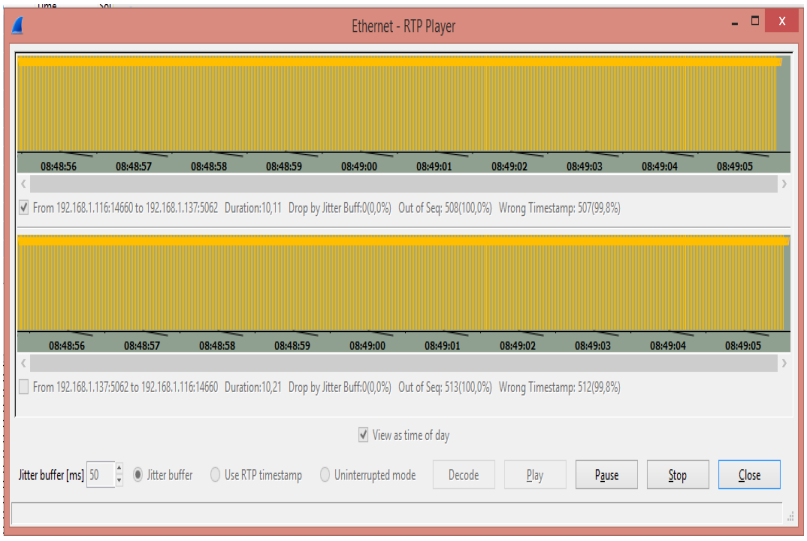


Ilustración 108: Captura de audio cifrado con Wireshark
Fuente: El Autor (2015).

Con esta comprobación la implementación está lista para ser configurada en el servidor de *(VoIP),* que está en funcionamiento en el Hospital Isidro Ayora de Loja. Se debe mencionar que por cuestiones ajenas a la voluntad del investigador, no se realiza la implementación, debido el administrador del departamento de *(TIC),* aduce que actualmente la red de datos misma que contempla la red de *(VoIP),* está sujeta a constantes cambios, tanto físicos como lógicos, por ejemplo la re-distribución de *(VLAN), (voz, datos)* y de usuarios, asignándose por roles, con el fin de mejorar las políticas de seguridad, razón por la cual, la aplicación será implementada cuando el administrador del departamento de *(TIC),* disponga la realización de los cambios en el servidor *(VoIP),* del Hospital Isidro Ayora de Loja. Cumpliendo así con los objetivos planteados en la presente investigación.

7. DISCUSIÓN

7.1. EVALUACIÓN DEL OBJETIVO DE INVESTIGACIÓN.

El proyecto de tesis se desarrolló cumpliendo con los requisitos establecidos en cada una de las faces, cumpliendo de esta forma los objetivos específicos que se planteó en el inicio de esta investigación, misma que se describen a continuación:

Tabla 47: Evaluación de los objetivos planteados.

OBJETIVOS ESPECÍFICOS	RESULTADO
Analizar la situación actual de la red de *(VoIP)*, del Hospital Isidro Ayora de Loja, mediante el uso de herramientas informáticas.	Para poder llevar a cabo este objetivo, se realizaron entrevistas al personal del departamento de *(TIC)*, con el fin de conocer la infraestructura, funcionamiento y procedimientos de la red de *(VoIP)*. Además se utilizó herramientas informáticas de seguridad *(sniffers)*, para realizar un pentest y determinar las vulnerabilidades en la red de *(VoIP)*, utilizando la metodología *(OSSTMM)*, de la misma manera se utilizó la metodología *(OCTAVE)*, para realizar una valoración de riesgos en los activos críticos de la institución, gracias a ello se culminó de forma exitosa con este objetivo.
Realizar un análisis comparativo de los protocolos existentes para la seguridad de redes *(VoIP)*.	Para la ejecución de este objetivo se realizó un análisis de las características más relevantes de los protocolos *(IPSec)* y *(SSL/TLS)*, por ser firmes candidatos para encriptar la voz sobre *(IP)*. Por las características que presenta la red *(VoIP)*, se eligió el protocolo *(SSL/TLS)*, por ser el que se acopla a la infraestructura de la red y de esta forma la seguridad en las comunicaciones *(VoIP)*, de la institución. La principal ventaja de este protocolo, es que se lo puede implementar en la plataforma Asterisk, permitiendo establecer un canal cifrado, para realizar las comunicaciones, sin realizar modificaciones en la red *(VoIP)*, del Hospital.
Implementar el protocolo de seguridad en la red *(VoIP)* que se encuentra en el Hospital Isidro Ayora de Loja.	Para poder llevar a cabo este objetivo, se debió realizar un escenario de pruebas, donde se realizó un backup del servidor de *(VoIP)*, que está en funcionamiento, en el cual se configuro el protocolo *(SSL/TLS)*, para ello fue necesario actualizar el kernel de Asterisk, así mismo se modificaron los archivos de configuración de para configurar el soporte de *(SSL/TLS)*, en Asterisk, finalmente se configuró los terminales, obteniéndose un túnel criptográfico punto a punto, para establecer las comunicaciones las cuales circulan por el puerto *(UDP 5061)*, mismo que permite la transmisión de voz manera cifrada.
Realizar las pruebas del funcionamiento del protocolo implementado en la red *(VoIP)*.	Una vez realizadas las pruebas de configuración, se puede notar que los paquetes ya no se transmiten en texto plano, es decir, ahora se transmiten por un canal cifrado, evitándose de esta forma la interpretación o *eavesdropping*, en las comunicaciones, la denegación de servicio, entro otros por ende, la red *(VLAN)*, de voz queda establecida con un buen nivel de seguridad.

Fuente: El Autor (2015).

7.2. VALORACIÓN TÉCNICA, ECONÓMICA, AMBIENTAL.

En el siguiente apartado, se dará a conocer el detalle de los recursos que son necesarios para llevar a cabo esta investigación.

7.2.1. Valoración técnica y económica.

La inversión económica, para el desarrollo de esta investigación se establece en término medio, debido a que la gran mayoría de herramientas informáticas que fueron utilizadas trabajan bajo una plataforma de software libre (GNU/LINUX). Lo que se requiere es tiempo, para realizar los análisis, escáner y configuraciones en la red, razón por la cual, se implementa el número de horas trabajadas, el financiamiento de los recursos materiales y equipos de trabajo, han sido proporcionados tanto por el Tesista como por el departamento de *(TIC),* del Hospital Isidro Ayora de Loja. Para la ejecución del presente proyecto el equipo que se utilizo es el siguiente:

Un ordenador para realizar las pruebas de penetración a la red, así mismo para poder acceder al servidor remotamente, cuyas características principales son:

Tabla 48: Características de computador intruso.

ORDENADOR	CARACTERISTICAS
Procesador	Intel(r) core(tm) i7-2670qm CPU @ 2.20ghz
Video Card	Intel(r) HD Graphics 3000
Memory	8 GB
Operating system	Microsoft Windows 8.1 Profesional Edition (build 9600), 64-bit Kali Linux 1.2 LTS Edition home 64-bits

Fuente: El Autor (2015).

Este equipo esta dotados de dos sistemas operativos tomando como el principal el sistema operativo *(Kali-Linux),* por contar con más de 300 herramientas (sniffers), para realizar pruebas de penetración integradas en su kernel, facilitando la tarea del investigador, de las cuales, las más importantes fueron: *nmap; hping3; wireshark; enumiax; sipcrack; hydra; medusa; brute force hitag2; ettercap-graphical; svmap.*

El sistema operativo *(Microsoft Windows 8.1),* se lo utilizo para levantar la documentación de la investigación, el cual cuenta con herramientas propias de esta plataforma como *Microsoft Office, WinSCP y PuTTy (multiplataforma)* para poder interactuar con el servidor Asterisk. Así mismo se instaló Packet Tracer para realizar los diseños y esquenas de la topología de la red.

El servidor de *(VoIP)*, fue utilizado el que se encuentra en funcionamiento el Hospital Isidro Ayora de Loja, el cual cuenta con un núcleo 5.9 de *CentOS*, en el cual, está funcionando *Asterisk* 1.8.0.20 y *Elastix* 2.4, mismo que se utilizó para realizar las pruebas de penetración o testing. Para la implementación y configuración de las medidas de seguridad se utilizó un servidor de pruebas ajeno a la institución, esta cuenta con la misma versión del sistema operativo, en el cual se instaló un backup del servidor que se encuentra en funcionamiento en el Hospital para contar con las mismas configuraciones.

Así mismo se utilizó dos máquinas *(Toshiba i5, DELL i5)*, con sistemas operativos Microsoft Windows que sirvieron como clientes, para poder realizar y comprobar las configuraciones realizadas en el servidor y poder realizar las llamadas ya sea entre los teléfonos *(IP)* físico o los softphones *(PhonerLite).* Cuyas características se detallan a continuación:

Tabla 49: Características de los equipos clientes.

DELL	CARACTERISTICAS
Procesador	Intel(R) Core(TM) i5-2430 M CPU @ 2.40ghz 2.40
Video Card	Intel(R) HD Graphics 3000
Memory	6 GB
Operating system	Microsoft Windows 8 Profesional Edition (build 9600), 64-bit
TOSHIBA	**CARACTERISTICAS**
Procesador	Intel(R) Core(TM) i5-4200 CPU @ 1.60GHz
Video Card	Intel Family (R) HD Graphics
Memory	4.0 GB
Operating system	Microsoft Windows 8 Profesional Edition (build 9600), 64-bit

Fuente: El Autor (2015).

Los teléfonos *(IP) (Yealink, Atcom)* que se utilizó para esta investigación fueron proporcionados por la institución.

Un router *(netxx)* inalámbrico para realizar una red *(LAN)* y poder configurar y comprobar las medidas de seguridad realizadas.

- **Valoración ambiental.**

La solución propuesta, como tal, genera un daño mínimo al medio ambiente, por realizarse las configuraciones a nivel de *software*, por ende, el único daño que se genera es al momento de utilizar energía eléctrica.

8. CONCLUSIONES

Una vez finalizado el presente proyecto donde se implementa medidas de seguridad en la red de *(VoIP),* del Hospital Isidro Ayora de Loja, se dedujeron las siguientes conclusiones:

- Con la configuración e implementación del protocolo de seguridad *(TLS),* en el servidor de *Asterisk* se contrarrestó ataques como el eavesdropping *(MitM),* es decir, se redujo drásticamente las escuchas indebidas en la red, ya que *(TLS),* genera un túneles cifrados para la transmisión de la comunicación entre los dos extremos *(origen, destino)* y de esta manera proteger la integridad, disponibilidad y confidencialidad de la información.

- Las soluciones que se implementaron en el archivo `sip.conf`, tuvieron éxito porque se logró bloquear a usuarios anónimos que intentaban acceder al sistema, con el fin de obtener información del servidor, de esta manera se ha logrado contrastar las vulnerabilidades encontradas, como la *(DoS),* sin embargo, es importante pensar que estas no son las únicas soluciones posibles y que no habrá medida de seguridad que brinde el 100%, de fiabilidad, pero existen métodos para corregir estas vulnerabilidades, sobre todo, está el sentido común del administrador de la red, para realizar medidas de protección y despistar a los usuarios mal intencionados que quieran ingresar a sus sistema.

- Durante la etapa de análisis y el testing de vulnerabilidades aplicadas a las comunicaciones *(VoIP),* se demostró que existen amenazas de seguridad, causadas por contar con las configuraciones por defecto del servidor *Asterisk*, falta de robustez en sus contraseñas o las mismas contraseñas para el acceso a los sistemas, además, se tenía puertos innecesarios abiertos en el servidor los cuales mostraban los servicios que se están corriendo en cada uno de ellos, debido a esto se facilitó la tarea para ingresar de manera anónima al sistema, estas vulnerabilidades se corrigieron con la instalación de la herramienta *fail2ban* y asegurando el puerto *(SSH),* del servidor.

- El uso de herramientas informáticas *(sniffer),* facilita la tarea del investigador para determinar las vulnerabilidades informáticas dentro de una organización se logró

determinar que el servidor de comunicaciones *(VoIP)* del Hospital estaba sujeto a vulnerabilidades con un alto riesgo de probabilidad, como son las escuchas indebidas en la red *(eavesdropping).*

- Con la configuración de los parámetros de seguridad en el archivo `sshd_config`, se demostró que se reduce potencialmente el acceso al sistema, ya que a que se asigna permisos únicos para administrados de la red, autenticándose únicamente por un clave privada, con esto estamos bloqueando a usuarios mal intencionados que intenten ingresar al sistema, por lo tanto se reduce al mínimo las vulnerabilidades de cracking de contraseñas y accesos no autorizados.

- Los problemas de seguridad en redes *(VoIP)* no solo radican en los protocolos en los que se apoyan para generar los servicios de telefonía. Hay que tener muy en cuenta la seguridad de la red de datos por las que se trasmite, debido a que la tecnología *(VoIP)* hereda las vulnerabilidades de una red de datos tradicional.

- Los procesos de la metodología *(OCTAVE)* permiten llevar a cabo un proceso minucioso y sistemático,, mientras que la metodología *(OSSTMM)* dice como se tiene que realizar una evaluación de seguridad, razón por la cual resulta satisfactorio la fusión de estas dos tecnologías, ya que juntas permiten realizar una evaluación completa a los activos de una organización. Por medio de estas metodologías se conoció los puntos críticos en la red *(VoIP)* y se supo cómo evaluarlos, de esta forma se determinó la probabilidad de amenazas y los ataques a los que están sujetos estos activos, luego se los clasifica de acuerdo a la magnitud e impacto; los riesgos más altos son utilizados para determinar una estrategia de seguridad cuyo fin es contrarrestar dicha vulnerabilidad y evitar ataques que puedan degradar el servicio de la tecnología *(VoIP)* y por ende el funcionamiento dela institución.

9. RECOMENDACIONES

- Realizar de manera periódica un evaluación de las medidas de seguridad implementadas a la red y a *(VoIP),* o en si una auditoría de sistemas por lo menos una vez al año.

- Crear políticas de seguridad de la información, para garantizar una correcta seguridad tanto en servidores como en terminales.

- Se recomienda implementar *(OpenVPN),* en los sistema *(VoIP),* por considerarse, una medida de seguridad adicional, para reforzar, la encriptación en las comunicaciones, que dicho sea de paso son fáciles de implementar, sin necesidad de hacer cambios en la red.

- Los dispositivos que se encuentran en la red *(VoIP),* como *switch* y *router*, deben estar actualizados en términos de *firmware* y actualizaciones de seguridad

- Ubicar el *hardware* en sitios seguros, obedeciendo políticas de seguridad, para que no tengan acceso personas particulares, sino personas debidamente autorizadas.

- Se debe utilizar una metodología que contemple todas las etapas de un proyecto, como son el análisis, diseño e implementación, para que el proyecto pueda ser evaluado en cada etapa y se pueda concluir con éxito.

- Al ser una tecnología que está en constante evolución *(VoIP),* se recomienda al responsable de la administración, estar en constante aprendizaje, de nuevas técnicas de protección *(VoIP)* y de las nuevas vulnerabilidades o riesgos y así poderlos afrontar de mejor manera en un futuro.

- En vista que el Hospital Isidro Ayora de Loja, cuenta con un 90% de teléfonos que no soportan *(TLS),* descritos en el análisis de la situación actual, razón por lo cual, se recomienda cambiar de tecnología que soporte esta configuración, con el fin de mantener seguras las comunicaciones, entre los usuarios de esta tecnología.

- Configurar los equipos del cliente y exigir el uso correcto de las contraseñas.
- No emplear la misma contraseña para todos los servicios y equipos.
- No utilizar contraseñas con fecha de nacimiento, nombres o números de teléfonos.
- Obtener el firmware que se necesita desde los sitios oficiales de Internet.
- No instalar software que no sea original o pre instalado sin el soporte original.
- No utilizar cuentas con privilegios administrativos para navegar por Internet.
- Actualizar periódicamente los servicios instalados en los servidores
- Revisar diariamente las alertas proporcionadas por el servidor.
- Deshabilitar puertos que no se estén utilizando en los equipos.
- Utilizar contraseñas que contengan mínimo 8 caracteres, con letras mayúsculas, minúsculas números y caracteres especiales.
- Usar estrictamente conexiones *(SSH),* para la administración y configuración de los equipos.
- Obtener copias de seguridad cada vez que se realicen cambios en los servidores, donde impliquen la configuración de políticas.
- Cambiar las configuraciones por defecto por ser una potencial amenaza para la seguridad
- Cambiar la contraseña de equipos y servidores, cuando se ha identificado algunos accesos no autorizados.
- Obtener copias de seguridad de la configuraciones de los equipos de forma trimestral
- El departamento de *(TIC)*, debe respaldar, las plataformas de *(VoIP)* y terminales de la institución.
- Todo respaldo que se realice periódicamente o esporádicamente, debe contar con una documentación mínima que sirva de guía, para el área de operación y/o mantenimiento.
- Prohibir a los usuarios dar a conocer su contraseña a terceras personas
- Si el usuario sospecha que su contraseña ha sido comprometida, avisar inmediatamente al departamento de *(TIC)* para su cambio.

10. BIBLIOGRAFÍA

[1] J. A. C. Falcón, VoIP : la telefonía de Internet, España: Editorial Paraninfo, 2010.

[2] José Manuel Huidobro, David Roldán Martínez, Tecnología VoIP: la telefonía por Internet, Puebla: Alfa Omega Grupo Editor, 2010.

[3] J. M. H. Moya, Redes y servicios de telecomunicaciones, Madrid: Thomson Editores Spain S.A, 2006.

[4] M. J. L. Campos, SEGURIDAD EN VOZ SOBRE IP, Valparaíso: Editorial FUGA , 2010..

[5] W. Stalling, Fundamentos de Seguridad en Redes Aplicaciones y Estandares, Madrid: Imprenta FARESO, S.A. , 2013.

[6] Menalkiawn, Manual Básico De Seguridad Informática Para Activistas, Barcelona: Editorial Klinamen, 2013.

[7] Pablo GonzalesPeres german sanches garces jose miguel soriano , Pentesting con kali, Madrid: OxWORD Computing S.L. Printed-Spain, 2013.

[8] A. Mogollón, Analisis Comparativo: Metodologías de análisis de Riesgo, Barquisimeto: Monte Avila Editores Latinoamericana, 2011.

[9] Meucci, Matteo; Muller, Andrew, OWASP Testin Guide, Nueva York: Penguin Random House U.S.A - New York, NY, 2010.

[10] B. Rathore, Information Systems Secury Assessment Framework, Colorado: Social Science Research Council, 2009.

[11] P. Herzog, «OSSTMM 2.1.,» *INSTITUTE FOR SECURITY AND OPEN (ISECOM),* vol. II, nº 8, pp. 12-23, 2003.

[12] Fernández-Laviada, Ana, La gestión del riesgo operacional, Madrid: Infoprint, S.L, 2010.

[13] A. Lopez, El portal de ISO 27001 en Espanol., Madrid: Clara M. de la Fuente Rojo, 2010.

[14] A. S. Tanenbaum, Redes de comptadoras, Puebla: Camara Nacional de la Idustria Editorial Mexicana Reg. Num 1031, 2003.

[15] Eduardo Magaña Lizarrondo Edurme Mendi, Manuel Prieto Jesus Villadangos, Comunicaciones y redes de computadores, Madrid: PEARSON EDUCACIÓN.S.A., 2012.

[16] A. I. Manzanares, METODOLOGÍA PARA LA VALIDACIÓN DE PROTOCOLOS DE SEGURIDAD IPESC, LEGANÉS: Thomson Editores Spain S.A., 2010.

[17] Jaime Gutiérrez, Juan Tena , Protocolos Critográficos y seguridad en redes, Santander: Servicio de Publcaciones de la Universidad de Cantabria , 2013.

[18] C. M. University, «Software Engineers Institute,» Carnegie Mellon University , 16 Julio 2001. [En línea]. Available: http://www.sei.cmu.edu/. [Último acceso: 18 Mayo 2015].

[19] Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, Gray Hat Hacking, United States: The McGraw-Hill Companies, 2011.

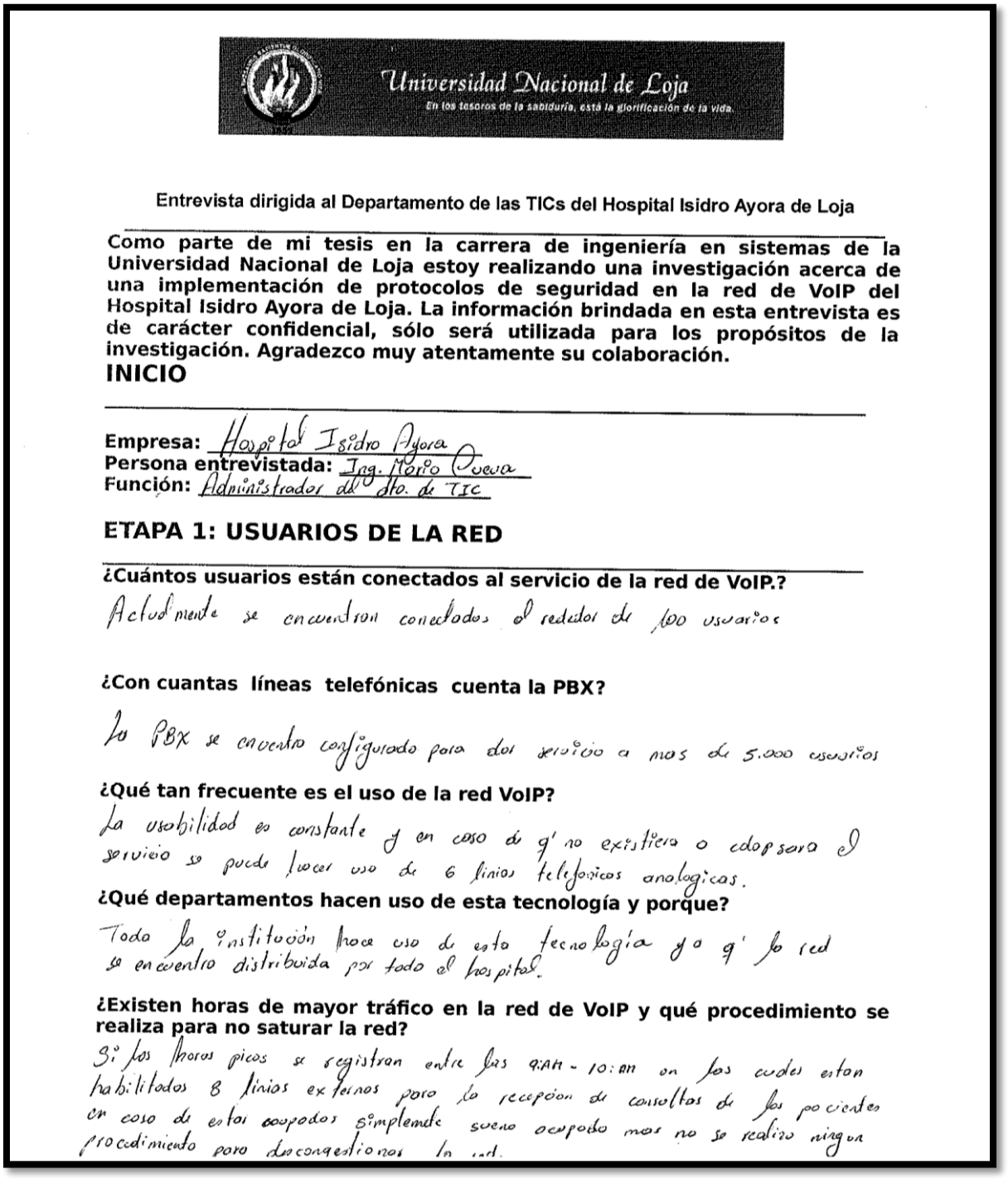
[20] J. Almeida, «Aplicaciones para Asterisk,» 6 Agosto 2013. [En línea]. Available: http://juanelojga.blogspot.com/2013/08/srtp-y-tls-en-elastix-actualizado.html. [Último acceso: 20 Octubre 2015].

[21] NICOLAS ERNESTO ORTIZ HERNANDEZ, ROBERTO ANTONIO HOYOS LOAIZA, *MODELO DE ASEGURAMIENTO PARA REDES DE VOZ VoIP APLICABLE EN UN,* Bogota, D.C: CIS0830-SD02, 2009.

[22] J. Oliva, «SEGURIDAD EN ELASTIX,» 2 JULIO 2012. [En línea]. Available: https://jroliva.wordpress.com/2012/07/02/modulo-de-seguridad-en-elastix-restringir-el-acceso-al-entrorno-web/. [Último acceso: 13 Novienmbre 2015].

11. ANEXOS

ANEXO A. ENTREVISTA AL ADMINISTRADOR DE TICs



Universidad Nacional de Loja
En los tesoros de la sabiduría, está la glorificación de la vida.

Entrevista dirigida al Departamento de las TICs del Hospital Isidro Ayora de Loja

Como parte de mi tesis en la carrera de ingeniería en sistemas de la Universidad Nacional de Loja estoy realizando una investigación acerca de una implementación de protocolos de seguridad en la red de VoIP del Hospital Isidro Ayora de Loja. La información brindada en esta entrevista es de carácter confidencial, sólo será utilizada para los propósitos de la investigación. Agradezco muy atentamente su colaboración.

INICIO

Empresa: Hospital Isidro Ayora
Persona entrevistada: Ing. Mario Cueva
Función: Administrador del dto. de TIC

ETAPA 1: USUARIOS DE LA RED

¿Cuántos usuarios están conectados al servicio de la red de VoIP.?

Actualmente se encuentran conectados al rededor de 100 usuarios

¿Con cuantas líneas telefónicas cuenta la PBX?

La PBX se encuentra configurado para dar servicio a mas de 5.000 usuarios

¿Qué tan frecuente es el uso de la red VoIP?

La usabilidad es constante y en caso de q' no existiera o colapsara el servicio se puede hacer uso de 6 lineas telefonicas analogicas.

¿Qué departamentos hacen uso de esta tecnología y porque?

Toda la institución hace uso de esta tecnología ya q' la red se encuentra distribuida por todo el hospital.

¿Existen horas de mayor tráfico en la red de VoIP y qué procedimiento se realiza para no saturar la red?

Si las horas picas se registran entre las 9:AM - 10:AM en las cuales estan habilitados 8 lineas externas para la recepcion de consultas de los pacientes en caso de estar ocupadas simplemte suena ocupado mas no se realiza ningun procedimiento para descongestionar la red.

ETAPA 2: ESTRUCTURA Y DISEÑO DE LA RED

¿Cómo se encuentra diseñada la estructura de la red?

Cuento con 202 puntos de red aproximadamente los cuales 106 son puntos de red y 96 puntos para voz el cableado es UTP categoria 6 los solo para 48 puntos de red

¿La red de VoIP es solo interna o se comunica con otra troncal fuera de esta entidad?

La red de VoIP es solo de uso interno no tiene salido con otra entidad.

¿La empresa cuenta con una sala de servidores para los equipos de red?

No se cuenta con una sala apropiada para la infraestructura de red ya q' la institución no cuenta con el presupuesto necesario ni el espacio físico para alvergar toda la infraestructura.

ETAPA 3: EQUIPO DE LA RED DE VOIP

¿Cuál es el proveedor de servicio de internet que actualmente está conectado al Backbone?

El proveedor q' actualmente tiene la institución es (CNT) Corporación Nacional de Telefonia.

¿Qué servidor se utilizan para la tecnología de la red VoIP?

HP word 6 Quad Core

¿Esta tecnología trabaja bajo software libre o algún software privativo?

Bajo Software libre (AsteriskK) en el cual se implemento (elastix) para la PBX con un nucleo de (Centos 5.4)

¿La estructura física de la red VoIP se implementó bajo algún estándar o norma?

El 90% de la instalacion del cableado estructurada esta bajo categoria (5e) el cual se la realizo hace 5-6 años atras (lo cual ya es necesario cambiar)

¿Cuenta con algún software donde pueda administrar a los usuarios que utilizan esta red?

Si para la administracion de los usuarios se la realiza mediante Zentyal 2.2.2 q' es es un SO distribución de Linux para servidores.

ETAPA 4: OPERATIVIDAD DE LA RED

¿Para dar el servicio de VoIP se tiene segmentada la red a través de VLANs?

Todos la red se encuentra segmentada a través de VLAN la cuales estan dando servicio a cada grupo de usuario con el fin de no saturar la red.

¿Desde el servicio de VoIP se da otro servicio adicional?

No ya q' existe una VLAN asignada al servicio de Voz la cual esta con una priorizacion de servicio con el fin de no saturar la red.

¿Utiliza algún firewall u otros controles de acceso para proteger los servidores?

Si se utiliza firewall e incluso un IDS (sistema de deteccion de intrusos) con el fin de proteger la red interno como amenazo externas.

¿Utiliza reglas o ACL para protección de la información?

Si en cada una las VLANs se configuran reglas con el fin de brindar cierto tipo de seguridad

¿Qué protocolos están implementados actualmente para la seguridad de este servicio?

No se encuentran implementado ningun protocolo de seguridad lo q' nos hace vulnerables con la informacion q' se transmite. Para la calidad de servicio se encuentran implementados 802.1q y 802.1p.

¿La entidad tiene políticas o normas, para realizar implementaciones de algún servicio de esta índole, o simplemente el técnico se encarga de hacerlo?

No existen politicas de red Standarizadas solo se dan capacitaciones para la usabilidad de ciertos servicios como: correos, simbia, Quipux, etc.

¿Cuál es el procedimiento para implementar un nuevo usuario a la red?

Segun el requerimiento del usuario simplemente se le agrega un nuevo punto de red y se le agrega al sistema.

¿Cuándo los usuarios requieren acceder a este servicio se le da un usuario y autenticación?

Simplemente se les agrega a la PBX una nueva extención pues el el usuario no manejo ninguna autenticacion ya q' eso solo tiene conocimiento el administrador de la red

¿Hay algún programa para divulgar medidas de seguridad en su empresa?

Cuando esto sucede simplemente se acude al punto donde se registra el incidente y se empieza a buscar y no se da una ninguna capacitación de esto en la empresa, o solo a ciertos personas de forma verbal.

ETAPA 5: PROBLEMAS ACTUALES DE LA RED

¿Actualmente la red presenta algún problema ya sea en la parte física o lógica?

Si se han presentado ataques como denegación de servicio, asimiso se descubrieron escuchas en la red por el mismo personal interno (existe interferencia en ciertos horas).

¿Cuándo se presenta algún incidente ya sea por negación de servicio con el usuario o por saturación de la red como es el procedimiento para habilitar la conectividad?

Se busca de forma empírica en el lugar donde se realiza el incidente

¿Se ha presentado alguna vez un incidente donde la red fue víctima de alguna escucha indebida (Eavesdropping), ataque de denegación de servicio (DoS) etc.?

Directamente no pero si se han registrado este tipo de incidentes en alguna ocasion fue una broma pero si se puede dar esto en la red.

¿Cuándo se establece una comunicación entre los usuarios de la red estos pueden discutir cualquier tipo de información entre los mismos o se maneja alguna política interna para transmitir información sumamente delicada?

Si ellos comunican todo tipo de información no existia politica o restricion alguna

¿Si usted les da una contraseña tiene activado algún control para bloquear el servicio después de algún número de intentos fallidos?

Si pero solo con ciertos personas como Administrador o Gerente o personal tecnico y poseen conocimiento informatico con el fin de evitar errores o incidentes por desconocimiento.

¿Alguna vez se ha realizado alguna auditoría de seguridad en la red de VoIP?

Si lo hicieron hace unos 2 años otros cuando se implemento los nuevos unidades de Hemodialis y quemados.

MINISTERIO DE SALUD PÚLICA
HOSPITAL GENERAL ISIDRO AYORA
DEPARTAMENTO TIC'S

ANEXO B. CARTA DE AUTORIZACIÓN.

UNIVERSIDAD NACIONAL DE LOJA

OFICIO-CIS-UNL

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

Of. N° 465 CIS-AEIRNNR-UNL
Loja, 27 de abril de 2015

Señor Ingeniero
Byron Guerrero
GERENTE HOSPITAL ISIDRO AYORA
Ciudad.

De mi consideración:

Mediante el presente me dirijo a usted con la finalidad de solicitar de la manera más comedida se sirva dar las facilidades al Sr. **CRISTIAN LEONARDO CALDERÓN ORDÓÑEZ** con CI 1104617053, estudiante del décimo módulo de la Carrea de Ingeniería en Sistemas de la Universidad Nacional de Loja, para que puedan recolectar la siguiente información:

- Aplicar entrevistas al encargado o administrador de la red de VoIP existente en el Hospital Isidro Ayora.
- Realizar encuestas a los usuarios finales de red de VoIP.
- Conocer las políticas y procedimientos que se lleva a cabo en el departamento de TIC's para dar el servicio de VoIP a un usuario.
- Acceder a las PBX con el fin de realizar pruebas de usabilidad del servicio de Volp.
- Tener acceso al servidor y a la configuración de la red de Volp.
- Acceder al servidor de la red de VoIP para poder realizar la implementación, del o los protocolos de seguridad.
- Permiso para poder realizar pruebas de configuraçiones en los terminales de la red VoIP.

Pedido que lo hago en razón de que dicha información servirá para la realización y desarrollo de su proyecto de tesis titulado "**IMPLEMENTACIÓN DE PROTOCOLOS DE SEGURIDAD PARA LA RED DE VoIP DEL HOSPITAL ISIDRO AYORA DE LOJA.**", debiendo indicar que, la información brindada y recolectada, será de carácter confidencial, y será utilizara únicamente con el propósito de la investigación antes indicada.

Sin otro particular me suscribo de usted.

Cordialmente,

MINISTERIO DE SALUD PÚLICA
HOSPITAL GENERAL ISIDRO AYORA
DEPARTAMENTO TIC´S

Ing. Walter Rodrigo Tene Ríos
COORDINADOR DE LA CARRERA DE INGENIERÍA EN SISTEMAS.

C.c. Archivo,
Elisa Orellana

ANEXO D. METODOLOGÍA OSSTMM

El Manual de la Metodología Abierta de Comprobación de la Seguridad *(OSSTMM, Open Source Security Testing Methodology Manual)* es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet. Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría. Se encuentra en constante evolución. Para mayor claridad, *ISECOM* aplica los siguientes términos a los diferentes tipos de sistemas y de testeos de seguridad de redes, basados en tiempo y costo para el Testeo de Seguridad de Internet:

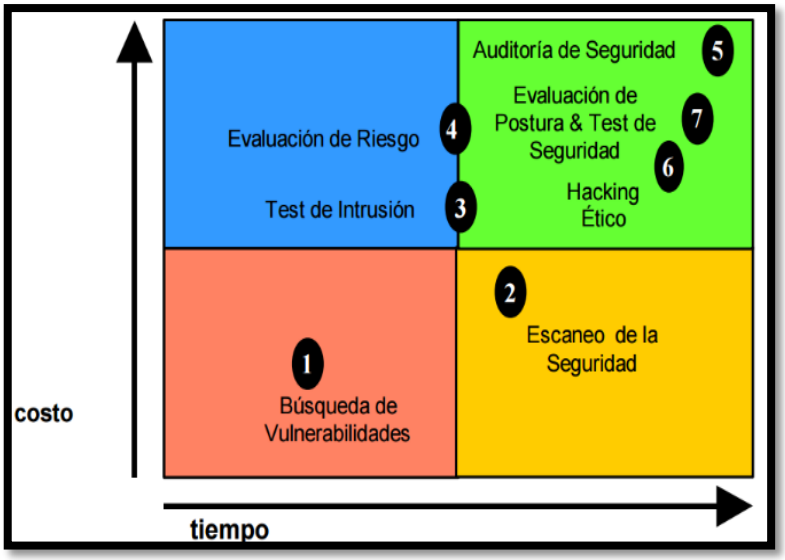


Ilustración 109: Valoración de la Metodología OSSTMM.
Fuente: INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES Pete Herzog (2000)

Mapa de Seguridad

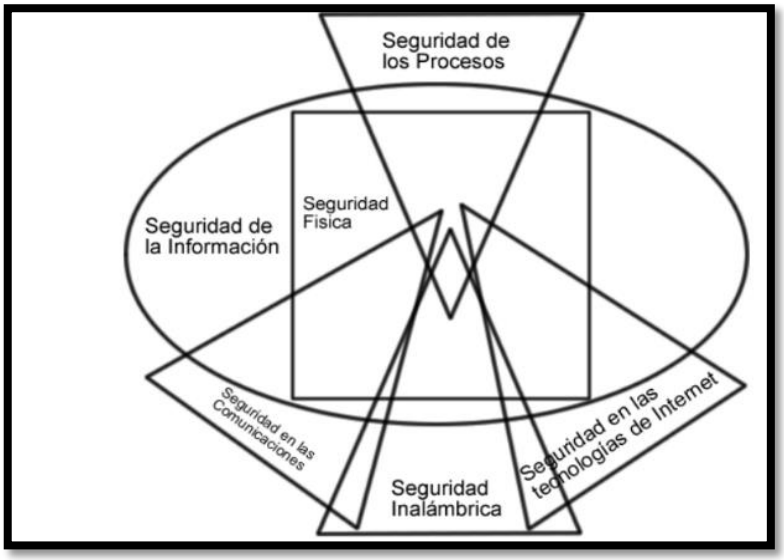


Ilustración 110: Mapa grafico de la metodología OSSTMM.
Fuente: INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES Pete Herzog (2000).

La lista de módulos del mapa de seguridad son los elementos primarios de cada sección. Cada módulo debe incluir todas las Dimensiones de Seguridad que están integradas con tareas a ser desarrolladas. Para desarrollar un análisis de seguridad *OSSTMM* de una sección particular, todos los módulos de la sección deben ser desarrollados y aquellos para los que no exista infraestructura y no pueda ser verificada, deben definirse como NO APLICABLE en la hoja de datos *OSSTM* anexa al informe final. Esta corresponde al ambiente de un análisis de seguridad y está compuesta por seis secciones equivalentes a las de este manual. Las secciones se superponen entre si y contienen elementos de todas las otras secciones. Un análisis apropiado de cualquier sección debe incluir los elementos de todas las otras secciones, directa o indirectamente.

Tabla 50: Secciones de la Metodología (OSSTMM).

SECCIÓN	MODULO
Seguridad de la Información	Revisión de la Inteligencia Competitiva Revisión de Privacidad Recolección de Documentos
Seguridad de los Procesos	Testeo de Solicitud Testeo de Sugerencia Dirigida Testeo de las Personas Confiables
Seguridad en las tecnologías de Internet	Exploración de Red Identificación de los Servicios del Sistema Búsqueda y Verificación de Vulnerabilidades Testeo de Aplicaciones de Internet Enrutamiento Testeo de Sistemas Confiados Testeo de Control de Acceso Testeo de Sistema de Detección de Intrusos Testeo de Medidas de Contingencia Descifrado de Contraseñas Testeo de Denegación de Servicios Evaluación de Políticas de Seguridad
Seguridad en las Comunicaciones	Testeo de PBX Testeo del Correo de Voz Revisión del FAX Testeo del Modem
Seguridad Inalámbrica	Verificación de Radiación Electromagnética (EMR) Verificación de Redes Inalámbricas [802.11] Verificación de Redes Bluetooth Verificación de Dispositivos de Entrada Inalámbricos Verificación de Dispositivos de Vigilancia Inalámbricos Verificación de Dispositivos de Transacción Inalámbricos Verificación de RFID Verificación de Sistemas Infrarrojos
Seguridad Física	Revisión de monitoreo Evaluación de Controles de Acceso Revisión de Respuesta de Alarmas Revisión de Ubicación Revisión de Entorno

Fuente: El Autor (2015)

ANEXO E. METODOLOGÍA OCTAVE.

OCTAVE utiliza un enfoque de tres fases para examinar las cuestiones de organización y tecnología, reuniendo una visión global de las necesidades de seguridad de la organización de la información. El método utiliza talleres para fomentar la discusión abierta y el intercambio de información sobre los activos, las prácticas de seguridad y estrategias.

FASES Y SUS PROCESOS

FASE 1: GENERAR PERFILES DE ACTIVOS BASADOS EN LA AMENAZA.

Esta es una evaluación organizacional y se refiere a dos tareas importantes:

- Recopilación de información de los distintos niveles de la organización.
- Análisis de esa información.
- El equipo de análisis determina cuales activos son más importantes para la organización (activos críticos) e identifica lo que se está haciendo para proteger esos activos.

Proceso 1: Identificar los conocimientos de Dirección

Este proceso despierta el conocimiento de los altos directivos. Estos gerentes fueron seleccionados durante la preparación de *OCTAVE* para proporcionar una buena muestra de la alta dirección de la organización. El proceso 1 consta de las siguientes actividades:

- **Identificar los elementos importantes:** Los altos directivos definir qué bienes son importantes para ellos y la organización. También priorizar los activos para identificar los cinco más importantes.

- **Describir las áreas de preocupación:** Para los cinco valores más importantes, altos directivos describen situaciones en las que tales activos se ven amenazados.

- **Definir los requerimientos de seguridad de los activos importantes:** Los altos definen los requisitos de seguridad para los activos importantes.

- **Identificar las estrategias actuales de protección y vulnerabilidades organizacionales:** Los altos directivos completan las encuestas basadas en el catálogo de prácticas, discuten sus respuestas para proporcionar más información sobre lo que se está y no se está haciendo bien en términos de seguridad.

- **Revisar el alcance de la evaluación:** Las áreas operativas y sus gerentes de los talleres en el Proceso 2 se seleccionaron inicialmente durante las actividades de preparación para *OCTAVE*. Esta es una segunda oportunidad para los gerentes de alto nivel, habiendo participado en el proceso, para modificar o agregar áreas operativas y gerentes a la lista.

Proceso 2: Identificar los conocimientos en el área de gestión operativa.

El proceso 2 provoca el conocimiento de los administradores de las áreas operativas. Estos son los responsables de las áreas seleccionadas en el momento de la definición del alcance de *OCTAVE*. Estas áreas operacionales proporcionar una buena sección transversal de la organización. El proceso 2 consta de las siguientes actividades: La identificación de los activos importantes:

- **Descripción de las áreas de interés:** Para los cinco valores más importantes, los gerentes de operaciones de la zona describen situaciones en las que tales activos se ven amenazados.

- **Definición de los requisitos de seguridad para los activos importantes:** Es responsabilidad de la zona de definir los requisitos de seguridad para los activos importantes.

- **La identificación de las estrategias actuales de protección y vulnerabilidades de la organización:** Los gerentes operativos del área completan las encuestas basadas en el catálogo de prácticas, discuten sus respuestas para proporcionar información adicional sobre lo que se está haciendo bien y lo que no se está haciendo en términos de seguridad.

- **Verificación de los participantes del personal:** Los miembros del personal de los talleres en el proceso 3 se seleccionaron inicialmente durante las actividades de preparación para *OCTAVE*. Esta es una segunda oportunidad para los administradores de las áreas operativas, habiendo participado en la preparación, para modificar o añadir personal a la lista.

Proceso 3: Identificar los conocimientos del personal

El proceso 3 despierta el conocimiento por parte del personal en general y el personal de las tecnología de la información *(TI).* Todo el proceso consiste en las siguientes actividades *(pueden existir diferencias para las actividades dirigidas al personal del TI):*

- **La identificación de los activos importantes**: los miembros del personal definen qué activos son importantes para ellos y la organización. También priorizan los activos para identificar los cinco más importantes. El personal de *(TI),* en particular, debe centrarse en cuáles son los activos que necesitan para hacer su trabajo.

- **Descripción de las áreas de preocupación:** para los cinco valores más importantes, los integrantes describen situaciones en las que tales activos se ven amenazado

- **Definición de requisitos de seguridad para los activos importantes:** los miembros del personal definir los requisitos de seguridad para los activos importantes.

- **La identificación de las estrategias actuales de protección y vulnerabilidades de la organización:** los integrantes completan las encuestas basadas en el catálogo de prácticas. Discuten sus respuestas para proporcionar información adicional sobre lo que se está haciendo bien y lo que no se está haciendo en términos de seguridad. El personal en general y el personal de *(TI)* tienen diferentes encuestas.

Proceso 4: Crear perfil de Amenaza

El proceso 4 integra toda la información recogida durante los talleres de recolección de conocimiento en los procesos 1 a 3 y crea perfiles de amenaza para un conjunto de activos críticos. En el proceso 4 las actividades son realizadas por el equipo de análisis *(con miembros adicionales, si se desea)*. Se compone de las siguientes actividades:

- **Consolidación de datos preliminar:** el equipo de análisis recoge las listas de activos, requisitos de seguridad, y áreas de interés recogidos en los procesos de 1 a 3 en un formato utilizable

- **Selección de los activos críticos:** de todos los activos identificados por los altos directivos y operativos, generales y personal de *(TI)*, los más críticos son elegidos por el equipo de análisis.

- **Definición de los requisitos de seguridad para los activos críticos**: el equipo de análisis refina cualquier información obtenida durante los procesos de 1 a 3 para llegar a un conjunto final de requisitos de seguridad.

- **La determinación de las amenazas a los activos críticos:** las áreas de interés definidas durante los procesos de 1 a 3 se refinan y se expanden los perfiles de amenaza.

FASE 2: IDENTIFICAR LAS VULNERABILIDADES DE LA INFRAESTRUCTURA

Se trata de una evaluación de la infraestructura de información. El equipo de análisis examina los principales componentes operacionales y sus debilidades (vulnerabilidades tecnológicas) que pueden dar lugar a una acción no autorizada contra los activos críticos.

Proceso 5: Identificar los componentes clave.

El proceso 5 identifica los componentes claves de la infraestructura que deben ser examinados en busca de vulnerabilidades tecnológicas para cada activo crítico. El equipo de análisis identifica los principales sistemas de tecnología de información y los componentes de cada activo crítico. Los casos específicos se seleccionan para su evaluación. Este proceso consta de las siguientes actividades:

- **Identificar las clases principales de componentes:** Un sistema de interés se identifica para cada activo crítico. Topología u otros tipos de mapas de la red se

utiliza para revisar los activos críticos “en vivo” y cómo se accede a ellos. Las clases principales de los componentes se seleccionan basándose sobre cómo el activo se accede y usa. Toda la información se registra en el libro de Activos perfil adecuado.

- **La identificación de los componentes de infraestructura para examinar:** Para cada tipo de componente, el equipo de análisis selecciona componentes específicos de esa clase para evaluar. El departamento de *(TI)* debe proporcionar las direcciones de red específicas o ubicaciones físicas necesarias para organizar la evaluación. Todos los resultados se registran en el libro de Activos perfil adecuado.

Proceso 6: Evaluar los componentes seleccionados.

Durante el proceso 6 se evalúan los principales sistemas y componentes para cada activo fijo en busca de vulnerabilidades tecnológicas. El equipo de análisis, junto con los miembros del personal de TI, ejecuta las herramientas de evaluación, analizan los resultados y generan resúmenes para cada activo crítico. La coordinación y la planificación son necesarias para minimizar el impacto en la organización y su personal.

FASE 3. ESTRATEGIA Y PLAN DE DESARROLLO

Es la planificación de las medidas y reducción de los riesgos. Se clasifican en los siguientes elementos:- evaluación de los riesgos- Estrategia de protección- Ponderación de los riesgos- Plano de reducción de los riesgos.

Proceso 7: Análisis de Conducta de riesgo

Durante el Proceso 7, El equipo de análisis identifica el impacto de las amenazas a los activos críticos, crea criterios para evaluar esos riesgos, y evalúa los impactos sobre la base de esos criterios. Esto produce un perfil de riesgo de cada activo crítico. El proceso 7 consta de las siguientes actividades:

- **Identificar el impacto de las amenazas a los activos críticos:** Para cada activo crítico, las declaraciones de impacto real de la organización (por ejemplo, la pérdida de la vida del paciente) se definen para cada resultado de amenaza *(por ejemplo, la modificación de los registros de pacientes).*

- **Crear criterios de evaluación de riesgos:** Usando las declaraciones de impacto a partir de la primera actividad, un conjunto general de criterios de evaluación de impacto se definen por las amenazas a los activos críticos de la organización. Las definiciones de los tres niveles de evaluación cualitativa - alta, media y baja - se definen para múltiples aspectos *(por ejemplo, los impactos financieros u operativos).*

Proceso 8: Desarrollar una estrategia de protección

En el proceso 8 el equipo de análisis crea una estrategia de protección para los planes de ordenamiento y mitigación para los activos críticos, basados en el análisis de la información recogida. Los altos directivos luego revisan, refinan y aprueban la estrategia y los planes.

Trabajo previo:

Compilación de los resultados de la encuesta: - Los resultados de las encuestas realizadas durante los talleres 1 a 3 se compila para buscar esas prácticas que la mayoría creen que se realizan bien, y los que la mayoría consideran que es una vulnerabilidad.

Revisar la información: La información de los procesos anteriores se revisa. Esto incluye las vulnerabilidades, prácticas, información sobre riesgos y requisitos de seguridad para los activos críticos.

Crear una estrategia de protección: La estrategia de protección se estructura en torno al catálogo de las prácticas. Se dirige a aquellas prácticas que el equipo de análisis considera que deben ser implementados o mejorados.

ANEXO E. COMPARACIÓN DE LAS METODOLOGÍA OSSTMM Y OCTAVE

En el siguiente anexo, se realiza un comparativa de las metodologías diseñadas para la gestión de riesgos, de la cuales se elige la más idónea, para la realización de la presente investigación.

Comparativa de Metodologías – Valoración de los elementos de análisis:

	Activo	Valoracion	Amenaza	Vulnerabilidad	Probabilidad que ocurra	Impacto	Riesgo
Magerit	Activo X	Valor del Activo (medido en €)	Amenaza Y	No lo requiere	Frecuencia Z	% del valor del activo que se pierde sí el impacto se produce	Valor de la perdida diaria que resulta de la multiplicacion del valor del activo con la probabilidad de ocurrencia de la amenaza
CRAMM	Activo X	[1-5]	Amenaza Y	Vulnerabilidad W	Frecuencia Z [1-5]	[1-5]	Escala [3 a 15]
NIST SP 800-30	Activo X	Alto-Medio-Bajo	Amenaza Y	Vulnerabilidad W	Frecuencia Z Alto-Medio-Bajo	Alto-Medio-Bajo	Alto, medio y bajo
Octave	Activo X	Busca el riesgo más alto es un árbol de desición	Amenaza Y	Vulnerabilidad W	Frecuencia Z		Busca el riesgo más alto es un árbol de desición

Ilustración 111: Valoración de los elementos de análisis

Fuente: Análisis Comparativo: Metodologías de análisis de Riesgos Abraham Mogollón 2011

Comparativa de Metodologías:

Puntos a Destacar	Magerit	CRAMM	NIST SP 800-30	Octave
País que la creo	España	Reino Unido	Estados Unidos	Estados Unidos
Responsable del Producto	Secretaría de Estado para la Administración Pública	Cramm. El cual pertenece a Siemens	National Institute of Standards and Technology (NIST)	Software Engineering Institute (SEI) y Carnegie Mellon University (CMU)
WebSite	Versión 1: http://www.csi.map.es/csi/pg5m22.htm Versión 2: http://www.csi.map.es/csi/pg5m20.htm	http://www.cramm.com/	http://www.csrc.nist.gov/index.html Publicaciones: http://www.csrc.nist.gov/publications/nistpubs/	http://www.cert.org/octave/
Versiones	Versión 1 (1997) Versión 2 (2006)	Ultima versión: CRAMM NATO V5.3	Publicación 800-30 (2002)	OCTAVESM Method Version 2.0
Herramienta para aplicar la metodología	Herramientas: * PILAR * CHINCHON	Un gran numero de herramientas de analisis y gestión de la información resultante de estas (ejemplo: CRAMM Express)	Según lo investigado, la norma no especifica un producto en concreto para el analisis	Según lo investigado, la norma no especifica un producto en concreto para el analisis, habla genericamente de 'Vulnerability Evaluation Tools'
Principales Conceptos	Activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas	Activos, amenazas, vulnerabilidades, riesgos, salvaguardas (contramedidas)	Amenazas, vulnerabilidades, riesgos, controles	Activos, amenazas, vulnerabilidades, riesgos

Ilustración 112: Valoración de los elementos de análisis

Fuente: Análisis Comparativo: Metodologías de análisis de Riesgos Abraham Mogollón 2011

A continuación se analizan las características más importantes de las metodologías Margerit, CRAMM, NIST SP 800-30 y OCTAVE.

Comparativa de Metodologías:

Puntos a Destacar	Magerit	CRAMM	NIST SP 800-30	Octave
Fases	1- Planificación del Proyecto de Riesgos (como consideraciones iniciales para arrancar el proyecto de Análisis y Gestión de Riesgos) 2- Análisis de riesgos (Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable) 3- Gestión de riesgos (Se identifican las funciones y servicios de salvaguarda reductoras del riesgo) 4- Selección de salvaguardas (plan de implantación de los mecanismos de salvaguarda elegidos)	1- Identificación y valoración de activos (se identifican los activos físicos, software, y los activos de datos que conforman los sistemas de información) 2- Valoración de las amenazas y vulnerabilidades (determinar cuál es la probabilidad de que esos problemas ocurran) 3- Selección y recomendación de contramedidas (CRAMM contiene una gran librería de más de 3000 contramedidas organizadas en 70 grupos)	1- Iniciación (identificar riesgos es usado para soportar el desarrollo de los requerimientos del sistema) 2- Desarrollo o adquisición (El sistema IT es diseñado, expresado y propuesto o construido) 3- Implementación (los activos de seguridad del sistema son configurados, habilitados, testeados y verificados 4- Operación o mantenimiento (las actividades de mantenimiento para la reducción del riesgo son realizadas) 5- Disposición (las actividades de administración de riesgos son realizadas en los componentes del sistema)	1- Construcción de las vulnerabilidades basadas en los activos (visión organizacional) 2- Identificación de las vulnerabilidades de la infraestructura (visión tecnológica) 3- Desarrollo de estrategia de seguridad y planes de mitigación de las vulnerabilidades (estrategia y plan de desarrollo)
Principales Características	* Habla de análisis algorítmico con 3 modelos: cualitativo, cuantitativo y escalonado * En la versión 2 posee 3 documentos: Catalogo, Metodo y Tecnicas	* > 400 tipos de activos * 38 tipos de amenazas * > 25 tipos de impactos * 7 medidas de riesgo * > 3500 controles	* Otorga gran importancia a los controles * Habla de perfiles claves dentro de la organización respecto a la responsabilidad de la administración del riesgo	* Posee 'Self-Direction'. Una pequeño equipo del personal de la misma organización es involucrado en los procesos de implementación de la metodología (personal de IT y de otros departamentos) * Creación de un pequeño equipo interdiciplinario de analisis de la información * Acercamiento basado en workshop donde personas de distintos niveles de la organización trabajan para identificar las vulnerabilidades basandose en los activos * Catalogos de la información: Catalogos de practicas, Perfil de activos, catalogo de vulnerabilidades * Habla de un balance entre 3 aspectos: Tecnología, Riesgo Operacional y Prácticas de seguridad

Ilustración 113: Valoración de los elementos de análisis

Fuente: Análisis Comparativo: Metodologías de análisis de Riesgos Abraham Mogollón 2011

Comparativa de Metodologías:

Puntos a Destacar	Magerit	CRAMM	NIST SP 800-30	Octave
Aplicación	* Analisis de riesgos * Gestión del riesgos * Plan Director de Seguridad	* Analisis de riesgos * Gestión del riesgos * Plan Director de Seguridad	* Analisis de riesgos * Gestión del riesgos * Plan Director de Seguridad	* Analisis de riesgos * Gestión del riesgos * Plan Director de Seguridad
Quien lleva a cabo la metodología	* Pequeño grupo interdiciplinario conformado por empleados de la misma empresa	* Pequeño grupo interdiciplinario conformado por empleados de la misma empresa	* Pequeño grupo interdiciplinario conformado por empleados de la misma empresa	* Pequeño grupo interdiciplinario conformado por empleados de la misma empresa
Costo	* No tiene costo, ya que es una normativa de libre aplicación * Plantea un analisis de costo beneficio, expresa una formula de ROI (Retorno de la inversión)	La versión 4 costaba por el año 2001: * Para una compañía comercial: £2800 + £850 al año de mantenimiento * Para agencias y departamentos del estado britanico: £1600 + £850 al año de mantenimiento	* Habla de costo relacionado con el beneficio, otorgando una condición relativa al costo de un plan director de seguridad, siempre que el costo sea menor al costo del riesgo analizado y solventado, el costo será bajo	* Uso Interno: Gratuito * Uso Externo: Se debe comprar la licencia al SEI si se quiere implementar la metodología a un tercero
Resultado del analisis (outputs)	Resultados ordinales y cardinales	* Tabla de valorazión del riesgo sobre los activos (escala de 1 a 10)	* Lista de controles recomendados * Resultados de la documentación	Fase 1: Activos Critivos, requerimientos criticos para activos criticos, vulnerabilidades de activos criticos, lista de practicas de seguridad actuales, lista de vulnerabilidades actuales de la organización Fase 2: Componentes clave, vulnerabilidades tecnologicas actuales Fase 3: Riesgos de los activos criticos, metricas del riesgo, estrategia de protección, planes de mitigación del riesgo

Ilustración 114: Valoración de los elementos de análisis

Fuente: Análisis Comparativo: Metodologías de análisis de Riesgos Abraham Mogollón 2011

ANEXO F. VALORACIÓN DE LOS ACTIVOS CRÍTICOS DE HW Y SW.

Tabla 51: Matriz de riesgos activos de Hardware

ACTIVOS HARDWARE				
AMENAZAS	**PROBABILIDADES**	**MAGNITUD DE DAÑO (IMPACTO)**		**RIESGO**
Corte de energía	2	Revelación	1	1
		Pérdida -Destrucción	1	2
		Interrupción	2	4
Acceso no autorizado	3	Revelación	1	3
		Pérdida -Destrucción	2	6
		Interrupción	1	3
Robo de equipos	2	Revelación	1	2
		Pérdida-Destrucción	3	6
		Interrupción	3	6
Acciones mal intencionados o por desconocimiento	1	Revelación	1	2
		Pérdida –Destrucción	1	1
		Interrupción	2	2
Incendios	1	Revelación	1	1
		Perdida-Destrucción	3	3
		Interrupción	3	3
Filtraciones de agua	1	Revelación	1	1
		Perdida-Destrucción	2	2
		Interrupción	2	2
Sismos	1	revelación	1	1
		Perdida-Destrucción	2	2
		Interrupción	2	2
Sobrecarga eléctrica	1	Revelación	1	1
		Perdida-Destrucción	1	1
		Interrupción	2	2
Discontinuidad del servicio (fallas de hardware)	1	Revelación	1	1
		Perdida-Destrucción	1	1
		Interrupción	3	3
Instalación y configuración inadecuada	2	revelación	1	2
		Perdida-Destrucción	1	2
		Interrupción	2	4

Fuente: El Autor (2015).

Tabla 52: Matriz de riesgos activos de software

ACTIVOS SOFTWARE				
AMENAZAS	**PROBABILIDADES**	**MAGNITUD DE DAÑO (IMPACTO)**		**RIESGO**
Acceso no autorizado	1	Revelación	2	2
		Pérdida -Destrucción	1	1
		Interrupción	2	2
Copias no autorizadas	1	Revelación	2	2
		Pérdida -Destrucción	1	1
		Interrupción	1	1
Robo de contraseñes	1	Revelación	2	2
		Pérdida-Destrucción	1	1
		Interrupción	2	2
Inasistencia de planes mantenimiento preventivos y correctivos	2	Revelación	1	2
		Pérdida –Destrucción	3	6
		Interrupción	3	6
Degeneración del servicio	2	Revelación	1	2
		Perdida-Destrucción	2	4
		Interrupción	2	4
Destrucción o modificación del sistema operativo o aplicaciones	1	Revelación	1	1
		Perdida-Destrucción	3	3
		Interrupción	3	3
Manipulación inadecuado del sistema operativo aplicaciones	1	Revelación	1	1
		Perdida-Destrucción	3	3
		Interrupción	3	3
Malware	3	Revelación	1	3
		Perdida -Destrucción	2	6
		interrupción	1	3

Fuente: El Autor (2015).

ANEXO G. VALORACIÓN DE ATAQUES A LA VOIP

VECTORES CLÁSICOS EXTERNOS

ENUMERACIÓN DNS (O FOOTPRINTING)

En una auditoria esta técnica se utiliza durante una fase inicial de obtención de información sobre el objetivo. Básicamente consiste en utilizar los servidores DNS del sistema atacado para obtener direcciones IP validas de esa infraestructura. Si el servicio estuviese mal configurado el atacante podría mapear incluso toda la infraestructura auditada. Para el caso de la VoIP los registros DNS involucrados son los de servicios (SRV), que indican la dirección de los servidores SIP, IAX o H.323 para ese dominio. Existen numerosas herramientas de uso genérico capaces de implementarlo, por ejemplo: Metasploit (módulo dnsenum.rb)

- **Probabilidad: Alta;**
- **Impacto: Bajo;**
- **Valoración del riesgo: Medio.**

INDEXADO DE EQUIPOS.

Al igual que existen buscadores de contenidos existen también buscadores de servicios, entre los que se incluyen SIP y la web (paneles de gestión). Estos tienen indexados una gran cantidad de los mismos clasificados según el tipo e incluso la versión (Shodan es el nombre del más conocido). Desde el punto de vista del atacante es una fuente inagotable de recursos. Siempre que el ataque no sea dirigido este dispondrá de un alto número de equipos que, de antemano, va a saber que son vulnerables a un determinado vector.

- **Probabilidad: Alta;**
- **Impacto: Bajo;**
- **Valoración del riesgo: Medio.**

"BANNER-GRABBING" (O FINGERPRINTING).

El escaneo de servicios es el siguiente paso lógico durante una intrusión, una vez conocidos los nodos involucrados, es necesario conocer que software concreto ejecutan. En el caso de SIP es muy similar al del escaneo HTTP, se hace una petición típica y se parase de la respuesta la información que puede ser importante. Sipvicius (herramienta svmap.py) y Metasploit (módulo options.rb) soportan esta característica a día de hoy. Es

importante señalar que normalmente, y en especial para el caso de UDP, es un proceso mucho más rápido que herramientas más genéricas como el Nmap.

- **Probabilidad: Alta;**
- **Impacto: Bajo;**
- **Valoración del riesgo: Medio**

"BRUTE-FORCE" DE EXTENSIONES

El protocolo SIP establece que el servidor ha de responder de forma diferente durante un registro ante las combinaciones usuario correcto/contraseña incorrecta que usuario incorrecto/contraseña incorrecta. Debido a este hecho es bastante sencillo tratar de adivinar extensiones validas utilizando la fuerza bruta. En la configuración de los servidores SIP comunes, como Asterisk, existen parámetros para evitar este comportamiento, pero este mecanismo se puede "bypassear". Para el caso del Kamailio (un softswitch open source), la configuración por defecto evita este problema. Las principales herramientas que lo implementan son también Sipvicius (svwar.py) y Metasploit (enumerator.rb).

- **Probabilidad: Alta;**
- **Impacto: Medio**;
- **Valoración del riesgo: Alto**

"BRUTE-FORCE" DE CONTRASEÑAS

Este caso es similar al anterior, pero ahora, una vez conocida una extensión valida, el atacante tratara de adivinar la contraseña asociada. Una vez más Sipvicius (svcrack.py) y Metasploit lo soportan, para el segundo no lo hace la distribución oficial. Pero en Quobis hemos desarrollado un módulo capaz de llevar a cabo estas tareas (sipcrack.rb).

- **Probabilidad: Alta;**
- **Impacto: Alto;**
- **Valoración del riesgo: Alto.**

FALLAS CONOCIDAS Y "0-DAYS".

Al igual que para el resto de servicios, las actualizaciones de los servidores son fundamentales. De esta forma estaremos protegidos ante exploits que saquen provecho de fallas conocidas y que podrían ocasionar una denegación de servicio o incluso ejecución remota de código. Un caso especial de este vector de ataque son los conocidos como "0-days", que aprovechan vulnerabilidades dispone ninguna actualización para mitigarlas. La verdad es que no existen demasiados exploits en la red en comparación con

otras tecnologías, aunque si algunos. En lo referente a los "fueres" que se utilizan para detectar estas vulnerabilidades nos gustaría destacar VoIP, algo antiguo pero bastante eficiente. Otros como Peach, de propósito más general y mucho más conocidos (también más potentes) pueden ser configurados para la tecnología que nos ocupa.

- **Probabilidad: Baja;**
- **Impacto: Alto;**
- **Valoración del riesgo: Medio**

SPOOFING.

El "spoofing" o suplantación de identidad no supone un riesgo en sí mismo, normalmente se utiliza en conjunción con alguna de las otras técnicas. Para el caso de la VoIP es algo a tener muy en cuenta debido al uso generalizado, como comentamos, del protocolo UDP, vulnerable al mismo. En teoría este vector lo deberían de controlar los operadores, pero normalmente no es así y mucho menos en el caso de países como China.

- **Probabilidad: Baja;**
- **Impacto: Bajo;**
- **Valoración del riesgo: Bajo.**

(D)DOS POR INUNDACIÓN

Desde nuestro punto de vista la denegación de servicio (distribuida) es uno de los vectores más a tener en cuenta por varios motivos:

- La VoIP es una tecnología muy sensible a variaciones en el ancho de banda, porque pueden producir micro cortes en las conversaciones actuales e impedir nuevas llamadas y registros.

- Solo es cuestión de tiempo que los servidores de VoIP pasen a ser el objetivo de grupos hacktivistas, organizaciones y gobiernos, como lo es ahora la web.

- Normalmente los agresores no tienen demasiado claro el proceso de auditoría de una infraestructura IP. Por lo que en la mayoría de las ocasiones los intentos de intrusión van a desencadenar incidentes de este tipo.

- Aunque en un principio se pudiera pensar lo contrario el uso del spoofing cada día es más común. De hecho los últimos meses varias organizaciones han sufrido incidentes importantes debido al poder de amplificación de este vector.

- **Probabilidad: Media;**
- **Impacto: Alto;**
- **Valoración del riesgo: Alto**

MALWARE.

Para el agresor lo importante es conseguir un beneficio económico, y la vía más fácil casi siempre es infectar el equipo de la víctima con un troyano para acceder a la información que le sea necesaria, en este caso a los credenciales SIP. Para esto suelen servirse de Ingeniería social y algún exploits pack comprado en el mercado negro. Normalmente incluyen diversos "0-days" y vulnerabilidades recientes del navegador, Java, Adobe Reader, etc. De esta forma la probabilidad de infección de un usuario medio es altísima.

- **Probabilidad: Media;**
- **Impacto: Alto;**
- **Valoración del riesgo: Alta.**

ATAQUE CON PAQUETES INVITE

No son tan comunes, pero si se ven alguna vez. En este caso el atacante trata de llamar (paquete INVITE) sin estar registrado previamente, el objetivo final es el mismo que para el caso anterior, realizar una llamada a un número de teléfono para obtener algún beneficio. Realmente no funcionan con la configuración por defecto de la mayoría de los sistemas SIP típicos ya que, aunque se permiten INVITES (llamadas) a usuarios no registrados, previamente se les solicita una autenticación por medio de un reto.

- **Probabilidad: media;**
- **Impacto: baja**;
- **Valoración del riesgo: baja**

VECTORES CLÁSICOS INTERNOS

ESCUCHAS ILEGALES (EAVESDROPPING).

Consiste en llevar las tradicionales escuchas telefónicas al mundo de la VoIP. Mediante la intercepción de paquetes de señalización y "stream" de voz y/o video el atacante puede escuchar una conversación sin ser partícipe de la misma. Para evitarlo se debe separar física o lógicamente los segmentos de red dedicados a voz de los dedicados a datos. Además se recomienda cifrar las comunicaciones, tanto a nivel de señalización (por ejemplo usando SIP sobre TCP/SSL, como el tráfico de media. ZRTP es la opción a escoger si se desea disponer de cifrado extremo a extremo, porque SRTP confía en un tercero (el servidor) durante la negociación de las claves.

- **Probabilidad: Media;**
- **Impacto: Alto;**
- **Valoración del riesgo: Alto**

CRACKING DE CONTRASEÑAS.

Cuando el atacante captura tráfico de señalización SIP (sin TLS) en la red, de estos paquetes puede obtener los hash MD5 de las contraseñas. Mediante el uso de una de las múltiples herramientas que existen para tal fin estas podrían ser crackeadas. Por medio de herramientas como oclHascat el proceso se acelera de forma considerable por utilizar la potencia de la tarjeta gráfica. Entre las más conocidas se puede destacar Caín, que permite tanto la captura del tráfico como el cracking del hash MD5. Una opción interesante son sitios como md5Crack. Se sube el hash a la misma y, en caso de tener la cadena original correspondiente a ese valor almacenada, la devuelve. Para evitar este tipo de ataques, además del cifrado, se recomienda el uso de Contraseñas robustas.

- **Probabilidad: Media;**
- **Impacto: Alto;**
- **Valoración del riesgo: Alto**

MANIPULACIÓN/INTERRUPCIÓN

Usando un atacante está situado entre las dos partes de una comunicación y es capaz de interceptar y modificar tráfico hay una serie de técnicas que puede utilizar. Además de la escucha de las comunicaciones, que se comentó anteriormente, el atacante podría comento anteriormente, el atacante podría alterar la conversación (omitiendo, repitiendo o insertando media), finalizar la llamada (DoS) o enviarla a un destino incorrecto. Para evitar este tipo de ataques, además de fortificar las comunicaciones a nivel de red, se recomienda implementar un sistema de identificación y autentificación suficientemente robusto para garantizar que los dos extremos de la llamada son quien dice ser. Algunas herramientas que soportan este vector son RTPInsertSound y RTPMixSound, publicadas con el libro Hacking VoIP Exposed.

- **Probabilidad: Baja;**
- **Impacto: Medio;**
- **Valoración del riesgo: Medio.**

SERVIDORES TFTP

Comúnmente se incluyen servidores TFTP en la infraestructura (sobre todo en las de gran tamaño) para permitir la auto-provisión de los teléfonos VoIP. Además esta comunicación muchas veces no se cifra porque no todos los modelos lo soportan. Existen herramientas específicas, pero cualquier sniffer es capaz de obtener las credenciales SIP de la traza sin problemas.

- **Probabilidad: Media;**
- **Impacto: Alto;**
- **Valoración del riesgo: Alto.**

SALTO ENTRE VLAN

Aunque una de las medidas recomendadas es la separación física o lógica (mediante VLANs) del tráfico de voz y datos, si no se realiza correctamente esta configuración puede no garantizarnos la seguridad que buscamos. Mediante el uso de herramientas como VoIPHopper, pensada en un principio para la auditoria de este tipo de redes, un atacante puede "saltar" de un segmento de red a otro. A continuación podría aplicar cualquiera de las técnicas anteriores. Para evitar esto se debe seguir las recomendaciones de seguridad de cada fabricante de los dispositivos de switching y networking utilizados.

- **Probabilidad: Baja;**
- **Impacto: Alto**
- **Valoración del riesgo: Media.**

NUEVOS VECTORES

SPIT

Funciona como el SPAM (SPAM over Internet Telephony) pero afectando, en este caso, a la VoIP. Consiste en la generación automática de llamadas de forma masiva. Hasta ahora no se había convertido en un problema muy extendido debido al elevado coste de la infraestructura necesaria, personal y coste de las llamadas. Pero con el incremento de los despliegues VoIP y la reducción de los costes de las llamadas (o el uso de PBX comprometidas) el número de ataques SPIT se ha incrementado de forma notable. Entre las contramedidas a este tipo de ataque se puede destacar: sistemas de autenticación de identidad, sistemas de filtrado (listas negras y listas blancas, sistemas de CAPTCHA's de voz, filtro de contenidos de audio, etc.). Otra vez en el libro Haking VoIP Exposed incluye Spitter, una herramienta que implementa esto, aunque cualquier centralita software podría hacerlo mediante el uso de scripts.

- **Probabilidad: Media;**
- **Impacto: Bajo;**
- **Valoración del riesgo: Bajo.**

VISHING

Técnica análoga al Phishing que mediante la combinación de ingeniería social y tecnologías de VoIP, permite al criminal engañar a personas para obtener datos delicados

como pueden ser datos de tarjetas de crédito o cuentas bancarias, o datos personales que permitan la suplantación de identidad. El atacante además, mediante técnicas de "Caller-Id spoofing", puede suplantar la identidad (número de teléfono) de una entidad bancaria o una compañía legitima, para no levantar sospechas por parte de la persona atacada. Las soluciones son las mismas que para el caso anterior.

- **Probabilidad: Media;**
- **Impacto: Alta;**
- **Valoración del riesgo: Alto.**

BOTNET SIP.

En la Defecan del año 2011 Iftach Ian Amit e Itzik Kotler implementaron una prueba de distribuir malware. Es decir, diseñaron una Botnet en la que los nodos/repositorios eran capaces de comunicarse entre sí enviando comandos en forma de tonos DTMF. La ventaja de este tipo de malware es su invisibilidad ante mecanismos de inspección de paquetes, por tratarse de tráfico VoIP, que además podría estar cifrado. Finalmente proponían un mecanismo similar para soportar una red VPN con las mismas ventajas.

- **Probabilidad: Baja;**
- **Impacto: Alta;**
- **Valoración del riesgo: Media.**

OCCUPYPHONES

Variante de ataque DoS que consiste en saturar el teléfono público del objetivo mediante la realización de un gran número de llamadas en un corto periodo de tiempo. Para este fin se hace uso de tecnologías VoIP, por una parte para abaratar costes y por otra parte, para facilitar su automatización. Incluso existen empresas que proporcionan el "servicio" de inundar por encargo ciertos objetivos.

- **Probabilidad: Baja;**
- **Impacto: Medio;**
- **Valoración del riesgo: Medio.**

ANEXO H. COMPARACIÓN DE IPSEC Y SSL/TLS

Tabla 53: Algoritmos de cifrado en SSL/TLS e IPSec

ALGORITMOS DE CIFRADO				
Protocolo	**Algoritmo**	**Tipo**	**Tamaño de la llave**	**Tamaño de bloque**
SSL/TLS/IPsec	DES-CBC	Bloque	56bits	8 bytes
SSL/TLS/IPsec	3 DES	Bloque	168bits	8 bytes
IPsec	Blowfish-CBC	Bloque	128bits	8 bytes
IPsec	AES-CBC128,192 y 256	Bloque	128bits;192bits;	16bytes
SSL/TLS	DES40-CBC	Bloque	40 bits	8 bytes
SSL/TLS	FORTEZZA-CBC	Bloque	96bits	20 bytes
SSL/TLS	IDEA-CBC	Bloque	128 bits	8 bytes
SSL/TLS	RC2-CBC-40	Bloque	40 bits	8 bytes
SSL/TLS	RC4-128	stream	128 bits	-
SSL/TLS	RC4-40	stream	40 bits	-
SSL/TLS/IPsec	NULL	stream	0 bits	-

Fuente: El Autor (2015).

Tabla 54: Algoritmos HASH en SSL/TLS E IPSec

Algoritmos HASH		
Protocolo	**algoritmo**	**Tamaño resultado**
SSL/TLS IPSec	MD5	128 bits
SSL/TLS IPSec	SHA-1SHA-256 YSHA-384	160bits,256bits,384bits
SSL/TLS IPSec	NULL	0bytes

Fuente: El Autor (2015).

Tabla 55: Intercambio de claves entre SSL/TLS e IPSec

Mecanismo de Autenticación e intercambio	Protocolo
PSK Pre share key	SSL\TLS
HMAC	SSL\TLS
Certificados Digitales	SSL\TLS
IKE	IPSec
KERBEROS	IPSec
Diffie Hellman	SS\TLS/IPSec

Fuente: El Autor (2015).

- **VELOCIDAD DE TRANSFERENCIA DE 100 MB – SSL/TLS VPN**

Algoritmo	Tiempo(Seg)	Tiempo (Seg) LZO
DES SHA1	40	40
3DES SHA1	46	41
AES 128 SHA1	36	35
AES 256 SHA1	34	35

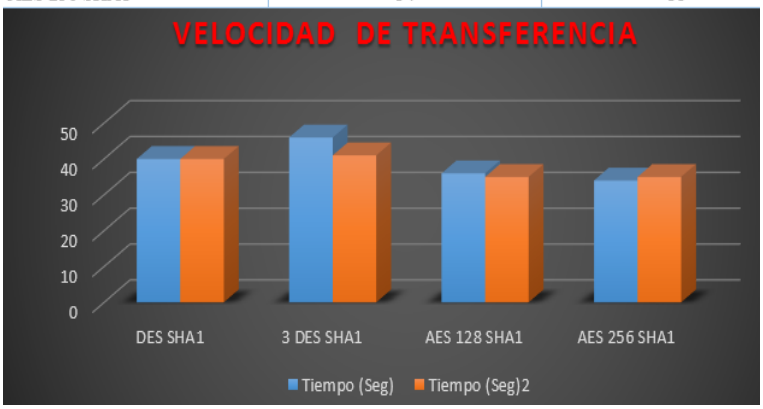


Ilustración 115: Velocidad de Transferencia del protocolo TLS.
Fuente: El Autor (2015).

- **VELOCIDAD DE TRANSFERENCIA DE 100 MB – IPSEC - VPN**

MODOS	ALGORITMO DE CIFRADO			
	Integridad	3DES	AES 128	AES 256
IKE ESP	MD5	48 Seg	57 Seg	56 Seg
IKE ESP	MD5 SHA1	69 Seg	38 Seg	39 Seg
Agresivo	MD5	54seg	49 Seg	46 Seg

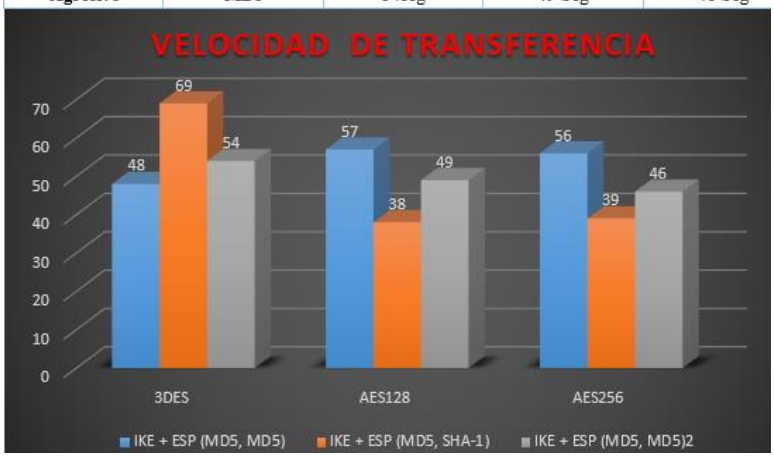


Ilustración 116: Velocidad de transferencia del protocolo IPSec.
Fuente: El Autor (2015).

ANEXO I. CONFIGURACIÓN DE SOFTPHONE PARA EL CIFRADO TLS

Para el caso de los PhonerLite se debe realizar lo siguiente

- Hacer clic en la configuración de la ficha.
- Haga clic en la Red de la ficha y, a continuación, especifique los siguientes ajustes:

    - Puerto local: 5061
    - Tipo de Conexión preferida: *(TLS)*

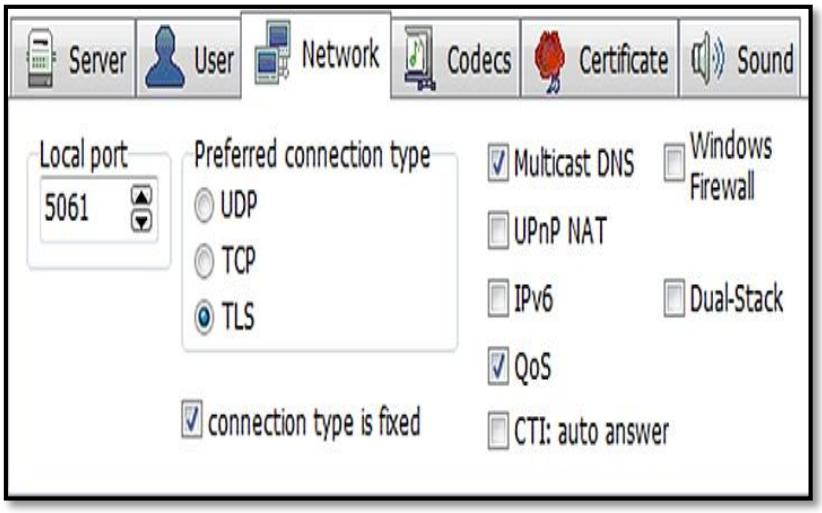


Ilustración 117: Configuración de la red en PhonerLite
Fuente: Barracuda Networks Technical Support. (2011)

- Se carga el certificado `ca.crt`
- **Cargar Windows CA** - Seleccione esta casilla de verificación.

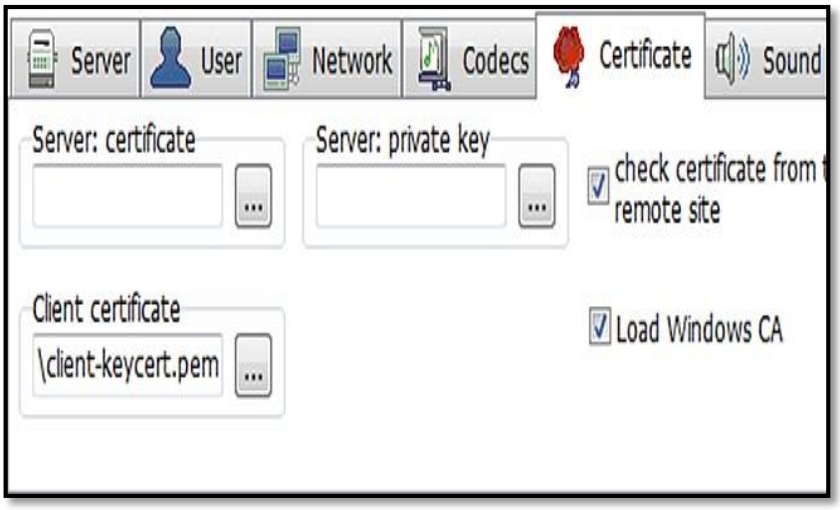


Ilustración 118: Cargar certificado ca.crt en PhonerLite
Fuente: Barracuda Networks Technical Support. (2011)

ARTÍCULO CIENTÍFICO

CERTIFICACIÓN

Loja, 14 de Noviembre de 2015

Lic.
Sergio Fernando Ramón Villa
DOCENTE DE IDIOMA INGLÉS
COLEGIO: Hernando de Benavente (Palanda).

Certifica:

Que el egresado **Cristian Leonardo Calderón Ordoñez,** de la Universidad Nacional de Loja, carrera de Ingeniería en Sistemas y autor del trabajo titulado: **"IMPLEMENTACIÓN DE PROTOCOLOS DE SEGURIDAD PARA LA RED VOIP DEL HOSPITAL ISIDRO AYORA DE LOJA"** que cumple con los requisitos y normas y reglas gramaticales del idioma inglés, las cuales ha sido revisadas minuciosamente para dar cumplimiento con la sección de summary de dicho trabajo.

Es todo cuanto puedo decir en honor a la verdad, consecuentemente el interesado puede hacer uso para los fines pertinentes.

ATENTAMENTE

Sergio Fernando Ramón Villa
LICENCIADO EN CIENCIAS DE LA EDUCACIÓN
ESPECIALIDAD INGLES
N° Reg. 1008-13-1195971