UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERIA Y APLICADAS

CARRERA INGENIERIA EN INFORMATICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN

"ANÁLISIS E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL VPN CON TUNELES DE SEGURIDAD EN EL TRANSPORTE DE DATOS CON UN SERVIDOR CENTOS LINUX: CASO PRÁCTICO: PROPUESTA DE IMPLEMENTACIÓN EN LAUNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI".

Proyecto de Investigación presentado previo a la obtención del Título de INGENIERO EN INFORMATICA Y SISTEMAS COMPUTACIONALES.

Autor:

Oña Llumitasig Diego Javier

Director:

PhD. Gustavo Rodríguez

Latacunga - Ecuador

Mayo 2016

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la Unidad Académica de Ciencias de la Ingeniería y Aplicadas; por cuanto, el o los postulantes: Diego Javier Oña Llumitasig con el título de Proyecto de Investigación:**ANÁLISIS E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL VPN CON TUNELES DE SEGURIDAD EN EL TRANSPORTE DE DATOS CON UN SERVIDOR CENTOS LINUX: CASO PRÁCTICO: PROPUESTA DE IMPLEMENTACIÓN EN LA UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**,han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, Mayo2016

Para constancia firman:

…… ……

Ing. Segundo Corrales
LECTOR 1

Ing. Verónica Zapata
LECTOR 2

……..……..

Lcda. Susana Pallasco

LECTOR 3

www.utc.edu.ec
Av. Simón Rodríguez s/n Barrio El Ejido /San Felipe. Tel: (03) 2252346 – 2252307 - 2252205

DECLARACIÓN DE AUTORÍA

Yo Diego Javier Oña Llumitasig declaro ser autor (a) del presente proyecto de investigación: "**ANÁLISIS E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL VPN CON TUNELES DE SEGURIDAD EN EL TRANSPORTE DE DATOS CON UN SERVIDOR CENTOS LINUX: CASO PRÁCTICO: PROPUESTA DE IMPLEMENTACIÓN EN LA UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**", siendo el PhD. Gustavo Rodríguez director del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

.....

Diego Javier Oña Llumitasig

C.I. 0503081960

www.utc.edu.ec
Av. Simón Rodríguez s/n Barrio El Ejido /San Felipe. Tel: (03) 2252346 – 2252307 - 2252205

AVAL DEL DIRECTOR DE TESIS

En calidad de Director del Trabajo de Investigación sobre el tema:

"ANÁLISIS E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL VPN CON TUNELES DE SEGURIDAD EN EL TRANSPORTE DE DATOS CON UN SERVIDOR CENTOS LINUX: CASO PRÁCTICO: PROPUESTA DE IMPLEMENTACIÓN EN LA UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI".

Del señor Oña Llumitasig Diego Javier, de la Carrera de Ingeniería en Informática y Sistemas Computacionales.

CERTIFICO QUE:

Una vez entregado el documento a mi persona considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la **Evaluación del Tribunal de Validación de Proyecto de Investigación** que el Honorable Consejo Académico de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, Mayo, 2016

EL DIRECTOR

.....

PhD. Gustavo Rodríguez

CI. 1757001357

EL DIRECTOR DE TESIS

www.utc.edu.ec
Av. Simón Rodríguez s/n Barrio El Ejido /San Felipe. Tel: (03) 2252346 – 2252307 - 2252205

AGRADECIMIENTO

Agradezco infinitamente a mis padres por apoyarme en todo momento, sin importar la situación en la que nos hemos encontrado.

A esta noble y querida institución UNIVERSIDAD TECNICA DE COTOPAXI que me acogió para que pudiera seguir mis estudios y así salir adelante a base de esfuerzo y dedicación.

A mi grupo de trabajo Ing. Segundo Corrales y PhD. Gustavo Rodríguez por su paciencia y compartir sus conocimientos y experiencias conmigo.

A cada una de las personas que me ayudaron incondicionalmente de una u otra manera para que este gran sueño se haga realidad.

Agradezco a mis familiares y amigos que confiaron en mí dándome apoyo constante para que siga adelante y no desmaye en el proceso de este gran sueño.

Y como olvidarme de mis queridos profesores que compartieron sus conocimientos desde la escuela hasta la universidad, ya que han formado parte fundamental en mi vida.

Diego

DEDICATORIA

A mi dios por ayudarme día a día iluminado mi camino y seguir adelante a pesar de todo lo que me ha tocado vivir para llegar a estas instancias, el cual forma una parte fundamental en mi vida.

A mi madre querida María Ercelinda quien es la persona más importante en mi vida ya que sin ella nada hubiese sido igual, admiro tu coraje, fuerza, perseverancia, respeto y amor, me has enseñado a salir adelante siempre, a tu lado he pasado momentos muy lindos y a la vez muy duros y difíciles, pero cada uno de ellos los hemos superado juntos agradezco a dios desde fondo de mi corazón que seas mi madre.

A mis hermanos que de alguna u otra manera me han ayudado a pesar de no estar cerca. Por sus consejos y apoyo incondicional.

A mi tío José Miguel quien este donde este siempre lo llevare en mi corazón, gracias por tus consejos y apoyo, para mi fuiste como un segundo padre y me siento muy orgulloso de que seas parte de este gran logro en mi vida.

Diego

INDICE GENERAL

INDICE DE TABLAS Y GRAFICOS

TABLAS

GRAFICOS

UNIVERSIDAD TECNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TITULO:" ANÁLISIS E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL VPN CON TUNELES DE SEGURIDAD EN EL TRANSPORTE DE DATOS CON UN SERVIDOR CENTOS LINUX: CASO PRÁCTICO: PROPUESTA DE IMPLEMENTACIÓN EN LA UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**".**

Autor: Diego Javier Oña Llumitasig

RESUMEN

En este proyecto se analiza y se implementa un modelo de seguridad de red y datos que ayudan a la protección de la información de intrusos no deseados que podrían perjudicar de una u otra manera la integridad de cada institución , por ende se apuesto interés en el tema de seguridades ya que forman parte de un una nueva tecnología formada por certificados de autenticación, llaves de seguridad tanto como del servidor y los clientes y a la ves la incorporación de túneles que permiten el traslado del tráfico de datos e información segura en la nube y que forman parte fundamental de una **Red Privada Virtual VPN.** Se ha tomado en cuenta la necesidad de los usuarios de la Unidad de Admisión y Nivelación de la Universidad Técnica de Cotopaxi, para el envío y recepción segura de información utilizando tecnologías actuales dentro de los parámetros establecidos por normas de seguridad. Para el desarrollo del presente trabajo investigativo se aplican herramientas tecnológicas que están dentro del mercado de la informática como son la **Red Privada Virtual VPN** el cual cumple todos los requerimientos de seguridad para su implementación.

Palabras clave: Red Privada, Sistemas Operativos, Certificados, Transferencia de Datos, Configuración.

UNIVERSIDAD TECNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TITULO:" ANÁLISIS E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL VPN CON TUNELES DE SEGURIDAD EN EL TRANSPORTE DE DATOS CON UN SERVIDOR CENTOS LINUX: CASO PRÁCTICO: PROPUESTA DE IMPLEMENTACIÓN EN LA UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**".**

Autor: Diego Javier Oña Llumitasig

ABSTRACT

In this project a network security model is analyzed an applied in order to protect information from unwanted intruders that could hurt in one or another way the institution integrity, therefore the interest is looking at the issue where securities are implemented as part of a new technology by authentication certificates, security keys as well as server and clients and also the incorporation of tunnels that allow the data transfer and secure information in the cloud and they would be an essential part of a Virtual Private Network (VPN).It has taken into account the users need at the Admission and Leveling Unit in the Technical University of Cotopaxi, for sending and receiving secure information by using current technologies within the parameters set by safety standards. For the development of this research technological tools that are within the computing market such as virtual private network VPN were applied which meets all safety requirements for implementation apply.

Key words: Private Network, Operating Systems, Certificates, Data Transfer, Settings.

AVAL DE TRADUCCION

En calidad de Docente del Idioma Inglés del Centro Cultural de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal CERTIFICO que: La traducción del resumen de tesis al Idioma Inglés presentado por el señor Egresado de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas: **OÑA LLUMITASIG DIEGO JAVIER**, cuyo título versa **"ANÁLISIS E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL VPN CON TUNELES DE SEGURIDAD EN EL TRANSPORTE DE DATOS CON UN SERVIDOR CENTOS LINUX: CASO PRÁCTICO: PROPUESTA DE IMPLEMENTACIÓN EN LA UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI"**, lo realizó bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a los peticionarios hacer uso del certificado de la manera ética que estimen conveniente.

Latacunga, Mayo del 2016

Atentamente,

M. Sc Lidia Rebeca Yugla Lema
DOCENTE CENTRO CULTURAL DE IDIOMAS
C.C. 050265234-0

www.utc.edu.ec

Av. Simón Rodríguez s/n Barrio El Ejido /San Felipe. Tel: (03) 2252346 – 2252307 - 2252205

PROYECTO DE TITULACIÓN

INFORMACIÓN BÁSICA

PROPUESTO POR:

Diego Javier Oña Llumitasig.

TEMA APROBADO:

Análisis e implementación de una Red Privada Virtual VPN con túneles de seguridad en el transporte de datos con un servidor Centos Linux: caso práctico: propuesta de implementación en la Unidad de Admisión y Nivelación de la Universidad Técnica de Cotopaxi.

CARRERA:

Ingeniería en Informática y Sistemas Computacionales

DIRECTOR DE PROYECTO DE TITULACIÓN:

PhD. Gustavo Rodríguez

EQUIPO DE TRABAJO:

Diego Javier Oña Llumitasig

LUGAR DE EJECUCIÒN:

Unidad de Admisión y Nivelación de la Universidad Técnica de Cotopaxi, ubicada en el sector de San Felipe del cantón Latacunga Provincia de Cotopaxi.

TIEMPO DE DURACIÒN DEL PROYECTO:

Febrero- Mayo 2016

LÍNEA(S) Y SUBLINEAS DE INVESTIGACIÓN:(Fuente: Comité de Investigación UTC, "Líneas de Investigación UTC")

- **Línea de investigación:**

Tecnologías de la información y comunicación (TICs).

- **Sublínea de Investigación de la Carrera:**

Diseño, implementación y configuración de redes y Seguridad Computacional, aplicando normas y estándares internacionales.

TIPO DE INVESTIGACIÓN

En este proyecto se utilizara el tipo de investigación descriptiva porque se va a realizar un análisis de las seguridades con las que debería contar un servidor al momento de transportar datos e información, por ende se analiza los beneficios que debería tener al utilizar túneles y certificados de autenticación, ya que de esta manera se puede interpretar cada una de las tecnologías que forman parte de la red y a identificar los procesos existentes en la implementación de nuevas y mejores tecnologías basados a mejorar la calidad del servicio y seguridad de red.

INFORMACIÓN DEL PROYECTO

1. TÍTULO DEL PROYECTO

Análisis e implementación de una Red Privada Virtual VPN con túneles de seguridad en el transporte de datos con un servidor Centos Linux: caso práctico: propuesta de implementación en la Unidad de Admisión y Nivelación de la Universidad Técnica de Cotopaxi.

2. TIPO DE PROYECTO/ALCANCE:

En el presente tema se ha elegido el tipo de proyecto investigativo ya que se va a realizar análisis de procesos y funcionamientos de cada una de las capas de red y de cómo mejorar la seguridad en el en transporte y el envío de datos y paquetes permitiendo dar un óptimo desempeño a las mismas.

3. ÁREA DEL CONOCIMIENTO

- Las Redes en procesos industriales, de la calidad y seguridad laboral, así como la educación y comunicación para el desarrollo humano y social.
- Optimización de recursos en redes de comunicaciones.
- Redes de Distribución de Contenidos.

4. SINOPSIS DEL PROYECTO

Con este proyecto se pretende incursionar en un nuevo método de seguridad de red y datos, a la vez interconectar computadoras de forma certificada dentro de la red, dando lugar a una nueva forma de comunicación segura utilizando una red virtual, para lo cual se ha visto la necesidad de realizar un análisis en la seguridad que se presentan al momento de navegar en internet, que permitirá determinar la aplicación, con el único propósito de mejorar el servicio de red. Se ha puesto en énfasis determinar las seguridades que existen actualmente al utilizar túneles ya que se ha visto la necesidad de profundizar en este tipo de tecnología. Con la finalidad de demostrar he implementar los avances tecnológicos de este proyecto el cual se lo va a realizar en el UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

5. DESCRIPCIÓN DEL PROBLEMA

El aumento del número de conexiones y la incorporación a la red de datos e información muy importantes, ha provocado que en la UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, ubicada en el sector de San Felipe del cantón Latacunga Provincia de Cotopaxi, se ha visto la necesidad de implementar nuevas y mejores tecnologías en la red, mejorando notablemente la seguridad en el envío de datos e información relevante, actualmente en la Institución Financiera y muchas otras empresas están siendo afectadas debido a las vulnerabilidades encontradas en los últimos VPN pptpd y debido a que es compatible con todos los sistemas operativos recientes por defecto. Se ha elegido una VPN con certificados de autenticación más que nunca por su libertad y la

privacidad en línea cuando está amenazada. Los gobiernos y los proveedores de Internet quieren controlar lo que puede y no se puede ver, mientras se mantiene un registro de todo lo que haces, e incluso el tipo de aspecto sombrío al acecho alrededor de la cafetería, o la puerta del aeropuerto pueden tomar sus datos bancarios más fácil de lo que piensa. Un auto alojado VPN le permite navegar por la web de la manera que se esperaba anónima y sin supervisión, a través del cual todos sus datos en línea pasa de ida y vuelta. Cualquier aplicación que requiera una conexión a internet funciona con este auto alojado VPN, incluyendo su navegador web, cliente de correo electrónico, y el programa de mensajería instantánea, manteniendo todo lo que haces en línea está oculto de las miradas indiscretas, mientras que enmascara su ubicación física y que le da acceso sin restricciones a cualquier sitio web o servicio web, no importa donde se encuentre.

5.1 Definición del Problema:

¿Como contribuir a la seguridad de red, datos e información en la UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, provocado por la falta de uso de alternativas tecnológicas en seguridad de red y datos por parte de los administrativos de la unidad?

6. OBJETIVO(S)

6.1 Objetivo General

Implementar tecnología actual de seguridad de red, datos e información en la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, en base al análisis e implementación de una VPN con túneles de certificados de autenticación, que se constituyan como una herramienta de seguridad para el mejoramiento del servicio.

6.2 Objetivos Específicos

- Analizar la fundamentación teórica relacionados con el tema de la investigación, para orientar el uso eficiente de la información y materiales.
- Recopilar información de la UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, que permita visualizar los estándares y plataformas existentes en la unidad.
- Implementar equipo tecnológico que permita mejorar la seguridad de red y datos e información utilizando una VPN con túneles de certificados de autenticación.

7. OBJETO DE ESTUDIO Y CAMPO DE ACCIÓN

En la transferencia de datos e información existen diferentes tipos de problemas como son su libertad y la privacidad en línea que se ve amenazada. Los gobiernos y los proveedores de Internet son los que manejan la red y quieren controlar lo que puede y no se puede ver, existe también incluso el tipo de aspecto sombrío al acecho alrededor de nosotros, provocando que la red de diferentes sitios de navegación se tornen altamente inseguras, por lo que se pretende realizar un análisis de seguridad en redes, Siendo el campo de acción la creación de una red privada virtual VPN con túneles de certificados de autenticación.

8. JUSTIFICACIÓN

En Ecuador actualmente es notable la demanda existe de la creación de nuevas instituciones sean estas públicas o privadas creando consigo la utilización de nuevas redes priorizando la comunicación total y parcial entre los mismos, todos con el único propósito de tener la información rápida y segura, por ende cada una de estas instituciones invierten principalmente en equipos tecnológicos que permiten el trasporte de datos e información y así aprovechar esta herramienta que permite el desarrollo de los mismos.

En el cantón Latacunga provincia de Cotopaxi se ha evidenciado la falta de uso de las tecnologías de red acordes a la actualidad ya que al no existir seguridad al momento de recibir y enviar paquetes de datos, ya que en su mayoría las empresas no conocen de la las VPN Red Privada Virtual , algunos de ellos ya lo ha implementado ya que sus beneficios son varios y mientras que en otras empresas lo que ha impedido por falta de conocimiento en la adquisición de equipo tecnológico acordes a las necesidades para realizar mejoras en base a la seguridad informática en cada una de sus dependencias ya que es uno primordial contar es con una implementación acorde a sus necesidades de cada organización.

En la actualidad el desarrollo y aplicación de nuevas y mejores tecnologías ha hecho que muchas empresas, cooperativas financieras, bancos, compañías instituciones públicas y privadas, acojan favorablemente tecnologías de redes informáticas que han marcado una nueva tendencia a la hora de mejorar, ahorrar tiempo y ampliar sus servicios, con el único afán de conectarse entre sí enviando y recibiendo datos e información segura, veraz y oportuna únicas de cada institución, por ende en la UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, no está al margen de utilizar equipos tecnológicos, sin embargo se ha podido identificar que en la UNIDAD DE ADMISION Y NIVELACION existe un número significativo de usuarios que hacen uso de la red, el cual no garantiza ningún tipo de seguridad al hacer uso de esta herramienta tan útil y necesaria en el proceso de comunicación, dada al número de usuarios que actualmente utilizan la red. Cabe recalcar que al hacer uso de esta herramienta se daría un mejor uso a la transferencia de datos puesto que nos brindara mayor seguridad al momento de navegar en la red, por ende se ha tomado muy en cuenta los avances

tecnológicos en la web por esta razón muy pronto todas las empresas y compañías estarán dispuestas utilizarlas ya que presenta una gran ayuda en el ámbito de seguridad principalmente.

Después de lo expuesto anteriormente se ha decidido implementar una red virtual VPN con túneles de autenticación, donde generará mayores resultados en el transporte seguro de datos, mejorando la comunicación de punto a punto en el tráfico de red de distribución o encaminamiento de paquetes fiables y seguros, y a su vez al momento de mejorar la seguridad en la red en base a sus capacidades y disponibilidad de realizar actividades informáticas dentro del UNIDAD DE ADMISION Y NEVELACION.

Al contar con la información bibliográfica suficiente la cual es necesaria para tener los conocimientos claros, normas y de su modo de uso, esto permitirá que en la Universidad Técnica de Cotopaxi cumpla con estándares de calidad para el mejoramiento de la institución dando un claro ejemplo de desarrollo y crecimiento académico, de este modo se puede beneficiar al engrandecimiento de la Universidad con el uso de estas nuevas herramientas de red que servirán para el mejoramiento de las políticas de seguridad de datos.

El financiamiento de esta investigación y posterior generación de la aplicación correrá por cuenta propia de los investigadores pero se contara con el auspicio de la Universidad Técnica de Cotopaxi quien permitirá la implementación y pruebas.

Mediante el desarrollo de este proyecto se beneficiara directamente a la UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, debido a que se implementará sistemas de seguridad de navegación de red y para salvaguardar datos e información relevantes propios de la unidad.

En este ámbito investigativo se contará con la participación del Ing. Segundo Corrales quien será el técnico en el área de redes de internet quien nos guiara con sus conocimientos en el tema de investigación que se pretende realizar con este proyecto para garantizar que se lo realice de manera adecuada y cumpliéndola satisfactoriamente.

9. MARCO TEÓRICO

9.1 Antecedentes

Red de Computadoras

Stallings , (2006) menciona que "una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios (p.25).

9.2 Redes Informáticas

Como en todo proceso de comunicación se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones. Un ejemplo es Internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectadas básicamente para compartir información y recursos.

Stallings , (2006) menciona que "la estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI" (p. 25).

Este último, estructura cada red en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

9.3 Componentes Básicos de las Redes

Stallings (2006) menciona que "para poder formar una red se requieren elementos: hardware, software y protocolos. Los elementos físicos se clasifican en dos grandes grupos: dispositivos de usuario final (hosts) y dispositivos de red. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación" (p.27).

El fin de una red es la de interconectar los componentes hardware de una red, y por tanto, principalmente, las computadoras individuales, también denominados hosts, a los equipos que ponen los servicios en la red.

9.4 Software

Salmeron (2007) menciona que "el software de una computadora es un conjunto de instrucciones de programas detalladas que controlan y coordinan los componentes hardware de una computadora y controlan las operaciones de un sistema informático" (p. 36).

El auge de las computadoras del siglo pasado y en el actual siglo XXI, se debe esencialmente al desarrollo de sucesivas generaciones de software potentes y cada vez más amistosas ("fáciles de usar").

Sistema operativo de red: permite la interconexión de ordenadores para poder acceder a los servicios y recursos. Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red. En muchos casos el sistema operativo de red es parte del sistema operativo de los servidores y de los clientes.

Software de aplicación: en última instancia, todos los elementos se utilizan para que el usuario de cada estación, pueda utilizar sus programas y archivos específicos. Este software puede ser tan amplio como se necesite ya que se puede incluir procesadores de texto, paquetes integrados, sistemas administrativos de contabilidad y áreas afines, sistemas especializados, correos electrónicos, etc. El software adecuado en el sistema operativo de

red elegido y con los protocolos necesarios permite crear servidores para aquellos servicios que se necesiten.

9.5 Hardware

Según Salmeron (2007) indica que "hardware es el substrato físico en el cual existe el software" (p.45) El hardware abarca todas las piezas físicas de un ordenador (disco duro, placa base, memoria, tarjeta aceleradora o de vídeo, salida de audio, lectora de cd, microprocesadores, salida de vídeo, puertos USB entre otras).

Para lograr el enlace entre las computadoras y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarrojos o radiofrecuencias para redes inalámbricas), es necesaria la intervención de una tarjeta de red, con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras computadoras, empleando un protocolo para su comunicación y convirtiendo a esos datos a un formato que pueda ser transmitido por el medio (bits, ceros y unos). Cabe señalar que a cada tarjeta de red le es asignado un identificador único por su fabricante, conocido como dirección MAC (Media Access Control), que consta de 48 bits (6 bytes). Dicho identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuado.

9.6 Servidores

Morales (2010) Indica que "servidores son los equipos que ponen a disposición de los clientes los distintos servicios. En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos" (p. 48).

Los Servidores almacenan información en forma de páginas web y a través del protocolo HTTP lo entregan a petición de los clientes (navegadores web) en formato HTML.

9.7 MODELO OSI

El modelo OSI (Open Systems Interconnection) fue creado por la ISO y se encarga de la conexión entre sistemas abiertos, esto es, sistemas abiertos a la comunicación con otros sistemas. Los principios en los que basó su creación eran: una mayor definición de las funciones de cada capa, evitar agrupar funciones diferentes en la misma capa y una mayor simplificación en el funcionamiento del modelo en general.

Se trata de una normativa estandarizada útil debido a la existencia de muchas tecnologías, fabricantes y compañías dentro del mundo de las comunicaciones, y al estar en continua expansión, se tuvo que crear un método para que todos pudieran entenderse de algún modo, incluso cuando las tecnologías no coincidieran. De este modo, no importa la localización geográfica o el lenguaje utilizado. Todo el mundo debe atenerse a unas normas mínimas para poder comunicarse entre sí. Esto es sobre todo importante cuando hablamos de la red de redes, es decir, Internet.

Este modelo divide las funciones de red en siete capas diferenciadas:

Tabla 1: REPRECENTACION DE CAPAS MODELO OSI

	CAPA	FUNCION	PROTOCOLOS
7	Aplicación	Servicios para el usuario como e-mail, servicios de archivos e impresión, emulación de terminal, loguin, etc. Solamente las aplicaciones de PC que trabajen en red encuadra en la capa Aplicación.	DNS, FTP, HTTP, IMAP, IRC, NFS, NTP, POP3, SMTP, SSH, Telnet
6	Presentación	Frecuentemente forma parte del sistema operativo y se encarga de dar formato los datos.	XDR, ASN.1, SMB, AFP
5	Sesión	Conexión y mantenimiento del enlace	TLS, SSH, RPC, NetBIOS
4	Transporte	Realiza el control de extremo a extremo de la comunicación, proporcionando control de flujo y control de errores. Esta capa es asociada frecuentemente con el concepto de confiabilidad.	TCP, UDP, RTP, SCTP, SPX
3	Red	Proporciona la posibilidad de rutear la información agrupada en paquetes.	IP, ICMP, IGMP, X.25, ARP, RARP, BGP, OSPF, RIP
2	Enlace	Organiza los bits en grupos lógicos denominado tramas o frames. Proporciona además control de flujo y control de errores.	Ethernet, Token Ring, PPP, Frame Relay, ATM, FDDI
1	Físico	Define las reglas para transmitir el flujo de bits por el medio físico	cable, radio, fibra óptica

Realizado por: Investigador

9.8 MODELO TCP/IP

Este modelo es el implantado actualmente a nivel mundial: fue utilizado primeramente en ARPANET y es utilizado actualmente a nivel global en Internet y redes locales. Su nombre deriva de la unión de los nombres de los dos principales protocolos que lo conforman: TCP en la capa de transporte e IP en la capa de red.

Las capas están jerarquizadas. Cada capa se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones son variables con cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que esos servicios se llevan a cabo. De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados.

9.8.1 Capas de Red

Capa 4 o capa de aplicación: aplicación, asimilable a las capas: 5 (sesión), 6 (presentación) y 7 (aplicación), del modelo OSI. La capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI. Crearon una capa de aplicación que maneja aspectos de representación, codificación y control de diálogo.

Capa 3 o capa de transporte: transporte, asimilable a la capa 4 (transporte) del modelo OSI.

Capa 2 o capa de internet: Internet, asimilable a la capa 3 (red) del modelo OSI.

Capa 1 o capa de acceso al medio: acceso al medio, asimilable a la capa 2 (enlace de datos) y a la capa 1 (física) del modelo OSI.

9.9 CLASIFICACIÓN DE LAS REDES

Una red puede recibir distintos calificativos de clasificación en base a distintas taxonomías: alcance, tipo de conexión, tecnología, etc.

9.9.1 Por Alcance

Red de área personal

Red inalámbrica de área personal

Red de área local

Red de área local inalámbrica .

Red de área de campus

Red de área metropolitana

Red de área amplia Red de área de almacenamiento

Red de área local virtual

9.9.2 Por Relación Funcional

Cliente-servidor es la arquitectura que consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.

Peer-to-peer, o red entre iguales, es aquella red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

9.9.3 Por Tecnología

Red punto a punto (point to point, PtP) es aquella en la que existe multitud de conexiones entre parejas individuales de máquinas. Este tipo de red requiere, en algunos casos, máquinas intermedias que establezcan rutas para que puedan transmitirse paquetes de datos. El medio electrónico habitual para la interconexión es el conmutador, o switch.

Red de Difusión (broadcast) se caracteriza por transmitir datos por un sólo canal de comunicación que comparten todas las máquinas de la red. En este caso, el paquete enviado es recibido por todas las máquinas de la red pero únicamente la destinataria puede procesarlo. Los equipos unidos por un concentrador (hub), forman redes de este tipo.

Red multipunto, dispone de una línea o medio de comunicación cuyo uso está compartido por todas las terminales en la red. La información fluye de forma bidireccional. Los terminales pueden estar separados geográficamente.

9.9.4 Por Topología Física

Red en bus (bus o "conductor común") o Red lineal (line): se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos.

Red en anillo(ring) o Red circular: cada estación está conectada a la siguiente y la última está conectada a la primera.

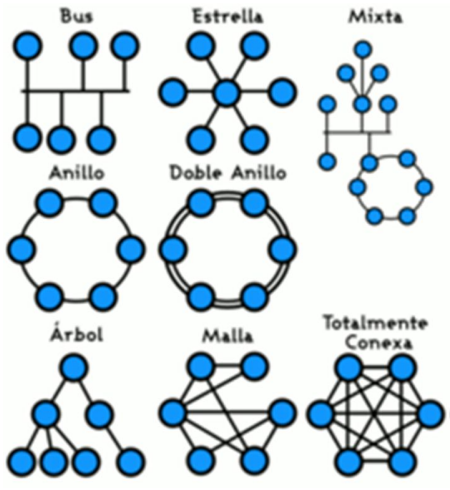
Red en estrella (star): las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.

Red en malla (mesh): cada nodo está conectado a todos los otros.

Red en árbol (tree) o Red jerárquica: 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 salvo en que no tiene un nodo central.

Red híbrida o Red mixta: se da cualquier combinación de las anteriores. Por ejemplo, circular de estrella, bus de estrella, etc.

GRAFICO 1: MODELO TOPOLOGIA FISICA



Fuente: https://es.wikipedia.org/wiki/Red_de_computadoras#/media/File:Topolog%C3%ADa_de_red.png

9.9.5 Por Grado de Autentificación

Red privada: Es una red que solo puede ser usada por algunas personas y que está configurada con clave de acceso personal.

Calero , Huidrobo, & Blanco (2006) destancan que "red privada se entiende aquella que si bien puede hacerse uso de ciertos elementos proporcionados por los operadores la mayor parte de sus elementos son privados y sobre todo su gestión y control es realizado por el propio usuario, aunque pueden ser personas subcontratadas" (p.14).

Red de acceso público: 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.

9.9.6 Por Grado de Difusión

- Una intranet
- La Internet

9.9.7 Por Servicio o Función

Red comercial proporciona soporte e información para una empresa u organización con ánimo de lucro.

Red educativa proporciona soporte e información para una organización educativa dentro del ámbito del aprendizaje.

Red para el proceso de datos proporciona una interfaz para intercomunicar equipos que vayan a realizar una función de cómputo conjunta.

9.10 PROTOCOLOS DE REDES

PROTOCOLO DE RED

Stallings (2006) expresa que "el concepto de protocolo de red se utiliza en el contexto de la informática para nombrar a las normativas y los criterios que fijan cómo deben comunicarse los diversos componentes de un cierto sistema de interconexión. Esto quiere decir que, a través de este protocolo, los dispositivos que se conectan en red pueden intercambiar datos" (p. 137).

Existen diversos protocolos, estándares y modelos que determinan el funcionamiento general de las redes. Destacan el modelo OSI y el TCP/IP. Cada modelo estructura el funcionamiento de una red de manera distinta. El modelo OSI cuenta con siete capas muy definidas y con funciones diferenciadas y el TCP/IP con cuatro capas diferenciadas pero que combinan las funciones existentes en las siete capas del modelo OSI.

9.10.1 Http

El Protocolo de Transferencia de Hipertexto se usa en todas las transacciones que tienen lugar en Internet, ya que cuenta con la definición de la semántica y la sintaxis que deben usar los servidores, los proxies y los clientes (todos componentes de la arquitectura web) para entablar una comunicación entre ellos.

9.10.2 Ftp

El Protocolo de Transferencia de Archivos, por su parte, se utiliza cuando se desea enviar y recibir archivos de un sistema a otro, siempre que ambos se basen en la arquitectura cliente-servidor y que se encuentren conectados a una red que cumpla con el TCP, explicado en la definición de protocolo de comunicación..

9.10.3 Smtp

Con un nombre menos conocido que los dos anteriores, el Protocolo para transferencia simple de correo es utilizado una cantidad incalculable de veces al día por usuarios de todo el mundo, ya que da forma al intercambio de mensajes de correo electrónico (también conocido como e-mail o email) entre una amplia gama de dispositivos, como ser los

teléfonos móviles, las tabletas y los ordenadores. Se trata de un estándar oficial cuya operación se encuentra en manos de los proveedores de servicios de email.

9.10.4 Pop

El Protocolo de Oficina de Correo o de Oficina Postal brinda a los usuarios la posibilidad de recibir y almacenar el correo electrónico en un equipo local. En la actualidad se prefiere el uso de POP3, la versión más reciente, dado que las primeras dos se consideran obsoletas.

9.11 EL PROTOCOLO IPV4

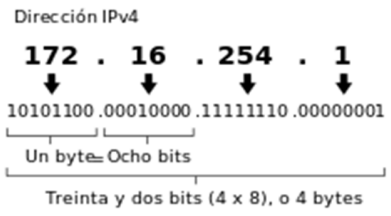
IPv4

El Protocolo de Internet versión 4, es la cuarta versión del Internet Protocol (IP), y la primera en ser implementada a gran escala. Definida en el RFC 791. IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4 294 967 296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LAN).Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos (ver abajo), ya hace varios años se vio que escaseaban las direcciones IPv4.

Las direcciones disponibles en la reserva global de IANA pertenecientes al protocolo IPv4 se agotaron oficialmente el lunes 31 de enero de 2011. Los Registros de Internet deben, desde ahora, manejarse con sus propias reservas, que se estima, alcanzaran hasta el 2020.

9.11.1 Notación IPv4

GRAFICO 2: DIRECCIONAMIENTO IPV4



Fuente: https://es.wikipedia.org/wiki/IPv4

Detalle de una dirección IPv4, expresada en notación decimal separada por puntos.

Las direcciones IPv4 se pueden escribir de forma que expresen un entero de 32 bits, aunque normalmente se escriben con decimales separados por puntos. La siguiente tabla muestra varias formas de representación de direcciones IPv4:

Tabla 2: DETALLES DE DIRECCIONAMIENTOS IPV4

Notación	Valor	Conversión desde decimal separado por puntos
Decimal separada por puntos	192.0.2.235	-
Hexadecimal separada por puntos	0xC0.0x00.0x02.0xEB	Cada octeto se convierte individualmente a la forma hexadecimal
Octal separada por puntos	0301.1680.0002.0353	Cada octeto se convierte de individualmente en octal
Hexadecimal	0xC00002EB	Concatenación de octetos de la forma hexadecimal separada por puntos
Decimal	3221226219	El número hexadecimal expresado en decimal
Octal	030000001353	El número hexadecimal expresado en octal

Realizado por: Investigador

9.11.2 Desperdicio de direcciones

El desperdicio de direcciones IPv4 se debe a varios factores.

Uno de los principales es que inicialmente no se consideró el enorme crecimiento que iba a tener Internet; se asignaron bloques de direcciones grandes (de 16 271 millones de direcciones) a países, e incluso a empresas.

Otro motivo de desperdicio es que en la mayoría de las redes, exceptuando las más pequeñas, resulta conveniente dividir la red en subredes. Dentro de cada subred, la primera y la última dirección no son utilizables; de todos modos no siempre se utilizan todas las direcciones restantes. Por ejemplo, si en una subred se quieren acomodar 80 *hosts*, se necesita una subred de 128 direcciones (se tiene que redondear a la siguiente potencia de base2); en este ejemplo, las 48 direcciones restantes ya no se utilizan.

9.11.3 Análisis Comparativo del protocolo IPv4 vs IPv6

Tabla 3: ANALISIS COMPARATIVO DEL PROTOCOLO IPV4 VS IPV6

Protocolo versión:	CONCEPTO	ESTRUCTURA	VENTAJAS	DESVENTAJAS	DIRECCIONES ADMITIDAS
Ip v 4	Es la cuarta versión del protocolo Internet Protocol (IP), y la primera en ser implementada a gran escala.	Está compuesta de 4 grupos de 8 bits (32 bits), cada uno 8x4=32; se puede decir que 4 grupos decimales donde cada uno está formado por 3 dígitos.	✓ Direcciones de 32 bits. ✓ Formato de cabecera más grande. ✓ Configuración manual. ✓ Direcciones Broadcast. ✓ Contiene enlaces con fibra óptica.	✓ Elevada demanda de direcciones IP. ✓ No posee seguridad. ✓ Limita el crecimiento del internet.	Soporta 4.294.967.296 (232) direcciones de red diferentes
Ip v 6	Es la versión 6 del protocolo de Internet (Internet protocol) un estándar en desarrollo del nivel de red encargado de dirigir y encaminar los paquetes a través de una red.	Está compuesto de ocho grupos de cuatro caracteres cada uno, compuestas por un prefijo de 64 bits y un identificador de interfaz también de 64 bits. Además se complica un poco la cosa ya que los grupos en vez de expresarse en notación decimal lo harán en hexadecimal y la separación no se hará por un punto si no por dos puntos. Por ejemplo: 2001:DB8:0:2F3B:2AA:FF:FE28:9C5A	✓ Direcciones de 128 bits. ✓ Formato de cabecera más sencillo. ✓ Configuración automática. ✓ Direcciones multicast. ✓ Seguridad incorporada (encriptación de la información).	✓ La necesidad de extender un soporte permanente para IPv6 a través de todo Internet y de los dispositivos conectados a ella. ✓ Para estar enlazada al universo IPv6 durante la fase de transición, todavía se necesita una dirección IPv4 o algún tipo de NAT	Soporta 340282366920938463374607431768211456 (2 elevado a 128) de direcciones

Fuente: https://es.scribd.com/doc/95966649/Cuadro-comparativo-ipv4-ipv6-docx

9.12 PROTOCOLO IPv6

IPv6

Martinez (2009) menciona que "el Internet Protocolo versión 6 (IPv6) es una versión del protocolo Internet Protocol (IP), definida y diseñada para reemplazar a Internet Protocolo versión 4, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet" (p. 48).

El nuevo protocolo IPv6 dispone de 340 billones de billones de billones (sextillones) de direcciones, lo que hace que la cantidad de direcciones de IPv4 parezca insignificante. Con este mayor espacio de direcciones, IPv6 ofrece una variedad de ventajas en términos de estabilidad, flexibilidad y simplicidad en la administración de las redes. También es probable que la era IPv6 genere una nueva ola de innovación en las aplicaciones y las ofertas de servicio ya que, termina con la necesidad de direcciones compartidas.

IPv4 posibilita 4 294 967 296 (232) direcciones de host diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada dispositivo, teléfono, PDA, Tablet, etc. En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 o 340 sextillones de direcciones) —cerca de 6,7 × 1017 (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra.

La nueva estructura de la cabecera del protocolo IPv6 se caracteriza por tener:

- Direcciones de 128 bits.
- Campos de longitud fija.

Fue creada prácticamente para mejorar la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad.

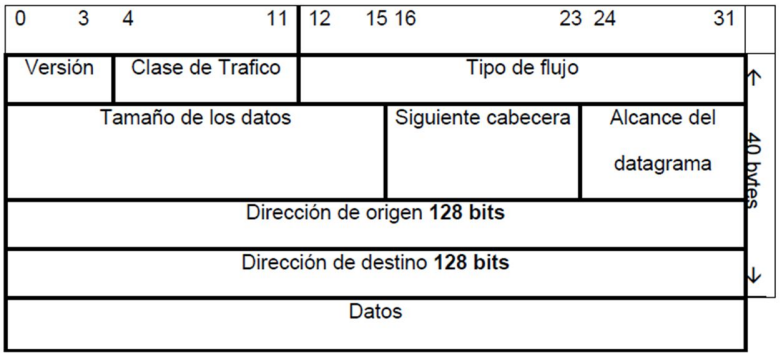
9.12.1 Características Principales

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza el procesamiento por parte del router.
- Posibilidad de empaquetar datos de más de 65.355 bytes.
- Seguridad en el núcleo del protocolo (IPsec).
- Capacidad de etiquetas de flujo donde prioriza la calidad de servicio en tiempo real. Por ejemplo video conferencia.
- Autoconfiguración: la autoconfiguración de direcciones es más simple en direcciones Aggregatable Global Unicast, facilitando el cambio de proveedor de servicios.
- Movilidad, posibilita que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- Ruteo más eficiente.
- Calidad de servicio (QoS) y clase de servicio (CoS).
- Capacidades de autenticación y privacidad.

9.12.2 Arquitectura IPv6

La nueva cabecera del protocolo IPv6 es una evolución de la cabecera IPv4 no se han introducido grandes cambios a la estructura misma, solo se ha mejorado y optimizado. Se han suprimido algunos campos obsoletos y se han ampliado algunas características para hacer frente a las nuevas necesidades de los usuarios como son las comunicaciones en tiempo real y dando prioridad a la seguridad.

GRAFICO 3: ESTRUCTURA DE UN DATAGRAMA



Fuente: http://arquitectura89.webnode.es/ipv6/

Versión (4 bits): Es el primer campo del data grama. Permite diferenciar que versión de datagrama se recibe IPv4 o IPv6.

Clase de Trafico (8 bits): Este campo asigna la prioridad del datagrama, una de las nuevas aportaciones para conseguir controlar el flujo de la información.

Tipo de Flujo (16 bits): Permite especificar que una serie de datagramas deben recibir el mismo trato.

Tamaño de Datos (16 bits): Al igual que en IPv4 especifica el tamaño que tendrán los datos, lo que permite un tamaño máximo de 64K en principio.

Siguiente Cabecera (8 bits): Indica el router que tras el datagrama viene algún tipo de extensión.

En IPv6 se definen una serie de cabeceras de extensión que se sitúan fuera del datagrama básico permitiendo al usuario personalizar el tipo de datagrama. Podemos tener varios extensiones de cabecera tan solo indicando en el campo de siguiente cabecera de cada una el tipo de cabecera que vendrá a continuación.

Tabla 4: ALCANCE DE UN DATAGRAMA

Valor decimal	Abreviatura	Descripción
0	HBH	Nodo por Nodo
4	IP	IP en IP (encapsulación en IPv4)
5	ST	Stream
43	RH	Cabecera de Encaminamiento (Routing Header)
44	FH	Cabecera de Fragmentación (Fragment Header)
51	AH	Cabecera de Autenticación (Authentication Header)
52	ESP	Encrypted Security Payload
59	NULL	Ninguna cabecera siguiente
60	DO	Destination Options Header
194	JBGR	Jumbogram

Fuente: https://es.wikipedia.org/wiki/IPv6

Alcance de Datagrama (8 bits): Indica el número de máximo de cabeceras de routers que puede atravesar un datagrama hasta llegar a su destino. Este campo es equivalente al tiempo de vida TTL de la versión 4.

9.12.3 Cabeceras de Extensión del Protocolo IPv6

Son encabezados opcionales, enlazados uno después de otro, que van después del encabezado básico de IPv6. Un paquete IPv6 puede llevar uno o múltiples extensiones de encabezados o inclusive no llevar ninguno. A continuación se definen las Extensiones de Encabezados:

Cabecera de Opciones Salto-por-Salto (protocolo 0). Éste es usado para paquetes Jumbograma y la Alerta de Ruteador.

Cabecera de Opciones de Destino (protocolo 60). Lleva información opcional que está específicamente dirigida a la dirección de destino del paquete.

Cabecera de Enrutamiento (protocolo 43). Puede ser usado por un nodo fuente IPv6 para forzar a que un paquete atraviese ruteadores específicos en su trayectoria al destino.

Cabecera de Fragmentación (protocolo 44). En IPv6 se recomienda que el mecanismo PMTUD esté en todos los nodos. Si un nodo no soporta PMTUD y debe enviar un paquete más grande que el MTU se utiliza el Encabezado de Fragmentación.

Cabecera o de Autenticación (protocolo 51). Este se utiliza en IPSec para proveer autenticación, integridad de datos y protección ante una repetición, e incluye también protección a algunos campos del encabezado básico de IPv6.

Cabecera de Carga de Seguridad Encapsulada (protocolo 50). Es usado en IPSec para proveer autenticación, integridad de datos, protección ante repetición y confidencialidad del paquete IPv6.

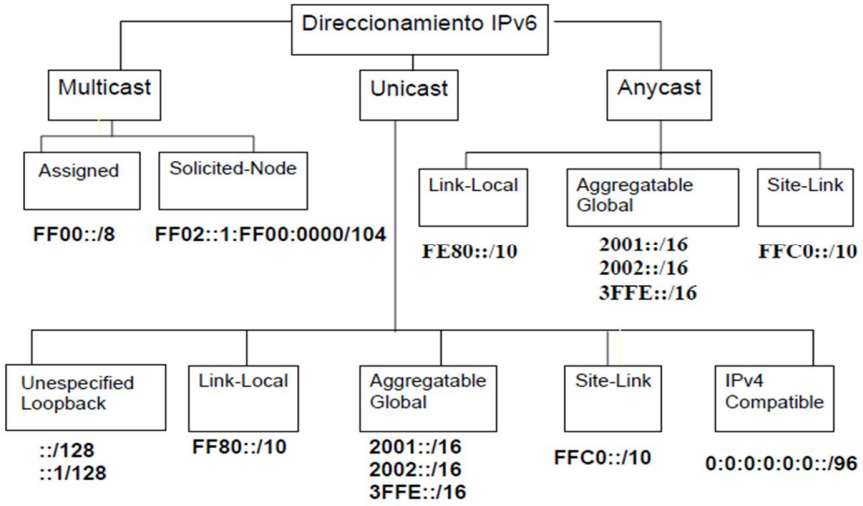
9.12.4 Direccionamiento IPv6

Las direcciones IPv6 son identificadores de interfaces o conjuntos de interfaces de 128 bits por lo que se tiene tres tipos de direcciones en función al tipo de destino.

Los cambios introducidos por IPv6 no sólo son en cantidad de direcciones sino que incluyen nuevos tipos, representaciones y sintaxis.

- **Unicast:** este grupo de direcciones se caracteriza por identificar un único nodo de manera que paquete enviado a una dirección unicast es entregado a la interfase identificada por esa dirección.
- **Multicast:** Se utiliza para identificar un paquete enviado a una dirección multicast es procesado por todos los miembros del grupo multicast.
- **Anycast:** Se asigna a múltiples interfases (usualmente en múltiples nodos). Un paquete enviado a una dirección anycast es entregado a una de estas interfases, usualmente la más cercana.

GRAFICO 4: TIPO DE DIRECCIONES EN FUNCION DEL TIPO DE DESTINO



Fuente: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/

También se tienen tres tipos de direcciones en función del alcance:

- Enlace Local: Se utiliza en un enlace sencillo y para mecanismos de autoconfiguración, descubrimiento de vecinos y en redes sin ruteadores.
- Sitio Local: Contiene información de subred dentro de la dirección. Son enrutadas dentro de un sitio, pero los ruteadores no deben enviarlas fuera de éste. Además es utilizada sin un prefijo global.
- Agregable Global: Son las direcciones IPv6 utilizadas para el tráfico de IPv6.

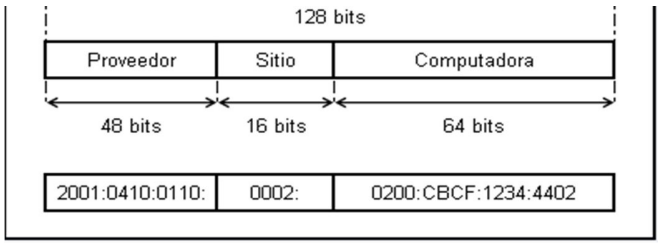
Consta de tres partes:

GRAFICO 5: CLASIFICACION DE DIRECCIONES SEGUN ENLACE

Fuente: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/

La siguiente figura muestra como ejemplo al prefijo 2001:0410:0110::/48 que es asignado por un proveedor a una organización. Dentro de la organización el prefijo 2001:0410:0110:0002::/64 es habilitado en una subred. Finalmente, un nodo en esta subred tiene la dirección 2001:0410:0110:0002:0200:CBCF:1234:4402.

GRAFICO 6: NOTACION DEL PROTOCOLO IPV6



Fuente: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/

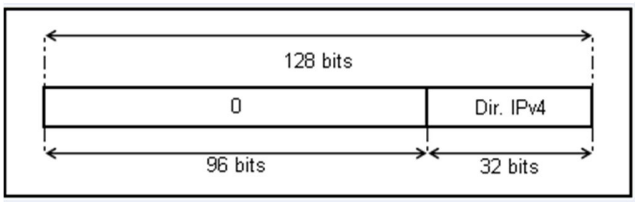
Loopback. En IPv6 se representa en el formato preferido por el prefijo 0000:0000:0000:0000:0000:0000:0000:0001 y en el formato comprimido por ::1.

Sin-Especificar. Indica la ausencia de una dirección y es usada para propósitos especiales. Es representada en el formato preferido con el prefijo 0000:0000:0000:0000:0000:0000:0000:0000 y con :: en el formato comprimido.

Compatible con IPv4. Es utilizada por los mecanismos de transición en computadoras y ruteadores para crear automáticamente túneles IPv4. De esa forma se entregan paquetes IPv6 sobre redes IPv4

.

GRAFICO 7: DIFERENCIAS EN ALCANCE IPV4 E IPV6



Fuente: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/

Asignada Multicast. Está definida para la operación del protocolo IPv6. En la siguiente tabla se presentan las Direcciones Asignadas Multicast y su área de funcionamiento.

Tabla 5: DIRECCIONAMIENTO MULTICAST

Dirección Multicast	Área de Funcionamiento	Significado	Descripción
FF01::1	Nodo	Todos los nodos	Todos los nodos en la interfase local
FF01::2	Nodo	Todos los enrutadores	Todos los enrutadores en la interfase local
FF02::1	Enlace Local	Todos los nodos	Todos los nodos en el enlace local
FF02::2	Enlace Local	Todos los enrutadores	Todos los enrutadores en el enlace local
FF05::2	Sitio	Todos los enrutadores	Todos los enrutadores en un sitio

Fuente: https://es.wikipedia.org/wiki/IPv6#Direccionamiento_IPv6

9.12.5 Notación de Direcciones

En la arquitectura del Direccionamiento del Protocolo de Internet versión 6 existen tres formatos para representar direcciones IPv6.

9.12.5.1 El formato preferido

Este representa los 32 caracteres hexadecimales que forman la dirección. Es el más cercano a la forma en que la computadora procesa la dirección.

GRAFICO 8: NOTACION DE DIRECCION PREFERIDA

Ejemplos de direcciones IPv6 en formato preferido
0000:0000:0000:0000:0000:0000:0000:0000
0000:0000:0000:0000:0000:0000:0000:0001
2001:0410:0000:1234:FB00:1400:5000:45FF
3FFE:0B00:0C18:0001:0000:1234:AB34:0002
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Fuente: https://es.wikipedia.org/wiki/IPv6#Direccionamiento_IPv6

9.12.5.2 El formato comprimido

Mediante una representación comprimida que se utiliza para simplificar la escritura de la dirección.

Campos sucesivos de ceros:

GRAFICO 9: NOTACION FORMATO COMPRIMIDO

Formato Preferido	Formato comprimido utilizando ::
0000:0000:0000:0000:0000:0000:0000:0000	::
0000:0000:0000:0000:0000:0000:0000:0001	::0001
2001:0410**:0000:**1234:FB00:1400:5000:45FF	2001:0410::1234:FB00:1400:5000:45FF
3FFE:0B00:0C18:0001**:0000:**1234:AB34:0002	3FFE:0B00:0C18:0001::1234:AB34:0002
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF	FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Fuente: https://es.wikipedia.org/wiki/IPv6#Direccionamiento_IPv6

La dirección FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF es una dirección que no puede ser comprimida.

9.12.5.3 Campos con ceros al inicio

El segundo método para comprimir direcciones se aplica a cada uno de los campos hexadecimales de 16 bits que tienen uno o más ceros al inicio.

GRAFICO 10: NOTACION CEROS AL INICIO

Formato Preferido	Formato comprimido
0000:0000:0000:0000:0000:0000:206.123.31.2	0:0:0:0:0:0:206.123.31.2 o ::206.123.31.2
0000:0000:0000:0000:0000:0000:ce7b:1f01	0:0:0:0:0:0:ce7b:1f01 o ::ce7b:1f01
0000:0000:0000:0000:0000:FFFF:206.123.31.2	0:0:0:0:0:FFF:206.123.31.2 o ::FFFF:206.123.31.2
0000:0000:0000:0000:0000:FFFF:ce7b:1f01	0:0:0:0:0:FFFF:ce7b:1f01 o ::FFFF:ce7b:1f01

Fuente: https://es.wikipedia.org/wiki/IPv6#Direccionamiento_IPv6

9.12.6 Mecanismos de Transición

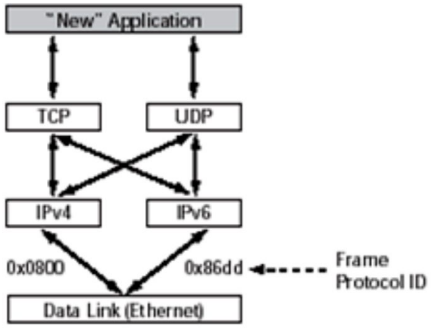
Los mecanismos de transición son un conjunto de mecanismos y de protocolos implementados en hosts y routers, junto con algunas guías operativas de direccionamiento

designadas para hacer la transición de Internet al IPv6 con la menor interrupción posible. En general, los mecanismos de transición pueden clasificarse en tres grupos:

9.12.6.1 Doble pila

Para que un nodo se pueda comunicar tanto con nodos IPv6 como IPv4, la solución más rápida es pensar en la doble pila de protocolos. Teniendo cada nodo una dirección IPv4 e IPv6 enrutable, se conseguirá que se produzca la comunicación.

GRAFICO 11: RE`PRECENTACION DEL MECANISMO DOBLE PILA

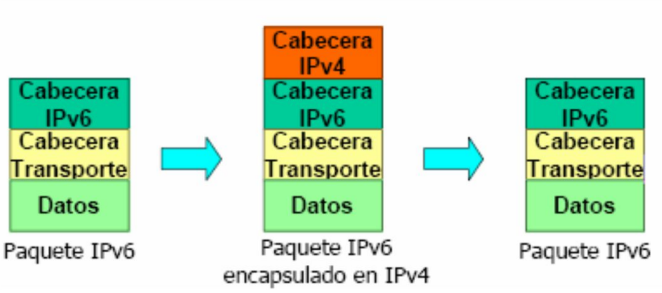


Fuente: https://es.wikipedia.org/wiki/Mecanismos_de_transici%C3%B3n_IPv6

9.12.6.2 Túneles

Los "túneles" permiten conectarse a redes IPv6 "saltando" sobre redes IPv4. Estos túneles trabajan encapsulando los paquetes IPv6 en paquetes IPv4 teniendo como siguiente capa IP el protocolo número 41. Encapsulan un paquete IP dentro de otro, es un mecanismo conocido y se usa en la actualidad sobre todo para crear redes privadas virtuales.

GRAFICO 12: REPRECENTA CION FUNCIONAMIENTO DE LAS CAPAS POR TUNELES



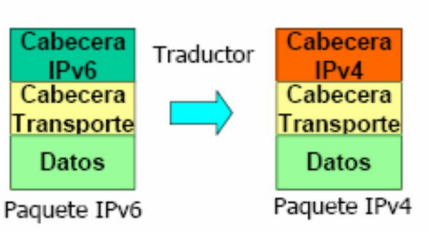
Fuente: https://es.wikipedia.org/wiki/Mecanismos_de_transici%C3%B3n_IPv6

9.12.6.3 Traducción

La "traducción" es necesaria cuando un nodo que únicamente soporta IPv4 intenta comunicar con un nodo que solamente soporta IPv6.

Su funcionamiento se basa en traducir, en un elemento de red los paquetes de un formato a otro.

GRAFICO 13: MECANISMO DE TRADUCCION



Fuente: https://es.wikipedia.org/wiki/Mecanismos_de_transici%C3%B3n_IPv6

9.13 Redes MPLS

Según Minei & Lukey (2010) definen “es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un router” (p.113).

La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la QoS; además, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla.

Su capacidad para dar prioridad a los paquetes que transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP.

9.13.1 Tipos de Redes MPLS

Diaz , Alzorriz, Sancristobal, & Castro (2014) definen que “son infraestructuras especialmente activadas para proporcionar redes privadas virtuales. En este caso la RPV no en un protocolo o protocolos de cifrados para encapsular la comunicación” (p.154).

Existen dos tipos de RPV:

RPVs de nivel 3: en este tipo de redes privadas virtuales el proveedor de servicio participa en el encaminamiento de nivel 3 del cliente. Este tipo de RPVs son especialmente atractivas para clientes que desean que sea el proveedor quien aporte la experiencia técnica para el funcionamiento eficiente de su red privada virtual y son a las que normalmente nos referimos cuando se habla de RPV-MPLS

RPVs a nivel 2: en este caso el proveedor de servicios interconecta las distancias sedes del cliente a través de la tecnología de nivel 2(capa de enlace) como puede ser ATM, Frame Relay o Ethernet. Este tipo de RPVs son especialmente atractivas para aquellos clientes que quieran mantener el control de su propio encaminamiento de nivel 3.

LANs privadas virtuales (VPLS- Virtual Private LAN Service): en este tipo de soluciones el cliente ve la red completa del proveedor de servicio como un gran computador, de esta forma la red de área amplia (WAN) es como una red unificada a la que accede mediante Ethernet.

9.13.2 Arquitectura Mpls

Elementos

LER (Label Edge Router): elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS.

LSR (Label Switching Router): elemento que conmuta etiquetas

LSP (Label Switched Path) o Intercambio de rutas por etiqueta: nombre genérico de un camino, es decir, del túnel MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.

LDP (Label Distribution Protocol): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.

FEC (Forwarding Equivalence Class): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

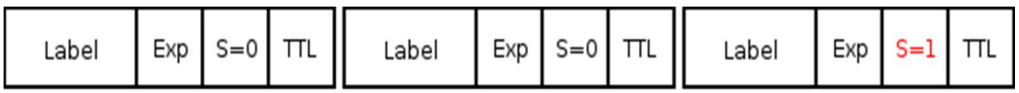
CABECERA MPLS:

GRAFICO 14: CABECERA PRINCIPAL MPLS

Fuente: http://www.rau.edu.uy/ipv6/queesipv6.htm#05

PILA DE ETIQUETAS MPLS

GRAFICO 15: PILA DE ETIQUETAS MPLS



Fuente: http://www.rau.edu.uy/ipv6/queesipv6.htm#05

MPLS funciona anexando un encabezado a cada paquete. Dicho encabezado contiene una o más "etiquetas", y al conjunto de etiquetas se le llama pila o "stack".

9.14 IPSEC

Según Doraswamy & Harkins (2006) definen "es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado" (p. 114).

IPsec (abreviatura de Internet Protocol Security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

Una ventaja importante de IPsec frente a SSL y otros métodos que operan en capas superiores, es que para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

9.14.1 Arquitectura de Seguridad

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección.

IPsec está implementado por un conjunto de protocolos criptográficos para

(1) asegurar el flujo de paquetes

(2) garantizar la autenticación mutua y

(3) establecer parámetros criptográficos.

IPsec toma las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

9.14.2 Propósito de Diseño

IPsec fue proyectado para proporcionar seguridad en modo transporte (extremo a extremo) del tráfico de paquetes, en el que los ordenadores de los extremos finales realizan el

procesado de seguridad, o en modo túnel (puerta a puerta) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red de área local) por un único nodo.

IPsec se introdujo para proporcionar servicios de seguridad tales como:

Cifrar el tráfico (de forma que no pueda ser leído por nadie más que las partes a las que está dirigido.

Validación de integridad (asegurar que el tráfico no ha sido modificado a lo largo de su trayecto.

Autenticar a los extremos (asegurar que el tráfico proviene de un extremo de confianza.

Anti-repetición (proteger contra la repetición de la sesión segura.

9.14.3 Modos

Podemos establecer dos modos básicos de operación de IPsec: modo transporte y modo túnel.

Modo Transporte

En modo transporte, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera. El modo transporte se utiliza para comunicaciones ordenador a ordenador.

Modo Túnel

En el modo túnel, todo el paquete IP es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

9.14.4 Protocolos IPsec

IPsec consta de tres protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6:

Authentication Header (AH): proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.

Encapsulating Security Payload (ESP): proporciona confidencialidad y la opción -altamente recomendable- de autenticación y protección de integridad.

Internet key exchange (IKE): emplea un intercambio secreto de claves para establecer el secreto compartido de la sesión. Se suelen usar sistemas de Criptografía de clave pública o clave pre-compartida.

9.14.5 Estructura IPsec

El protocolo contiene un primer encabezado llamado Cabecera de Autenticación - Autenticación (AH), el cual provee integridad y autenticación del origen y protección contra duplicados.

La Autenticación de Encabezado IPSec protege la integridad de la mayoría de los campos de encabezado de IPv6, excepto a aquellos que cambian sobre los enrutamientos, de la misma forma como lo hace el campo “Límite de Salto” del paquete, adicionalmente el AH autentica el origen por medio de un algoritmo de cifrado.

El segundo encabezado llamado “Encapsulado de Seguridad de Carga Útil” - IPsec (ESP Encapsulating Security Payload), el cual provee confidencialidad, autenticación del nodo origen, integridad interna del paquete y protección contra duplicación.

9.15 RED PRIVADA VIRTUAL VPN

Red privada virtual

Una red privada virtual en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.1 Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

La conexión VPN a través de Internet es técnicamente una unión wide area network (WAN) entre los sitios pero al usuario le parece como si fuera un enlace privado de allí la designación "virtual private network".

GRAFICO 16: PROCESO DEL FUNCIONAMIENTO DE UNA VPN

Fuente: http://computerhoy.com/paso-a-paso/internet/como-conectarte-crear-configurar-tu-propia-red-vpn-7981

9.15.1 Características Básicas de la Seguridad VPN

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación.

Autentificación y autorización: ¿quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

Integridad: de que los datos enviados no han sido alterados. Para ello se utilizan funciones de Hash.

Confidencialidad/Privacidad: dado que solamente puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado.

No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.

Control de acceso: se trata de asegurar que los participantes autenticados tiene acceso únicamente a los datos a los que están autorizados.

Auditoría y registro de actividades: se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.

Calidad del servicio: se trata de asegurar un buen rendimiento, que no haya una degradación poco aceptable en la velocidad de transmisión.

9.15.2 Requisitos Básicos

Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.

Cifrado de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos si son interceptados. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que únicamente pueden ser leídos por el emisor y receptor.

Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

9.15.3 Tipos de VPN

Básicamente existen cuatro arquitecturas de conexión VPN:

VPN Acceso Remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

VPN Punto a Punto

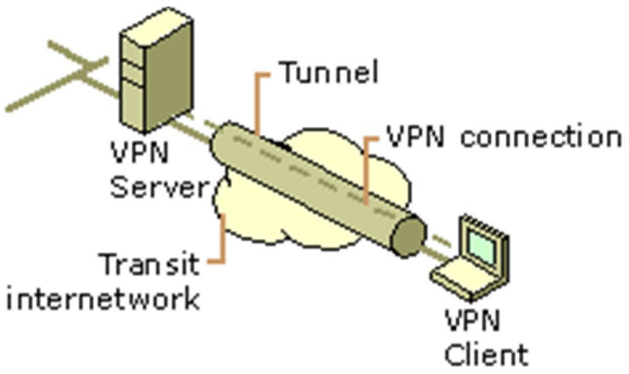
Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales.

Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (unidades de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

GRAFICO 17: MECANISMO DE PROTECCION VPN



Fuente: http://es.ccm.net/contents/258-vpn-redes-privadas-virtuales

9.15.4 VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que solamente el personal de recursos humanos habilitado pueda acceder a la información.

9.15.4.1 Implementaciones

Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software.

Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de inter operatividad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general.

Ventajas

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.

9.15.5 Tipos de conexión

Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentifica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall

Una conexión VPN firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

VPN en entornos móviles

La VPN móvil se establece cuando el punto de terminación de la VPN no está fijo a una única dirección IP, sino que se mueve entre varias redes como pueden ser las redes de datos de operadores móviles o distintos puntos de acceso de una red Wifi.3 Las VPNs móviles se han utilizado en seguridad pública dando acceso a las fuerzas de orden público a aplicaciones críticas tales como bases de datos con datos de identificación de criminales, mientras que la conexión se mueve entre distintas subredes de una red móvil.

Se utilizan para moverse entre redes sin perder la sesión de aplicación o perder la sesión segura en la VPN. En una VPN tradicional no se pueden soportar tales situaciones porque se produce la desconexión de la aplicación, time outs7 o fallos, o incluso causar fallos en el dispositivo.

9.16 OPENVPN

OpenVPN es una solución de conectividad basada en software libre, OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo la licencia GPL, de software libre.

Es un producto de software creado por James Yonan en el año 2001 y que ha estado mejorando desde entonces.

Es una solución multiplataforma que ha simplificado la configuración de VPN's frente a otras soluciones más antiguas y difíciles de configurar como IPsec y haciéndola más accesible para gente inexperta en este tipo de tecnología.

9.16.1 Factores de OPENVPN

La aceleración de los procesos de negocios y su consecuente aumento en la necesidad de intercambio flexible y rápido de información.

Muchas organizaciones tienen varias sucursales en diferentes ubicaciones así como también tele trabajadores remotos desde sus casas, quienes necesitan intercambiar información sin ninguna demora, como si estuvieran físicamente juntos.

La necesidad de las redes de computación de cumplir altos estándares de seguridad que aseguren la autenticidad, integridad y disponibilidad.

9.16.2 Protocolos

- Las soluciones de VPN pueden ser implementadas a diferentes niveles del modelo OSI de red.
- Implementaciones de capa 2 - Enlace
- El encapsulamiento a este nivel ofrece ciertas ventajas ya que permite transferencias sobre protocolos no-IP,
- Implementaciones de capa 3 - Red
- IPsec es la tecnología más aceptada en este punto y fue desarrollada como un estándar de seguridad de Internet en capa 3. IPsec se pude utilizar para encapsular cualquier tráfico de capa 3 pero no el tráfico de capas inferiores, Existen dos métodos principales usados por IPsec:
- Implementaciones de capa 7 - Aplicación
- También es posible establecer túneles en la capa de aplicación y de hecho son ampliamente utilizados El usuario accede a la VPN de la organización a través de un browser iniciando la conexión en un sitio web seguro.
- OpenVPN es una solución para VPN que implementa conexiones de capa 2 o 3, usa los estándares de la industria SSL/TLS para cifrar y combina todas las características mencionadas anteriormente en las otras soluciones VPN.
- Su principal desventaja por el momento es que hay muy pocos fabricantes de hardware que lo integren en sus soluciones. Sin embargo, en sistemas basados en Linux se puede implementar sin problemas mediante software.

9.16.3 Seguridad VPN

Para cifrar datos se usan Passwords o claves de cifrado.

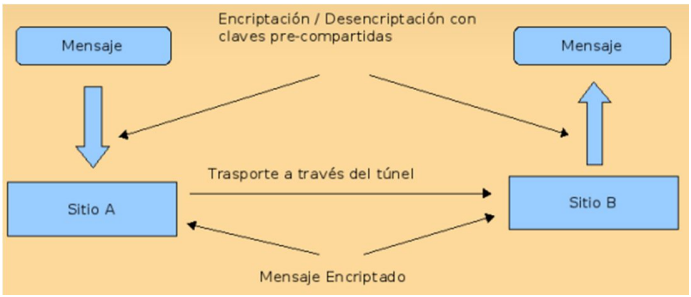
OpenVPN tiene dos modos considerados seguros, uno basado en claves estáticas pre-compartidas y otro en SSL/TLS usando certificados y claves RSA.

Cuando ambos lados usan la misma clave para cifrar y descifrar los datos, estamos usando el mecanismo conocido como "clave simétrica" y dicha clave debe ser instalada en todas las máquinas que tomarán parte en la conexión VPN.

Cifrado simétrico y claves pre-compartidas

Cualquiera que posea la clave podrá descifrar el tráfico, por lo que si un atacante la obtuviese comprometería el tráfico completo de la organización ya que tomaría parte como un integrante más de la VPN.

GRAFICO 18: MECANISMO DE SEGURIDAD DE UNA OPENVPN



Fuente:http://es.ccm.net/contents/258-vpn-redes-privadas-virtuales

Tabla 6: ANALISIS COMPARATIVO ENTRE IPSECVPN Y OPENVPN

IPSEC	OPENVPN
➢ Estándar de la tecnología VPN ➢ Plataformas de hardware (dispositivos, aparatos) ➢ Tecnología conocida y probada ➢ Muchas interfaces gráficas disponibles ➢ Modificación compleja del stack IP ➢ Necesidad de modificaciones críticas al kernel. ➢ Necesidad de permisos de administrador ➢ Diferentes implementaciones de distintos proveedores pueden ser incompatibles entre si ➢ Configuración compleja y tecnología compleja ➢ Curva de aprendizaje muy pronunciada ➢ Necesidad de uso de múltiples puertos y protocolos en el firewall ➢ Problemas con direcciones dinámicas en ambas puntas ➢ Problemas de seguridad de las tecnologías IPsec	➢ No compatible con IPsec ➢ Solo en computadoras, pero en todos los sistemas operativos disponibles, ya comienzan a encontrarse dispositivos que cuentan con OpenVPN ➢ Probada y sigue en crecimiento ➢ Sin interfaces gráficas profesionales, aunque ya existen algunos proyectos prometedores ➢ Tecnología sencilla ➢ Interfaces de red y paquetes estandarizados ➢ Ejecuta en el espacio del usuario y puede ser chroot-ed. ➢ Tecnologías de cifrado estandarizadas ➢ Facilidad, buena estructuración, tecnología modular y facilidad de configuración ➢ Fácil de aprender e implementar ➢ Utiliza sólo un puerto del firewall ➢ Trabaja con servidores de nombres dinámicos como DynDNS o No-IP con reconexiones rápidas y transparentes ➢ SSL/TLS como estándar de criptografía ➢ Control de tráfico (Traffic shaping) ➢ Velocidad (más de 20 Mbps en máquinas de 1Ghz) ➢ Compatibilidad con firewall y proxies ➢ Ningún problema con NAT (ambos lados puede ser redes NATeadas) ➢ Posibilidades para road Warriors

Realizado por: Investigador

9.17 GNU/Linux

Es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux con el sistema operativo GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU,) y otra serie de licencias libres.

Es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo.

9.17.1 Características:

El sistema viene acompañado del código fuente.

A pesar de que "Linux" se denomina en la jerga cotidiana al sistema operativo, este es en realidad solo el Kernel (núcleo) del sistema. La verdadera denominación del sistema operativo es "GNU/Linux" debido a que el resto del sistema se maneja con las herramientas del proyecto GNU y con entornos de escritorio (como GNOME), que también forma parte del proyecto GNU aunque tuvo un origen independiente. Es una distribución, usándose el término sistema operativo en el sentido empleado en el ecosistema Unix, lo que en cualquier caso significa que Linux es solo una pieza más dentro de GNU/Linux. Sin embargo, una parte significativa de la comunidad, así como muchos medios generales y especializados.

9.17.2 Centos 7 Server

Es un sistema robusto que permite a los usuarios optar por tecnología ágil, veras y sobretodo gratuito que permite a muchas personas desarrollarse en varios aspectos de la vida diaria.

Es un sistema operativo de código abierto, basado en la distribución Red Hat Enterprise Linux, operándose de manera similar, y cuyo objetivo es ofrecer al usuario un software de "clase empresarial" gratuito. Se define como robusto, estable y fácil de instalar y utilizar. Desde la versión 5, cada lanzamiento recibe soporte durante diez años, por lo que la actual versión 7 recibirá actualizaciones de seguridad hasta el 30 de junio de 2024.

10. HIPÓTESIS O FORMULACIÓN DE PREGUNTA CIENTÍFICA

Como lograr el análisis e implementación de una red privada virtual VPN con túneles certificados de autenticación que permita el incremento de la seguridad de red en el transporte de datos e información que se utiliza en la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

11. VARIABLES DE INVESTIGACIÒN:

Variable Independiente: Implementación de una red privada virtual VPN con túneles de autenticación.

Variable Dependiente: Incremento de la seguridad de red en el transporte de datos e información.

12. METODOLOGÍA

En este parte del proyecto se presenta la perspectiva metodológica, expresada en el tipo de investigación, diseño, población, muestra, los documentos de recolección de información y el sistema propuesto.

12.1Método General

En el presente proyecto se utilizara el método científico o experimental ya que permite recopilar información y comprobar ideas.

La esencia del método científico consiste en planteamiento de preguntas y búsqueda de respuestas las cuales deben ser susceptibles de comprobación.

El presente estudio se ubica dentro de una investigación de tipo proyecto factible a entender por su objetivo el cual es implementar tecnología actual de seguridad de red y datos en la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI en base a la interpretación del análisis e implementación de una red privada virtual VPN con túneles certificados de autenticación, que se constituyan como una herramienta de seguridad para el mejoramiento del servicio.

Esta investigación está basada en el método científico.

12.2Método Teórico

Permiten descubrir en el objeto de investigación las relaciones esenciales y las cualidades fundamentales, no detectables de manera censo perceptual. Por ello se apoya básicamente en los procesos de abstracción, análisis, síntesis, inducción y deducción.

Entre los métodos teóricos se destacan fundamentalmente:

12.2.1 Método Histórico

Consiste en el estudio de un objeto o fenómeno, tomando en cuenta tanto el tiempo como el espacio en donde se ubica. Luego se establece la relación que existe en ambos.

Caracteriza al objeto en sus aspectos más externos, a través de la evolución y desarrollo histórico del mismo.

12.2.2 Método Lógico

Reproduce en el plano teórico la esencia del objeto de estudio, investigando las leyes generales y primordiales de su funcionamiento y desarrollo. Dentro del método lógico están incluidos el Método Hipotético Deductivo, el Método Causal y el Método Dialéctico, entre otros.

12.3Método empírico

El método empírico es un modelo de investigación científica, que se basa en la lógica empírica y que junto al método fenomenológico es el más usado en el campo de las ciencias sociales y en las ciencias descriptivas. Por lo tanto los datos empíricos son sacados de las pruebas acertadas y los errores, es decir, de experiencia. Su aporte al proceso de investigación es resultado fundamentalmente de la experiencia. Estos métodos posibilitan revelar las relaciones esenciales y las características fundamentales del objeto de estudio.

12.3.1 Encuesta

Una encuesta es un estudio observacional en el cual el investigador busca recaudar datos por medio de un cuestionario prediseñado, y no modifica el entorno ni controla el proceso que está en observación. Los datos se obtienen a partir de realizar un conjunto de preguntas normalizadas dirigidas a una muestra representativa o al conjunto total de la población estadística en estudio, formada a menudo por personas, empresas o entes institucionales, con el fin de conocer estados de opinión, características o hechos específicos. Se va a seleccionar las preguntas más convenientes, de acuerdo con la naturaleza de la investigación.

Esta técnica nos permitirá obtener información por medio de un cuestionario, tales como su criterio personal, necesidades, molestes entre otros, esta información será de gran importancia para el trabajo de investigación.

12.4Técnicas e Instrumentos

Los instrumentos están compuestos por escalas de medición. Todos los pasos previos realizados hasta este punto, se resumen en la elaboración de un instrumento apropiado para la investigación.

Se ha podido generar un instrumento determinado que es la encuesta para la recopilación de la información el cual nos facilitará generar la información a los involucrados directos mediante un esquema que nos ayudará a realizarlo facilitándonos la información necesaria para la investigación.

12.4.1 Diseño de la Encuesta

El diseño de la encuesta está basado en un cuestionario que contiene preguntas abiertas y cerradas. Las primeras permiten que cada persona responda ampliamente su respuesta. Mientras que las preguntas cerradas tienen opciones prediseñadas de respuesta.

12.4.2 Aplicación de la Encuesta

APLICACIÓN DE LA ENCUESTA MEDIANTE UN CUESTIONARIO DESARROLADO PREVIO A LA OBTENCION DE RESULTADOS EN LA UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

1. Utiliza internet para abrir aplicaciones?

TABLA N°1

Internet

Opciones	Valor	%f
SI	44	100%
NO	0	0%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°1

Internet

FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

La grafica demuestra que la respuesta SI alcanza el 100% y el NO posee un 0% de los encuestados el cual indica que poseen conocimiento básico sobre lo que significa el uso de internet.

2. Cree usted que en la UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI existe la debida seguridad en el envío y recepción de la información?

TABLA N°2

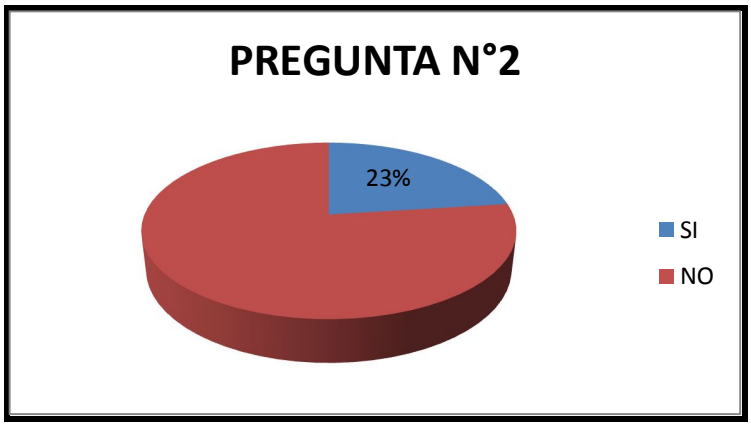
Seguridad en el envío

Opciones	**Valor**	**%f**
SI	10	23%
NO	34	77%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°2

Seguridad en el envío



FUENTE: SISTEMA NACIONAL Y ACREDITACION SNA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

Al realizar el análisis en el grafico se obtiene que el 23% de los encuestados cree que existe seguridad de los datos en la unidad y el 77% de los encuestados piensa que no tienen la seguridad adecuada por la cual es factible la implementación de seguridades.

3. Que tan seguro cree usted que es el envío de información atreves de la red?

TABLA N°3

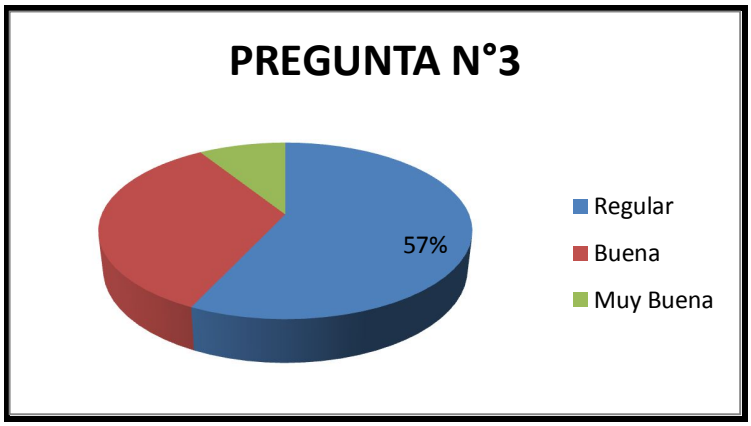
Envío de información

Opciones	Valor	%f
Regular	25	57%
Buena	15	34%
Muy buena	4	9%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°3

Envío de información



FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

Como se puede observar en el gráfico el 57% de los encuestados cree que el envío de información es regular. El 34% cree que es buena para así evitar que personas desconocidas entren a la red y manipulen fácilmente la información, y el 9% cree que es muy buena por la cual necesita un cien por ciento de confiabilidad en el acceso a la red y así evitar problemas a futuro.

4. Conoce usted si existe algún tipo de seguridad que proteja la información dentro del **UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**?

TABLA N°4

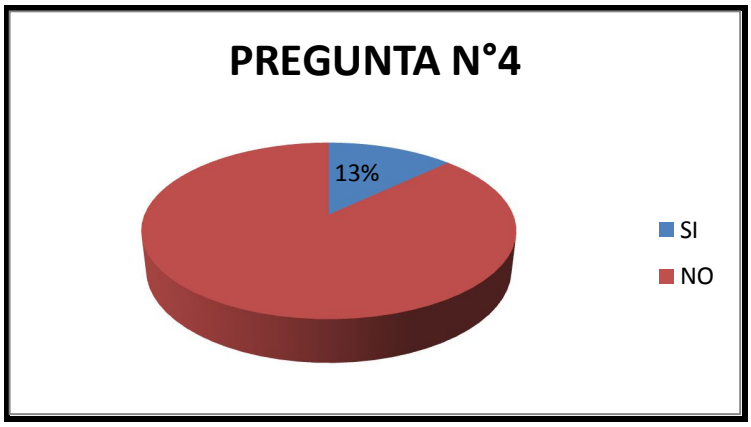
Existencia de información

Opciones	**Valor**	**%f**
SI	6	13%
NO	38	87%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°4

Existencia de información



FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

La grafica demuestra que el 87% desconocen estos tipos de seguridad debido al desconocimiento de la misma, y el 13% creen que existen algún método de seguridad para proteger los datos en la red.

5. Alguna vez ha existido manipulación externa o indebida de los datos por personas no pertenecientes a la institución?

TABLA N°5

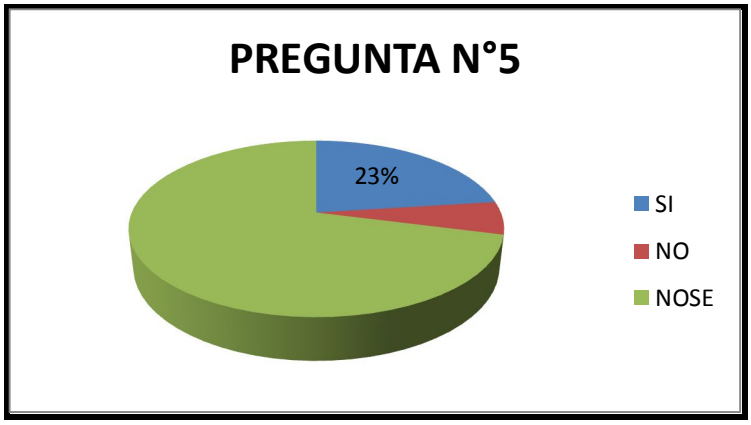
Manipulación indebida de la información

Opciones	Valor	%f
SI	10	23%
NO	4	6%
NOSE	30	71%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°5

Manipulación indebida de la información



FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

Análisis:

Con esto se demuestra que el 23% de las personas manifiestan que si ha existido manipulación de información y el 6% de los encuestados dice que no ha existido manipulación de datos pero el 71% de los encuestados afirman no saber si ha existido manipulación de la información.

6. Cree usted que la información manipulada indebidamente puede perjudicar a la **UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**?

TABLA N°6

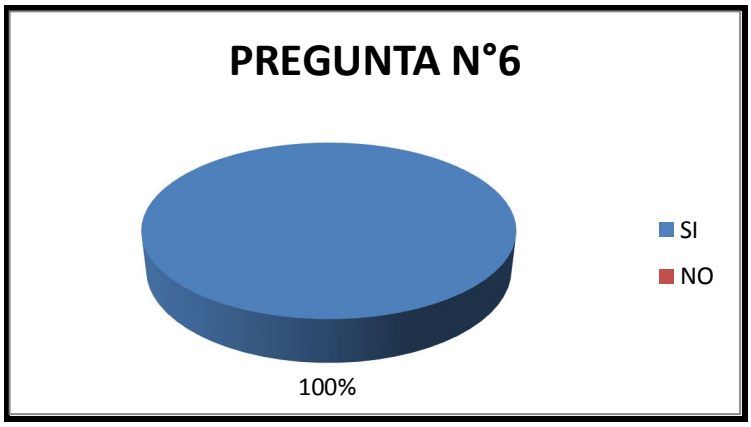
Perjuicio a la institución

Opciones	**Valor**	**%f**
SI	44	100%
NO	0	0%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°6

Perjuicio a la institución



FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

El 100% de los encuestados cree que la manipulación de inadecuada de los datos puede perjudicar en muchos aspectos a la **UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI,** por lo que se requiere seguridad dentro de la red.

7. Alguna vez ha experimentado que la información que usted envió no ha llegado a no ha llegado su destino final?

TABLA N°7

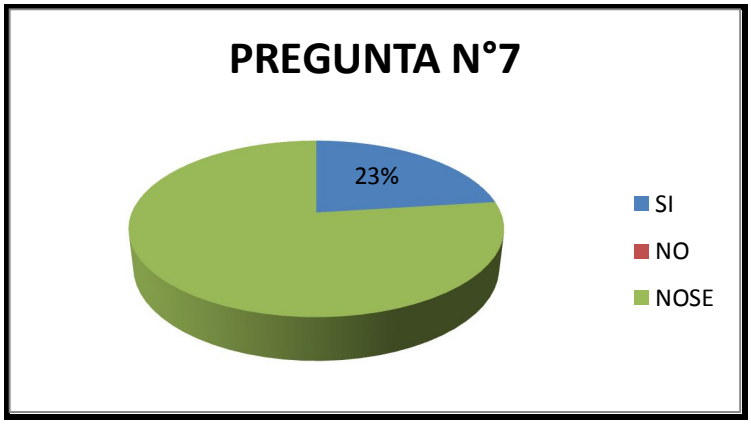
Destino de la información

Opciones	Valor	%f
SI	10	23%
NO	0	0%
NOSE	34	77%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°7

Destino de la información



FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

De acuerdo a la gráfica el 23% dice que ha enviado información y no ha llegado a su destinatario, en cambio el 0% no le ha ocurrido este inconveniente pero el 77% dice que no sabe si la información ha llegado satisfactoriamente a su destino.

8. Alguna vez se ha tratado de implementar algún tipo de seguridad dentro de la **UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**?

TABLA N°8

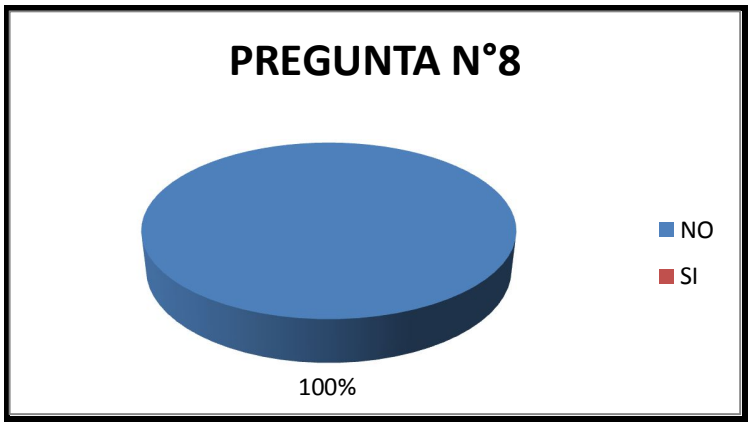
Implementar seguridades

Opciones	**Valor**	**%f**
SI	0	0%
NO	44	100%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°8

Implementar seguridades



FUENTE:UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

El 100% de los encuestados dice que nunca se a intentado implementar algún tipo de seguridad dentro de la **UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**.

9. Estaría usted de acuerdo que se implemente algún método de seguridad para el manejo de datos e información dentro del SNA de la universidad?

TABLA N°9

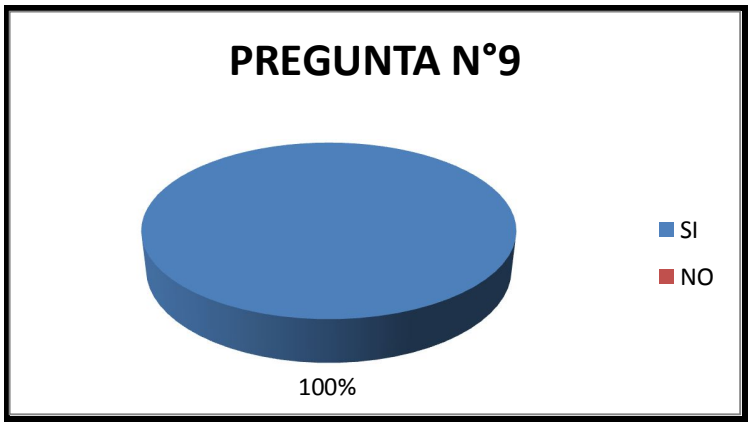
Implemento de seguridad

Opciones	Valor	%f
SI	44	100%
NO	0	0%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°9

Implemento de seguridad



FUENTE:UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

El 100% de los encuestados están de acuerdo que se debería implementar métodos de seguridad para la protección de la información que se produce dentro de la **UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**.

10. Le gustaría tener una comunicación segura sin ningún tipo de ataques externos dentro de la **UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**?

TABLA N°10

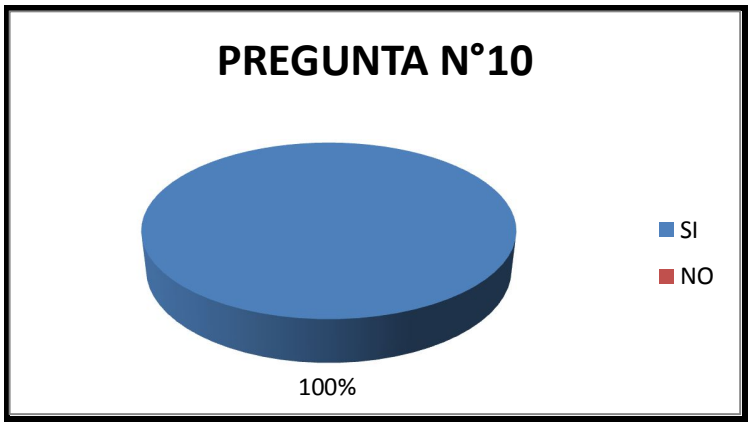
Comunicación segura

Opciones	**Valor**	**%f**
SI	44	100%
NO	0	0%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NEVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°10

Comunicación segura



FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

Todos los encuestados afirman que se sentirían más seguros al momento de acceder a datos e información propios de cada una de las personas que laboran dentro de la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

11. Apoyaría usted este proyecto de seguridad de información en la red y que a la vez sea aplicado dentro de la **UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**?

TABLA N°11

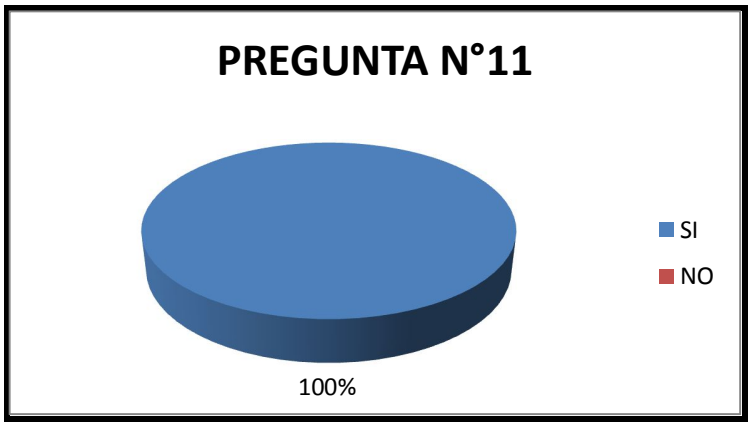
Apoyo a la investigación

Opciones	**Valor**	**%f**
SI	44	100%
NO	0	0%
TOTAL	44	100%

FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

GRAFICO N°11

Apoyo a la investigación



FUENTE:UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI
REALIZADO POR: EL INVESTIGADOR

Análisis:

El 100% de los encuestados apoya y aprueba este proyecto a ser aplicado dentro del UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, lo cual es satisfactorio para nosotros como investigadores implementar la seguridad en tan prestigiosa institución.

12.5Métodos específicos

Para el desarrollo del presente proyecto de investigación, se aplican herramientas tecnológicas como son las **VPN Virtual Private Network** el cual es uno de las más utilizados debido a su flexibilidad en los requerimientos de seguridad, estabilidad y netamente factible en el ámbito económico al momento de hacer este tipo de proyectos.

Antes de empezar debemos realizar el correcto estudio de factibilidad el cual nos va a proporcionas información necesaria para ver si se realiza o no el proyecto de investigación, para así no tener ningún contratiempo al momento de desarrollar cada proceso.

12.5.1 Estudio de Factibilidad

El estudio de factibilidad es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas propuestos, consta de tres aspectos básicos:

12.5.1.1 Factibilidad Técnica

Esta se refiere a los recursos disponibles como herramientas tecnológicas, conocimientos, habilidades, experiencia, que son necesarios para efectuar las actividades o procesos que requiere el proyecto.

El proyecto debe considerar si los recursos técnicos actuales son suficientes o deben complementarse.

Los equipos que están dentro de la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI cuentan con equipos y software que trabajan bajo el sistema operativo Windows 7 y con los requerimientos de instalación como son:

- Procesador 1GHz
- GB de memoria RAM
- Disco duro de 250 GB
- Tarjeta de video AMD
- Cable UTP
- Tarjeta de red
- Y los componentes de hardware en general.

12.5.1.2 Factibilidad Económica

Son los recursos económicos y financieros necesarios para desarrollar o llevar a cabo las actividades y procesos que forman parte esencial para el desarrollo del proyecto.

Para obtener los recursos básicos que deben considerarse:

Costo de estudio

Es el tiempo utilizado en la investigación de requerimientos y necesidades de la Unidad de Admisión y Nivelación de la Universidad técnica de Cotopaxi para la implementación correcta de las VPN.

Costo del desarrollo y adquisición

En este caso no fue necesario un capital considerable ya que la unidad cuenta implementos necesarios para el desarrollo del proyecto.

Costos directos

La adquisición de una maquina con características diferentes a las normales ya que en esta se va a instalar el servidor, ya que tiene que cumplir con todas las necesidades de los usuarios de la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

12.5.1.3 Factibilidad Operativa

Los usuarios de la unidad requieren un método de seguridad de red y datos a que garanticen dichos servicios, por esa razón se va a implementar una VPN (Virtual Private Network) ya que este tipo de tecnología satisfacen dichos requerimientos creando un ambiente seguro para navegar, enviar y recibir datos e información propias de cada persona y de la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

12.5.1.4 Expectativas de Usuario

Una de las principales es enviar y recibir información atreves de la red con toda seguridad en internet, también abrir documentación privada propias de cada usuario como son: cuantas bancarias, transacciones, pago de servicios entre otros ya que los datos se encuentran protegidos de todo tipo de ataques externos.

12.5.1.5 Expectativa de la Unidad

La unidad requiere seguridad tanto de información como de red por ende se implementara claves de acceso con certificados de autenticación tanto para usuarios como para el servidor gracias a este tipo de tecnología se puede lograr redes seguras.

Después de haber realizado el estudio de factibilidad, se procede a levantar los requerimientos propios de cada usuario y el ambiente en el cual se va a desarrollar el proyecto.

12.5.2 Requerimientos

Análisis:

Realizaremos el análisis de las deficiencias en seguridad y transporte de datos en la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

Se ha podido identificar que no existe ningún servicio que proporcione seguridad a datos relevantes de la unidad contra ataques externos que fácilmente podrían incursionar a través de la nube o internet.

Se ha podido observar que el personal que trabaja en esta área no cuenta con conocimientos de seguridad de red y datos.

No existe ninguna restricción al momento de ser parte de la red lo cual ha permitido que la red este saturada debido al gran número de usuarios que trabajan en esta área.

Los usuarios de esta unidad no saben si en verdad los la información enviada llega a su destino final.

Recolección de Datos:

Se realizara la recolección de datos que nos permitirán obtener un número exacto de computadoras ya sean de escritorio o portátiles que existen dentro de la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, el

cual nos permitirá analizar las diferentes configuraciones que necesita cada equipo para que se pueda conectar a la nueva red.

También se levantara un análisis a cada uno de los elementos tecnológicos para verificar su correcto funcionamiento y evitar contratiempos al momento de la instalación de la VPN.

Requisitos:

Analizaremos cada una de las maquinas que se encuentran dentro de la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, para ver si cumplen con los requisitos de factibilidad para la instalación de esta tecnología de red en cada una de ellas para su correcto funcionamiento dentro de la misma.

Una vez ya obtenida toda la información técnica de la aplicación del proyecto se procederá con la instalación de proyecto.

Para la instalación del sistema se debe examinar un lugar adecuado y estratégico dentro de la unida, a la vez verificar que el equipo que se va a utilizar como servidor cuente con las debidas garantías de funcionamiento.
Verificar características del equipo a utilizar como servidor.

Hardware:

- Procesador Intel Core i7 3.4 Ghz de 4ta Generación
- Tarjeta de red
- Tarjeta de video zogis 210 1gb ddr
- Salida video VGA
- Disco duro de 1000 GB
- Monitor de alta resolución LCD
- Memoria RAM de 8 GB.

Software:

- Sistema Operativo Centos 7 server Linux
- Paquetes adicionales (demonio) Fedora Linux

12.5.3 Implementación y Fase de Diseño

Los pasos para la configuración del servidor Centos 7 Linux que nos servirá como plataforma de soporte para la VPN son:

Instalación del sistema operativo Centos 7 server siguiendo cada uno de los pasos que se muestran en el manual de usuario (anexos).

- **Configuración de la tarjeta de red**

Paso seguido después de la instalación se debe configurar la tarjeta de red para así tener conexión a internet (manual de usuario).

- **Descarga de paquetes**

Se debe abrir el terminal para así descargar cada uno de los paquetes del repositorio de Fedora Linux requeridos para la instalación y configuración del servidor VPN el cual va a brindar las seguridades del caso a la unidad de Admisión y Nivelación de la Universidad Técnica de Cotopaxi.

- **Habilitar el repositorio epel en Centos.**

Una vez descargados el paquete requerido para el sistema se procede a la configuración de mismo el cual se debe activar para que comience a funcionar.

Se tienen que seguir cada uno de los pasos mencionados (manual de usuario), ya que la falta de líneas de código puede hacer que todo el sistema caiga.

- **Instalar VPN, Easy-rsa e iptables.**

Instalar VPN la versión más actual ya que forman una gran familia y cada vez se esta renovando además el sistema operativo Centos descarga por usted el más adecuado para su configuración.

Paso seguido atreves de EAsy-sra de configurando para que este tenga un valor dentro de su carpeta el cual sirve como repositorio en la carpeta el cual estará siempre lista a cualquier llamado

- **Configurar easy-rsa.**

Una vez ejecutado las líneas de código para su configuración se presiona enter para así acceder a los paquetes o repositorios que bien ya instalados por default dentro de cada uno. Hay que configurar el archivo que viene dentro del paquete instala do.es que aquí donde se crean las llaves de usuario y servidor.

Se debe tomar muy encuenta las c0omas a quitar ya que es un sistema muy complejo y se tendría problemas al momento de ejecutar la red privada virtual VPN

- **Reglas de seguridad:**

En esta parte donde se crear las llaves de autenticación se debe tomar muy encuentra las reglas de seguridad del mismo ya que si hace la configuración mal tendrá problemas en el funcionamiento de la red.

- **Configurar OPENVPN:**
- **Creación de certificados:**

Hay que tomar muy en cuenta al momento de configurar los certificados tanto del cliente como del servidor, este paso es muy importante ya que de este depende la comunicación del servidor hacia el cliente y viceversa.

Para creación de certificados se debe cambiar procesos en el cual se debe introducir debido a los dispositivos de cada máquina.

El certificado funciona como un permiso que recibe el cliente y el servidor ya que los dos van a manejar las un mismo tipo de cifrado de seguridad

- **Certificado SSL**

Un certificado SSL es un certificado digital utilizado por el protocolo para el encriptamiento de la información.

Este certificado es proporcionado por un proveedor y es enviado al cliente por el servidor con quien estamos estableciendo una conexión segura.

El certificado que vamos a crear tiene el mismo nivel de encriptamiento que cualquiera de estos proveedores autorizados puede entregar.

- **Deshabilitar firewalld y SELinux.**

Para desactivar firewalld y usar iptables tienes que desactivar firewalld, instale el servicio iptables, a continuación, habilitarlo. . Estas instrucciones deben ser los mismos para esta versión 7, Fedora 21, RHEL 7 (Red Hat Enterprise Linux 7) y distribuciones similares primer lugar vamos a detener y deshabilitar firewalld con los siguientes comandos (manual de usuario).

Eso es todo, que ahora está listo para usar iptables. Seguir adelante y añadir algunas reglas. Asegúrese de añadir reglas para ambos iptables e ip6tables.

- **Configurar iptables para openVPN.**

La forma de proteger sus datos personales con iptables que sugiero se familiarice antes de intentar los cambios. Se puede obtener información básica de un viejo hilo aquí. Una nota más es que los viejos "service iptables save" comando se utilizó para usar en el sistema de v (init) ya no funcionará en el nuevo systemd. Se puede utilizar el siguiente comando para guardar sus reglas de iptables (manual de usuario).

- **Iniciar OPENVPN servidor.**

Esto le pedirá que introduzca el nombre de usuario y la contraseña de la VPN. Después de iniciar la sesión, el equipo se puede conectar a la VPN. Para comprobar la conexión VPN, visite su motor de búsqueda favorito y escriba "dirección IP". Se le presentará con una lista de sitios web que muestran su dirección IP actual. Confirmar su dirección IP actual.

- **Configuración de la aplicación de cliente de OpenVPN.**

Para conectar con el servidor openvpn, el cliente requiere una clave y un certificado que ya creados, por favor descargue los 3 archivos de su servidor utilizando SFTP o SCP :

- **ca.crt**
- **client.crt**
- **client.key**

Si utiliza un cliente de Windows, a continuación, puede utilizar WinSCP para copiar los archivos. Después de crear un nuevo archivo llamado client.ovpn y la configuración de pasta a continuación (manual de uso de usuario)

13. POBLACION Y MUESTRA

POBLACION

Para el desarrollo del proyecto se enfocara de manera directa a la siguiente población que labora de forma directa en la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

ADMINISTRATIVOS: 5

DOCENTES: 39

TOTAL: 44

MUESTRA

Se ha tomado en cuenta a aquellas personas que utilizan computadoras conectadas a la red las cuales amerita para la aplicación de la muestra en la **UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI**.

13.1DISEÑO ESTADISTICO

Un modelo estadístico es una expresión simbólica en forma de igualdad o ecuación que se emplea en todos los diseños experimentales y en la regresión para indicar los diferentes factores que modifican la variable de respuesta.

13.2CALCULO DE LA MUESTRA

Para el cálculo de la muestra se utilizó la estadística descriptiva que es una gran parte de la estadística y que se dedica a recolectar, ordenar, analizar y representar un conjunto de datos, con el fin de describir apropiadamente las características de los datos obtenidos.

Este análisis es muy básico ya que se hace un estudio calculando una serie de medidas de tendencia central, para ver en qué medida los datos se agrupan o dispersan en torno a un valor central.

Para la obtención de resultados es necesario aplicar la siguiente formula:

Equivalencias:

- **n:** Tamaño de la muestra
- **PQ:** Coeficiente de la muestra = 0.25
- **N:** Población = 44
- **E:** Error que se admite = 8% = 0.08
- **K:** Coeficiente de corrección paramétrica = 2

FÓRMULA

$$n = \frac{N}{(\epsilon^2)(N-1)+1}$$

$$n = \frac{44}{(0{,}05^2)(44-1)+1}$$

$$n = \frac{44}{(0{,}0025)(43)+1}$$

$$n = \frac{44}{1.10}$$

$n = 40$ ⇨ 40

14. PRESUPUESTO

14.1RECURSOS TECNOLOGICOS

Los recursos tecnológicos utilizados en esta investigación son los siguientes:

- Computadoras de escritorio
- Impresora
- Internet
- Plataforma Windows 8.
- Plataforma Linux
- Conexión de datos

14.2DETALLE PRESUPUESTO

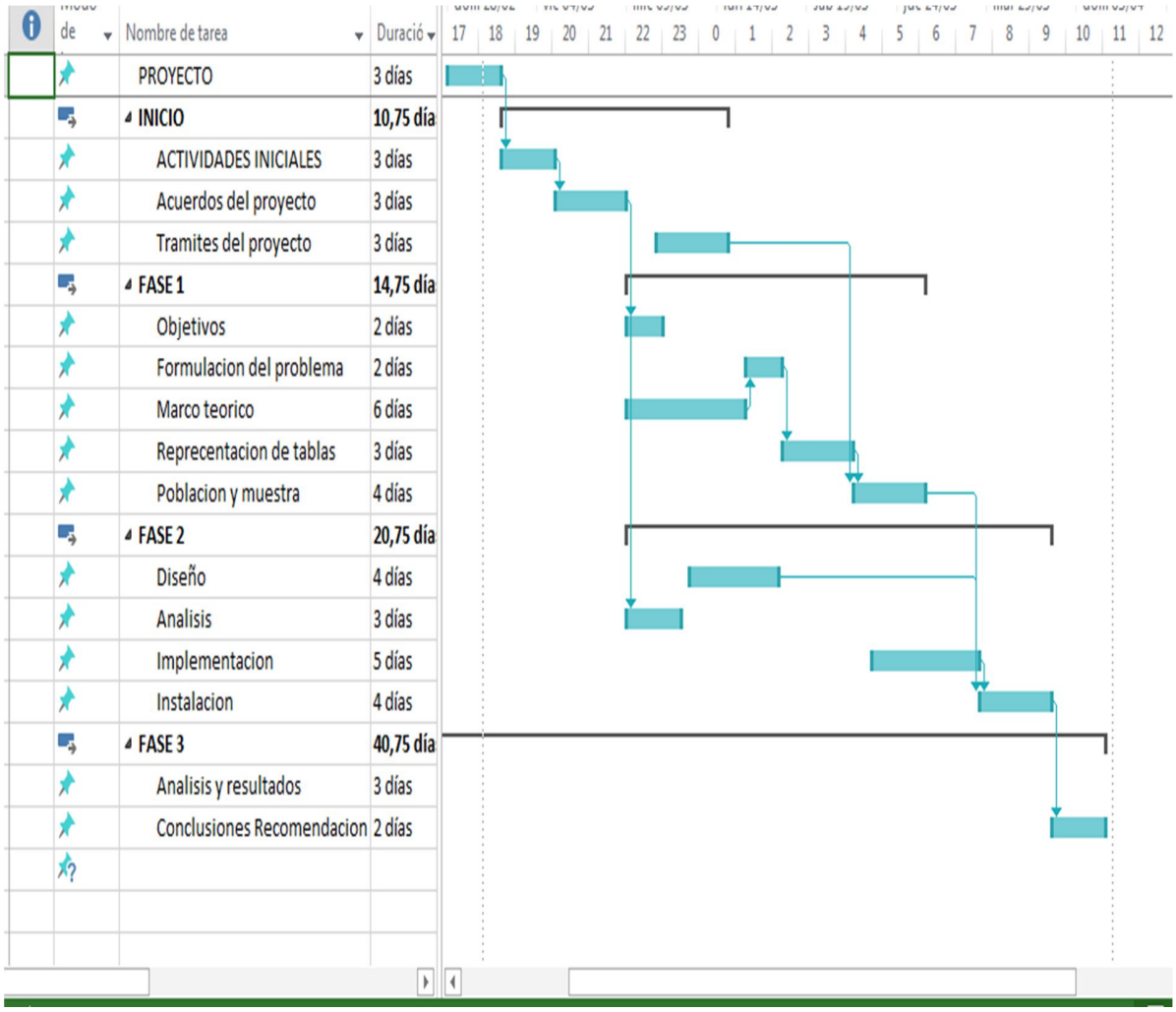
Tabla 7: DETALLES DE GASTO GENERAL

GASTOS DIRECTOS			
DETALLES	CANTIDAD	V. UNITARIO	V.TOTAL
Computadoras de escritorio	2	1500	3000
Internet	50	25	1250
Resma de papel	4	3,5	14
Esferos graficos	12	0,3	3,6
Impresiones	300	0,05	15
Cacle UTP	50	0,9	45
Kit de herramientas informaticas	2	50	100
Empastados	3	15	45
Anillados	3	2	6
Fotocopias	1000	0,02	20
solicitud	10	0,5	5
TOTAL			4503,6

Realizado por: Investigador

15. CRONOGRAMA

GRAFICO 19: CRONOGRAMA ESTABLECIDO DEL DESARROLLO DEL PROYECTO



Realizado por: Investigador

16. ANALISIS Y DISCUSIÓN DE LOS RESULTADOS

Los resultados se fueron desarrollando de forma gradual, en base a los escenarios planteados, enfocados sobre la vulnerabilidad del punto de acceso analizando la seguridad de conexión a la red y verificar el acceso a cada usuario al aplicar seguridad.

Para la práctica se utilizó varios implementos tecnológicos de hardware y software, como el servidor Centos7 Linux como punto de acceso, estaciones de trabajo o clientes Windows 7 y dispositivos de red.

La máquina adquirida cumple con los propósitos establecidos al inicio del proyecto dando como resultado que los usuarios de la UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

Para la conexión del servidor se configura en la nueva red VPN es el que se encargará de recibir a los clientes Windows por medio de claves, llaves y certificados que permiten una conexión segura dando lugar a una de las principales faces de la instalación.

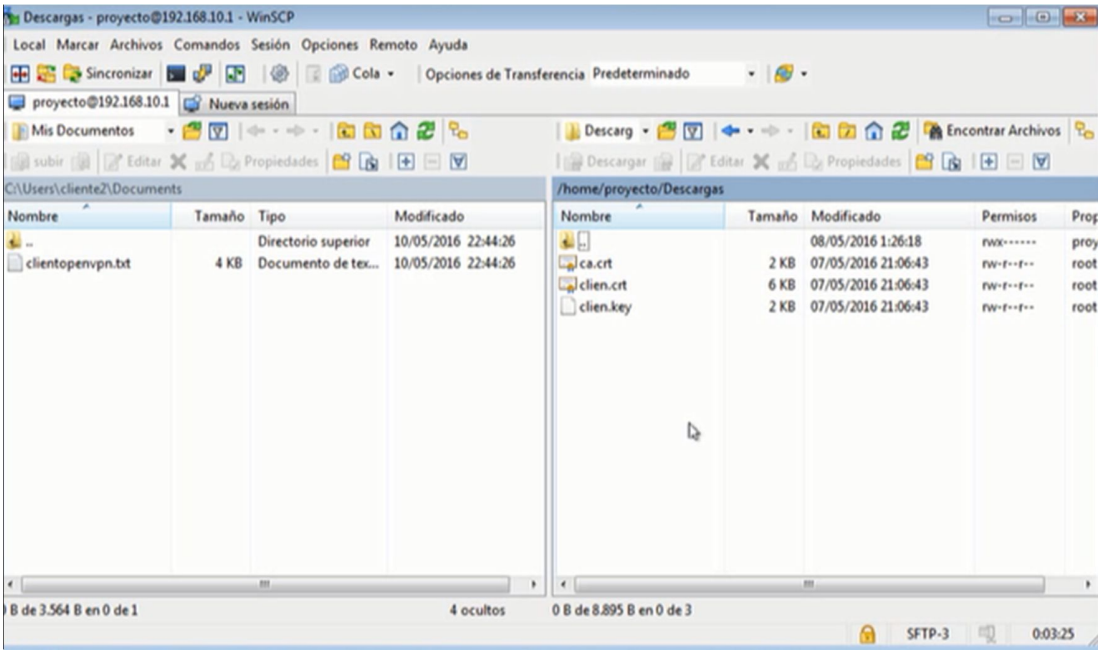
Esta ventana es la que se ve al momento de la ejecución del opnVPN ya que este permite la comunicación de las maquinas a través de la red.

GRAFICO 20: CREACION DE LA RED EN CENTOS 7

Realizado por: Investigador

Se realizó también la configuración manual de sistema operativo Windows7 como clientes de la nueva red privada virtual ya instalada y funcionando de la mejor manera, para así poder visualizar la ventana principal para la conexión a la nueva red privada virtual propuesta inicialmente.

GRAFICO 21: CREACION DE LA RED VPN EN WINDOWS 7



Realizado por: Investigador

Para el acceso de un cliente que no tenga la configuración VPN obtuvimos cero conexiones a la red el cual no permite el acceso sin que se haga la configuración de certificados que permita respuestas ya que para conectarse el cliente necesita obligatoriamente hacer la configuración adecuado dentro del equipo.

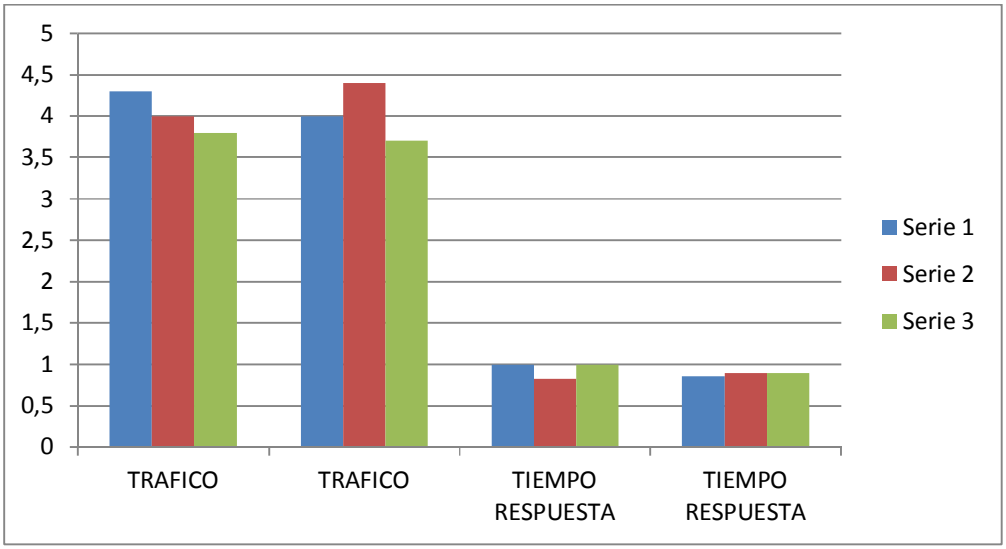
La grafica presentada demuestra la conectividad de la maquina servidor cliente:

Los datos elevados demuestran las maquinas antes y después de aplicar seguridades VPN.

La grafica menor representa el tiempo de respuesta de las maquinas una vez ya conectadas a la nueva red virtual.

16.1PRUEBAS

GRAFICO 22: REPERECENTACION DE RESULTADOS A LAS SERIES APLICADAS



Realizado por: Investigador

Se realizaron y describieron las pruebas realizadas con la red privada virtual VPN, la relevancia de aplicar servicios de seguridad ante una evidente y comprobada vulnerabilidad de las estaciones de trabajo.

Extraer el tráfico de una LAN es sencillo ya que existen programas que determinan valores y sin contar con los servidores de red e internet y a futuro representa problemas serios ya que no se puede confiar en los sistemas que vienen por defecto

La resistencia a la estrategia de ataques es parte fundamental en las prestaciones de la red donde se ha configurado la red privada virtual VPN, bajo la evaluación de dichas prestaciones para garantizar la seguridad del servicio.

17. CONCLUSIONES

- VPN proporciona seguridad de navegación y datos creando un túnel de seguridad el cual está compuesto por certificados que ayuda a que los intrusos existentes dentro de la nube se mantengan al margen de la red.
- Los certificados y claves de autenticación son proporcionadas a las maquinas clientes desde el servidor para así crea una llave única que permite el ingreso a la nueva red privada virtual.
- VPN proporciona seguridad dentro de la nube sin crear algún tipo de interferencia en la red, proporciona toda libertad de navegación sin interrumpir el libre tráfico de datos desde y hacia la nube.
- VPN no es compatible con IPsec porque son dos estructuras diferentes con la diferencia de que VPN proporciona seguridad dentro de la nube, mientras que IPsec proporciona seguridad de datos con encriptación.

18. RECOMENDACIONES

- Se recomienda a las instituciones públicas y privadas utilizar este tipo de tecnología como forma de ayuda en seguridad de información.
- Se debe instalar paquetes actualizados antes de configuración OPEN VPN esto se debe a las nuevas actualizaciones que forman parte fundamental de la seguridad virtual.
- Ser utilizado por una persona que tenga conocimientos en el área.
- Verificar cada una de las máquinas existentes antes de la instalación de la red debido a que por el momento VPN no es compatible con ciertos programas.
- Mucho cuidado al instalar y configurar el servidor Centos Linux debido a su configuración en por medio de códigos y este depende mucho del correcto funcionamiento de la red.

19. REFERENCIAS

BIBLIOGRAFIA CITADA

- Baena, v. (2010). Teorias y lineas de investigacion cientifica. UOC.
- Calero , J., Huidrobo, M., & Blanco, A. (2006). Redes de area local: Administración de sistemas informáticos. Madrid: Thomson Ediciones.
- dias, g. (2008). Proceso y herramientas para seguridad de las redes. madrid: fuente.
- Diaz , G., Alzorriz, I., Sancristobal, E., & Castro , M. (2014). Procesos y herramientas para seguridad de redes. UNED.
- Doraswamy, N., & Harkins, D. (2006). La biblia de la seguridad para internet, intranets y redes privadas virtuales. Prentece Hall Profesional.
- Egg, A. (2011). Aprender a investigar: Nociones básicas para la investigación. Argentina: Brujas.
- Lerma, H. (2012). Metodologia de la investigación. Bogota: ECOE.
- Loubet Orozco, R. (2006). Metodologia y técnicas de investigación. ACCO EDITORES.
- Martinez, J. P. (2009). IPv6 para todos: Guia de uso y aplicaciones para diversos entornos. Argentino: Internet Society.
- Mendez, C. (2010). Metodología, diseño y desarrollo del proceso de investigación, con enfancis en ciencias empresariales. Mexico: LIMUSA S.A.
- Minei, I., & Lukey, J. (2010). Aplicaciones habilidadas para la evolución y la nuevas tecnologías emergentes. EE.UU: Wiley.
- Morales, M. (2010). Analítica web parea empresas arte, ingenio y anticipación. Barcelona: UOC.
- Salmeron , A. (2007). Informatica. Conceptos fundamentales. Argentina: Prentice Hall.
- Stallings , W. (2006). Comunicaciones y redes de computadoras. Madrid (España): Pearson educacion S.A.

BIBLIOGRAFIA VIRTUAL

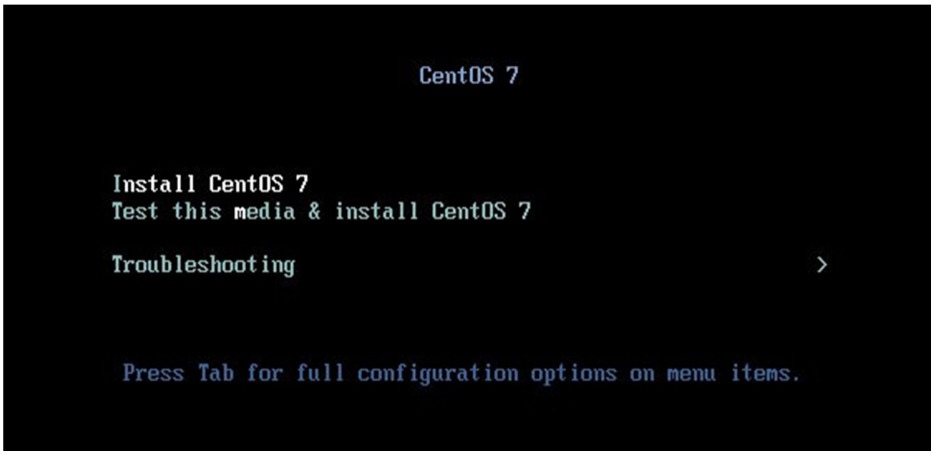
- Trafico; Diccionario de términos; http://definicion.de/trafico/#ixzz3iGB79SXS; Recuperado el 28 de 7 de 2015
- Benitez, C. (s.f.). Biblioteca en linea. Recuperado el 2 de 10 de 2015, de Openlibra: http://www.etnassoft.com/biblioteca
- Brin, Serguéi; Pague, Larry;. (04 de 09 de 1998). Libros Google. Recuperado el 25-15 de 9-10 de 2015, de Compañia Google: https://books.google.com.ec/books

ANEXOS

20. ANEXOS

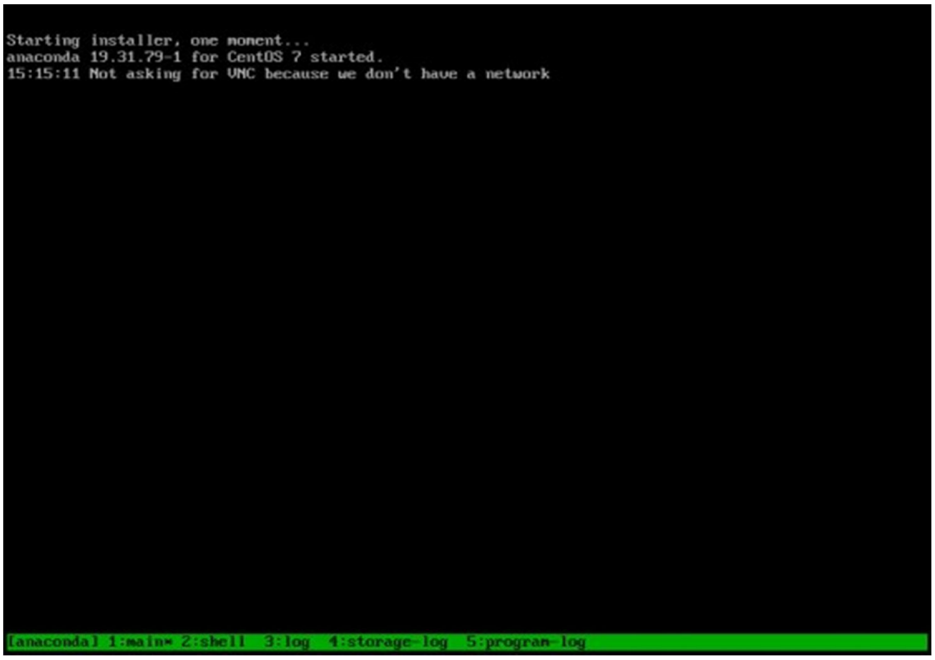
ANEXO 1

Instalando Centos 7



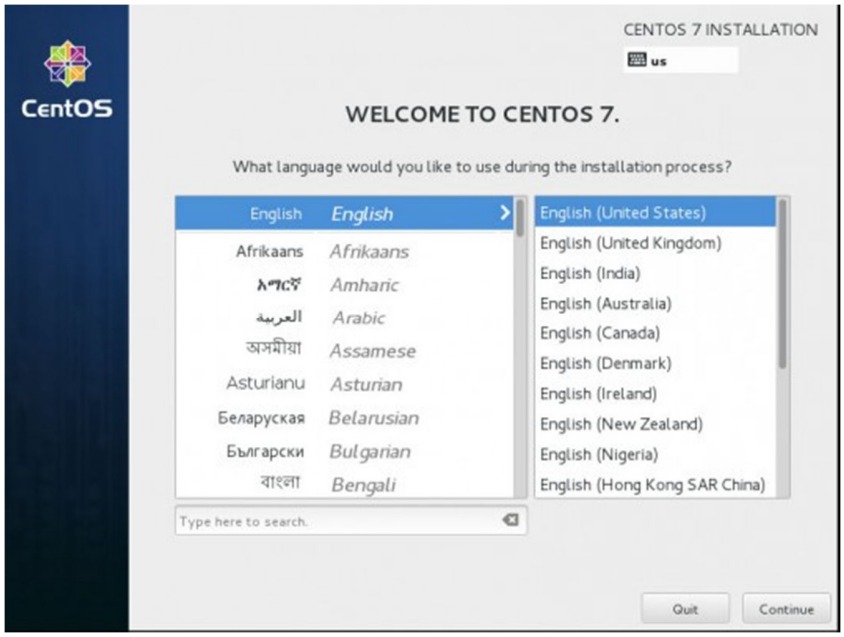
ANEXO 2

Debemos de seleccionar donde dice Install CentOs



ANEXO 3

Selección de idioma



ANEXO 4

Escoger destino de la instalación

ANEXO 5

Seleccionamos la unidad donde deseamos instalar.

ANEXO 6

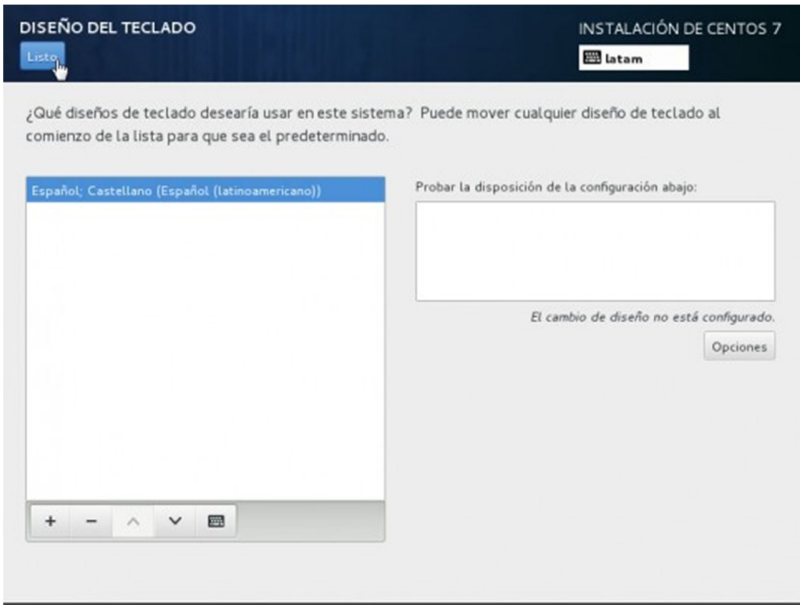
Luego en la sección de Regionalización seleccionamos Fecha & Hora.

ANEXO 7

Nos saldrá una imagen donde configuráremos la Zona horaria y la.

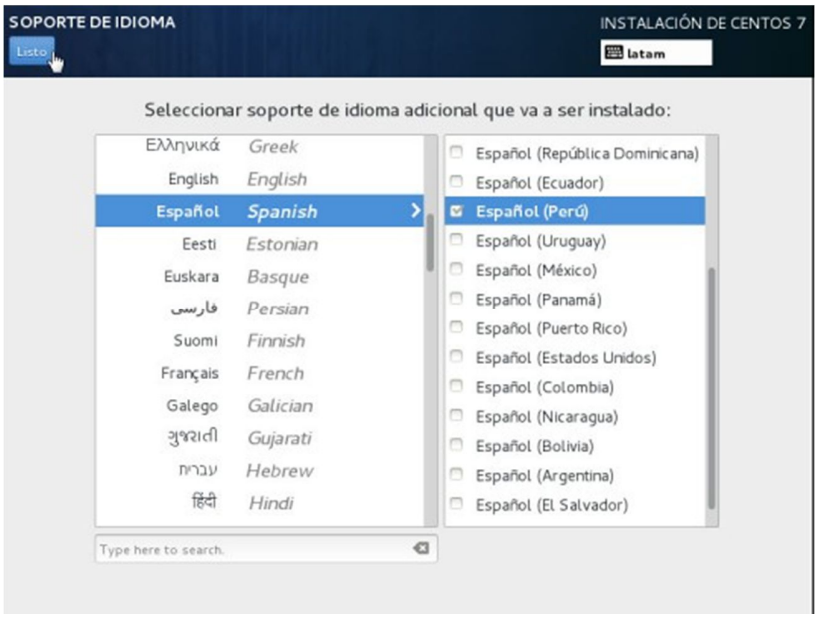
ANEXO 8

Verificamos que este correcto con nuestra Zona horaria.



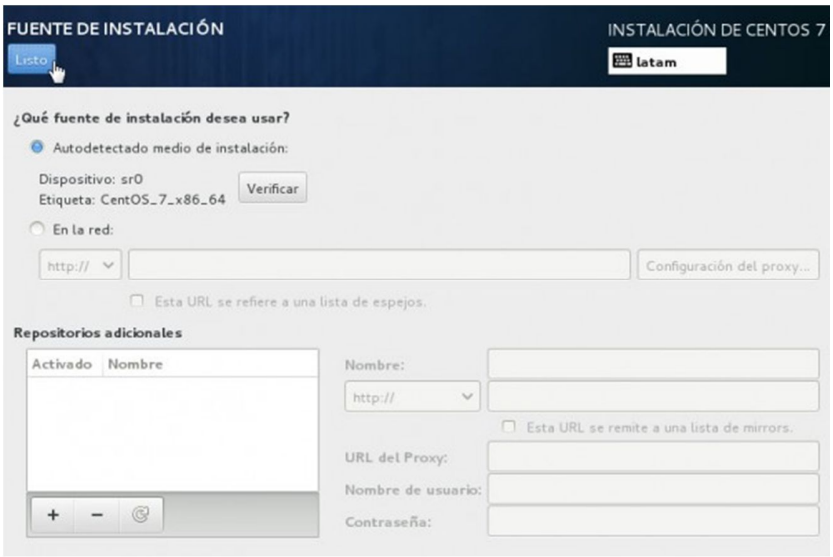
ANEXO 9

También tenemos en la sección Regionalización la opción Soporte de idioma.



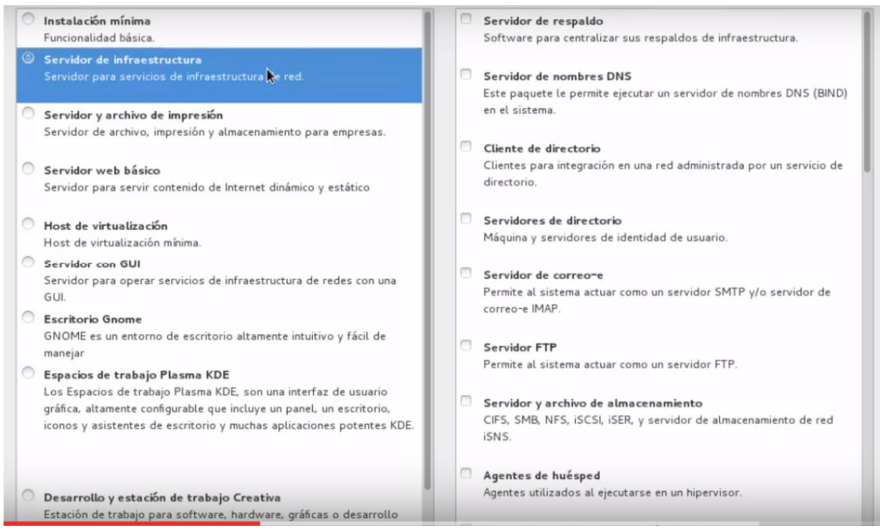
ANEXO 10

En la Sección Software seleccionamos auto detectado de instalación.



ANEXO 11

Selección de software, colocamos la opción servidor de infraestructura



ANEXO 12

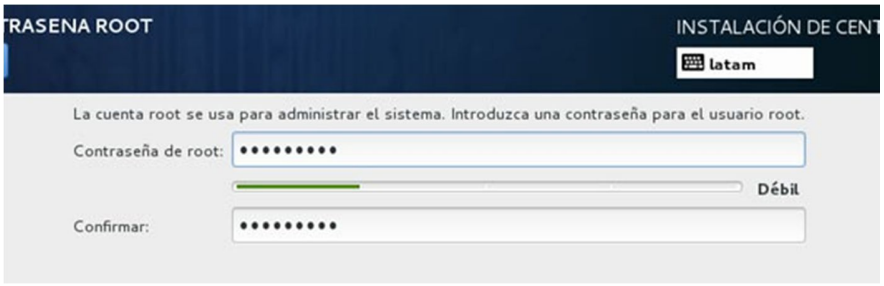
En la sección Sistema seleccionamos Destino de instalación, seleccionamos la unidad.

ANEXO 13

Terminado eso le damos Comenzar instalación.

ANEXO 14

Escribimos la contraseña de root:

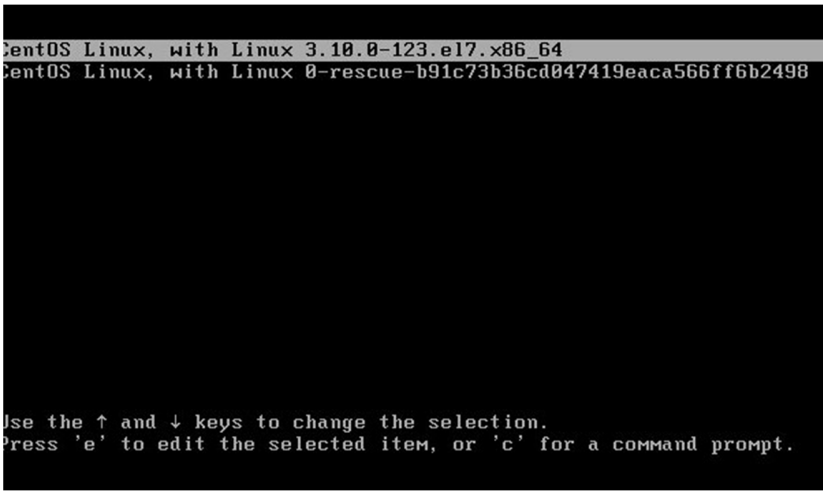


ANEXO 15

Volvemos a escribir la contraseña para que pueda hacer la verificación.

ANEXO 16

Reiniciando



ANEXO 17

Configurar las interfaces de Red en Centos 7

```
# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
```

ANEXO 18

En siguiente paso a realizar, es localizar el archivo de configuración de la interfaz]:

```
# cd /etc/sysconfig/network-scripts/
```

```
# ls
 ifcfg-enp0s3
 ifcfg-lo
 ...
```

```
# su -
# nano ifcfg-enp0s3
```

```
TYPE=Ethernet
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=enp0s3
UUID=b7... ...32a
ONBOOT=no
HWADDR=08:x:xx:xx:xx:A7
IPADDR0=
PREFIX0=
GATEWAY0=
DNS1=
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
```

ANEXO 19

Los parámetros anteriores deben ser configurados según lo que te indique el proveedor de internet.

```
BOOTPROTO=static
IPV6INIT=no
IPV6_AUTOCONF=no
ONBOOT=yes
IPADDR0=192.168.0.77
PREFIX0=24
GATEWAY0=192.168.0.1
DNS1=192.168.0.2
```

```
# systemctl stop NetworkManager
# systemctl disable NetworkManager
```

```
rm '/etc/systemd/system/multi-user.target.wants/NetworkManager.service'
rm '/etc/systemd/system/dbus-org.freedesktop.NetworkManager.service'
rm '/etc/systemd/system/dbus-org.freedesktop.nm-dispatcher.service'
```

ANEXO 20

Una vez hecho esto debes reiniciar el servicio de red:

```
# systemctl restart network.service
```

ANEXO 21

Hacer un ping hacia una Ip que te responda y validar que hay comunicación, por ejemplo:

```
# ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=64 time=6.16 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=64 time=1.40 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=64 time=4.52 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=64 time=1.49 ms
^C
--- 192.168.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.403/3.396/6.161/2.032 ms
```