UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

SEMINARIO DE GRADUACIÓN
"SEGURIDAD INFORMÁTICA"

Tema:

"VPN (RED PRIVADA VIRTUAL) USANDO SOFTWARE LIBRE PARA DISMINUIR LOS ATAQUES EAVESDROPPING EN LA RED DE COMUNICACIÓN VOIP EN LA FACULTAD DE INGENIERIA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO"

Proyecto de Trabajo de Graduación. Modalidad: SEMINARIO DE GRADUACIÓN, Presentado previo a la obtención del título de Ingeniera en Sistemas Computacionales e Informáticos.

AUTOR: Casicana Apupalo Sandra Verónica

TUTOR: Ing. Luis Solís

Ambato – Ecuador
Mayo - 2013

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema: **"VPN (RED PRIVADA VIRTUAL) USANDO SOFTWARE LIBRE PARA DISMINUIR LOS ATAQUES EAVESDROPPING EN LA RED DE COMUNICACIÓN VOIP EN LA FACULTAD DE INGENIERIA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO"** , de la señorita Sandra Verónica Casicana Apupalo, estudiante de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales, de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Mayo de 2013

EL TUTOR,

Ing. Luis Solís

AUTORÍA

El presente trabajo de investigación titulada **"VPN (RED PRIVADA VIRTUAL) USANDO SOFTWARE LIBRE PARA DISMINUIR LOS ATAQUES EAVESDROPPING EN LA RED DE COMUNICACIÓN VOIP EN LA FACULTAD DE INGENIERIA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO".** Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Mayo, 2013.

Sandra Verónica Casicana Apupalo

CC: 180428768-6

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Hernando Buenaño e Ing. David Guevara revisaron y aprobaron el Informe Final del trabajo de graduación titulado **"VPN (RED PRIVADA VIRTUAL) USANDO SOFTWARE LIBRE PARA DISMINUIR LOS ATAQUES EAVESDROPPING EN LA RED DE COMUNICACIÓN VOIP EN LA FACULTAD DE INGENIERIA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO",** presentado por la señorita Sandra Verónica Casicana Apupalo de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

PRESIDENTE DEL TRIBUNAL

Ing.Msc. Edison Álvarez

---	---
DOCENTE CALIFICADOR	DOCENTE CALIFICADOR
Ing. Msc. David Guevara	Ing. Hernando Buenaño

DEDICATORIA

Sabiendo que jamás encontraré la forma de agradecer su constante apoyo y confianza, sólo espero que comprendan que mis ideales, esfuerzos y logros han sido y serán también suyos e inspirados en ustedes.

Al culminar este paso más en mi vida académica dedico este esfuerzo a mis padres (Josefina y Carlos), hermanos (Diego, Darío) y a toda mi familia quienes con su apoyo incondicional siempre están conmigo.

VERÓNICA CASICANA

AGRADECIMIENTOS

Al dar por terminada esta etapa académica, me permito extender mi gratitud a la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la UTA.

A cada uno de mis compañeros, amigos y docentes por las experiencias compartidas ya que estos recuerdos formaran parte fundamental en la búsqueda del mejoramiento profesional.

Agradezco a las personas más importantes en mi vida mis padres y hermanos a quienes admiro y adoro con todo mi corazón.

VERÓNICA CASICANA

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

RESUMEN EJECUTIVO

La presente investigación consta de 7 Capítulos en los cuales se describe todo el desarrollo de la tesis.

Este trabajo pretende ser un gran aporte para la facultad ayudando a disminuir uno de tantos delitos informáticos como son los ataques Eavesdropping en la red VoIP.

Existen varios métodos que evitan de alguna forma los ataques informáticos, para el presente trabajo se desarrolla procedimientos necesarios para la implementación de una Red Privada Virtual en el sistema de comunicaciones VoIP de la facultad.

CAPITULO I: El Problema.- Se especifica el problema.

CAPITULO II: Marco Teórico.- Se delimita los antecedentes investigativos, fundamentación legal y la categorización de variables.

CAPITULO III: Marco Metodológico.- Se describe el enfoque, tipo de investigación, y Operacionalización de variables.

CAPITULO IV: Análisis e interpretación de resultados.- Se realiza las encuestas al personal requerido y la comprobación de la hipótesis.

CAPITULO V: Conclusiones y Recomendaciones.

CAPITULO VI: Propuesta.

CAPITULO VII: Conclusiones y Recomendaciones de la Propuesta.

Finalmente se encuentra los anexos que contiene el modelo de la encuesta aplicada.

INTRODUCCIÓN

Previo al desarrollo del presente trabajo se explicará los principales términos a tratar en el transcurso de todo el trabajo como son: VoIP (voz sobre un protocolo de internet), VULNERABILIDADES Y MEDIDAS DE PROTECCIÓN en el Sistema de VoIP, ATAQUES EAVESDROPPING, VPN que es la técnica de seguridad que se aplica con el objetivo de evitar los ataques especificados.

Para demostrar la importancia y validez que tiene una VPN en la Red VoIP se trabajará sobre un escenario detallado a continuación:

Dos máquinas se comunicarán entre sí mediante softphone a las cuales se denominará víctimas y una tercera maquina será denominada atacante en la cual se intentará escuchar llamadas de forma secreta.

En el presente proyecto se analizará un ataque en específico denominado Eavesdropping. Para realizar la captura del tráfico se usará la herramienta Wireshark la cual ya trae funcionalidad y filtros para redes VoIP.

Wireshark será instalada en la maquina denominada atacante con el fin de escanear la red y poder demostrar que el ataque Eavesdroping podría existir en la red VoIP.

Finalmente se creará un tutorial con los procedimientos para la implementación de la Red Privada Virtual (VPN) como medida de seguridad para prevenir los ataques mencionados.

CAPITULO I

1. EL PROBLEMA

1.1 Tema

VPN (Red Privada Virtual) usando software libre para disminuir los ataques Eavesdropping en la red de comunicación VoIP en la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato.

1.2 Planteamiento del Problema

1.2.1 Contextualización

A nivel de Latinoamérica el uso de las comunicaciones a través de VoIP avanza a pasos agigantados y no podemos dejar desapercibida la inseguridad informática a la que ésta es inherente.

Cristhian Cabrera, "Realizó un estudio sobre las vulnerabilidades que sería capaz de encontrar en un entorno como Elastix en México. Escaneando todas las posibles redes del país y buscó cuantos equipos utilizan ésta distribución y los resultados que encontró fueron preocupantes. Los resultados encontrados fueron.

25.4 millones de hosts escaneados 69 mil tienen el puerto 443 abierto 467 equipos eran Elastix.

287 tienen algún tipo de dato secreto que se puede obtener fácilmente como la contraseña de FreePBX, contraseña de Elastix o contraseñas de extensiones.

Los mismos 287 tienen el puerto SIP (Protocolo de Inicio de Sesiones) abierto.

261 tenían algún tipo de contraseña default para FreePBX.

26 aún tenían la contraseña de palosanto para Elastix.

31 usan la misma contraseña en FreePBX que en Elastix.

42 aún usan FreePBX 2.5.x que muestra la contraseña de administrador en texto plano." (Cabrera, 2011)

Desde posibles extensiones se pueden sacar llamadas sin pagar un solo centavo, ocasionando tráfico VoIP que en pocas horas se convierte en facturas millonarias de teléfono.

A nivel de Ecuador el riesgo no deja de ser menor, las empresas ya se han manifestado por los altos porcentajes en pérdidas económicas e información confidencial.

Paul Estrella, Ante la supuesta vulnerabilidad en FreePBX reportada en su sitio web manifiesta lo siguiente.

"Hasta el momento no hemos podido confirmar esta supuesta vulnerabilidad, eso no quiere decir que no existe, por lo que seguimos investigando. Por lo pronto lo único razonable es actualizar CentOS vía yum update. El uso de los parches propuestos por FreePBX no está recomendado porque podría agravar la situación y además elimina los repos de Elastix." (Estrella, 2011)

Los riesgos no son menores en Instituciones Educativas ya que la información que se distribuye a través de un medio de comunicación VoIP es de mucha relevancia para la institución.

En la Facultad de Ingeniería en Sistema Electrónica e Industrial los riesgos podría expandirse por la filtración de información además el prestigio institucional puede estar en riesgo al ser tomada información confidencial con fines delictivos.

1.2.2 Análisis Crítico

Figura 1. Árbol de Problemas

Elaborado por: Investigador

Una configuración sin las medidas preventivas y adecuadas para los ataques informáticos en el Sistema de comunicaciones VoIP, en la mayoría de los casos a más de inestabilizar el sistema afecta directamente a los administradores del sistema, al existir la negación de privilegios y al no permitir un rendimiento óptimo del sistema.

Lamentablemente la tecnología VoIP como todas las tecnologías vienen incluido problemas en cuanto a seguridades y es necesario aplicar varias tecnologías y procedimientos como medidas de protección. Cada uno de los elementos que forman parte del funcionamiento de esta tecnología como ruteadores, teléfonos, nuevos protocolos y sistemas operativos en medida que estos se usen el peligro aumenta y llegan a ser blanco de nuevos ataques y vulnerabilidades.

Los delitos informáticos surgen a partir que los computadores aparecen y por naturaleza el ser humano aprovechar todos sus recursos. Lamentablemente aquellos que carecen de ética usan la tecnología VoIP para acceder a información confidencial con fines delictivos.

1.2.3 Prognosis

De continuar con la fuga de información y la toma pasiva de los datos con fines delictivos es necesaria la implementación de una Red Privada Virtual usando software libre para disminuir ataques a los cuales se los conoce como EAVESDROPPING en la red de comunicación VoIP en la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato.

Esto evitará que la Facultad sea propensa a la intercepción de información confidencial que podría ser usada con fines delictivos.

1.2.4 Formulación del Problema

¿La implementación de una Red Privada Virtual usando software libre servirá para disminuir los ataques EAVESDRIPPING en la red de comunicación VoIP en la Facultad de Ingeniería en Sistemas Electrónica e Industrial?

1.2.5 Preguntas directrices

- ¿Entre los tipos de VPN cuál se debería aplicar al sistema VoIP?

- ¿Qué técnicas de ataque usa el EAVESDROPPING en el sistema VoIP?

- ¿Qué procedimientos de seguridad se debería aplicar para evitar los ataques Eavesdropping en el Sistema VoIP de la FISEI?

1.2.6 Delimitación del Problema

Campo: Científico basado en la Tecnología Informática

Área: Seguridad Informática.

Aspecto: Seguridades en la Telefónica VoIP

Tiempo: Durante 12 meses a partir de la aprobación del proyecto

Espacio: Facultad de Ingeniería en Sistemas Electrónica e Industrial de Ambato.

La recolección de la información del presente proyecto está siendo tomada entre el año 2008 al 2011.

1.3 Justificación

La razón por la cual se realizará el estudio y análisis a las intercepciones de información conocida como EAVESDROPPING es debido al acceso de delincuentes informáticos al sistema de comunicación VoIP de la Facultad. Por tal razón es importante conocer sus debilidades para poder evitar estos ataques.

Con este estudio se pretende evitar daños en datos que viajen mediante VoIP y que no accedan a la información personas desautorizadas.

El impacto será alto, porque al implementar una Red Privada Virtual usando software libre disminuirá los ataques a los cuales se los conoce como EAVESDROPPING en la red de comunicación VoIP en la FISEI y responde a la necesidad de solucionar y prever problemas futuros.

Los beneficiarios de este tema de investigación serán los usuarios del sistema así como sus administrativos pues la información de voz y datos será más segura al momento de intercambiar información mediante el sistema de comunicaciones VoIP.

El proyecto es factible porque la Facultad de Ingeniería en Sistemas Electrónica e Industrial cuenta con los recursos humanos y tecnológicos que se requiere para el presente proyecto

1.4 Objetivos

General

Implementar una VPN (Red Privada Virtual) usando Software Libre para evitar los ataques EAVESDROPPING que podrían existir en el sistema de comunicación VoIP con la finalidad de evitar la fuga de información en la FISEI.

Específicos

- Investigar qué tipo de VPN se debe aplicar en el sistema VoIP de la FISEI.
- Determinar los tipos de técnicas usadas para el ataque EAVESDROPPING.
- Plantear una propuesta para evitar los ataques Eavesdropping usando Software Libre con las seguridades que requiere la información de la FISEI.

CAPITULO II

2. MARCO TEÓRICO

2.1 Antecedentes Investigativos

Una vez consultado en el repositorio de la Universidad Técnica de Ambato se ha encontrado investigaciones que tienen cierta similitud con el tema de investigación planteado.

El proyecto citado a continuación pretende implementar una solución integral de telefonía que satisfaga las necesidades de comunicación de los usuarios y de instituciones educativas, que sea económicamente rentable y que permita a sus usuarios estar conectados dentro y fuera de localidades a través de la red mundial de datos Internet.

Fernando Alberto Álvarez Marín

"Diseño de una red telefónica IP interna entre los colegios San José – La Salle de Guayaquil y Hno. Miguel – La Salle de Quito e implementación de un prototipo, usando como central telefónica servidores con Sistema Operativo libre y Software libre.

El uso de la tecnología Voz sobre IP permitirá abaratar los costos de comunicación entre dos instituciones educativas y a su vez estar a la vanguardia tecnológica con un sistema de alta calidad. ” (Marin, FA Alvarez, 2006)

La cita a continuación planteada realiza el análisis de algunas de las amenazas que afectan a las redes de VoIP, aprovechando cualquier debilidad de la red. Los autores pretenden mostrar la importancia de la seguridad en un sistema VoIP.

Jessica Vanessa Gaibor Ortega, Pablo Raúl Caicedo Arellano

“Análisis y Estudio de herramientas para prevenir y solucionar amenazas de Seguridad en Sistemas de Voz Sobre IP

El estudio se basa en trabajar sobre dos máquinas de la PBX que se comunican entre sí, y una tercera maquina intrusa que ha logrado ingresar a la red y capturar 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 de una transmisión de manera no autorizada” (Gaibor)

Conclusión:

Cuando normalmente instalamos y configuramos un nuevo sistema no siempre se toma en cuenta las medidas básicas de seguridad informática en este caso en Elastix. Como cambiar las claves que por defecto están pre establecidas por el sistema, aparentemente es una falta inocente y no siempre la tomamos en cuenta convirtiéndose a largo plazo en un gran peligro, la institución que use el sistema se aflorará en cuantiosas sumas de dinero sin justificación. Si se toma en cuenta esos detalles el sistema no será tan vulnerable para intrusos informáticos.

2.2 Fundamentación Legal

CONSTITUCION DE LA REPUBLICA DEL ECUADOR

Sección primera

Educación

Art. 347.- Será responsabilidad del Estado:

8.- Incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales.

Sección octava

Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

2.3 Fundamentación Teórica

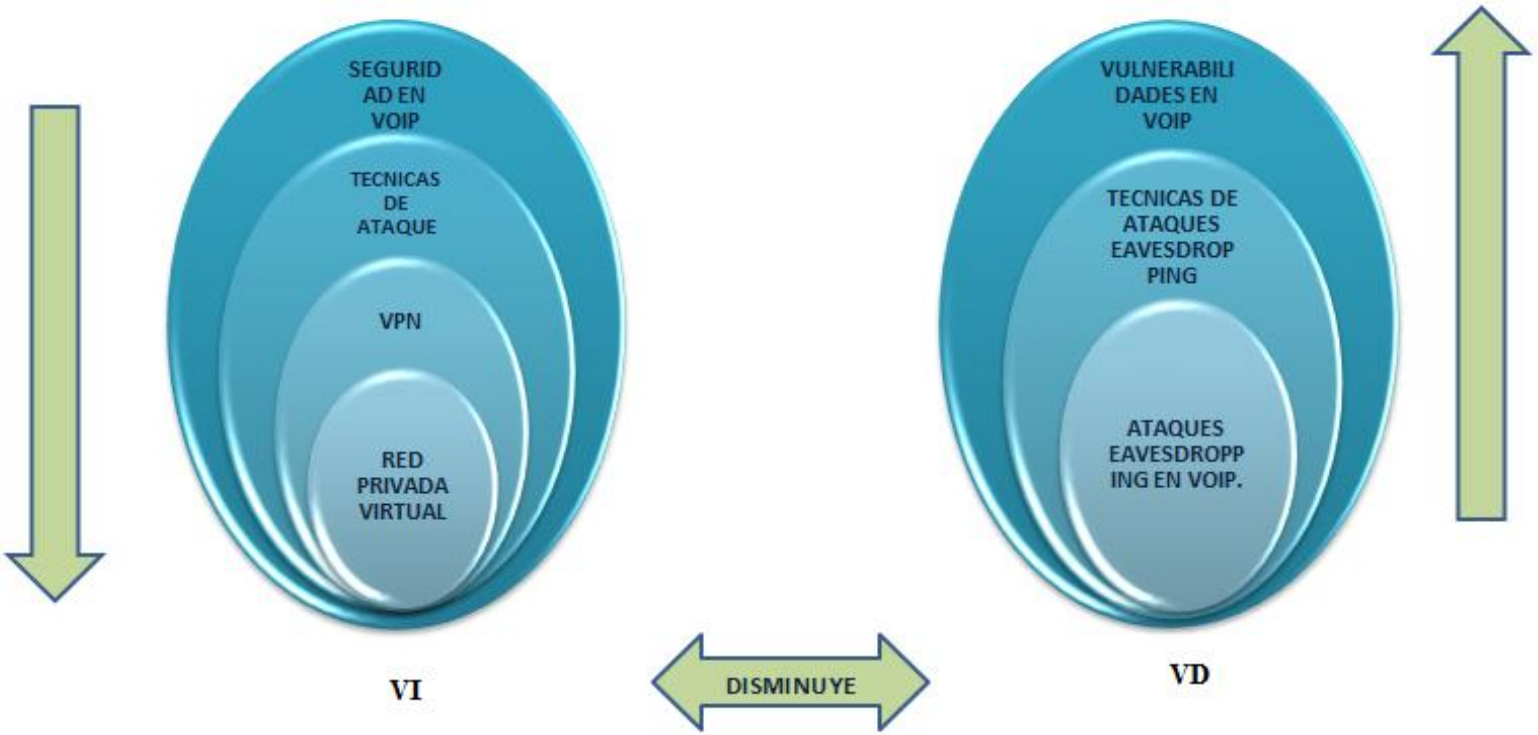


Figura 2 Categorización de Variables

Elaborado por: Investigador

2.3.1 Categorización Fundamental de la VI

2.3.1.1 Seguridad en VoIP

VoIP está expuesta a todas las violaciones de seguridad que son naturales para el uso del Internet, aunque el uso de VoIP es tan seguro como el envío de mensajes de correo electrónico o el pago de facturas en línea, o incluso más seguro.

La seguridad es fundamental en cualquier entorno pero se vuelve imprescindible cuando lo que está en juego es pasar el servicio de telefonía de la red de comunicaciones con mayores niveles de disponibilidad y mayor despliegue del mundo, como es la RTC (Red Telefónica Conmutada), a las nuevas redes convergentes de voz y datos.

Varios argumentos de que la voz es sólo una aplicación más de las que corren sobre una red IP, pese a tener la buena intención de quitar miedos a los usuarios, no es del todo cierto. Es preferible asumir desde un primer momento que la VoIP plantea aspectos muy específicos que le distingue de las aplicaciones de datos convencionales, como la necesidad de disponer de mayores niveles de rendimiento y disponibilidad. Y como todos los relacionados con la seguridad. (MEGAZINE, 2012)

2.3.1.2 Técnicas de Ataque

A continuación se enumera los tipos de ataques que pueden llevarse a cabo sobre comunicaciones VoIP:

- Denegación de Servicio (Denial of Service (DoS) Attacks)
- Manipulación de Mensajes de Señalización SIP (Registration Manipulation and Hijacking)
- Compromiso de la Autenticación de los terminales / usuarios (Authentication Attacks)
- Manipulación del Identificador de Llamada (Caller ID Spoofing)
- Man-in-the-middle Attacks
- Saltos de redes (VLAN Hopping)

- Escuchas de las conversaciones (Passive and Active Eavesdropping)
- Spamming over Internet Telephony (SPIT)
- VoIP phishing (Vishing)

De todos los ataques es más sencillo de llevar a cabo es la interceptación de la conversación, esto puede realizarse con la utilización de un simple analizador de protocolos, y posterior reesamblado de las conexiones TCP/UDP. Esto se debe principalmente, a que la comunicación de voz que se realiza con VoIP no se encuentra cifrada. (GONZALEZ, 2011)

2.3.1.3 VPN

"VPN o Red Privada Virtual es una red de información privada que hace uso de una infraestructura pública de telecomunicaciones, que conecta diferentes segmentos de red o usuarios a una red principal, manteniendo la privacidad a través del uso de un protocolo de túnel o aislamiento así como de otras tecnologías que proveen seguridad."

"Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos, a distintos puntos remotos mediante el uso de una infraestructura pública de transporte.

Los paquetes de datos de la red privada viajan por medio de un túnel definido en la red pública" (Molina)

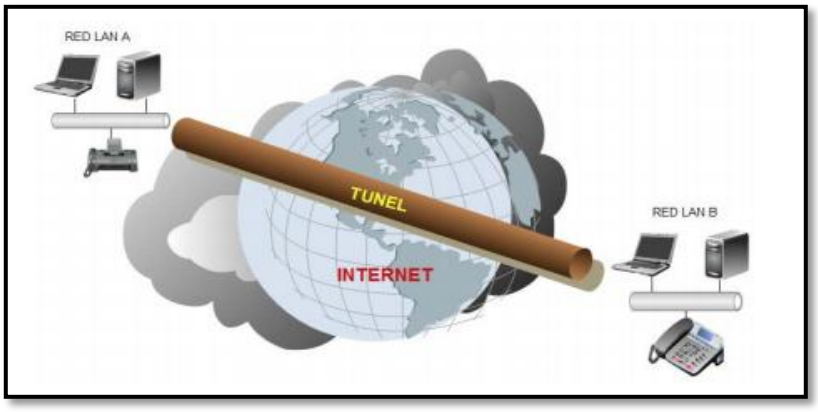


Figura 3 Estructura VPN

Fuente: http://repo.uta.edu.ec/bitstream/handle/123456789/79/t601e.pdf?sequence=1

a. Funcionamiento de una VPN

"Los datos viajan a través de una VPN, desde el servidor dedicado parten los datos, llegando al firewall que hace la función de una pared para engañar a los intrusos de la red, después los datos llegan a la nube de Internet donde se genera un túnel dedicado únicamente para que nuestros datos con una velocidad garantizada, con un ancho de banda también garantizado lleguen al firewall remoto y terminen en el servidor remoto.

Las VPNs pueden enlazar las oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante protocolos como Internet, IP, IPSec, Frame Relay, ATM (Modo de transferencia asíncrona)." (CRYPTEX, 2008)

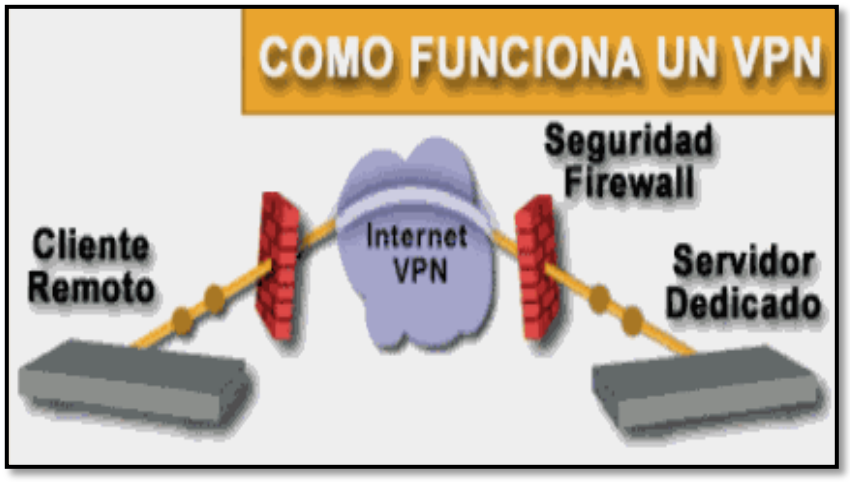


Figura 4 Funcionamiento VPN

Fuente: http://www.slidefinder.net/m/molina/molina/30142339

Tecnología de Túnel

"Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de transito se envían los datos sin problemas." (Farrasaranjueztk, 2011)

Herramientas de un VPN

VPN Gateway

Software

Firewall

Router

2.3.1.4 Aspectos positivos de una VPN

- "La principal motivación del uso y difusión de esta tecnología es la reducción drástica de los costos directos relacionados con las comunicaciones, tanto en líneas dial-up como en conexiones WAN dedicadas.

- Se puede en cualquier momento aumentar el ancho de banda de su conexión VPN contactándose en cualquier momento, y según su necesidad, con su proveedor de servicios de Internet.
- No se compromete la seguridad de la red empresarial.
- El cliente remoto adquiere la condición de miembro de la LAN con permisos, directivas de seguridad.
- El cliente tiene acceso a todos los recursos ofrecidos en la LAN como impresoras, correo electrónico, base de datos.
- Acceso desde cualquier punto del mundo, siempre y cuando se tenga acceso a internet." (Pamela Isabel Gonzales)

2.3.1.5 Tipos de VPN

a. "Sistemas Basados en Hardware

Este tipo de VPNs se caracterizan por tener en cada extremo de la red LAN de cada empresa un Ruteador o Router el cual tiene a función abrir y cerrar el túnel para proteger la información utilizando encriptación y cifrado. Además proporcionan facilidades en la administración, son seguros y fáciles de usar e instalar.

b. Sistemas basados en firewall

Este tipo de VPN aprovecha las características del "Firewall" o "Cortafuego" para restringir el acceso a la red o la generación de registros de posibles peligros, y ofrecen además otras opciones como traducción de direcciones o facilidades de autenticación.

La desventaja de este tipo de VPN es que afecta el rendimiento del sistema.

Algunos fabricantes de Firewalls ofrecen en sus productos procesadores dedicados para encriptación para minimizar el efecto del servicio VPN en el sistema.

c. Sistemas basados en software

Estos sistemas basados en software son utilizados en el caso de que los dos extremos que deseen comunicarse en forma remota y privada no pertenezcan a la misma empresa.

La ventaja de este sistema es la flexibilidad pues se puede decidir que trafico será enviado por el túnel VPN.

La desventaja consiste en que estos sistemas son difíciles de administrar, ya que necesitan estar familiarizados con el sistema operativo Cliente, la aplicación VPN y los mecanismos de seguridad adecuados.**”** (Salas, 2011)

2.3.1.6 Arquitecturas de conexión VPN

a. **“VPN de acceso remoto**: Éste es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan a la empresa desde sitios remotos (oficinas comerciales, domicilios, hotel, aviones, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.
b. **VPN punto a punto:** Este esquema se utiliza para conectar oficinas remotas con la sede central de una organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las oficinas remotas se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar las costosas conexiones punto a punto tradicionales.**”** (http-peru :: Arquitecturas Conexión VPN, 2012)

2.3.1.7 RED PRIVADA VIRTUAL USANDO SOFTWARE LIBRE

Las VPNs representan una gran solución para las empresas e instituciones en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha convertido en un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro.

El uso de métodos de autentificación en implementación de VPNs asegura que sólo los usuarios autorizados acceden a la VPN de la organización.

Es un método de seguridad para evitar el robo de información confidencial que afecta a la infraestructura de IPs usando métodos de encriptación con VPN.

2.3.2 Categorización Fundamental de la VD

2.3.2.1 Vulnerabilidades en VoIP

"Las vulnerabilidades y amenazas contra la voz sobre IP son numerosas y van en aumento. El potencial daño que los atacantes pueden hacer a los sistemas a través de la VoIP es alarmante, ya que heredan las vulnerabilidades que sufren las redes de datos por que se apoyan en PBX y servidores IP, plataformas que son seguras si las redes también lo son.

Norton by Symantec, Las líneas de VoIP son susceptibles a los tipos de ataques a los que están expuestos las conexiones web y correo electrónico." (Norton by Symantec. Las vulnerabilidades de VoIP, 2011)

a. Principales Vulnerabilidades:

1) **Spam.-** El sistema VoIP está expuesto al marketing no deseado, más conocido como SPIT (Spam sobre Telefonía por Internet).
2) **Interrupciones**.- Son ataques de red como gusanos y virus que pueden interrumpir el servicio o desconectar el servicio de VoIP.

3) **Phishing de voz.-** Conocido como Vishing se da cuando un atacante se contacta con el usuario mediante VoIP e intenta engañarlo para que divulgue los datos personales como información de tarjetas de crédito o cuentas bancarias.
4) **Perdida de privacidad**.- El tráfico de VoIP no está cifrado, lo que facilita a que los intrusos escuchen las conservaciones de VoIP.
5) **Hacking**.- Los Hackers podrían acceder a la conexión VoIP y utilizar las líneas para hacer llamadas.
6) **Red y energía**.- Si el servicio de internet falla se interrumpirá el servicio de VoIP con el riesgo no poder realizar llamadas en caso de emergencia."

b. Principales Precauciones

La comunicación VoIP ofrece excelentes beneficios y funciones útiles, de modo que lo único que tiene que hacer es asegurarse de implementarla de forma segura teniendo en cuenta las siguientes precauciones.

1) **Seguridad del equipamiento.** Seleccione el equipamiento VoIP que aplica los estándares actuales de seguridad inalámbrica como acceso protegido de Wi-Fi (WPA), WPA2, y también IEEE 802.11i.
2) **Autenticación y cifrado.** Active las funciones de autenticación y cifrado que se encuentran disponibles con su sistema VoIP. Esto mantendrá a las personas no autorizadas alejadas de su red y protegerá la privacidad de sus llamadas.
3) **Firewall de VoIP.** Use un firewall específicamente diseñado para el tráfico de VoIP. El firewall identificará llamadas inusuales y supervisará los signos de posibles ataques.
4) **Dos conexiones.** Si es posible, tenga una conexión de Internet separada para su línea de VoIP de modo que los virus o los ataques que implican una amenaza para los datos de su red no afecten a su teléfono.
5) **Protección actualizada.** Utilice tecnología actualizada de antivirus y antispam en sus dispositivos.

6) **Concienciación.** Usted puede convertirse en una sólida línea de defensa si está atento a posibles actividades extrañas en su línea de VoIP y se familiariza con las técnicas que usan los atacantes. (Cevallos Calderón, 2011)

2.3.2.2 Técnicas de ataques Eavesdropping

TECNICAS USADAS POR EAVESDROPPING	CARACTERISTICA
Sniffing	Capturar paquetes de información que circulan por la red con la utilización de una herramienta apropiada para ello, instalada en un equipo conectado a la red; o bien mediante un dispositivo especial conectado al cable. En redes inalámbricas la captura de paquetes es más simple, pues no requiere de acceso físico al medio.
AIRsniffing	Captura de paquetes de información que circulan por redes inalámbricas. Para ello es necesario contar con una placa de red wireless configurada en modo promiscuo y una antena.
War Driving y Netstumbling	Consisten en circular por un vecindario o zona urbana, con el objeto de capturar información transmitida a través de redes inalámbricas. Lo que en ocasiones las hace más vulnerables es la falta de seguridad con que se encuentran implementadas (HARO DÌAZ, 2011)

Tabla 1 Técnicas de ataques eavesdropping

Elaborado por: Investigador

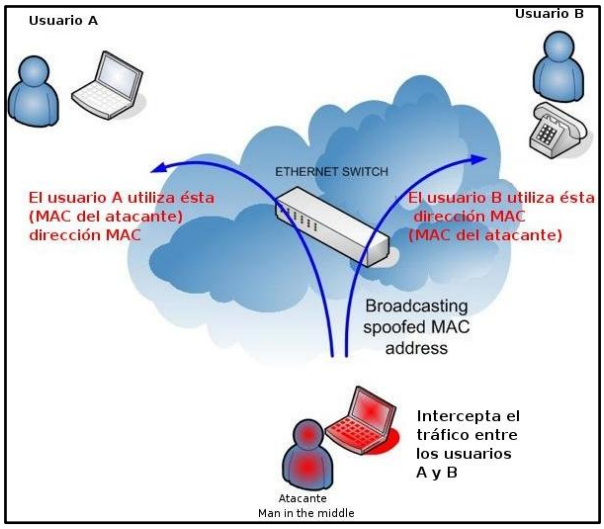


Figura 5 Ataques eavesdropping

Fuente: http://blog.txipinet.com/2006/10/11/40-seguridad-en-voip-iii-captura-de-conversaciones-o-eavesdropping/

a. Eavesdropping

Se traduce como escuchar secretamente.

Es la escucha sin ser partícipe de una conversación entre varias personas.

El Eavesdropping intercepta la señalización y los streams (transmisión de video o audio remotamente a través de una red) de audio de una conversación. Los mensajes de señalización utilizan protocolos separados, es decir, UDP (Protocolo de Datagrama de Usuario) o TCP (Protocolo Orientado a la Conexión). Los streams normalmente se transportan sobre UDP utilizando el protocolo RTP (Protocolo de Tiempo Real). (Sagarminaga, 2011)

b. Impacto de Eavesdropping

El impacto de esta técnica es más que evidente, interceptando comunicaciones es posible obtener toda clase de información sensible y altamente confidencial. Y aunque en principio se trata de una técnica puramente pasiva, razón por la cual hace difícil su detección, es posible intervenir también de forma activa en la comunicación insertando nuevos audios redireccionar o impedir que los datos lleguen a su destino.

c. Forma de interceptar de Eavesdropping

Las formas de conseguir interceptar una comunicación pueden llegar a ser tan triviales como esnifar el tráfico de la red si los datos no van cifrados. Existen excelentes sniffers como ethereal/Wireshark que permitirán capturar todo el tráfico de segmentos de la red. Por el contrario, lo normal sería encontrarse dentro de redes conmutadas por lo que para esnifar el tráfico que no vaya dirigido a un equipo serán necesarias otras técnicas más elaboradas como realizar un "Main in the Midle" utilizando Envenenamiento ARP .

d. Herramientas de captura de tráfico

Entre las herramientas que se puede utilizar se encuentra el conocido programa ettercap, Cain & Abel, la suite de herramientas para Linux Dsniff y vomit (Voice over misconfigured Internet telephones) por citar algunos ejemplos.

Hay que señalar también la creciente utilización de redes inalámbricas supone en muchos casos una vía más a explotar por parte del intruso. Redes Wifi mal configuradas junto con una infraestructura de red insegura puede facilitar el trabajo del intruso a la hora de acceder a la red VoIP para lanzar sus ataques. (Gil)

2.3.2.3 Ataques EAVESDROPPING en VoIP.

Eavesdropping cuenta con ciertas diferencias frente a interceptar datos y voz.

En VoIP se diferencia básicamente en dos partes dentro de la comunicación:
La señalización y el flujo de datos los cuales utilizarán protocolos diferentes. En la señalización el protocolo a usar es el SIP mientras que en el flujo de datos normalmente se utilizará el protocolo RTP sobre UDP.

2.4 Hipótesis

La implementación de una Red Privada Virtual usando software libre disminuiría los ataques EAVESDROPPING en la red de comunicaciones VoIP de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato.

2.5 Señalamiento de Variables

V I: Red privada virtual.

V D: Ataques EAVESDROPPING en VoIP.

CAPITULO III

3. MARCO METODOLÓGICO

3.1 Enfoque

El presente trabajo investigativo tomará un enfoque cuali-cuantitativo por las siguientes consideraciones:

Enfoque Cualitativo

La investigación cualitativa requiere un profundo entendimiento del comportamiento humano y las razones que lo gobiernan. La investigación cualitativa busca explicar las razones de los diferentes aspectos de tal comportamiento. (WIKIPEDIA1)

Por cuanto las técnicas cualitativas permitieron conocer, analizar y recolectar información, opiniones y criterios de las personas involucradas en el problema, los cuales fueron: Administrador de Red y personal Administrativo.

Permitiendo de esa forma a la investigación tener una orientación, percepción y perspectiva clara del problema, con el objetivo de contextualizar lodo lo relacionando al problema.

Enfoque Cuantitativo

La metodología cuantitativa es aquella que permite examinar los datos de manera científica, o más específicamente en forma numérica, generalmente con ayuda de herramientas del campo de la estadística. (WIKIPEDIA, Investigación cuantitativa)

Según el párrafo anterior se puede acotar que el enfoque es cuantitativo porque para el análisis de la información obtenida mediante encuestas se puede usar herramientas estadísticas.

3.2 Modalidades básicas de la investigación.

La presente investigación tiene las siguientes modalidades:

- **Modalidad bibliográfica o documentada**

Se ha considerado esta modalidad porque se ha tomado de fuentes de información como tesis de grado, revistas, anuncios, blogs, libros, revistas virtuales, bibliotecas virtuales.

- **Modalidad experimental**

Se ha considerado la relación de la variable independiente por cuanto una Red Privada Virtual y su relación con la variable dependiente la cual disminuiría los Ataques EAVESDROPPING en VoIP.

- **Modalidad de Campo**

Se ha considerado esta modalidad debido a que el investigador irá a recoger la investigación primaria directamente de los involucrados a través de encuestas.

3.3 Tipos de Investigación

Se ha realizado la investigación exploratoria la misma que permitió plantear el problema de investigación la fuga de información en el sistema de comunicaciones VOP en la FISEI, como de la misma manera ayudó a plantear la hipótesis La implementación de una Red Privada Virtual usando software libre disminuiría los ataques EAVESDROPPING en la red de comunicaciones VoIP de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato

Se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar en tiempo y espacio, construyendo el análisis crítico, contextualización y los antecedentes investigativos.

Por otro lado se ha tomada la investigación correlacional ya que ha permitido medir la compatibilidad de la variable independiente Red privada virtual con la variable dependiente Ataques EAVESDROPPING en VoIP.

3.4 Población y Muestra

3.4.1 Población

El estudio realizado se enfocó para beneficiar a los Administradores de Red y para el personal Administrativo de la facultad. Los cuales fueron acogidos para la aplicación del proyecto.

CARGO	NUMERO DE PERSONA
Administrador de Redes	1
Personal Administrativo	9

Tabla 2 Población
Elaborado por: Investigador

3.4.2 Muestra

En consideración al tamaño de la población se va a trabajar con todos sus componentes integrados por el Administrador de Redes y Personal Administrativo de la FISEI, lo cual permitirá obtener resultados más confiables.

Cálculo de la muestra:

$$N = \frac{PQN}{(N-1)E^2/K^2 + PQ}$$

$$\text{n} = \frac{0{,}25(10)}{(10-1)0{,}1^2/2^2 + 0{,}25}$$

$$\text{n} = \frac{2.5}{(9)0{,}01/4 + 0{,}25}$$

$$\text{n} = \frac{2.5}{0.09/4 + 0{,}25}$$

$$\text{n} = \frac{2.5}{0.00225 + 0{,}25}$$

$$\text{n} = \frac{2.5}{0.2725}$$

$$\text{n} = 9.1743$$

$$n = 9$$

3.5 Operacionalización de Variables

3.5.1 **Variable Independiente**: Red privada virtual

CONCEPTO	**CATEGORIA**	**INDICADORES**	**ITEMS**	**TÉCNICAS E INSTRUMENTOS**
Métodos de seguridad para evitar el **robo** de información **confidencia**l que afecta a la **infraestructura** de IP usando métodos de encriptación con VPN**.**	Robo Confidencialidad Infraestructura IP	Secuestro, Filtración, suplantación Datos empresa, Datos empleados VPN	¿Qué tipo de robos ha sufrido su sistema? ¿Qué datos fueron filtrados por los atacantes? ¿Qué infraestructura de red implementa la empresa?	Encuesta al administrador de sistema VoIP (cedula del entrevistado) Personar Administrativo.

Tabla 3 Operacionalización Variable Independiente

Elaborado por: Investigador

3.5.2 Variable Dependiente: Ataques EAVESDROPPING en VoIP.

CONCEPTO	CATEGORIA	INDICADORES	ITEMS	TÉCNICAS E INSTRUMENTOS
Escucha secretamente conversaciones VoIP por parte de clientes que no participan en dicha conversación, con el objetivo de interceptar la señalización y los streams de audio.	Escucha	Información filtrada Usurpación de identidad	¿Qué información se ha escuchado?	Encuesta al administrador de sistema VoIP (cedula del entrevistado) Personar Administrativo.
	Secretamente	Clonación de información	¿Cómo ha afectado el filtro de tal información?	
	Interceptar	Filtración,	¿Cómo afecto a la Facultad los datos interceptados?	
	Mensajes	Conversaciones	¿Qué mensajes fueron alterados?	

Tabla 4 Operacionalización de Variable Dependiente
Elaborado por: Investigador

3.6 Recolección y análisis de la información

TIPOS DE INVESTIGACIÓN

SECUNDARIA	PRIMARIA
Se recolecta de estudios realizados anteriormente. Se encuentra registrada en documentos y material digital: libros electrónicos, tesis de grado, revistas, periódicos. Las fuentes de información son: bibliotecas, hemerotecas, archivos, centros de documentación.	Se recolecta directamente a través del contacto directo con los administradores del sistema de VoIP

Tabla 5 Recolección y análisis de la información
Elaborado por: Investigador

RECOLECCIÓN DE LA INFORMACIÓN

PREGUNTAS	EXPLICACION
¿Para qué?	Implementar una Red privada virtual usando software libre para disminuir los ataques Eavesdropping en la red de comunicación VoIP en la FISEI de la UTA.
¿Para qué? ¿A qué personas? Con que aspectos	Recolectar información primaria para comprobar y contrastar con la hipótesis. La población se tomara de los administradores de sistemas de VoIP. Variable Independiente.- Ataques EAVESDROPPING en VoIP.

	Variable Dependiente.- Red privada virtual usando software libre.
Quien	Verónica Casicana
Cuando	De acuerdo al cronograma establecido
Lugar de recolección de la información	Instituciones con sistemas de VoIP
Cuantas veces	1 sola vez
Que técnica de recolección	Encuesta
Con que	(cedula de la entrevistada)
En qué situación.	Situación normal y cotidiana.

Tabla 6 Recolección de la información
Elaborado por: Investigador

3.7 Procesamiento y análisis de la información.

- **Análisis de los datos**

La presentación de los datos se hará a través de un resumen por cada pregunta de la entrevista realizada al Administrador de Sistemas y Redes de la Facultad y al Personal Administrativo de la Facultad.

Interpretación de los resultados.

Estudiar cada uno de los resultados por separado.

Redactar una síntesis e interpretación cualitativo general de los resultados.

CAPITULO IV

4. ANALISIS E INTERPRETACÓN DE LOS RESULTADOS (Encuesta)

Una vez finalizada la encuesta al Administrador de Sistemas y Redes y al personal administrativo de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, la información obtenida fue tabulada y analizada de forma sistemática de acuerdo a las preguntas planteadas, además interpretados de forma estadística para obtener resultados más confiables.

Se utilizó tecnología y herramientas de Microsoft, como es el Excel 2010, lo que nos permitirá presentar gráficas entendibles y apropiadas; que nos ayudará a apreciar adecuadamente la distribución de las respuestas a las preguntas tabuladas anteriormente.

Al finalizar, después de cada gráfica se realiza un análisis e interpretación de cada pregunta, lo cual ayudó a entender la situación de la facultad con respecto al problema planteado.

ENCUESTA REALIZADA AL ADMINISTRADOR DE REDES Y AL PERSONAL ADMINISTRATIVO DE LA FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL DE LA UTA.

Pregunta 1. ¿Cuáles son las formas de comunicación que se usa actualmente en la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la UTA?

El teléfono ( )

Los libros ( )

Correo electrónico ( )

Redes Sociales ( )

Teléfonos Móviles ( )

	ITEMS	**FRECUENCIA**	**%**
1	El teléfono	8	80
2	Los libros	0	0
3	Correo electrónico	2	20
4	Redes Sociales	0	0
5	Teléfonos Móviles	0	0
TOTAL		**10**	**100**

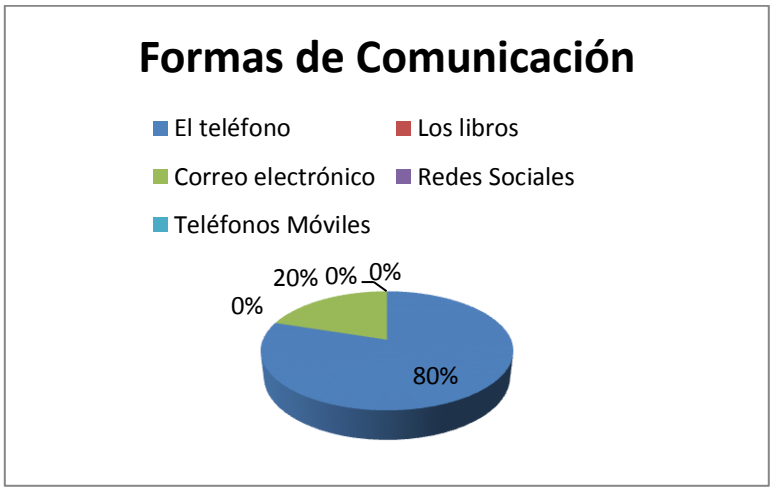


Tabla 7 Pregunta 1

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 80% que representa 8 personas nos indica que en la facultad el medio de comunicación más usado es el teléfono; el 20% que representa 2 personas nos indican usan el correo electrónico como medio para transmitir datos.

Por lo tanto según José Miguel Roca Chillida el teléfono está presente en todos los lugares en los que se pasa la mayor parte del tiempo (trabajo, calle, domicilio, etc.), de forma que se ha generalizado de manera silenciosa y se ha deslizado hasta los lugares más íntimos de las actividades individuales

Pregunta 2. ¿Considera Usted que la comunicación que viaja mediante los medios de comunicación está fuera del alcance de delitos informáticos?

a. Si ( )

b. No ( )

	ITEMS	FRECUENCIA	%
1	SI	0	0
2	NO	10	100
TOTAL		**10**	**100**

Tabla 8 Pregunta 2

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 100% que representa la totalidad de las personas encuestadas nos indica que la comunicación que viaja mediante los medios de comunicación actuales en la FISEI está al alcance de delitos informáticos.

Por lo tanto según Wikipedia La inseguridad informática es la falta o poca presencia de seguridad informática en un sistema operativo, aplicación, red o dispositivo, esto permite su demostración por hackers éticos (sombreros blancos) o su explotación por hackers mal intencionados (sombreros negros).

Pregunta 3. Que información comparte mediante los diferentes medios de comunicación

Información trabajo ( )

Información privada ( )

Anuncios publicitarios ( )

Entretenimiento ( )

Para hacer negocios ( )

	ITEMS	FRECUENCIA	%
1	Información trabajo	9	90
2	Información privada	0	0
3	Anuncios publicitarios	0	0
4	Entretenimiento	0	0
5	Negocios	1	10
TOTAL		**10**	**100**

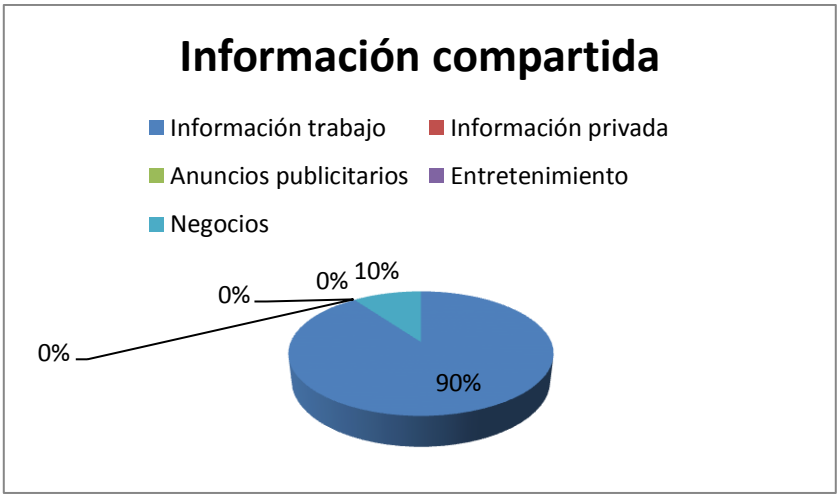


Tabla 9 Pregunta 3

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 90% que representa 9 personas nos indica que la información que se comparte mediante los diferentes medios de comunicación es relacionada al trabajo y el 10% que representa a 1 persona la información que comparte mediante los medios de comunicación son de negocios.

Pregunta 4. ¿Mediante qué medio de comunicación transmite la información?

a. Teléfono ( )

b. Celular ( )

b. Redes sociales ( )

b. Telefonía IP ( )

b. Correo electrónico ( )

	ITEMS	FRECUENCIA	%
1	Teléfono	4	40
2	Celular	1	10
3	Redes Sociales	0	0
4	Teléfono IP	0	0
5	Correo Electrónico	5	50
TOTAL		**10**	**100**

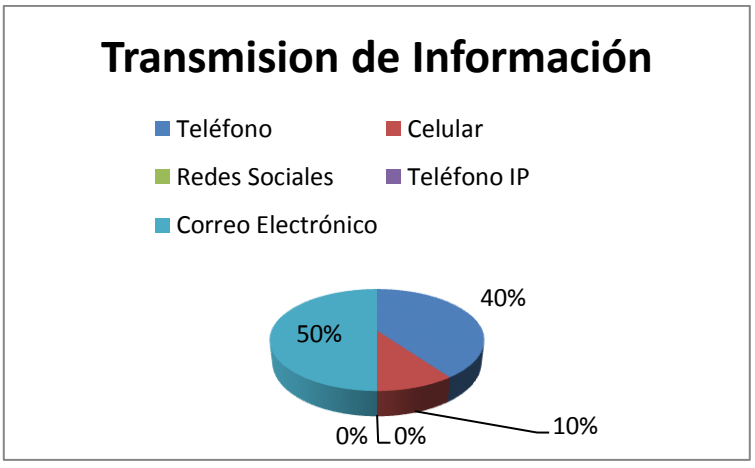


Tabla 10 Pregunta 4

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 50% que representa 5 personas nos indica para transmitir información dentro de la facultad usan el correo electrónico, el 40% que representa a 4 personas nos indica que usan el teléfono y el 10% que representa a 1 persona usa el celular como medio para comunicarse.

Pregunta 5. ¿Cómo califica al servicio contratado para la transmisión de información telefónica?

a. Muy Buena ( )

b. Buena ( )

c. Regular ( )

d. Mala ( )

	ITEMS	FRECUENCIA	%
1	Muy Bueno	1	10
2	Bueno	7	70
3	Regular	2	20
4	Mala	0	0
TOTAL		**10**	**100**

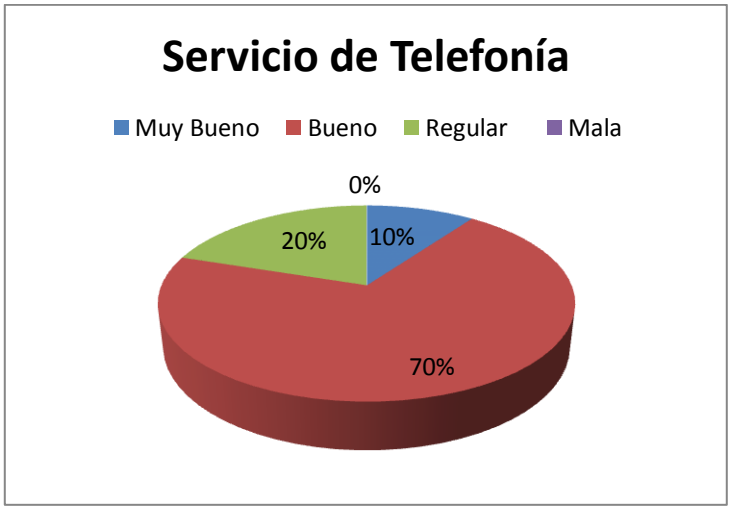


Tabla 11 Pregunta 5

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 70% que representa 7 personas nos indican que el servicio de telefonía es bueno, el 20% que representa a 2 personas nos indica que el servicio de telefonía es regular y el 10% que representa a 1 persona nos indica que es muy bueno.

Pregunta 6. ¿Qué tipo de tráfico se transmite actualmente a través de la tecnología utilizada?

a. Datos ( )

b. Voz ( )

c. Video ( )

	ITEMS	FRECUENCIA	%
1	Datos	1	10
2	Voz	7	70
3	Video	2	20
TOTAL		**10**	**100**

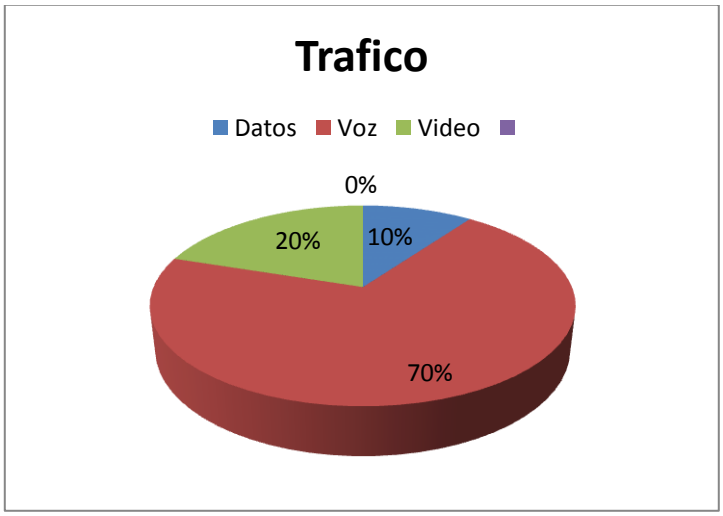


Tabla 12 Pregunta 6

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 70% que representa 7 personas nos indican que se transmite voz, el 20% que representa a 2 personas nos indica que transmite voz y el 10% que representa a 1 persona nos indica que transmite datos.

Pregunta 7. ¿Considera Usted que la red utilizada actualmente por la institución, es menos costosa en relación a otras tecnologías de transmisión de información?

a. Si ( )

b. No ( )

	ITEMS	FRECUENCIA	%
1	Si	5	50
2	No	5	50
TOTAL		**10**	**100**

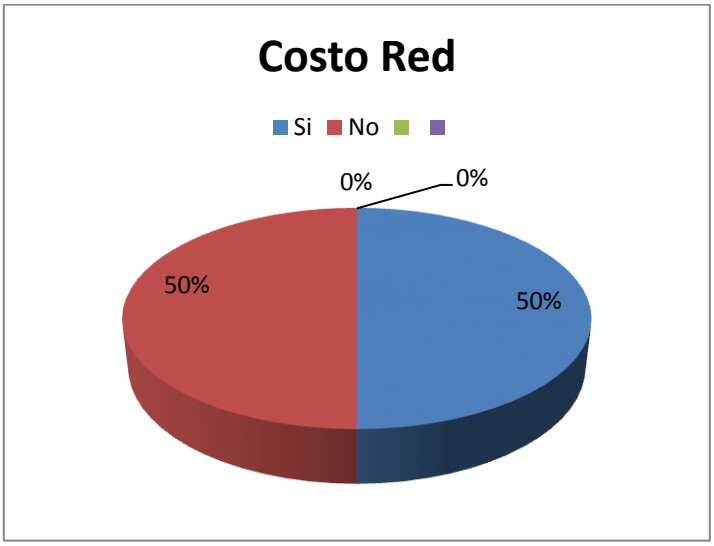


Tabla 13 Pregunta 7

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 50% que representa 5 personas nos indican que el servicio de comunicación si es costosa y el 50% que representa a 5 persona nos indica que no.

Pregunta 8. ¿Cree usted que es importante implementar procedimientos para evitar que delincuentes informáticos accedan a información confidencial? ¿Por qué?

Si ( ),……

No ( ),……

	ITEMS	FRECUENCIA	%
1	Si	10	100
2	No	0	0
TOTAL		**10**	**100**

Tabla 14 Pregunta 8

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 100% que representa 10 personas nos indican que si es importante implementar procedimientos para evitar que delincuentes informáticos accedan a información confidencial

Pregunta 9. ¿Conoce usted sobre la Red Privada Virtual?

a. Si ( )

b. No ( )

	ITEMS	FRECUENCIA	%
1	Si	6	60
2	No	4	40
TOTAL		**10**	**100**

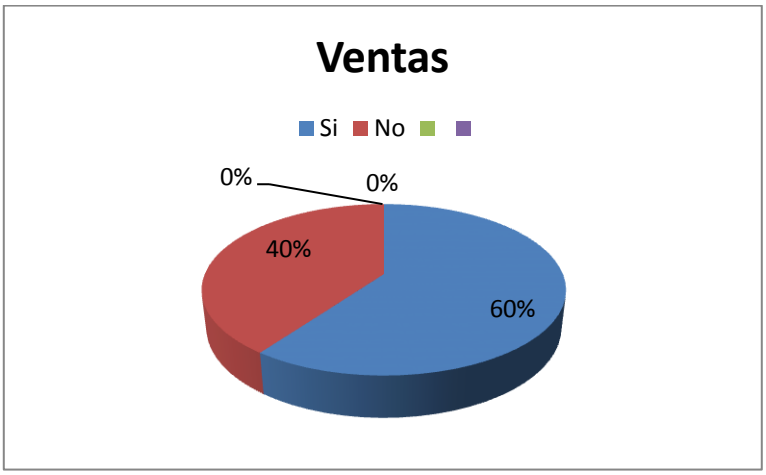


Tabla 15 Pregunta 9

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 60% que representa 6 personas nos indican que si conoce sobre la Red Privada Virtual y el 40% que representa a 4 persona nos indica que no.

Pregunta 10. ¿Cree usted que es importante implementar una Red Privada Virtual como medida de seguridad para evitar ataques informáticos hacia la transmisión de datos y voz?

a. Si ( ),

b. No ( ),

	ITEMS	FRECUENCIA	%
1	Si	10	100
2	No	0	0
TOTAL		**10**	**100**

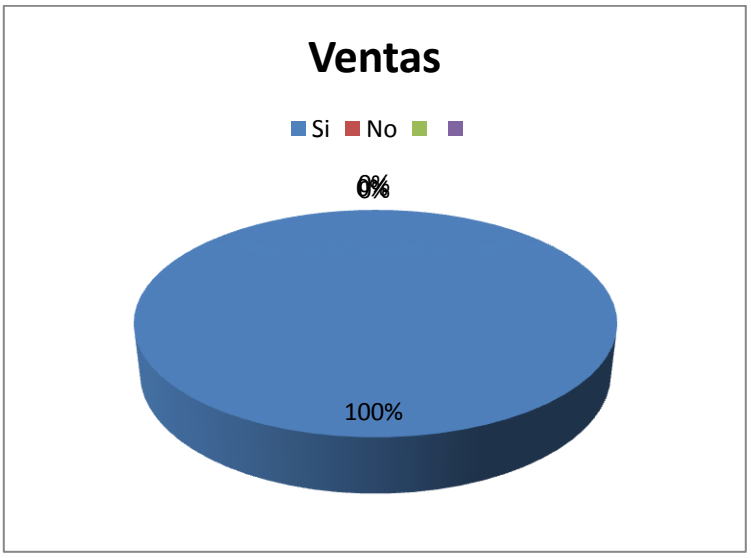


Tabla 16. Pregunta 10

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 10% que representa 10 personas nos indican que es importante implementar una Red Privada Virtual como medida de seguridad para evitar ataques informáticos hacia la transmisión de datos y voz

Pregunta 11. ¿Cuáles cree que serían las razones para implementar una nueva alternativa tecnológica para la transmisión de información de voz, datos y video?

a. Económicas ( )

b. Seguridad ( )

c. Calidad ( )

	ITEMS	FRECUENCIA	%
1	Económicas	2	20
2	Seguridad	8	80
3	Calidad	0	0
TOTAL		**10**	**100**

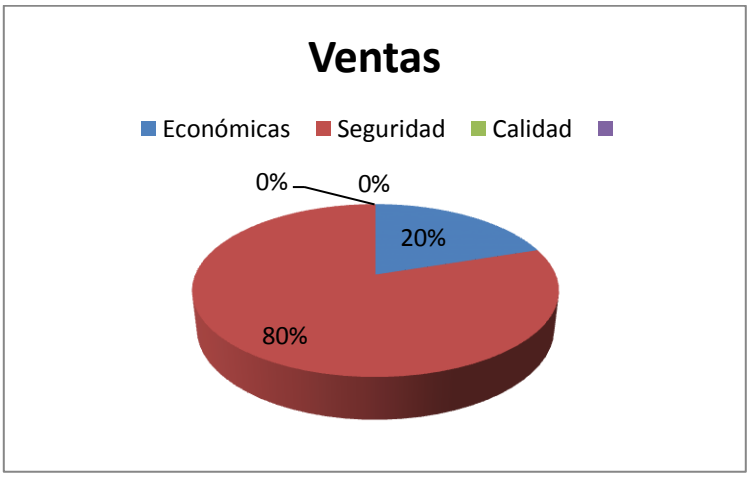


Tabla 17 Pregunta 11

Elaborado por: Investigador

ANALISIS E INTERPRETACIÓN

De las 10 personas encuestadas, el 80% cree que por Seguridad serían la razón para implementar una nueva alternativa tecnológica para la transmisión de información de voz, datos y video y el 20% que representa a 2 persona nos indica que sería por economía.

Comprobación de la Hipótesis

Se ha tomado en cuenta tres preguntas discriminantes, la numero 2, 8 y 10 de la encuesta aplicada, debido a que los resultados arrojados indican que :

Los medios de comunicación usada actualmente en la institución pueden estar propensos a ser víctima de delitos informáticos por la importancia de la información que viaja y ser fácilmente manipulada con fines delictivos.

Además el personal administrativo encuestado deduce que si es importante implementar procedimientos de seguridad para evitar ataques informáticos, por lo cual surge la importancia de diseñar procedimientos para que una Red Privada Virtual beneficie tanto al Área administrativa y Redes como a toda la Facultad.

Y de acuerdo a resultados obtenidos la creación de la VPN será muy favorable para la seguridad en el Sistema VoIP.

Previo al análisis e interpretación de resultados se ejecutó también la herramienta Nessus para identificar las vulnerabilidades del sistema y obtener un diagnóstico más legible.

CAPITULO V

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- ✓ Se concluye que la mayoría del personal Administrativo no se encuentra seguro de que la información que transmiten mediante la red este fuera del alcance de delitos informáticos (Enc Preg.2)
- ✓ Según previa investigación se concluye que medianamente el personal administrativo conoce sobre aplicaciones de seguridad como VPNs. (Enc. Preg.9)
- ✓ Los medios por los cuales se transmite la información de voz, datos y video no ayudan en la economía de la Facultad puesto que es muy costosa. (Enc. Preg. 7)
- ✓ Se necesita procedimientos de seguridad en el sistema de comunicaciones VoIP de la facultad. (Enc. Preg. 11)

5.2 Recomendaciones

✓ Se recomienda aplicar medidas de seguridad informática en las diferentes áreas de la Facultad con el objetivo de salvaguardar los datos que viajan mediante diferentes medios de comunicación.

✓ Se recomienda Fomentar el uso de aplicaciones con software libre en las diferentes Áreas de la Facultad. Que puede ser mediante capacitaciones, talleres, etc.

✓ Es importante usar todas las ventajas de contar con el Servidor Elastix implementado en la facultad.

✓ Se recomienda implementar una Red Privada Virtual (VPN) usando software libre para disminuir los ataques Eavesdropping en la red de comunicación VoIP en la Facultad De Ingeniería En Sistemas Electrónica E Industrial De La Universidad Técnica De Ambato

CAPITULO VI

6 PROPUESTA

6.1 Datos Informativos

- **Titulo**

VPN (Red Privada Virtual) usando software libre para disminuir los ataques eavesdropping en la red de comunicación VoIP en la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato.

- **Institución Ejecutora:**

Facultad de Ingeniería en Sistema Electrónica e Industrial de la Universidad Técnica de Ambato.

- **Director De Tesis:**

Ing. Luis Solís

- **Beneficiario:**

Facultad de Ingeniería en Sistema Electrónica e Industrial de la Universidad Técnica de Ambato.

- **Ubicación:**

Campus Huachi, - Av. Chasquis y Rio Payamino - Edificio Zeta.

- **Tiempo estimado para la ejecución:**

Fecha de inicio: Febrero de 2012

Fecha de Finalización: Mayo de 2013

- **Equipo técnico responsable:**

Investigador: Verónica Casicana

Administrador sistemas:

Coordinador: Ing. Luis Solís

6.2 Antecedentes de la Propuesta

La Facultad de Ingeniería en Sistemas Electrónica e Industrial FISEI usa Internet como medio de comunicación, el cual permite a sus usuarios contar con: correo electrónico, redes sociales entre otros. Estos medios no dejan de ser inseguros en cuanto a filtración de información se refiere. Además cuenta con un medio de comunicación llamado telefonía IP o telefonía en internet qué al hacer uso de Internet no deja de estar propenso a la Inseguridad Informática.

Por tal razón se da la necesidad de implementar una Red Privada Virtual (VPN) como herramienta de seguridad en el sistema de comunicaciones VoIP dentro de la FISEI, siendo el objetivo principal evitar los ataques EAVESDROPPING de información

confidencial de la red VoIP de la institución. Para poder asegurar la red VoIP, es necesario conocer y detectar las debilidades con las que cuenta el sistema.

Luego de investigaciones realizadas la institución cuenta con los equipos y sistemas de comunicación necesarias para la ejecución del proyecto, sin embrago los equipos no se encuentran actualmente en funcionamiento ya que el proyecto sobre la implementación de un sistema de comunicaciones de VoIP para la UTA utilizando software libre Elastix fue desarrollado hace varios años, esto provocó que los datos requeridos para el análisis no tengan antecedentes históricos.

Cabe recalcar que existen varias herramientas de seguridad para sistemas de VoIP. Para la presente investigación se ha tomado una de ellas con un previo análisis de costos y principalmente en la seguridad.

6.3 Justificación

El proyecto a continuación ha sido desarrollado con la finalidad de detectar y evitar ataques contra el servidor de comunicaciones VoIP de la FISEI. Además exponer una de las medidas de contingencia que se puede aplicar para su correcto funcionamiento, siendo la mejor opción la implementación de una Red Privada Virtual (VPN) como medida de seguridad informática.

La implementación de una VPN cumple con los requerimientos para proveer de seguridad al sistema ya que es un método para asegurar la transmisión de voz, datos y video.

VoIP transmite voz convertida a digital como corriente de datos, la solución de VPN en VoIP logra el cifrado de la voz por completo, aplicando los mecanismos estándares para cifrar datos disponibles en la colección de protocolos para la VPN.

Es por ello que se recomienda la ejecución de este proyecto ya que al contar con una red de comunicaciones VoIP con seguridades el uso de este medio de comunicación se podría expandir para toda la Universidad tomando en cuenta los altos beneficios que dispone.

6.4 Objetivos

6.4.1 Objetivo General

Implementar una VPN (Red Privada Virtual) usando Software Libre para evitar los ataques EAVESDROPPING que pudieran existir en el sistema de comunicación VoIP con la finalidad de evitar la fuga de información en la FISEI.

6.4.2 Objetivos Específicos

- Realizar un estudio y análisis de cómo actúan los ataques Eavesdroping en el sistema VoIP.
- Determinar las herramientas necesarias para monitorear los ataques Eavesdroping en el sistema.
- Plantear los procedimientos necesarios para la implementación de la VPN como medida de seguridad en el sistema de VoIP.

6.5 Análisis de Factibilidad

La propuesta es variable en varios ámbitos que son los siguientes:

- **Política**

De acuerdo a las políticas internas establecidas a nivel de seguridad informática el proyecto es viable para aplicar en la Facultad de Ingeniería Electrónica e Industrial porque requieren que los datos estén protegidos de filtraciones.

- **Socio Cultural**

El proyecto ayuda a la seguridad informática de la FISEI, al contar con mayor protección contra delincuentes informáticos en el sistema de VoIP evitará desprestigio de la institución al existir filtración de información.

- **Tecnológico**

El proyecto tiene por objetivo mejorara la seguridad informática en la Facultad, y así mismo hacer uso de la tecnología VoIP de una forma segura.

Para desarrollar el presente proyecto la Facultad cuenta con el equipo tecnológico necesario:

Servidor para Elastix, Softphone, Tarjetas, Red Interna

- **Equidad de género**

La implementación del proyecto puede ser realizada y posteriormente monitoreada por personas de cualquier género.

- **Ambiental**

La implementación del proyecto no afecta al medio ambiente por que no usamos sustancias que afecte al ecosistema.

- **Económico-financiero**

La Facultad de Ingeniería en Sistemas Electrónica e Industrial cuenta con el financiamiento necesario para los elementos requeridos para la implementación del presente proyecto.

- **Legal**

El proyecto se sujeta a todas las leyes que el estado y diferentes organismos ecuatorianos lo disponen.

6.6 Informe Técnico

A medida que crece la popularidad de VoIP, aumentan las preocupaciones por la seguridad de las comunicaciones y la telefonía IP. VoIP es una tecnología que se apoya en las capas y protocolos ya existentes de las redes de datos. Por eso en cierto modo la telefonía IP va a heredar ciertos problemas de las capas y protocolos ya existentes, siendo algunas de las amenazas más importantes de VoIP problemas clásicos de seguridad que afectan al mundo de las redes de datos. Por supuesto, existen también multitud de ataques específicos de VoIP.

Figura 6 Seguridad en VoIP

Fuente: http://dc236.4shared.com/doc/cy6WGNPT/preview.html

6.6.1 VoIP Segura

"Es esencial que VoIP se asiente sobre una infraestructura de red segura, protegida por cortafuegos bien administrados. Es muy recomendable la existencia en la red de sistemas de antivirus actualiza dos que la protejan de ataques de virus, gusanos y troyanos. La detección de muchos ataques se puede realizar instalando sistemas de detección de intrusos (IDS) o de prevención (IPS) en los lugares estratégicos de la red. Serán capaces de detectar y prevenir ataques contra los protocolos (Fuzzing),

ataques contra servicios (Exploits y vulnerabilidades), escaneos y ciertos tipos de ataques DoS." (ASTUDILLO, 2011)

6.6.2 Ataques en la capa de Seguridad en las Aplicaciones y Protocolos de VoIP

Fraudes,

SPIT SPAM,

Vishing Phising,

Fuzzing, Floods,

Secuestro de sesiones Hijacking,

Interceptación Eavesdroping. (SEGU-INFO, 2011)

6.6.3 Eavesdropping (Escucha no autorizada)

Se traduce como escuchar secretamente, es el término con el que se conoce la escucha de conversaciones VoIP por parte de clientes que no participan en una conversación. (HARO DÌAZ, 2011)

Técnicas para Eavesdropping

TECNICAS USADAS POR EAVESDROPPING	CARACTERISTICA
Sniffing	Capturar paquetes de información que circulan por la red con la utilización de una herramienta apropiada para ello, instalada en un equipo conectado a la red; o bien mediante un dispositivo especial conectado al cable. En redes inalámbricas la captura de paquetes es más simple, pues no requiere de acceso físico al medio.
AIRsniffing	Captura de paquetes de información que circulan por redes inalámbricas. Para ello es necesario contar con una placa de red wireless configurada en modo promiscuo y una antena.
War Driving y Netstumbling	Consisten en circular por un vecindario o zona urbana, con el objeto de capturar información transmitida a través de redes inalámbricas. Lo que en ocasiones las hace más vulnerables es la falta de seguridad con que se encuentran implementadas.

Tabla 18 Técnicas para Eavesdropping

Elaborado por: Investigador

La escucha en la VoIP no es el tradicional eavesdropping que se realiza en las redes de datos, aunque el concepto general continúa siendo el mismo. Las escuchas en VoIP requieren interceptar la señalización y los flujos de medios de una conversación. Hay que tener en cuenta que los mensajes de señalización y la media usan diferentes protocolos y puertos (UDP, TCP, RTP). Los flujos de media son transportados sobre UDP utilizando el protocolo RTP (Real Time Protocol).

Para este ataque se puede utilizar la herramienta Wireshark y Ettercap o en Windows Cain & Abel. (Bytecoders, 2011)

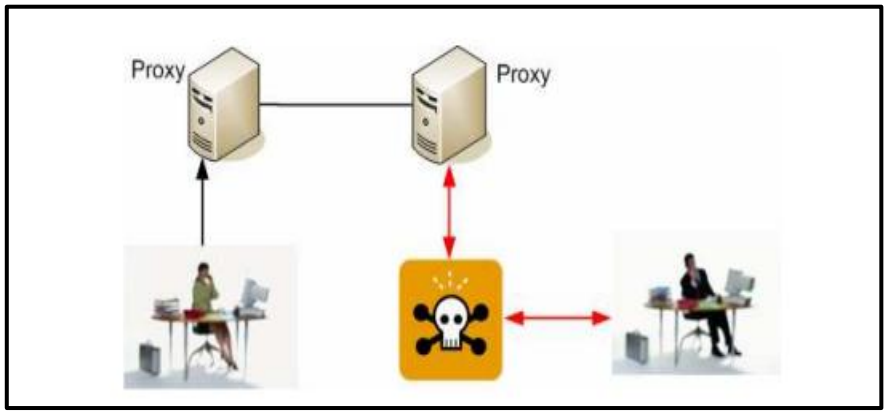


Figura 7 Ejemplo de eavesdropping

Fuente: http://www.uv.es/=montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf

6.6.4 Distribuciones Libres para VoIP

La voz sobre IP (VoIP) tiene sus bases en el mundo del software libre, ya que la mayor parte de los protocolos de Internet fueron diseñados para trabajar originalmente sobre sistemas Unix, del cual se origina GNU/Linux.

a. Asterisk

Es un software que proporciona funcionalidades de una central telefónica PBX, y que originalmente fue desarrollada para funcionar con el sistema operativo GNU/Linux, soportando muchos protocolos VoIP como lo son SIP, H.323, IAX y MGCP.

Para facilitarnos la instalación y posteriormente la administración de Asterisk, tenemos una serie de distribuciones libres con Asterisk reconfigurado e interfaz administrativa web, entre las que podemos mencionar. (WIKIPEDIA, WIKIPEDIA, 2013)

b. Elastix

Basado en CentOS Linux, incluye FreePBX. Distribución libre de Servidor de Comunicaciones Unificadas que incluye VoIP PBX, fax, mensajería instantánea, Email y colaboración. (Elastix, 2011)

c. Trixbox

Basado en CentOS Linux, incluye FreePBX entorno gráfico. Es una PBX con servicio para VoIP, diseñado para empresas de 2 a 500 empleados. (GuatchWuard, 2011)

d. Thirdlane

Basado en Linux y FreeBSD, es fácil de instalar, adaptar al cliente y gestionar. Usa Webmin como plataforma para la administración. Es una distribución comercial de pago. (Eric arrestad, 2011)

6.6.5 Red Privada Virtual

Virtual Private Network (VPN) es un grupo de dos o más sistemas de ordenadores, habitualmente conectados a una red corporativa privada, que se comunican con seguridad sobre una red pública.

A las VPN se les llama privadas porque se establecen específicamente entre el emisor y el receptor de la información, y virtuales porque no se necesita un medio físico directo entre los comunicantes.

Al usar una VPN, se crea una conexión privada segura a través de una red pública como Internet. Los usuarios remotos pueden hacer una llamada local a Internet, y no usar llamadas de larga distancia.

Al momento es la manera más acertada de encriptar la comunicación IP. (Chavarría, 2011)

6.6.6 Tipos de VPN

a. "Sistemas Basados en Hardware

Este tipo de VPNs se caracterizan por tener en cada extremo de la red LAN de cada empresa un Ruteador o Router el cual tiene a función abrir y cerrar el túnel para proteger la información utilizando encriptación y cifrado. Además proporcionan facilidades en la administración, son seguros y fáciles de usar e instalar.

b. Sistemas basados en firewall

Este tipo de VPN aprovecha las características del Firewall o Cortafuego para restringir el acceso a la red o la generación de registros de posibles peligros, y ofrecen además otras opciones como traducción de direcciones o facilidades de autenticación.

La desventaja de este tipo de VPN es que afecta el rendimiento del sistema.

Algunos fabricantes de Firewalls ofrecen en sus productos procesadores dedicados para encriptación para minimizar el efecto del servicio VPN en el sistema.

c. Sistemas basados en software

Estos sistemas basados en software son utilizados en el caso de que los dos extremos que deseen comunicarse en forma remota y privada no pertenezcan a la misma empresa.

La ventaja de este sistema es la flexibilidad pues se puede decidir que trafico será enviado por el túnel VPN.

La desventaja consiste en que estos sistemas son difíciles de administrar, ya que necesitan estar familiarizados con el sistema operativo Cliente, la aplicación VPN y los mecanismos de seguridad adecuados.**”** (Salas, 2011)

6.6.7 Arquitecturas de conexión VPN

“VPN de acceso remoto: Éste es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan a la empresa desde sitios remotos (oficinas comerciales, domicilios, hotel, aviones, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

VPN punto a punto: Este esquema se utiliza para conectar oficinas remotas con la sede central de una organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las oficinas remotas se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar las costosos conexiones punto a punto tradicionales.**”** (http-peru :: Arquitecturas Conexión VPN, 2012)

6.6.8 Requerimientos de una VPN

- Autenticación de Usuarios.- Verifica la identidad de los usuarios y restringir el acceso a la VPN solo a usuarios autorizados.
- Administración de Direcciones.- Asignar direcciones del cliente sobre la red privada, y asegurar que las direcciones privadas sigan siendo privadas.

- Encriptación de datos.- Los datos que viajan sobre la red pública, son transformadas a una forma ilegible para los usuarios que no posean privilegios de acceso.
- Administración de claves.- Se lleva un mantenimiento para las claves de encriptación para los clientes y los servidores.
- Soporte Multiprotocolo.- Manejar protocolos comunes, usando las redes públicas.

6.6.9 Detección de vulnerabilidades en la red VoIP

- **OpenVAS**

Escáner de vulnerabilidades, muy similar al Nessus, desarrollado por la comunidad de software libre.

- **NMAP**

Es una herramienta popular incluida en Red Hat Enterprise Linux que puede ser usada para determinar la distribución de la red. Nmap ha estado disponible por muchos años y es probablemente la herramienta más usada para reunir información..

Escáner para auditorías de seguridad en red. Permite escanear servicios TCP, UDP, ICMP, RPC, etc.

Para detectar vulnerabilidades en la red actual se usó la herramienta Nessus.

- **NESSUS**

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos.

En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios Exploits para atacarlo.

Los resultados del escaneo pueden ser exportados como informes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

A continuación en el gráfico se observa las vulnerabilidades que se encontró en el sistema de comunicaciones VoIP de la FISEI.

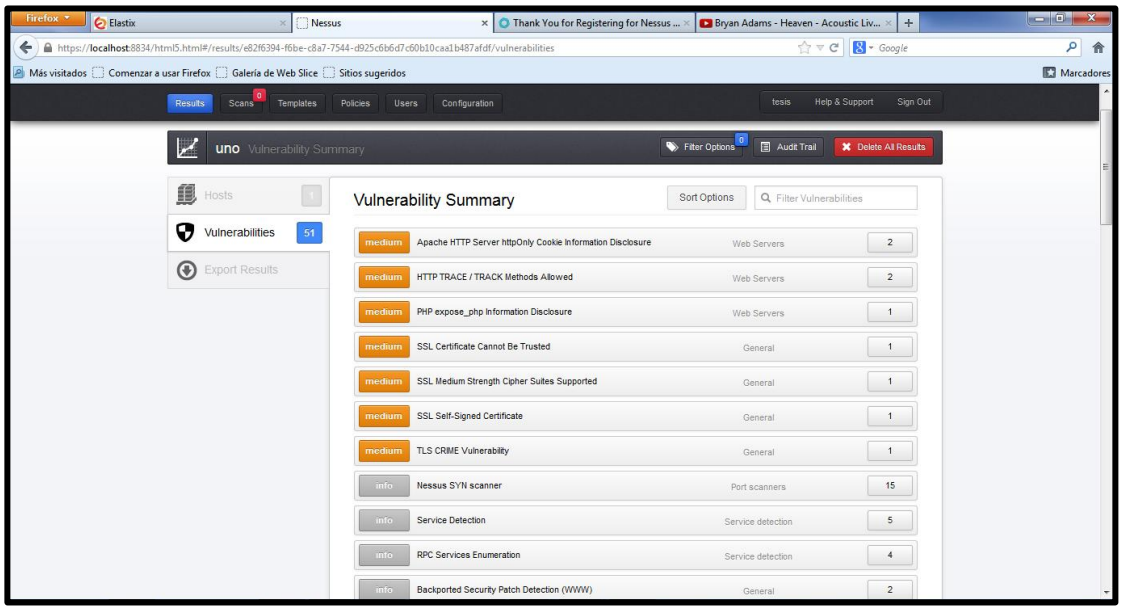


Figura 8 Escaneo de vulnerabilidades con Nessus

Fuente: Investigador

6.6.10 Captura de tráfico

Para este trabajo se aplicó la captura de trafico eavesdropping aplicando la técnica Sniffing, se usó las aplicaciones Wireshark el cual ya trae funcionalidad y filtros para redes VoIP.

Wireshark.- "Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo

de software y protocolos. Cuenta con todas las características estándar de un analizador de protocolos.” (VILLALON, 2011)

Se determinó una instancia de Wireshark para realizar la captura. Una vez abierto, se realizó los siguientes pasos:

Se seleccionó los parámetros de captura de la aplicación; desde el menú capture se seleccionó la interfaz a través de la cual se captura el tráfico (se puede seleccionar filtros de captura). Una vez establecidos, pulsar Accepter para comenzar la captura.

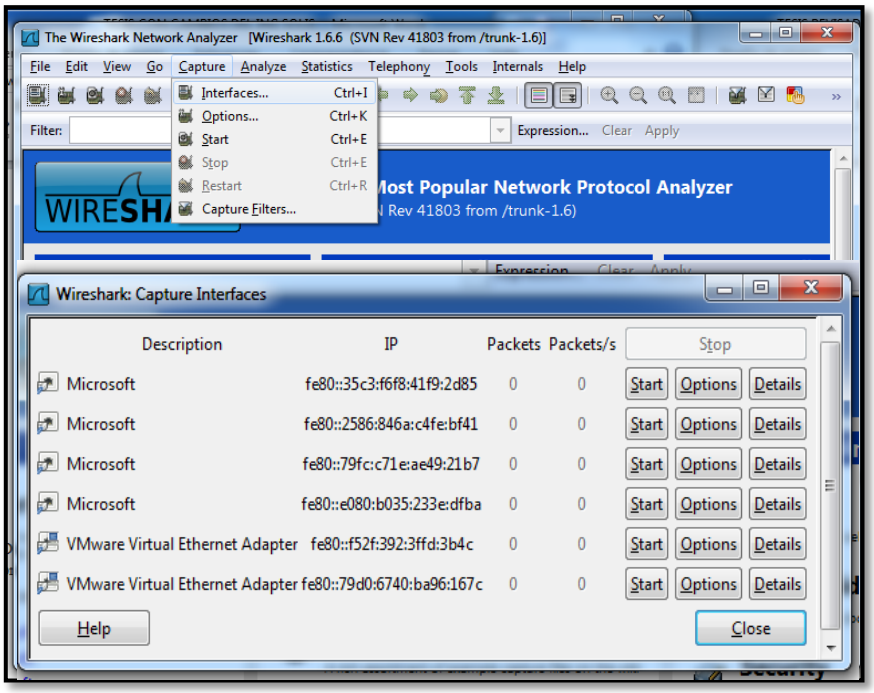


Figura 9 Captura de tráfico con Wireshark

Fuente: Investigador

Una vez capturados un número considerable de paquetes, se finaliza la captura, tras lo cual, se observó en la consola de Wireshark, la lista de paquetes capturados.

En este caso:

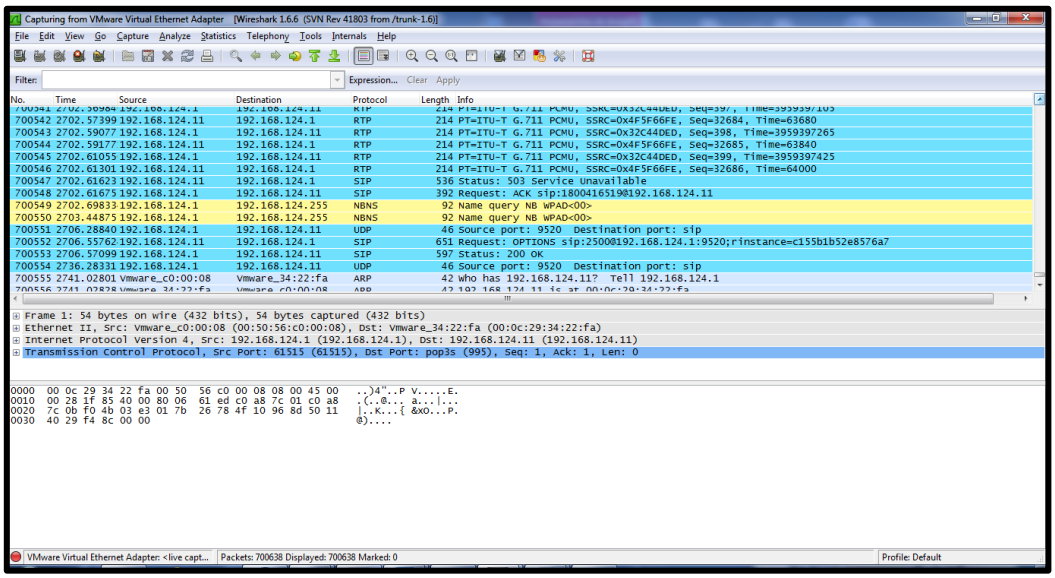


Figura 10 Lista de paquetes capturados

Fuente: Investigador

En este punto, se puede realizar distintos tipos de análisis de la red VoIP:

Estadísticas del protocolo de señalización SIP; pulsando en el menú

Statistics -> SIP -> Create Stat, donde se puede ver estadísticas de los distintos tipos de mensajes del protocolo:

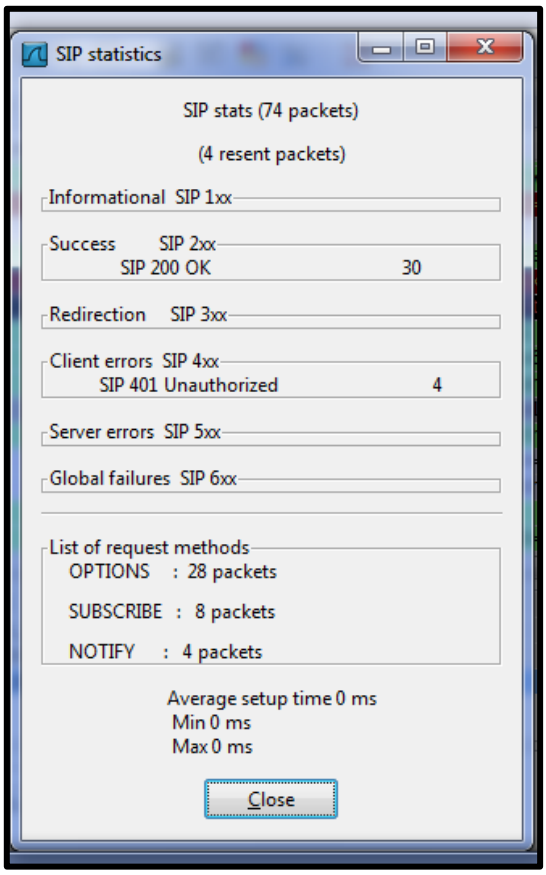


Figura 11 Estadística del protocolo de señalización SIP

Fuente: Investigador

Estadísticas del protocolo de transporte RTP; Se seleccionó uno de los paquetes RTP capturados y se pulsó en el menú “Statistics -> RTP -> RTP Streams“, donde se pudo ver los flujos RTP capturados.

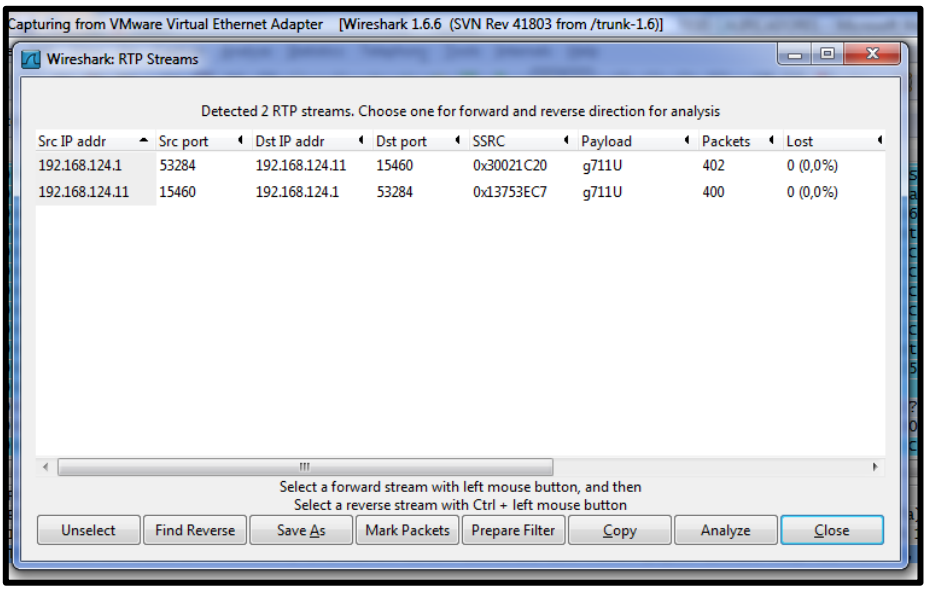


Figura 12 Estadísticas del protocolo de transporte RTP

Fuente: Investigador

Por ultimo para la captura de llamadas VoIP pulsar en el menú “Statistics -> VoIP Calls” se pudo ver todas las llamadas capturadas:

En el grafico se observa las llamadas de la PLANTA1 configurado previamente para el personal administrativo de la primera planta.

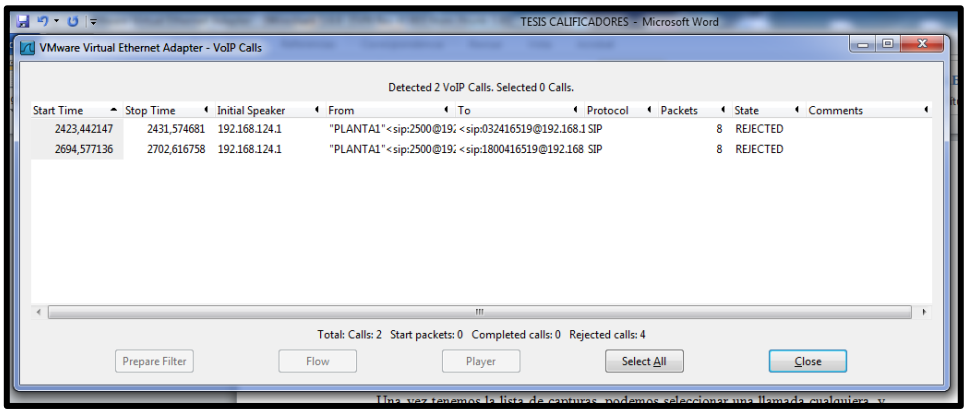


Figura 13 Estadísticas de llamadas VoIP

Fuente: Investigador

Una vez obtenida la lista de capturas, se seleccionó una llamada cualquiera, y se pudo obtener datos más concretos, como el intercambio de mensajes de señalización SIP (Pulsando la opción Graph).

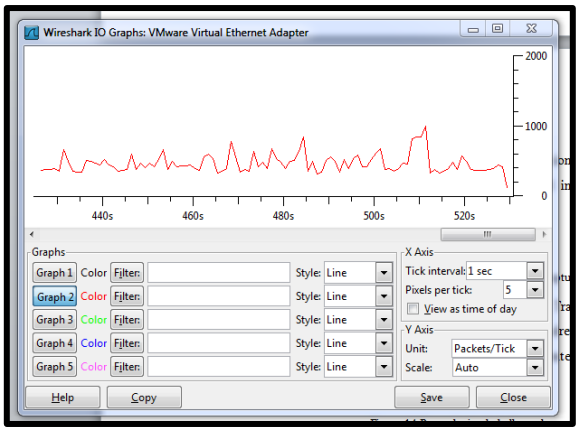


Figura. 14 Análisis de la llamada capturada

Fuente: Investigador

Y finalmente, reproducir la propia llamada capturada. Tras pulsar el botón "Player" en la pantalla anterior, se decodifico el paquete, y podremos ver los distintos streams de audio, pudiendo reproducirlos de forma independiente o conjunta:

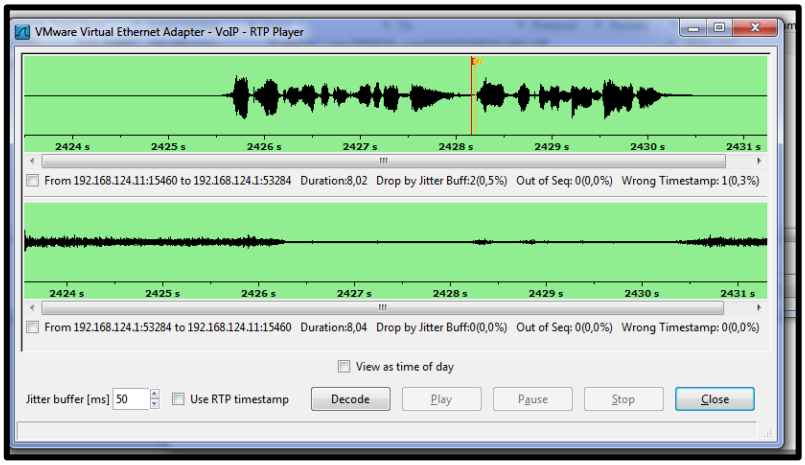


Figura 15. Reproduciendo la llamada capturada

Fuente: Investigador

6.6.11 PROGRAMAS PARA MONTAR UNA VPN

Una de las ventajas de la banda ancha, es que se puede ampliar la red local de ordenadores a cualquier parte del mundo, siempre que exista una conexión de internet.

“Se intenta englobar las virtudes de todos ellos en tan solo tres programas. Uno libre, otro gratuito y otro de pago. Los tres con similares funciones y válidos para Linux, Mac y Windows.

- **LogMeIn Hamachi**

El atributo principal de este cliente es la facilidad de uso. Para ello se debe crear una cuenta, instalar el programa y usar la dirección IP que nos proporciona. Y así con el resto de los ordenadores.

Aunque la aplicación es gratuita, el problema es que como el servidor VPN lo gestiona la empresa proveedora del programa, no podemos ejercer ningún control o configuración de la red.

Tener en cuenta que con esta aplicación gratuita no es posible conectar más de 16 ordenadores. Si se necesita de más, tienen una versión comercial con la que ofrece conectar hasta 256 equipos.

- **Cisco VPN**

Considerada la VPN con mayor excelencia, pero tiene un costo. Cisco es una empresa con una alta presencia en entornos corporativos y educativos. Cualquier cosa que se necesite para administrar el sistema para la red virtual, Cisco lo implementa.

- **OpenVPN**

Una aplicación libre y abierta para configurar de forma muy sencilla una VPN. Funciona de forma tradicional y controlada, instalando un servidor VPN en uno de

los ordenadores y los programas clientes en el resto de las máquinas que forman la red.

Además es capaz de importar configuraciones de otros programas comerciales y también está incluido en algunos routers de red para una mejor adaptación.” (RK2, 2010)

En el ámbito de la seguridad VoIP, el uso de una Red Virtual Privada (VPN) es una metodología muy recomendada para incrementar la seguridad en la red.

OpenVPN es un software libre utilizado para crear redes virtuales privadas, que implementa conexiones de capa 2 o 3 y usa los estándares de la industria SSL (Secure Sockets Layer)/TLS (Transport Layer Security) para cifrar.

OpenVPN tiene dos modos considerados seguros, uno basado en claves estáticas pre-compartidas y otro en SSL/TLS usando certificados y claves RSA. SSL/TLS es una de las mejores tecnologías de cifrado para asegurar la identidad de los integrantes de la VPN. Cada integrante tiene dos claves, una pública y otra privada, la clave privada debe permanecer secreta mientras la clave pública debe ser intercambiada para que puedan enviar mensajes.

6.6.12 VENTAJAS Y DESVENTAJAS DE PROGAMAS PARA VPN

APLICACION	VENTAJAS	DESVENTAJAS
LogMeIn Hamachi	• Aplicación libre y abierta • Configuración sencilla	• No es posible conectar más de 16 ordenadores. • No podemos ejercer ningún control o configuración de la red.
Cisco VPN	• VPN con mayor excelencia • Apta para entornos corporativos y educativos • Implementación acorde a los requerimientos para administrar el sistema para la red virtual.	• Tiene un costo
OpenVPN	• Aplicación libre y abierta para configurar. • Forma tradicional y controlada • Importa configuraciones de otros programas comerciales. • Está incluido en algunos routers de red • Conexiones de capa 2 o 3. • Seguridad por Usar los estándares SSL/TLS o claves estáticas para cifrar. • Protección de los usuarios remotos.	• Sin interfaces gráficas profesionales. • Utiliza sólo un puerto del firewall. • Todavía son relativamente pocos los que saben cómo usar OpenVPN.

Tabla 19. Ventajas y Desventajas

Fuente: Investigador

6.6.13 OPENVPN

OpenVPN es el protocolo VPN premier diseñado para redes de banda ancha modernas, pero no es compatible con los dispositivos móviles y tablets. OpenVPN ofrece un encriptado de 256-bits y es extremadamente estable y rápido en las redes con largas distancias y alto tiempo de espera. Provee mayor seguridad que PPTP y requiere menor uso de CPU que L2TP/IPsec. (Farrasaranjueztk, 2011).

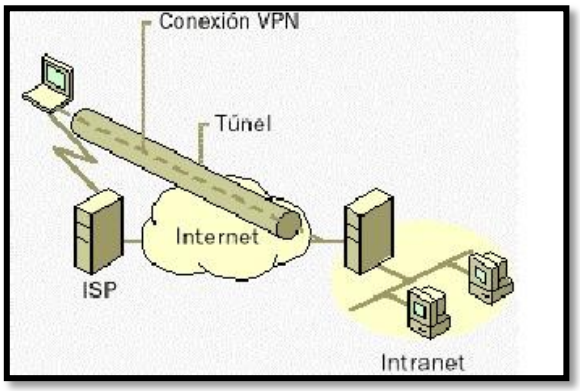


Tabla 20. Estructura de conexión VPN

Fuente: http://wwwisis.ufg.edu.sv/wwwisis/documentos/TE/621.385-Z25i/621.385-Z25i-Capitulo%20I.pdf

a) Compatibilidad de OpenVPN

Encriptación	160 bits 256 bits
Sistemas Compatibles	Windows Mac OS X Linux
Compatibilidad	Compatible con la mayoría de sistemas operativos de ordenadores de escritorio.
Seguridad	Ofrece la máxima seguridad. Los datos se autentican usando certificados digitales.
Velocidad	Ofrece los más altos rendimientos. Confiable en

	conexiones de alta latencia.
Configuración	Fácil de configurar con software.
Estabilidad	Proporciona la mejor estabilidad y confiabilidad. Se desempeña bien detrás de ruteadores inalámbricos, en redes Wi-Fi públicas y en poco confiables.
Conclusión	OpenVPN proporciona el mejor desempeño y la mayor seguridad. Se Recomienda OpenVPN para ordenadores de escritorio incluyendo Windows, Mac OS X y Linux.

Tabla 21.Características d Open VPN.

Fuente: Investigador

6.6.14 CONFIGURACIÓN DE LA VPN EN EL SISTEMA VOIP.

Configuramos las IPs del computador por el cual accedimos a la interfaz gráfica del servidor Elastix.

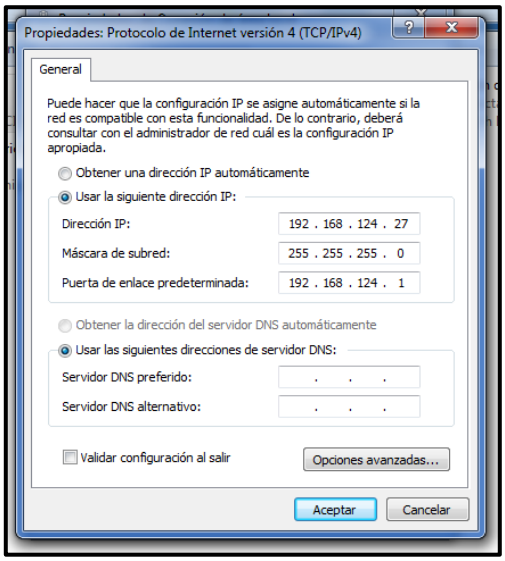


Figura 16. Configuración IP

Fuente: Investigador

IP: 192. 168.124.27 MASC: 255.255.255.0 BROAD: 192.168.124.1

Mediante un browser en el computador configurado anteriormente accedimos a la pantalla principal del servidor Elastix en donde nos pidió Nombre del servidor y Contraseña.

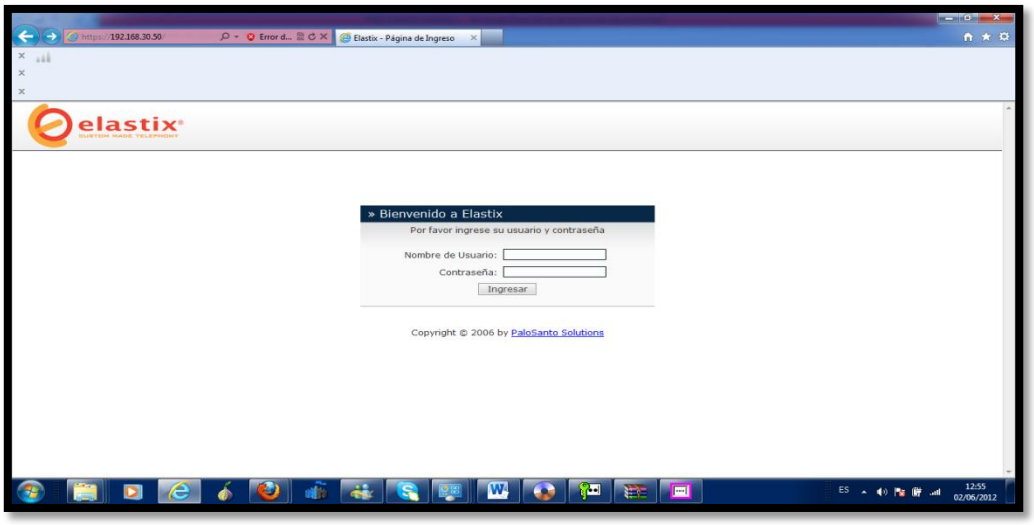


Figura 17. Pantalla de acceso a Elastix

Fuente: Investigador

En el siguiente gráfico podemos observar la pantalla principal del Servidor Elastix.

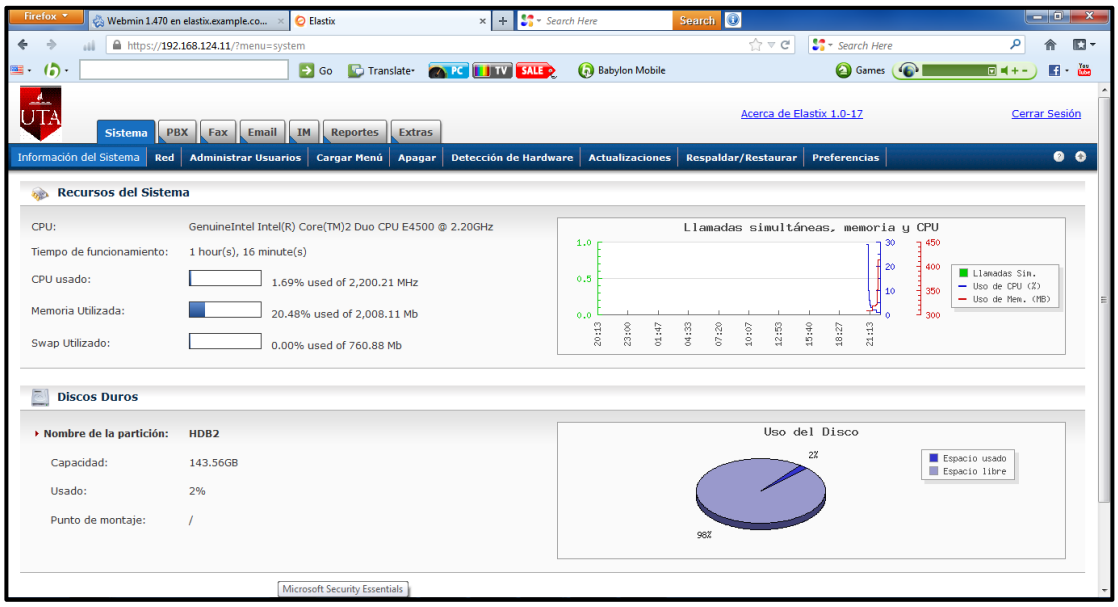


Figura 18. Pantalla principal Elastix

Fuente: Investigador

Configuración del Servidor VoIP

Configuración de extensiones

En primera instancia luego de ingresar a la interfaz gráfica de Elastix nos dirigimos al menú PBX, por defecto se accede a la Configuración PBX, y en esta sección escogemos del panel izquierdo la opción Extensiones. Y procedemos a crear una nueva extensión.

En nuestro caso la extensión SIP

EXTENCIONES CREDAS: (**LAB1 2500), (LAB2 2501), (LAB3 2502)**

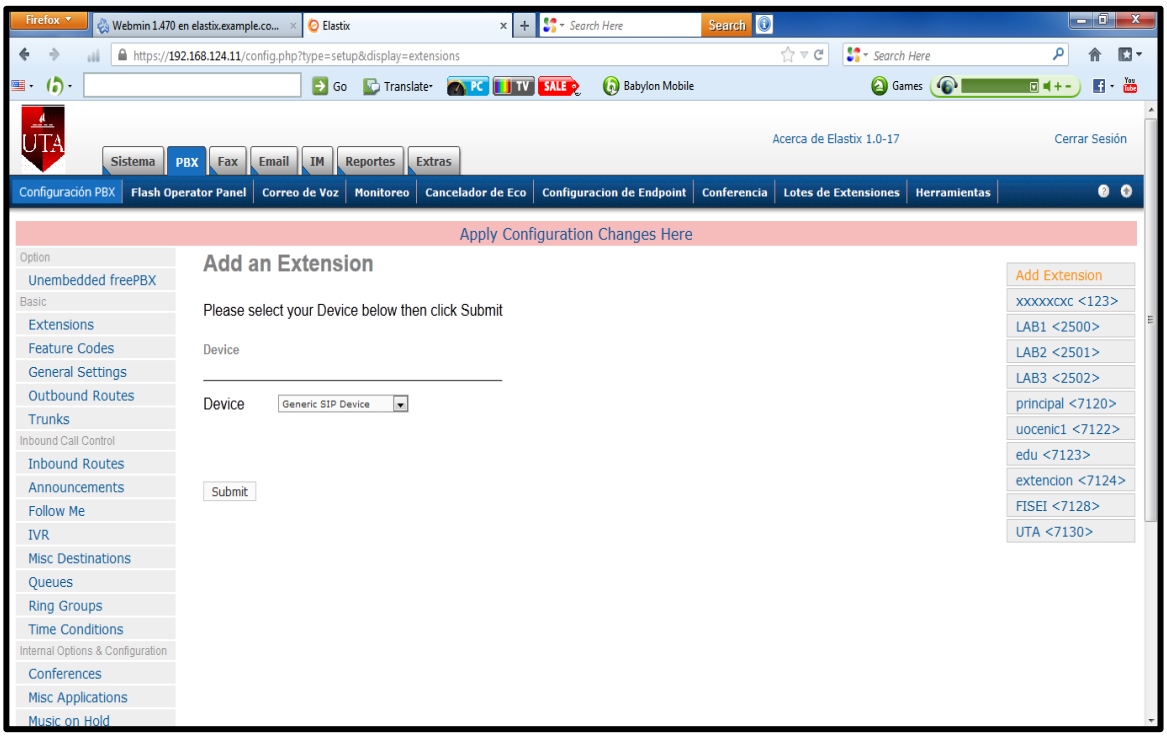


Figura 19. Configuración de Elastix

Fuente: Investigador

Creación de troncal SIP

Configuración de rutas entrantes

Para ello es necesario saber dónde se quiere recibir las llamadas, para esto hay que configurar una IVR(Respuesta de Voz Interactiva) denominada Menú Principal, y las llamadas se recibirán por la troncal ZAP(DAHDI).

Para configurar la ruta entramos al menú PBX en el panel izquierdo seleccionamos “Rutas Entrantes”, le damos un nombre descriptivo y en la sección “Set Destination” escogemos el destino en este caso la IVR(Interactive Voice Response- Respuesta de Voz Interactiva).

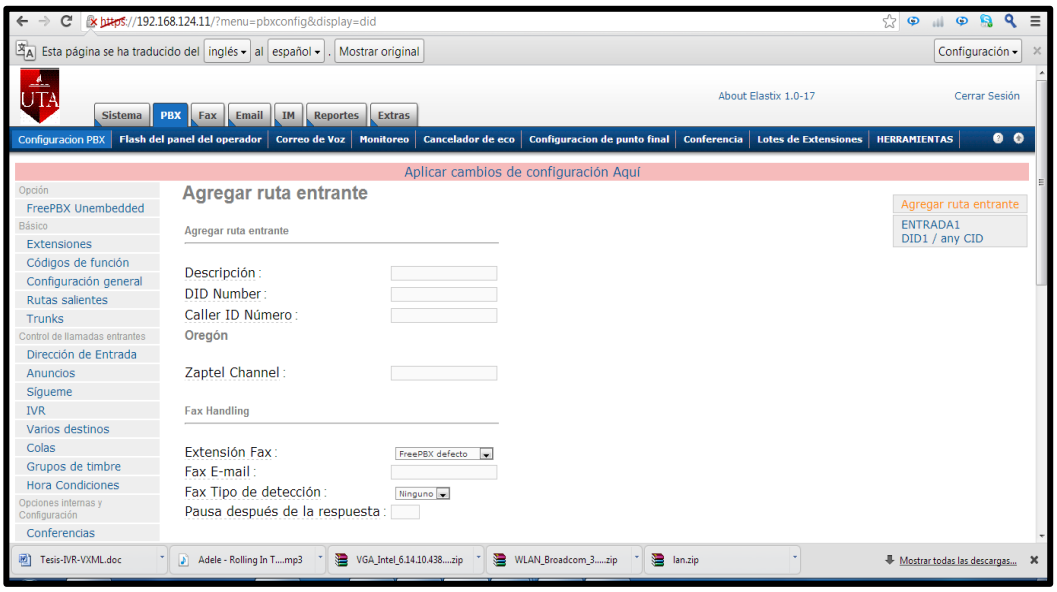


Figura 20. Configuración de rutas entrantes

Fuente: Investigador

Configuración de rutas salientes

Ingresar al menú “PBX” en el panel de la izquierda seleccionamos “Rutas Salientes” y le damos click, aparecerá el menú donde en “Route Name” pondremos un nombre descriptivo, en nuestro caso “saliente”.

Es importante colocar un plan de marcado adecuado, en nuestro caso lo hemos seleccionado de tal manera que solo se pueda realizar llamadas locales.

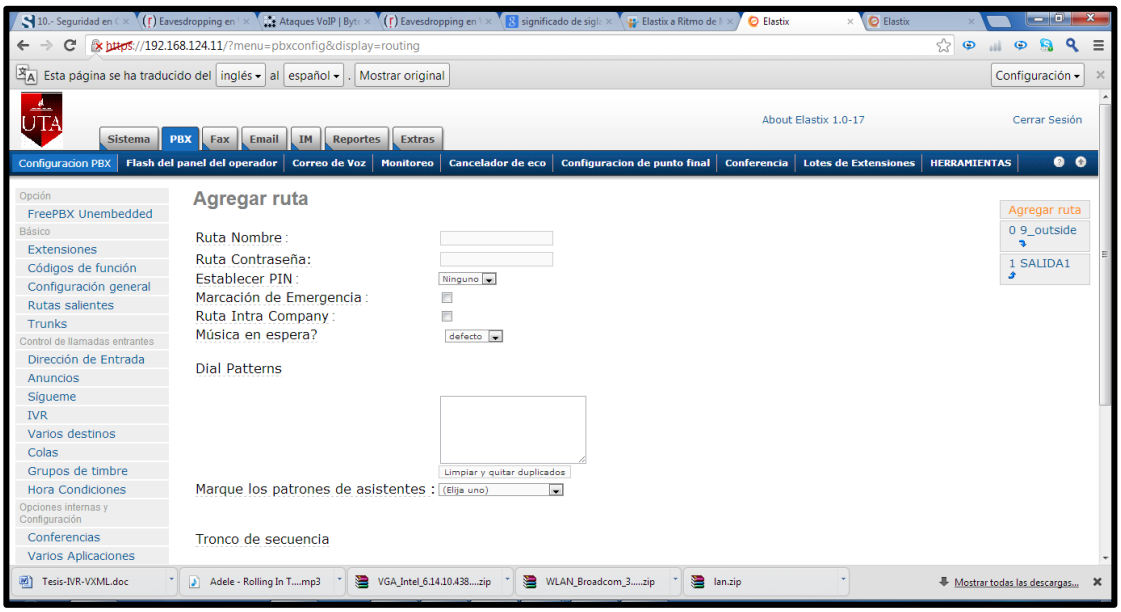


Figura 21. Configuración de rutas salientes

Fuente: Investigador

Configuración de las maquinas salientes.

Hardware

Intel Core i3 2.53 GHz

Memoria RAM de 4, 00 GB

Disco duro de 500G

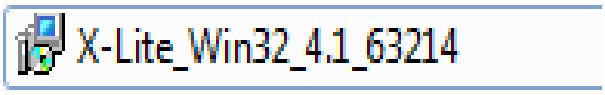
SOFTWARE UTILIZADO

1.- XLITE

Instalación.

Después de habernos descargado el softphone correctamente procedemos a instalar sobre el sistema operativo que uso actualmente Windows 7.

Damos click en el ícono que dice X-Lite_Win32_4.1_63214.



Aparece el programa de instalación. Y continúo con las instrucciones que se detallan en la descarga.

Figura 22. Inicio de instalación softphone XLite

Fuente: Investigador

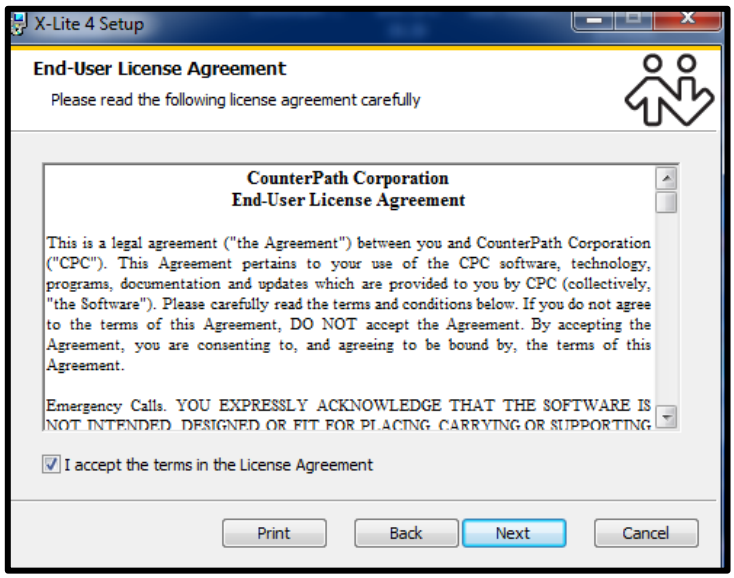


Figura 23. Aceptación de licencia software XLite

Fuente: Investigador

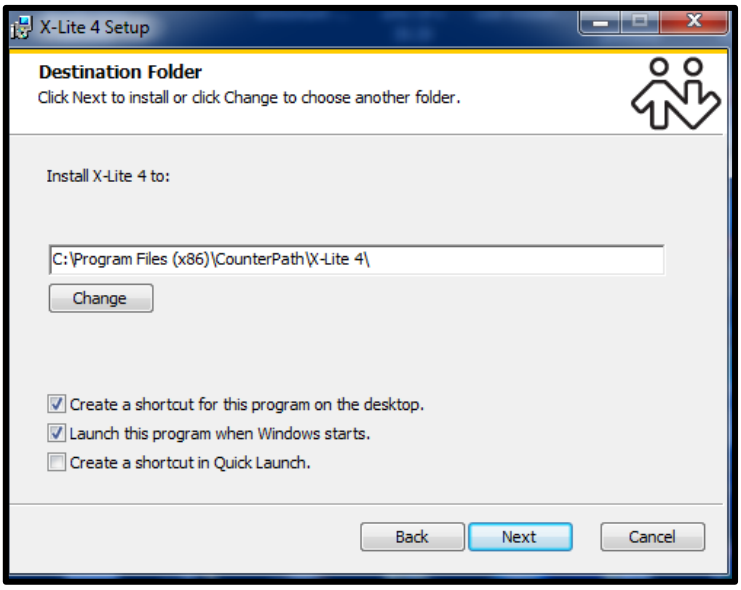


Figura 24. Ubicación en disco

Fuente: Investigador

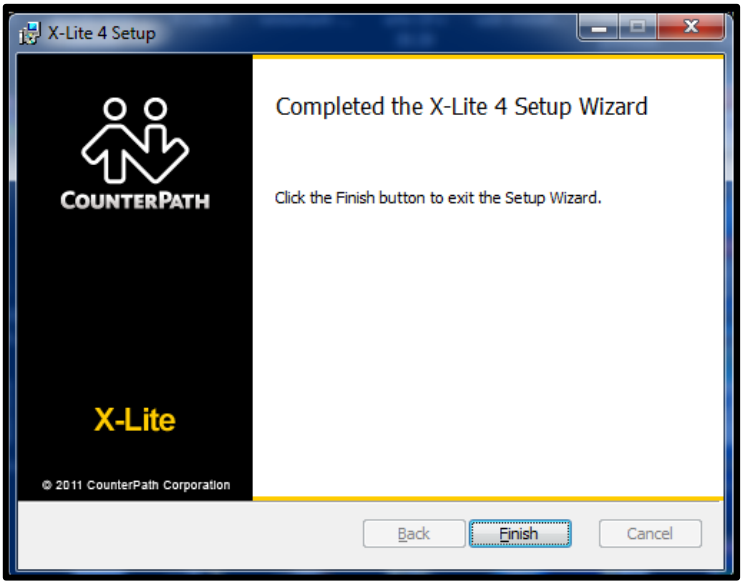


Figura 25. Fin Instalación

Fuente: Investigador

Configuración del softphone X-Lite:

Cuando finalice la instalación, damos doble click en icono de X-Lite que aparecerá en el escritorio:

Aparecerá, la opción softphone. Damos click en “Account Settings”.

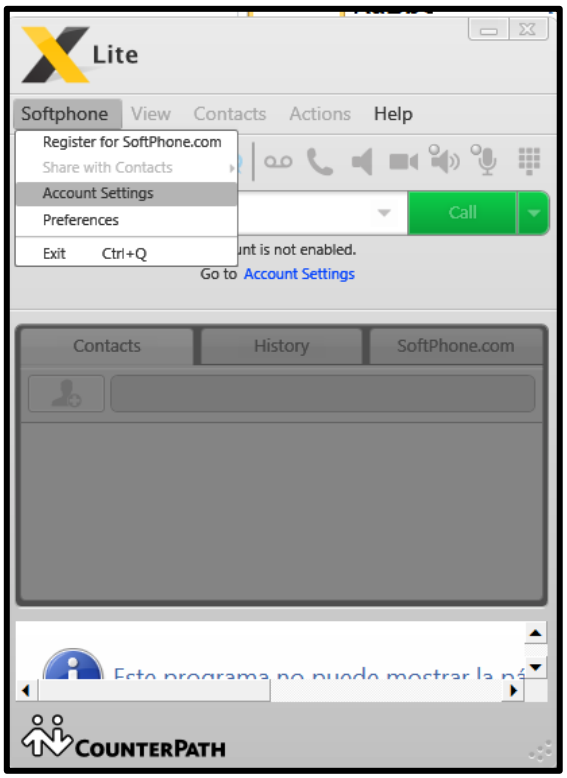


Figura 26. Instalación

Fuente: Investigador

Y nos desplegara todas las opciones para configurar nuestra extensión.

"Display Name": escribiremos el nombre del departamento que va a utilizar esta extensión. Este campo puede perfectamente estar en blanco, debido a que el nombre que está asignado en la extensión ya está configurado en la PBX.

"User Name": pondremos el número de extensión que configuramos, que es la 2500.

"Password": donde debemos escribir la clave que le asignamos en el "Secret", colocamos 2500 también.

Authorization User Name: aquí debemos colocar el mismo valor que tenemos en "User Name" 2500.

"**Domain":** colocamos la dirección IP de nuestra central Elastix que es 192.168.124.27.

“Proxy” “Address”: colocamos la dirección IP 192.168.124.27

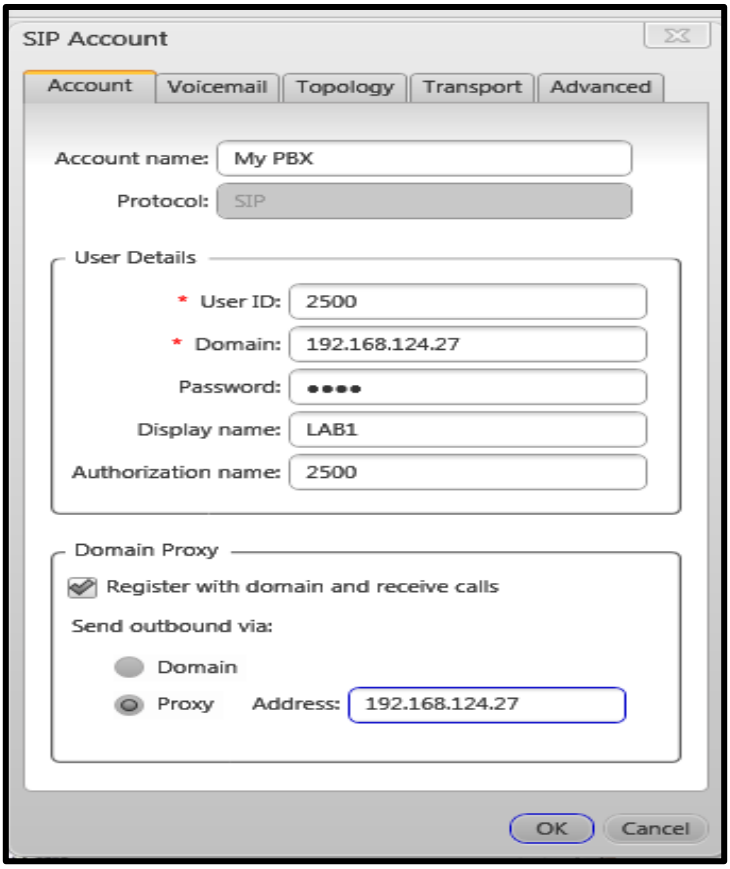


Figura 27. Configuración

Fuente: Investigador

Luego, solo le damos a “OK” y nuestro teléfono ya está registrado en nuestra central Elastix y se desplegará el número de extensión en la pantalla.

2.- ZOIPER COMUNICATOR

Instalación.

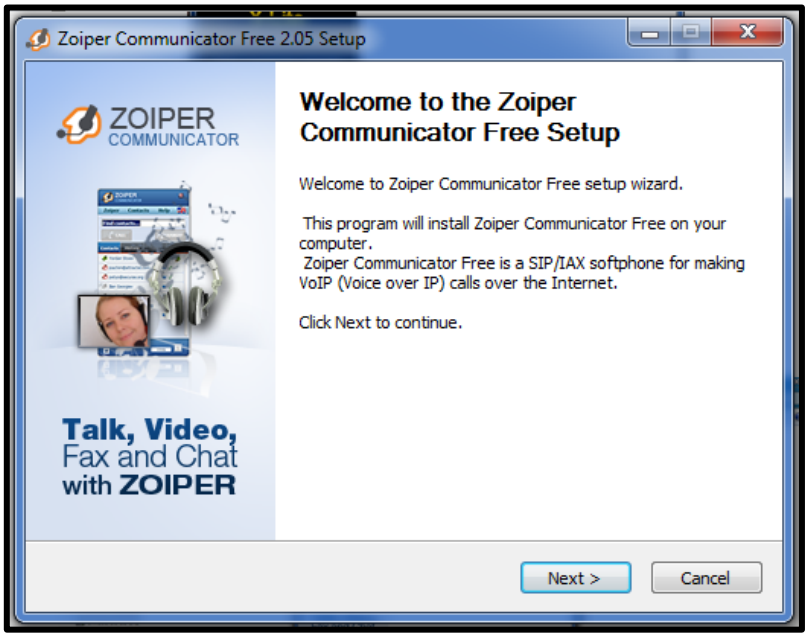


Figura 28. Inicio Instalación Zoiper

Fuente: Investigador

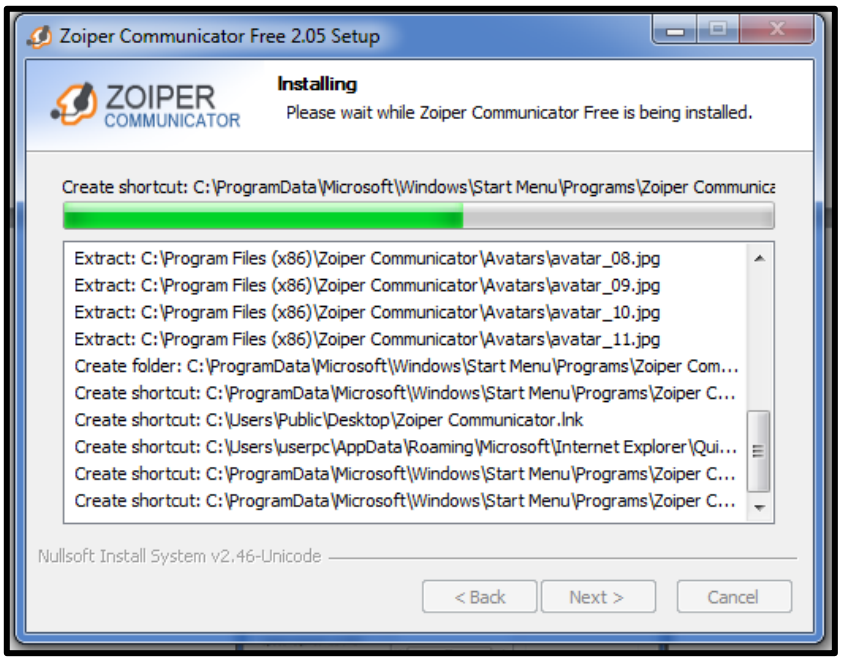


Figura 29. Fin Instalación

Fuente: Investigador

Configuración del softphone Zoiper Comunicator:

Cuando finalice la instalación, damos doble click en el icono Zoiper Comunicator que aparecerá en el escritorio:

Se procede a configurar.

En la parte superior elegimos la primera que es "Zoiper" y seleccionamos "preferences".

En "**preferences**": nos aparecen una serie de opciones a configurar. Damos click en **"Add new IAX account**" y nos aparecerá un cuadro donde pondremos LAB2 como nombre descriptivo de la cuenta.

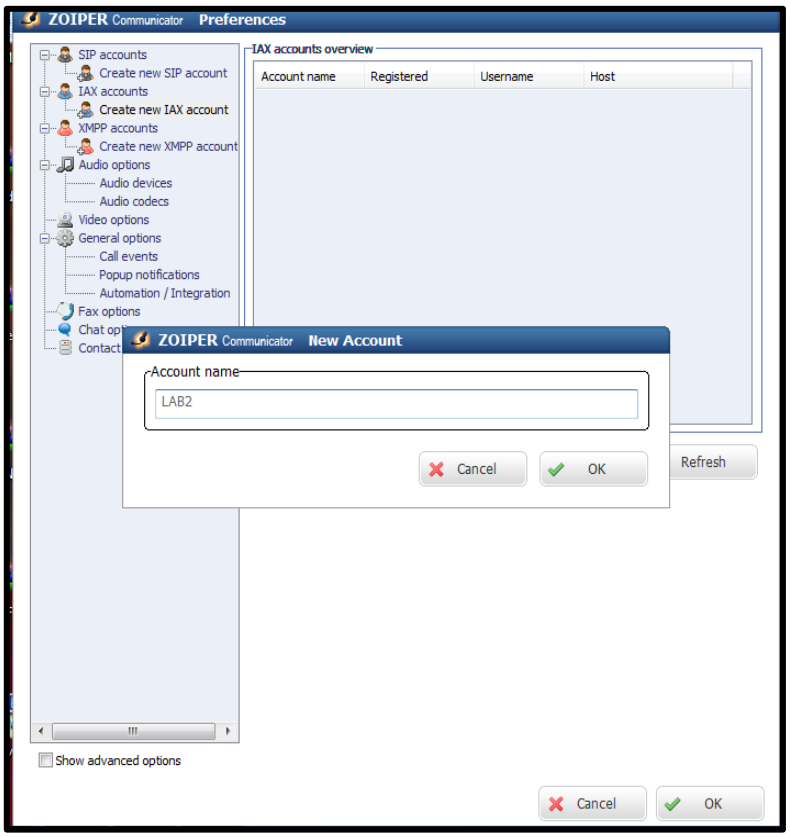


Figura 30. Configuración Zoiper

Fuente: Investigador

"Server Hostname/IP": agregamos la dirección IP de nuestra central Elastix 192.168.124.27.

"Username": colocamos el número de extensión "2520".

"Password" colocamos la contraseña "2520".

Los campos de **"Caller ID Name" y "Caller ID Number"** dejamos en blanco y por ultimo damos clic en "OK".

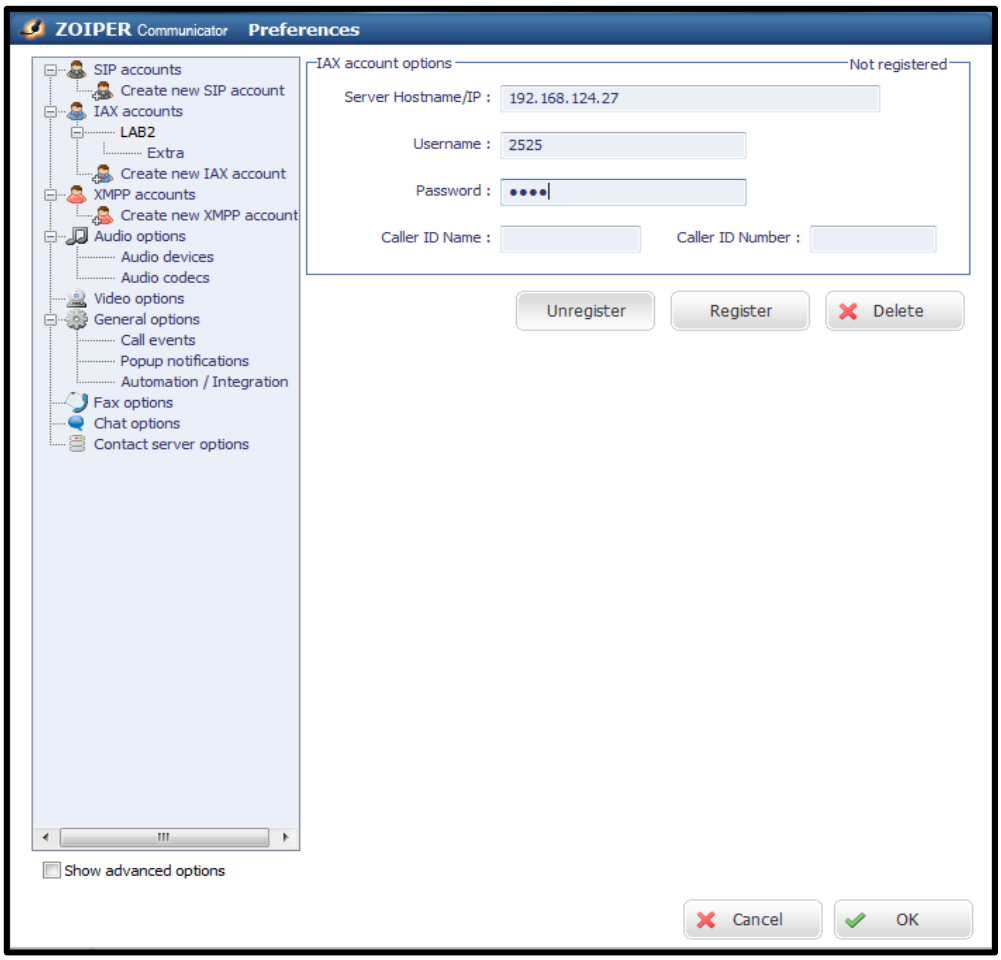


Figura 31. Configuración Hostname

Fuente: Investigador

Se procedió a configurar las IPs del Servidor Elastix con la red de la facultad (192.168.124…), para posteriormente comunicarnos entre softphone con diferentes máquinas de la facultad.

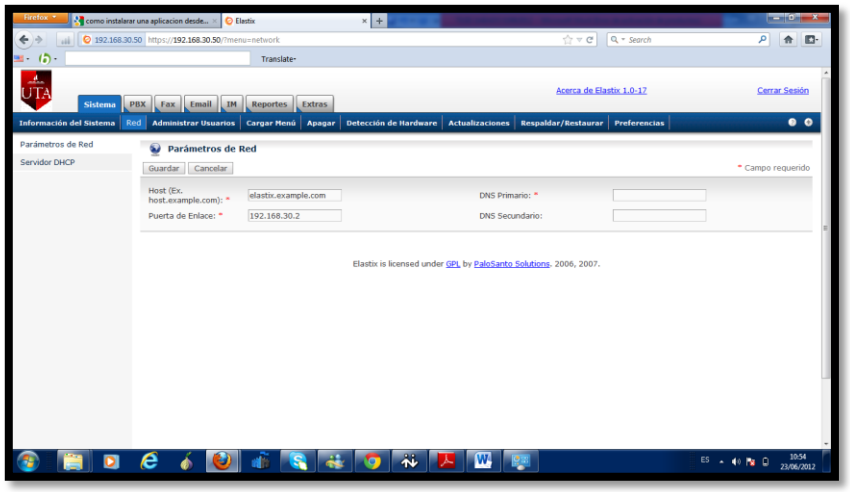


Figura 32. Configuración IPs Servidor Elastix

Fuente: Investigador

Para cambiar la dirección IP se puede realizar por:

- Un browser ingresando a la pestaña Sistema-Red.
- Consola en el servidor Elastix digitando Setup.

RESPALDO DEL SERVIDOR ELASTIX.

Antes de empezar con la implementación de la VPN se sacó una copia de respaldo de nuestro servidor Elastix con la finalidad de salvaguardar la configuración actual.

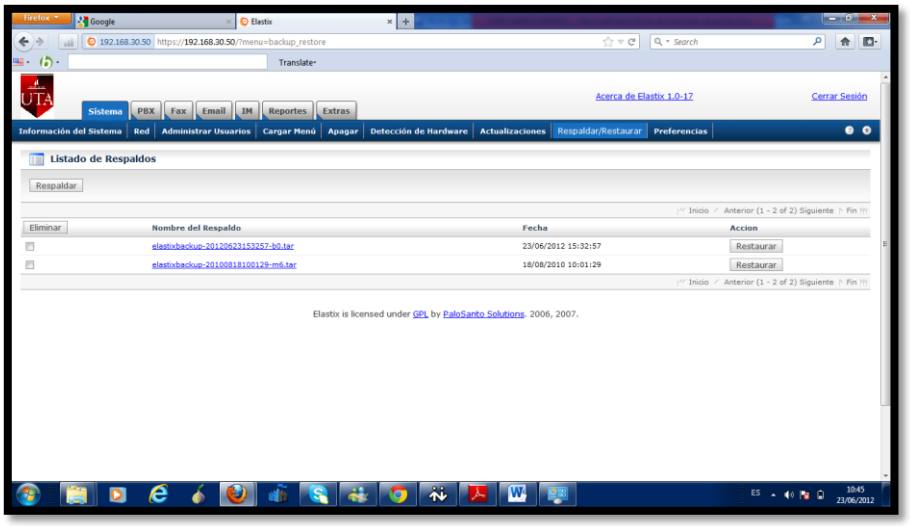


Figura 33. Respaldo del Servidor Elastix

Fuente: Investigador

Para el presente proyecto se usó un softphone para las diferentes comunicaciones.

Se configuró dos tipos de extensiones llamadas LAB1 Y LAB2 para realizar las pruebas con dos softphone de marcas ZOIPER Y XLITE instalados en dos máquinas diferentes.

6.6.15 Configuración de VPN en el Servidor Elastix

Para empezar con la configuración es necesario que en nuestro servidor estén instalados todos los requerimientos necesarios con la finalidad de no tener inconvenientes con el proceso de instalación de programas para la VPN.

Es necesario instalar el paquete **rpmforge** que permitirá agregar repositorios extras a los que por defecto viene en Centos. Esto sirve para instalar programas vía Yum, que no están en los repositorios originales /etc/yum.repos.d/CentOS-Base.repo.

Descargar e instalar rpmforge-release-0.3.6-1.el5.rf.i386.rpm

[root@elastix] # wget http://205.196.122.127/8k9q2ovygnbg/1gymwfdd23m/rpmforge-release-0.3.6-1.el5.rf.i386.rpm

[root@elastix] # rpm –ivh rpmforge-release-0.3.6-1.el5.rf.i386.rpm.

Instalación programa OpenVPN para el servidor Elastix.

Para la instalación del paquete se puede realizar directamente descargándonos desde el internet desde la url http://acelnmp.googlecode.com/files/openvpn-as-1.8.4-CentOS5.i386.rpm o descargándolo a nuestro computador para luego copiar en un flash memory e instalar en el servidor.

- Para instalar directamente desde el internet:

[root@elastix] # wget http://acelnmp.googlecode.com/files/openvpn-as-1.8.4-CentOS5.i386.rpm

- Para esta ocasión se instaló usando un flash memory:

Monte el flash memory que contiene el paquete openvpn con extensión .rpm

[root@elastix] # mount /dev/sda1 /mnt/usb

[root@elastix usb] # rpm –ivh openvpn-as-1.8.4-CentOS5.i386.rpm

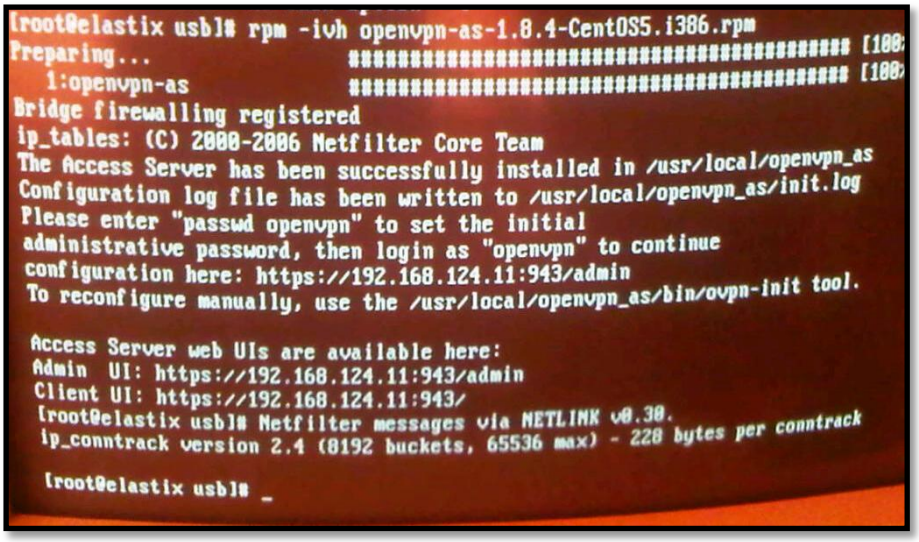


Figura 34. Instalación Open VPN

Para iniciar con la configuración en el servidor Elastix se podía realizar mediante la consola del servidor y en esta ocasión se optó por administrar de forma gráfica para ello se usó la herramienta Webmin.

[root@elastix] # rpm -ivh webmin-1.470-1.noarch.rpm

Una vez instalado se ingresó a un navegador de internet y se coló la IP en el siguiente formato:

192.168.124,11:10000

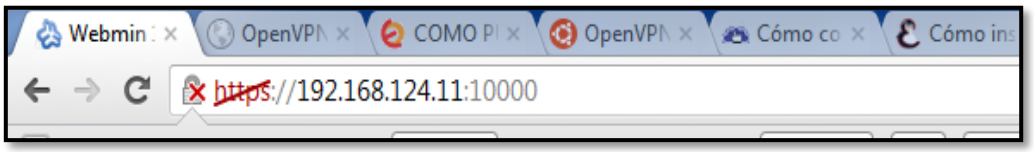


Figura 35. Acceso a Webmin

Surgió una pantalla en el navegador en el cual se ingresó el password y la contraseña del servidor Elastix.

En la opción **Módulos** de Webmin se instaló el módulo openvpn para Webmin, para ello se debe marcar la opción de "Desde dirección URL ftp o http" y en la casilla

colocar la dirección web http://my-file-vps.googlecode.com/files/openvpn-2.0.wbm.gz, que es de donde se obtuvo el instalador de OpenVPN para Webmin.

6.6.16 Configuración del Servidor OpenVPN

Desde el root, crear el fichero **/etc/yum.repos.d/AL-Server.repo**:

[root@elastix] # vi /etc/yum.repos.d/AL-Server.repo,

Ingresar el siguiente contenido:

[AL-Server]
name=AL Server para Enterprise Linux $releasever
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgcheck=1
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY

Importar la firma digital de Alcance Libre ejecutando lo siguiente desde el root:

[root@elastix] #rpm --import

Se instalan los depósitos yum, los paquetes RPM de OpenVPN, Shorewall y vim-enhanced.

[root@elastix] #yum -y install openvpnshorewall vim-enhanced

Dentro del directorio

[root@elastix] # /etc/openvpn/se

copiar los ficheros openssl.cnf, whichopensslcnf, pkitool y vars, localizados en /etc/openvpn/easy-rsa/2.0/:

cp /usr/share/openvpn/easy-rsa/2.0/openssl.cnf ./
cp /usr/share/openvpn/easy-rsa/2.0/whichopensslcnf ./
cp /usr/share/openvpn/easy-rsa/2.0/pkitool ./
cp /usr/share/openvpn/easy-rsa/2.0/vars ./

Editar las últimas líneas del fichero /etc/openvpn/vars, que corresponden a lo siguiente:

export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL=me@myhost.mydomain

Reemplazar por:

export KEY_COUNTRY="ECU"
export KEY_PROVINCE="Tung"
export KEY_CITY="Ambato"
export KEY_ORG="FISEI"
export KEY_EMAIL=svcasicana@hotmail.com

Datos que corresponden a la ubicación del servidor VPN y el departamento de la institución.

Para que se carguen las variables de entorno configuradas, se ejecutó la siguiente línea de comando:

[root@elastix] # source /etc/openvpn/./vars

Ejecutar el fichero /usr/share/openvpn/easy-rsa/2.0/clean-all con sh.

[root@elastix] # sh /usr/share/openvpn/easy-rsa/2.0/clean-all

Crear el certificado del servidor:

[root@elastix] # sh /usr/share/openvpn/easy-rsa/2.0/build-ca

Crear el fichero dh1024.pem, el cual contiene los parámetros del protocolo **D**iffie-**H**ellman, de 1024 bits:

[root@elastix] # sh /usr/share/openvpn/easy-rsa/2.0/build-dh

El protocolo **D**iffie-**H**ellman permite el intercambio secreto de claves entre dos partes, que en nuestro estudio corresponden a cada uno de los usuarios de la PBX y el servidor Elastix. Este protocolo es usado para el cifrado de una sesión.

Generar la firma digital con la siguiente línea de comando:

[root@elastix] # sh/usr/share/openvpn/easy-rsa/2.0/build-key-serverserver

Crear los certificados para ambos usuarios de la PBX (para los usuarios 192.168.11.12 y 192.168.11.13. Con líneas de comando:

[root@elastix] # sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente1
[root@elastix] # sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente2

Usar los certificados creados y las configuraciones realizadas, en el fichero:

vi /etc/openvpn/servidorvpn-udp-1194.conf, editándolo con lo siguiente:

[root@elastix] # vi /etc/openvpn/servidorvpn-udp-1194.conf

port 1194
protoudp
dev tun
#---- Sección de llaves -----
cakeys/ca.crt
certkeys/server.crt
keykeys/server.key
dhkeys/dh1024.pem
#----------------------------
server 192.168.11.24 255.255.255.0

ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status-servidorvpn-udp-1194.log
verb 3

Ingresar la IP 192.168.11.24, porque es recomendable usar una red privada para evitar conflictos entre los host del Sistema VoIP cuando el túnel se encuentre activo. Con mascara 255.255.255.0 porque permitirá a 253 clientes conectarse a la VPN.

Usar el mandato restorecon sobre el directorio /etc/openvpn a fin de asignar los contextos adecuados.

[root@elastix] # restorecon -R /etc/openvpn/

Crear los ficheros ipp.txt y openvpn-status-servidorvpn-udp-1194.log:

[root@elastix] # cd /etc/openvpn/
[root@elastix] # touch ipp.txt
[root@elastix] # touch openvpn-status-servidorvpn-udp-1194.log

Aplicar contextos de lectura y escritura (openvpn_etc_rw_t) a los ficheros que contiene el directorio /etc/openvpn:

[root@elastix] # cd /etc/openvpn/
[root@elastix] # chcon -u system_u -r object_r -t openvpn_etc_rw_t ipp.txt
[root@elastix] # chcon -u system_u -r object_r -t openvpn_etc_rw_t openvpn-status-servidorvpn-udp-1194.log

Iniciar el servicio openvpn:

[root@elastix] # serviceopenvpnStart

Para que el servicio de OpenVPN esté activo en el siguiente inicio del sistema, usar el mandato chkconfig de la siguiente forma:

[root@elastix] # chkconfigopenvpnon

6.7 METODOLOGÍA

La solución al problema determinado en el sistema de VoIP Elastix en la FISEI se obtuvo mediante previas investigaciones y entrevistas realizadas al administrador del sistema con la finalidad de elegir la mejor solución al problema.

Para ello se escaneó la red con el objetivo de determinar los dispositivos y extensiones con las que cuenta la PBX.

Se trabajó con herramientas de escaneo instaladas en la máquina del atacante con la finalidad de indicar la importancia que tiene implementar seguridades en el sistema de VoIP.

Finalmente se aplicó el método de encriptación VPN como solución para prevenir los ataques eavesdropping en la red de comunicaciones VoIP.

CAPITULO VII

7 CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones

- ✓ Se concluye que los ataques eavesdropping permiten acceder a información confidencial de los usuarios de la Red VoIP.
- ✓ Se ha detectado que, en la versión del servidor actual del Sistema Elastix 1.0-17 existen vulnerabilidades en cuanto a actualizaciones y requisitos necesarios para la configuración de la VPN.
- ✓ Para el uso de OpenVPN fue necesarios contar con conocimientos básicos de comandos para software libre.
- ✓ Se determinó que el uso de OpenVPN es una aplicación libre y abierta para configurar, lo que no sucede con otras aplicaciones como LogMeIn, Cisco en las cuales no se puede ejercer el control total de la VPN si no se cumple especificaciones de adquisición para cada una.
- ✓ Se concluye que la Red de comunicaciones VoIP esta propensa a diversos ataques informáticos como por ejemplo la intercepción de paquetes, concluyendo así que la red es insegura.

7.2 Recomendaciones

- ✓ Se recomienda aplicar medidas preventivas de seguridad de la información para evitar ataques eavesdropping en la Red VoIP.
- ✓ Se recomienda la actualización del servidor Elastix a una versión que sea compatible con la configuración de la VPN.
- ✓ Se recomienda llevar actualizaciones continuas del Sistema Elastix con el objetivo de contar con mayor protección en la configuración de la VPN.
- ✓ Se recomienda seguir usando aplicaciones de software libre e impulsar su uso en toda la facultad.
- ✓ El uso de herramientas con software libre beneficiará al financiamiento del proyecto al no tener que adquirir licencias de programas en cuantiosas cantidades.
- ✓ Se recomienda la implementación de una Red Privada Virtual con software libre como medida de seguridad a los ataques eavesdropping.

GLOSARIO DE TERMINOS

ARP spoofing.- Es una técnica usada para infiltrarse en una red ethernet conmutada (basada en switches y no en hubs), que puede permitir al atacante leer paquetes de datos en la LAN (red de área local), modificar el tráfico, o incluso detenerlo.

Botnets.- Redes de ordenadores infectados controlados por usuarios remotos.

Eavesdropping. - Escuchar secretamente

Exploits.- Es una pieza de software, o una secuencia de comandos con el fin de causar un error o un fallo en alguna aplicación, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado).

Fuzzing.- Un término empleado para referirse a las técnicas de software automatizadas, capaces de generar y enviar datos secuenciales o aleatorios a una o varias áreas o puntos de una aplicación, con el objeto de detectar defectos o vulnerabilidades existentes en el software auditado.

Gatekeepers.- Es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs.

Gateways H.323 (GW).- Es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada.

IDS.- Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red.

INVITE.- Permite invitar un usuario o servicio para participar en una sesión o para modificar parámetros en una sesión ya existente.

Man-in-the-middle.- Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

PBX.- Central telefónica conectada directamente a la red pública de telefonía.

Protocolo IP.- Un protocolo usado para la comunicación de datos a través de una red.

Phishing.- Adquisición fraudulenta de información personal confidencial.

RTP.- Es la abreviación de Real-time Transport Protocol, por su denominación en inglés. Es un estándar creado por la IETF para la transmisión confiable de voz y video a través de Internet.

SPIT.- Es la denominación de un nuevo tipo de publicidad en línea similar al spam, que probablemente se propagará a la par con el desarrollo de la telefonía IP.

Spam.- Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido

Streams.- Es la distribución de multimedia a través de una red de computadoras de manera que el usuario consume el producto al mismo tiempo que se descarga

Tráfico Broadcast.- Se genera cuando un dispositivo de la red envía paquetes a todos los dispositivos de la red.

Topologías.- La topología de red se define como una familia de comunicación usada por los computadores que conforman una red para intercambiar datos.

Terminales H3.23.- Es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU)

UDP.- Son las siglas de Protocolo de Datagrama de Usuario (en inglés User Datagram Protocol) un protocolo sin conexión que, como TCP, funciona en redes IP.

Vulnerabilidades.- Las vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad, en un sistema comprometido.

VoIP.- Voz sobre Protocolo de Internet

BIBLIOGRAFÍA:

Bytecoders. (07 de 05 de 2011). Obtenido de http://bytecoders.net/content/ataques-voip.html

Norton by Symantec. Las vulnerabilidades de VoIP. (09 de 06 de 2011). Recuperado el 20 de 11 de 2011, de http://es.norton.com/voip-security-a-primer/article

http-peru :: Arquitecturas Conexión VPN. (2012). Obtenido de http://www.http-peru.com/arquitectura_conexion_vpn.php

Actual, P. (07 de 08 de 2008). *Syncrom*. Recuperado el 05 de 11 de 2011

Alvarez, F. A. (s.f.). Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/2977/1/5494.pdf

Anónimo. (s.f.). *Seguridad de la información*. Obtenido de http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Arronategui, U. (2009). *SEGU - INFO*.

ASTUDILLO, I. G. (19 de 03 de 2011). *TecnoIP 3*. Obtenido de http://www.slideshare.net/gastudillob/tecnoip-3

Augusto Sepúlveda. (22 de 10 de 2009). *Blog Oficial de Elastix.* Obtenido de http://blogs.elastix.org/es/2009/10/22/recomendaciones-de-seguridad-en-elastix/

Cabrera, C. (09 de Marzo de 2011). *Asterisk México*. Obtenido de Cursos, asesoría y ayuda sobre Asterisk: http://asteriskmx.com/2011/03/estadisticas-de-inseguridad-en-elastix/

Castillo, M. P. (2011). *Monografías*. Obtenido de http://www.monografias.com/trabajos15/virus-informatico/virus-informatico.shtml

Cevallos Calderón, V. F. (2011). *Detección de intrusiones en una red de comunicaciones en la capa 7 utilizando el L 7- FILTER* . SANGOLQUI.

Chavarría, P. G. (Lunes 17:31:00 de Junio de 2011). *ESPOL*. Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/2564/1/5040.pdf

Computing, S. (s.f.). *Sisistema Informaticos mas inteligentes*. (Una nueva era de IT) Recuperado el 27 de 10 de 2011, de http://www-

03.ibm.com/systems/ec/smartercomputing/?ca=smartercomputing&me=html&met=exli&re=smartercomputing

Cosme, M. U. (04 de Agosto de 2009). *Métodos de seguridad en la información*. Obtenido de http://urielruizc.wordpress.com/2009/08/04/metodos-de-seguridad-en-la-informacion/

CRYPTEX. (17 de Enero de 2008). *Blog dedicado al estudio de la Seguridad de la Información - Privacidad - Seguridad Informatica - Auditoria informática.* Obtenido de http://seguridad-informacion.blogspot.com/2008/01/top-5-de-vulnerabilidades-voip-en-2007.html

Edgardo Martín Barrios. (s.f.). *Monografias.com*. (Tecnico Universitario en Informatica Aplicada. Egresado de la Facultad de Ingenieria – Universidad Nacional del Nordeste Chaco – Argentina.) Recuperado el 05 de 11 de 2011, de http://www.monografias.com/trabajos14/comunicacion/comunicacion.shtml

El rincon del vago Medios físicos de transmisión de datos. (s.f.). Recuperado el 06 de 11 de 2011, de http://html.rincondelvago.com/medios-fisicos-de-transmision-de-datos.html

Elastix, E. T.-I. (29 de Junio de 2011). *Elastix Información, Tutoriales, Noticias Guias Tecnicas, etc.* Recuperado el 05 de 10 de 2011, de Consideraciones de seguridad en Elastix: http://www.caponline.webatu.com/elastixtech/consideraciones-de-seguridad-en-elastix/

Eric arrestad, V. d. (20 de Octubre de 2011). *WinRed.com*. Obtenido de Principales amenazas para la seguridad VoIP : http://winred.com/innovacion/principales-amenazas-para-la-seguridad-voip/gmx-niv59-con13776.htm

Estrella, P. (23 de Agosto de 2011). *Acerca de la supuesta vulnerabilidad reportada por FreePBX*. Obtenido de http://lists.elastix.org/pipermail/general-es/2011-August/011693.html

Farrasaranjueztk. (2011). *Tecnologia VPN.*

Gaibor, J. V. (s.f.). Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/14637/1/TESIS_GAIBOR_VANESSA_CAICEDO_PABLO.pdf

Galo Rafael Iturralde Orellana ESPOL. (2006). Recuperado el 04 de 11 de 2011, de www.dspace.espol.edu.ec/bitstream/123456789/3001/1/5518.pdf

Gil, R. G. (s.f.).

GONZALEZ, J. (21 de 11 de 2011). *SEGURIDAD PARA TODOS.* Obtenido de http://www.seguridadparatodos.es/2011/11/seguridad-voip-amenazas.html

GUAGALANGO, R. (Agosto 2011). *Evaluación técnica de la seguridad informática del Data Center de la Escuela Politécnica del Ejército.* SANGOLQUÍ - Ecuador.

GuatchWuard. (19 de 10 de 2011). (Principales amenazas para la seguridad VOIP) Obtenido de http://winred.com/innovacion/principales-amenazas-para-la-seguridad-voip/gmx-niv59-con13776.htm

HARO DÌAZ. (2011). *Tipos de amenazas y ataques en seguridad informática.*

IN., F. W. (s.f.). *Nessus*. Obtenido de http://es.wikipedia.org/wiki/Nessus

international, S. F. (s.f.). *Seguridad de la información*. Obtenido de http://imaginar.org/iicd/index_archivos/TUS5/introduccion.pdf

INTERNET. (2012). Obtenido de http://www.ie.uia.mx/tit/ot03/proy14/vpnprin.htm

Marin, FA Alvarez. (2006). Recuperado el 05 de 11 de 2011, de www.dspace.espol.edu.ec/bitstream/123456789/4990/2/7922.doc

MEGAZINE. (2012). *Las preocupaciones de seguridad de VoIP.* Obtenido de http://megazine.co/las-preocupaciones-de-seguridad-de-voip_9e7b.html

Molina, I. M. (s.f.). *REDES PRIVADAS VIRTUALES (VPN).*

Olsen, H. A. (29 de mayo de 2009). *Las Noticias de la Quinta Region.* Obtenido de http://www.login.cl/cms/opinion/cartas-al-director/272-usurpacion-de-identidad-en-notarias

Pamela Isabel Gonzales. (s.f.). *Metodos de Encriptación Para Redes Privadas Virtuales.* Recuperado el 11 de 2011, de http://es.scribd.com/doc/60915413/Cifrado-VPN

Raboy, M. (23 de Enero de 2006). *Medios de comunicación*. Obtenido de http://vecam.org/article683.html

RK2. (03 de 11 de 2010). *COLOFONDRIOS*. Obtenido de http://colofondrios.blogspot.com/2010/03/los-3-mejores-programas-para-montar-una.html

ROMERO, M. (2005). *Definición de un plan de seguridad informática para la empresa PROMIX ECUADOR C.A(Tesis).* SANGOLQUÍ - ECUADOR.

RUIZ, G. M. (2010). *Estudio e implementacion de mecanismos de seguiridad WPA2 para un sistema de distribucion.....* Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/641/1/38T00258.pdf

S.R.L, F. S. (04 de 11 de 2011). Obtenido de Inseguridad en Elastix: estadísticas actualizadas: http://www.fenixsolutions.com.ar/telefonia/asterisk/inseguridad-en-elastix-estadisticas-actualizadas/

Sagarminaga, P. G. (2011). *informática en general* (http://blog.txipinet.com/2006/10/11/40-seguridad-en-voip-iii-captura-de-conversaciones-o-eavesdropping/ ed.).

Salas, R. N. (15 de 10 de 2011). *INVESTIGACIONES.* Obtenido de http://repo.uta.edu.ec/bitstream/handle/123456789/79/t601e.pdf?sequence=1

SEGU-INFO. (27 de 10 de 2011). *Seguridad de la Información*. Recuperado el 27 de 11 de 2011, de http://www.segu-info.com.ar/ataques/ataques.htm

Ugalde, G. N. (12 de Noviembre de 2010). *Tipos de Intrusos Informáticos*. Obtenido de http://gnu2801.blogspot.com/2010/11/tipos-de-intrusos-informaticos.html

VILLALON, J. L. (14 de MARZO de 2011). *SECURITY AT WORK*. Obtenido de http://www.securityartwork.es/2008/03/14/eavesdropping-en-voip/

VoIP:, R. G. (s.f.). *Ataques, Amenazas y Riesgos.* (Vniversidad de Valencia) Obtenido de http://www.portantier.com/downloads/seguridad_voip.pdf

Wikipedia. (2011). *Antimalware*. Obtenido de http://es.wikipedia.org/wiki/Malware.

WIKIPEDIA, F. (09 de 01 de 2013). *WIKIPEDIA*. Obtenido de http://es.wikipedia.org/wiki/Asterisk

WIKIPEDIA, F. (s.f.). *Investigación cuantitativa.* Obtenido de http://es.wikipedia.org/wiki/Investigaci%C3%B3n_cuantitativa

WIKIPEDIA1. (s.f.). *Investigación cualitativa.* Obtenido de http://es.wikipedia.org/wiki/Investigaci%C3%B3n_cualitativa

World, I. C. (s.f.). Obtenido de http://www.interpol.int/es/Criminalidad/Delincuencia-inform%C3%A1tica/Ciberdelincuencia

ANEXOS

Anexo1.

UTA

FACULTAD DE INGENIERIA EN SISTEMAS ELECTRONICA E INDUSTRIAL

AMBATO

ENCUESTA

DIRIGIDO A:

Personal Administrativo y Administradores de Redes y Sistemas**.**

OBJETIVO

Señores, su veracidad en las respuestas permitirá al investigador desarrollar de forma real y efectiva la realización del proyecto.

Agradezco su colaboración.

INSTITUCION:

Facultad de Ingeniería en Sistemas Electrónica e Industrial

INSTRUCCIONES:

Marque con una (X) en la respuesta que usted crea conveniente.

Pregunta 1. ¿Cuáles son las formas de comunicación que se usa actualmente en la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la UTA.?

a. El teléfono ( )
b. Los libros ( )
c. Correo electrónico ( )
d. Redes Sociales ( )
e. Teléfonos Móviles ( )

Pregunta 2. ¿Considera Usted que la comunicación que viaja mediante los medios de comunicación está fuera del alcance de delitos informáticos?

a. Si ( )
b. No ( )

Pregunta 3. Que información comparte mediante los diferentes medios de comunicación

a. Información trabajo ( )
b. Información privada ( )
c. Anuncios publicitarios ( )
d. Entretenimiento ( )
e. Para hacer negocios ( )

Pregunta 4. ¿Mediante qué medio de comunicación transmite la información?
a. Teléfono ( )
b. Celular ( )
b. Redes sociales ( )
b. Telefonía IP ( )
b. Correo electrónico ( )

Pregunta 5. ¿Cómo califica al servicio contratado para la transmisión de información telefónica?

a. Muy Buena ( )
b. Buena ( )
c. Regular ( )
d. Mala ( )

Pregunta 6. ¿Qué tipo de tráfico se transmite actualmente a través de la tecnología utilizada?

a. Datos ( )
b. Voz ( )
c. Video ( )

Pregunta 7. ¿Considera Usted que la red utilizada actualmente por la institución, es menos costosa en relación a otras tecnologías de transmisión de información?

a. Si ( )
b. No ( )

Pregunta 8. ¿Cree usted que es importante implementar procedimientos para evitar que delincuentes informáticos accedan a información confidencial? Por qué?

a. Si ( ), ……
b. No ( ) ……

Pregunta 9. ¿Conoce usted sobre la Red Privada Virtual?

a. Si ( )
b. No ( )

Pregunta 10. ¿Cree usted que es importante implementar una Red Privada Virtual como medida de seguridad para evitar ataques informáticos hacia la transmisión de datos y voz?

a. Si ( ),
b. No ( ),

Pregunta 11. ¿Cuáles cree que serían las razones para implementar una nueva alternativa tecnológica para la transmisión de información de voz, datos y video?

a. Económicas ( )
b. Seguridad ( )
c. Calidad ( )

GRACIAS POR SU COLABORACION