UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE ESTUDIOS DE POSGRADO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN REDES Y TELECOMUNICACIONES

TEMA:

"Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo"

TESIS DE GRADO

Previo a la obtención del Título de:

MAGÍSTER EN REDES Y TELECOMUNICACIONES.

AUTOR

Carlos Diego Gordón Gallegos

DIRECTOR

Ing. M.Sc. David Guevara

AMBATO - ECUADOR

2010

Al Consejo de Posgrado de la UTA

El comité de defensa de la Tesis de Grado **"Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo"**. Presentado por Carlos diego Gordón Gallegos y conformada por: Los Señores miembros del Tribunal de Defensa; Director de Tesis Ing. M.Sc. David Guevara y presidido por Ing. M.Sc. Oswaldo Paredes, Presidente de POSGRADO FISEI; Ing. M.Sc. Luis Velásquez Medina Director del CEPOS-UTA, una vez escuchada la defensa oral y revisada la tesis escrita en la cual se ha constatado el cumplimiento de las observaciones realizadas por el mismo, remite la presente tesis para su uso y custodia en las bibliotecas de la UTA.

Ing. M.Sc. Oswaldo Paredes.
Presidente de POSGRADO FISEI.

Ing. M.Sc. Luis Velásquez Medina.
Director del CEPOS-UTA

Ing. M.Sc. Vicente Morales.
Director Académico Administrativo

Ing. M.Sc. David Guevara.
Director de la Tesis

Ing. M.Sc. Vicente Morales.
Miembro del Tribunal

Ing. M.Sc. Teresa Freire.
Miembro del Tribunal

Ing. M.Sc. Jaime Ruíz.
Miembro del Tribunal

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación, nombrado por el H. Consejo Superior de Postgrado de la Universidad Técnica de Ambato:

CERTIFICO:

Que el trabajo de investigación: **"Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo"** presentado por el maestrante. Carlos Diego Gordón Gallegos, estudiante del programa de Maestría en Redes y Telecomunicaciones II Edición, reúne los requisitos y meritos suficientes para ser sometido a la evaluación del jurado examinador que el H. Consejo de Postgrado designe.

Ambato, Julio 2010

_____

Ing. M.Sc. David Guevara

DIRECTOR DE LA TESIS

AUTORÍA DE LA INVESTIGACIÓN

La información contenida y los criterios emitidos en el presente trabajo investigativo: “Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo”, junto con las ideas, análisis, conclusiones y propuesta, son de responsabilidad exclusiva de mi persona, como autor de esta tesis.

Ambato, julio 2010

Carlos Diego Gordón Gallegos	Ing. M.Sc. David Guevara
AUTOR	**DIRECTOR**

DEDICATORIA

El presente trabajo investigativo va dedicado para todos los maestros que de una u otra forma realizan la actividad de Diseño de Redes, lo utilicen, y consigan resultados muy beneficiosos, así como también a la juventud estudiosa para que desarrollen sus estrategias de diseño y se formen como excelentes profesionales al servicio del país.

AGRADECIMIENTO

A mis padres que siempre me han apoyado y nunca han desconfiado en mis capacidades. Quienes me han acompañado en mis triunfos y derrotas. Y en especial a Myriam la razón de mi existencia y mi gran amor.

A la Universidad Técnica de Ambato por su apertura para formar profesionales de cuarto nivel con gran categoría.

A mi tutor Ing. MSc. David Guevara, por su apoyo y guía continua para la realización del presente trabajo.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE GRÁFICAS

RESUMEN EJECUTIVO

UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE ESTUDIOS DE POSGRADO

MAESTRÍA EN REDES Y TELECOMUNICACIONES VERSIÓN II

"Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo"

Autor: Carlos Diego Gordón Gallegos
Tutor: Ing. MSc. David Guevara

Resumen

La tecnología va evolucionando progresivamente de acuerdo a las exigencias de la sociedad y requiere de una adecuación continua a dichos requerimientos. Cada

día aparecen nuevas propuestas para mejorar el servicio de las empresas, por lo que son considerados primordiales los cambios que ocurren por mejorar la vida de los seres humanos.

Brindar mejor servicio a los clientes es el objetivo primordial del Ilustre Municipio de Pelileo, para lo cual debe realizar su proceso de trabajo con la mayor eficiencia y los mejores elementos.

Se considera que la comunicación entre las Sucursales del Municipio de Pelileo es el elemento fundamental y por ello se requiere aportar para que la comunicación tenga una seguridad muy efectiva y ese es el objetivo primordial de nuestra investigación.

El trabajo está estructurado en siete capítulos:

El capítulo I detalla el análisis del Contexto, determinando las causas y consecuencias así como también la delimitación del problema en estudio.

En el capítulo II, se describe el Marco Teórico que se constituye en el principal elemento de nuestra investigación en donde se describen todos los conceptos de nuestro estudio.

El capítulo III, nos da a conocer la Metodología, que se ha empleado para la realización del presente trabajo de investigación, que explica el procedimiento que se siguió para la recolección y procesamiento de la información.

En el capítulo IV, se explica específicamente el Análisis e Interpretación de Resultados, es decir, el procesamiento que se realizó con los datos utilizando la metodología que se describió en el capítulo anterior.

El capítulo V, describe las Conclusiones a las que se llegaron luego de realizarse el proceso minucioso de investigación, así como también se indica las Recomendaciones pertinentes de esta tesis.

En el capítulo VI, describe íntegramente la Propuesta de nuestro trabajo investigativo en el cual se plantea una solución para tratar de resolver la problemática que ha sido motivo de nuestra tesis.

INTRODUCCIÓN

El término seguridad proviene del latín securitas que se refiere a la ausencia de riesgo o también a la confianza en algo o alguien. La seguridad es un estado de ánimo, una sensación, una cualidad intangible. Se puede entender como un objetivo y un fin que el hombre anhela constantemente como una necesidad primaria.

Cuando una entidad realiza sus actividades de forma segura todos sus servicios son eficientes y brinda satisfacción a sus clientes. Ante esta realidad se considera como objetivo primordial mejorar la seguridad de la comunicación de las Sucursales del Municipio de Pelileo pero considerando mejorarlo en varios aspectos, así tenemos:

Reducir los costos económicos y brindar un servicio de seguridad muy confiable es la prioridad de la presente investigación, por ello se considera la necesidad de

la utilización de software libre que no requiere de recursos económicos para su implementación.

El sistema operativo utilizado para el proyecto de investigación es IPCop que es un firewall muy efectivo y con la combinación de Zerina permite implementar un túnel virtual muy confiable y seguro para la comunicación de las sucursales del Ilustre Municipio de Pelileo.

Finalmente es necesario indicar que a más de crear el túnel virtual se realizaron pruebas de Hackeo para verificar el grado de confiabilidad de nuestra propuesta. Las pruebas realizadas se relacionan a la identificación de puertos abiertos para realizar ataques, Password Sniffing o rastreo de claves, ARP poisoning o envenenamiento ARP y Denied of Service o denegación de servicio, las cuales luego de ser ejecutadas nos proporcionaron resultados muy halagadores y permitieron determinar que el túnel virtual sí provee una seguridad muy confiable en la comunicación de las sucursales del Ilustre Municipio de Pelileo.

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema de Investigación

Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo (IMP).

1.2 Planteamiento del Problema

1.2.1 Contextualización

Macro

Actualmente, todas las entidades relacionadas con la temática de redes alrededor del mundo saben que deben alcanzar un buen nivel de calidad en su servicio lo que constituye el eje fundamental para cumplir con su misión y visión.

Meso

De este modo en el Ecuador se considera que, proveer a los usuarios de una Red de datos eficiente y segura a través del internet es de gran importancia ya que deben cumplir con estándares internacionales y estar al nivel de otras entidades similares a nivel internacional.

Micro

En el cantón Pelileo existen entidades en distintas áreas como Colegios y varias Empresas Públicas y Privadas, que no consideran la importancia de proveer de una red de datos eficiente y segura que sea el factor fundamental para brindar un

servicio de alta calidad a los usuarios y alcanzando de esta forma el nivel de competitividad con otras ciudades del País y del mundo.

El Ilustre Municipio del cantón Pelileo, con el afán de realizar un mejoramiento en el servicio de red de Datos para todos los usuarios de la Red, requiere llevar a cabo un estudio de nuevas alternativas para disponer de una red de datos eficiente y sobre todo segura ante los distintos ataques de intrusos y al flujo de información maliciosa.

En consecuencia no se ha tomado en consideración esta problemática y se ha conservado políticas de seguridad que resultan insuficientes ante los distintos ataques de intrusos, virus informáticos y flujo de información maliciosa, lo cual ha afectado enormemente al tipo de servicio que brinda la Red de Datos del Ilustre Municipio del cantón Pelileo. Por lo tanto es necesario reducir el impacto de este problema llevando a cabo los correctivos necesarios.

1.2.2 Análisis Crítico

La comunicación mediante una red, es fundamental en cualquier entidad y en especial en un lugar donde se transmite información muy relevante y confidencial en la red de datos como lo es en el Municipio del cantón Pelileo, por lo que se requiere de un estudio que permita obtener mejores rendimientos de servicio que brinde todas las seguridades ante el ataque de virus y diversos códigos maliciosos manejados por Sniffing y Spoofing cuando se comunica a través del Internet.

Una de nuestras principales armas para enfrentarnos ante esta problemática es la tecnología que en la actualidad está muy avanzada con relación a la seguridad de redes y hará posible brindar mejor servicio en la red de datos del Ilustre Municipio del cantón Pelileo.

Por otra parte es importante manifestar que para generar cambios en la realidad se necesita saber manejar los medios que se disponen y darle el mejor uso, para lo cual se comenzará analizando la red de datos del Ilustre Municipio del cantón Pelileo, que es algo real y que a la vez se puede adecuar para nuestras expectativas.

1.2.3 Prognosis

A medida que la ciencia va evolucionando aceleradamente, es necesario que las instituciones desarrollen estrategias que brinden un servicio y seguridad a los usuarios de calidad, además que estén acorde al avance tecnológico. Caso contrario, si no se emplea innovación en un servicio seguro, en un futuro no muy lejano, no se podrá consolidar el cambio que se busca en el servicio a los empleados y clientes de las dos sucursales del Ilustre Municipio del cantón Pelileo y se continuará con la misma forma de pensar tradicionalista y sin noción de los problemas que enfrentan los usuarios ante una red muy lenta e insegura y expuesta libremente al ataque de intrusos en el internet.

1.2.4 Formulación del problema

¿De qué manera, una red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre, incide en la seguridad del enlace de las sucursales del Ilustre Municipio de Pelileo?

1.2.4 Preguntas Directrices

Las preguntas directrices que conducirán el presente trabajo de investigación son las siguientes:

- ¿Cuáles son las características de la infraestructura de la red de datos con la que cuenta el Ilustre Municipio del cantón Pelileo?
- ¿Cuál es el estado de la seguridad de datos en el IM Pelileo una herramienta adecuada para comunicar las dos sucursales mediante internet utilizando protección a nivel de protocolos de capa dos del modelo TCP/IP?
- ¿Es factible proponer una infraestructura de red que brinde seguridad en la comunicación de la red de datos entre las dos sucursales del Ilustre Municipio del cantón Pelileo?

1.2.5 Delimitación

El presente trabajo investigativo se llevará a cabo en el Ilustre Municipio del cantón Pelileo en el periodo Diciembre 2009 – Julio 2010 y está destinada a utilizar la infraestructura de red existente implementada con software libre, además está dirigido para los empleados y usuarios del Municipio de Pelileo.

1.3 Justificación

La aplicación de la nueva tecnología permite resolver varios problemas y con una gran ventaja en el aspecto de servicio que ofrece una red de datos, de este modo los empleados del Municipio de Pelileo experimentan un servicio en la red, que brinda máxima seguridad en la comunicación por internet utilizando software libre.

La transferencia de información en una entidad pública requiere ser ágil, eficiente, no debe demandar gastos económicos adicionales y debe ser muy segura, es por ello, la necesidad de un sistema que brinde seguridad garantizada con un excelente servicio a todas las personas relacionadas con el Ilustre Municipio de Pelileo.

El grupo beneficiario lo conforman los empleados, administrativos y clientes que de alguna u otra manera están vinculados con del Ilustre Municipio de Pelileo. Cuando se fusionan eficientemente las herramientas tecnológicas con el servicio a las personas el impacto que se genera es altamente beneficioso y se obtienen resultados muy satisfactorios ya que se despierta el interés tanto en los administrativos como en los empleados.

Haciendo un estudio interno se determina que el Ilustre Municipio de Pelileo posee una red de datos que puede adecuarse para brindar mayor seguridad en la comunicación entre dos sucursales mediante Internet. Es por ello la razón de nuestra investigación que trata de dar mejor uso de una red de datos y además brindar mejor servicio a los administrativos y empleados ya que cada instante se

comunican entre las dos sucursales para actualizar datos acceden por medio del Internet y están expuestos al ataque de intrusos.

Finalmente es importante destacar que la investigación tiene factibilidad de llevarse a cabo ya que se requieren recursos los cuales están al alcance de nuestras manos. Con el empleo de la tecnología actual se obtendrá información muy valiosa a través del Internet y también existe bibliografía suficiente lo cual permitirá el mejor desarrollo de este trabajo. En relación al aspecto financiero se dispone de los recursos económicos suficientes que permitirán cubrir los gastos que demande la investigación.

1.4 Objetivos

GENERAL:

- Elaborar el diseño y simulación de la Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo.

ESPECÍFICOS:

- Analizar la infraestructura de Red de datos con la que cuenta el Ilustre Municipio de Pelileo.
- Realizar un diagnóstico sobre las características fundamentales de la

protección a nivel de protocolos de capa dos del modelo TCP/IP, en el IMP.

- Proponer el diseño y simulación de una Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP, que brinde seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo

CAPÍTULO II
MARCO TEÓRICO

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

Una vez realizada la revisión de bibliografía relacionada con este proyecto se determina que es una temática nueva y ha llamado la atención previa de otros investigadores de modo que ya existen investigaciones previas que van a aportar enormemente para esta investigación.

2.2 Fundamentación Filosófica

En el aspecto ontológico, que se refiere a la realidad imperante y como es, la presente investigación se relaciona con múltiples realidades ya que el proceso de evolución que experimentan los diferentes centros de servicio a la ciudadanía es distinto y depende de varios factores como lo son los recursos Humanos, Económicos, Tecnología, etc., que da como resultado que la realidad del Ilustre Municipio de Pelileo sea distinta a la de otras instituciones púbicas del país, con lo cual se identifica que estamos centrados en el paradigma naturalista.

2.3 Fundamentación Legal

El presente trabajo investigativo está sustentado en el Decreto 1014 firmado por el Presidente Constitucional de la República Rafael Correa, en el manifiesta que el Software Libre es una Política de Estado para ser adoptado por todas las entidades.

Además la Ley de Educación manifiesta según su capítulo 2, artículo 3, inciso g, que dice: “Impulsar la investigación y la preparación en las áreas: técnica, artística y artesanal.” “Ministerio de Educación del Ecuador - Legislación Educativa,

Documentos legales". Lo cual sustenta el principal objetivo de este trabajo que es el de investigar minuciosamente la de Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo (IMP).

2.4 Categorías Fundamentales

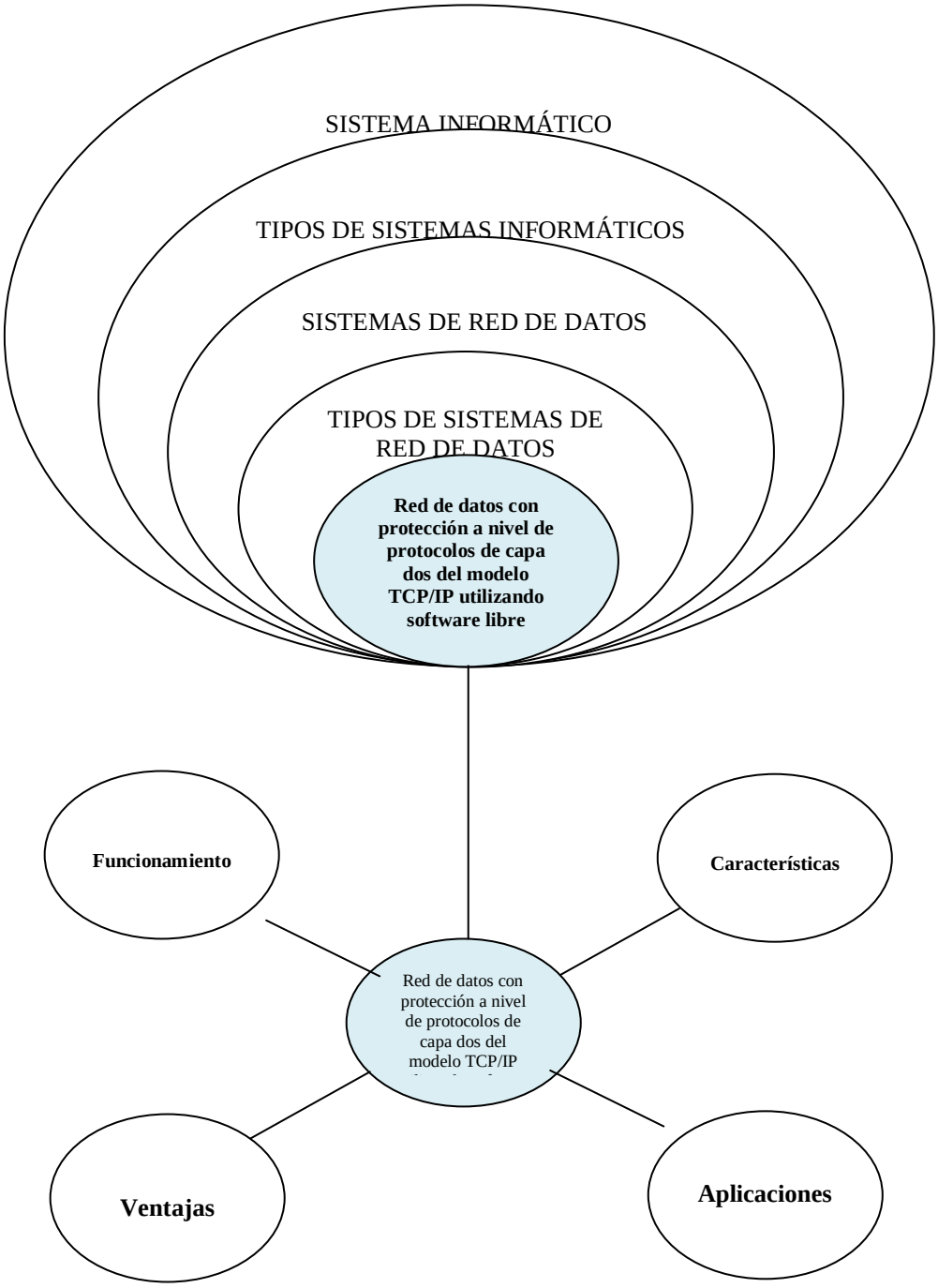

Figura 2.1 Variable Independiente

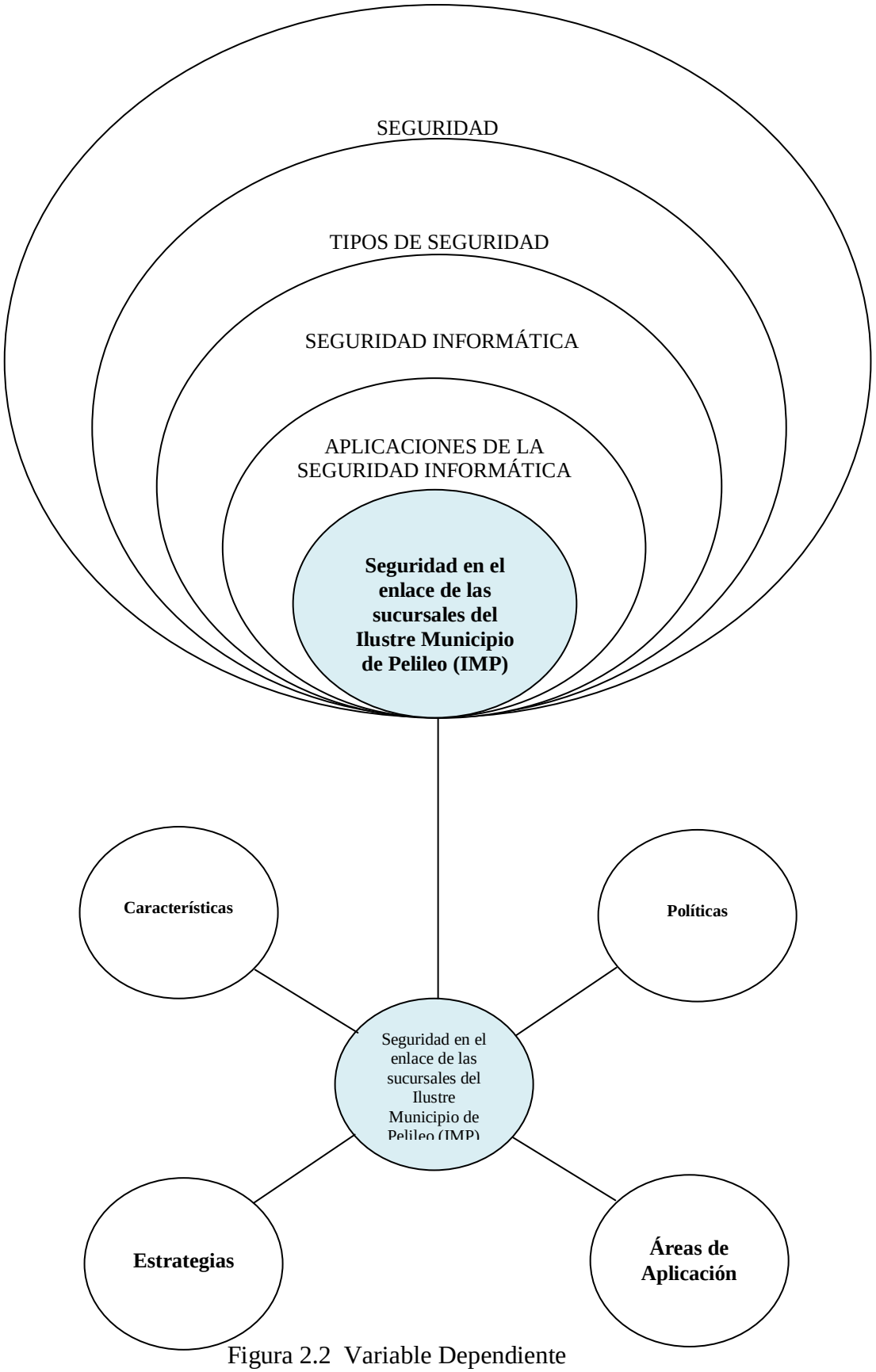

Figura 2.2 Variable Dependiente

Sistema Informático

"Un sistema informático como todo sistema, es el conjunto de partes interrelacionadas, hardware, software y de Recurso Humano (humanware). Un sistema informático típico emplea una computadora que usa dispositivos programables para capturar, almacenar y procesar datos. La computadora personal o PC, junto con la persona que lo maneja y los periféricos que los envuelven, resultan de por sí un ejemplo de un sistema informático"[1].

Incluso la computadora más sencilla se clasifica como un sistema informático, porque al menos dos componentes (hardware y software) tienen que trabajar unidos. Pero el genuino significado de "sistema informático" viene mediante la interconexión. Muchos sistemas informáticos pueden interconectarse, esto es, unirse para convertirse un sistema mayor.

Tipos de Sistema Informático

Existen varios tipos de sistemas informáticos, los técnicamente eruditos a menudo pueden configurar sistemas diferentes para que se puedan comunicar entre sí usando un conjunto de reglas y restricciones conocidas como protocolos. Los protocolos tratan precisamente de definir la comunicación dentro de y entre sistemas informáticos distintos pero conectados entre sí.

[1] Diccionario Informático, www.alegsa.com.ar/Dic/sistema%20informatico.php

En el proceso de comunicación existe el riesgo de la pérdida de información, ante esta falencia aparecen los sistemas de prevención que es el objetivo fundamental del presente proyecto de investigación.

Sistemas de Red de Datos

Es un sistema por el cual se interconectan distintos equipos usando un solo medio de transmisión[2].

Consiste en varias computadoras y periféricos cableados juntos en un área limitada, como el departamento de una compañía o un solo edificio.

Las redes locales se instalan para compartir recursos, por ejemplo impresoras o discos duros; para compartir información, por ejemplo bases de datos; para tener acceso a computadores centrales; para tener comunicación más expedita, por ejemplo usando el correo electrónico; y para tener conectividad, por ejemplo interconexión de diferentes equipos de distintos proveedores.

Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos. Para simplificar la comunicación entre programas (aplicaciones) de distintos equipos, se definió el Modelo OSI por la ISO, el cual especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un alcance definido. Así como también se definió el modelo TCP / IP.

[2] http://www.geocities.com/v.iniestra/apuntes/redes/ Redes de Datos

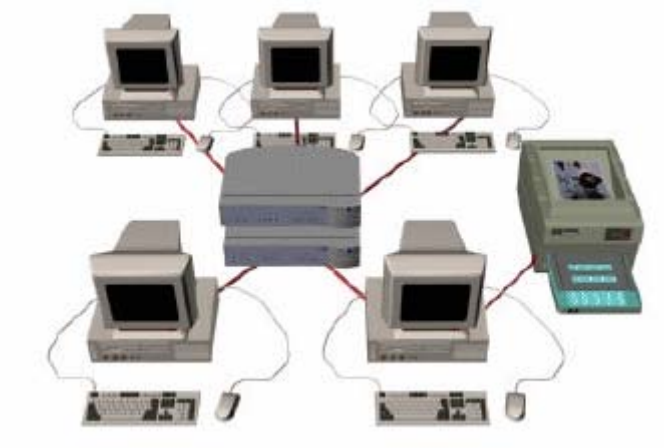

Figura 2.3 Red de Datos

Tipos de Sistemas de Red de Datos

Existen varios tipos de sistemas de red de datos considerando diversos criterios, así tenemos:

Por alcance:

Red de área personal (PAN)

Red de área local (LAN)

Red de área de campus (CAN)

Red de área metropolitana (MAN)

Red de área amplia (WAN)

Por método de la conexión:

Medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros Tipos de cables.

Medios no guiados: radio, infrarrojos, microondas, láser y otras redes Inalámbricas.

Por relación funcional:

Cliente-servidor.

Punto a Punto.

Red de Datos con Protección a Nivel de Protocolos de Capa dos del Modelo TCP/IP Utilizando Software Libre.

Una red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP "es una forma de enlazar redes distantes geográficamente de una empresa donde se utiliza un medio público para el tráfico de datos entre las redes que generalmente es el Internet. Su principal característica es crear túneles virtuales de comunicación entre las redes, de forma que los datos trafiquen encriptados por estos túneles, aumentando la seguridad en la transmisión y recepción de los datos"[3].

La red de datos con la protección a nivel de protocolos será implementada con software libre por varios beneficios como son el bajo costo económico ya que no se requieren licencias, así como también la visión de no utilizar hardware adicional para la implementación. El software se lo puede descargar libremente del internet y no tiene restricciones.

[3] Vpn Linux ipsec

Funcionamiento de una Red de Datos con Protección a Nivel de Protocolos

Las Redes de datos que están separadas físicamente y se comunican mediante internet requieren implementar protección ya que están expuestas al ataque de intrusos y virus. Para ello utilizan las Redes Virtuales Privadas (VPN) que comunican en forma segura utilizando criptografía.

Las VPN poseen sus propios protocolos de comunicación que actúan en conjunto con el protocolo TCP/IP, permitiendo que un túnel virtual sea establecido en los datos que se trafican encriptados. Entre ellos podemos destacar protocolo de tunneling punto a punto (PPTP), Protocolo de Tunneling de capa dos (L2TP) y el Protocolo de seguridad en Internet IPSEC.

Características de una Red de Datos con Protección a Nivel de Protocolos

Una red de datos con protección a nivel de protocolos se caracteriza por tener los siguientes elementos:

Tunelamiento:

La información es transferida en forma encriptada, dando la idea de creación de un túnel virtual, como se muestra en la figura, donde los datos que están traficando por el mismo permanecen ininteligibles para aquellos que los pueden capturar. Esto garantiza que la información al ser capturada por personas sea muy difícil entenderla, a menos que descubran la clave de encriptación para descifrar la información.

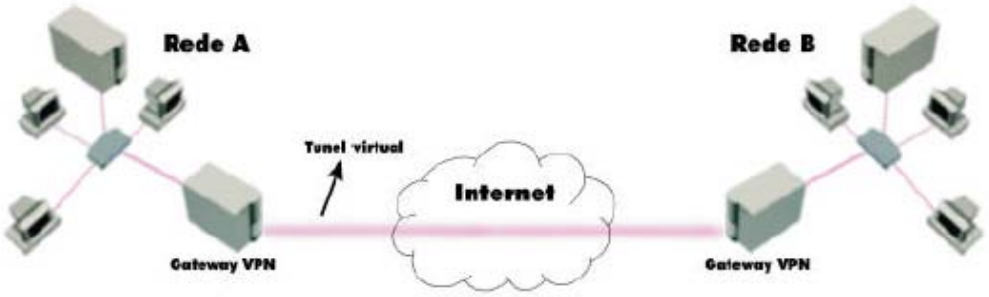

Figura 2.4 Tunelamiento

Autenticación de los extremos

Los mensajes son autenticados para asegurar que sean vistos sólo por usuarios válidos, a través de protocolos de autenticación, que generalmente implementan algoritmos hash, de esta forma, si alguna parte de un mensaje es alterada durante una transmisión, el paquete es descartado y se evita un ataque de tipo Replay.

Transporte Subyacente

El protocolo TCP/IP es la base de internet, y es ampliamente utilizado en las redes de comunicaciones. Pero es inseguro porque no es proyectado para seguridad. Por ello una VPN utiliza una infraestructura de red ya existente de TCP / IP para transmitir los paquetes por la internet, solo adicionando algunos encabezados como se indica la figura. Esto hace que los dispositivos VPN utilicen un mecanismo de transporte subyacente para que se comuniquen, o que posibilite la instalación desde cualquier parte de una red reduciendo los costos (Koleniskov y Hatch, 2002)

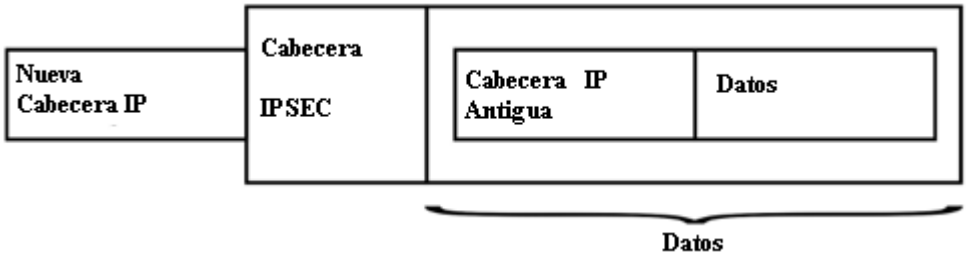

Figura 2.5 Transporte Subyacente

Ventajas de una Red de Datos con Protección a Nivel de Protocolos

Las ventajas de utilizar una VPN están relacionadas a la seguridad, transparencia, facilidad de administración y reducción de costos.

Una VPN garantiza el fortalecimiento de las funciones vitales de seguridad, autenticación, confidencialidad, integridad y control de acceso, reduciendo los riesgos de ataque externos como IP spoofing, man in the middle, e injeccion de paquetes de comunicación.

La transparencia nos indica a los usuarios, las aplicaciones o computadores que perciban una localización física de los recursos que están siendo utilizados permitiendo que sean accesados en lugares remotos como si estuviesen presentes localmente, facilitando el gerenciamiento de las redes y disminuyendo las necesidades de tratamiento para los administradores.

La reducción de costos es una de las principales ventajas de la VPN, ya que se usa la conexión local de internet y no es necesario el uso de líneas dedicadas o servidores para acceso remoto cuyo mantenimiento es relativamente mas caro comparado con una VPN.

A pesar de las ventajas indicadas anteriormente, también se tienen desventajas como son:

Una VPN puede consumir mucho tiempo de implementación.

La dificultad de localizar los defectos.

La relación de confianza entre redes interconectadas.

Disponibilidad de internet.

Aplicaciones de una Red de Datos con Protección a Nivel de Protocolos

Una red de datos con protección de protocolos se implementa con redes de larga distancia para troncalizar la actualización de la información en el banco de información como lo es para manejar toda la información por parte de la propia empresa y no depender de terceros como lo son las líneas dedicadas que demandan de un gran valor económico.

Se emplea en empresas para flexibilizar el trabajo de sus funcionarios, permitiendo que realicen sus funciones desde la comodidad de su casa. Principalmente cuando existen grandes distancias desde la empresa hacia sus residencias o cuando están en viaje de negocios.

Seguridad

“Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadoras, es

muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros"[4].

Tipos de Seguridad

La seguridad puede ser implementada en diversos niveles, así tenemos en el área militar, comercial e informática, destacando que el presente trabajo investigativo está centrado en la seguridad informática que constituye un recurso necesario para la red de datos de la FISEI.

Seguridad Informática

"La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización"[5].

Para que un sistema se pueda definir como seguro debe tener estas características:

- **Autenticidad**: Verifica que una persona con quien se está truncando información confidencial sea realmente quien debería ser.
- **Integridad**: Asegura que los datos no sean alterados durante una transmisión.

[4] MARTINEZ, David, Seguridad en redes, http://exa.unne.edu.ar/depar/areas/informatica
[5] Seguridad Informática, http://www.monografias.com/trabajos/hackers/hackers.shtml

- **Confidencialidad**: limita el acceso a la información, generalmente a través del uso de criptografía.
- **Control de Acceso**: Limita el acceso y la utilización de recursos únicamente para personas autorizadas.
- **Disponibilidad**: Mantiene los recursos disponibles en cualquier momento incluso durante los ataques.
- **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de la Internet, para no permitir que su información sea comprometida.

Criptografía

Un aspecto importante de tratar es la criptografía. Que se deriva de del griego

Kryptos = Escondido, oculto.

Grafía = escrita.

Por lo que puede ser definida como el arte o ciencia para asegurar los mensajes, de modo que solo las personas autorizadas puedan leerlo, garantizando de esta forma la confidencialidad, autenticidad, integridad y no repudio (Schneier, 1996)

Dependiendo del tipo de clave utilizada la criptografía se clasifica en:

Criptografía Simétrica: se basa en la simetría de las claves, o sea, que la misma clave que se utiliza para encriptar un mensaje se utiliza para desencriptarlo. La

clave es llamada privada y permite troncalizar la información entre el emisor y receptor por un canal seguro.

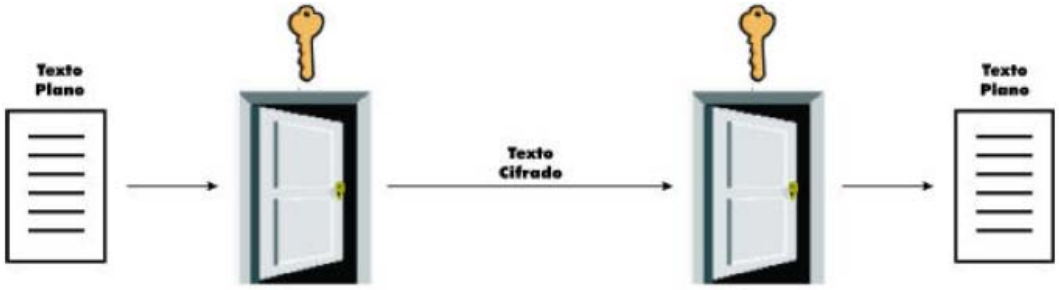

Figura 2.6 Criptografía Simétrica

Existen los siguientes algoritmos de encriptación

- ***Data Encryption Standard* (DES) –** 56 bits.
- ***Triple Data Encryption Standard* (3DES) –** 112 bits.
- ***Advanced Encryption Standard* (AES) –** 128, 192 o 256 bits.
- ***Blowfish* –** 448 bits.
- ***Carlisle Adams and Stafford Tavares* (CAST) –** 128 o 256 bits.
- ***Twofish* –** 128, 192 o 256 bits.
- ***Serpent* –** 128, 192 o 256 bits.

Criptografía Asimétrica: este tipo de criptografía en cambio utiliza dos claves distintas, una privada y otra pública. Se puede utilizar cualquiera de las dos claves para cifrar el mensaje, en cambio, solo una clave inversa debe ser utilizada para descifrar el mensaje. Por ejemplo: el emisor utiliza una clave pública para cifrar el mensaje y enviarlo en cambio el receptor debe utilizar la clave privada para descifrar el mensaje. De esta forma se garantiza la autenticidad y confidencialidad.

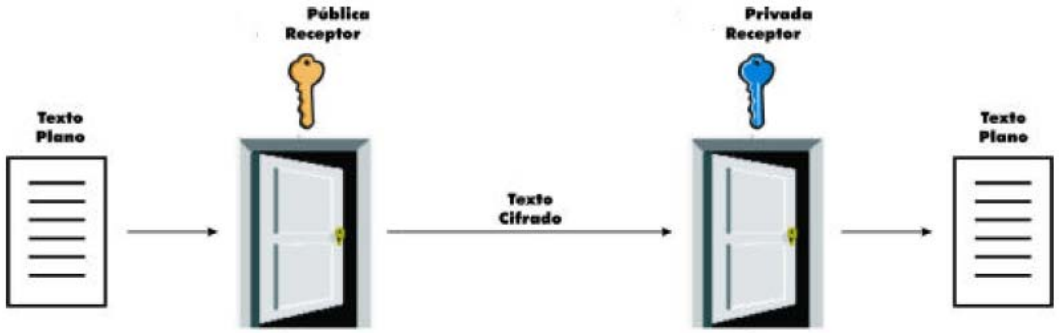

Figura 2.7 Criptografía Asimétrica

Aplicaciones de la Seguridad Informática

En la seguridad informática es fundamental considerar como sus variantes el aspecto de qué debemos defendernos, así tenemos la seguridad ante personas, amenazas lógicas, catástrofes.

a) Personas

La mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Así tenemos: Ex empleados, curiosos, hackers, crackers, terroristas.

b) Amenazas lógicas

Bajo la etiqueta de "amenazas lógicas' encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello. Algunas de las amenazas con que nos podemos encontrar son:

- Software incorrecto
- Herramientas de seguridad
- Bombas lógicas
- Virus

- Gusanos
- Caballos de Troya
- Técnicas salami
- Spam
- Spyware

c) Catástrofes

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que podamos pensar).

De todas las formas de implementar seguridad que se detallaron anteriormente es importante manifestar que el propósito del presente trabajo investigativo es determinar la manera de implementar seguridad ante las diversas amenazas lógicas.

Seguridad en el Enlace de las Sucursales del Ilustre Municipio de Pelileo (IMP).

"En general las redes de instituciones públicas como son los Municipios siempre han sido mucho más permisivas que las de otro tipo de institución o empresa. Sin embargo, a través del tiempo Internet se ha tornado mucho más peligrosa debido a la gran variedad de usuarios que actualmente la utilizan"[6]. Lo cual justifica un cambio de enfoque en la administración de las redes universitarias razón por la

[6] Universidad de Chile, Seguridad en las redes de Datos, http://www.ing.puc.cl/esp/infgeneral

cual es fundamental realizar el estudio de un sistema de prevención de intrusos para reducir los peligros en la red de datos.

Características de Seguridad en el Enlace de las Sucursales del Ilustre Municipio de Pelileo

La seguridad en la red de datos debe estar empleada en toda organización ya que debe estar a la vanguardia de los procesos de cambio. Caracterizándose por:

- Disponer de información continua, confiable y en tiempo.
- Tener poder ya que se posee la información y que es reconocida como:
  - Crítica, indispensable para garantizar la continuidad operativa de la organización.
  - Valiosa, es un activo corporativo que tiene valor en sí mismo.

Es por ello lo esencial de preservar la seguridad en las redes de datos ya que la información que maneja el Ilustre Municipio del Cantón Pelileo es muy valiosa y confidencial.

Políticas de Seguridad en el Enlace de las Sucursales del Ilustre Municipio de Pelileo

Las políticas de seguridad representan los lineamientos que se deben seguir para implementar una seguridad muy efectiva en la red en este caso como lo es el Ilustre Municipio del Cantón Pelileo, así podemos citar las siguientes políticas.

- Todos los usuarios responsables del uso de un ordenador deben garantizar que está protegido por una contraseña suficientemente robusta, es decir, no trivial o evidente.

- Deben aplicarse periódicamente todas las actualizaciones de seguridad para el sistema operativo que esté usando.
- Los sistemas operativos deben de estar protegidos mediante antivirus eficaces.
- No compartir carpetas sin contraseña.
- En la medida de lo posible sustituir los protocolos que no encriptan las contraseñas por otros que si las encripten.
- No instalar servicios de red que no se vayan a usar

Estrategias de Seguridad en el Enlace de las Sucursales del Ilustre Municipio de Pelileo

Las estrategias de seguridad representa la forma de cómo van a ser implementadas las políticas de seguridad en las organizaciones y como lo es el caso de el Ilustre Municipio del Cantón Pelileo. Para lo cual es importante fundamentarse en las siguientes recomendaciones.

- **Recomendación UIT–T E.sec1: "Requisitos de seguridad de las redes de telecomunicaciones"**[7], contiene una visión general y un marco en los cuales se identifican las amenazas a la seguridad de las redes de telecomunicaciones en general (fijas y móviles, de voz y de datos) y contiene orientaciones para planificar contramedidas que se puedan tomar para reducir los riesgos dimanantes de las amenazas.
- **Recomendación UIT–T E.sec.2: "Organización de incidentes y tratamiento de incidentes de seguridad (directrices)"**. El objeto de esta

[7] Las Normas de Seguridad, http://www3.gartner.com/5_about/press_releases/pr11june2003c.jsp

Recomendación es analizar, estructurar y sugerir un método para establecer una organización de gestión de incidentes en el cual se estudie el transcurso y la estructura del incidente.

Ámbitos de Aplicación de Seguridad en el Enlace de las Sucursales del Ilustre Municipio de Pelileo

La seguridad en la red de datos tiene como ámbitos de aplicación todas las dependencias conectadas a la red y que requieren un nivel de seguridad determinado para la información que disponen, es por ello que la implementación de un IPS en la FISEI será el elemento fundamental para garantizar la seguridad en la red de esta facultad.

2.5 Hipótesis

La Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre mejorará la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo (IMP).

2.6 Señalamiento de Variables de la Hipótesis

Variable Independiente:

Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre

Variable Dependiente:

Seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo

CAPÍTULO III
METODOLOGÍA

CAPÍTULO III

METODOLOGÍA

3.1 Enfoque

La investigación se ha fundamentado en el Paradigma Cualitativo porque el problema requiere investigación interna, interesa la interpretación del efecto que se consiga con el estudio de un sistema de prevención de ataques, sus objetivos plantean acciones inmediatas que se las debe tomar para corregir lo más pronto las falencias existentes en la red de datos del Ilustre Municipio de Pelileo debido al ataque de intrusos y virus, determina una hipótesis lógica que busca un fin específico, requiere de un trabajo de campo con todos los empleados del IMP y el jefe de sistemas, además sus resultados no son generalizables ya que nuestro estudio va a ser particularizado solo para mejorar la seguridad en la Red de Datos del Ilustre Municipio de Pelileo.

3.2 Modalidad Básica de la Investigación

La modalidad que empleara en nuestro trabajo investigativo será:

De Campo, porque se la llevará a cabo en las instalaciones del IMP. Además es importante considerar las siguientes características que debe poseer nuestra investigación:

Aplicada, ya que está orientada a utilizar Software y Hardware especializado;

Descriptiva, puesto que se preocupa de analizar, describir, interpretar las experiencias

que se adhieren en el proceso de comunicación;

De Acción, porque estará orientada a lograr cambios en la Red de Datos del Ilustre Municipio de Pelileo.

3.3 Nivel o Tipo de Investigación

El presente trabajo de investigación tiene la característica de ser Exploratorio ya que permitirá desarrollar la estructura de protección y seguridad para mejorar el desempeño de la red de datos del IMP. Además nos permite sondear y consecuentemente dar el tratamiento necesario a problemas que se generan en el funcionamiento de la red.

3.4 Población Y Muestra

La población y universo de estudio estará integrada por el Personal Administrativo, del área de Sistemas del IMP, se detalla en el siguiente cuadro.

Población	**Frecuencia**	**%**
Personal Administrativo	7	100
Personal del Área de Sistemas	8	100

Tabla 3.1 Población y Muestra

3.5 Operacionalización de Variables

Variable Independiente: Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre

<table>
<tr><th>VARIABLE</th><th>CONCEPTUALIZACIÓN</th><th>DIMENSIONES</th><th>INDICADORES</th><th>ITEMS</th></tr>
<tr>
<td rowspan="2">Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre.</td>
<td rowspan="2">Sistema que tiene la funcionalidad de conectar varios usuarios con funcionalidad de protección a nivel de protocolos.</td>
<td>• Sistema de red</td>
<td>• Informático
• Mecánico
• Electrónico</td>
<td>¿Una red con capacidad de proteger a nivel de protocolos es: ?
Altamente Fiable
Fiable
Insegura

¿Qué nivel de desempeño eficiente tiene una red con software libre: ?
Alto
Medio
Bajo</td>
</tr>
<tr>
<td>• Protección</td>
<td>• Hardware
• Software</td>
<td>¿La implementación de una red con protección a nivel de protocolos en el IMP es: ?
Muy difícil
Difícil
Fácil

¿Cómo determina la administración de una red con software libre y protección a nivel de protocolos?
Fácilmente Administrable
Medianamente Administrable
Difícilmente Administrable</td>
</tr>
</table>

Tabla 3.2 Variable Independiente

Variable Dependiente: seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo

<table>
<tr><th>VARIABLE</th><th>CONCEPTUALIZACIÓN</th><th>DIMENSIONES</th><th>INDICADORES</th><th>ITEMS</th></tr>
<tr>
<td>Seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo</td>
<td>Procedimiento mediante el cual se establecen políticas para evitar distintos ataques en la red de Datos</td>
<td>• Políticas

• Ataques</td>
<td>• Integral
• Militar
• Social

• Virus
• Spam
• Spyware
• Nivel de Hardware
• Intrusos</td>
<td>¿Cómo considera las políticas de seguridad implementada en la red del IMP?
<table><tr><td>Muy efectivas</td><td></td></tr><tr><td>Efectivas</td><td></td></tr><tr><td>Deficientes</td><td></td></tr></table>
¿De qué forma considera la rapidez en que se lleva a cabo la implementación de políticas de seguridad en el IMP. ?
<table><tr><td>Muy rápida</td><td></td></tr><tr><td>Rápida</td><td></td></tr><tr><td>Lenta</td><td></td></tr></table>
¿Cómo considera el nivel de desempeño de los empleados para gestionar políticas de seguridad en la red de datos?
<table><tr><td>Óptimo</td><td></td></tr><tr><td>Normal</td><td></td></tr><tr><td>Deficiente</td><td></td></tr></table>
¿De qué forma, la red del IMP provee servicio de protección de ataques a los usuarios?
<table><tr><td>Altamente satisfactoria</td><td></td></tr><tr><td>Satisfactoria</td><td></td></tr><tr><td>Poco satisfactoria</td><td></td></tr></table></td>
</tr>
</table>

Tabla 3.3 Variable Dependiente

3.6 Recolección de Información

El presente trabajo investigativo empleará como técnica la Observación que se caracteriza por ser de tipo:

- Directa: porque la investigación se realizará en contacto con el personal del Área de Sistemas, Empleados y Administrativos del IMP.
- Participante: ya que el proceso se lo llevará a cabo compartiendo experiencias directamente con el personal del Área de Sistemas.
- Estructurada: debido a que se realizará la investigación basándose en una planificación metódica y críticamente ejecutada ya que se encargará de plantear un esquema de seguridad en la red con un sistema de seguridad eficiente.
- Individual: porque únicamente el autor tendrá interacción con el personal del Área de Sistemas del Ilustre Municipio de Pelileo.
- Campo: ya que el estudio se llevará a cabo en las instalaciones del IMP.
- Intersubjetiva: debido a que la observación va a ser mutua entre el investigador y el personal del Área de Sistemas.

Como instrumentos se empleará:

- Cuaderno de Notas: donde se describirá lo experimentado con el sistema de seguridad.
- Anecdotario: que permitirá registrar los incidentes que se generan durante el proceso de proceso de análisis de implementación de seguridad a nivel de protocolos.
- Encuesta: muy útil para recoger la información empleando un cuestionario que se encargará de averiguar todos los aspectos más relevantes del análisis de los protocolos de capa dos para implementar la seguridad.

3.7 Procesamiento y Análisis

La información recogida en el proceso de investigación será objeto de revisión crítica que

permitirá discernir la información más relevante para nuestro estudio y descartar la información no pertinente e incompleta que no nos muestre con claridad el efecto del análisis de los protocolos de capa dos para implementar la seguridad.

El plan a llevarse a cabo será el siguiente:

- Para el procesamiento:

Se utilizarán representaciones gráficas como lo son diagramas circulares y representación de barras que permiten destacar las relaciones más relevantes entre los datos obtenidos de las variables de estudio como lo es la red de datos con protección a nivel de protocolos y su aplicación para mejorar la seguridad en la red de datos del IMP.

Además es importante destacar que la representación gráfica nos permite conseguir una representación ordenada de la información que incluyen comparaciones porcentuales entre los distintos parámetros de las variables de la investigación.

- Para el análisis:

Se lo llevará a cabo sobre los resultados estadísticos obtenidos en el procesamiento realizado previamente en donde se toma en cuenta las relaciones fundamentales entre los objetivos y la hipótesis que permitirán considerar como está afectando el sistema de prevención de intrusos en el mejoramiento de la seguridad.

Interpretación: fundamentada en el marco teórico que se desarrolla en la investigación y que nos permite darnos cuenta de los resultados positivos que se obtienen.

Finalmente de acuerdo a la interpretación que se realice permitirá comprobar la hipótesis y establecer las respectivas conclusiones y recomendaciones del estudio la red de datos con protección a nivel de protocolos y su aplicación para mejorar la seguridad en la red de datos del IMP.

CAPITULO IV
ANALISIS E INTERPRETACION DE RESULTADOS

CAPITULO IV

ANALISIS E INTERPRETACION DE RESULTADOS

4.1 Información del proceso.

La comunicación entre las Sucursales del Ilustre Municipio de Pelileo se lo lleva a cabo vía telefónica, celular o mensajería. Sin proporcionar ninguna característica de seguridad, ante esta realidad es necesario emplear una estrategia para que las sucursales del municipio se comuniquen de una manera segura y eficiente.

4.2 Análisis del Problema.

En la investigación de campo se determinó que la comunicación entre las Sucursales del Municipio de Pelileo es inadecuada y muy costosa, ya que es necesario conocer el proceso del servicio que proporciona cada sucursal a cada momento.

Se identificó que las sucursales del Ilustre municipio de Pelileo tienen servicio de Internet proporcionado por la CNT y que solo lo utilizan para acceder a la web. Analizando alternativas para implementar la comunicación se determina que es posible utilizar un canal público como lo es el internet para comunicar las dos Sucursales del Ilustre Municipio de Pelileo.

Un elemento muy importante para implementar la comunicación segura entre las sucursales del Municipio de Pelileo es la utilización de un Firewall conocido como IPCop.

Distribución IPCop

IPCop es una distribución Linux que implementa un cortafuegos (o *firewall*) y proporciona una simple interfaz web de administración basándose en una computadora personal. Originalmente nació como una extensión de la distribución SmoothWall cuyo desarrollo había estado congelado bastante tiempo.

Figura 4.1 Logo IPCop

IPCop tiene como objetivos ser un cortafuegos administrado a través de una interfaz web, con funcionalidades básicas y avanzadas, yendo (a manera de ejemplo) desde el simple filtrado de paquetes hasta la asignación de ancho de banda fijo a cada puesto de trabajo o la configuración de redes virtuales VPN. **IPCop** se actualiza desde el Interfaz Web de manera muy sencilla, incluyendo actualizaciones del Kernel.

IPCop solo tiene instaladas las herramientas justas para su función como firewall, limitando el daño que podría hacer un intruso que comprometiera el sistema. Si se desea ampliar la funcionalidad existen extensiones, comunes con SmoothWall, que permiten instalar todo tipo de utilidades como por ejemplo instalar Nmap para escanear IP `s.

Topologías de red soportadas: Permite la implementación de diferentes topologías de red, ya sea desde la simple LAN que sale a internet, hasta la creación de una zona desmilitarizada (DMZ), soportando también la inclusión de una red inalámbrica.

Las diferentes zonas las divide en colores, siendo:

- **Roja** = zona de Internet,
- **Verde** = Red de Área Local (LAN) cableada,
- **Naranja** = zona desmilitarizada (DMZ, para la granja de servidores),
- **Azul** = zona inalámbrica (Wireless).

INFORMACIÓN GENERAL	
Modelo de desarrollo	Software Libre
Última versión estable	1.4.20 24 de julio de 2008
Tipo de núcleo	Monolítico
Interfaz gráfica por defecto	Interfaz web
Licencia	GPL / AGPL/ BSD
Estado actual	En desarrollo
Idiomas	Español / Inglés

Tabla 4.1 Información General IPCop

Funcionalidades de IPCop

Se determinan las siguientes funcionalidades:

Libertades del software libre
De acuerdo con tal definición, el software es "libre" si garantiza las siguientes libertades:

Libertad	Descripción
0	la libertad de usar el programa, con cualquier propósito.
1	la libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a tus necesidades.
2	la libertad de distribuir copias del programa, con lo cual puedes ayudar a tu prójimo.
3	la libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie.
Las libertades 1 y 3 requieren acceso al código fuente porque estudiar y modificar software sin su código fuente es muy poco viable.	

Tabla 4.2 Libertades del Software Libre

Zerina, software para generar el túnel virtual

Es un software en la categoría de Software Libre, que permite crear un túnel virtual entre dos puntos de una Red Pública.

Protocolo UDP

User Datagram Protocol (UDP) es un protocolo mínimo de nivel de transporte orientado a mensajes documentado en el RFC 768 de la IETF.

En la familia de protocolos de Internet UDP proporciona una sencilla interfaz entre la capa de red y la capa de aplicación. UDP no otorga garantías para la entrega de sus mensajes y el origen UDP no retiene estados de los mensajes UDP que han sido enviados a la red. UDP sólo añade multiplexado de aplicación y suma de verificación de la cabecera y la carga útil. Cualquier tipo de garantías para la transmisión de la información deben ser implementadas en capas superiores

User Datagram Protocol (UDP)	
Familia:	Familia de protocolos de Internet
Función:	Intercambio de datagramas a través de una red.
Ubicación en la pila de protocolos	
Aplicación	DNS, DHCP, NTP, ...
Transporte	UDP
Red	IP
Enlace	Ethernet, Token Ring, FDDI, ...
Estándares:	RFC 768 (1980)

Tabla 4.3 Protocolo UDP

El protocolo UDP se utiliza por ejemplo cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

Puertos de Comunicación

UDP utiliza puertos para permitir la comunicación entre aplicaciones. El campo de puerto tiene una longitud de 16 bits, por lo que el rango de valores válidos va de 0 a 65.535. El puerto 0 está reservado, pero es un valor permitido como puerto origen si el proceso emisor no espera recibir mensajes como respuesta.

Los puertos 1 a 1023 se llaman puertos "bien conocidos" y en sistemas operativos tipo Unix enlazar con uno de estos puertos requiere acceso como superusuario.

Los puertos 1024 a 49.151 son puertos registrados.

Los puertos 49.152 a 65.535 son puertos efímeros y son utilizados como puertos temporales, sobre todo por los clientes al comunicarse con los servidores.

993/tcp	**IMAP4 sobre SSL (E-mail)**
995/tcp	POP3 sobre SSL (E-mail)
1080/tcp	SOCKS Proxy
1337/tcp	suele usarse en máquinas comprometidas o infectadas
1352/tcp	IBM Lotus Notes/Domino RCP

Tabla 4.4 Puestos de Utilización preestablecida

Seguridad Mediante Cifrado

Cifrado Simétrico

La criptografía simétrica se basa en la utilización de la misma clave para el cifrado y para el descifrado, es decir, la robustez de un algoritmo de cifrado simétrico recae en el conocimiento de dicha clave. Sus ventajas son la sencillez de implementación, su rapidez y la robustez que provee. La siguiente figura esboza un criptosistema de clave secreta o simétrica:

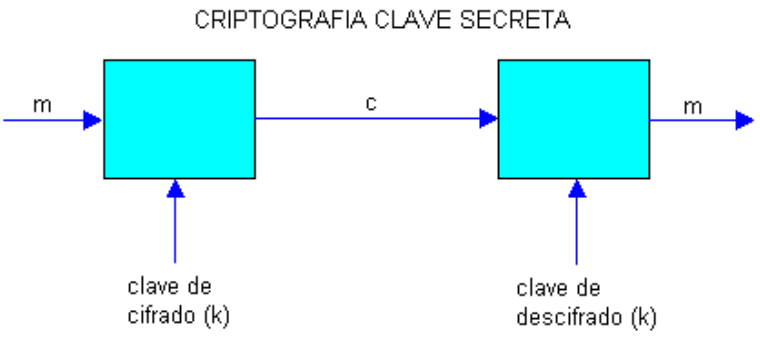

Figura 4.2 Cifrado Simétrico

Algoritmos de cifrado simétrico

IPCop tiene la capacidad de implementar los siguientes algoritmos de cifrado:

ALGORITMO	DESCRIPCIÓN
DES	El DES (*Data Encription Standard* o *Estándar de Encriptación de Datos*) Es el algoritmo de cifrado simétrico más estudiado, mejor conocido y más empleado del mundo.
Triple-DES	Consiste en encriptar tres veces una clave DES. Esto se puede hacer de varias maneras: DES-EEE3: Tres encriptaciones DES con tres claves distintas.
AES	El AES (*Advanced Encription Standard* o *Estándar Criptográfico Avanzado*) es un algoritmo de cifrado por bloques destinado a reemplazar al DES como estándar.
RC2	El RC2 es un algoritmo de cifrado por bloques de clave de tamaño variable diseñado por Ron Rivest de RSA Data Security (la RC quiere decir *Ron's Code* o *Rivest's Cipher*). El algoritmo trabaja con bloques de 64 bits y entre dos y tres veces más rápido que el DES
RC4	El RC4 es un algoritmo de cifrado de flujo diseñado por Ron Rivest para RSA Data Security. Es un algoritmo de tamaño de clave variable con operaciones a nivel de byte.
RC5	El RC5 es un algoritmo parametrizable con tamaño de bloque variable, tamaño de clave variable y número de rotaciones variable. Los valores más comunes de los parámetros son 64 o 128 bits para el tamaño de bloque
IDEA	El IDEA (*International Data Encription Algorithm*) es un algoritmo de cifrado por bloques de 64 bits iterativo. La clave es de 128 bits. La encriptación precisa 8 rotaciones complejas.
SAFER	El SAFER (*Secure And Fast Encription Routine*) es un algoritmo de cifrado por bloques no propietario. Está orientado a bytes y emplea un tamaño de bloque de 64 bits y claves de 64 (SAFER K-64) o 128 bits (SAFER K-128).
Blowfish (BS)	Es un algoritmo de cifrado por bloques de 64 bits desarrollado por Scheiner. La clave tiene tamaño variable (con un máximo de 448 bits) y se emplea para generar varios vectores de subclaves.
CAST	Algoritmo de cifra basado en un secreto compartido (clave). CAST-128: Cifra el texto en bloques de 64 bits. Utiliza claves de 40 a 128 bits. CAST-256: Cifra el texto en bloques de 128 bits. Utiliza claves de 128, 192 o 256 bits.
ECB (Electronic Code Book).	Se parte el mensaje en bloques de *k* bits, rellenando el ultimo si es necesario y se encripta cada bloque. Para desencriptar se trocea el texto cifrado en bloques de *k* bits y se desencripta cada bloque.
CBC (Cipher Block Chaining)	Este método soluciona el problema del ECB haciendo una o-exclusiva de cada bloque de texto en claro con el bloque anterior cifrado antes de encriptar.
OFB (Output Feedback Mode)	Este sistema emplea la *clave de la sesión* para crear un bloque pseudoaleatorio grande (*pad*) que se aplica en o-exclusiva al texto en claro para generar el texto cifrado.
CFB (Cipher Feedback Mode)	Variante del método anterior para mensajes muy largos.
Cifrado de flujo de datos	Generalmente operan sobre 1 bit (o sobre bytes o palabras de 16 ó 32 bits) de los datos de entrada cada vez. El algoritmo genera una secuencia (*secuencia cifrante* o *keystream* en inglés) de bits que se emplea como clave. La encriptación se realiza combinando la secuencia cifrante con el texto en claro.

4.3 Interpretación de Resultados.

Después del análisis previo, se da como alternativa de solución; la implementación de un túnel a través del internet con la distribución IPCop el cual proporciona una seguridad muy efectiva y se identifican las siguientes características.

- La distribución IPCop es muy liviana, sencilla y elemental para implementar un firewall poderoso y proporciona una simple interfaz web de administración basándose en una

computadora personal por lo que no se requieren factores económicos muy reducidos lo cual es muy favorable para su factibilidad de implementación.

- El software Zerina es una herramienta muy efectiva que al ser implementada junto con IPCop permiten crear un túnel muy eficiente que evita las intrusiones y ataques externos.

- El protocolo UDP trabaja de una manera muy liviana y rápida ya que sólo envía los paquetes en una dirección y no necesita de la confirmación de recepción, de modo que los paquetes no van a estar navegando en la red en grandes cantidades para ser fácilmente capturados por los hackers

- La versatilidad de la utilización de diversos puertos para establecer la comunicación por el túnel virtual de las Sucursales del Ilustre Municipio de Pelileo permite cambiar periódicamente los números de puerto de modo que será muy difícil identificar el puerto de comunicación por parte de los hackers.

- Una de las fortalezas más importantes es la utilización de algoritmos simétricos combinados que proporcionan una seguridad muy eficiente que difícilmente será descifrada por los atacantes.

4.4 Comprobación de la hipótesis

Luego de analizar los resultados obtenidos podemos determinar que con la utilización de software libre que permite implementar criptografía simétrica muy efectiva, control de puertos y protocolos se puede comprobar que la Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre mejorará la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo (IMP).

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones.

- Un túnel virtual brinda un nivel de seguridad muy efectivo ya que todos los paquetes viajan encriptados con potentes algoritmos de encriptación y protección a nivel de protocolos que evitan ser fácilmente manipulados por personas sin escrúpulos que navegan en la red pública.
- Una red con seguridad a nivel de protocolos posee una característica fundamental que es la de crear una red virtual con direcciones IP que difícilmente son identificadas en el internet y que solo lo conoce la persona que creó el túnel virtual.
- Cuando se crea el túnel virtual se generan certificados encriptados con información muy importante de la empresa, que solo lo comparten los Firewalls / Routers que están interconectados entre sí generando el túnel virtual. Esto provee el nivel de seguridad muy aceptable en nuestra red del ilustre Municipio de Pelileo.
- Analizando el comportamiento del túnel virtual en la simulación se puede determinar que presenta una seguridad muy elevada ante el ataque de diversos hackers ya que no da a conocer el puerto de comunicación ni las direcciones IP virtuales que se utiliza en la comunicación.
- La creación de un túnel virtual a través del internet utilizando software libre y específicamente IPCop representa la manera más económica y eficiente de crear una red con seguridad a nivel de protocolos ya que no se debe comprar ningún tipo de software ya que todo es gratuito.

5.2 Recomendaciones.

- Es necesario considerar que si bien es cierto el túnel virtual brinda un nivel de seguridad muy efectivo, pero no representa un sistema 100% seguro, ya que conocemos que ningún sistema es perfecto. Ante esto debemos establecer políticas de seguridad que nos proveerán de una seguridad más confiable.
- El protocolo a utilizar para brindar la seguridad es recomendable que sea UDP porque es un protocolo no orientado a la conexión y no necesita del reenvío de paquetes para que sean fácilmente interceptados por los hackers.
- Es recomendable la utilización de clave de encriptación simétrica ya que constituye una sola clave y va ha ser compartida entre las dos sucursales mediante un certificado de autenticación lo cual permite implementar una seguridad muy confiable con la utilización de políticas de seguridad efectivas.
- Es necesario recomendar que el número de puerto y la dirección virtual se la cambie periódicamente, ya que si bien es cierto, las pruebas de Hackeo no pueden revelarlos, pero habrá un momento que pueda ser descubierto por otro hacker y se perdería nuestra seguridad.
- Es muy primordial recomendar que el software libre si bien no tiene costo, pero si demanda de investigación adicional y es necesario que se esté actualizando con nuevas versiones de IPCop y Zerina o también desarrollar una configuración para mejorar dicho software libre.

CAPÍTULO VI
PROPUESTA

CAPÍTULO VI

PROPUESTA

6.1 Datos Informativos:

6.1.1 Título:
Simulación de la Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo

6.1.2 Beneficiarios
Empleados y Administrativos del Ilustre Municipio del Cantón Pelileo

6.1.3 Ubicación
País: Ecuador, Provincia: Tungurahua, Ciudad: Pelileo.

6.1.4 Tiempo estimado para la ejecución
Seis meses Enero - Junio 2010

6.2 Antecedentes de la propuesta

Revisando materiales investigados anteriormente se registra que ya han existido propuestas de implementación de redes con seguridad, pero no relacionadas con la protección a nivel de protocolos de capa dos del modelo TCP/IP, de este modo se espera que el presente trabajo investigativo logre aportar para que el objetivo de mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo se haga una realidad.

6.3 Justificación

Habiendo analizado las conclusiones que surgieron de la investigación, es necesario llevar a cabo nuevas alternativas que permitan proporcionar seguridad en la comunicación de las sucursales del Ilustre Municipio de Pelileo ya que la información confidencial que comparten dichas sucursales atraviesa un medio de comunicación público que puede ser accedido por cualquier persona y es necesario evitar el acceso de dichas personas ajenas.

Todas las acciones a llevarse a cabo están orientadas a conseguir una comunicación entre las sucursales del Ilustre municipio de Pelileo y sin la necesidad de requerimientos económicos adicionales por lo que se utiliza software libre. Es por ello la necesidad de proponer la Simulación de la Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo.

6.4 Objetivos

General:

- Simular la Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo

Específicos:

- Establecer y aplicar los criterios de selección y adecuación de Hardware y Software para implementar la seguridad a nivel de protocolos en la comunicación de las Sucursales del Municipio.
- Elaborar un ambiente de interacción de los distintos componentes de la red que permite la comunicación segura de las Sucursales del Ilustre Municipio de Pelileo
- Proporcionar a los Administradores de la red del municipio y a través de ellos difundir a los usuarios de la red para que prueben la alternativa de simulación y proporcionen sus expectativas.

6.5 Análisis de factibilidad

La factibilidad de llevar a cabo la propuesta planteada es afirmativa, puesto que el Ilustre Municipio de Pelileo y la Universidad Técnica de Ambato, específicamente la carrera de Ingeniería Electrónica ofrecen el apoyo necesario para su desarrollo.

Así también es importante manifestar que el software necesario para desarrollar el trabajo es de fácil adquisición ya que es software libre y se puede obtener gratuitamente del internet por lo que se convierte en un aporte fundamental y un apoyo efectivo para llevar a cabo exitosamente nuestro trabajo.

6.6 Fundamentación Científico – Técnica

La comunicación de dos sucursales se las puede llevar a cabo utilizando varios medios que pueden significar el empleo de grandes cantidades económicas o como también pueden representar un costo reducido. Ante esta situación se ha buscado una alternativa para que no represente gasto económico a la empresa o institución, por ello se utiliza software libre Linux que no tiene costo de licencia.

Técnicamente se puede manifestar que la comunicación seleccionada de acuerdo a las disponibilidades del Municipio de Pelileo es por medio de la Red utilizando el medio Público que en nuestro caso es el Internet.

Finalmente es importante indicar que en una red se puede proporcionar seguridad de distintos modos, pero el más efectivo de acuerdo a nuestro trabajo investigativo es crear un túnel virtual a través del medio público para lo cual implementamos seguridad a través de protocolos, puertos y algoritmos de encriptación que nos permiten conseguir nuestro objetivo fundamental.

6.7 Metodología, Modelo Operativo

Las operaciones a llevarse a cabo para simular la Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo contempla el siguiente procedimiento.

Análisis de Requerimientos.

El Ilustre Municipio de Pelileo (IMP) es una entidad del estado que está dedicada a prestar servicio a la comunidad en diferentes áreas como son:

Alcaldía	Biblioteca	Aula Virtual
Dirección Financiera	Dirección Administrativa	Dirección de Planificación
Obras Públicas	Rentas	Tesorería
Contabilidad	Recaudación	Computación

Además el IMP cuenta con recursos humanos, materiales y tecnología de punta, satisfaciendo eficientemente las necesidades de los usuarios pelileños para lo cual se proyecta realizar sus funciones en dos sucursales. La Sucursal Principal en la Matriz San Pedro de Pelileo y la Sucursal secundaria en la Parroquia García Moreno a 10 Km de distancia. .

La demanda de usuarios en recaudación y en las direcciones Financiera, Administrativa y de Planificación es muy grande, razón por la cual estas dependencias laboran en las dos sucursales. la información que comparten es muy valiosa por lo que se requiere implementar seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo.

El objetivo primordial del presente trabajo de investigación es proporcionar protección y seguridad a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre en el enlace de las sucursales del Ilustre Municipio de Pelileo. El medio de comunicación que se

utilizará será un medio público como el Internet y para proveer seguridad se pretende crear un túnel a nivel del internet creado mediante protocolos de capa dos del modelo TCP/IP.

Diseño del Túnel a través del internet

Análisis de las características de infraestructura de red en el Ilustre Municipio de Pelileo (IMP).

La red del IMP está representada en el siguiente diagrama

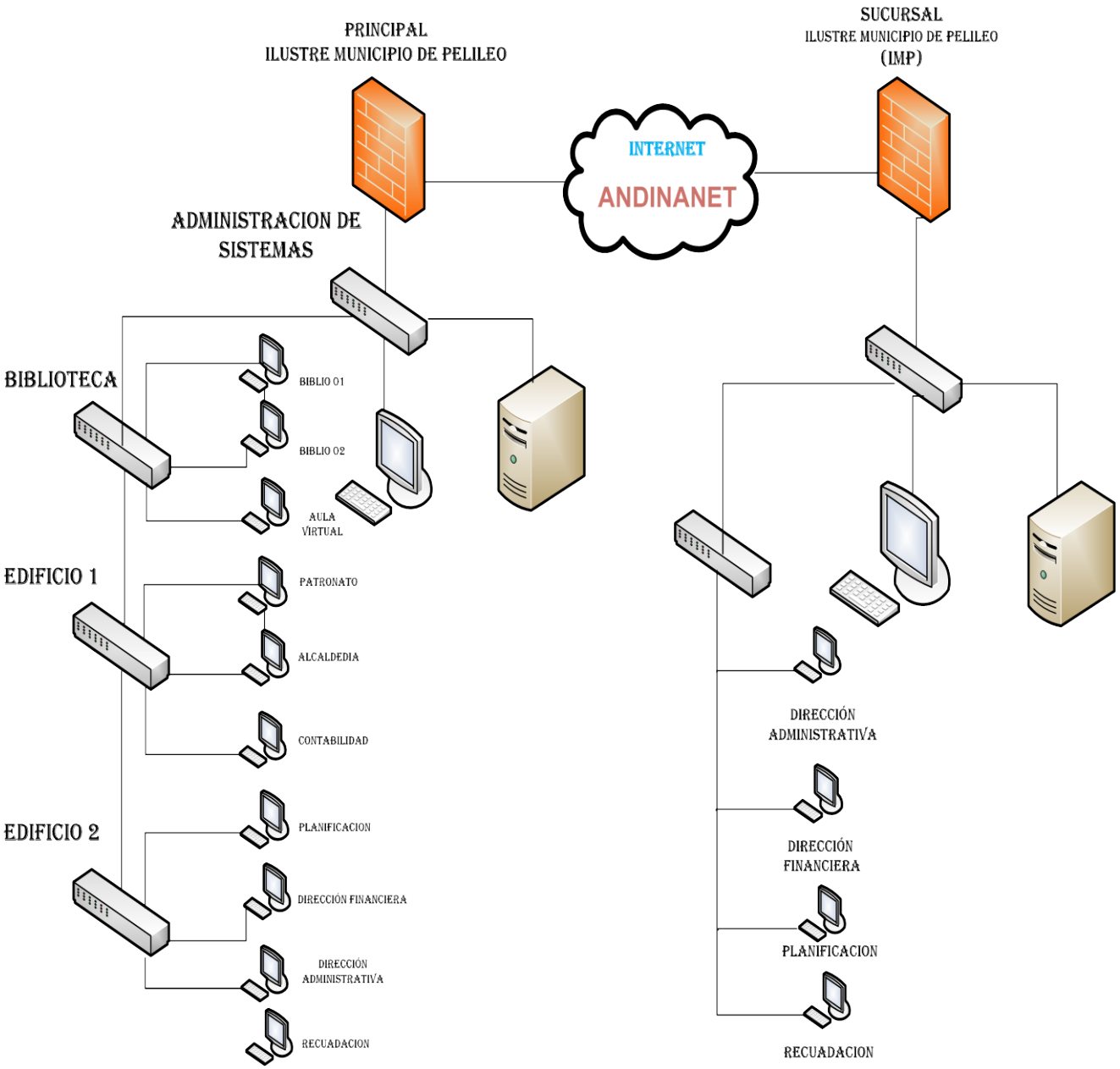

Figura 6.1 Diagrama Red del Municipio de Pelileo

La IMP principal consta de tres edificios como son: Edificio1, Edificio 2 y Biblioteca. Además el IMP Sucursal consta de un solo edificio

El objetivo del presente proyecto es proporcionar seguridad en un canal público creando un túnel con autenticación en las tramas de los protocolos de modo que la nueva red se verá de la siguiente forma.

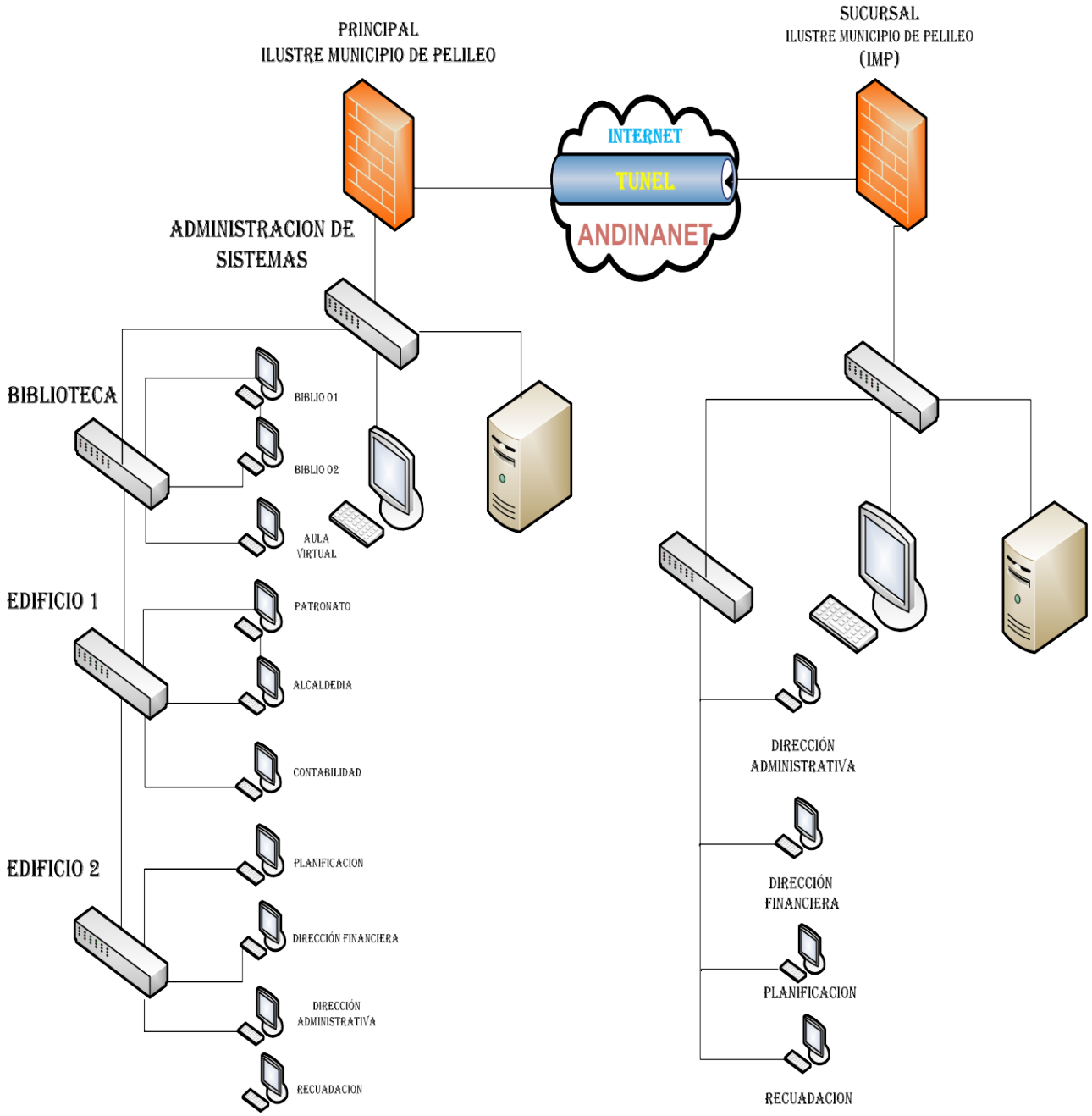

Figura 6.2 Túnel Virtual que Interconecta las Sucursales en el Municipio de Pelileo

Requerimientos generales de instalación y seguridad.

Las máquinas que van a trabajar como Routers van a tener como sistema operativo IPCop v.1.4.20 deben cumplir con los siguientes requerimientos.

Sistema/Hardware	Requerimiento/recomendaciones	
Procesador	Intel Pentium o procesadores compatibles.	
Memoria RAM	256 megabytes.	
Almacenamiento	4 gigabytes de disco duro. Soporta dos tipos de dispositivos IDE y SCSI.	
Interfaz de Red	La conexión a internet es a través de un dispositivo de banda ancha como un cable módem, ADSL, por lo que se requiere dos tarjetas de red NIC.	
Teclado	Compatible con el Hardware y Sistema Operativo.	
Tarjeta de Video	Requerida sólo al instalar Icop.	
Monitor	Requerida sólo al instalar Icop.	
CD-ROM	Requerida sólo al instalar Icop.	
Floppy	Necesario solo para versiones anteriores.	
Tipo de conexión a internet	Internet	Una NIC adecuada es requerida.
	EMPRESA	ANDINANET
	Conexión ADSL	Una tarjeta PCI compatible o un módem USB es requerido.
	Velocidad	1Mbps x 512Kbps Canal 2 a 1
	Direccionamiento IP	IP 190.152.11.121/30 190.152.11.122 Privado 10.162.64.0/ 24 10.162.66.0 / 24 MUNICIPIO PELILEO PRINCIPAL RED 190.152.11.121/30 GREEN 10.162.64.1/24 MUNICIPIO PELILEO SUCURSAL RED 190.152.11.122/30 GREEN 10.162.66.1/24

Tabla 6.1 Hardware y Software Requerido.

Instalación y configuración de componentes.

Instalando IPCop v.1.4.20.

Para realizar la instalación es necesario seguir los siguientes pasos:

Paso 1: Arranque
Insertar el CD con el software IPCop en el drive CD ROM, si no tiene el software, descargarlo de la siguiente dirección http://sourceforge.net/projects/ipcop/files/ y luego grabar en el CD. Vemos la ventana que aparece al arrancar el instalador.

Figura 6.3 Instalación de IPCop v.1.4.20

Paso 2: Idioma

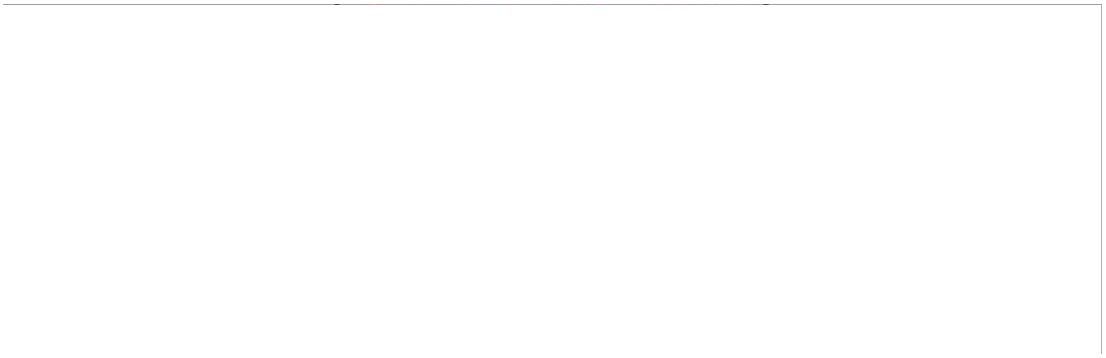

Figura 6.4 Idioma de IPCop v.1.4.20.

Paso 3: Bienvenida

Figura 6.5 Bienvenida de IPCop v.1.4.20.

Paso 4: Respaldo

Figura 6.6 Selección del respaldo.

Paso 5: Configuración De Red

Figura 6.7 Inicio de la Configuración de Red.

Paso 6: Identificación Primera Nic

Figura 6.8 Primera NIC

Paso 7: Ip Para Nic Verde Municipio Principal

Figura 6.9 IP NIC verde Municipio Principal

Paso 8: Ip Para Nic Verde Municipio Sucursal

Figura 6.10 IP NIC verde Municipio Sucursal

Paso 9: Nombre Router Municipio Principal

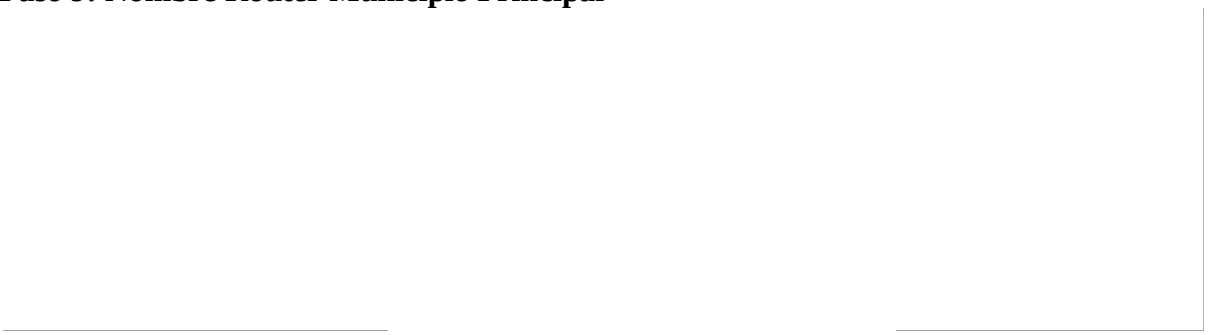

Figura 6.11 Router Municipio Principal

Recomendación para nombres de Host: Por seguridad es necesario utilizar sólo caracteres en minúsculas con en el nombre del host. Usted está permitido utilizar guiones “-“ y puntos “.”. Pero No puede utilizar números, espacios, guiones bajos ‘_’ o cualquier otro signo de puntuación “.”.

Paso 10: Nombre Router Municipio Sucursal

Figura 6.12 Router Municipio Sucursal

Paso 11: Menú Configuración De Red

Figura 6.13 Menú de Configuración de Red

Paso 12: Elección De Tipo De Configuración De Red

Figura 6.14 Tipo de Configuración de Red

IPCop v.1.4.20 es compatible con los siguientes tipos de configuración de red que a continuación se explica detalladamente:

Tipo	Explicación
Green (Red is modem/ISDN)	Seleccione si IPCop v.1.4.20 Express utilizará: • Una tarjeta de interfaz de red (NIC) para conectarse a la red interna que está protegiendo. • Una tarjeta de módem o RDSI para conectarse a internet o red externa.
Green + Orange (Red is modem/ISDN)	Seleccione si IPCop v.1.4.20 Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una zona desmilitarizada. • Una tarjeta de módem o RDSI para conectarse a internet o red externa.
Green +Red	Seleccione si IPCop v.1.4.20 Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a internet o red externa.
Green + Orange + Red	Seleccione si IPCop v.1.4.20 Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una zona desmilitarizada. • Una tarjeta NIC para conectarse a internet o red externa.
Green + Purple (Red is modem/ISDN)	Seleccione si IPCop v.1.4.20 Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una red inalámbrica. • Una tarjeta de módem o RDSI para conectarse a internet o red externa.
Green + Purple + Orange (Red is modem/ ISDN)	Seleccione si IPCop v.1.4.20 Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una red inalámbrica. • Una tarjeta NIC para conectarse a una zona desmilitarizada. • Una tarjeta de módem o RDSI para conectarse a Internet o red externa.
Green + Purple + Red	Seleccione si IPCop v.1.4.20 Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una red inalámbrica. • Una tarjeta NIC para conectarse a Internet o red externa.
Green + Purple + Orange + Red	Seleccione si IPCop v.1.4.20 Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una red inalámbrica. • Una tarjeta NIC para conectarse a una zona desmilitarizada. • Una tarjeta NIC para conectarse a Internet o red externa.

Tabla 6.2 Tipos de Configuración de Red.

En nuestro caso seleccionamos green + red (verde + rojo) porque esta configuración se ajusta efectivamente para nuestro tipo de diseño ya que se requiere proteger la red interna mientras se está conectado al internet

PASO 13: Configuración de Red GREEN + RED

Figura 6.15 Menú de Configuración de Red GREEN + RED

Paso 14: Interfaz Green

Figura 6.16 Interfaz GREEN previamente reconocida y asignada

Paso 15: Interfaz RED

Figura 6.17 Interfaz RED

Paso 16: Finalización de asignación de Tarjetas.

Figura 6.18 Tarjetas Asignadas con Éxito

Paso 17: Configuración De Direcciones

Figura 6.19 Configuración de direcciones IP

Paso 18: Asignación De Direcciones Ip

Figura 6.20 Selección de Interfaz

Paso 19: Asignación a Interfaz Roja Municipio Principal

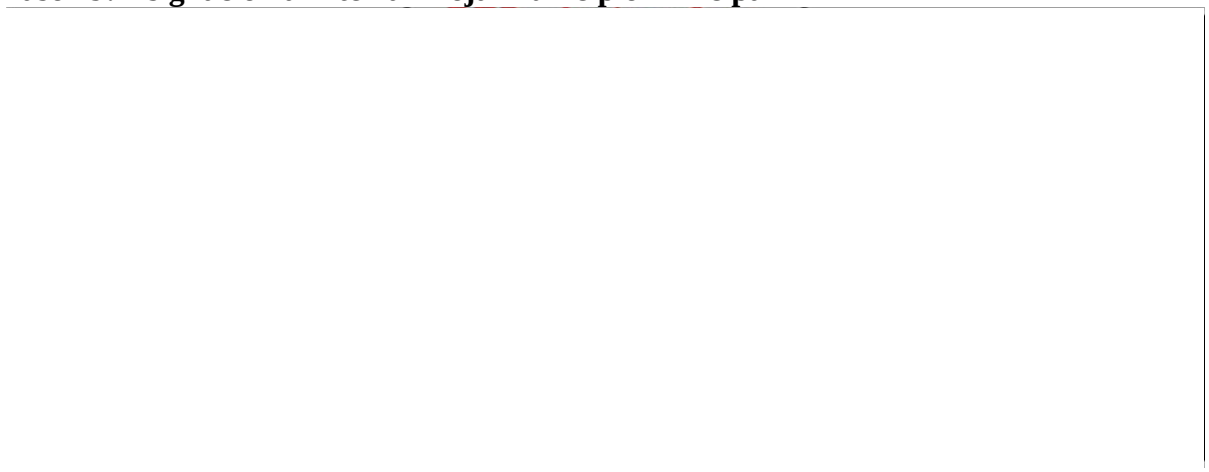

Figura 6.21 IP de Interfaz Roja Municipio Principal

Paso 20: Asignación a Interfaz Roja Municipio Sucursal

Figura 6.22 IP de Interfaz Roja Municipio Sucursal

Paso 21: Fin configuración de Direcciones

Figura 6.23 Finalizando la Configuración de Interfaces

Paso 22: Contraseña ROOT

Figura 6.23 Contraseña de root

Recomendación para contraseñas:	**Escriba una contraseña segura para la cuenta de administrador.** **Mínimo = 6 caracteres** **Máximo = 25 caracteres**
Las contraseñas de ROOT para las sucursales del municipio son:	Contraseña ROOT Municipio Principal: municipioprincipal Contraseña ROOT Municipio Sucursal: municipiosucursal
Importante	La contraseña de ROOT posee el control total de IPCOP y se utiliza para iniciar sesión en la consola de IPCop.

Tabla 6.3 Contraseñas de ROOT.

Paso 23: Contraseña ADMINISTRADOR

Figura 6.25 Contraseña de Administrador

Las contraseñas de ADMINISTRADOR para las sucursales del municipio son:	**Contraseña ADMINISTRADOR Municipio Principal: adminprincipal** **Contraseña ADMINISTRADOR Municipio Sucursal: adminsucursal**
Importante	La contraseña de administrador se utiliza para acceder remotamente a IPCop desde un cliente con un navegador web y realizar la rutina de configuración y gestión.

Tabla 6.4 Contraseñas de ADMINISTRADOR.

Paso 24: Fin De Instalación

Figura 6.26 Fin de la Instalación

Paso 25: Arrancando IPCop

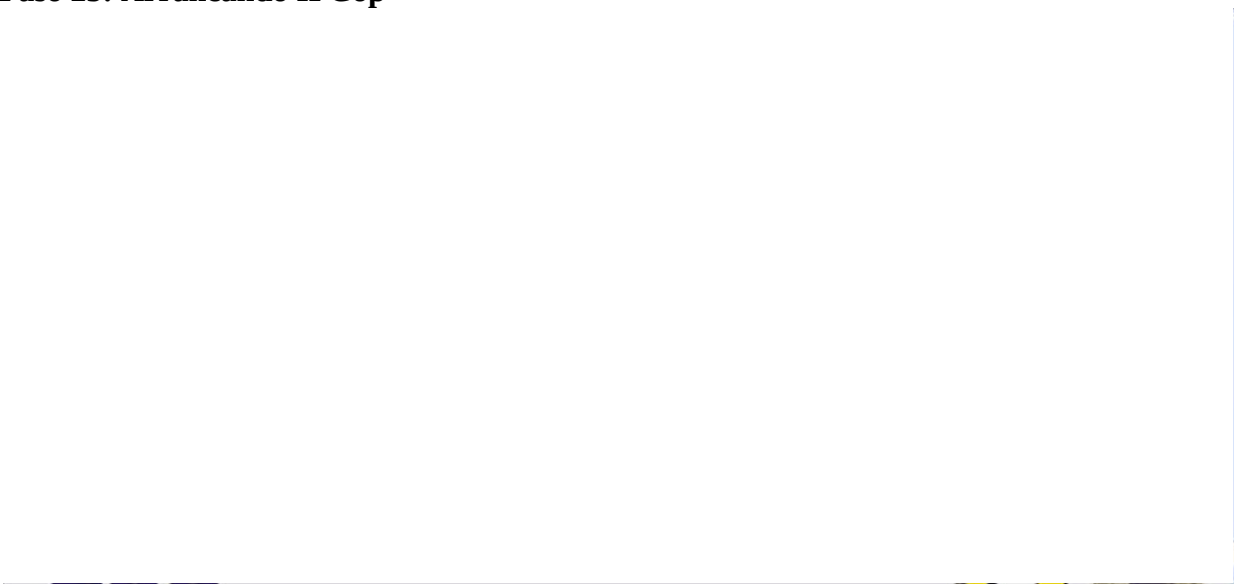

Figura 6.27 Arranque de IPCop por primera vez.

Acceso a IPCop por Primera vez desde un Terminal Remoto

Paso 1: Accediendo a IPCop desde el navegador Web de un Cliente.

Utilizando un navegador a su elección, escriba la dirección IP de la interfaz verde de su router IPCop.

Figura 6.28 Ubicando la Dirección en el Navegador Web

Paso 2: Autenticación IPCop

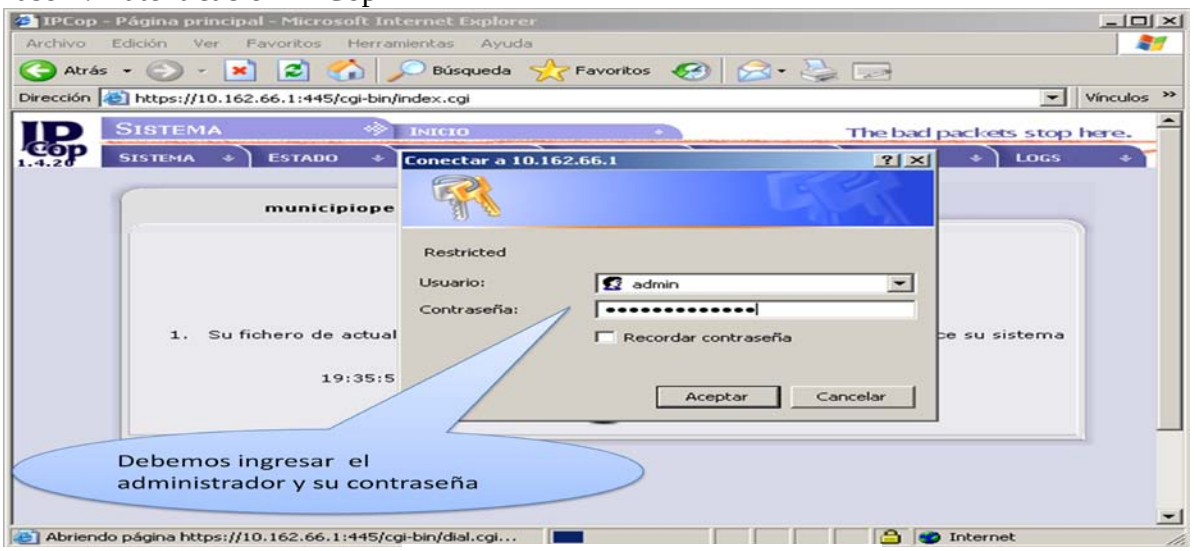

Figura. 6.29 Autenticación en IPCop.

Información que debe ingresar:

CAMPO	INFORMACIÓN
Usuario	Ingrese admin. Este es el nombre por defecto de la cuenta de administración de IPCop v.1.4.20.
Contraseña	Ingrese la contraseña que especificó para la cuenta admin durante la instalación de IPCop v.1.4.20.
Importante	Este proceso se lo realiza tanto en el IPCop del Municipio Principal como del Municipio Sucursal.

Tabla 6.5 Autenticación en IPCop.

Paso 3: Página Principal de IPCop

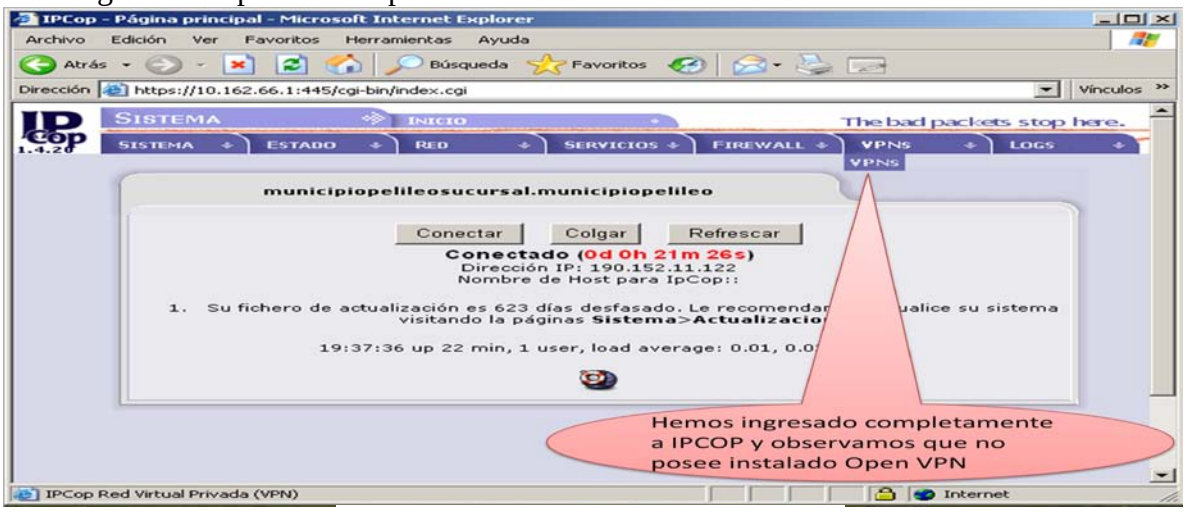

Figura. 6.30 Página principal de IPCop.

Instalación de Zerina

IPCop no viene cargado con la herramienta para crear el túnel virtual que necesitamos para proporcionar la seguridad requerida a nivel de protocolos.

El software Zerina se lo puede descargar de: http://www.zerina.de/zerina/files/alpha/ZERINA-0.9.7a14-Installer.tar.gz .

Para cargar la herramienta requerida es necesario instalar Zerina en IPCop. En este caso se debe realizar una conexión remota a IPCOP para cargar el software Zerina en su sistema operativo para ello utilizamos WinSCP.

El software WinSCP lo puede descargar de:

http://sourceforge.net/projects/winscp/files/WinSCP/4.2.7/winscp427setup.exe/download

Paso 1: Arranque WinSCP

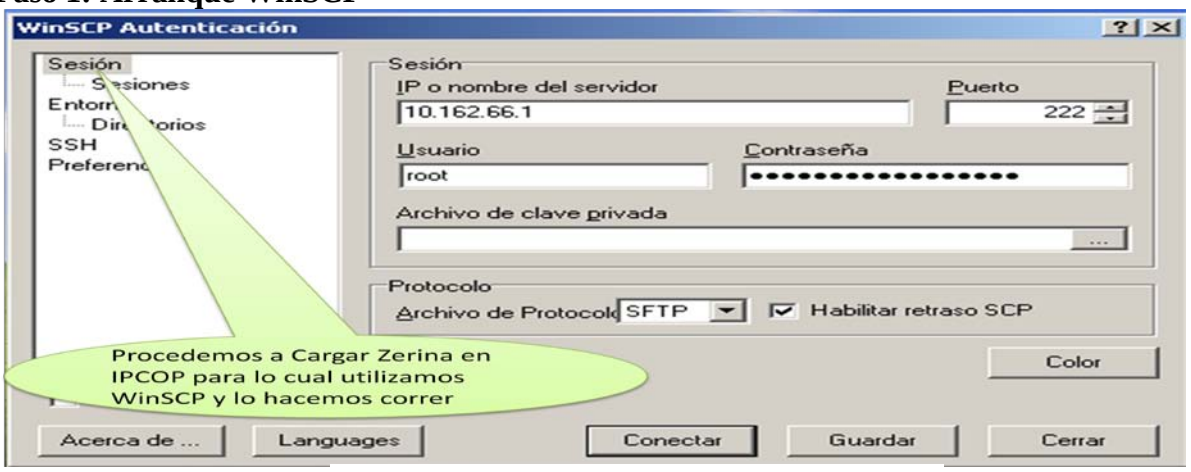

Figura. 6.31 Arranque de WinSCP en el cliente.

Arrancamos WinSCP e ingresamos la siguiente información.

CAMPO	INFORMACIÓN
IP o nombre del servidor	Ingresamos la dirección 10.162.64.1 para Municipio Principal, ó 10.162.66.1 para Municipio Sucursal
puerto	Cualquier puerto, de preferencia el 222
usuario	root
contraseña	La requerida para la sucursal en cuestión

Tabla 6.6 Información de Arranque de WinSCP

Paso 2: Accesando a IPCop

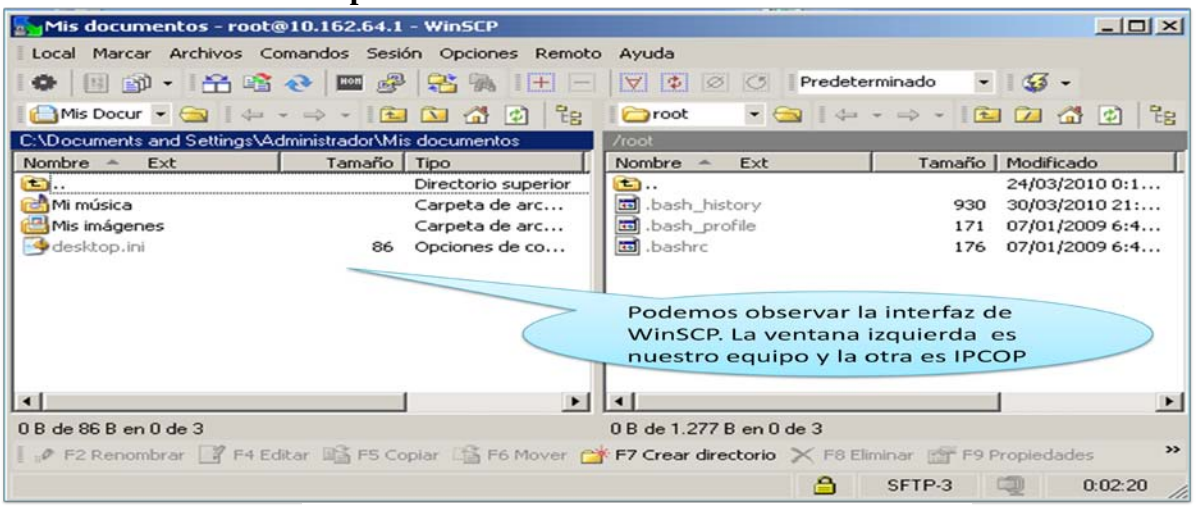

Figura. 6.32 Accesando a IPCop mediante WinSCP.

Paso 3: Buscando Zerina

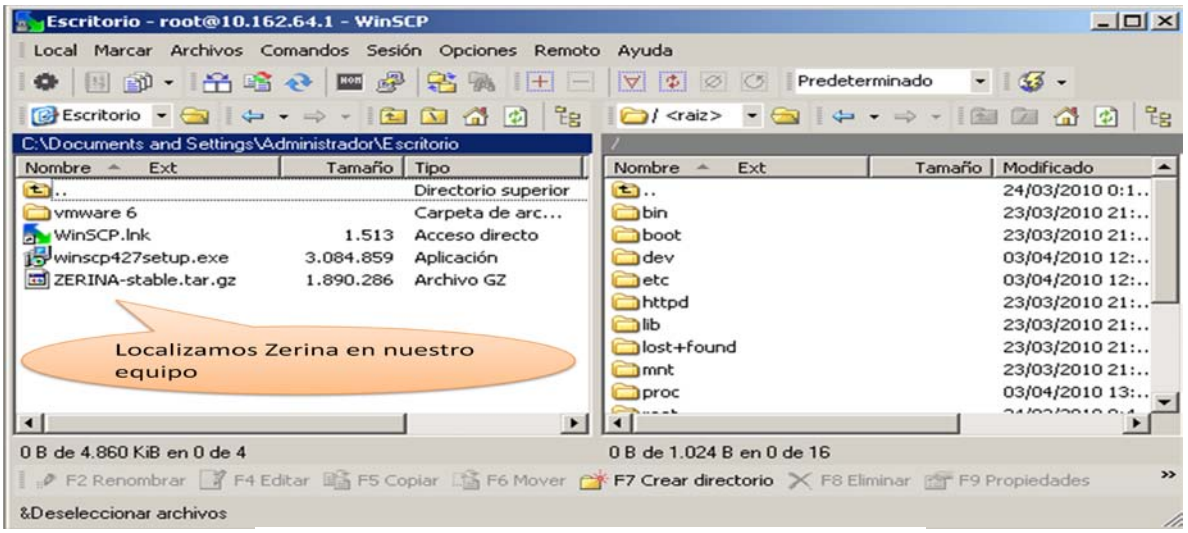

Figura. 6.33 Buscando Zerina en la máquina cliente.

Paso 4: Copiando Zerina

Figura. 6.34 Copiando Zerina en IPCOP.

Paso 5: Zerina ya copiado

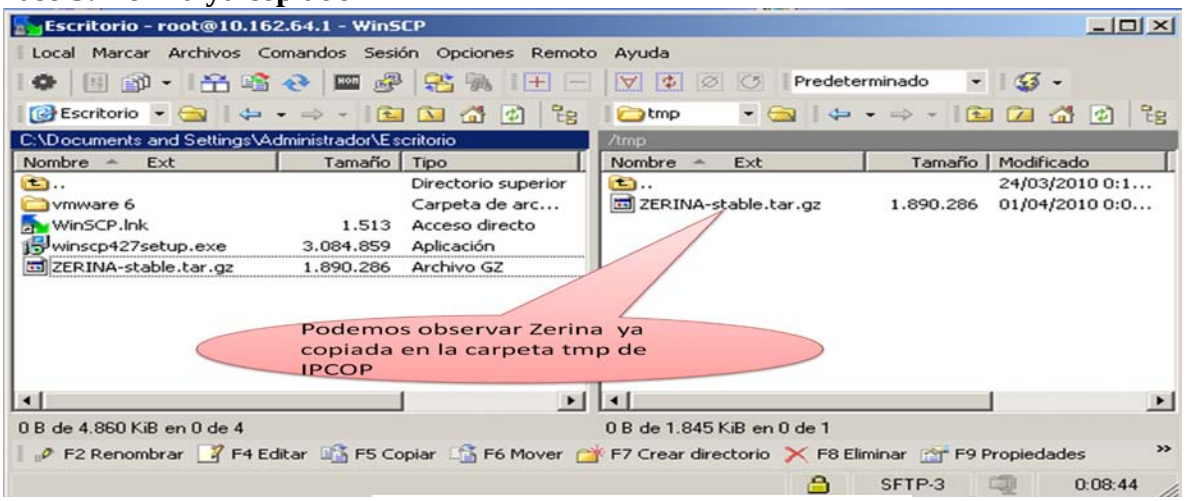

Figura. 6.35 Zerina ya copiado en IPCOP.

Paso 6: Ubicando Zerina por la Consola

Luego de haber cargado Zerina en IPCop es necesario dirigirnos a la consola de IPCop para instalarlo completamente

Figura. 6.36 Ubicando Zerina por la Consola

Paso 7: Descomprimiendo Zerina

Descomprimimos con la instrucción:

tar xzvf ZERINA-0.9.7a14-Installer.tar

Figura. 6.37Descomprimiendo Zerina.

Paso 8: Arranque de la Instalación

Figura. 6.38 Arranque de la instalación Zerina.

Paso 9: Ventana de Arranque

Figura. 6.39 Ventana de Arranque de Zerina.

Paso 10: Modificación de Versión

Figura. 6.40 Modificación de Versión.

Paso 11: Fin de la Instalación

Figura. 6.41 Fin de Instalación de Zerina.

Paso 12: Verificación de la Instalación

Figura. 6.42 Verificación de Zerina instalado en IPCop

Es importante mencionar que este proceso se debe realizar en los Routers IPCop de las dos sucursales tanto en el Municipio Principal como en el Sucursal.

Creación del Túnel Virtual

Configurando el Municipio Principal

Paso 1: Autoridades Certificadoras

Es necesario crear los correspondientes certificados, para ellos presionaremos sobre el botón **"Generar certificados de Raíz/Anfitrión"**, y aparece la siguiente imagen:

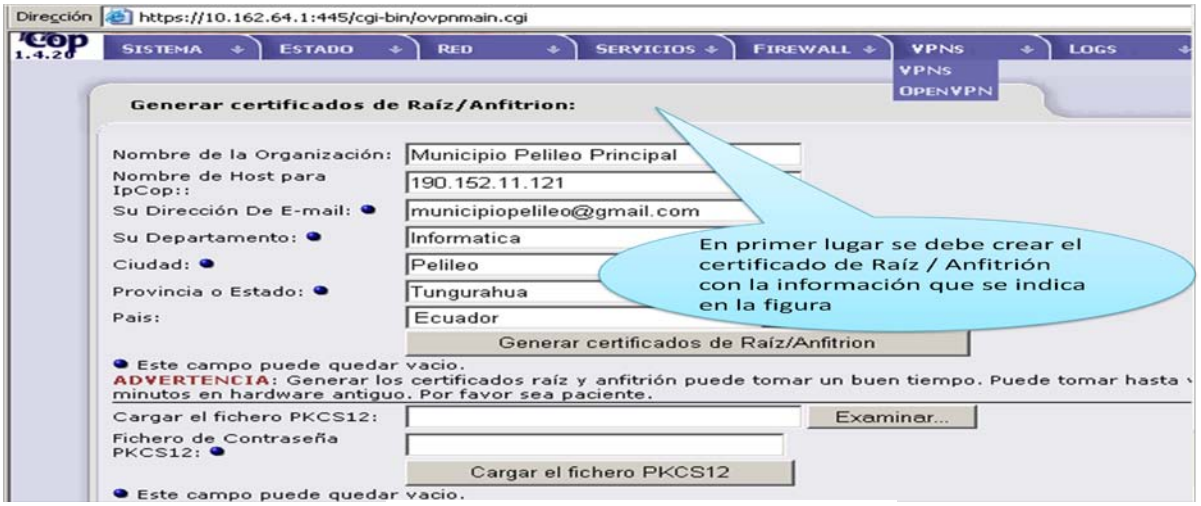

Figura. 6.42 Autoridades certificadoras.

En la siguiente tabla se detalla la información más importante que se debe ingresar:

CERTIFICADO RAÍZ / ANFITRION

CAMPO	INFORMACIÓN
Nombre de la Organización	Municipio Pelileo Principal
Nombre de Host para IPCop	190.152.11.121
Su dirección de E-mail	municipiopelileo@gmail.com
Su Departamento	Informatica
Ciudad	Pelileo
Provincia o Estado	Tungurahua
País	Ecuador

Tabla 6.7 Información Certificado Raíz

Finalmente se crea los certificados se muestran en la página principal, en la sección correspondiente.

Paso 2: Tipo De Conexión

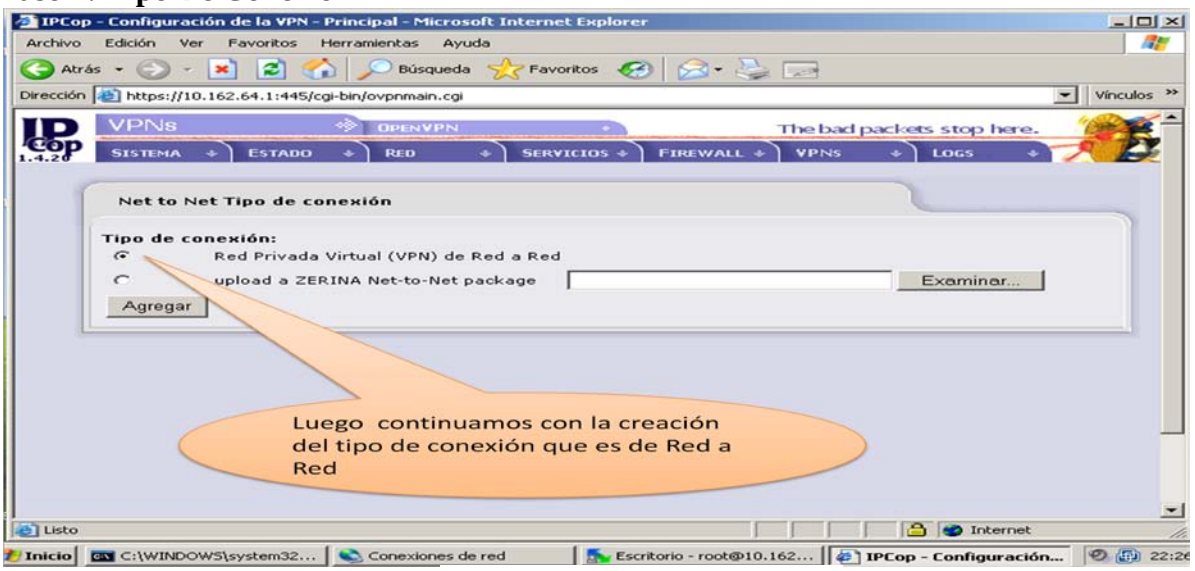

Figura. 6.43 Tipo de Conexión.

Paso 3: Información Municipio Pelileo

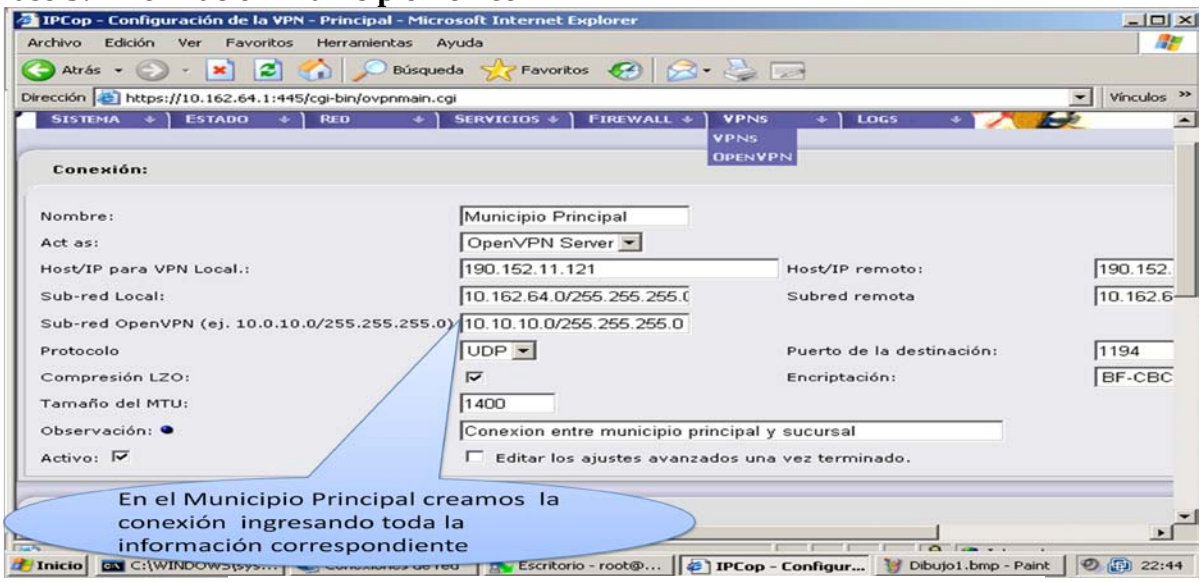

Figura. 6.44 Información de Conexión Municipio Principal (a) .

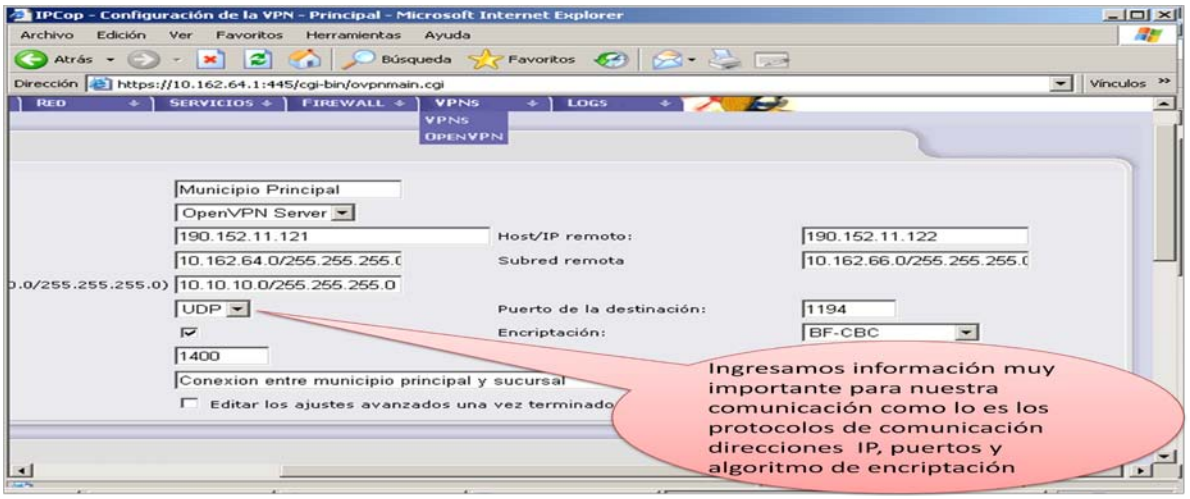

Figura. 6.45 Información de Conexión Municipio Principal (b).

En la siguiente tabla se detalla la información más importante que se debe ingresar:

CAMPO	INFORMACIÓN
Nombre	Municipio Principal
Act as	Open VPN Server
Host/IP para VPN local	190.152.11.121 (Interfaz Roja del Municipio Principal)
Sub-red local	10.162.64.0/255.255.255.0 (Interfaz Verde del Municipio Principal)
Sub-red OpenVPN	10.10.10.0/255.255.255.0 (Es nuestra red virtual que crea el túnel)
Protocolo	UDP (Protocolo utilizado para proporcionar la seguridad)
Compresión LZO	Marcamos esta opción, para que la conexión sea más eficiente
Tamaño MTU	1400 (Valor por defecto)
Observación	Conexión entre municipio principal y sucursal
Activo	Marcamos esta opción, para que la conexión permanezca activa
Host/IP remoto	190.152.11.122 (Interfaz Roja del Municipio Sucursal)
Sub-red remota	10.162.66.0/255.255.255.0 (Interfaz Verde del Municipio Sucursal)
Puerto de la destinación	1194 (Puerto que e utiliza para la conexión y se puede cambiar por políticas de seguridad)
Ecriptación	BF-CBC (Algoritmo seleccionado por su versatilidad)

Tabla 6.8 Información Municipio Principal

Paso 4: Archivo De Autenticación

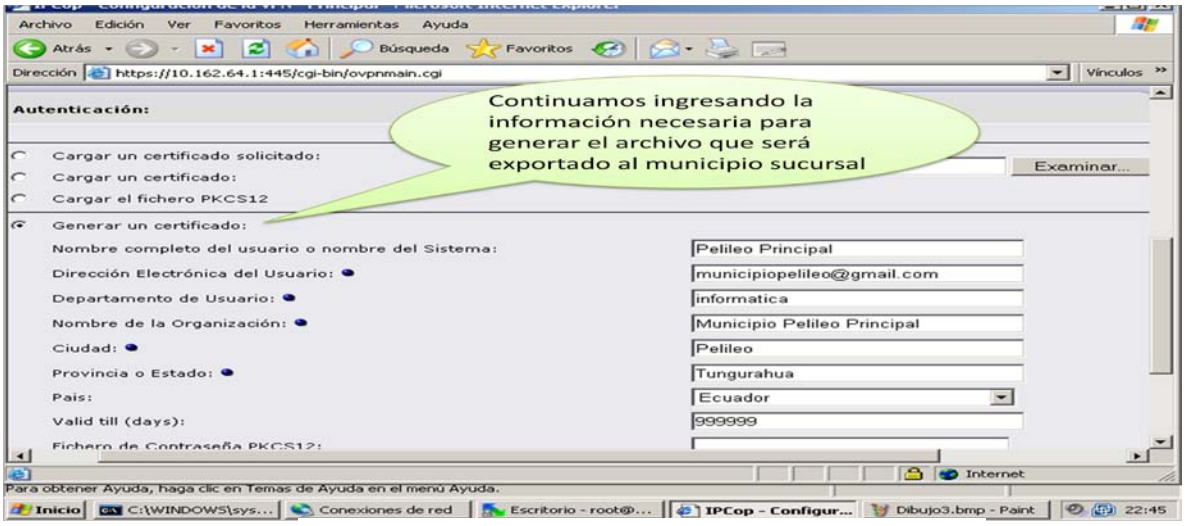

Figura. 6.46 Generación de Archivo de Autenticación

En la siguiente tabla se detalla la información más importante que se debe ingresar:

CAMPO	INFORMACIÓN
Nombre completo del usuario o nombre del Sistema	Pelileo Principal
Dirección Electrónica del Usuario	municipiopelileo@gmail.com
Departamento de Usuario	Informática
Nombre de la Organización	Municipio Pelileo Principal
Ciudad	Pelileo
Provincia o Estado	Tungurahua
País	Ecuador
Valid til (days) / Válido hasta (días)	999999

Tabla 6.9 Información Certificado Municipio Principal

Paso 5: Seleccionando Guardar

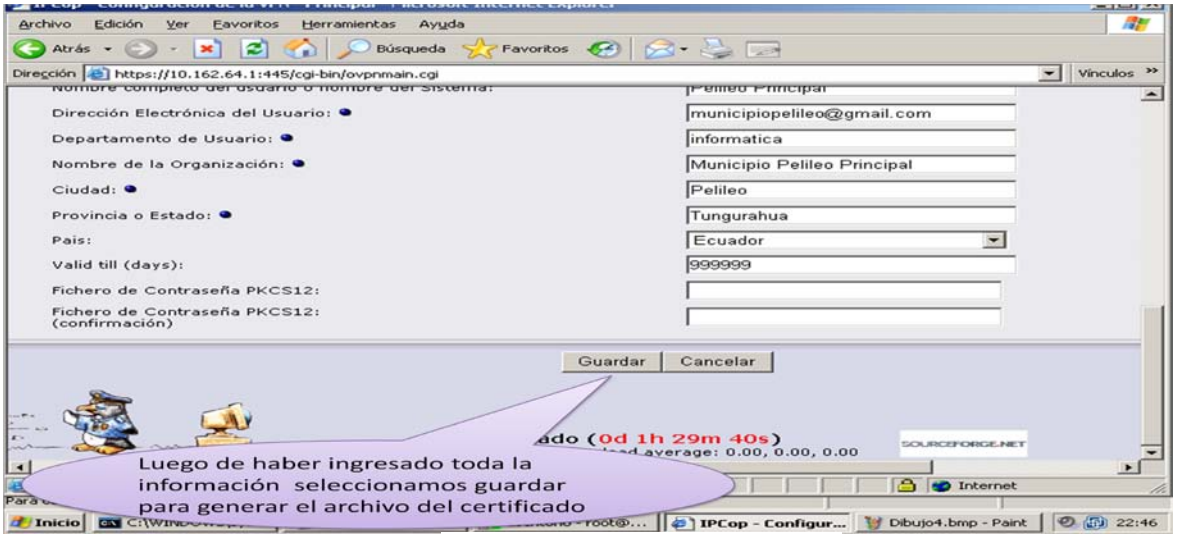

Figura. 6.47 Selección Guardar

Paso 6: Ejecutando Guardar

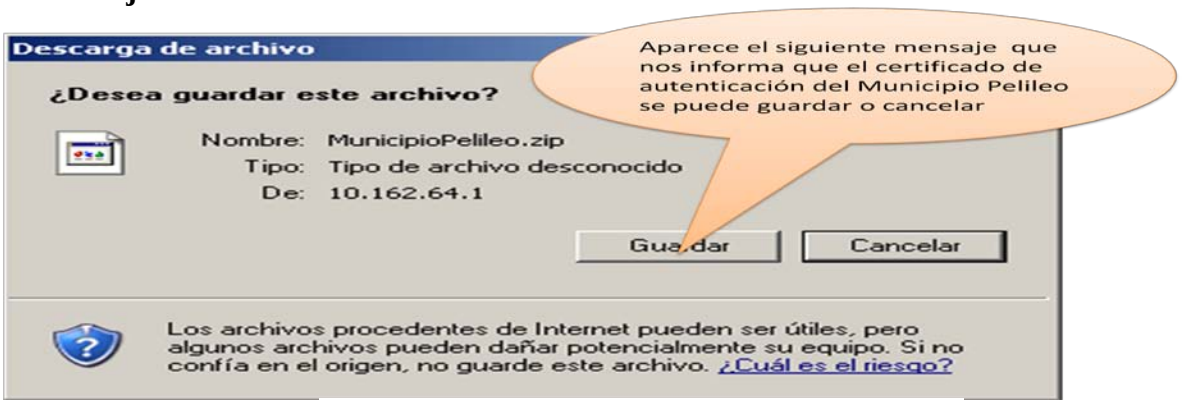

Figura. 6.48 Guardando Archivo de Autenticación

Paso 7: Archivo De Autenticación

Figura. 6.49 Archivo de Autenticación Guardado en el escritorio

Es importante indicar que este archivo de autenticación se debe cargar en el IPCop del Municipio Sucursal para que los dos extremos del túnel compartan el mismo archivo de autenticación y puedan comunicarse en forma segura.

Configurando el Municipio Sucursal

Paso 1: Certificado Digital

Figura. 6.50 Certificado Raíz / Anfitrión en el Municipio sucursal

PASO 2: Información Certificado Digital

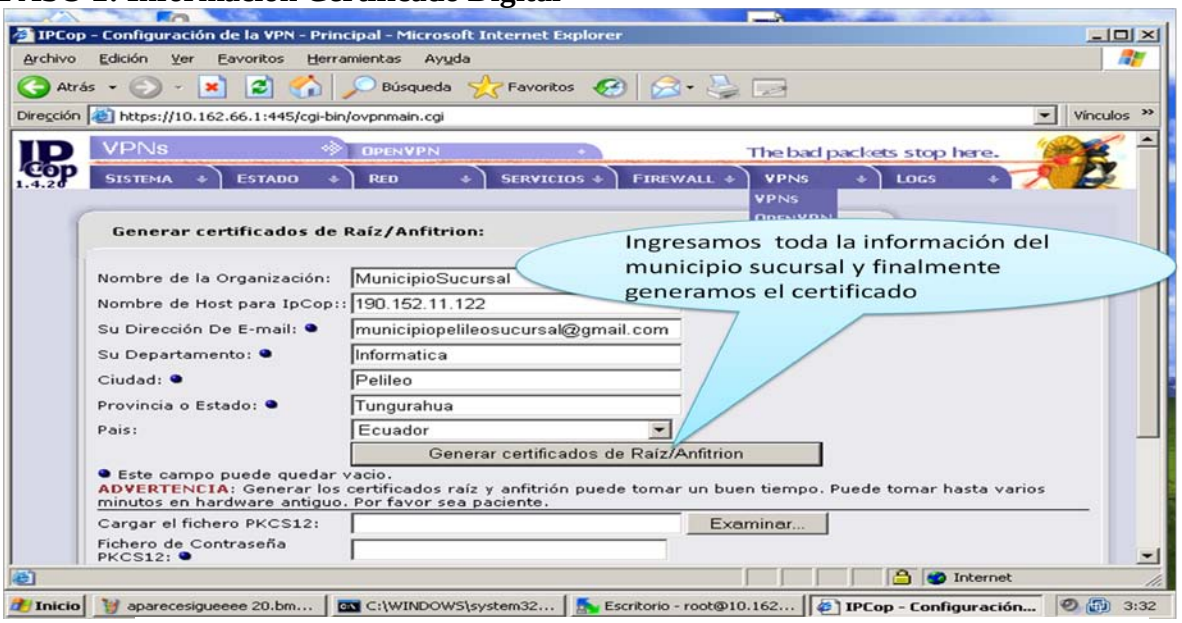

Figura. 6.51 Información Certificado Raíz / Anfitrión en el Municipio Sucursal

En la siguiente tabla se detalla la información más importante que se debe ingresar:

CERTIFICADO RAÍZ / ANFITRIÓN

CAMPO	INFORMACIÓN
Nombre de la Organización	MunicipioSucursal
Nombre de Host para IPCop	190.152.11.122
Su dirección de E-mail	municipiopelileosucursal@gmail.com
Su Departamento	Informatica
Ciudad	Pelileo
Provincia o Estado	Tungurahua
País	Ecuador

Tabla 6.10 Información Certificado Municipio Sucursal

Paso 3: Cargar Archivo De Autenticación

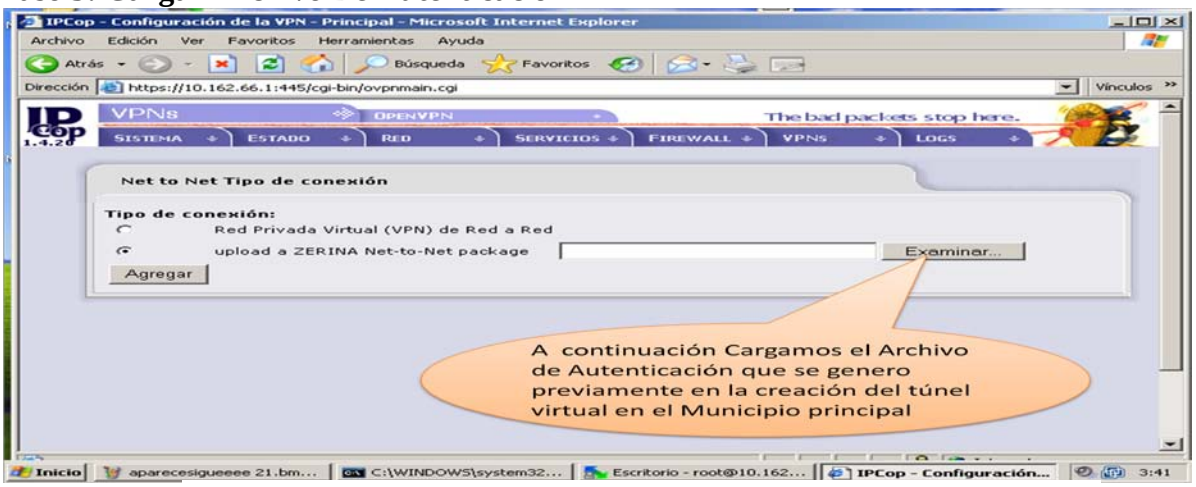

Figura. 6.52 Cargar Archivo de Autenticación en el Municipio Sucursal

Paso 4: Buscando Archivo De Autenticación

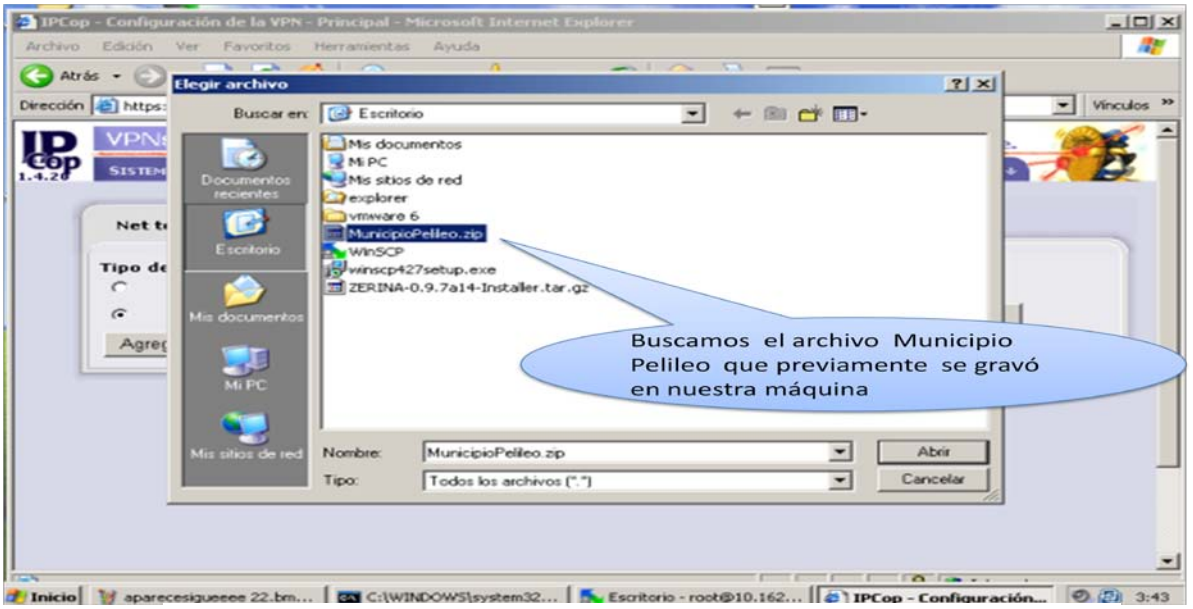

Figura. 6.53 Buscando Archivo de Autenticación en el Municipio Sucursal

PASO 5: Información del archivo de Autenticación Cargado

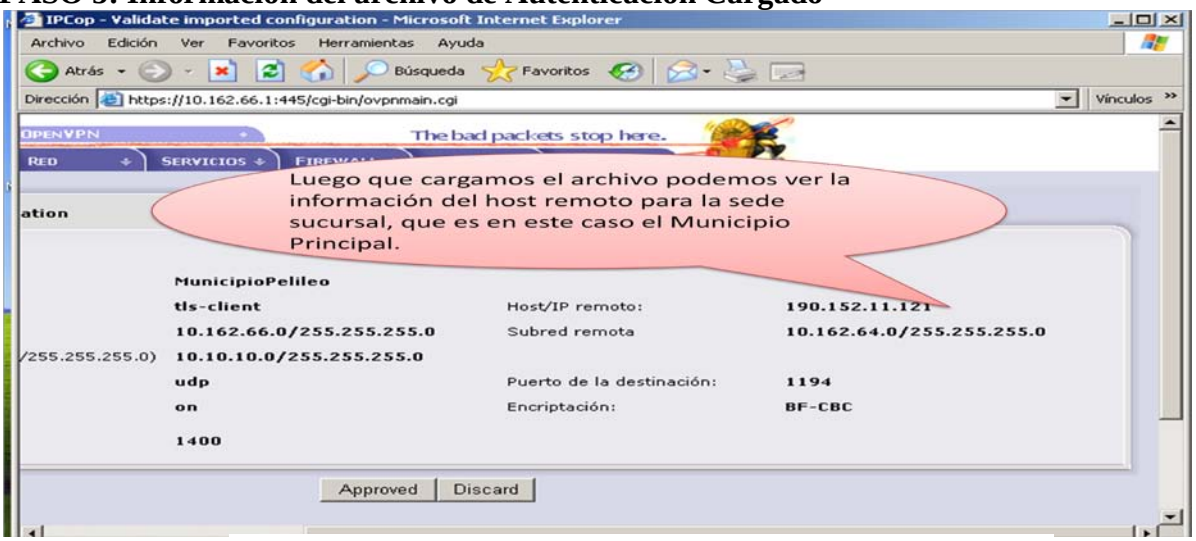

Figura. 6.54 Información del Archivo de Autenticación Cargado

Paso 6: Estado Inicial Del Túnel Virtual.

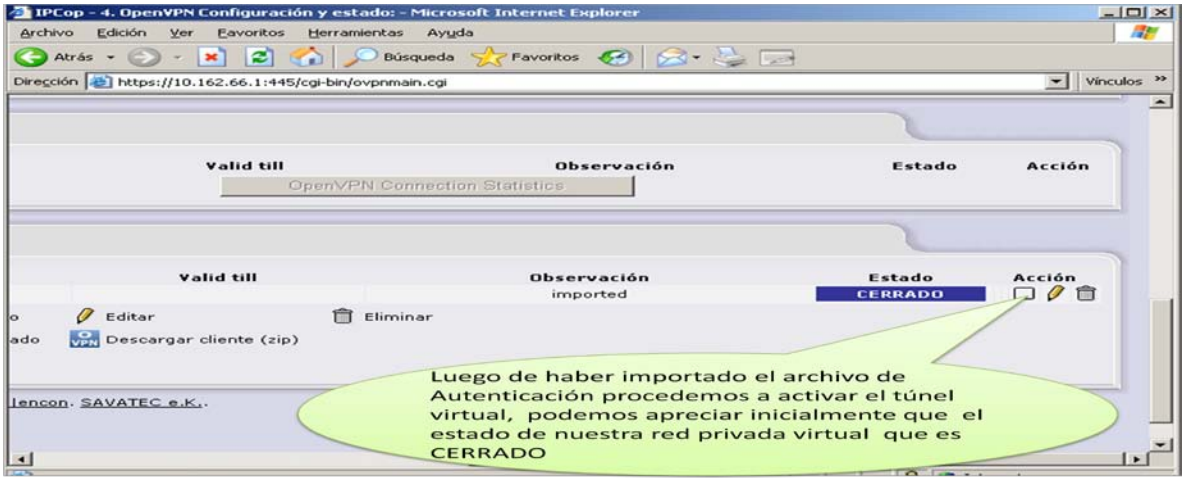

Figura. 6.55 Estado Inicial del Túnel Virtual.

Paso 7: Estado Abierto Del Túnel Virtual

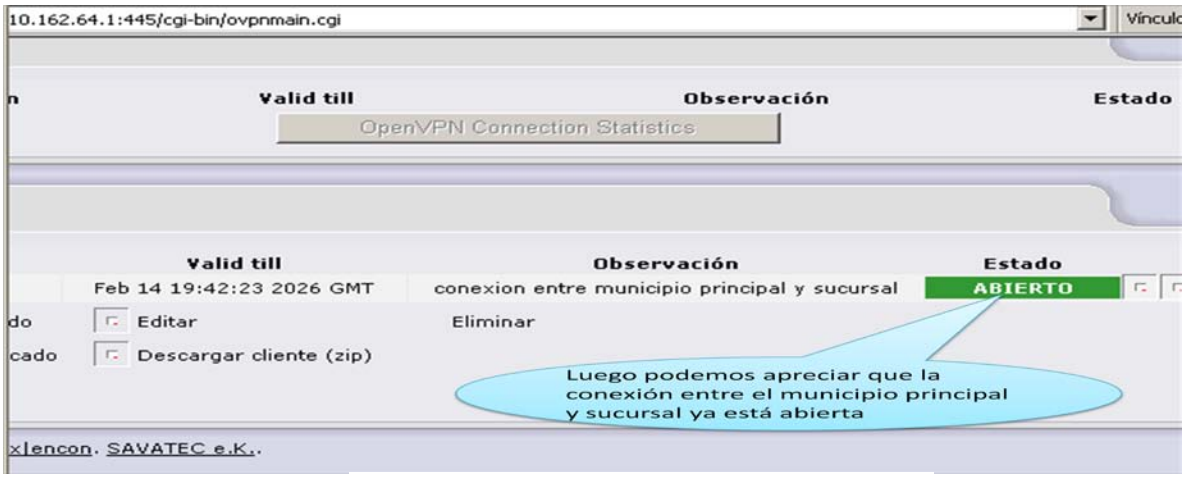

Figura. 6.56 Estado Abierto del Túnel Virtual

Es necesario indicar que al Cambiar el estado de CERRADO a ABIERTO, nos indica que la configuración del Túnel Virtual se ha realizado con éxito y que está trabajando eficientemente brindando seguridad muy efectiva.

6.8 Administración Ejecución de Pruebas

Unos de los puntos principales que han sido siempre motivo de quebraderos de cabeza para adminis tradores y gestores de redes es el tema de la seguridad. La seguridad en la manera de mantener íntegra y salvo toda la información confidencial que viaja através de la misma red, manteniendo cifrados seguros, evitando escuchas ajenas , accesos seguros y un largo etc.

6.8.1 Pruebas de Conectividad.

La conectividad puede ser verificada desde distintos terminales así tenemos:

Desde IPCop que permite identificar las interfaces físicas conectadas, puerto y protocolo.

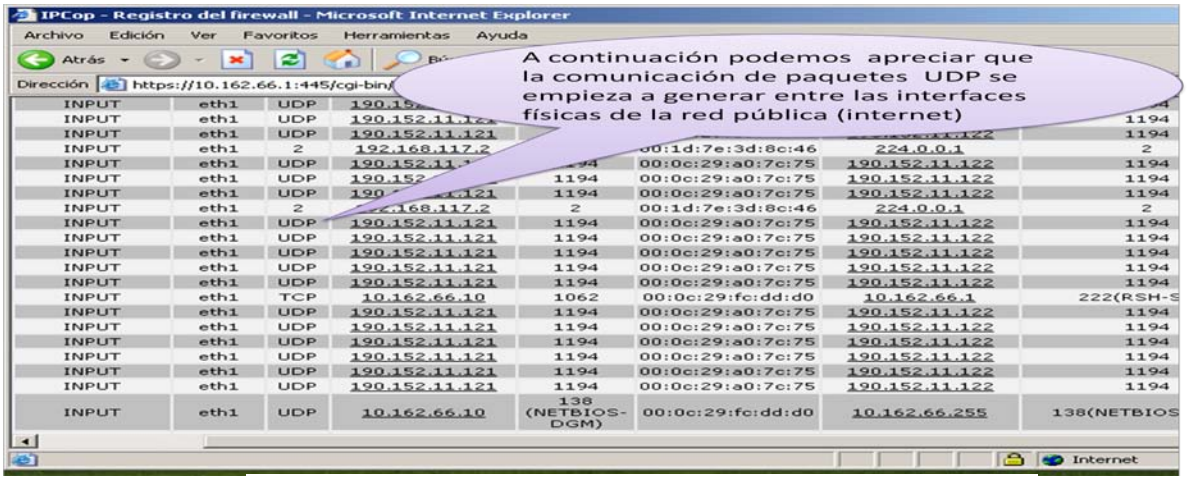

Figura. 6.57 Interfaces Físicas conectadas, Puerto y Protocolo

Haciendo ping a la interface verde del Municipio Principal

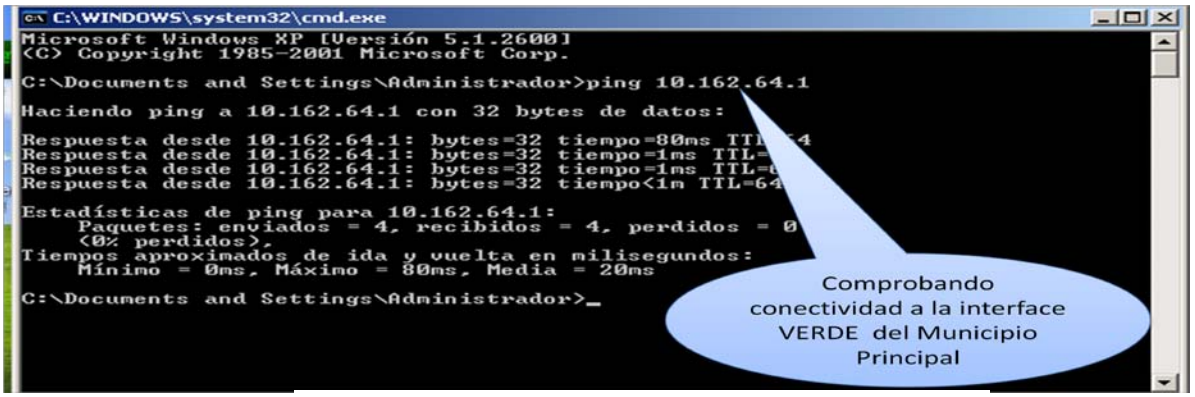

Figura. 6.58 Ping Interface Verde Municipio Principal

Haciendo ping a la interface Roja del Municipio Principal

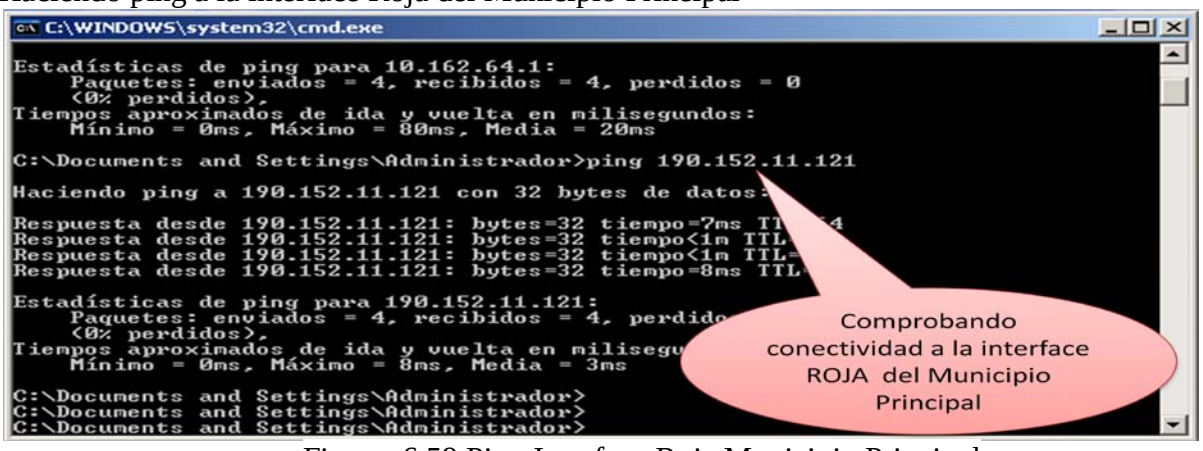

Figura. 6.59 Ping Interface Roja Municipio Principal

Haciendo ping a la interface Roja del Municipio Sucursal

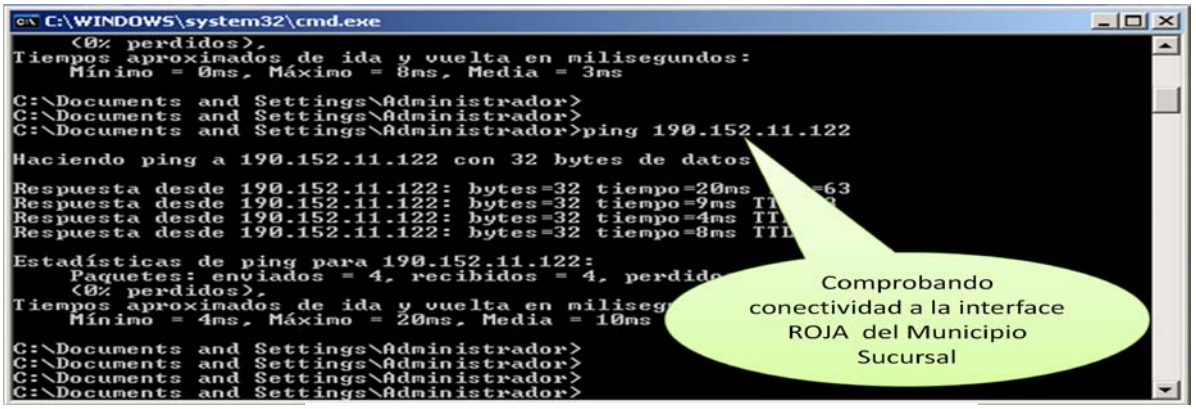

Figura. 6.60 Ping Interface Roja Municipio Sucursal

Haciendo ping a la interface Verde del Municipio Sucursal

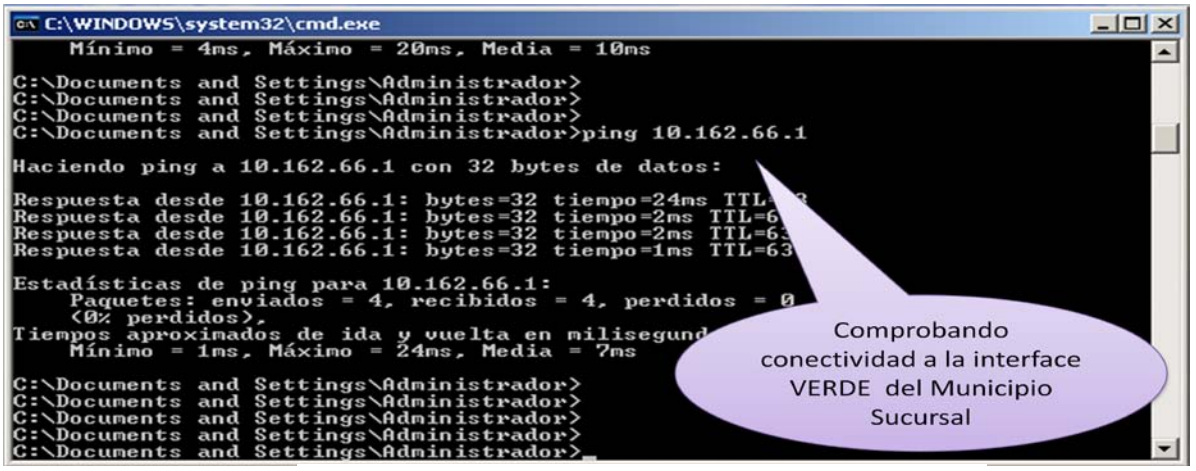

Figura. 6.61 Ping Interface Verde Municipio Sucursal

Haciendo ping a otro Cliente Remoto en el Municipio Sucursal

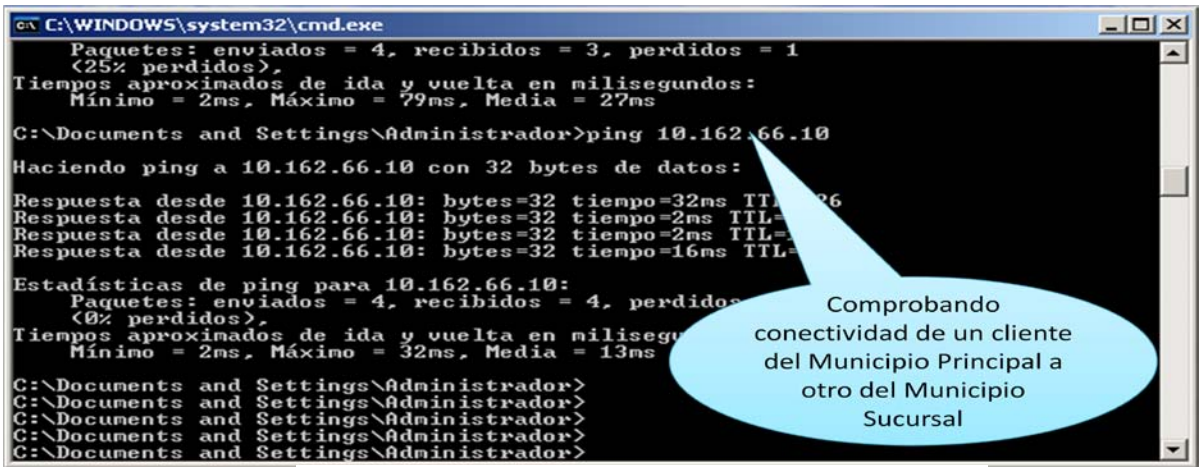

Figura. 6.62 Ping Cliente Remoto Municipio Sucursal

Las pruebas de seguridad nos permitieron determinar que si existe la comunicación eficiente entre las sucursales del Ilustre municipio de Pelileo.

6.8.2 Pruebas de Seguridad frente a Ataques

Para la realización de Hackeo a nuestro túnel virtual se han considerado dos puntos de ataque primordiales así tenemos:

a) Ataque del hacker en la red Pública (Internet)
b) Ataque del Hacker en la LAN Interna

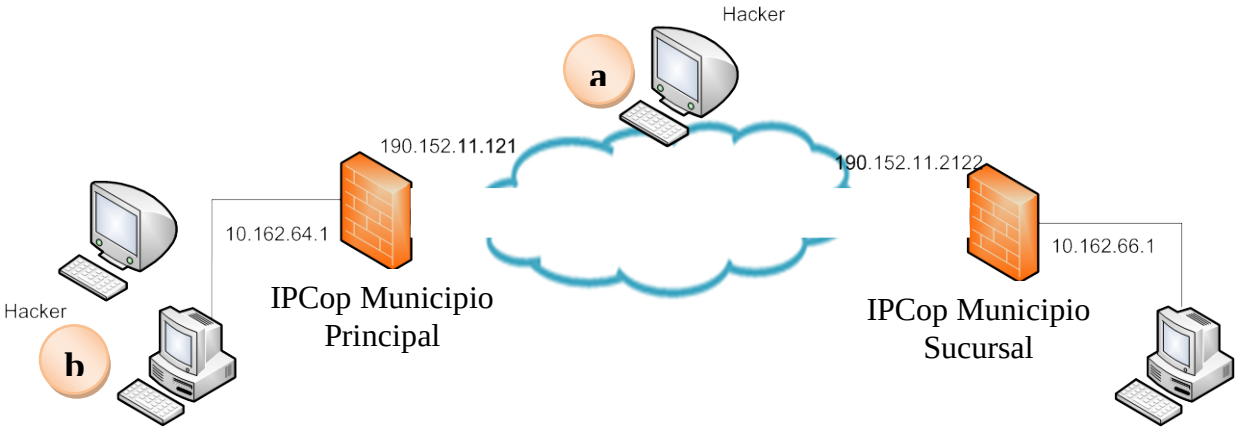

Figura. 6.63 Ping Cliente Remoto Municipio Sucursal

Los ataques que se llevaron a cabo desde los dos puntos estratégicos son los siguientes:

Escaneo de puertos (PORT SCAN)

El término escáner de puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un cortafuego.

El escaneo de puertos es una técnica muy utilizada por hackers y administradores penetrar a un sistema de comunicaciones ya que es la mejor y más efectiva para generar daño en el equipo víctima.

Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos.

Existen varios programas escaneadores de puertos. Así tenemos Port Scan, Nmap, etc. Para este caso utilizamos Port Scan y lo vamos apreciar en ejecución a continuación.

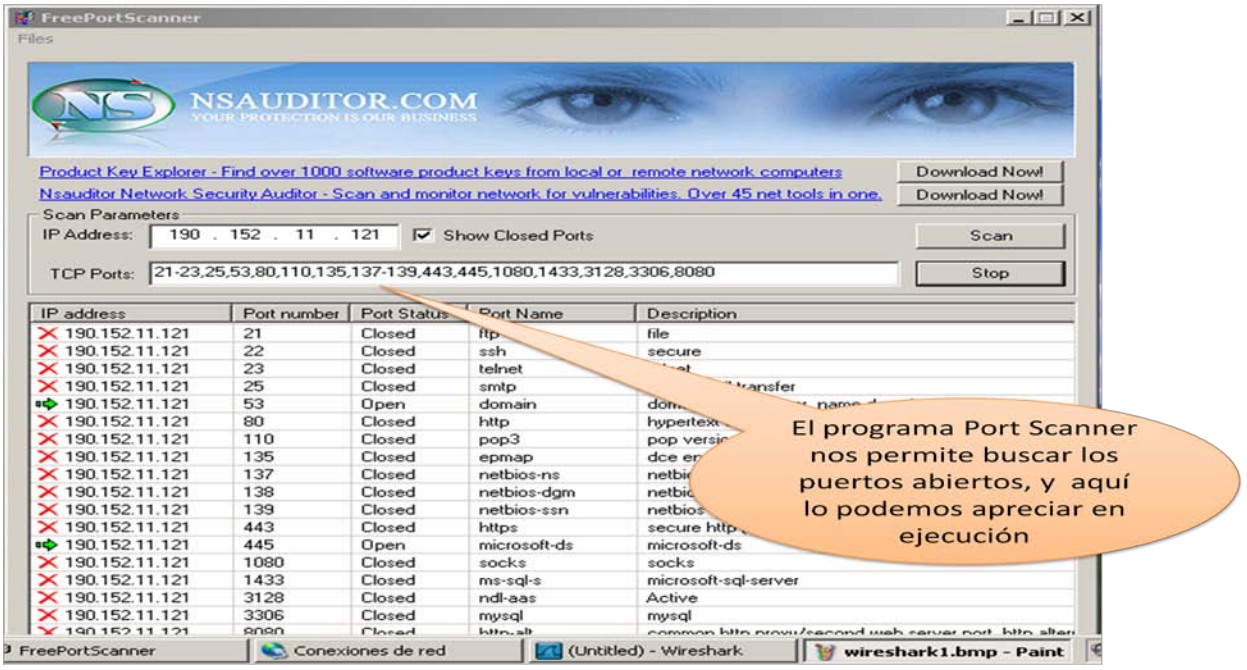

Figura. 6.64 Port Scanner en Ejecución

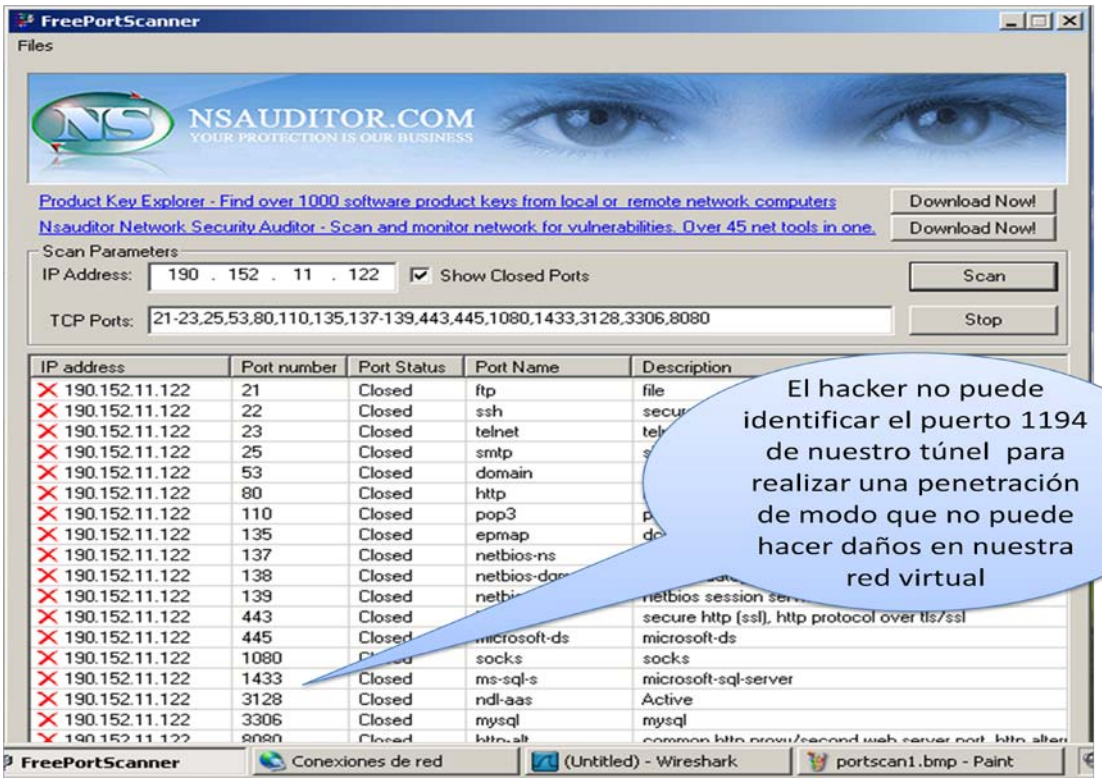

Figura. 6.65 Port Scanner no identifica el puerto 1194

Al ejecutar el programa Port Scan nos indica varios puertos pero no nos revela el puerto por el cual se ha creado el tunel de conexión entre el Municipio Principal y Sucursal que es el puerto 1194.

Búsqueda de Claves (PASSWORD SNIFFING)

Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

Es muy frecuente crackear una password explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte la empresa. Por ser el uso de passwords la herramienta de seguridad más cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (como se define una password?, a quien se está autorizado a revelarla?) y una administración eficiente (cada cuanto se están cambiando?)

Existen varios programas para obtener las claves de ingreso así tenemos, Wireshark, Ettercap. En las siguientes gráficas podemos ver la ejecución de Wireshark.

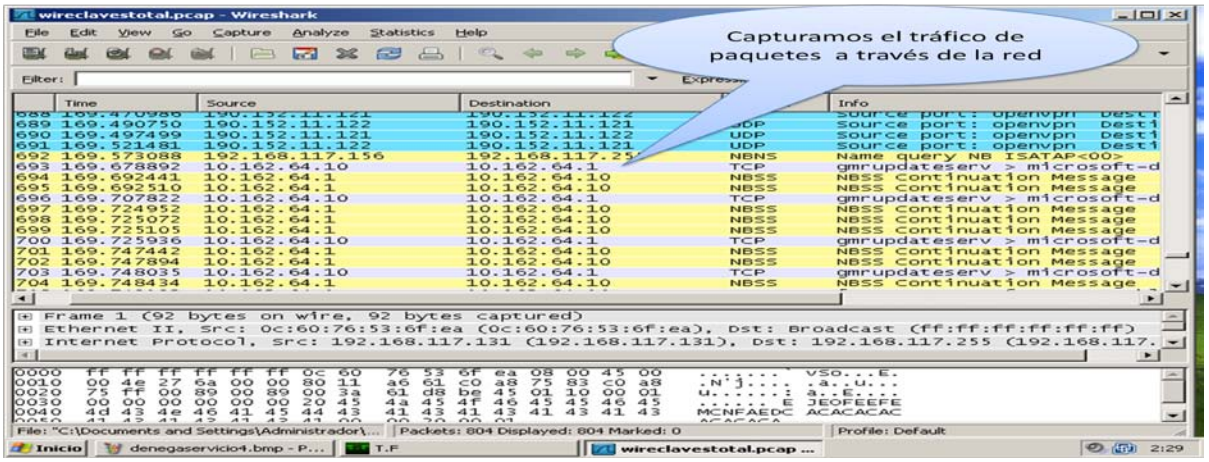

Figura. 6.66 Capturando tráfico de la red.

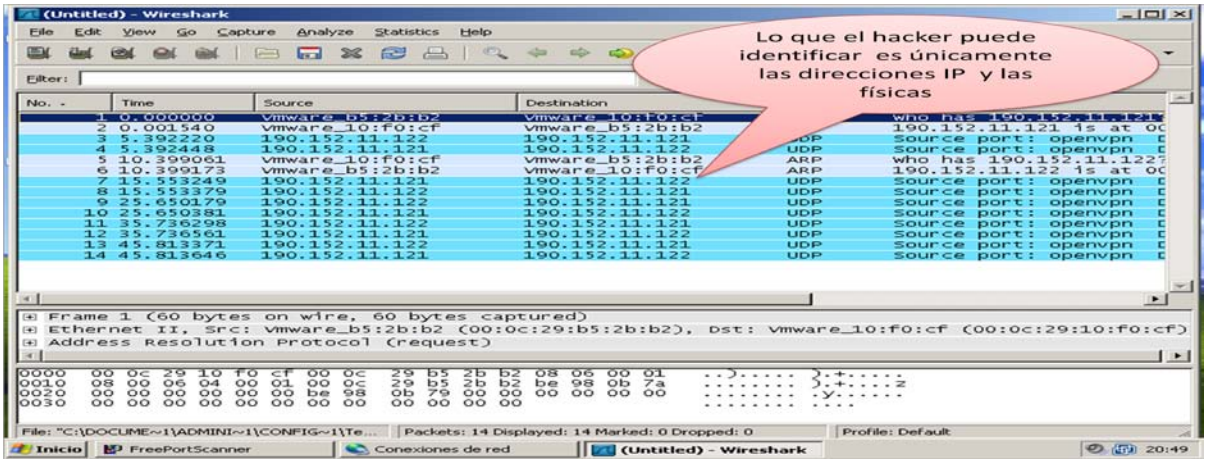

Figura. 6.67 Identificación de direcciones IP

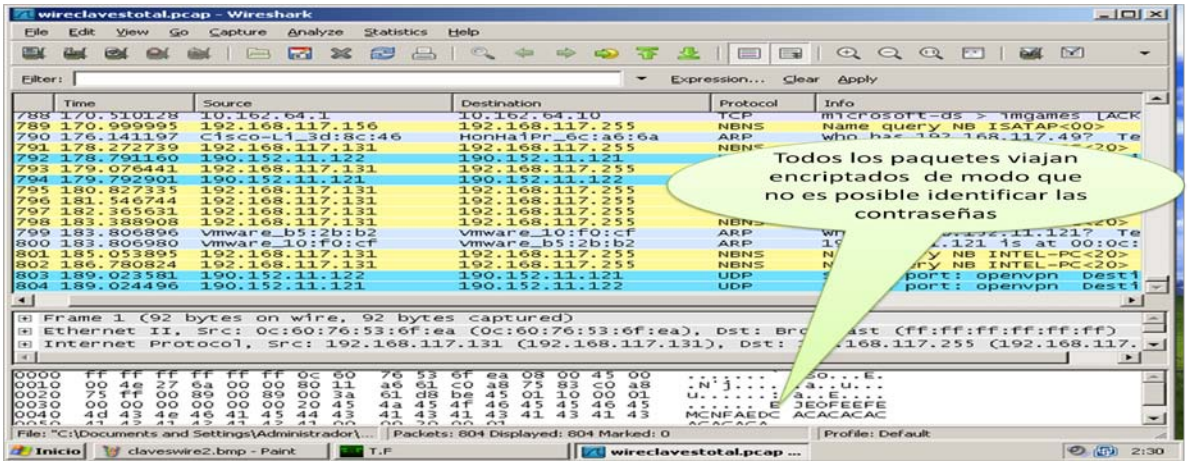

Figura. 6.68 No se identifica la Clave.

Podemos observar que las claves no pueden ser obtenidas ya que la comunicación se realiza con paquetes que utilizan un eficiente algoritmo de encriptación de modo que es difícil desencriptarlo.

Envenenamiento ARP (ARP SPOOFING)

El objetivo es envenenar la comunicación que se produce en el protocolo de comunicación de paquetes ARP, que es el protocolo de resolución de direcciones responsable de convertir las direcciones de protocolo de alto nivel (direcciones IP) a direcciones de red físicas (MAC). Así pues, este breve trabajo explicaremos básicamente el funcionamiento del

protocolo ARP, para centrarnos en donde puede afectar a la seguridad de nuestra red, y una vez hallamos definido el problema y el punto débil, veremos la potencia de la herramienta Ettercap que es capaz de explotar satisfactoriamente la vulnerabilidad a la que nos referimos.

Siempre que un host desea enviar cualquier tipo de información IP a otro host, deberá conocer la MAC del destino para poder transmitir. Es necesario enviar una petición ARP a la red, por medio de lacual sólo responderá el host destino diciendo al origen su dirección hardware.

Existen varios programas para realizar envenenamiento ARP pero el más potente es Ettercap que lo vemos a continuación en ejecución. En la siguiente secuencia de imágenes podemos apreciar la ejecución de Ettercap y el ataque que realiza a nuestro túnel virtual.

Figura. 6.69 Ettercap en Ejecución.

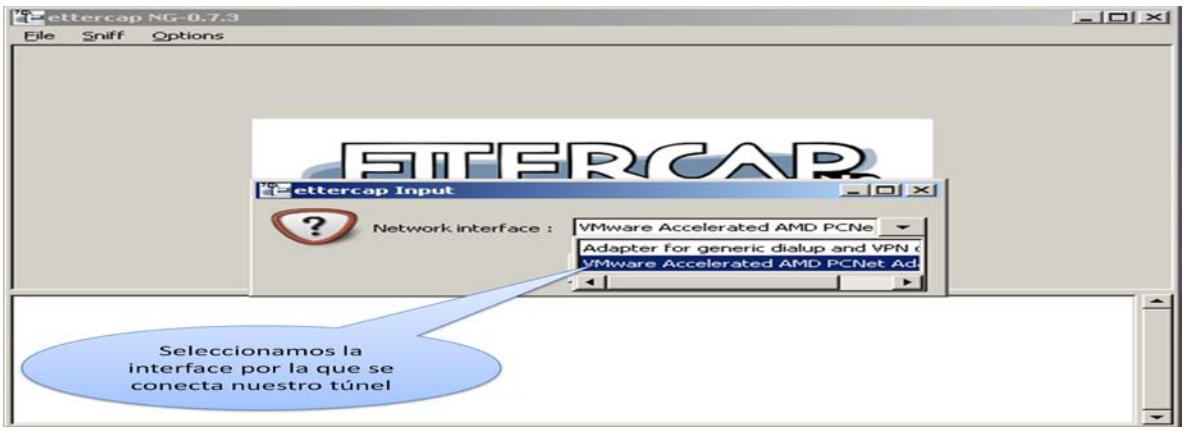

Figura. 6.70 Seleccionando la interfaz.

Figura. 6.71 Información que proporciona Ettercap

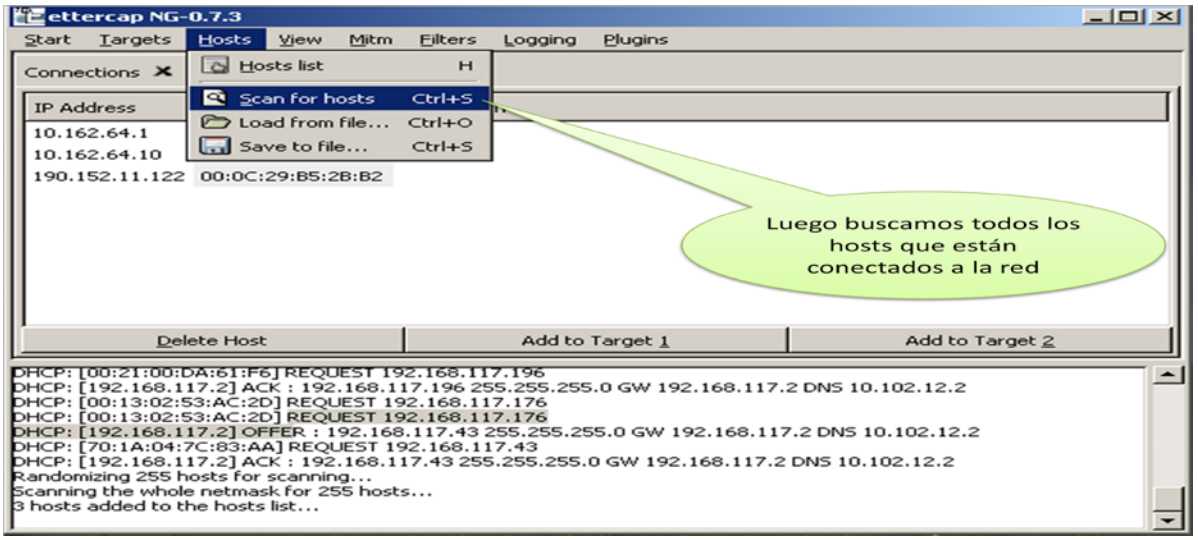

Figura. 6.72 Identificando Hosts

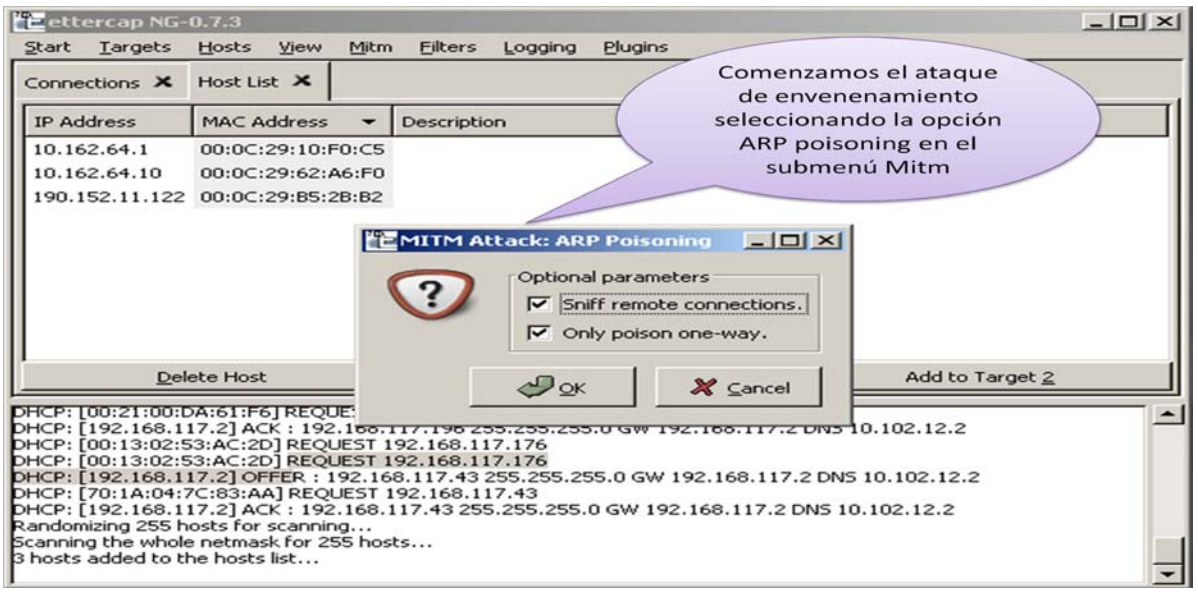

Figura. 6.73 Comenzando el Ataque de Envenenamiento

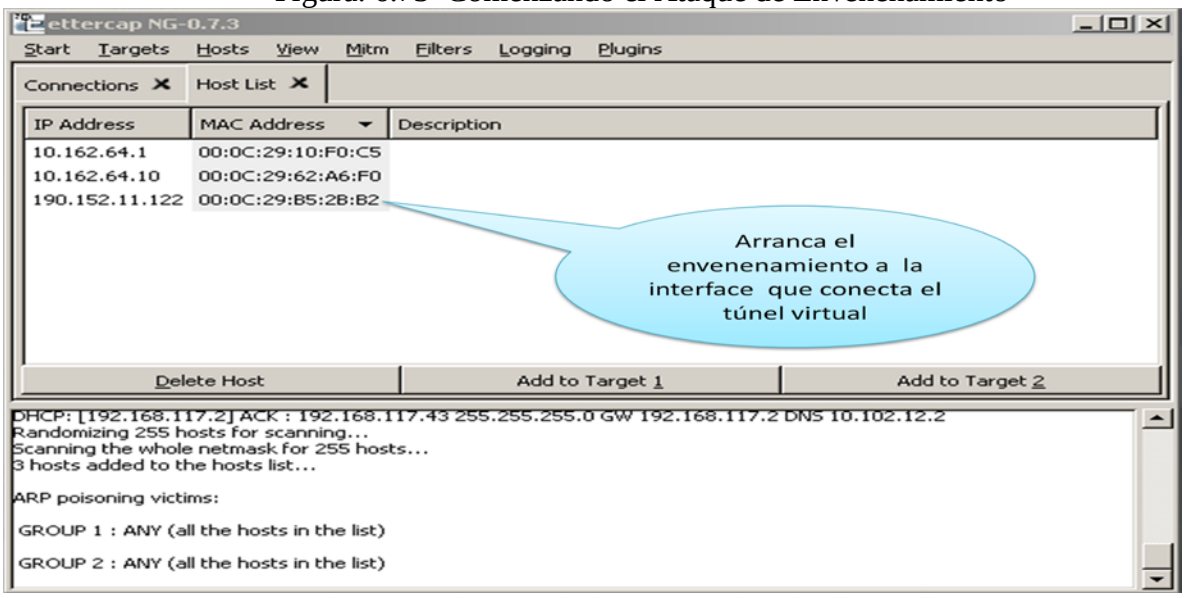

Figura. 6.74 Envenenamiento a la interfaz del túnel virtual

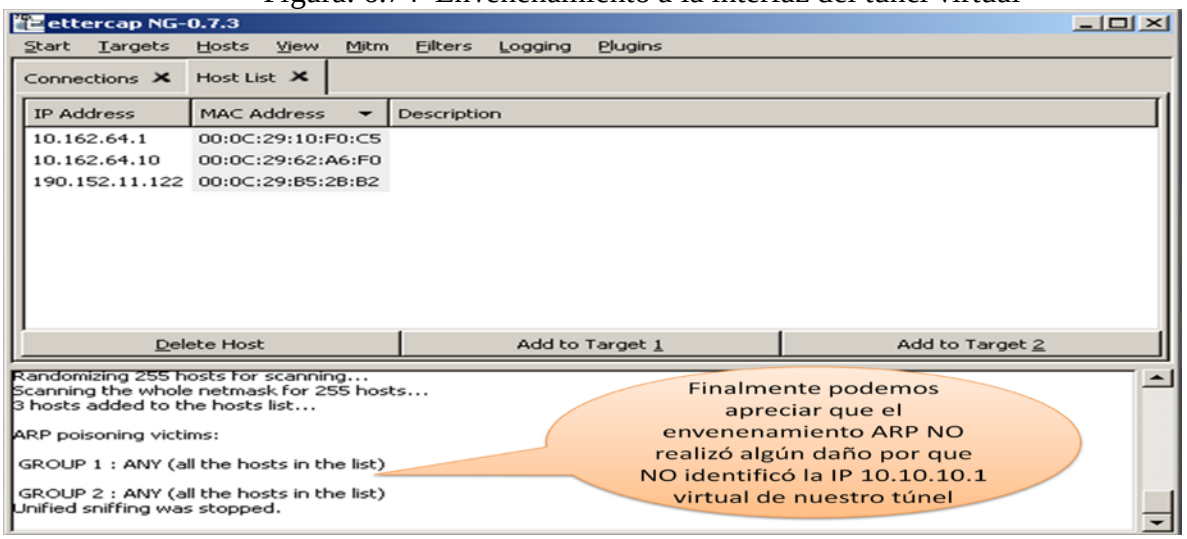

Figura. 6.75 El envenenamiento no identificó la dirección IP virtual

Finalmente es importante manifestar que el procedimiento de comunicación se realiza en el túnel que hemos creado con un nivel de encriptación muy alto, y no se revela las direcciones IP que conectan el túnel de modo que no es posible envenenar los paquetes ARP.

Denegación de Servicio (DENIAL OF SERVICE)

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS (de las siglas en inglés Distributed Denial of Service) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

Conclusiones.

Un ataque de "Denegación de servicio" impide el uso legítimo de los usuarios al usar un servicio de red. El ataque se puede dar de muchas formas. Pero todas tienen algo en común: utilizan el protocolo TCP/IP para conseguir su propósito.

Hay varias herramientas para realizar la denegación de servicio entre ellas podemos citar Thunderflood que lo vemos en ejecución a continuación.

Figura. 6.76 Arrancando Thunderflood

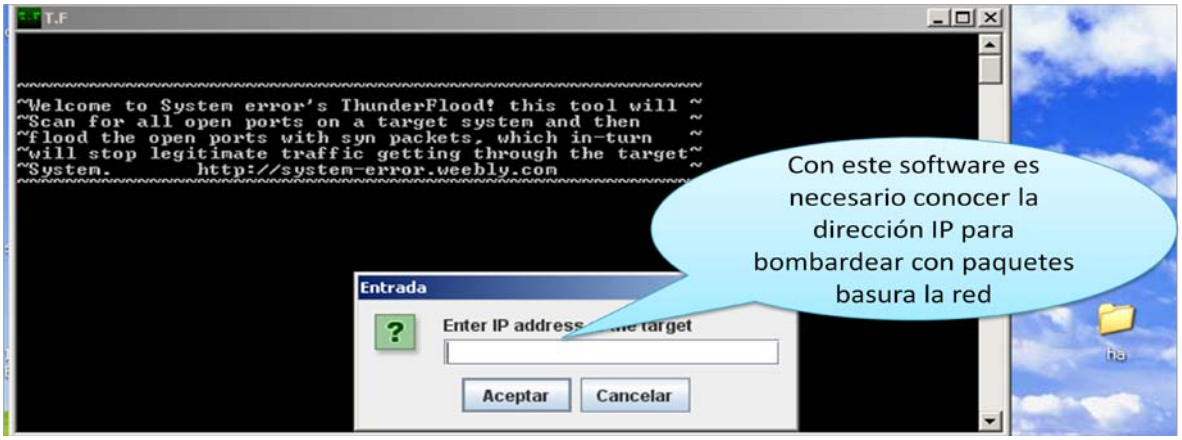

Figura. 6.77 Ingresando la dirección IP.

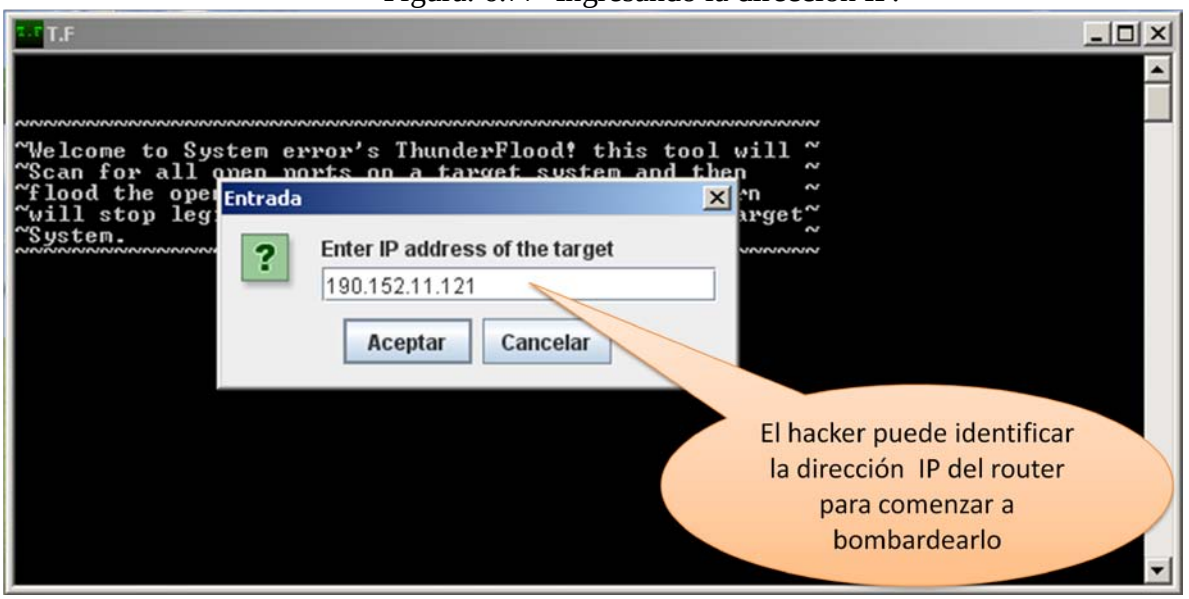

Figura. 6.78 Dirección IP que el Hacker puede identificar

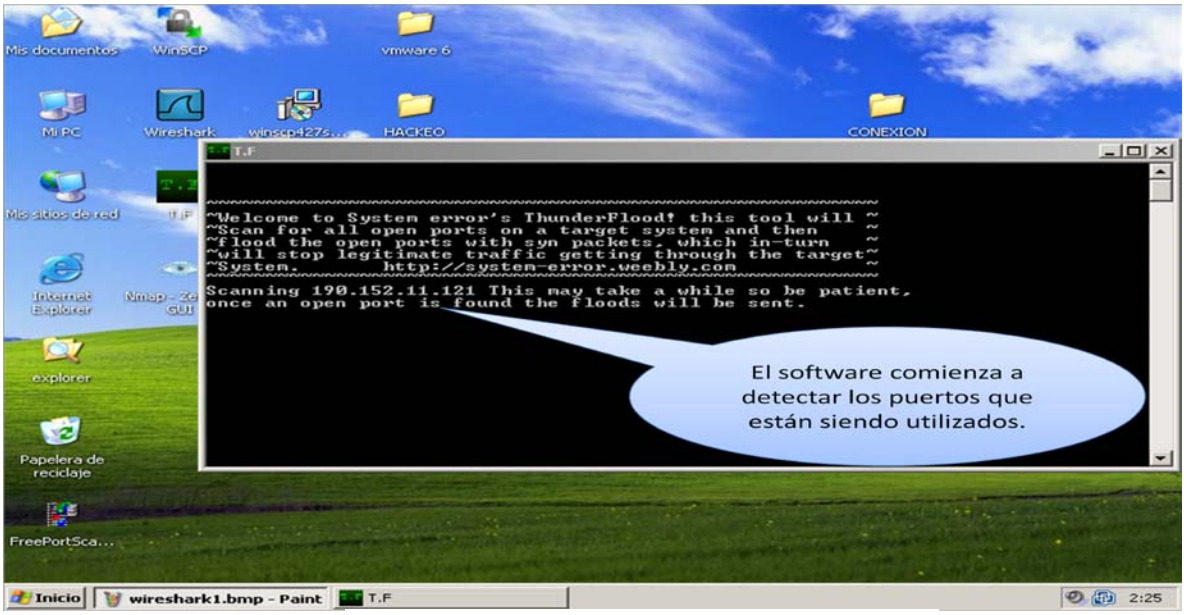

Figura. 6.79 Comienza la búsqueda de puertos

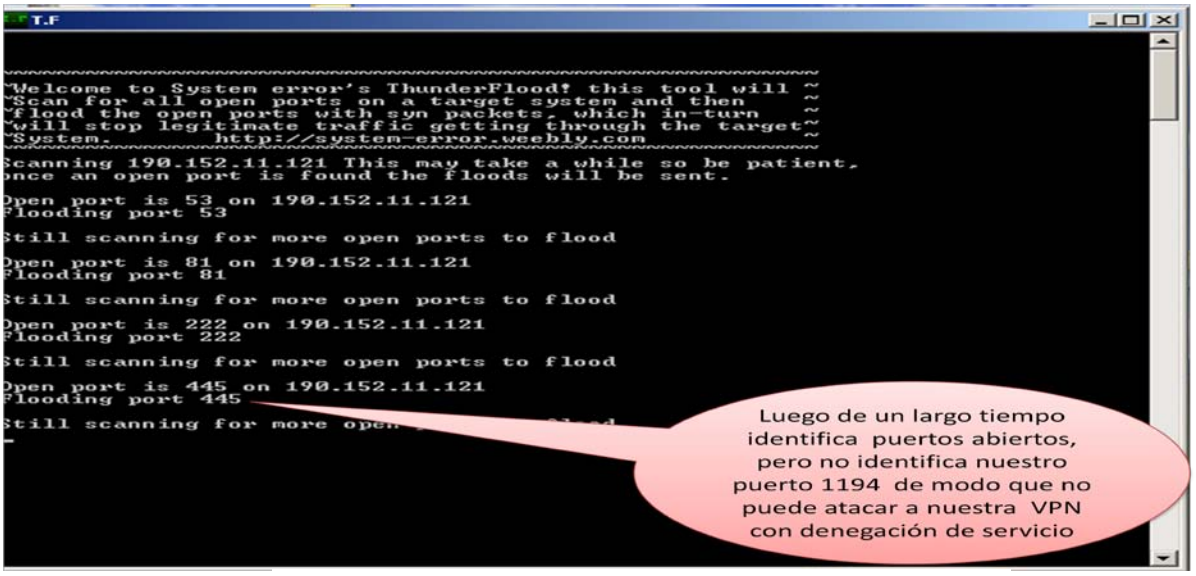

Figura. 6.80 No se identifica el Puerto y no puede Atacar

El puerto por el cual se genera el túnel de la comunicación entre el Municipio de Pelileo Principal y la Sucursal no es identificado de modo que el ataque de denegación de servicio no genera efecto alguno en nuestra comunicación.

6.9 Previsión de la Evaluación

Análisis del Hacker ubicado en la red Pública (Internet)

El Hacker ubicado en la red pública no puede identificar la dirección IP virtual del túnel , ni el número de puerto. Esto representa un grado de seguridad muy confiable ya que el hacker no puede fácilmente penetrar en la red y hacer daño. Además se tiene la facilidad de cambiar periódicamente la dirección IP virtual y el número de puerto de modo que será muy difícil que el hacker pueda identificar estos parámetros para hacer daños en la red.

Análisis del Hacker ubicado en la red LAN Interna (Municipio)

Para este caso se puede indicar que ocurre la misma situación que al estar ubicado en la red pública. Pero es importante indicar que un hacker ubicado en la Red Interna puede hacer mayor daño, ya que es más fácil acceder y obtener claves para destruir el sistema, y ante esto se debe implementar excelentes políticas de seguridad en los administradores de la red del Ilustre municipio de Pelileo.

6.10 Bibliografía

Fuentes bibliográficas:

Internet:

- DICCIONARIO INFORMATICO. (10 de junio de 2009) , www. alegsa. com. ar/Dic /sistema %20 informatico.php
- MARTINEZ, David. (10 de junio de 2009). Seguridad en redes. http://exa. unne.edu.ar /depar/areas /informatica
- SAHAGÚN, Marco (10 de junio de 2009). Seguridad Informática. http://www. monografias.com /trabajos/ hackers/hackers.shtml
- UNIVERSIDAD DE CHILE. (10 de junio de 2009). Seguridad en las redes de Datos. http://www. ing.puc.cl/esp/infgeneral

- CARDOSO, Luis. (10 de junio de 2009) .Las Normas de Seguridad. http://www3. gartner.com /5_about/press_releases/pr11june2003c.jsp

- REDES DE DATOS. (10 de octubre de 2009) http: //www .geocities .com /v.iniestra /apuntes/redes/

- RED DE COMPUTADORAS. (10 de octubre de 2009) http://es. wikipedia.org /wiki/Red _ de_computadoras

6.11 Anexos

6.11.1 Glosario de Términos.

ADSL: Son las siglas de Asymmetric Digital Subscriber Line ("Línea de Suscripción Digital Asimétrica"). ADSL es un tipo de línea DSL. Consiste en una transmisión de datos digitales (la transmisión es analógica) apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando el alcance no supere los 5,5 km. medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

BASES DE DATOS: Una base de datos o banco de datos (en ocasiones abreviada BB.DD.) es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

CONECTIVIDAD: Es la capacidad de un dispositivo (un PC, periférico, PDA, móvil, robot, electrodoméstico, coche, etc.) de poder ser conectado (generalmente a un PC u otro dispositivo) sin la necesidad de un ordenador, es decir en forma autónoma. Asimismo es el grado de conexión entre entidades sociales, gubernamentales y de cualquier índole entre sí.

CRIPTOGRAFÍA: La máquina alemana de cifrado Lorenz, usada en la Segunda Guerra Mundial para el cifrado de los mensajes para los generales de muy alto rango.

La criptografía (del griego κρύπτω *krypto*, «oculto», y γράφω *graphos*, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información mediante técnicas

especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos

ENCRIPTAR: Es una manera de codificar la información para protegerla frente a terceros. Por lo tanto la encriptación informática sería la codificación la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red.

HUMANWARE: Son los usuarios de las computadoras. Básicamente somos los humanos que tenemos contactó con estas máquinas. El concepto "HUMANWARE" es usado para resaltar la importancia del "lado Humano" de la interacción entre los principales actores involucrados en los procesos de reestructuración, reingeniería y modernización empresarial para garantizar el éxito.

INTERCONEXIÓN: Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

INFRAESTRUCTURA DE RED DE DATOS: La infraestructura de una red de datos, es la parte más importante de toda nuestra operación como administradores, dado que si nuestra estructura de medio de transporte es débil y no lo conocemos, por lo tanto nuestra red de datos no puede tener un nivel alto de confiabilidad, por lo que en esta sección proporcionaremos las mejores prácticas para tener o mejorar una infraestructura de red confiable.

IMP.- Ilustre Municipio de Pelileo.

Lempel-Ziv-Oberhumer (LZO) :es un algoritmo de la compresión de datos que se centra en velocidad de la descompresión. El algoritmo es el sin pérdidas y la puesta en práctica de la referencia es el hilo de rosca seguro.

Las versiones de LZO están disponibles para el Perl, el pitón y las idiomas de Java.

MODELO OSI.- El **modelo de referencia de Interconexión de Sistemas Abiertos** (OSI, Open System Interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

MTU: La unidad máxima de transferencia (*Maximum Transfer Unit* - MTU) es un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un Protocolo de Internet.

PERIFÉRICOS: En informática, se denominan periféricos a los aparatos o dispositivos auxiliares e independientes conectados a la unidad central de procesamiento de una computadora.

SOFTWARE LIBRE. El software libre (en inglés *free software*, esta denominación también se confunde a veces con gratis por el doble sentido del inglés *free* en castellano) es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, cambiado y redistribuido libremente.

SNIFFING: En informática, un packet sniffer es un programa de captura de las tramas de red. Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, UTP, fibra óptica etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él.

SPOOFING: En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Existen diferentes tipos dependiendo de la tecnología a la que nos refiramos.

SISTEMA INFORMÁTICO: Un sistema informático como todo sistema, es el conjunto de partes interrelacionadas, hardware, software y de Recurso Humano (humanware). Un sistema informático típico emplea una computadora que usa dispositivos programables para capturar, almacenar y procesar datos.

SISTEMAS DE SEGURIDAD: La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

SISTEMA DE PREVENCIÓN DE INTRUSOS: Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de *Prevención de Intrusos* es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

TCP/IP: Son las siglas de Protocolo de Control de Transmisión/Protocolo de Internet (en inglés *Transmission Control Protocol/Internet Protocol*), un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red.

TUNELES VIRTUALES: Se trata de una solución para conexión segura (encriptada) entre sucursales, trabajadores remotos y oficinas centrales a través de Internet.

VIRUS INFORMATICOS.- Un virus informático es un programa o software que se autoejecuta, sin el permiso o el conocimiento del usuario. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

VPN.- Significa por sus siglas en ingles virtual private network (red virtual privada). La Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada , como por ejemplo Internet.

6.11.2 Encuesta:

¿Una red con capacidad de proteger a nivel de protocolos es: ?

Altamente Fiable	
Fiable	
Insegura	

¿Qué nivel de desempeño eficiente tiene una red con software libre: ?

Alto	
Medio	
Bajo	

¿La implementación de una red con protección a nivel de protocolos en el IMP es: ?

Muy difícil	
Difícil	
Fácil	

¿Cómo determina la administración de una red con software libre y protección a nivel de protocolos?

Fácilmente Administrable	
Medianamente Administrable	
Difícilmente Administrable	

¿Cómo considera las políticas de seguridad implementada en la red del IMP?

Muy efectivas	
Efectivas	
Deficientes	

¿De qué forma considera la rapidez en que se lleva a cabo la implementación de políticas de seguridad en el IMP. ?

Muy rápida	
Rápida	
Lenta	

¿Cómo considera el nivel de desempeño de los empleados para gestionar políticas de seguridad en la red de datos?

Óptimo	
Normal	
Deficiente	

¿De qué forma, la red del IMP provee servicio de protección de ataques a los usuarios?

Altamente satisfactoria	
Satisfactoria	
Poco satisfactoria	