UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TEMA: "IMPLANTACIÓN DE LA RED LAN INALAMBRICA EN LA BANDA DE 3.8 GHZ, UTILIZANDO CÓDIGOS DE ENCRIPTACIÓN PKI Y VPN PARA SEGMENTACIÓN DE NODOS A TRAVES DE SOFTWARE LIBRE VERSION CENTOS EN LA DIRECCIÓN NACIONAL DE COMUNICACIONES DE LA POLICIA"

TESIS PREVIO LA OBTENCIÓN DEL TITULO DE INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

POSTULANTES:

- **AREQUIPA AVILES CARMEN AMELIA**
- **CHAMBA MELO SAYDA CECILIA**

DIRECTOR DE TESIS:

ING. PATRICIO NAVAS MOYA

LATACUNGA – ECUADOR

2010

AUTORIA

Las ideas, opiniones y comentarios en este documento son de exclusiva responsabilidad de las autoras, egresadas: Arequipa Aviles Carmen Amelia y Chamba Melo Sayda Cecilia.

Egda. Arequipa Aviles Carmen Amelia
C.C. Nº 050265449-4

Egda. Chamba Melo Sayda Cecilia
C.C. Nº 210020805-3

CERTIFICACIÓN

HONORABLE CONSEJO ACADEMICO DE LA UNIVERSIDAD TECNICA DE COTOPAXI

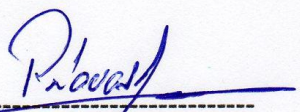
De mi consideración.

Cumpliendo con lo estipulado en el capítulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que las postulantes: Arequipa Aviles Carmen Amelia, Chamba Melo Sayda Cecilia han desarrollo su tesis de grado de acuerdo al planeamiento formulado en el plan de tesis con el tema: **"Implantación de una red LAN inalámbrica en la banda de 3.8 GHz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre en la Dirección Nacional de Comunicaciones"** cumpliendo con los objetivos planeados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 14 de julio del 2010

Atentamente,



Ing. Patricio Navas M.
DIRECTOR DE TESIS

POLICÍA NACIONAL
DIRECCIÓN NACIONAL DE COMUNICACIONES
CENTRO DE DATOS-SIIPNE

CERTIFICACIÓN

Yo Cbop. Tlgo. Javier Alexis Orellana Peñaherrera, con C.C. 171021569-8 , en calidad de Administrador de la red de la Dirección Nacional de Comunicaciones de la Policía Nacional, certifico que las señoritas **Arequipa Aviles Carmen Amelia con C.C. 050265449-4** y **Chamba Melo Sayda Cecilia con C.C 210020805-3**; egresadas de la Universidad Técnica de Cotopaxi de la Especialidad Ingeniería Informática y Sistemas Computacionales, han concluido la IMPLANTACIÓN DE UNA RED LAN INALÁMBRICA EN LA BANDA DE 3.8 GHZ, UTILIZANDO CÓDIGOS DE ENCRIPTACIÓN PKI Y VPNs PARA SEGMENTACIÓN DE NODOS CON EL USO DE SOFTWARE LIBRE Y SUS HERRAMEINTAS.

Dicho trabajo ha sido entregado y comprobado su funcionamiento, sujetándose a las especificaciones y requerimientos técnicos solicitados.

Es todo cuanto puedo certificar; pudiendo los interesados hacer uso lícito del presente documento como lo creyeren conveniente.

Quito, julio del 2010.

POLICIA NACIONAL
DIVISION INFORMATICA
DIRECCION NACIONAL DE COMUNICACIONES

Tlgo. Javier Orellana
CABO PRIMERO DE POLICIA (A)
TECNICO ADMINITRADOR DINACOM-SIIPNE.

AGRADECIMIENTO I

Agradezco a dos personas en especial mi madre Carmita que con su amor infinito se convirtió en mi Ángel Guardián y a mi hija Danahe que con ternura y amor me dio fuerza para alcanzar mi meta profesional.

A la Dirección Nacional de Comunicaciones por brindarme las facilidades para poder realizar el proyecto de titulación.

Al director del proyecto Ing. Patricio Navas, quien me guió con sus conocimientos y experiencia en la elaboración de la Tesis.

A quienes imparten día a día su sabiduría y conocimientos, nuestros Maestros ya que junto a su enseñanza he logrado alcanzar esta meta, de la misma manera agradecer a todas las autoridades y empleados quienes laboran en tan prestigiosa institución.

Y a mi Universidad Técnica de Cotopaxi por haberme permitido obtener en sus aulas mi sueño de ser una profesional de la República.

Carmen A.

AGRADECIMIENTO II

Al culminar con esta etapa de mi vida, quiero expresarme por medio de este papel mi eterno agradecimiento a Dios por brindarme la salud, la vida y sabiduría que ha guiado mis pasos y a mi familia porque gracias a ellas he podido concluir con esta meta.

Y de manera muy especial a mi mami Fanny que con su Amor infinito ha sido mi guía en toda mis metas trazadas, a mi padre Manrrique que aun ya no estando en la tierra encontró la manera de hacerme sentir su presencia y brindarme su apoyo divino, a mi hermana Ximena y a mi hermano Jonathan que con su alegría y apoyo me ayudaron a cumplir cada una de mis aspiraciones.

A los docentes de la Universidad Técnica de Cotopaxi, por proporcionarme los conocimientos necesarios para poder defenderme en la vida profesional.

El agradecimiento más sincero a las personas que fueron parte de mi vida universitaria, amigos, compañeros, profesores, siendo los primeros en venir a mi mente el Ing. Patricio Navas Director de mi tesis, Ing Orellana Asesor de la Institución de la Policía Nacional y a todas mis mejores amigas, consiguiendo con cada una de sus acciones tener un lugar muy importante en mi corazón.

SAYDA

DEDICATORIA I

El presente trabajo investigativo está dedicado principalmente a Dios por haberme dado el regalo más preciado y valioso como es la vida, a mi madre y a mi padre, que desde el inicio de mi vida supieron educarme con amor y paciencia, inculcándome los mejores valores para ser una persona de bien siendo para mí el pilar fundamental durante la vida universitaria puesto que me apoyaron en todo momento con abnegación para poder llegar a cumplir mis metas tan anheladas y por último a mi hija que es el mejor regalo que Dios me dio, siendo ella mi motivación de mi vida.

Carmen A.

DEDICATORIA II

Este trabajo lo dedico principalmente a Dios por darme las fuerzas necesarias de seguir viviendo por el propósito de alcanzar mis metas para terminar lo empezado, a los mejores padres de este planeta a quienes amo mucho Fanny Melo y Manrrique Chamba quienes desde mi niñez me inculcaron y apoyaron en mi trayectoria con el único fin de encaminarme por el camino del bien.

Al esfuerzo que toda persona realiza en el momento de cumplir con cada objetivo, porque no solo lo realizan por satisfacción propia, sino dedicándolo a quienes en realidad merecen todos los elogios.

Al sentimiento más hermoso el AMOR; que es la fuente de vida para todas las personas en especial para mí, porque gracias a este lindo sentimiento él nos brinda grandes alegrías y también tristezas y así permite que día a día nos acerquemos más a nuestro Dios.

SAYDA

INDICE GENERAL

CONTENIDO **PÁG.**

CAPÍTULO I

CAPÍTULO II

TRABAJO DE CAMPO

CAPITULO III

PROPUESTA

ÍNDICE DE TABLAS

TABLA **PÁG**

ÍNDICE DE GRÁFICOS

GRÁFICOS **PÁG**

RESUMEN

El presente trabajo investigativo comprende la importancia de implantar una red LAN inalámbrica en la banda de 3.8 GHz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre en la Dirección Nacional de Comunicaciones (DINACOM), la misma que garantizará el flujo de información y de esta manera, facilitará la toma de decisiones para el mejoramiento del servicio de red con la innovación de la banda C.

El mercado de la seguridad VPN (Redes Privadas Virtuales) es nuevo y todos los estándares están permanentemente evolucionando, sin embargo existen protocolos que hoy en día se utilizan como estándares de comunicación de tipo VPN. Mismas que están unidas por túneles virtuales, en lugar de estarlo físicamente, ya que permitirá aumentar la seguridad de las comunicaciones facilitando la conexión entre máquinas de distintos rangos con IP's fijas o dinámicas.

La transmisión de la información se realizará por medio de códigos de encriptación PKI (Infraestructura de clave pública) dando autenticidad, confidencialidad, integridad y seguridad a los datos. Con el uso del Sistema Operativo de software libre habrá reducción de costes por lo que es gratuito, tendrá mayor rapidez en el manejo de la información.

El presente trabajo deja un documental en la DINACOM para ayuda del personal policial que servirá de guía de cómo está estructurada la red inalámbrica con sus respectivas seguridades.

SUMMARY

This investigative work is based on the importance to introduce a LAN wireless network in the band of 3.8 GHz, using encryption codes PKI and VPN for nodes segmentation through free software in the Dirección Nacional de Comunicaciones (DINACOM), it will guarantee the information flux, as a result of this, it will facilitate the taking of decisions, in order to improve the network service with the innovation.

The security market VPN (Virtual Private Network), is new and all standards are changing permanently, however, actually there are protocols are used as communication standards of VPN rate, which are linked by virtual tunnels, instead of being physically, since it will permit to increase the communication security, helping the connection among machines of different rank with fixed or dynamic IP`s.

The transmition of information will do through PKI encryption codes (Public Key Infraestructure) giving authenticity, confidentially, integrity and security to the datum's. With the Operative System used of free software, there will be cost decieasement because it is free; it will be faster in the information management.

This work provided a documental in the DINACOM, in order to help Police personnel which will be useful as guide of how it is structured the wireless network and their security aspects.

CERTIFICACIÓN DE TRADUCCIÓN

Yo, Gloria del Consuelo Moya Heredia, portadora de la Cédula de Ciudadanía 050028127-3, en calidad de Profesional del Área de Inglés, tengo a bien **CERTIFICAR:** que las egresadas de la Universidad Técnica de Cotopaxi, señoritas: Arequipa Aviles Carmen Amelia portadora de la Cédula de Ciudanía Nº 050265449-4 y Chamba Melo Sayda Cecilia portadora de la Cédula de Ciudadanía Nº 210020805-3, han realizado la debida corrección con mi persona del Summary de la Tesis de Grado con el Tema: **"IMPLANTACIÓN DE UNA RED LAN INALAMBRICA EN LA BANDA DE 3.8 GHZ, UTILIZANDO CÓDIGOS DE ENCRIPTACIÓN PKI Y VPN PARA SEGMENTACION DE NODOS A TRAVES DE SOFTWARE LIBRE EN LA DIRECCIÓN NACIONAL DE COMUNICACIONES DE LA POLICÍA"**, el cual se encuentra bien estructurado, por lo que doy fe del presente trabajo.

Por tal motivo faculto a las peticionarias hacer uso del presente certificado como a bien lo consideren.

Licda.Gloria del Consuelo Moya H.
PROFESOR

Latacunga, julio 2010

INTRODUCCIÓN

Las aplicaciones más frecuentes de las redes inalámbricas ya sean de transmisión o distribución datos, contribuyen al mejoramiento del servicio de la red LAN que se distribuyen en todos los departamentos de la Dirección Nacional de Comunicaciones de la Policía Nacional. En este caso interesa determinar conocer el flujo de datos que estén activas, controlar el mal uso de los recursos existentes y de la misma manera asegurar la información.

Este estudio es de gran importancia para la implantación de seguridades en la red inalámbrica ya que permitirá garantizar el flujo de la información. La DINACOM, en los actuales momentos se ha convertido en una de las principales instituciones a nivel nacional, ya que desde allí se maneja toda la información del personal policial, civil, transito, entre otros. Por esta razón surge la necesidad de implantar seguridades en la comunicación dentro de la Institución.

El objetivo general de este trabajo es implantar la red LAN inalámbrica en la banda de 3.8 GHz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre en el Campus de la Dirección Nacional de Comunicaciones de la Policía. Como objetivos específicos se ha planteado los siguientes:

Realizar un estudio de calidad y servicio en la implantación de la red LAN inalámbrica para detectar problemas y por ende dar soluciones.

Identificar los beneficios que brinda la banda de 3.8 GHz en la dirección Nacional de Comunicaciones.

Permitir la comunicación entre redes distantes físicamente utilizando códigos de encriptación PKI y VPN a través de software libre.

Se demostró como hipótesis general que la implantación de la red LAN inalámbrica en la banda de 3.8 GHz utilizando códigos de encriptación PKI y VPN para segmentación de nodos mejoro la calidad de servicio y seguridad para el administrador y usuarios, comprobando mediante las encuestas y entrevistas aplicadas a todo el personal de la DINACOM.

La mencionada Institución ha visto con buenos ojos la Implantación de la red LAN inalámbrica en la banda de 3.8 GHz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre, ya que gracias a este proyecto se logrará proteger la información dando seguridad y reduciendo costes, de esta manera proporcionan a los usuarios tener acceso a la información en tiempo real y en forma segura en cualquier lugar dentro de la institución. En la actualidad existe el ingreso de intrusos que podrían irrumpir la información; por lo que urge dicha implantación que es de mucha importancia para la Institución con el objetivo que solo los usuarios, administradores e información legitimada puedan utilizar la red inalámbrica.

El presente trabajo de investigación está establecido en tres capítulos, distribuidos de la siguiente manera:

El capítulo I concerniente a la fundamentación teórica, donde se indica algunos temas informáticos que van dentro del mismo para el desarrollo de la implantación de la red.

En el capítulo II, se hace referencia a una breve descripción de la institución, Dirección Nacional de Comunicaciones y al trabajo de campo, donde se aplico los instrumentos de investigación como son: la encuesta a los señores policías de la Dirección Nacional de Comunicaciones y la entrevista realizada a los señores administradores de la red, posteriormente se efectuó el procesamiento de datos, por medio de la tabulación de los mismos, así como su presentación por medio de graficas de pastel, interpretación y análisis de los resultados obtenidos, los mismos que sirvieron de base para la comprobación de la hipótesis planteada.

En el capítulo III, relacionado con la propuesta de investigación se presenta de manera detallada la implantación de la red LAN en la banda de 3.8 Ghz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre, así como también se enuncia las conclusiones y recomendaciones finales del trabajo de investigación, siendo estos los resultados del trabajo de campo realizado en la Dirección Nacional de Comunicaciones, además se incluye la bibliografía y el glosario de términos para su correcto entendimiento del presente documento.

Finalmente se puede manifestar que se pudo satisfacer las expectativas tanto de los investigadores como de los administradores de la DINACOM, puesto que se logro cumplir a cabalidad con los objetivos de implantar la red con una banda de 3.8 Ghz y sus respectivas seguridades en nuestro país con tecnología de punta.

CAPITULO I

1 RED LAN INALAMBRICA BAJO SOFTWARE LIBRE CON SUS RESPECTIVAS SEGURIDADES.

1.1 Historia de redes

Introducción.

En realidad, la historia de la red se puede remontar al principio del siglo XIX. El primer intento de establecer una red amplia estable de comunicaciones, que abarcara al menos un territorio nacional, se produjo en Suecia y Francia a principios del siglo XIX. Estos primeros sistemas se denominaban de telégrafo óptico y consistían en torres, similares a los molinos, con una serie de brazos o bien persianas. Estos brazos o persianas codificaban la información por sus distintas posiciones. Estas redes permanecieron hasta mediados del siglo XIX, cuando fueron sustituidas por el telégrafo. Cada torre, evidentemente, debía de estar a distancia visual de las siguientes; cada torre repetía la información hasta llegar a su destino. Un sistema similar aparece, y tiene un protagonismo especial, en la novela *Pavana*, de Keith Roberts, una ucronía en la cual Inglaterra ha sido conquistada por la Armada Invencible.

Posteriormente, la red telegráfica y la red telefónica fueron los principales medios de transmisión de datos a nivel mundial.

Las primeras redes construidas permitieron la comunicación entre una computadora central y terminales remotas. Se utilizaron líneas telefónicas, ya que estas permitían un traslado rápido y económico de los datos. Se utilizaron procedimientos y protocolos ya existentes para establecer la comunicación y se incorporaron moduladores y demoduladores para que, una vez establecido el canal físico, fuera posible transformar las señales digitales en analógicas adecuadas para la transmisión por medio de un módem.

Pero la verdadera historia de la red comienza en los 60 con el establecimiento de las redes de conmutación de paquetes. Conmutación de paquetes es un método de fragmentar

mensajes en partes llamadas paquetes, encaminarlos hacia su destino, y ensamblarlos una vez llegados allí.

La primera red experimental de conmutación de paquetes se usó en el Reino Unido, en los National Physics Laboratories; otro experimento similar lo llevó a cabo en Francia la Societe Internationales de Telecommunications Aeronautiques. Hasta el año 69 esta tecnología no llego a los USA, donde comenzó a utilizarla el ARPA, o agencia de proyectos avanzados de investigación para la defensa.

1.2 Definición

Los ordenadores suelen estar conectados entre sí por cables. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites.

Según RODRIGUEZ Jorge, (2000), dice **"**Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos. A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas**"**[1]

Los investigadores revelan que una red es una agrupación de varios computadores que comparten información para ejecutar procesos.

1.2.1 Tipos

El manual de referencia, Novell Netware, Cuarta Edición (2001, pág. 21,22), da a conocer los siguientes tipos de redes:

[1]http://www.pucelawireless.net/index.php?pagename=AccessPoint.

Red pública: Una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

Red privada: Una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

Red de área Personal (PAN): (Personal Area Network) Es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación del interpersonal), o para conectar con una red de alto nivel y el Internet.

Red de área local (LAN): una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización. Nota: Para los propósitos administrativos, LANs grande se divide generalmente en segmentos lógicos más pequeños llamados los Workgroups. Un Workgroups es un grupo de las computadoras que comparten un sistema común de recursos dentro de un LAN.

Red del área del campus (CAN): Se deriva a una red que conecta dos o más LANs los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

Red de área metropolitana (MAN): una red que conecta las redes de un área dos o más locales juntos pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Las rebajadoras (routers) múltiples, los interruptores (switch) y los cubos están conectados para crear a una MAN.

Red de área amplia (WAN): es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono. Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de transmisión de datos, y la capa de red.

Redes virtuales (VLANs): Las LANs virtuales (VLANs) son agrupaciones de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en sistemas informáticos de redes. Este concepto, fácilmente asimilable a grandes trazos implica en la práctica, sin embargo, todo un complejo conjunto de cuestiones tecnológicas.[2]

1.3 Redes inalámbricas

1.3.1 Origen

El origen de las LAN inalámbricas se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas. En mayo de 1985 el FCC3 (Federal Communications Comission) asignó las bandas IMS4 (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en spread spectrum (frecuencias altas).

[2] SHELDON, Tom, Novel Netware, Cuarta Edición, Mc Graw Hill, 2001.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

1.3.2 Definición

Un conjunto de computadoras que para intercambiar información entre ellas utilizan ondas electromagnéticas, con el objeto de transportar información de un punto a otro sin necesidad de una conexión física. Las ondas de radio frecuencia a menudo se refieren como portadoras de radio, debido a que su única función consiste en entregar la energía que conllevan al receptor remoto.

1.3.3 Elementos

Las redes locales inalámbricas se integran en una red privada igual que las otras redes locales. Por ejemplo, los puntos de acceso de la WLAN se conectan a un hub Ethernet y de este a un encaminador IP.

1.3.4 Servidor

Es la máquina principal de la red. Se encarga de administrar los recursos de esta y el flujo de la información. Algunos servidores son dedicados, es decir, realizan tareas específicas. Por ejemplo, un servidor de impresión está dedicado a imprimir; un servidor de comunicaciones controla el flujo de datos, etc.

Para que una máquina sea un servidor es necesario que sea una computadora de alto rendimiento en cuanto a velocidad, procesamiento y gran capacidad en disco duro u otros medios de almacenamiento.

1.3.4.1 Tipos de servidores

Según la dirección electrónica http://www.monografias.com/trabajos18/redes-computadoras/redes-computadores.html.

a) **Servidor DHCP.-** El DHCP es un protocolo de tipo cliente/servidor que se comunica por el puerto 67 y 68 a través de UDP, generalmente un servidor DHCP posee una lista de direcciones IP dinámicas y las va asignando a las maquinas clientes conforme estas van estando disponibles.
b) **Servidor DNS.-**Asocia distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. Cuando un equipo cliente solicita información desde un servidor de nombres, usualmente se conecta al puerto 53.
c) **Servidor LAMP.-**Un servidor LAMP es un conjunto de aplicaciones instaladas en un servidor Linux los cuales, al trabajar en conjunto logran dar vida a una aplicación mucho más grande y robusta.
d) **Servidor Openfire.-** Es un servidor Jabber/XMPP escrito en Java provee licencias comerciales y GNU. La administración del servidor se hace a través de una interfaz web, que corre por defecto en el puerto 9090 (HTTP) y 9091 (HTTPS). Los administradores pueden conectarse desde cualquier lugar y editar la configuración del servidor, agregar y borrar usuarios, crear cuartos de conferencia permanentes.
e) **Servidor Samba.-**Es la implementación de un código libre para la utilización del protocolo SMB (Server Message Block) el cual permite la compartición de archivos, impresoras y recursos en una red entre equipos Linux y otros.

f) **Servidor FTP.-** Es una de las herramientas más usadas en torno a la administración de portales web y tiene como principal función la transferencia de archivos.[3]

Al respecto los investigadores indican que existe una gran variedad de servidores para múltiples aplicaciones, que también brindan a los desarrolladores una interfaz para programación de aplicaciones, de tal manera que no tengan que preocuparse por el S.O.

1.4 Router.

Es un dispositivo que brinda los mismos servicios que un AP y además realiza funciones de control de esa señal ya que integra varias funciones como Firewall, Nat, Enrutamiento y los servicios de puerta de enlace en una conexión ADSL con este no se necesitarían un router adicional como en los AP, para el servicio ADSL.

GRAFICO Nº 1.1: Router
FUENTE: Grupo Investigador

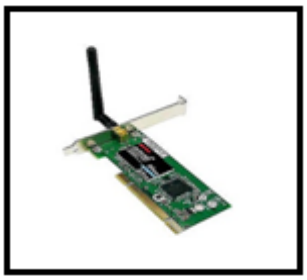
1.5 Tarjetas.

Son todas aquellas tarjetas que nos proporcionan conectividad inalámbrica. Las más conocidas son las que vienen en formato PCMCIA, para portátiles, aunque también las hay

[3] http://www.monografias.com/trabajos18/redes-computadoras/redes-computadores.html.

en formato PCI. Son equivalentes a una tarjeta de red normal, sólo que sin cables que en su posición tienen una pequeña antena. Su configuración a nivel de IP es igual que una tarjeta Ethernet de las alámbricas.[4]

GRAFICO Nº 1.2: TARJETA DE RED
FUENTE: Grupo Investigador



1.6 Antenas.

La dirección electrónica http://es.wikipedia.org/wiki/Wi-Fi dice que:

"Una antena es un dispositivo cuya misión es difundir o recoger ondas radioeléctricas. Las antenas sirven de emisor-receptor de una señal de radio. Estas amplifican la señal de los AP y los Router dándoles mayor rango de alcance o cobertura".

GRAFICO Nº 1.3: ANTENA PARABÓLICA
FUENTE: Grupo Investigador

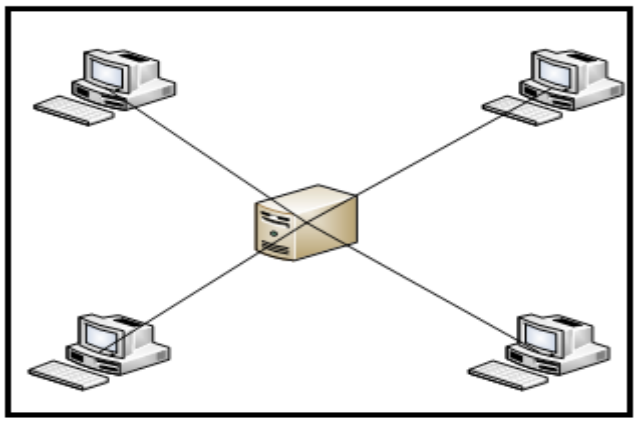
[4] http://es.wikipedia.org/wiki/Wi-Fi.

1.7 TOPOLOGÍAS DE REDES

1.7.1 Topología en estrella.

Todos los elementos de la red se encuentran conectados directamente mediante un enlace punto a punto al nodo central de la red, quien se encarga de gestionar las transmisiones de información por toda la estrella. Evidentemente, todas las tramas de información que circulen por la red deben pasar por el nodo principal, con lo cual un fallo en él provoca la caída de todo el sistema. si bien esta topología obliga a disponer de un cable propio para cada terminal adicional de la red. La topología de Estrella es una buena elección siempre que se tenga varias unidades dependientes de un procesador.

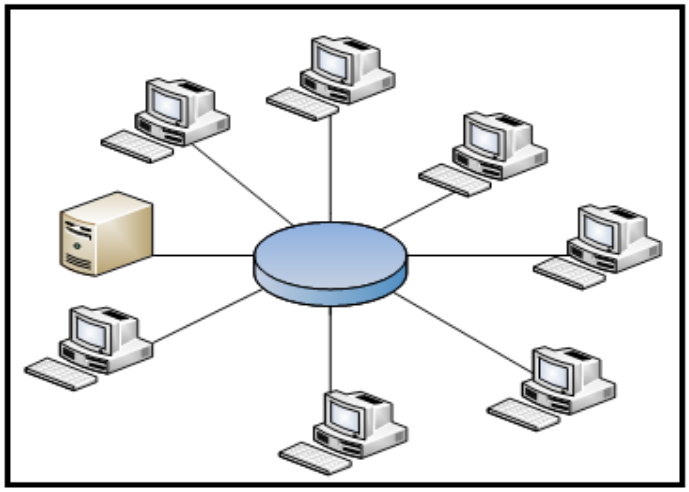
GRÁFICO Nº 1.4: TOPOLOGÍA ESTRELLA
FUENTE: Grupo Investigador



1.7.2 Topología en anillo

Los nodos de la red se disponen en un anillo cerrado conectado a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el nodo principal es quien gestiona conflictos entre nodos al evitar la colisión de tramas de información. En este tipo de topología, un fallo en un nodo afecta a toda la red aunque actualmente hay tecnologías que permiten mediante unos conectores especiales, la desconexión del nodo averiado para que el sistema pueda seguir funcionando. La topología de anillo está diseñada como una arquitectura circular, con cada nodo conectado directamente a otros dos nodos.[5]

GRÁFICO Nº1.5: TOPOLOGÍA ANILLO
FUENTE: Grupo Investigador

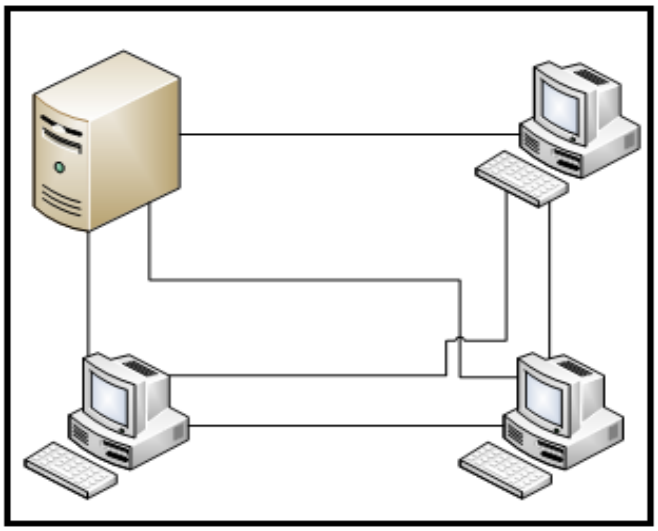


1.7.3 Topología Malla

En la topología malla, cada uno de los nodos se conecta directamente mediante un túnel con otro nodo de la red, creando una maraña de interconexiones. Este tipo de topologías elimina los inconvenientes de la topología estrella, pero presenta la desventaja de un gran aumento en el tiempo de mantenimiento y en las dificultades para añadir nuevos nodos en la red.

[5] http://www.geocities.com/TimesSquare/Chasm/7990/topologi.htm

GRÁFICONº 1.6: TOPOLOGÍA MALLA
FUENTE: Grupo Investigado



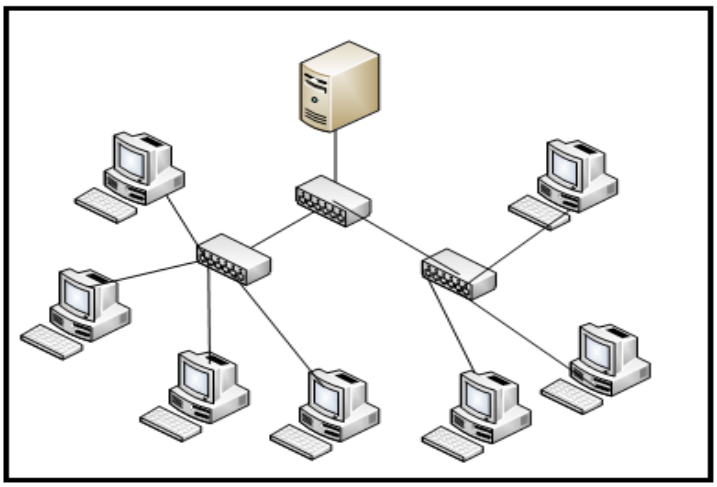
1.7.4 Topología Árbol

Topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas.

Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

Cuenta con un cable principal (backbone) al que hay conectadas redes individuales en bus

GRÁFICO Nº1.7: TOPOLOGÍA ÁRBOL
FUENTE: Grupo Investigador



1.8 ESTÁNDARES DE CALIDAD DE LAS REDES INALAMBRICAS

1.8.1 Descripción

El autor SHELDON, Tom (2004, pág. 4,5) Cuarta Edición enuncia que:

"Esta cláusula específica la extensión de la alta tarifa del PHY para el sistema directo del espectro de la extensión de la secuencia (DSSS) (clausula 15 del IEEE 802.11, en el año 1999, mas luego se aplica como alta tarifa PHY para la banda 2.4 gigahertz señalada para los usos de ISM".[6] Dicha extensión de las estructuras del sistema DSSS en las capacidades de la tarifa de datos, según lo descrito en la cláusula 15 del IEEE 802.11, en el año 1999, para proporcionar 5.5 Mbit/s y 11 tarifas de datos de carga útil de Mbit/s además del 1 Mbps y de 2 tarifas de Mbps. Para proporcionar las tarifas más altas, el código complementario 8-chip que afina (CCK) se emplea como el esquema de la modulación. La tarifa que salta es 11 megaciclos, que es igual el sistema DSSS descrito en la cláusula 15 de IEEE 802.11,del año 1999, así proporcionando la misma anchura de banda ocupada del canal. La nueva capacidad básica descrita en esta clausula se llama el espectro directo de la extensión de la secuencia de alta tarifa (hora DSSS).

[6] SHELDON, Tom, España, Editorial Mac Graw Hill, 2004.

La alta tarifa básica PHY utiliza el mismo preámbulo y el jefe de PLCP que el DSSS PHY, así que PHYs puede coexistir en el mismo BSS y puede utilizar el mecanismo de la conmutación de la tarifa de la manera prevista.

1.8.2 Definición

El primer componente del estándar IEEE 802.11 fue ratificado en 1997 y luego en 1999, cuando también se realizaron las primeras extensiones. La estructura de los estándares de la IEEE es tal que las extensiones se elaboran como modificaciones del estándar original y se nombran agregándole una letra al nombre del estándar. En el caso del 802.11, tenemos extensiones como 802.11a, 802.11b, etc. En realidad, el estándar 802.11es solo una parte de un conjunto más amplio de estándares de IEEE: el 802.11.

1.8.3 Tipos estándares de redes

El Protocolo de red o también Protocolo de Comunicación es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.

1. IEEE 802.3, estándar para Ethernet
2. IEEE 802.5, estándar para Token Ring
3. IEEE 802.11, estándar para Wi-Fi
4. IEEE 802.15, estándar para Bluetooth

1.8.4 Estándar IEEE 802.11 (Wi-Fi)

Bajo el título de “Redes Wi-Fi”, donde Wi-Fi proviene de Wireless Fidelity, agrupamos a un conjunto de redes de área local donde el medio de acceso es inalámbrico. Actualmente,

las redes Wi-Fi están basadas en el conjunto de estándares IEEE**802.11** (IEEE: Institute of Electrical and Electronic Engineers).[7]

1.9 Banda C

1.9.1 Definición.

La **Banda-C** es un rango del espectro electromagnético de las microondas que comprende frecuencias de entre 3,8 y 4,2 GHz y desde 5,9 hasta 6,4 GHz. Fue el primer rango de frecuencia utilizado en transmisiones satelitales. Básicamente el satélite actúa como repetidor, recibiendo las señales en la parte alta de la banda y remitiéndolas hacia la Tierra en la banda baja, con una diferencia de frecuencia de 2.225 MHz. Normalmente se usa polarización circular, para duplicar el número de servicios sobre la misma frecuencia.

1.9.2 Características

- ✓ Frecuencia de entrada 3.8-4.2 GHz
- ✓ Frecuencia de salida 950-1750 MHz
- ✓ Número de salidas 1 Osciladores locales 5150 MHz
- ✓ Tipo de guía de ondas Prime Focus Ganancia mayor 65 dB
- ✓ Consumo 200 mA Alimentación 10-14.5(V) 15.5-25(H)
- ✓ Temperatura de ruido 15 K. 41.27 metros
- ✓ GANANCIAS EN dBi 41.27 metros
- ✓ RELACIÓN F/D 6.10 metros
- ✓ DISTANCIA FOCAL EN METROS 1.09 metros
- ✓ NÚMERO DE SECCIONES 1 metro

1.9.3 Ventajas

[7] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 2000 Edition.

- ✓ Velocidad máxima alta
- ✓ Soporte de muchos usuarios a la vez
- ✓ Rango de señal muy bueno y difícil de obstruir.

1.10 Frecuencia 3.8 GHz.

1.10.1 Definición

Al operar en la frecuencia de 3.8 GHz, se tiene un mejor rendimiento del enlace ya que no van a existir interferencias con otros equipos que se encuentren operando.

1.10.2 Ventajas

- Disponibilidad mundial.

- Tecnología más barata.

- Robustez frente a lluvias.

- Una buena cobertura.

- Técnicas más eficientes FDMA y TDMA frente a CDMA.

- Estaciones más pequeñas (0.6..1.8m)

-Compatibilidad con las redes existentes.[8]

1.11 Tendencia a las telecomunicaciones

1.11.1 Introducción

[8] Hills "Large-Scale Wireless LAN Desing".IEEE Communications Magazine, vol.39,nº 11, noviembre 2001.

La especie humana es de carácter social, es decir, necesita de la comunicación; pues de otra manera viviríamos completamente aislados. Así, desde los inicios de la especie, la comunicación fue evolucionando hasta llegar a la más sofisticada tecnología, para lograr acercar espacios y tener mayor velocidad en el proceso.

1.11.2 Definición.

Según el autor FREDERMAN, Alan, Diccionario de Computación, (2002, pág, 10), expresa que: "Es un conjunto de medios de comunicación a distancia o transmisión de palabras, sonidos, imágenes o datos en forma de impulsos o señales electrónicas o electromagnéticas."[9]

1.11.3 Breve Historia

Desde las primeras máquinas programables manualmente (máquina diferencial de Babbage) o con procedimientos electrónicos (ENIAC, con tubos al vacío, en 1947), hasta nuestros días de potentes computadoras digitales que se han introducido en prácticamente todas las áreas de la sociedad (industria, comercio, educación, comunicación, transporte, etc.). Con todos estos avances tecnológicos y necesidades, la comunicación o transmisión de datos fue tomando cada vez más auge. Los primeros intentos y realizaciones en la tarea de conjugar ambas disciplinas - comunicaciones y procesamiento de datos - tuvieron lugar en Estados Unidos, donde durante años cuarenta del siglo XX se desarrollo una aplicación de inventario para la U.S. Army y posteriormente, en 1953, otra para la gestión y reserva de las plazas en la American Airlines, que constituyeron los dos primeros sistemas de procesamiento de datos a distancia.

Con esta nueva necesidad y estas herramientas, surgen las Redes de Computadoras, las cuales son ya muy comunes en nuestros días, en los inicios de la transmisión por televisión y con el uso de las computadoras, la especie humana logra lanzar un vehículo espacial y tiempo después lanza los primeros satélites artificiales. Los cuales son aparatos muy

[9] FREDERMAN, Alan, Diccionario de Computacion, Edicion marzo 2002, Bogota-Colombia.

sofisticados con fines múltiples (científicos, tecnológicos y militares). El primer satélite artificial, el Sputnik 1, fue lanzado por la Unión Soviética el 4 de octubre de 1957. El primer satélite de Estados Unidos fue el Explorer 1, lanzado el 31 de enero de 1958, y resultó útil para el descubrimiento de los cinturones de radiación de la Tierra.

En la actualidad hay satélites de comunicaciones, navegación, militares, meteorológicos, de estudio de recursos terrestres y científicos. La mayor parte de ellos son satélites de comunicación, utilizados para la comunicación telefónica y la transmisión de datos digitales e imágenes de televisión.[10]

1.12 Códigos de encriptación (PKI)

1.12.1 Definición

Según la dirección electrónica www.linuxparatodos.org dice que:

"PKI (*Public Key Infrastructure; en castellano, Infraestructura de Clave Pública*) se refiere a un grupo de soluciones técnicas basadas en criptografía de clave pública".[11]

Los criptosistemas de clave pública permiten omitir la necesidad de utilizar sistemáticamente un canal seguro para el intercambio de claves. Sin embargo, es necesario que la publicación a gran escala de claves públicas se base en una total confianza para garantizar que:[12]

- la clave pública pertenece realmente a su dueño,
- el dueño de la clave es de confianza,
- la clave tiene validez.

[10] Carballar, José A. El libro de las Comunicaciones del PC, HP, España,2006. Pág. 10-14
[11] www.linuxparatodos.org
[12] MIKHAILOVSKY Andrei A. (2005); El mundo de la seguridad inalámbrica;ediciones AMAYA S.A, Madrid

Así pues, la clave compuesta por dos partes (clave pública/clave privada) necesita estar asociada a un certificado otorgado por una tercera parte de confianza: la infraestructura de la clave pública.

Una PKI bien construida debe proporcionar:

• **Autenticidad**. La firma digital tendrá la misma validez que la manuscrita.

• **Confidencialidad**, de la información transmitida entre las partes.

• **Integridad**. Debe asegurarse la capacidad de detectar si un documento firmado ha sido manipulado.

• **No Repudio**, de un documento firmado digitalmente.

1.12.2 CARACTERISTICAS

La Autoridad de Certificación. La pieza central del "puzzle" y la que proporciona la base de confianza en la PKI. Constituido por elementos hardware, software y, evidentemente, humanos.

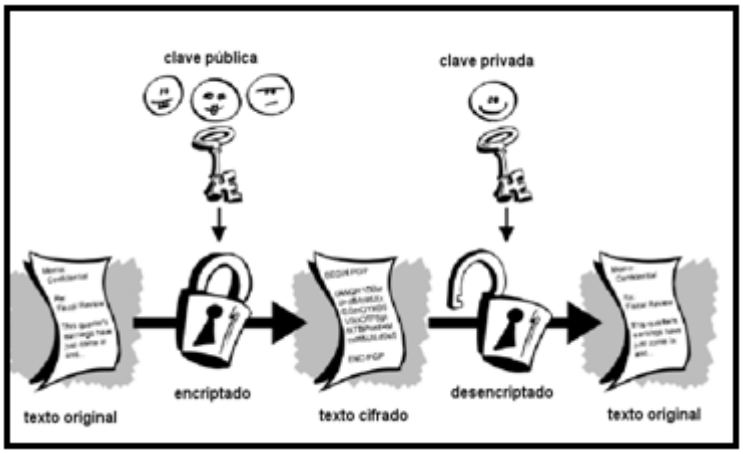
Publicación de Certificados. El repositorio de certificados permite a los usuarios operar entre ellos (p.e. para la validación de una Firma Digital), y es un requisito legal que cuente con una total disponibilidad de acceso.

Soporte de la Clave Privada. La elección de un buen soporte para que los usuarios custodien su clave privada es un punto esencial y complejo en si mismo (p.e. si la clave está en una SmartCard, es necesario diseñar el Sistema de Gestión de SmartCards que permita la emisión y distribución de las tarjetas a los usuarios).

Aplicaciones "PKI-Enabled". Se denomina así a las aplicaciones software capaces de operar con certificados digitales. Estas aplicaciones son las que dan el valor real de la PKI de cara al usuario.

Políticas de Certificación. Deben diseñarse una serie de políticas, o procedimientos operativos, que rigen el funcionamiento de la PKI y establecen los compromisos entre la Autoridad Certificadora y los Usuarios Finales. Estos documentos tendrán un carácter tanto técnico como legal.

GRÁFICO Nº 1.8: MODO DE ENCRIPTACIÓN
FUENTE: Grupo Investigador



1.12.3 Ventajas

- ✓ PKI de firma digital proporcionan una forma de certificar una operación, que tiene capacidad jurídica.
- ✓ PKI proporciona un método más fiable.
- ✓ Proporciona cifrado de datos. Debido a la encriptación, un tercero no puede modificar los datos sin el tamper reconociendo inmediatamente el resultado. Por lo tanto, el cifrado es muy útil en la toma de datos seguro.
- ✓ Ofrece encriptación de datos utilizando **la clave pública** del **destinatario** que hace que los datos sean ilegibles por cualquier tercero. Así pues, cualquiera que intente interceptar la transmisión de datos no sería capaz de leerlo.[13]

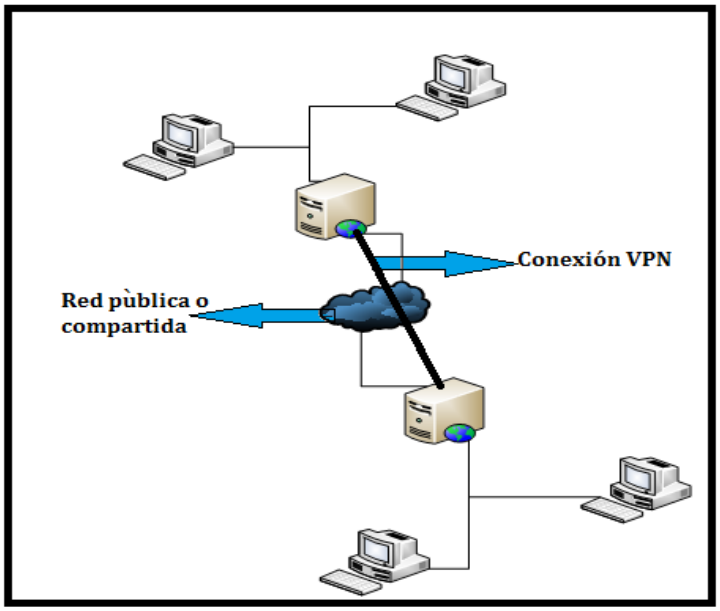
1.13 RED PRIVADA VIRTUAL (VPN)

[13] http://www.rsasecurity.pki.com

1.13.1 Definición

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

GRÁFICO Nº 1.9: VPN
FUENTE: Grupo Investigador



La VPN (Red Privada Virtual). Es una tecnología de red que permite una extensión de la red local sobre una red pública por ejemplo una empresa u organización. Con la implantación de la Red Privada Virtual (VPN), se desea proporcionar las siguientes facilidades:

- **Autenticación del usuario:** La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados.

- **Administración de direcciones:** La VPN debe establecer una dirección del cliente en una red privada y debe cerciorarse que las direcciones privadas se conserven así y no sean modificadas.
- **Codificación de datos:** los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.
- **Administración de claves:** La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.
- **Soporte de protocolos múltiples:** La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública.

1.13.2 Características

- ✓ Una **Red Privada Virtual (VPN)** consiste en dos máquinas (una en cada "extremo" de la conexión) y una ruta o "túnel" que se crea dinámicamente en una red pública o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos ordenadores son encriptados por el Point-to-Point Protocol, también conocido como PPP.

- ✓ Una **Red Privada Virtual** es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión.
- ✓ Los datos viajan encapsulados por el túnel, con una cabecera que contiene información sobre su destino y la ruta que debe tomar hasta llegar a él. En una VPN cada cliente tiene una dirección IP de forma que esta dirección sólo podrá ser vista por los componentes de la VPN, y no podrá ser accesible desde fuera.

- ✓ Las **VPN** constituyen una estupenda combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y lo escalable del acceso a través de Internet. Esta combinación hace de las Redes Privadas Virtuales o VPNs una **infraestructura confiable y de bajo costo** que satisface las necesidades de comunicación de cualquier organización.[14]

1.13.3 Herramientas de una VPN

VPN Gateway

Software

Firewall

Router

VPN Gateway

Dispositivos con un software y hardware especial para proveer de capacidad a la VPN Software.
Esta sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN.

1.13.4 Ventajas

Dentro de las ventajas más significativas podremos mencionar la integridad, confidencialidad y seguridad de los datos.

- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.

[14] http://www.microsoft.com/spain/isaserver/prodinfo/features.mspx

- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.[15]

1.13.5 ARQUITECTURAS VPN

El éxito de una VPN depende de una adecuada elección de la tecnología y del escenario, siempre acordes a las necesidades que se tengan.

La tecnología implica: técnicas de entunelamiento, autenticación, control de acceso, y seguridad de los datos; y los escenarios que se pueden construir son:

Intranet VPN (LAN-to-LAN VPN), Acceso Remoto VPN y Extranet VPN.

Intranet VPN (LAN-to-LAN VPN): En este escenario, múltiples redes remotas de la misma compañía son conectadas entre si usando una red pública, convirtiéndolas en una sola LAN corporativa lógica, y con todas las ventajas de la misma.

Acceso Remoto VPN: En este caso, un host remoto crea un túnel para conectarse a la Intranet corporativa. El dispositivo remoto puede ser un computador personal con un software cliente para crear una VPN, y usar una conexión conmutada, o una conexión de banda ancha permanente.

Extranet VPN: Esta arquitectura permite que ciertos recursos de la red corporativa sean accesados por redes de otras compañías, tales como clientes o proveedores. En este escenario es fundamental el control de acceso.[16]

1.14 SOFTWARE LIBRE

1.14.1 Definición.

El software libre es una cuestión de la libertad de los usuarios de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software.

---

[15] http://www.divisait.com/docs/Hojas%20de%20Aplicacion/VNPs%20y%20Redes%20Seguras_v.2.0_.pdf

[16] http://www.laserwifi.com/arquitecturavpn.htm

1.14.2 Características.

- ✓ Libertad de redistribución proporciona, en la práctica, una canal de distribución de gran eficiencia económica, y de muy bajo coste para el productor.
- ✓ Las posibilidades de modificación y de redistribución de las modificaciones facilitan la evolución y mejora técnica de los programas.
- ✓ Y de la aplicación de todas las libertades simultáneamente se deducen importantes sinergias, que hacen que el software libre se comporte de una forma tan especial.[17]

1.14.3 Ventajas.

1. Económico.- El bajo o nulo coste de los productos libres proporciona servicios y ampliar sus infraestructuras sin que se vean mermados sus intentos de crecimiento por no poder hacer frente al pago de grandes cantidades en licencias.

2. Libertad de uso y redistribución.- Permiten la instalación del software tantas veces y en tantas máquinas como el usuario desee.

3. Independencia tecnológica.- Permite el desarrollo de nuevos productos sin la necesidad de desarrollar todo el proceso partiendo de cero.

4. Fomento de la libre competencia al basarse en servicios y no licencias.- Este sistema permite que las compañías que den el servicio compitan en igualdad de condiciones al no poseer la propiedad del producto del cual dan el servicio.

5. Formatos estándar.- Permiten una inter operatividad más alta entre sistemas, evitando incompatibilidades.

6. Sistemas sin puertas traseras y más seguros.- El acceso al código fuente permite que tanto hackers como empresas de seguridad de todo el mundo puedan auditar los programas.

[17] Jesus M. Gonzalez-Barahona 2003-04-06

7. Corrección más rápida y eficiente de fallos.- El funcionamiento e interés conjunto de la comunidad ha demostrado solucionar más rápidamente los fallos de seguridad en el software libre, algo que desgraciadamente en el software propietario es más difícil y costoso.

8. Métodos simples y unificados de gestión de software.- Esto llega a simplificar hasta el grado de marcar o desmarcar una casilla para la gestión del software, y permiten el acceso a las miles de aplicaciones existentes de forma segura y gratuita.

9. Sistema en expansión.- El software libre ya no es una promesa, es una realidad y se utiliza en sistemas de producción por algunas de las empresas tecnológicas más importantes como IBM, SUN Microsystems, Google, Hewlett-Packard, etc.[18]

1.15 Sistema Operativo Linux

1.15.1 Definición.

Linux es un sistema operativo diseñado por cientos de programadores de todo el planeta, aunque el principal responsable del proyecto es Linus Tovalds. Su objetivo inicial es propulsar el software de libre distribución junto con su código fuente para que pueda ser modificado por cualquier persona, dando rienda suelta a la creatividad. El hecho de que el sistema operativo incluya su propio código fuente expande enormemente las posibilidades de este sistema. Este método también es aplicado en numerosas ocasiones a los programas que corren en el sistema, lo que hace que podamos encontrar muchísimos programas útiles totalmente gratuitos y con su código fuente. Linux es un sistema operativo totalmente gratuito.

1.15.2 Características

Multitarea: varios programas (realmente procesos) ejecutándose al mismo tiempo.

Multiusuario: varios usuarios en la misma máquina al mismo tiempo (y sin licencias para todos).

[18] http://congreso.hispalinux.es/

Multiplataforma: corre en muchas CPUs distintas, no sólo Intel.

Tiene protección de la memoria entre procesos, de manera que uno de ellos no pueda colgar el sistema.

Carga de ejecutables por demanda: Linux sólo lee de disco aquellas partes de un programa que están siendo usadas actualmente.

Política de copia en escritura para la compartición de páginas entre ejecutables: esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse.

Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.

Memoria virtual usando paginación (sin intercambio de procesos completos) a disco: una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha (se sigue denominando intercambio, es en realidad un intercambio de páginas).

La memoria se gestiona como un recurso unificado para los programas de usuario y para el caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y éste puede a su vez ser reducido cuando se ejecuten grandes programas.

Permite el uso de depuradores sobre los programas no sólo en ejecución sino también tras abortar éstos por cualquier motivo.

Todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario; además todo ello se puede distribuir libremente.

Los programas no tienen que hacer su propia emulación matemática. Cualquier máquina que ejecute Linux parecerá dotada de coprocesador matemático, será usada en lugar de la

emulación, pudiendo incluso compilar el propio kernel sin la emulación matemática y conseguir un pequeño ahorro de memoria.

Consolas virtuales múltiples: varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de video).

Acceso transparente a particiones MS-DOS (o a particiones OS/2 FAT) mediante un sistema de archivos especial: no necesitas ningún comando especial para usar la partición MS-DOS, parece un sistema de archivos normal de Unix (excepto por algunas graciosas restricciones en los nombres de archivo, permisos, y esas cosas).[19]

1.15.3 Ventajas

- ✓ Linux es uno de los sistemas operativos más robustos, estables y rápidos
- ✓ Linux es básicamente un duplicado de UNIX, lo que significa que incorpora muchas de las ventajas de este importante sistema operativo.
- ✓ En Linux pueden correr varios procesos a la vez de forma ininterrumpida como un servidor de red al tiempo que un procesador de textos, una animación, copia de archivos o revisar el correo electrónico.
- ✓ Seguridad porque es un sistema operacional diseñado con la idea de Cliente - Servidor con permisos de acceso y ejecución a cada usuario. Esto quiere decir que varios usuarios pueden utilizar una misma máquina al tiempo sin interferir en cada proceso.
- ✓ Linux es software libre, gratuito. Linux es popular entre programadores y desarrolladores e implica un espíritu de colaboración.
- ✓ Linux integra una implementación completa de los diferentes protocolos y estándares de red, con los que se puede conectar fácilmente a Internet y acceder a todo tipo de información disponible.

[19] http://www.monografias.com/trabajos/solinux/solinux.shtml

- ✓ Su filosofía y sus programas están dictados por el movimiento ``Open Source'' que ha venido creciendo en los últimos años y ha adquirido suficiente fortaleza para hacer frente a los gigantes de la industria del software.
- ✓ Linux puede ser utilizado como una estación personal pero también como un potente servidor de red.
- ✓ Linux incorpora una gama de sistemas de interfaz gráfica (ventanas) de igual o mejor calidad que otras ofrecidas en muchos paquetes comerciales.
- ✓ Posee el apoyo de miles de programadores a nivel mundial.
- ✓ El paquete incluye el código fuente, lo que permite modificarlo de acuerdo a las necesidades del usuario.
- ✓ Utiliza varios formatos de archivo que son compatibles con casi todos los sistemas operacionales utilizados en la actualidad.[20]

1.15.4 Plataformas de Linux.

UBUNTU

Distribución basada en Debian, con lo que esto conlleva y centrada en el usuario final y facilidad de uso. Muy popular y con mucho soporte en la comunidad. El entorno de escritorio por defecto es GNOME.

REDHAT ENTERPRISE

[20] http://www.maginvent.org/articles/linuxmm/Ventajas_Linux.html

Esta es una distribución que tiene muy buena calidad, contenidos y soporte a los usuarios por parte de la empresa que la distribuye. Es necesario el pago de una licencia de soporte. Enfocada a empresas.

FEDORA

Esta es una distribución patrocinada por RedHat y soportada por la comunidad. Fácil de instalar y buena calidad.

DEBIAN

Otra distribución con muy buena calidad. El proceso de instalación es quizás un poco más complicado, pero sin mayores problemas. Gran estabilidad antes que últimos avances.

OpenSuSE

Otra de las grandes. Fácil de instalar. Versión libre de la distribución comercial SuSE.

GENTOO

Esta distribución es una de las únicas que incorporaron un concepto totalmente nuevo en Linux. Es un sistema inspirado en BSD-ports. Podeis compilar/optimizar nuestro sistema.[21]

1.16 CentOS.

1.16.1 Definición.

CentOS es una distribución de Linux gratuita que está basada en la distribución Red Hat Enterprise Linux (RHEL). CentOS es muy similar al RHEL, pero gratuito, aunque no es mantenido por Red Hat. CentOS (CommunityENTerpriseOperatingSystem) es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.[22]

1.16.2 Características

- ✓ Fácil mantenimiento
- ✓ Idoneidad para el uso a largo plazo en entornos de producción
- ✓ Entorno favorable para los usuarios y mantenedores de paquetes

[21] http://www.iearobotics.com/personal/juan/publicaciones/art5/html/node2.html
[22] http://www.mastermagazine.info/articulo/10564.php

- ✓ Apoyo a largo plazo de las principales
- ✓ Desarrollo activo
- ✓ La infraestructura de la comunidad
- ✓ Abierto de gestión
- ✓ Modelo de negocio abierto
- ✓ Apoyo comercial - ofrecido por un socio proveedor[23]

1.16.3 Ventajas

- ✓ Incluye el clon: una activa y creciente comunidad de usuarios
- ✓ Rápidamente reconstruido, probado y QA'ed paquetes de erratas
- ✓ Un amplio espejo de red, desarrolladores que están continuada y sensible, libre de múltiples vías de apoyo incluyendo IRC Chat, listas de correo, foros, una dinámica de preguntas frecuentes

- ✓ Comercial se ofrece apoyo a través de un número de proveedores.
- ✓ CentOS existencia de la libre empresa una clase de computación plataforma para cualquiera que desee utilizarlo. CentOS 2 y 3 son totalmente compatibles reconstruye de RHEL 2 y 3, respectivamente.
- ✓ Redistribuir los paquetes y las fuentes de cumplir plenamente con RedHat requisitos de la redistribución. CentOS 2 y 3 están diseñados para personas que necesitan un sistema operativo de clase empresarial sin el costo, el apoyo, la certificación, la marca o nombre de RedHat.[24]

[23] http://www.taringa.net/posts/linux/1601181/CentOS-5_2.html
[24]http://www.taringa.net/linux/1601181/CentOS-5_2.html

CAPÍTULO II

TRABAJO DE CAMPO

2. ANALISIS DE CAMPO PARA LA IMPLANTACION DE LA RED LAN EN EL ENTORNO DE LA DIRECCIÓN NACIONAL DE COMUNICACIONES

2.1 ANTECEDENTES

En el año de 1960 el Punto IV dentro del Programa Alianza para El Progreso entrega a la Policía Nacional equipos que conforman el sistema convencional VHF-FM fijo-móvil, para las ciudades de Quito y Guayaquil, equipamiento que operaba en modo claro y con un sólo canal, así como también equipos HF (Radiofonía) los mismos que fueron instalados en

todas las capitales de provincia y sus principales Cantones, permitiendo una cobertura a nivel nacional, equipos que debido a su uso, falta de repuestos y condiciones atmosféricas de propagación quedaron fuera de servicio.

En el año de 1970 este sistema es mejorado en su capacidad, con la implementación de una Repetidora en la frecuencia VHF como punto de enlace y ampliación de cobertura, ubicadas una en Puengasi (Quito) y otra en Cerro Azul (Guayaquil), facilitando la utilización de 2 canales, que permitían operar en forma independientemente a los servicios urbano y de tránsito dentro de estas principales urbes. Sin embargo este sistema no disponía de ningún tipo de seguridad, ya que sus mensajes eran monitoreados y detectados permanentemente por personas inescrupulosas que tratan de obtener provecho de estas falencias, además la banda de frecuencias VHF es utilizada por empresas de seguridad privada, periodistas, empresas comerciales, entre otras.

En el año 1987 en el Gobierno del señor Ing. León Febres Cordero Presidente Constitucional de la República, se firma el Decreto Ejecutivo Nro. 2765 de fecha 31 de Marzo de 1987, otorgándole a la Compañía Francesa Alcatel Thomson la provisión e instalación de una red de tecnología vía microondas. El 5 de febrero de 1991 entra en funcionamiento esta red moderna de comunicación vía microondas (SMOP), enlazando a todas las capitales de provincia y 7 Cantones importantes, excepto a Galápagos, con servicios de telefonía fija, correo electrónico y fax. El diseño de la red obedece a las características propias de empleo policial para la transmisión de voz, sus exigencias estaban íntimamente relacionadas al cumplimiento la misión Institucional.

Adjudicación del contrato a la compañía TRANSTOOLS S.A. y UNISYS (España), el 8 de diciembre de 1999 y firmado el 28 de julio del 2001. El 31 de mayo del 2002 se aprueba el crédito para la ejecución del SII-PN a través del Deutsch Bank. El 13 de junio del 2002 el Comité de Implantación y el Sr. Comandante General aprueban la actualización tecnológica de los componentes del proyecto.

El plazo de ejecución del Proyecto SII-PN es de 18 meses. Es el medio de comunicación indispensable para la interconexión de las redes (LAN, MAN, WAN) del SII-PN, para la transferencia de datos desde las estaciones terminales en el país, hasta el Centro de Datos de la DINACOM.

La conectividad es proporcionada por empresas públicas o privadas, las que a través de contratos de arrendamiento ofrecen estos servicios en todo el territorio ecuatoriano. (Andinadatos, Etapa, Pacifictel, otros). Decreto Ejecutivo Reservado No. 25 de 3 de Octubre del 2001. La Policía Nacional contrata a la Empresa Motorola, la adquisición e instalación de 25 estaciones repetidoras, 66 estaciones de radio fijas, 22 inyectores de códigos y 1265 estaciones de radio móviles.

2.2 FUNCIONES

- Formular el programa anual de trabajo concordante al Plan estratégico elaborado por la Asesoría Técnica y someter a conocimiento y aprobación del Escalón Superior.
- Planificar, organizar, supervisar y evaluar los recursos técnicos, de todas las áreas informáticas de la Institución.
- Elaborar procesos de análisis administrativos permanentes y recomendar su aplicación en las dependencias policiales.
- Revisar los procedimientos de las dependencias a ser automatizadas y proponer su reorganización, de ser el caso.
- Evaluar el rendimiento de las dependencias con fines técnicos e informáticos y proponer alternativas de organización.
- Utilizar los medios técnicos de que dispone, para aportar a él o a los proyectos que la Dirección Nacional emprenda.

2.3 MISIÓN

La Dirección Nacional de Comunicaciones, tiene por misión esencial liderar la prestación de los servicios de comunicaciones e informática, a través de una constante preparación del elemento humano y la utilización de la tecnología adecuada que garantice la eficiencia y eficacia en su empleo, en beneficio institucional y de la comunidad.

2.4 VISIÓN

A la Dirección Nacional de Comunicaciones, le corresponde desarrollar las funciones de comunicaciones e informática, para apoyar todas las labores de la Policía Nacional a fin de optimizar la gestión institucional.

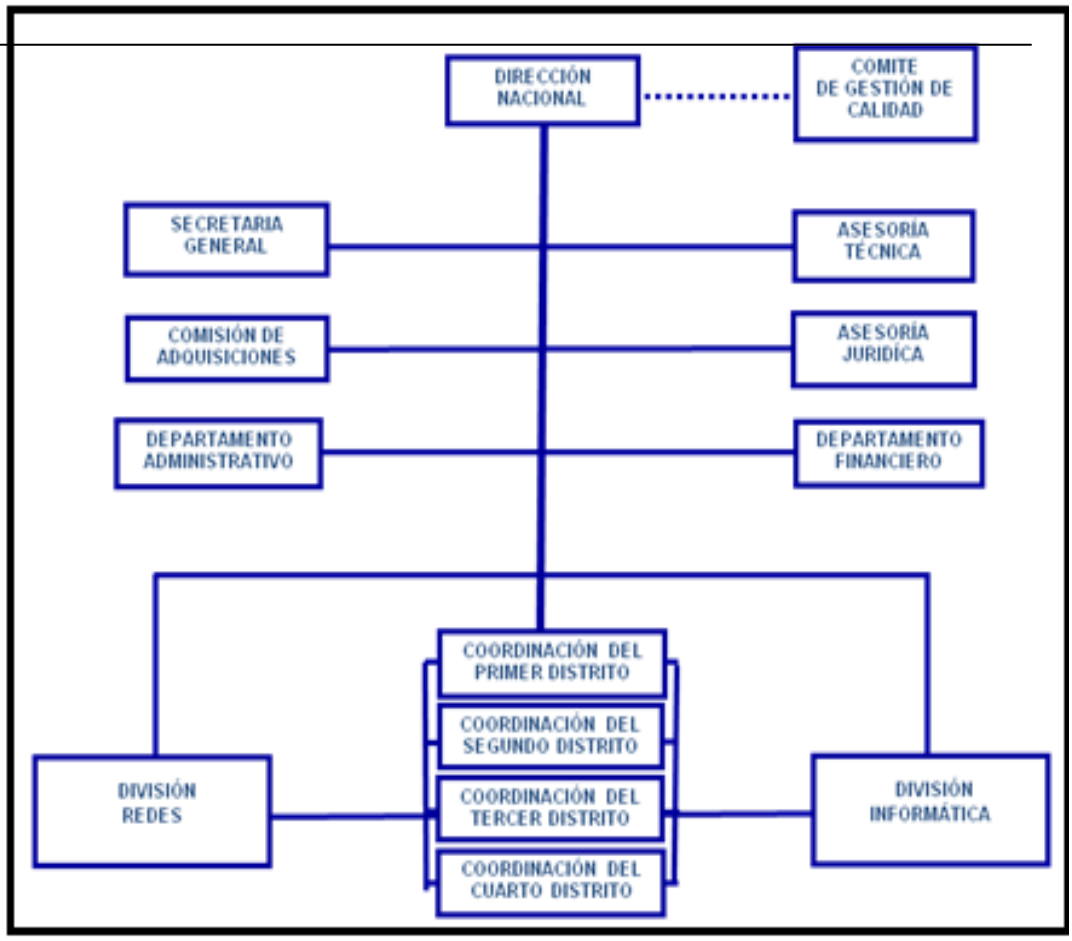
2.5 VALORES

- Comunicación
- Iniciativa
- Trabajo en Equipo
- Lealtad y Honestidad

2.6 ESTRUCTURA ORGANIZACIONAL

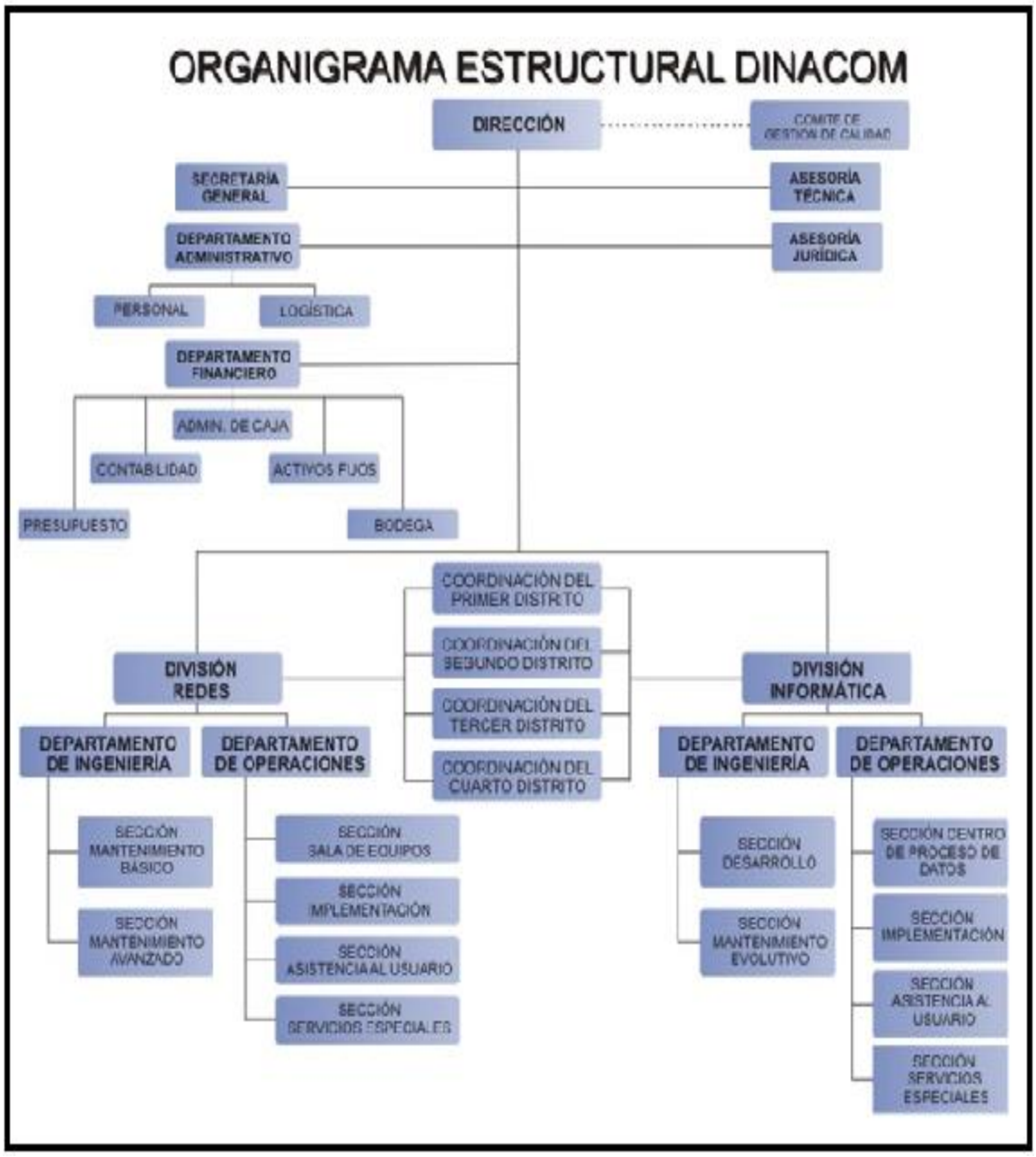
La Dirección Nacional de Comunicaciones de la policía, está organizada de la siguiente manera**:**

GRAFICO Nº 2.1: ESTRUCTURA ORGANIZACIONAL
FUENTE: Grupo Investigador



2.7 Organigrama estructural de la DINACOM

GRAFICO Nº 2.2: ORGANIGRAMA ESTRUCTURAL
FUENTE: Grupo Investigador



2.8 Análisis FODA

El diagnóstico de la situación actual se realizo con la participación de los Administradores de la red y los señores policías trabajadores de las diferentes áreas de la DINACOM.

TABLA Nº 2.1 MATRIZ FODA
FUENTE: Grupo Investigador

FORTALEZAS (+)	OPORTUNIDADES (-)
1. Policías y Jefes dispuestos a Capacitarse. 2. La comunidad policial práctica valores 3. Laboratorio de cómputo adecuado 4. Planificación adecuada a la realidad 5. Infraestructura de la Institución 6. Ubicación geográfica de la Institución	1. Existencia de Seminarios en Instituciones de Prestigio. 2. Apoyo de las autoridades y miembros policiales para la investigación tecnológica. 3. Convenios con Organismos Institucionales
DEBILIDADES (-)	AMENAZAS (-)
1. Falta de acondicionamiento de laboratorio de cómputo 2. Falta de motivación a los señores policías de la Institución 3. Falta de capacitación especializada y actualización en áreas especificas 4. Escaso liderazgo por parte de las autoridades	1. Descuido de las autoridades por pases intempestivos 2. Cambio de los policías a otras ciudades sin aviso previo 3. Contaminación ambiental 4. Desvalorización a los policías en la sociedad
PROBLEMAS	

2.9 Muestra

En la Dirección Nacional de Comunicaciones no existe una población extensa, razón por la cual no amerita el cálculo respectivo para la muestra.

La investigación del proyecto: **IMPLANTACIÓN DE LA RED LAN INALAMBRICA EN LA BANDA DE 3.8 GHZ, UTILIZANDO CÓDIGOS DE ENCRIPTACIÓN PKI Y VPN PARA SEGMENTACION DE NODOS A TRAVES DE SOFTWARE LIBREEN LA DIRECCIÓN NACIONAL DE COMUNICACIONES DE LA POLICIA,** llevó a la necesidad de aplicar los instrumentos de investigación como son las entrevistas y encuestas, realizadas con el fin de recolectar la información necesaria para realizar el desarrollo del sistema propuesto.

En lo referente a la entrevista se tomo como muestra a los Señores Administradores de la red de la Dirección Nacional de Comunicaciones de la Policía, con el único fin de obtener una interrelación y conocimiento profundo de cómo la Implantación de la red LAN inalámbrica en la banda de 3.8 GHz utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través del software libre, podrá influir en los procedimientos del proceso de implantación y manejo de la DNC.

Como también se aplicaron encuestas a los señores policías de cada uno de las áreas de trabajo: jefe del área de soporte Técnico y policías, jefe de Centro de Datos y policías, jefe de Dirección Financiera y policías, jefe de Redes y policías, jefe de Base de Datos y policías, jefe de Ingeniería y policías; muestra que involucra a todos los responsables directos de llevar en adelante el manejo integrado de toda la red inalámbrica y la seguridad que brinda con una velocidad más eficiente, señalando los problemas y dando soluciones a los mismos para que la Implantación de la red inalámbrica y los códigos de encriptación PKI y VPN pueda ser desarrollada de la mejor manera.

2.10 Análisis de los resultados de la entrevista realizada a los administradores de la red de la Dirección Nacional de Comunicaciones.

ENTREVISTA DIRIGIDA ALOS SEÑORES ADMINISTRADORES DE LA RED INALAMBRICA DE LA DIRECCION NACIONAL DE COMUNICACIONES DE LA POLICIA NACIONAL, ING. XAVIER ORELLANA E ING. JUAN CARLOS MEDINA

Para la Entrevista se planteó como principal objetivo conocer cuáles son las expectativas que se crean en los administradores de la red de la DINACOM con la implantación de una red inalámbrica en la banda de 3.8 GHz, el mismo que va a contar con seguridades que precautelen la información como son los códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre.

El Director de Informática considera que es importante cooperar con el avance tecnológico y más aún si va en beneficio de la Policía Nacional ya que la institución es una dependencia muy importante que se encarga de impartir sus servicios a la comunidad policial.

Administradores afirman que en la actualidad cuentan con equipos muy bien dotados tecnológicamente y que esto es un potencial que tiene que ser aprovechado por los señores policías, tratando siempre de cuidar ya que el beneficio o el perjuicio irían directamente contra ellos.

Por el momento para la administración de la red inalámbrica lo realizan 2 administradores, el primero para los departamentos de Soporte Técnico, Base de Datos, Redes y el segundo para los departamentos de Informática, Financiero y Personal.

De igual manera argumentan que no se puede pasar la administración de la red a personas particulares o ajenas a la institución ya que la Policía Nacional maneja información delicada y confidencial razón por la cual han tomado de manera positiva la implantación de la red con las seguridades planteadas así como también el uso del software libre que es un decreto del gobierno que toda institución pública o privada utilicen software libre.

INTERPRETACIÓN

Después de haber realizado la entrevista a los señores; Administrador de la red de la Dirección Nacional de Comunicaciones de la Policía Nacional, creemos conveniente realzar algunos aspectos, que como grupo investigador consideramos aportarán significativamente al proceso de la realización de la implantación de la red Inalámbrica en

la banda de 3.8 GHz, utilizando códigos de encriptación y VPN a través de software libre, que beneficiara sin lugar a duda a la Dirección Nacional de Comunicaciones, en el manejo y flujo de la información.

Tanto los Administradores de la Red, están completamente de acuerdo con la implantación de la red inalámbrica en la banda de 3.8 GHz utilizando códigos de encriptación PKI y VPN dentro de la Institución; porque con este proyecto se dará el mejoramiento de la fluidez de la información, seguridad en los aspectos tecnológicos, organizacional, funcional y económico.

2.10.1 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS EN LAS ENCUESTAS REALIZADAS A LOS SEÑORES POLICIAS DE LA DIRECCIÓN NACIONAL DE COMUNICACIONES.

Anexo N° 1 (Encuestas)

A continuación se muestra los resultados obtenidos luego de la aplicación del instrumento de investigación, como es la encuesta a los señores policías de la Dirección Nacional de Comunicaciones DNC**,** los mismos que son presentados a través de tablas, para luego hacerlo por medio de gráficas en pastel y finalmente efectuar el análisis e interpretación de los resultados:

1. ¿La recolección de información que maneja la Dirección Nacional de Comunicaciones de la Policía Nacional en la actualidad es:

TABLA N° 2.2 RECOLECCION DE LA INFORMACION

Opción	**Valor**	**%**
Manual	3	15%
Automatizada	3	15%
Mixta	14	70%

TOTAL	20	100%

FUENTE: Encuesta
REALIZADO POR: Grupo Investigador

VER ANEXO 2.1

GRÁFICO N° 2.3 RESULTADO DE LA RECOLECCION DE LA INFORMACION

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Los encuestados al respecto de la recolección de la información indican que en un 70% se efectúa de forma Mixta, resultando esta técnica bastante lenta y tediosa para los policías, los que tienen que entregar información rápida a los Jefes de los diferentes departamentos que existen en dicha Institución, por lo tanto se puede afirmar que es de vital importancia recolectar la información de una manera automatizada, por lo que mejorará los procesos.

2. Piensa usted que el manejo de la información que actualmente tiene la Dirección Nacional de Comunicaciones de la Policía Nacional es:

TABLA N°2.3 MANEJO DE LA INFORMACIÓN DE LA DNC

Opción	**Valor**	**%**
Excelente	3	15%
Buena	13	65%
Regular	4	20%

Mala		0%
TOTAL:	20	**100%**

FUENTE: Encuesta
REALIZADO POR: Grupo Investigador

VER ANEXO 2.2

GRÁFICO N°2.4 MANEJO DE LA INFORMACIÓN DE LA DNC

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Los señores policías de la DNC al respecto del manejo de la información que actualmente tienen es, en un 15% excelente, 65% buena y 20% regular, debido a varios factores que ellos nombran como negativos para el ágil manejo de la información como son la tardanza en recolectar la información, excesiva cantidad de datos en papel, etc. Por lo cual resultaría muy atractiva la opción de implantar una red LAN inalámbrica en la banda de 3.8 GHz que facilite el manejo de la información, dentro de la Institución.

3. Opina usted que con la implantación de la red inalámbrica en la banda de 3.8 GHz utilizando códigos de encriptación y VPN mejorará el control, manejo y seguridad en la información.

TABLA N°2.5 MEJORAMIENTO DEL CONTROL

Opción	**Valor**	**%**
En gran cantidad	20	100%
En media cantidad	0	0%

En ninguna cantidad	0	0%
TOTAL	20	100%

FUENTE: Encuesta
REALIZADO POR: Grupo Investigador

VER ANEXO 2.3

GRÁFICO N°2.6 MEJORAMIENTO DEL CONTROL

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Al respecto los señores policías encuestados indican en un 100%que con la implantación de la Red inalámbrica en la banda de 3.8 GHz utilizando códigos de encriptación y VPN se mejorará el control y manejo integrado de la información. Lo cual da la pauta al grupo de investigadores para que se aumente la posibilidad de manejar información hasta llegar a la excelencia.

4. Cree usted que es factible utilizar los códigos de encriptación PKI y VPN con tecnología inalámbrica para facilitar las labores de recolección de datos.

TABLA N°2.5 TECNOLOGÍA INALAMBRICA

Opción	**Valor**	**%**
Si	17	85%
No	3	15%

TOTAL	20	100%

FUENTE: Encuesta
REALIZADO POR: Grupo Investigador

VER ANEXO 2.4

GRÁFICO N°2.7 TECNOLOGÍA INALÁMBRICA

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En un 85% los señores policías se encuentran en total acuerdo, ya que al utilizar los códigos de encriptación PKI y VPN con tecnología inalámbrica a fin de facilitar las labores que ellos efectúan día por día en la recolección de los datos.las PKI son claves complementarias y solo pueden ser generadas una a partir de otra. Por cuanto con la tecnología inalámbrica se puede afirmar que se eliminará la necesidad de utilizar cables añadiendo flexibilidad al trabajo de recolección de datos en toda la extensión de los departamentos, que efectúan los miembros policiales.

5. Cree usted que con la implantación de la red inalámbrica utilizando códigos de encriptación PKI y VPN se agilitara el manejo integrado de la información.

TABLA N°2.6 MANEJO INTEGRADO DE INFORMACIÓN

Opción	**Valor**	**%**
Mucho	11	55%
Poco	7	35%
Nada	2	10%

TOTAL	20	100%

FUENTE: Encuesta
REALIZADO POR: Grupo Investigador

VER ANEXO 2.5

GRÁFICO N°2.8 MANEJO INTEGRADO DE INFORMACION

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En 55% de los encuestados indica que si se agilitará de manera considerable el manejo integrado de la información, con la implantación de la red inalámbrica utilizando códigos de encriptación PKI y VPN será considerable, en cambio un 35 % será escasa, con lo cual se puede atestiguar que es un menor riesgo entonces si es factible implantar la red inalámbrica, ya que las PKI y VPN constituyen una estupenda garantía de seguridad.

6. Piensa usted que con la implantación de la red inalámbrica en la banda de 3.8 GHz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre, se controlará el manejo y flujo de información.

TABLA N°2.7 MANEJO Y FLUJO DE INFORMACIÓN

Opción	**Valor**	**%**
Mucho	16	80%
Poco	4	20%
Nada	0	0%

TOTAL	20	100%

FUENTE: Encuesta
REALIZADO POR: Grupo Investigador

VER ANEXO 2.6

GRÁFICO N°2.6 MANEJO Y FLUJO DE INFORMACION

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Con respecto a que si con la implantación de la red inalámbrica utilizando códigos de encriptación PKI y VPN se controlará el manejo y flujo de información, el 80% de los miembros policiales indica que será factible, en cambio un 20% manifiesta que será poco provechoso. Con lo cual podemos interpretar que al utilizar la banda de 3.8 GHz, será más veloz y eficiente para el control y flujo de información por lo cual es favorable el adaptar software libre en la Institución para obtener mayor facilidad en la comunicación de la información.

2.11 COMPROBACIÓN DE LA HIPÓTESIS

2.11.1 ENUNCIADO

"La implantación de la red LAN inalámbrica en la banda de 3.8 GHz utilizando códigos de encriptación PKI y VPN para segmentación de nodos mejorara la calidad de servicio y seguridad para el administrador y usuarios".

2.11.2 COMPROBACIÓN:

De acuerdo a las respuestas de la entrevista realizada por el grupo investigador, hacia los funcionarios que administran la red en la DINACOM referente a la automatización de le recolección de campo, podemos concluir el proyecto propuesto indudablemente cumplirá con las expectativas trazadas por los postulantes, las cuales están basadas en los directivos de la DINACOM.

Continuando con las contestaciones de la entrevista encontramos concordancia de respuestas sobre la implantación de la red con sus respectivas seguridades, los administradores de la red entrevistados manifiestan su acuerdo, en que se desarrolle el proyecto, añadiendo a ello optimismo ya que esto ayudará de manera segura, eficiente y veras en el manejo de la información.

Continuando con la comprobación de la hipótesis, tenemos las encuestas en las que los encuestados, en la pregunta Nº 3, en la que un 100% considera que la institución debe contar con seguridades en el flujo de la información, demostrando interés ante la implantación del proyecto; es decir quienes intervienen en la institución, están de acuerdo que el proyecto propuesto asegurara el intercambio de datos entre los departamentos. Por último en la pregunta Nº 6, en la que un 80% opinan que con la implantación de la red inalámbrica en la banda de 3.8 GHz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre se controlará de manera rápida y segura en la transmisión de la información facilitando su trabajo.

2.12 CONCLUSIÓN:

Todo lo anteriormente expuesto confirma lo necesario para la Implantación de la red inalámbrica en la banda de 3.8 GHz utilizando códigos de encriptación PKI y VPN a través del software libre, ya que este contribuirá al manejo control y seguridad en la información de la Institución, así lo confirman las respuestas expresadas por los entrevistados y encuestados, la misma que fue aplicada a los señores administradores de la red y señores policías que trabajan en la Dirección Nacional de Comunicaciones.

La importancia de la implantación del proyecto, salta a la vista debido a que el uso de la tecnología hace que la transmisión de la información sea más fácil y sobre todo segura.

CAPITULO III

PROPUESTA

3.1 DESARROLLO DEL PROYECTO

3.1.1 TEMA: "IMPLANTACIÓN DE LA RED LAN INALAMBRICA EN LA BANDA DE 3.8 GHZ, UTILIZANDO CÓDIGOS DE ENCRIPTACIÓN PKI Y VPN PARA SEGMENTACIÓN DE NODOS A TRAVES DE SOFTWARE LIBRE VERSION CENTOS EN LA DIRECCION NACIONAL DE COMUNICACIONES DE LA POLICIA".

3.1.2 PRESENTACION

Actualmente, en la Dirección Nacional de Comunicaciones de la Policía no existe comunicación entre las computadoras que se encuentran en diferentes redes, motivo por el

cual la implantación de una Red Privada Virtual es una propuesta para dar solución a este problema, obteniendo de esta manera seguridad y confiabilidad al transmitir los datos de un lugar a otro, mediante la utilización de protocolos de autenticación y algoritmos de encriptación PKI, los mismos que vienen incluidos dentro del Sistema Operativo GNU/LINUX, el mismo que se utilizó para la implantación del prototipo de VPN en el presente estudio.

Es indispensable hacer notar que al tener una interconexión inalámbrica debemos tener seguridades para cuidar la carga de la red, ya que la frecuencia que utiliza la dirección es de 2.4 GHz, trabaja en forma simétrica y tiende a colapsar por el flujo de información; es por esta razón que no abastece al número de usuarios que tiene la institución. Además la dirección cuenta con equipos bajo licencia de software propietario por ende es un gasto innecesario.

Una adecuada distribución de los equipos de enlace se hace urgente ya que al tener antenas de gran capacidad y de amplia cobertura ubicadas en sitios estratégicos en la ciudad de Quito mismos que tienen vista para los cuatro puntos cardinales hace que exista interferencia por lo que al implementar la banda de 3.8 GHz con seguridades PKI y VPN en software libre haya mayor rapidez en la información, evitando que personas ajenas puedan ingresar a la red de la Dirección Nacional de Comunicaciones.

Cabe destacar que la Implantación de la red LAN inalámbrica en la banda de 3.8 GHz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre está establecido para dos tipos, administradores de la red quienes tienen ingreso ilimitado y a los usuarios para compartir información entre sí. Finalmente es necesario resaltar que nuestro proyecto de uso confidencial que a través de la red, permite que los usuarios puedan acceder a la información desde cualquier departamento de la Dirección.

3.1.3 OBJETIVO GENERAL

Implantar la red LAN inalámbrica en la banda de 3.8 GHz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre en el Campus de la Dirección Nacional de Comunicaciones de la Policía.

3.1.4 OBJETIVOS ESPECIFICOS

- Realizar un estudio de calidad y servicio en la implantación de la red LAN inalámbrica para detectar problemas y por ende dar soluciones.
- Identificar los beneficios que brinda la banda de 3.8 GHz en la dirección Nacional de Comunicaciones.
- Permitir la comunicación entre redes distantes físicamente utilizando códigos de encriptación PKI y VPN a través de software libre.

3.1.5 JUSTIFICACION.

La importancia de investigar este problema radica en ayudar a difundir la información, servicios e innovaciones tecnológicas del momento que se origina en la Institución, de modo eficiente, evitando todo tipo de duplicidad de la información, proporcionando una herramienta informática que permita en cualquier momento consultar y utilizar la información de manera coherente y consistente.

Las autoridades de la Dirección Nacional de Comunicaciones nos han dado apertura a la realización del proyecto de investigación planteado por nosotras las estudiantes de la Universidad Técnica de Cotopaxi para el desarrollo del mismo.

Con una VPN no se requiere adquirir canales dedicados excesivamente costosos, por lo que podemos ofrecer una mejor relación costo/beneficio y seguridad. La red privada virtual va a permitir la conexión de redes distantes físicamente para poder transmitir datos mediante un canal seguro de comunicación así como también la conexión de usuarios remotos hacia la VPN.

Con la aplicación del proyecto se comprobará que al implantar redes inalámbricas utilizando los códigos de encriptación PKI y VPN para la segmentación de nodos se

podrá compartir recursos entre los dispositivos utilizados por el administrador y los usuarios en sus oficinas, garantizando la seguridad y confiabilidad de datos mismos que serán transmitidos de forma segura entre un servidor y un cliente en una Red de área local (*LAN*).

Sin la necesidad de encontrarse físicamente en un mismo departamento, y así permite la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas, cumpliendo con las exigencias establecidas por la Dirección Nacional de Comunicaciones.

Mediante la implantación de la red LAN inalámbrica en la banda de 3.8 GHz, se conseguirá optimizar la administración y ejecución de los procesos de cada departamento de esta dependencia, en donde se necesitan de manera imprescindible los documentos para realizar la toma de decisiones, además se determinó que para su optimo funcionamiento se recurrirá a un servidor versión Centos 5 Linux por lo que es software free y no necesita licencias, y cuenta con las garantías para resguardar toda la información.

El proyecto tiene como base el método científico ya que éste es un método de estudio ordenado que incluye las técnicas de observación, reglas para el razonamiento y la predicción, ideas sobre la experimentación planificada y los modos de comunicar los resultados experimentales y teóricos necesarios para analizar e interpretar los resultados obtenidos.

Esta implantación de códigos de encriptación PKI y VPN se realizará basándose en la realidad en que se encuentra la Red Inalámbrica y a la vez beneficiara al personal de la Dirección Nacional de Comunicaciones de la Policía y así servirá como guía no solo para la misma sino para las diversas instituciones que requieran actualizar su red a través de una adecuada planificación que permitirá brindar al usuario servicios de calidad, estableciendo una mejor comunicación en cada una de las áreas y así garantizar el flujo de información adecuado, además un ancho de banda eficiente, así mismo controlar el acceso a las aplicaciones críticas de la red inalámbrica, a los datos y a los servicios, con el único objetivo que el Administrador y usuarios puedan utilizar la red sin que haya inconvenientes.

Consideramos que es factible realizar este proyecto ya que contamos con el respaldo del personal de la Dirección Nacional de Comunicaciones de la Policía, mismos que nos proporcionarán los Recursos Técnicos y Tecnológicos, que serán utilizados para realizar la implantación de la red LAN inalámbrica utilizando códigos de encriptación PKI y VPN para la segmentación de nodos, así como también contamos con la suficiente bibliografía para la culminación del mismo.

3.2 FACTIBILIDAD ECONÓMICA

Al tratarse de seguridades en redes inalámbricas siempre puede sonar a gastos extremadamente fuertes, pero al tener la Dirección Nacional de Comunicaciones de la Policía instalados equipos de última generación y en algunos casos configurables como son los routers d'link, tarjetas de red entre otros, de esta manera independiza su utilización, las antenas con las que cuenta la Institución son de igual manera las mejores del mercado misma que abasteció completamente de tecnología de telecomunicaciones a la DINACOM.

3.3 DESARROLLO DE LA PROPUESTA

3.3.1 SISTEMA OPERATIVO LINUX

En este punto de nuestro trabajo de investigación creemos necesario realizar una rápida pero concreta definición del Sistema Operativo Linux y las bondades que este puede brindar a los usuarios de servidores, al tratarse de un Sistema Open Source ha sido ampliamente difundido a nivel mundial por lo que siempre es interesante realizar un análisis

Linux es probablemente el acontecimiento más importante del software gratuito desde el original SpaceWar, o, más recientemente, Emacs. Se ha convertido en el sistema operativo para los negocios, educación, y provecho personal. Linux ya no es solo para gurús de UNIX que se sientan durante horas frente a sus computadores personales.

Lo que hace a Linux tan diferente es que es una implementación gratuita de UNIX. Fue y es desarrollado por un grupo de voluntarios, principalmente en Internet, intercambiando código, comentando fallos, y arreglando los problemas en un entorno abierto. El presente tema de investigación es una guía que facilitara algunas de las medidas que se deben tomar para garantizar un normal desenvolvimiento de servicios tanto para compartir recursos como para asegurar de manera optima la información de una empresa o institución.

3.3.2 Características

Multitarea: varios programas (realmente procesos) ejecutándose al mismo tiempo.

Multiusuario: varios usuarios en la misma máquina al mismo tiempo.

Multiplataforma: corre en muchas CPUs distintas.

Tiene protección de la memoria entre procesos, de manera que uno de ellos no pueda colgar el sistema.

Ejecuta grandes programas.

Todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario; además todo ello se puede distribuir libremente.

Soporta para muchos teclados nacionales o adaptados y es bastante fácil añadir nuevos dinámicamente.

Consolas virtuales múltiples: varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de video).

TABLA N 3.1: GNU/LINUX
REALIZADO POR: Grupo Investigador

GNU/LINUX	
Desarrollado	**Proyecto GNU**
Familia de S.O	GNU/Linux
Modelo de desarrollo	Software libre
Núcleo	Linux
Tipo de núcleo	Monolítico
Licencia	GPL
Precio	$0.00

TABLA N 3.2: Requerimientos del Sistema Linux
REALIZADO POR: Grupo Investigador

Hardware
Memoria RAM: 256-512 MB
Disco duro:2- 40 GB
Arquitecturas que soporta Linux
Procesador:
Intel x86 compatible (32 bit) (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD,Athlon/XP
Intel Itanium (64 bit)
Advanced Micro Devices AMD64 (Athlon 64, etc) e Intel EM64T (64 bit)
PowerPC/32 (Apple Macintosh PowerMac corriendo sobre procesadores G3 o G4 PowerPC)
IBM Mainframe (eServer zSeries y S/390)
Además tiene soporte para dos

arquitecturas no soportadas por su original

3.4 CENTOS (Community ENTerprise Operating System)

Centos es un clon a nivel binario, compilado por voluntarios a partir del código fuente.los desarrolladores de Centos usan este código fuente para crear un producto final, y esta líbreme y disponible para ser bajado y usado por el público.

TABLA Nº 3.3: Tabla Informativa de Centos
REALIZADO POR: Grupo Investigador

Centos	
Desarrollador	
CentOSDevelopmentTeam	
Familia de S.O	GNU/Linux
Modelo de desarrollo	Software libre
Núcleo	Linux
Tipo de núcleo	Monolítico
Licencia	GPL
Última versión	5.2

3.5 Instalación y configuración del servidor Samba.

Samba es una implementación libre del protocolo de archivos compartidos, configura directorios Unix-Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red, estos recursos aparecen como carpetas normales. Los usuarios de Linux pueden montar en sus sistemas de archivos estás unidades de red como si fueran

dispositivos locales, o utilizar la orden smbclient para conectarse a ellas muy al estilo del cliente de la línea de órdenes ftp.

En ocasiones pareciera que el compartir recursos es complicado y que tiene que realizarlo un experto y la verdad es que no es así, en este proyecto mostraremos la forma para instalar y configurar un servidor Samba de manera sencilla utilizando como sistema operativo del servidor la última versión de Centos.

Para llevar a cabo la instalación se necesitaran los siguientes paquetes:

- **samba**
- **samba-client**
- **samba-common**

Para instalar y verificar los paquetes completos de samba se utiliza la siguiente línea de código en el terminal como se muestra a continuación:

```
[root@server ~]# yum -y install samba*
[root@server ~]# cd /etc
[root@server etc]# rpm -qa | Grep samba
```

GRÁFICO Nº3.1: INSTALACIÓN DE SAMBA.
FUENTE: Grupo Investigador

```
[root@server ~]# yum -y install samba*
Iniciando servicios SMB:                    [OK]
Iniciando servicios MMB:                    [OK]
```

CARACTERISTICAS

TABLA Nº 3.4: Características del servidor FTP y SMB
REALIZADO POR: Grupo Investigador

FTP	SAMBA
La **conexión** de un usuario remoto al	Samba es una aplicación de servidor

servidor FTP puede hacerse como inicio de una sesión de un usuario que existe en el sistema o también como un usuario genérico que se llama *anónimo*	poderosa y versátil. Hasta los administradores bien empapados deben conocer sus habilidades y limitaciones antes de intentar una instalación y configuración
El **acceso** al sistema de archivos del servidor FTP está **limitado**, dependiendo del tipo de usuario que se conecta.	Actúa como un Backup Domain Controller (BDC) para un PDC basado en Samba
Una vez se ha establecido la conexión con el servidor FTP, el usuario tiene disponible el conjunto de **órdenes** FTP que permiten realizar las operaciones básicas de descarga(get) o subida(put) de archivos, junto con otras órdenes.	Asiste en la navegación de la red (con o sin NetBIOS). Autentifica las conexiones a dominios
Un **servidor** FTP es una aplicación que proporciona un mecanismo estándar de transferencia de archivos entre sistemas a través de redes	Actúa como un miembro servidor de dominio de Active Directory

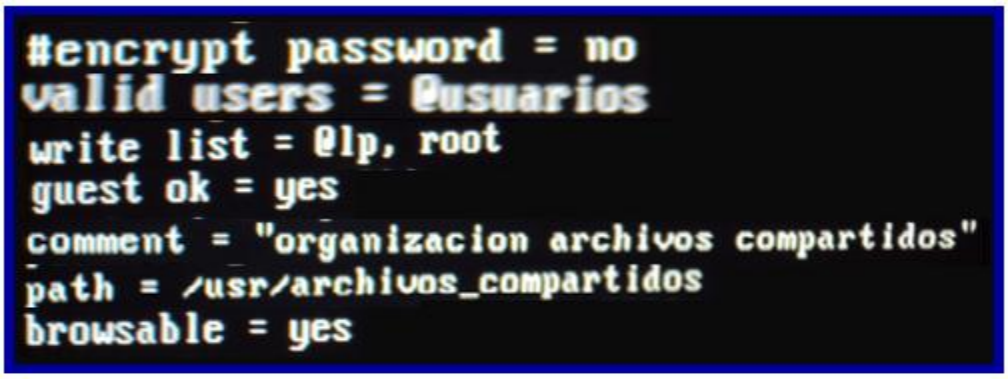
3.5.1 Configuración de los recursos compartidos

La configuración de los recursos que compartiremos deben ir especificados al final del fichero.

GRÁFICO Nº3.2: CONFIGURACIÓN DE SAMBA.
FUENTE: Grupo Investigador

Algunas de las opciones que podemos agregar a esta estructura son las siguientes:

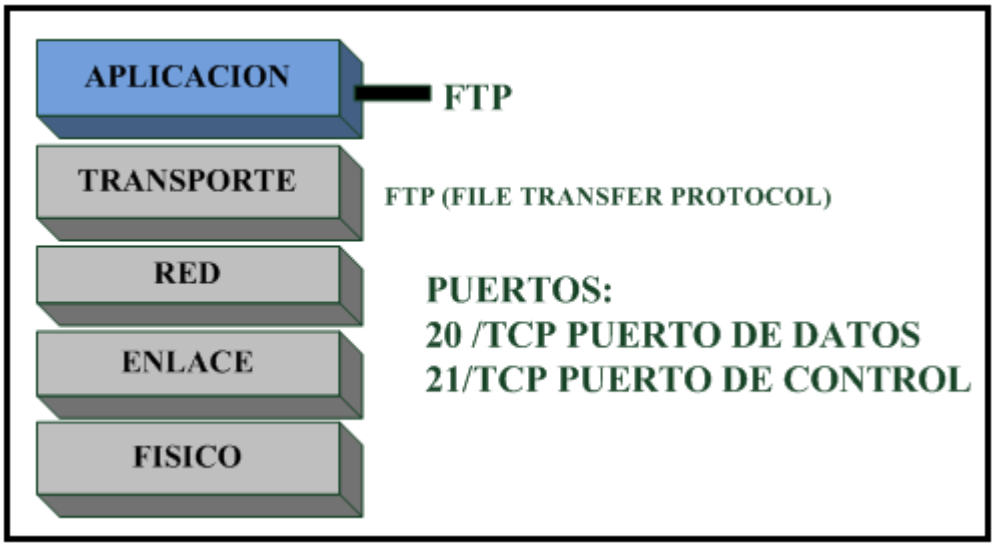
GRÁFICO Nº3.3: ESTRUCTURA SAMBA.
FUENTE: Grupo Investigador



3.6 Instalación y configuración del Servidor FTP.

El protocolo FTP (File Transfer Protocol) es una herramienta para la transferencia de archivos la cual puede ser efectuada desde una LAN (Red de área local) o en una WAN (Red de Área Amplia).Así mismo el protocolo FTP hace uso de los puertos 20 y 21 para la comunicación y control de datos, el puerto 20 es utilizado para el flujo de datos entre cliente y servidor. El puerto 21 es utilizando para el envío de órdenes del cliente hacia el servidor.

GRÁFICO Nº 3.4: ESTRUCTURA DEL FTP.
FUENTE: Grupo Investigador



3.6.1 Funcionamiento del Protocolo FTP

Generalmente se origina cuando el cliente FTP envía la petición al servidor para indicarle que requiere establecer una comunicación con él, entonces el cliente FTP inicia la conexión hacia el servidor FTP mediante el puerto 21 el cual establecerá un canal de control. A partir de este punto el cliente FTP enviara al servidor las acciones que este debe ejecutar para poder llevar a cabo el envío de datos.
Estas acciones incluyen parámetros para la conexión de datos así como también la manera en cómo serán gestionados y tratados estos datos.

Algunos de los parámetros enviados por el cliente FTP para la conexión de datos son los siguientes:

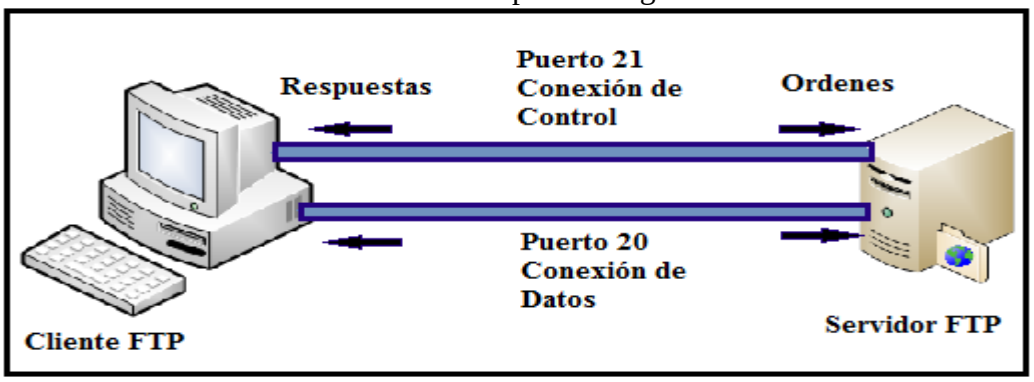
- Puerto de datos
- Modo de transferencia
- Tipo de representación y estructura

Los parámetros relacionados a la gestión de datos son los siguientes
- Almacenar
- Recuperar

- Añadir
- Borrar
- Obtener

El proceso de transferencia de datos desde el servidor hacia el cliente deberá esperar a que el servidor inicie la conexión al puerto de datos especificado (en modo activo) y luego de ello transferir los datos en función a los parámetros de conexión especificados anteriormente.

GRÁFICO Nº 3.5: FUNCIONAMIENTO DEL PROTOCOLO FTP.
FUENTE: Grupo Investigador

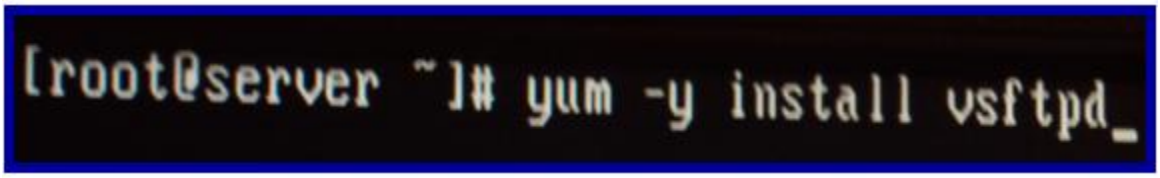


3.6.2 Configuración e instalación del servidor FTP.

La instalación de VSFTPD es relativamente sencilla, solo se debe teclear en el terminal el siguiente comando.

```
[root@server ~]# yum -y install vsftpd
```

GRÁFICO Nº 3.6: COMANDOS VSFTPD.
FUENTE: Grupo Investigador



Recuerde que este comando se debe ejecutar desde el root.

3.6.3 Ruta de configuración de VSFTPD

La configuración de VSFTPD se realizara sobre el fichero de configuración general propio deVSFTPD.

El fichero de configuración de VSFTPD lo encontramos en la siguiente ruta

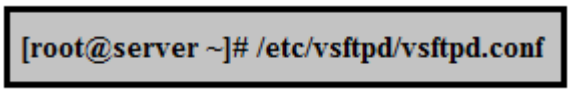


GRÁFICO Nº 3.7: RUTA DEL FICHERO DE CONFIGURACIÓN VSFTPD.
FUENTE: Grupo Investigador

3.6.4 Configuración del fichero vsftpd.conf

Para llevar a cabo la configuración de este fichero usamos el editor de textos VIM.

A continuación veremos las diferentes opciones que pueden ser habilitadas o negadas en el fichero de configuración **vsftpd.conf.**

3.6.5 Habilitando o negando accesos anónimos al servidor FTP.

Para habilitar el acceso anónimo al servidor FTP solo deberá teclear la palabra **YES**, caso contrario si usted desea tener deshabilitada esta opción solo deberá teclear la palabra **NO.** Por seguridad en esta opción ponemos **NO** ya que así evitamos el ingreso a extraños.

```
anonymous_enable=NO
```

3.6.6 Habilitar o negar la autenticación a los usuarios.

Para habilitar o negar los accesos autenticados de los usuarios locales en el servidor FTP deberá buscar la siguiente línea:

```
local_enable=YES
```

Tecleamos la palabra **YES** para habilitar la autenticación del usuario, dándole permiso de acceso a un recurso para que realice alguna operación**.**

3.6.7 Habilitar o negar la escritura en el servidor FTP

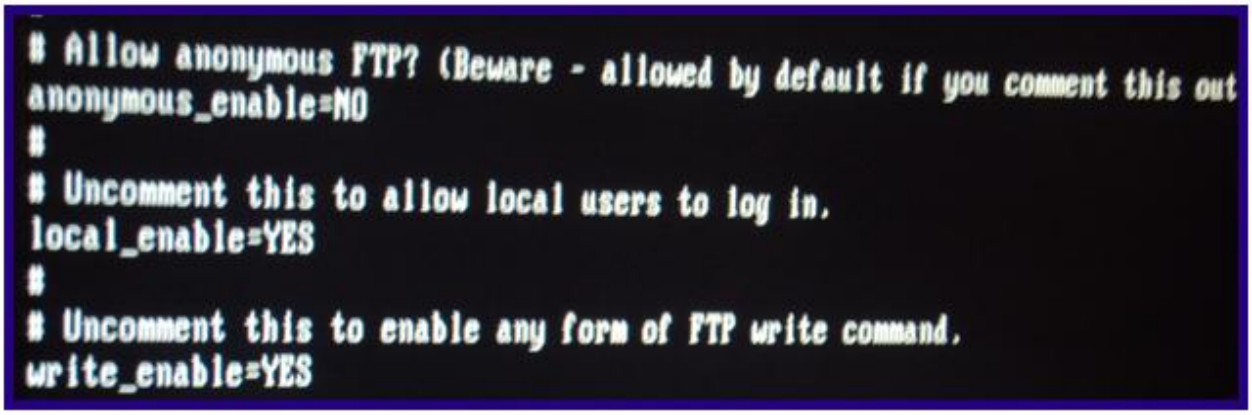
Para habilitar o negar la escritura en el servidor FTP deberá buscar la siguiente línea:

```
write_enable=YES
```

Una vez ubicada esta línea recuerde borrar (si es que esta) el signo de número **(#)** para habilitar esta función.

Establecemos el valor YES y así le damos permiso de escritura al usuario.

GRÁFICO Nº 3.8: PERMISOS DEL SERVIDOR FTP.
FUENTE: Grupo Investigador



3.6.8 Habilitar el acceso de usuarios FTP

El siguiente fichero de configuración debe ser creado por el administrador ya que se especifica al servidor FTP los usuarios que trabajaran dentro de su carpeta de trabajo. La ruta en la que se debe crear dicho fichero es la siguiente:

/etc/vsftpd

Y tendrá el siguiente nombre:

chroot_list

A este fichero deberán ser agregados los nombres de los usuarios de FTP que trabajaran en su directorio de trabajo, de esta manera se restringe a estos usuarios el acceso a otras partes del sistema operativo.

Para limitar a los usuarios a trabajar en su propia carpeta de trabajo se deberán editar las siguientes líneas del fichero **vsftpd.conf**

```
chroot_list_enable=YES
chroot_list_user=YES
```

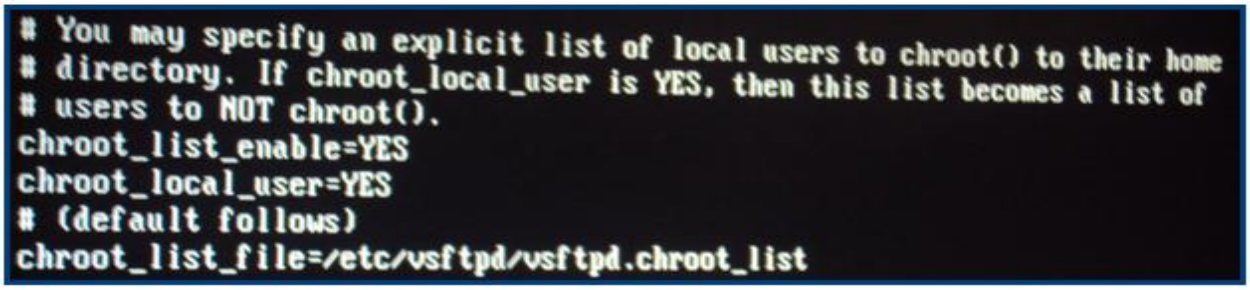
Habilitamos estos parámetros que indica al servidor FTP que los usuario solo podrá trabajar dentro de su carpeta de trabajo, para ello solo habrá que teclear la palabra **YES**.

El siguiente parámetro también lo habilitamos ya que se encuentra en función del anterior.

```
chroot_list_file=/etc/vsftpd/vsftpd.chroot_list
```

El parámetro indica la ruta en la cual se encuentra el fichero con los nombres de los usuarios que serán limitados a trabajar en su propia carpeta de trabajo.

GRÁFICO Nº 3.9: PERMISOS PARA LOS USUARIOS EN EL SERVIDOR FTP.
FUENTE: Grupo Investigador



3.6.9 Estableciendo permisos de escritura al servidor FTP.

Permisos en formato numérico octal

La combinación de valores de cada grupo de los usuarios forma un número octal, el bit x es 2^0 es decir 1, el bit w es 2^1 es decir 2, el bit r es 2^2 es decir 4, tenemos entonces:

- r = 4
- w = 2
- x = 1

TABLA Nº 3.5: FORMATO NÚMERICO OCTAL
REALIZADO POR: Grupo Investigador

- - -	= 0	No se tiene ningún permiso
- - x	= 1	Solo permiso de ejecución
- w	= 2	Solo permiso de escritura
- wx	= 3	Permisos de escritura y ejecución

r - -	= 4	Solo permiso de lectura
r – x	= 5	Permisos de lectura y ejecución
r w	= 6	Permisos de lectura y escritura
r w x	= 7	Todos los permisos establecidos, lectura, escritura y ejecución

Cuando se combinan los permisos del usuario, grupo y otros, se obtienen un número de tres cifras que conforman los permisos del archivo o del directorio. Esto es más fácil visualizarlo con algunos ejemplos:

TABLA Nº 3.6: PERMISOS DEL ARCHIVO
REALIZADO POR: Grupo Investigador

Permisos	**Valor**	**Descripción**
rw-------	600	El propietario tiene permisos de lectura y escritura.
rwx--x--x	711	El propietario lectura, escritura y ejecución, el grupo y otros solo ejecución.
rwxr-xr-x	755	El propietario lectura, escritura y ejecución, el grupo y otros pueden leer y ejecutar el archivo.
rwxrwxrwx	777	El archivo puede ser leído, escrito y ejecutado por quien sea.
r--------	400	Solo el propietario puede leer el archivo, pero ni el mismo puede modificarlo o ejecutarlo y por supuesto ni el grupo ni otros pueden hacer nada en el.
rw-r-----	640	El usuario propietario puede leer y escribir, el grupo puede leer el archivo y otros no pueden hacer nada.

La siguiente línea Indica que los archivos subidos al servidor quedarán con los permisos 022, es decir, sólo escritura para el grupo y los demás.

```
local_umask=022
```

3.6.10 Habilitar al usuario la función de subir contenido al servidor FTP.

En la siguiente línea habilitamos a los usuarios para que puedan subir datos al servidor FTP:

```
anon_upload_enable=YES
```

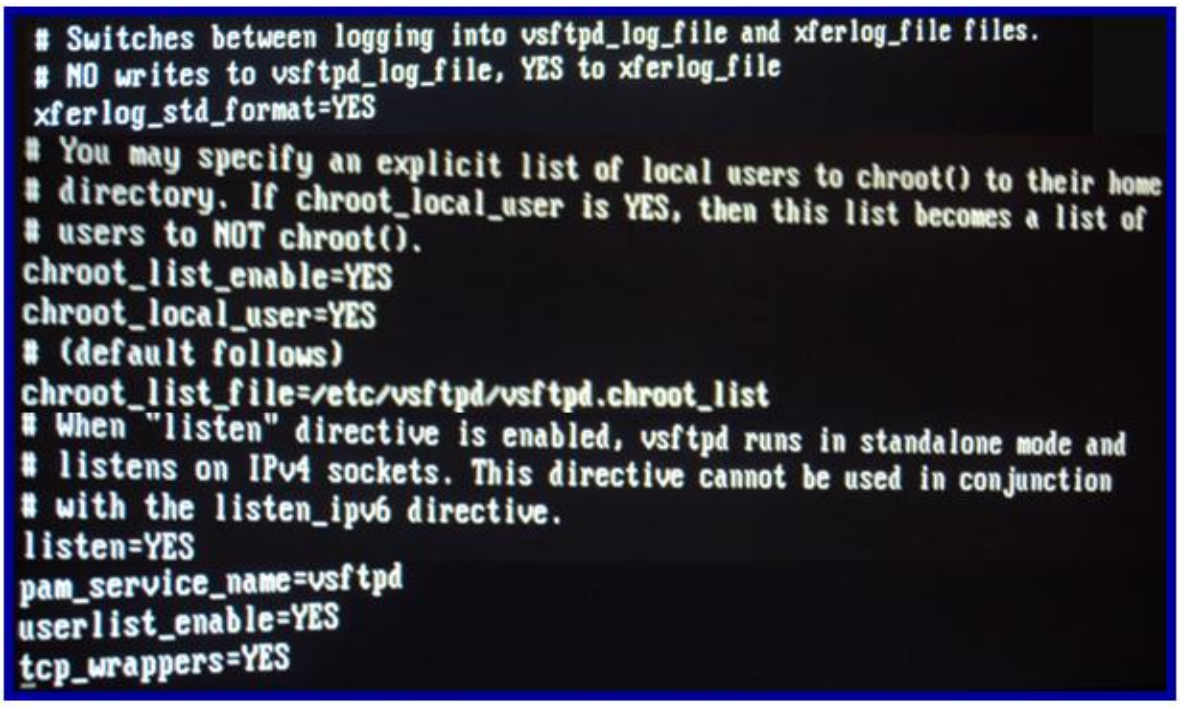
3.6.11 Habilitar al usuario la función de crear carpetas en servidor FTP

En la siguiente línea habilitamos a los usuarios para que puedan crear carpetas en el servidor FTP:

```
anon_mkdir_write_enable=YES
```

GRÁFICO Nº 3.10: PERMISOS PARA LOS USUARIOS EN EL SERVIDOR FTP.
FUENTE: Grupo Investigador

```
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# The target log file can be vsftpd_log_file or xferlog_file.
# This depends on setting xferlog_std_format parameter
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
```



3.7 Implantación de la VPN.

Con la implantación de la Red Privada Virtual, se desea proporcionar las siguientes facilidades:

- **Autenticación del usuario**

La VPN va hacer capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados.

- **Administración de direcciones**

La VPN va a establecer una dirección de cliente en la red privada y va a cerciorarse que las direcciones privadas se conserven así y no sean modificadas.

- **Codificación de datos**

Los datos que se van a transmitir a través de la red pública van hacer previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

- **Administración de claves**

Las VPN deben generar y renovar las claves de codificación para el cliente y el servidor.

3.7.1 Estrategia de implantación

La estrategia para la implantación de la VPN se detalla a continuación:

- Asegurar una infraestructura de red con el Sistema Operativo GNU/Linux, de manera que las computadoras puedan tener comunicación a través de un túnel.
- Verificar que los clientes tengan una configuración del protocolo TCP/IP que cuente con una dirección IP verdadera, debido a que este es un requerimiento muy importante para la configuración de la VPN.
- Realizar las configuraciones tanto del servidor VPN, así como de los clientes.
- Una vez configurada la VPN, se debe poner énfasis en las seguridades, con respecto a la información y al acceso de los clientes y además no pueden ser modificada por usuarios no autorizados o intrusos que tengan acceso a la red.

3.7.2 Creación de la seguridad VPN.

Se utiliza este tipo de VPN cuando se necesita enlazar a los sitios que son parte de una compañía u organización, en nuestro caso está compuesto por un servidor Central que conectará a dos clientes VPN entre sí, se crea entre una oficina central (servidor) y una o varias oficinas (clientes).

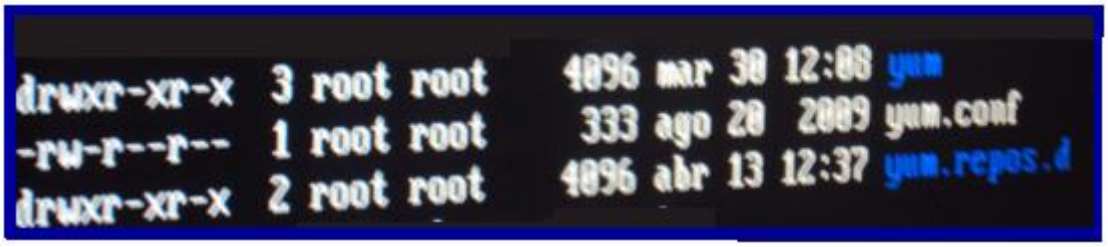
3.7.3 Creación del Fichero

Desde la terminal, creamos el fichero **/etc/yum.repos.d/AL-Server.repo**, utilizando el editor de texto **vi** y visualizamos el fichero creado con el comando **ll**.

```
[root@server etc]# vi /etc/yum.repos.d/AL-Server.repo
[root@server etc]# ll
```

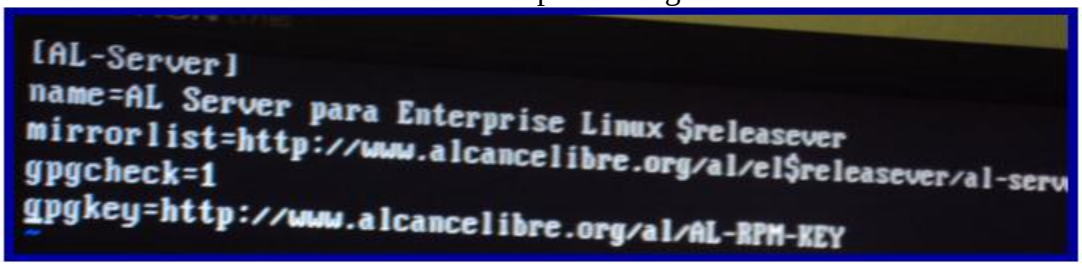
GRÁFICO Nº 3.11: CREACIÓN DEL FICHERO YUM.REPOS.D

FUENTE: Grupo Investigador



Añadimos al **nuevo fichero** el siguiente contenido desde internet:

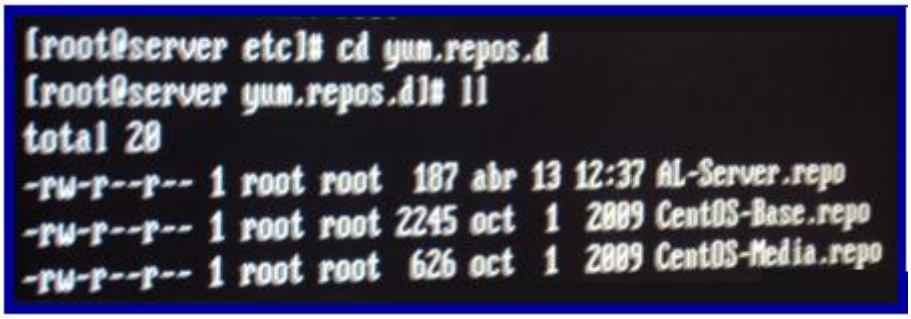
GRÁFICO Nº 3.12: FICHERO YUM.REPOS.D.
FUENTE: Grupo Investigador



A continuación verificamos los paquetes que se encuentran dentro del fichero, cambiándonos de directorio:

```
[root@server etc]# cd yum.repos.d
[root@server yum.repos.d]# ll
```

GRÁFICO Nº 3.13: PAQUETES DEL FICHERO YUM.REPOS.D.
FUENTE: Grupo Investigador



3.7.4 Instalación y configuración del Openvpn

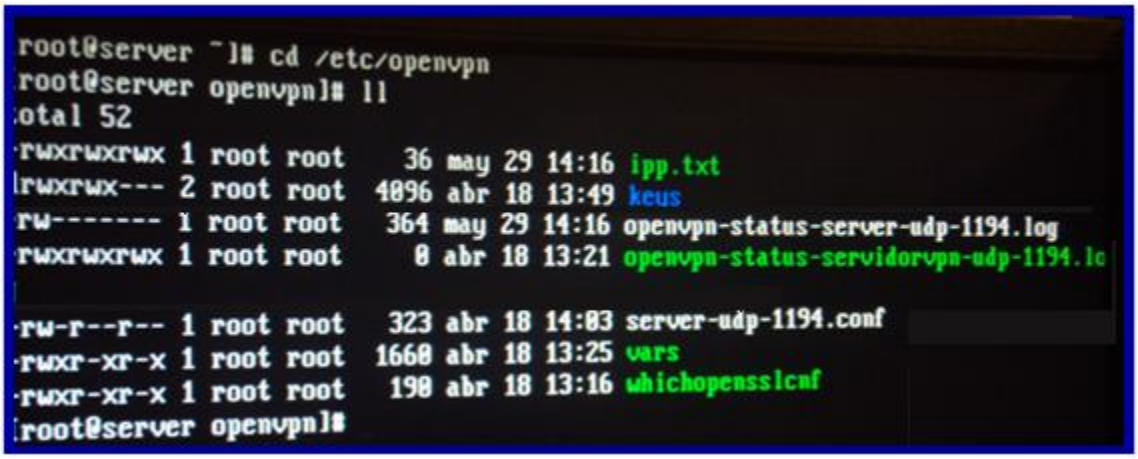
Luego de importar la firma digital de Alcance Libre, instalamos el paquete OpenVPN con el comando **yum**.

```
[root@server]# yum -y install openvpn*
```

Terminada la instalación cambiamos de directorio y visualizamos desde la terminal, el paquete instalado ejecutando lo siguiente:

```
[root@server ~]# cd /etc/openvpn
[root@server openvpn]# ll
```

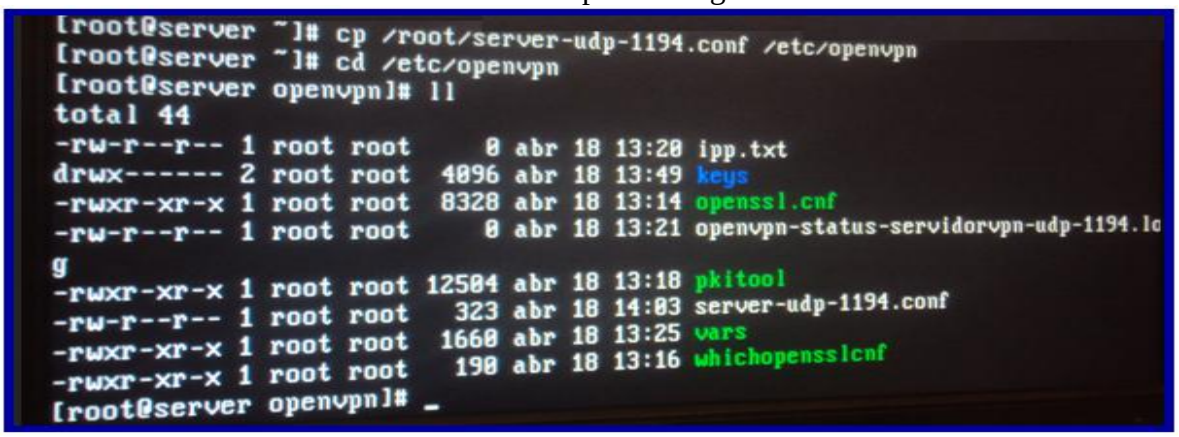
GRÁFICO Nº 3.14: PAQUETES DEL OPENVPN.
FUENTE: Grupo Investigador



En el servidor existe un archivo llamado server-udp-1194.conf que es el encargado de la configuración de la VPN, mismo que se ha de copiar a /etc/openvpn. Se puede copiar este archivo mediante la consola de comandos:

```
[root@server ~]# cp /root/server-udp-1194.conf /etc/openvpn
[root@server ~]# cd /etc/openvpn
[root@server openvpn]# ll
```

GRÁFICO Nº 3.15: ARCHIVO SERVER-UDP-1194.CONF.
FUENTE: Grupo Investigador



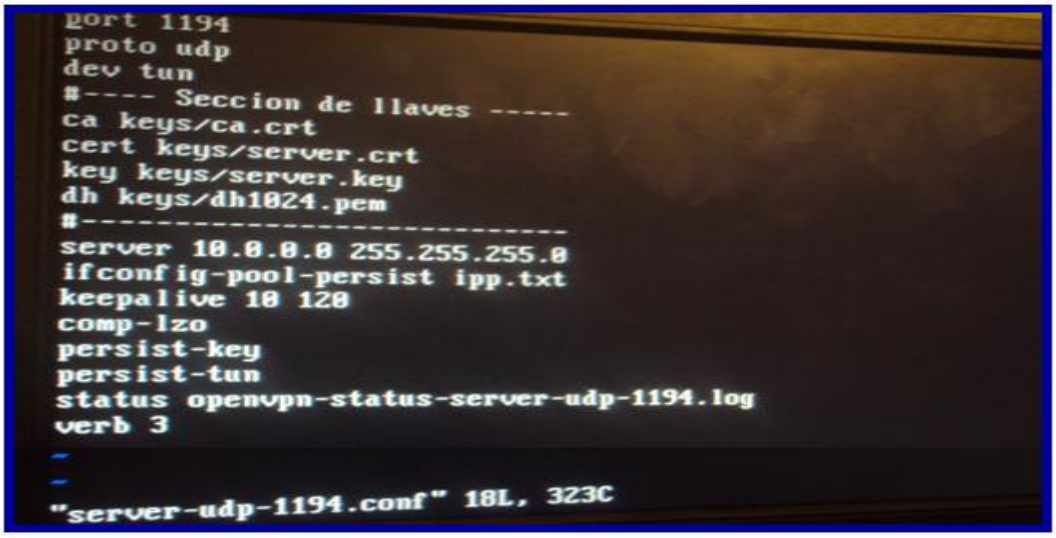
Desde ahora se trabaja con la copia del server-udp-1194.conf que se ha hecho, editamos el archivo con el siguiente editor de texto:

```
[root@server openvpn]# vi /etc/openvpn/server-udp-1194.conf
```

Se modifica el archivo añadiendo la ruta de los certificados y claves una vez establecidas las rutas, se guarda y se cierra el archivo.

En este apartado se ve el fichero de configuración server-udp-1194.conf situado en el servidor.

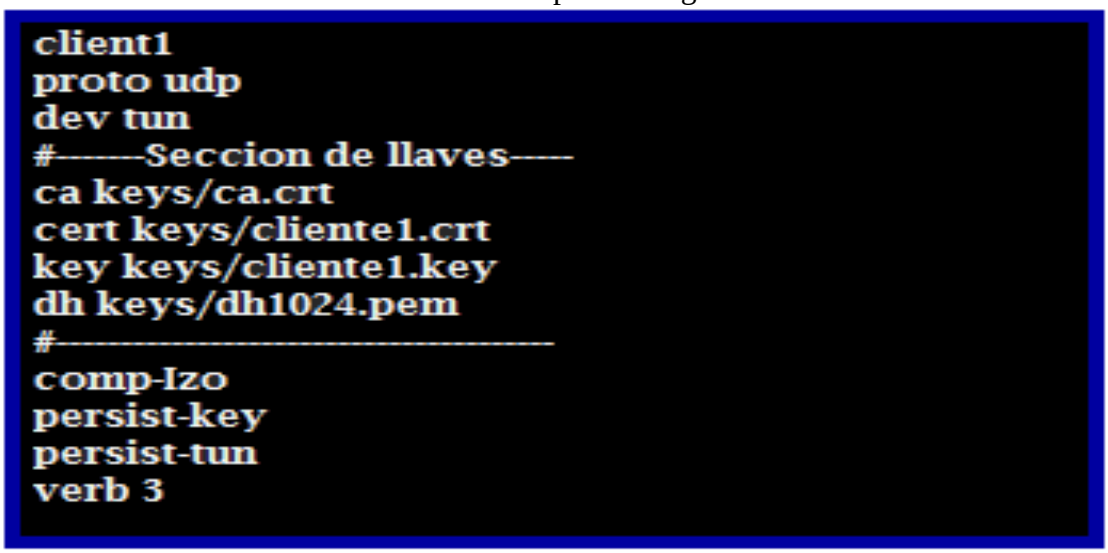
GRÁFICO Nº 3.16: VISUALIZACIÓN DEL ARCHIVO SERVER-UDP-1194.CONF.
FUENTE: Grupo Investigador



Para los clientes, se requiere haber configurado previamente el depósito de **AL Server**, descrito anteriormente.

En este apartado se visualiza el fichero de configuración client1.conf (en un cliente con Linux), situados en el cliente.

GRÁFICO Nº 3.17: VISUALIZACIÓN FICHERO DE CONFIGURACIÓN CLIENT1.CONF
FUENTE: Grupo Investigador



Si se ejecuta un ifconfig en la consola, en ese momento se lee el archivo client.conf y realiza la conexión. Nos asigna una IP privada de la VPN, y crea una interfaz de red virtual TUN.

GRÁFICO Nº 3.18: IP PRIVADA.
FUENTE: Grupo Investigador

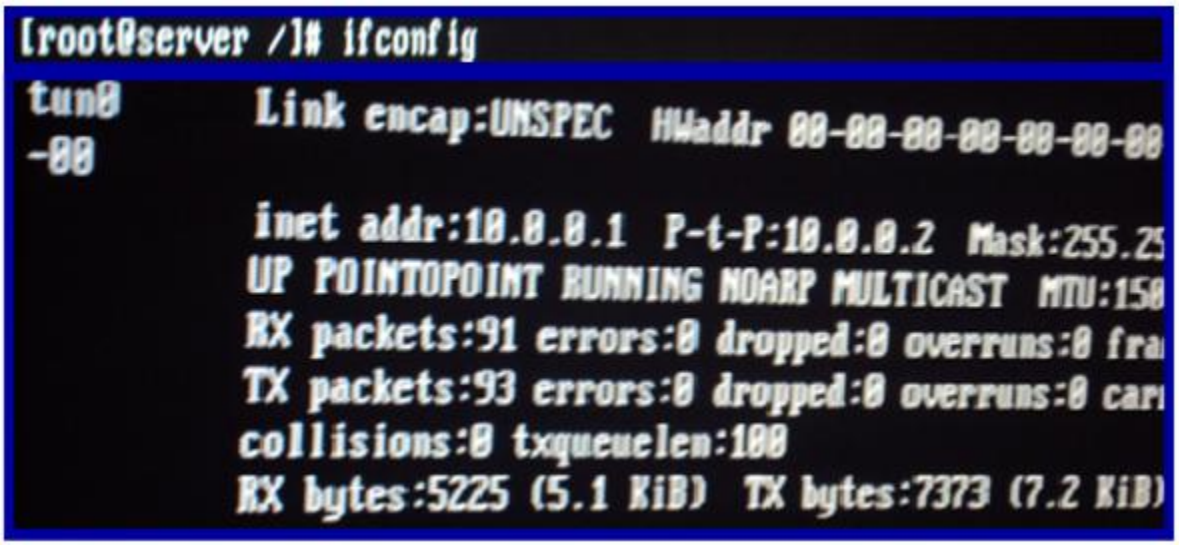


TABLA Nº 3.7: DESCRIPCIÓN DE LOS PARÁMETROS
REALIZADO POR: Grupo Investigador

Port:	Especifica el puerto que será utilizado para que los clientes vpn puedan conectarse al servidor.
Proto:	tipo de protocolo que se empleará en la conexión a través de VPN
dev:	Tipo de interfaz de conexión virtual que se utilizará el servidor openvpn.
Ca	Especifica la ubicación exacta del fichero de Autoridad Certificadora [.ca].
cert:	Especifica la ubicación del fichero [.crt] creado para el servidor.
key:	Especifica la ubicación de la llave [.key] creada para el servidor openvpn.
dh:	Ruta exacta del fichero [.pem] el cual contiene el formato de Diffie Hellman (requerido para **--tls-server** solamente).

server:	Se asigna el rango IP virtual que se utilizará en la red del túnel VPN.
Ifconfig-pool-persist:	Fichero en donde quedarán registradas las direcciones IP de los clientes que se encuentran conectados al servidor OpenVPN.
Keepalive 10 120 :	Envía los paquetes que se manejan por la red una vez cada 10 segundos; y asuma que el acoplamiento es abajo si ninguna respuesta ocurre por 120 segundos.
comp-lzo:	Específica los datos que recorren el túnel vpn serán compactados durante la trasferencia de estos paquetes.
persist-key:	Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser re leídos.
persist-tun:	Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down
Status	fichero donde se almacenará los eventos y datos sobre la conexión del servidor [.log]
verb 3:	Nivel de información (default=1). Cada nivel demuestra todo el Info de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

3.8 Instalación de la librería SSL (Secure Socket Layer)

Dependiendo del nivel de seguridad que se quiera instalar en nuestra VPN, existen unas librerías previas que se deben instalar.

OpenSSH es un robusto paquete de herramientas de administración y librerías relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenVPN y navegadores Web. Estas herramientas ayudan al sistema a implementar el protocolo SSL, así como otros protocolos relacionados con la seguridad, como el protocolo TLS.

OpenVPN lo utiliza para implementar la seguridad, utilizando el protocolo SSL/TLS. Este paquete de software es importante ya que tiene cierto nivel de seguridad al utilizar un S.O.

libre basado en GNU/Linux. También nos permite crear certificados digitales que se pueden aplicar a nuestro servidor.

Soporta algoritmos criptográficos tales como:

• Algoritmos de intercambio de clave pública: RSA, Diffie-Hellman.

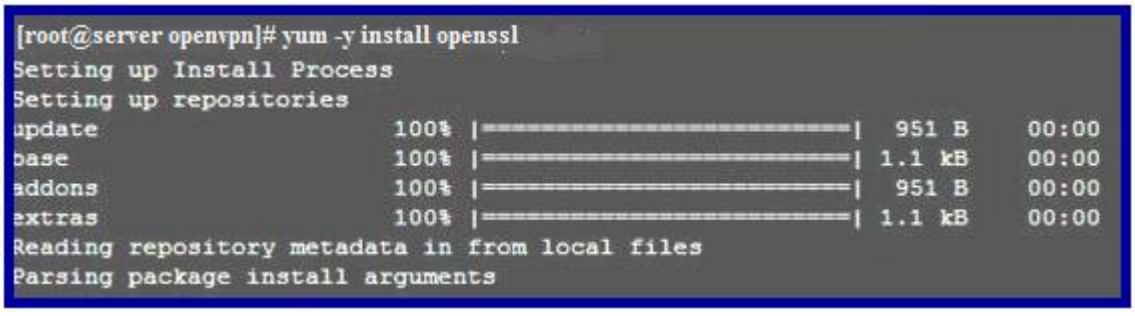
Además OpenSSL proporciona las siguientes herramientas y funciones:

• Genera y gestiona claves asimétricas y simétricas para los distintos algoritmos de cifrado.
• Genera números aleatorios y pseudos aleatorios.
• Utiliza algoritmos para firmar, certificar y revocar claves.
• Maneja y gestión formatos de certificados existentes en el mundo (X.509, PEM, PKCS7).
• Cálculo de resúmenes de mensajes.
• Cifrado y descifrado mediante algoritmos de cifrado.

OpenSSL es un software multiplataforma. Su instalación de penderá del S.O utilizado. Por ejemplo: En Linux se necesita la instalación previa deOpenSSL, y de las librerías necesarias. Para ello es posible hacerlo mediante interfaz gráfica, o bien por comandos:

```
[root@server openvpn]# yum -y install openssl
```

GRÁFICO Nº 3.19: INSTALACIÓN DEL OPENSSL .
FUENTE: Grupo Investigador



3.8.1 Creación de la PKI (Infraestructura de Clave Pública)

Para construir una VPN con OpenVPN 2.4 es necesario crear una PKI (Public Key Infrastructure).

Esta PKI está formada por:

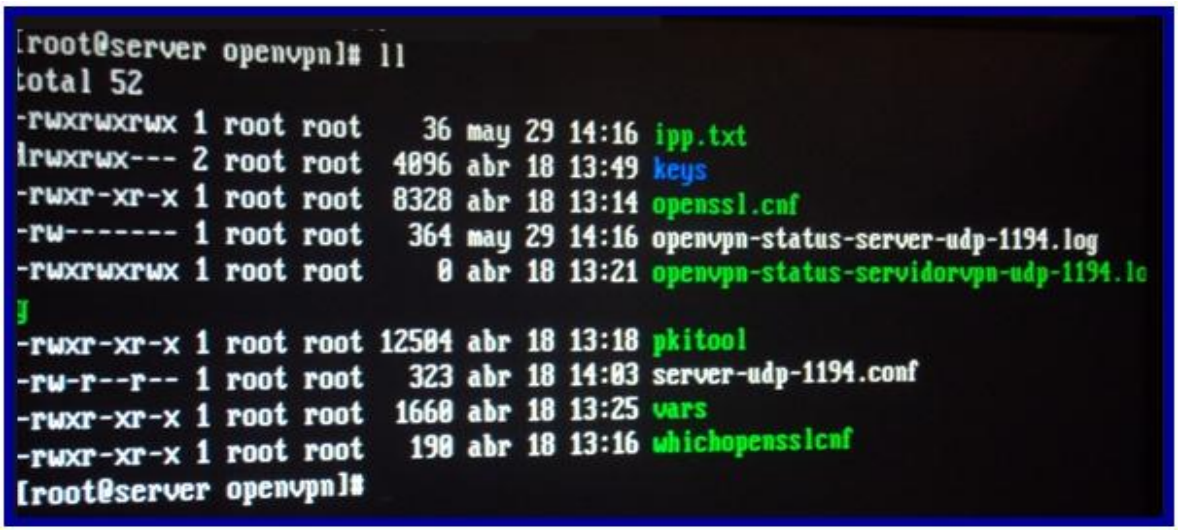
• Un certificado (conocido como clave pública) y una clave privada para el servidor y para cada cliente.

• Un Certificado para la CA y su clave, que se usará para firmar los certificados del servidor y los clientes.

A partir de ahora todo el proceso de generación de claves, certificados, y firma digital, se realizará desde el servidor u otra máquina designada para ello, que no sea un cliente. Esto es por seguridad, ya que no es conveniente que un cliente contenga todas las claves y certificados.

Visualización de la PKI.

GRÁFICO Nº 3.20: VISUALIZACIÓN DEL OPENSSL.
FUENTE: Grupo Investigador



3.8.2Generación del directorio keys.

Una vez instalado OpenVpn, la administración de la PKI para la creación de la clave y el certificado de la CA, se hará mediante unos scripts que vienen con OpenVPN los cuales explicaremos según su creación.

Mediante el siguiente comando se creará un nuevo directorio donde se almacenarán las claves privadas, los archivos de requerimiento de certificado (.csr), los certificados (.crt), y otros archivos como el serial y el index.txt.

```
[root@server ~]# mkdir -p /etc/openvpn/easy-rsa/2.0/keys
```

Desde el directorio en el que están los scripts editamos el archivo vars, en el que se encuentra la ruta del fichero donde se crearán las claves y certificados, el tamaño de las claves privadas (del servidor, cliente y CA), y los valores por defecto de algunos campos que se debe modificar.
Se modifican los siguientes parámetros con los valores de nuestra VPN:

```
[root@server openvpn]# vi /etc/openvpn/vars
```

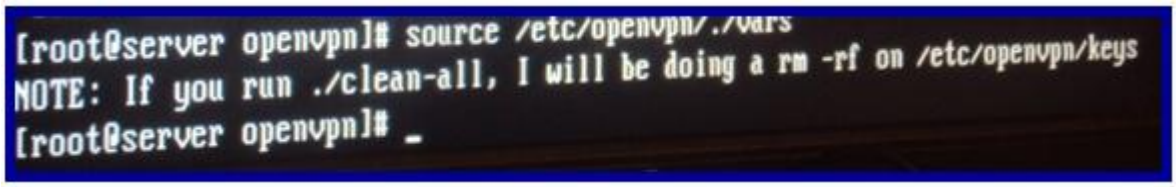
GRÁFICO Nº 3.21: DIRECTORIO KEYS.
FUENTE: Grupo Investigador

```
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="EC"
export KEY_PROVINCE="CO"
export KEY_CITY="Latacunga"
export KEY_ORG="unc"
export KEY_EMAIL="info@unc.com"
"vars" 68L, 1660C written
```

A fin de que carguen las variables de entorno que se acaban de configurar se debe ejecutar del siguiente modo. Cada vez que se vayan a generar nuevos certificados, debe ejecutarse el mandato anterior a fin de que carguen las variables de entorno definidas

```
[root@server openvpn]# source /etc/openvpn/ ./vars
```

GRÁFICO Nº 3.22: CARGA DE LAS VARIABLES DE ENTORNO.
FUENTE: Grupo Investigador



Se ejecuta el fichero a fin de limpiar cualquier firma digital que accidentalmente estuviera presente.

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

Lo anterior realiza un **rm -fr** (eliminación recursiva) sobre el directorio **/etc/openvpn/keys**, por lo que se eliminarán todas los certificados y firmas digitales que hubieran existido con anterioridad.

3.8.3 Ejecución del algoritmo Diffi-Hellman

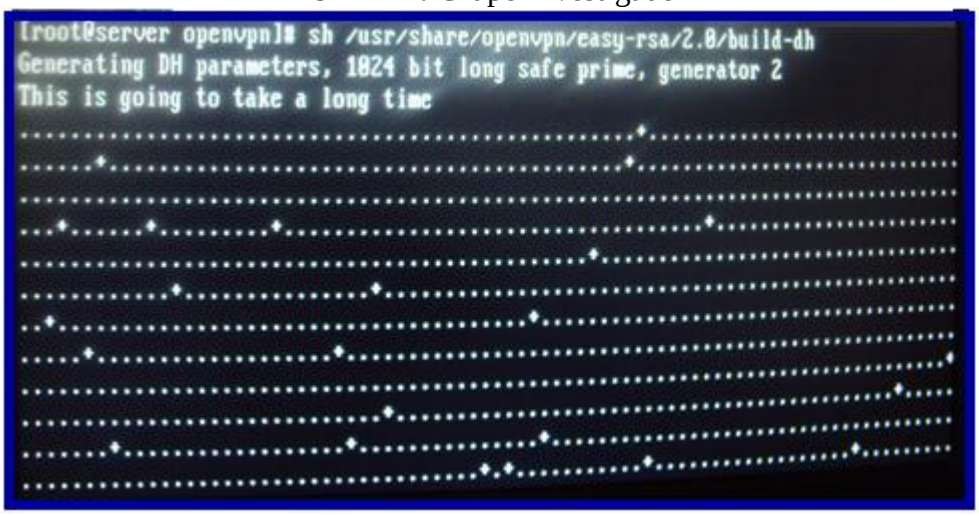
Para crear las claves privadas se usa el protocolo Diffie-Hellman, el cual genera claves simétricas, y permite el intercambio de las claves privadas de forma segura, mediante encriptación. Para la seguridad en OpenVPN, necesitaremos una Unidad Certificadora (CA) que se encargará de crear los certificados y las claves de seguridad. Además la CA necesita un certificado y clave maestra para generar los del servidor y clientes.

Se ejecuta el algoritmo dh1024.pem, el cual contendrá los parámetros del protocolo **D**iffie-**H**ellman, de 1024 bits. El protocolo **D**iffie-**H**ellman permite el intercambio secreto de claves entre dos partes que sin que éstas hayan tenido contacto previo, se emplea

generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión, como es el caso de una conexión VPN.

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

GRÁFICO Nº 3.23: CORRIDO DEL ALGORITMO DIFFI-HELLMAN.
FUENTE: Grupo Investigador



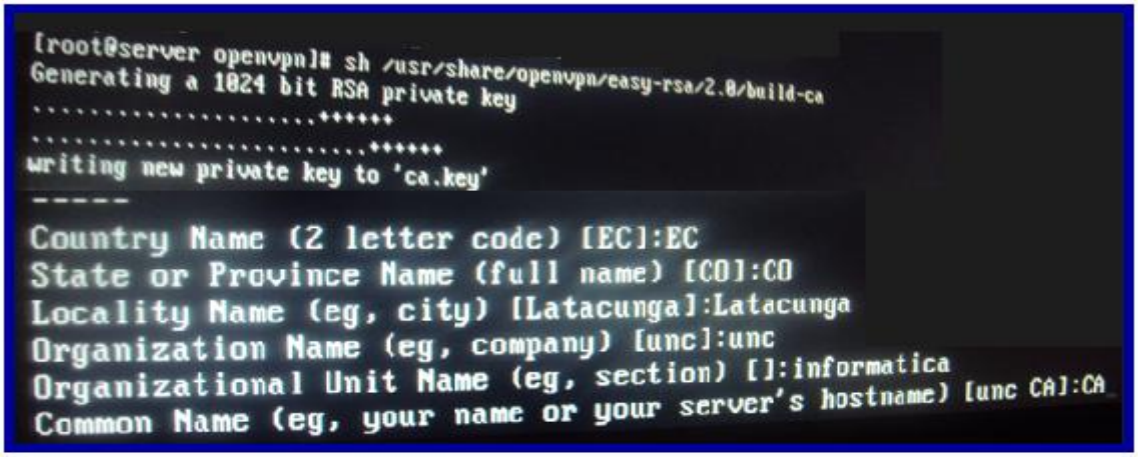
3.8.4 Generación de la Autoridad Certificadora CA

Para generar la clave privada y el certificado del servidor se toman los valores del archivo vars, la ca es la encargada de confirmar que el dueño de un certificado es realmente la persona que dice ser.
Para ello escribimos el siguiente comando en la consola:

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

GRÁFICO Nº 3.24: AUTORIDAD CERTIFICADORA CA.

FUENTE: Grupo Investigador



Con este procedimiento se han generado 3 ficheros:

• **ca.crt:** es el certificado público de la CA.

• **ca.key:** es la clave privada de la CA, la cual debe mantenerse protegida porque es la clave más importante de toda la PKI.

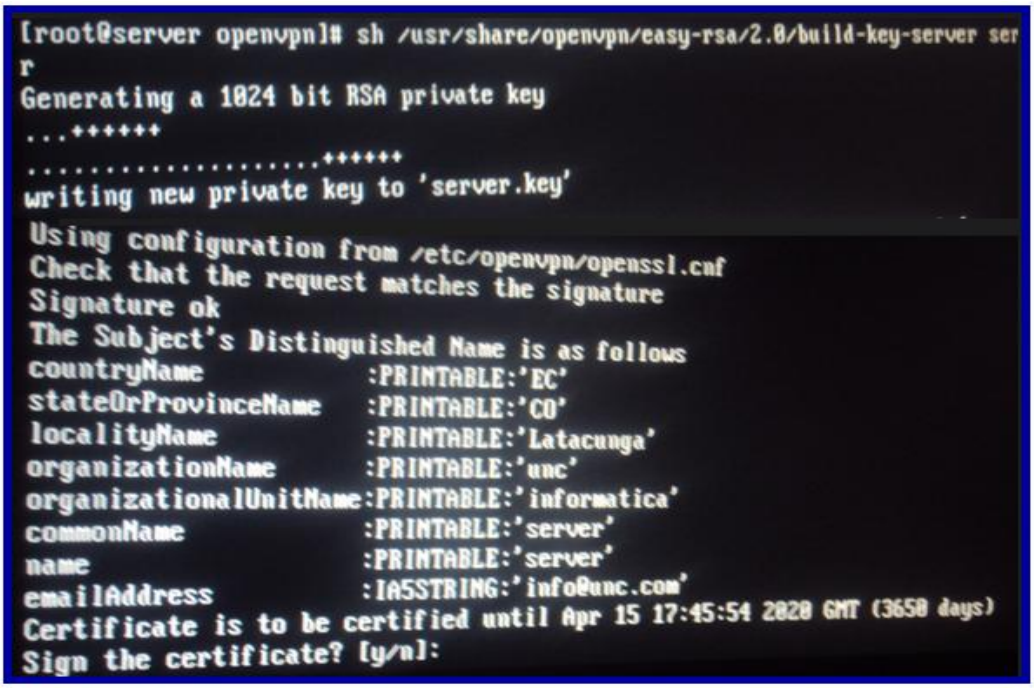
• **dh1024.pem:** generado a partir de los parámetros Diffie Hellman que se utiliza para poder intercambiar una clave entre dos participantes de manera segura.

3.8.5 Generación de clave y certificado para el servidor

Para generar la clave y el certificado del servidor se debe escribir el siguiente comando en la consola:

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

GRÁFICO Nº 3.25: CLAVE Y CERTIFICADO DEL SERVIDOR.
FUENTE: Grupo Investigador



Se han generado 3 ficheros nuevos:

• **servidor.crt:** es el certificado público del servidor.

• **servidor.key:** es la clave privada del servidor, que debe permanecer protegida.

• **servidor.csr:** este fichero sirve para poder crear el certificado del servidor en otra máquina que pueda crearlo y firmarlo, ya que este fichero tiene toda la información que le hace falta.

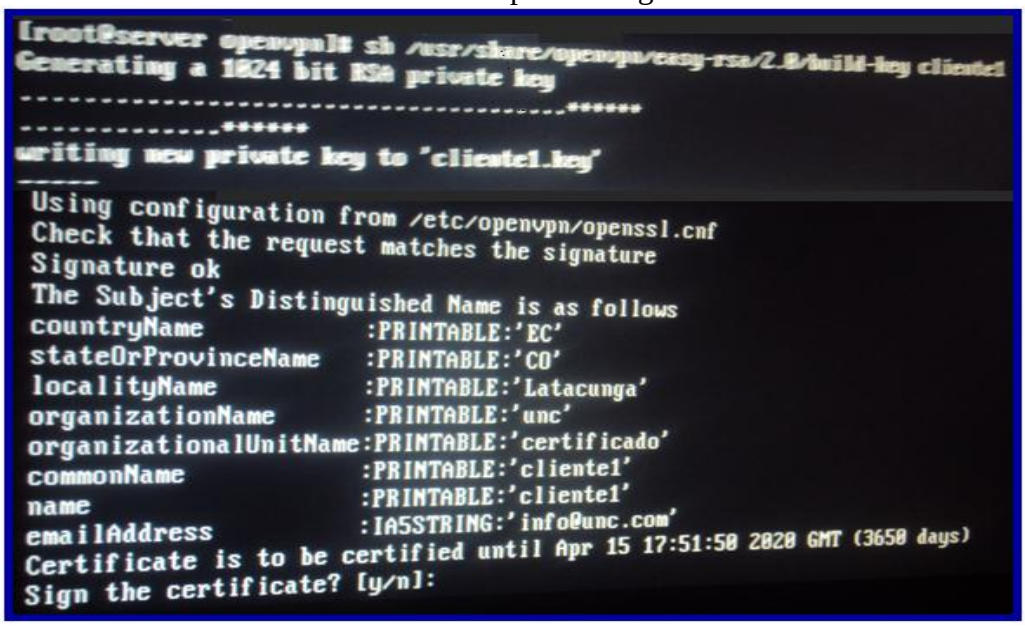
3.8.6 Generación de las firmas digitales para los clientes.

Para generar las claves y los certificados de los clientes los valores son tomados del archivo vars, con el nombre del argumento que se ha escrito como parámetro (en este caso se ha puesto cliente1)**.** Cada vez que se necesite añadir un nuevo cliente a la VPN, se debe crear un nuevo certificado y una nueva clave para ese cliente.

Para ello se debe ejecutar el siguiente comando:

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

GRÁFICO Nº 3.26: CLAVE Y CERTIFICADO DEL CLIENTE.
FUENTE: Grupo Investigador



Se han generado 3 ficheros nuevos:

• **cliente1.crt:** es el certificado público del cliente.

• **cliente1.key:** es la clave privada del cliente, que debe permanecer protegida.

• **cliente1.csr:** este fichero sirve para poder crear el certificado del cliente en otra máquina que pueda crearlo y firmarlo, ya que este fichero tiene toda la información que le hace falta.

Visualizacion de los certificados creados para el sevidor y clientes.

```
[root@server openvpn]# cd keys
[root@server keys]# ll
```

GRÁFICO Nº 3.27: CERTIFICADOS DEL SEVIDOR Y CLIENTES.
FUENTE: Grupo Investigador

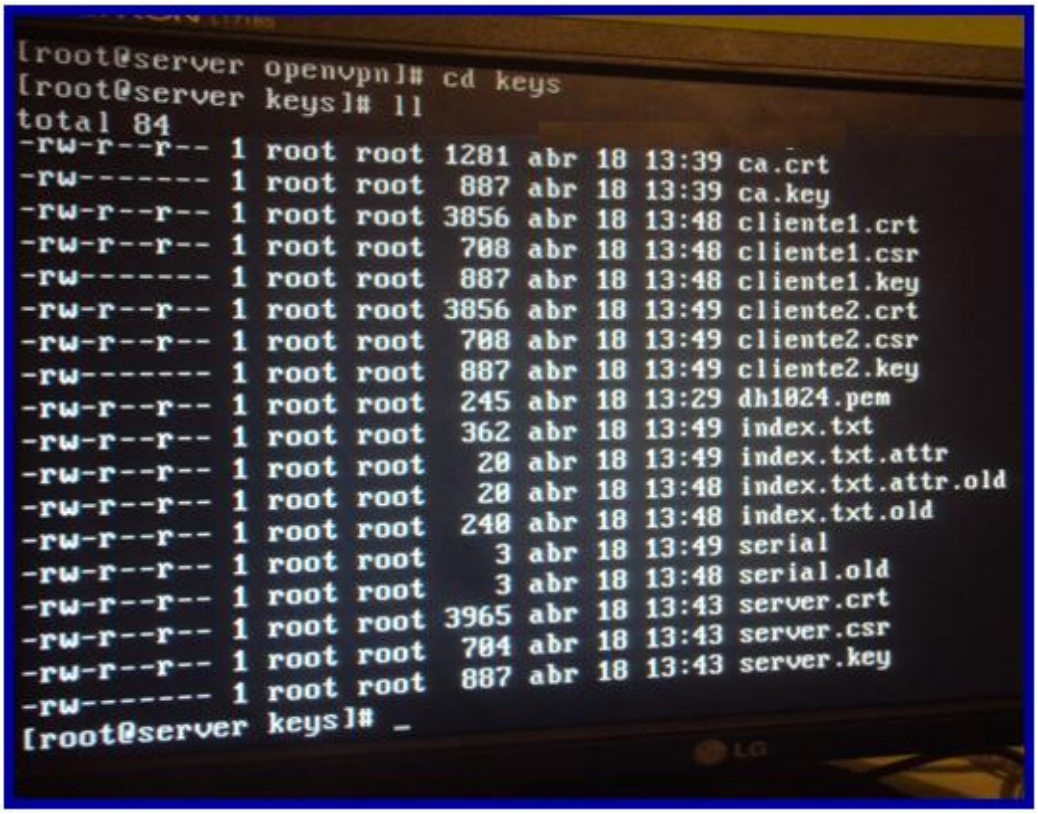


Tabla Nº 3.8: ARCHIVOS DE CERTIFICADOS Y CLAVES
REALIZADO POR: Grupo Investigador

Archivo	**Poseedor**	**Función**	**Secreto**
ca.crt	Servidor y todos los clientes	Certificado para root	**No**
ca.key	Unidad certificadora	Clave para root CA	**Si**
dh2048.pem	Servidor	Parámetros Diffie Hellamn	**No**
servidor.crt	Servidor	Certificado para servidor	**No**
servidor.key	Servidor	Clave privada para servidor	**Si**
clienteX.crt	ClienteX	Certificado para clienteX	**No**
clienteX.key	ClienteX	Clave privada para clienteX	**Si**

3.8.7 Configuración del Firewall-iptables.

Es una herramienta de firewall que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red. Las funciones más importantes del mismo, aunque no las únicas, son:

• Administración de la memoria para todos los programas y procesos en ejecución.

• Administración del tiempo de procesador que los programas y procesos en ejecución utilizan.

• Es el encargado de que sea posible acceder a los periféricos / elementos del ordenador de una manera cómoda.

Un firewall de iptables no es como un servidor, que se inicia o se detiene, o que se pueda caer por un error de programación, ya que iptables está integrado con el kernel y es parte del S.O. Para ello se ejecuta el comando iptables, con el que se añaden, borran, o crean reglas.

Es la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red. Permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Es un software disponible en prácticamente todas las distribuciones de Linux actuales.

Las reglas se agrupan en cadenas: cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en tablas: cada tabla está asociada con un tipo diferente de procesamiento de paquetes.

El kernel, dependiendo de si el paquete es para la propia máquina o para otra, consulta las reglas de firewall y decide qué hacer con el paquete según mande el firewall. Por tanto hay tres tipos de reglas en iptables que se describen brevemente a continuación:

- **INPUT chain** (Cadena de ENTRADA). Todos los paquetes destinados a este sistema atraviesan esta cadena (y por esto se la llama algunas veces LOCAL_INPUT o ENTRADA_LOCAL).
- **OUTPUT chain** (Cadena de SALIDA). Todos los paquetes creados por este sistema atraviesan esta cadena (a la que también se la conoce como LOCAL_OUTPUT o SALIDA_LOCAL).

- **FORWARD chain** (Cadena de REDIRECCIÓN). Todos los paquetes que pasan por este sistema para ser encaminados a su destino, recorren esta cadena.

Para crear las iptables para el túnel (tun0), las tarjetas de red (eth0) y servidores (FTP, SMB) utilizamos los siguientes comandos:

```
[root@server ~]# iptables -A INPUT -i tun0 -p udp --dport :1194 -j ACCEPT
[root@server ~]# iptables -A OUTPUT -o tun0 -p udp --dport :1194 -j ACCEPT
[root@server ~]# service iptables save
```

GRÁFICO Nº 3.28: CREACIÓN DEL FIREWALL-IPTABLES.
FUENTE: Grupo Investigador

Visualización de las iptables creadas.

```
[root@server ~]# iptables -nL
```

GRÁFICO Nº 3.29: VISUALIZACIÓN DEL FIREWALL-IPTABLES.
FUENTE: Grupo Investigador

```
# Generated by iptables-save v1.3.5 on Fri May 14 18:42:17 2010
*filter
:INPUT ACCEPT [12040:3328520]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [11346:2283440]
-A INPUT -i tun0 -p udp -m udp --dport 0:1194 -j ACCEPT
-A INPUT -i eth0 -p udp -m udp --dport 0:20 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 0:20 -j ACCEPT
-A INPUT -i eth0 -p udp -m udp --dport 0:21 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 0:21 -j ACCEPT
-A OUTPUT -o tun0 -p udp -m udp --dport 0:1194 -j ACCEPT
-A OUTPUT -o eth0 -p udp -m udp --dport 0:20 -j ACCEPT
-A OUTPUT -o eth0 -p tcp -m tcp --dport 0:20 -j ACCEPT
-A OUTPUT -o eth0 -p udp -m udp --dport 0:21 -j ACCEPT
-A OUTPUT -o eth0 -p tcp -m tcp --dport 0:21 -j ACCEPT
COMMIT
# Completed on Fri May 14 18:42:17 2010
```

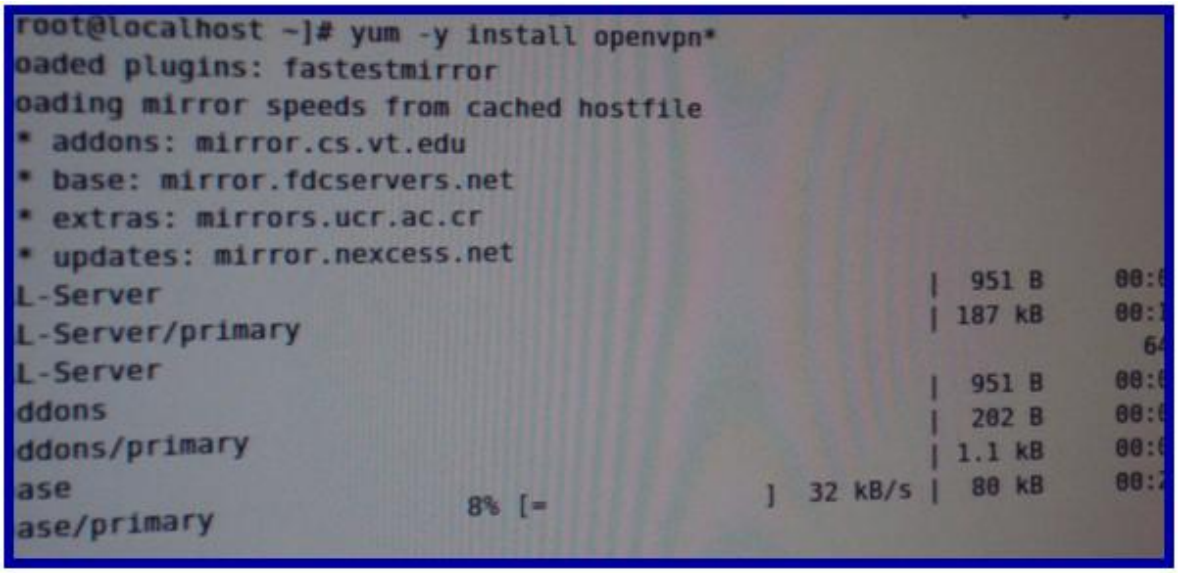
3.8.8 Instalación del paquete Openvpn en los clientes

Este es el método que funciona prácticamente en todas las distribuciones de Linux basadas en **CentOS** para todos los clientes.

Para instalar el paquete openvpn se utiliza el siguiente comando

```
[root@localhost ~]# yum -y install openvpn*
```

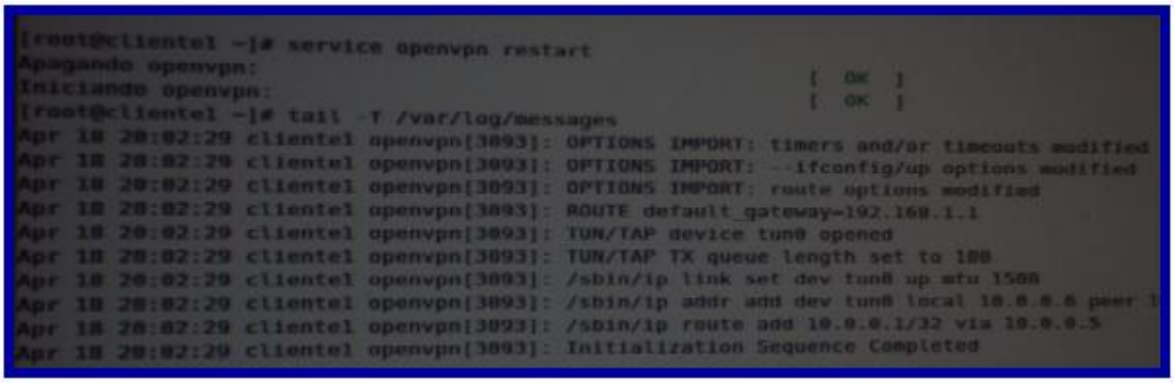
GRÁFICO Nº 3.30: OPENVPN PARA LOS CLIENTES.
FUENTE: Grupo Investigador



Para iniciar la conexión hacia la **VPN**, simplemente se inicia el servicio openvpn de la siguiente manera:

```
[root@cliente1 ~]# service openvpn restart
```

GRÁFICO Nº 3.31: INICIALIZACIÓN DE LA CONEXIÓN VPN.
FUENTE: Grupo Investigador



Para que la conexión se establezca automáticamente cada vez que se inicie el sistema, se utiliza el mandado **chkconfig** de la siguiente manera:

```
[root@cliente1 ~]# chkconfig openvpn on
```

3.8.9 Instalación del paquete Network Manager

Es una implementación que permite a los usuarios configurar interfaces de red de todos los tipos, sin necesidad de contar con privilegios de administración en el sistema. Es la forma más flexible, sencilla y práctica de conectarse a una red **VPN**.

Se requiere que los clientes tengan instalado el paquete **Network Manager-openvpn**, mismo que debe estar incluido en los depósitos Yum.

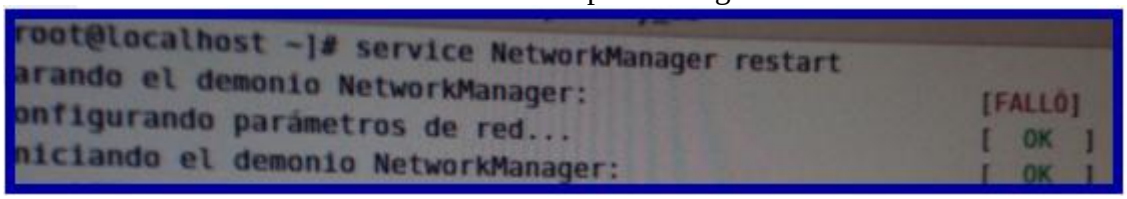
Para instalar a través del mandato **yum**, se hace de la siguiente manera:

```
[root@localhost ~]# yum -y install NetworkManager-openvpn
```

Se reinicia el sistema para que tengan efectos los cambios en el servicio Network Manager:

```
[root@localhost ~]# service NetworkManager restart
```

GRÁFICO Nº 3.32: SERVICIO NETWORK MANAGER
FUENTE: Grupo Investigador

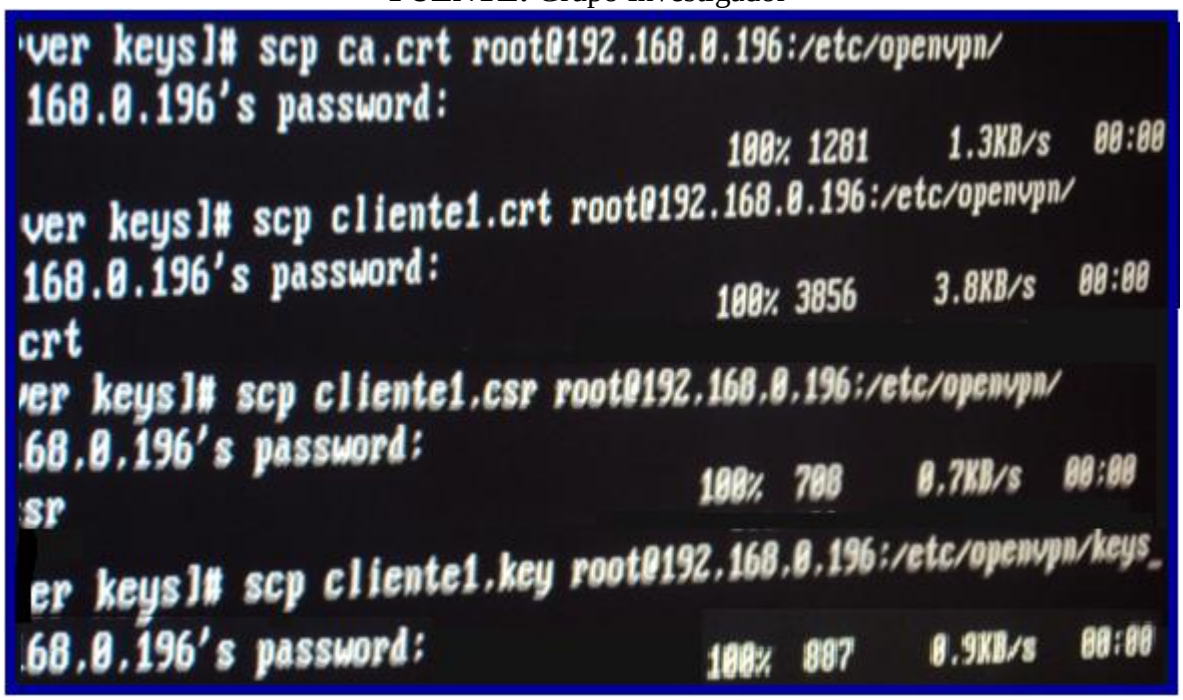


3.8.10 Protocolo de copia segura del servidor hacia los clientes.

```
[root@server keys]# scp ca.crt root@192.168.0.196:/etc/openvpn/
```

GRÁFICO Nº 3.33: COPIA DEL PROTOCOLO

FUENTE: Grupo Investigador



3.8.11 Instalación del software Filezilla

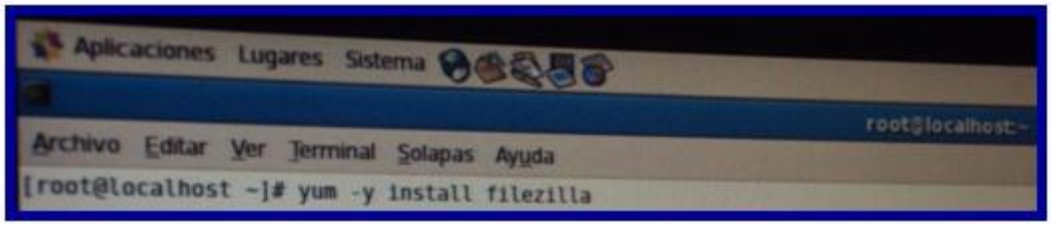
Filezilla es un programa comúnmente llamado "Cliente FTP", que incluye todo lo necesario para un programa de este tipo. Incorpora un administrador de servidores FTP para guardar las direcciones de los que se use con más frecuencia y así evitar tener que introducirlos cada vez.

Su interfaz es similar a la del Explorador de Windows, y muestra tanto la carpeta de tu PC como las carpetas remotas, permitiendo el paso de archivos de una a otra simplemente arrastrándolos.

Ejecución de los comandos para la instalación del Filezilla:

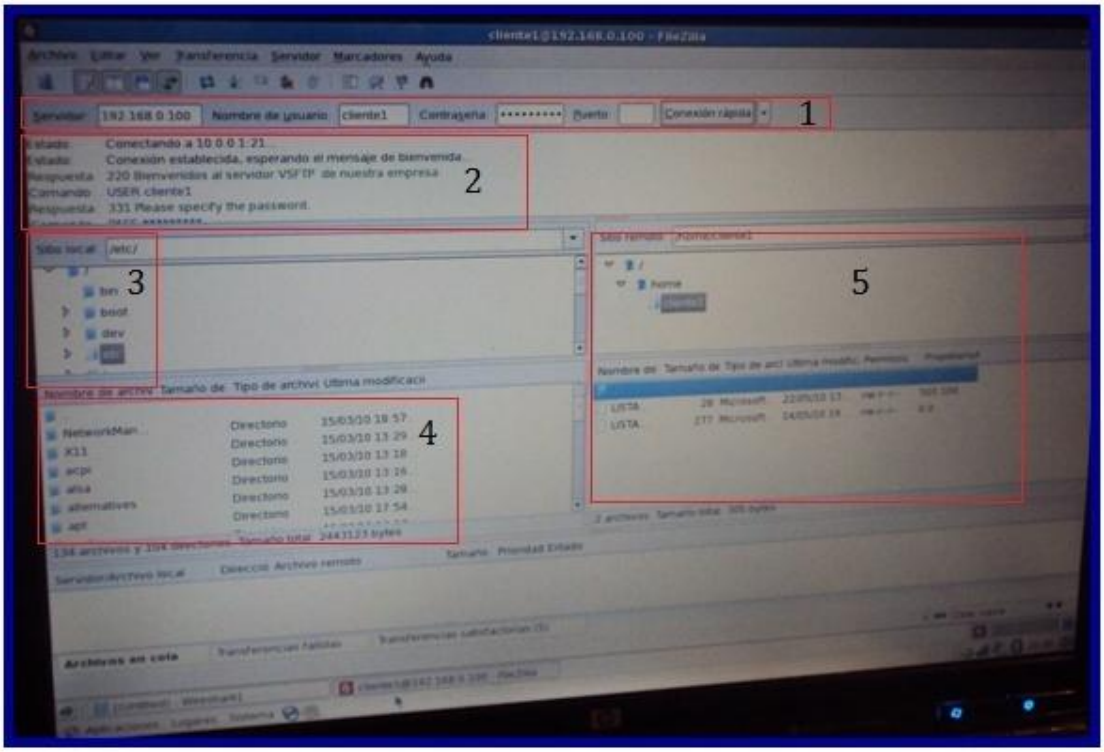
```
[root@server ~]# yum -y install filezilla
```

GRÁFICO Nº 3.34: INSTALACIÓN DEL SOFTWARE FILEZILLA
FUENTE: Grupo Investigador



Ya tenemos el programa instalado y en español, ahora vamos a explicar un poco para que sirve a cada parte del programa:

GRÁFICO Nº 3.35: SOFTWARE FILEZILLA
FUENTE: Grupo Investigador



1. Menú rápido de acceso, esta barra se usa para conectar, desconectar, actualizar rápidamente.
2. Da información sobre la conexión y comando usados por nuestro cliente ftp. En caso de producirse error lo reportara en rojo.
3. Aquí nos muestra el árbol de directorios del disco duro en el servidor.
4. Aquí los ficheros y directorios seleccionados en el árbol del punto 3.
5. Nos muestra los ficheros y directorios actuales que se encuentran en el cliente.

3.8.12 Software Wireshark

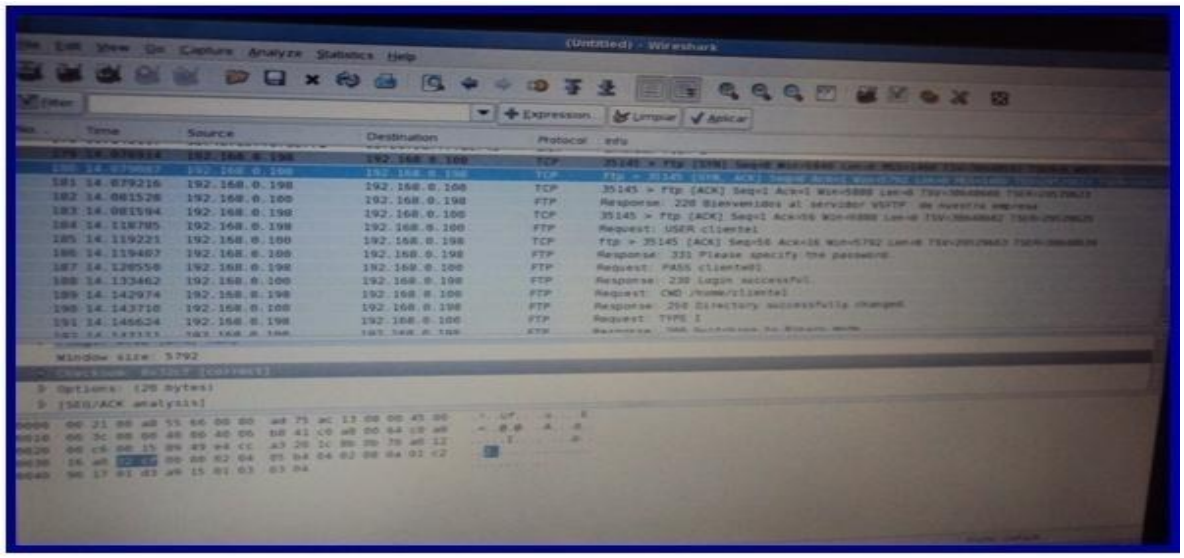
Wireshark es un analizador de tráfico de red multi-plataforma que se encuentra dentro del S.O Centos o a su vez se lo puede instalar a través de Internet. Este analizador captura paquetes de red y muestra dichos paquetes en tanto detalle como sea posible. Se puede pensar en un analizador de paquetes de red como un instrumento de medición utilizado para examinar lo que está sucediendo dentro de la red, similar a como un

electricista utiliza un voltímetro para examinar un cable de electricidad (pero a un nivel superior, por supuesto). En el pasado tales herramientas era muy costosas o propietarias, o ambas cosas al mismo tiempo, con la llegada de Wireshark todo ello cambió. Wireshark es tal vez uno de los mejores analizadores de paquetes de red en software libre disponible hoy día.

Aspectos importantes de Wireshark

- Trabaja tanto en modo promiscuo como en modo no promiscuo.
- Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
- Tiene una interfaz muy flexible.
- Gran capacidad de filtrado.
- Se ejecuta en más de 20 plataformas.
- Es compatible con más de 480 protocolos.
- Puede leer archivos de captura de más de 20 productos.

GRÁFICO Nº 3.36: SOFTWARE WIRESHARK
FUENTE: Grupo Investigador



Es un software importantísimo para los que necesiten examinar el tráfico de su computadora, para examinar el funcionamiento de algún programa debido a cualquier tipo de fallos, o para conocer el formato de un protocolo.

3.9 Banda C en la frecuencia de 3.8 GHz.

La banda C es un rango del espectro electromagnético de las microondas que comprende frecuencias de entre 3,8 y 4,2 GHz y desde 5 hasta 6,4 GHz, la Banda C exige antenas mayores que las demás. Aunque esto no es un problema mayor para instalaciones permanentes. Comparado con otras bandas, la Banda C es más confiable bajo condiciones adversas, principalmente lluvia fuerte y granizo. Al mismo tiempo, las frecuencias de Banda C son menos congestionadas que las de 2.4 GHz.

3.9.1 Distribución de equipos de la red inalámbrica en la frecuencia de 3.8 GHz.

Router

Router DIR-635 Dual de D-Link extiende la cobertura de la red Inalámbrica con frecuencia de 2.4 y 5 GHz, equipado con la tecnología Wireless N, este router de alto rendimiento proporciona total cobertura en toda la organización o empresa, al mismo tiempo que elimina los puntos muertos donde la señal antes no tenía acceso. El Router está diseñado para su funcionamiento en grandes instituciones y pensado para usuarios que desean una red de alto rendimiento.

Es un dispositivo que cumple con el estándar 802.11n y que ofrece un rendimiento real más rápido (hasta 650% más rápido que el estándar 802.11g) que una conexión inalámbrica 802.11g y que una Ethernet por cable a 100Mbps. Con tan solo conectar el Router Range Booster a un módem DSL, ya podrá compartir su acceso de alta velocidad a internet con cualquier persona que esté en la red.

El Router DIR-635 soporta las últimas características de seguridad inalámbrica para evitar el acceso no autorizado, ya sea desde la red inalámbrica o desde Internet. El soporte para

los estándares WPA y WEP garantiza que podrá usar la mejor encriptación posible, independientemente de los dispositivos de red que tengan los pc´s que se conecten a la red.

Además, el router incorpora un potente sistema de seguridad doble Firewall para evitar posibles ataques provenientes desde Internet. Al ofrecer el mejor rendimiento inalámbrico, completa seguridad para la red con mayor cobertura y compartir el acceso a Internet para todos los usuarios disponibles.

CARACTERÍSTICAS PRINCIPALES

- Motor de Calidad de Servicio (QoS) incluido y la última tecnología Wireless
- Cobertura de la red Inalámbrica con frecuencia de 2.4 y 5 GHz
- Rendimientos de hasta un 650% superior al estándar 802.11g y un alcance Inalámbrico hasta 5 veces mayor
- Excepcional cobertura gracias a la tecnología y compatibilidad con múltiples antenas.
- Mejores y más completas características de seguridad, incluyendo Firewall SPI y WPA para proteger su red de posibles intrusos.

GRÁFICO Nº 3.37: ROUTER DIR-635 DUAL.
REALIZADO POR: Grupo Investigador

TARJETA PCIWMP 600 N

La tarjeta de red inalámbrica WMP600N de Linksys funciona con la tecnología inalámbrica N que puede alcanzar un caudal de datos hasta 12 veces superior al de la tecnología inalámbrica G. Una vez instalada, se tendrá una red muy potente que permitirá compartir los datos más voluminosos con una rapidez impresionante, especialmente para los flujos, vídeo, sonido, los juegos de vídeo e incluso la telefonía en IP.

Características:

- Conexión del Adaptador Inalámbrico-N de alta velocidad con doble banda para las computadoras de escritorio.
- Opera en las bandas de radio de 2.4 y 5GHz con opción de seleccionar la que tenga la menor congestión en el área.
- La encriptación WPA2 de fortaleza industrial ayuda a proteger sus datos y su privacidad.
- Ofrece desempeño óptimo al conectarse con el Inalámbrico-N pero también se conecta a las redes Inalámbricas-G, -B y -A.

GRÁFICO Nº 3.38: TARJETA PCI WMP 600 N.
REALIZADO POR: Grupo Investigador

Adaptador de red USB Wireless-N con banda dual

El adaptador de red USB tiene el máximo rendimiento de conformidad con las especificaciones IEEE Standard 802.11. El rendimiento real de la capacidad de la red inalámbrica, la velocidad de los datos, el alcance y el área de cobertura pueden variar El rendimiento depende de diversos factores, condiciones y variables tales como la distancia desde el punto de acceso, el volumen del tráfico de red, las construcciones y sus materiales, el sistema operativo utilizado, la combinación de productos inalámbricos, las interferencias y otras condiciones adversas.

La encriptación WPA de potencia industrial ayuda a proteger la confidencialidad de la comunicación e información.

Características

- Conexión en red Wireless-N de banda dual de alta velocidad para la PC de escritorio o portátil
- La tecnología MIMO utiliza múltiples radios para crear señales robustas y maximizar el alcance y la velocidad con menos puntos muertos
- Es mucho más rápida que Wireless-G, pero también puede conectarse con redes Wireless-G, -B y -A
- Rendimiento con protección de su inversión: compatibilidad con los estándares de Wireless-B (802.11b) y Wireless-G (802.11g)
- Admite encriptación de hasta 256 bits (WEP, WPA y WPA2)
- Interfaz USB 2.0
- Asistente de configuración fácil de usar

GRÁFICO Nº 3.39: ADAPTADOR DE RED USB WIRELESS N.
FUENTE: Grupo Investigador

ANTENAS

Las seguridades que disponen las antenas que se encuentran implantadas en la Dirección Nacional de Comunicaciones se asignaron contraseñas de encriptación independientes para no alterar el normal funcionamiento de la red inalámbrica de los Departamentos y que la información pueda fluir de una manera más optima, cabe recalcar que el ancho de banda es el mismo en los departamentos que usted desee conectar.

Hoy en día se suelen utilizar antenas parabólicas, para conexiones a larga distancia, también se utilizan conexiones intermedias punto a punto entre antenas parabólicas.

Entre los modelos y variantes de antenas, se pueden distinguir dos grandes familias: Las antenas Direccionales y las antenas Omnidireccionales. Como su nombre lo indica, las direccionales emiten la señal hacia un punto en concreto, con mayor o menor precisión.

Las "Omni" por el contrario, emiten por igual en todas direcciones, en un radio de 360, dentro del grupo de antenas direccionales que utilizan la DINACOM, tenemos las de Rejilla o Grid, las parabólicas, aunque tienen su tela también hay que decir que cuanta más alta sea la ganancia de la antena, mayores distancias podemos cubrir con una antena, y con mejor calidad podremos captar señales que pudieran llegar muy débilmente.

Antena parabólica de rejilla cuadrada.

La antena cuadrada de la rejilla esta diseña para el sistema del espectro de extensión y su dimensión adentro se conforma con el diagrama del reflector de la alimentación, que

aseguran los trabajos de la antena en el mejor estado. También, esta antena ofrece alto aumento, distancia de funcionamiento larga, el peso ligero, la estructura compacta y el buen comando en resistencia del viento.

Características

- Antena parabólica 27dBi de la rejilla cuadrada adaptable a la frecuencia de 2.4 y 5 Ghz.
- Diseño a prueba de mal tiempo de la fibra de vidrio para el uso al aire libre
- Conectador femenino de N

Especificaciones

Gama de frecuencia: 5725-5850 megaciclos

Anchura de banda: 125 megaciclos

Aumento: dBi 27

Hembra del conectador N o varón de N

GRAFICO 3.40: ANTENA DE REJILLA DNC
REALIZADO POR: Grupo Investigador

Antena Parabólica.

Es un rango del espectro electromagnético de las microondas que comprende frecuencias de entre 3,7 y 4,2 GHz y desde 5,9 hasta 6,4 GHz. Es más confiable bajo condiciones

adversas, principalmente lluvia fuerte y granizo. Proveé a los usuarios acceso inalámbrico debanda ancha permitiendo libertad en la navegación en Internet y acceso a cualquier dato mientras se encuentre bajo la cobertura WiMAX en la oficina.

Características:

- Trabaja con los estándares 802.11g, a, b, n.
- Trabaja en las Banda de Frecuencia de 2.4 y 5 GHz.
- Tiene una buena cobertura.
- Compatibilidad con las redes existentes.

GRAFICO 3.41: ANTENAS PARABOLICAS DNC
REALIZADO POR: Grupo Investigador

CONCLUSIONES

- Con la Implantación de una red LAN inalámbrica en la banda de 3.8 GHz, utilizando códigos de encriptación PKI y VPN para segmentación de nodos a través de software libre en la Dirección Nacional de Comunicaciones se logra el objetivo principal de este trabajo, el mismo que permite que los datos de la DINACOM sean transmitidos a través de la red pública desde cada uno de los departamentos, proporcionando mayor rapidez, seguridad y confiabilidad.

- Luego de un análisis de las seguridades VPN y PKI se ha podido determinar que la implantación de estas es una de las mejores opciones de comunicación, ya que resulta muy beneficiosas tanto en aspectos económicos como en la fiabilidad de la transmisión de la información.

- Para la implantación de este trabajo se requiere tener un conocimiento detallado de la infraestructura de la red en donde se va a implantar, debido a que en base a dicho conocimiento se deberá seleccionar la arquitectura y las seguridades que se deben aplicar a la misma.

- La interconexión de redes constituye una tendencia fuerte en el manejo de transporte de información, debido a que los requerimientos de los usuarios son más complejos día a día y varían rápidamente, las soluciones de interconexión deben ser cada vez más cómodas y fáciles de implantar.

- Definitivamente la banda C seguirá siendo motivo de investigación, en un futuro, muchos estaremos utilizando esta tecnología incluso sin saberlo y el aporte que demos todos los profesionales involucrados en la red de información será fundamental.
- Se analizó que el S.O Linux es una alternativa totalmente viable, la institución está en la posibilidad de integrar en sus departamentos dicho sistema, sin costo comparando con los sistemas tradicionales mismos que tienen un costo elevado.

- En el presente estudio que se ha realizado sobre la banda C, software libre, la VPN y PKI hemos cumplido con los objetivos planteados para poder realizar la interconexión de los departamentos así como también de los usuarios a través de un canal seguro de comunicación.

RECOMENDACIONES

- Se recomienda que el personal encargado de manejar y realizar el monitoreo de los Servidores de la Institución, establezca las políticas de seguridad necesarias para

evitar el acceso a usuarios no autorizados a la información y de esta manera evitar modificaciones en la misma.

- Se recomienda a los Administradores de la red tener un Plan de Contingencias, qué permita dar una breve solución a los diversos problemas que se puedan presentar en está, en el caso de producirse desastres físicos o eléctricos.

- Se recomienda subir la velocidad del ancho de banda para tener una mejor conexión y transmisión de datos más rápida en todos los departamentos.

- Se recomienda a los administradores de la red (VPN y PKI) hacer un monitoreo continuo de logs que genera la VPN, para poder determinar quienes realizaron las conexiones y a que información accesaron.

DEFINICIÓN DE TÉRMINOS BÁSICOS

A

Accesibilidad: Permite asegurar quien puede acceder a la información y cuando.

Ancho de banda: En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un periodo

de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobites por segundo (kbps), o megabites por segundo (mps).

Autentificación: Determina si un usuario tiene permiso de acceso a un recurso o para realizar una operación.

Autenticidad: Permite asegurar el origen y destino de la información.

B

Backbone: Es la parte más robusta de una red donde se distribuyen cada una de sus sub redes.

C

Certificados digitales: Físicamente es un archivo de hasta 2 k de tamaño que contiene principalmente, los datos de una entidad, una persona o un servidor, la clave publica de esa entidad, y la firma de una autoridad certificadora que es reconocida con la capacidad de poder comprobar la entidad de la persona (o servidor) y valida la clave pública que es asociada a la entidad.

Cifrar: Es la acción que produce un texto cifrado (ilegible) a partir de un texto original.

Código: Conjunto de signos convencionales o instrucciones que permiten representar los datos para el manejo en la computadora.

Configurar: Definir opciones y parámetros para el correcto funcionamiento de un programa o para ajustar a nuestras necesidades el modo de operar el ordenador.

Contraseña o Password: Es una clave secreta que solo debe conocer el propietario de un acceso a un ordenador o de una cuenta de conexión a Internet.

Confidencialidad: La información solo está disponible para usuarios autorizados.

Cortafuegos: Firewall: filtra todo el tráfico de la red inspeccionando su origen y decidiendo si puede seguir hasta su destino dentro de la red.

Clave pública: Es la clave públicamente conocida, que se usa en la criptografía asimétrica.

Clave privada: La clave secreta de un sistema criptográfico de Clave Pública, usada para desencriptar los mensajes entrantes y firmar los salientes.

D

Dirección IP (Protocolo Internet): Dirección exclusiva que identifica a un host en una red. Identifica a un equipo como una dirección de 32 bits que es exclusiva en una red.

E

Encriptación: Base de la seguridad en la red. La encriptación codifica los paquetes de información que fluyen por la red, con el fin de evitar que accedan a dicha información terceras personas.

F

Firma digital: Es un método que se usa criptografía asimétrica y permite autenticar una entidad (persona o servidor), tiene una función igual que la firma convencionable

I

Implantación: Puesta en marcha un sistema.

Internet: Red global de equipos cuyas comunicaciones se realizan mediante un protocolo común TCP/IP.

Integridad: Permite asegurar que no se ha falseado la información.

N

Nodo: Generalmente ordenador o punto de una red en el que se producen operaciones de conmutación o similares. Tratándose en este aspecto, cada nodo precisa una conexión, que es un adaptador este proporciona un número (en hexadecimal) único en la red para poder distinguir de forma inequívoca el terminal.

P

Políticas: La política es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.

PKI Infraestructura de Clave Pública: Sistema de certificados digitales, Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet.

Protección de datos: Conjunto de técnicas utilizadas para preservar la confidencialidad, la integridad y la disponibilidad de la información.

Protocolo: Se define como el conjunto de reglas ya aprobadas que posibilitan la comunicación entre ordenadores o entre programas que de otra forma serian incompatibles.

R

Redes: Conjunto de ordenadores conectadas entre sí ya sea alámbricas o inalámbricamente

Redes Inalámbricas: Una red de área local inalámbrica es un sistema de comunicación de datos flexible que pueda reemplazar o extender una red de área local cableada LAN para ofrecer funcionalidad adicional.

S

Servidor: Se denomina así al ordenador que se encarga de suministrar lo necesario a una red, dependiendo de cuál sea la finalidad de esta.

T

Tarjeta de Red Inalámbrica: Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: CompactFlash, PCI, PCMCIA, USB.

TCP/IP: Las direcciones IP suelen representarse mediante notación decimal con puntos que muestra cada octeto (8 bits o un byte) de una dirección IP como su valor decimal y separa a cada uno de los octetos mediante un punto ejemplo 192.168.0.1

V

VPN - Red Privada Virtual: Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado.

BIBLIOGRAFIA

http://www.pucelawireless.net/index.php?pagename=AccessPoint.

http://www.monografias.com/trabajos18/redes-computadoras/redes-computadores.html.

http://es.wikipedia.org/wifi

SHELDON,Tom, Manual de referencia, España, Editorial Mc Graw Hill, 2004.

SHELDON,Tom, Novell Netware, Cuarta Edición , Mc Graw Hill, 2004

FREDERMAN, Alan, Diccionario de Computación, Edición marzo 2002, Bogota-Colombia.

www.linuxparatodos.org

Carballar, José A. El libro de las Comunicaciones del PC, HP, España, 2006. Pág. 10-14

http://congreso.hispalinux.es/

http://www.divisait.com/docs/Hojas%20de%20Aplicacion/VNPs%20y%20Redes%20Seguras_v.2.0_.pdf

http://es.wikipedia.org/wiki/Wi-Fi.

http://www.geocities.com/TimesSquare/Chasm/7990/topologi.htm

Hills "Large-Scale Wireless LAN Desing". IEEE Communications Magazine, vol.39,nº 11, noviembre 2001.

http://www.iearobotics.com/personal/juan/publicaciones/art5/html/node2.html

Jesus M. Gonzalez-Barahona 2003-04-06

KONSTANTIN GAVRILENKO (2005), Hacking Wireless, Editorial GRUPO AMAYA S.A, Madrid.

http://www.laserwifi.com/arquitecturavpn.htm

http://www.maginvent.org/articles/linuxmm/Ventajas_Linux.htm

http://www.mastermagazine.info/articulo/10564.php

http://www.microsoft.com/spain/isaserver/prodinfo/features.mspx

MIKHAILOVSKY Andrei A. (2005); El mundo de la seguridad inalámbrica; ediciones AMAYA S.A, Madrid

http://www.monografias.com/trabajos/solinux/solinux.shtml

MOREIRA, Adriano C. “2002”; DOCUMENTO IEEE ”Redes”, Universidad de Averio; Portugal.

RODRIGUEZ Jorge, Introducción a las Redes de Área Local, McGraw Hill, México, 2000. Pág 23, 28.

http://www.rsasecurity.pki.com

http://www.taringa.net/linux/1601181/CentOS-5_2.html
http://www.taringa.net/posts/linux/1601181/CentOS-5_2.html

VLADIMIROV Andrew A (2005), Seguridad de Redes Inalámbricas, Ediciones AMAYA MULTIMEDIA, Madrid, España.

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, ANSI/IEEE Std 802.11, 2000 Edition.