UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TESIS DE GRADO

TEMA:

"ANÁLISIS E IMPLEMENTACIÓN DEL PROTOCOLO DE SEGURIDAD IPSEC (INTERNET PROTOCOLO SECURITY) EN REDES DE DATOS BASADAS EN IPV6, ESTABLECIENDO CLAVES DE CIFRADO, EN LA EMPRESA BYPAS COMUNICACIONES, UBICADA EN LA CIUDAD DE QUITO, PROVINCIA DE PICHINCHA".

Tesis presentada previa a la obtención del título de Ingenieras en Informática y Sistemas Computacionales.

Autoras:

ELVIA LUCILA BARAHONA JAMI

EMMA ELIZABETH OÑA YÁNEZ

Director:

ING. PATRICIO NAVAS

Latacunga – Ecuador

Marzo 2014

AVAL DEL TRIBUNAL DE TESIS

En nuestra calidad de Miembros del Tribunal de la Defensa de Tesis Titulada "**ANÁLISIS E IMPLEMENTACIÓN DEL PROTOCOLO DE SEGURIDAD IPSEC (INTERNET PROTOCOLO SECURITY) EN REDES DE DATOS BASADAS EN IPV6, ESTABLECIENDO CLAVES DE CIFRADO, EN LA EMPRESA BYPAS COMUNICACIONES, UBICADA EN LA CIUDAD DE QUITO, PROVINCIA DE PICHINCHA**", de Autoría de las postulantes Barahona Jami Elvia Lucila y Oña Yánez Emma Elizabeth de la Carrera de Ingeniería en INFORMÁTICA Y SISTEMAS COMPUTACIONALES CIYA – UTC. Certificamos que se puede continuar con el trámite correspondiente.

Es todo cuanto podemos certificar en honor a la verdad.

Atentamente,

Ing. Jorge Rubio

Presidente

Lcda. Susana Pallasco

Miembro

Ing. Segundo Corrales

Opositor

AUTORÍA

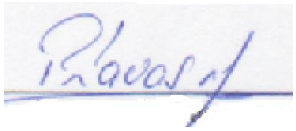
Los criterios emitidos en el presente trabajo de investigación. "**ANÁLISIS E IMPLEMENTACIÓN DEL PROTOCOLO DE SEGURIDAD IPSEC (INTERNET PROTOCOLO SECURITY) EN REDES DE DATOS BASADAS EN IPV6, ESTABLECIENDO CLAVES DE CIFRADO, EN LA EMPRESA BYPAS COMUNICACIONES, UBICADA EN LA CIUDAD DE QUITO, PROVINCIA DE PICHINCHA**", es de exclusiva responsabilidad de las tesistas.

……..	…….
Elvia Lucila Barahona Jami.	Emma Elizabeth Oña Yánez.
C.I. 050255735-8	**C.I.** 0503326578-7

AVAL DIRECTOR DE TESIS

Yo, ING. PATRICIO NAVAS, Docente de la Universidad Técnica de Cotopaxi y director de la presente tesis de grado: **"ANÁLISIS E IMPLEMENTACIÓN DEL PROTOCOLO DE SEGURIDAD IPSEC (INTERNET PROTOCOLO SECURITY) EN REDES DE DATOS BASADAS EN IPV6, ESTABLECIENDO CLAVES DE CIFRADO, EN LA EMPRESA BYPAS COMUNICACIONES, UBICADA EN LA CIUDAD DE QUITO, PROVINCIA DE PICHINCHA"** de autoría de los postulantes Barahona Jami Elvia Lucila C.I. 050255735-8, Oña Yánez Emma Elizabeth con C.I. 050332678-7, de la especialidad de Informática y Sistemas Computacionales. **CERTIFICO**: que ha sido prolijamente revisada. Por tanto, autorizo la presentación; la misma que está de acuerdo a las normas establecidas en el REGLAMENTO INTERNO DE GRADUACIÓN DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI, vigente.

Por lo expuesto, considero que reúne los requisitos y méritos suficientes para ser sometido a su estudio, aprobación y presentación pública.



Ing. Patricio Navas.

DIRECTOR DE TESIS.

C.I. 0502029275

By Pas Comunicaciones

Líderes en Soluciones integrales de Telecomunicaciones

Quito, 18 de Marzo del 2014

CERTIFICACION

A quien interese:

Por medio del presente, me permito certificar que las señoritas: Emma Oña y Elvia Barahona, realizaron la investigación como parte de su tesis de grado siendo ésta digna de resaltar por el empeño que tuvieron las mencionadas señoritas.

Es todo cuanto puedo certificar en honor a la verdad, pudiendo dar uso a la presente las señoritas como mejor les parezca.

Atentamente,

Ing. Byron A. Arevalo T.

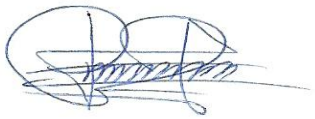
Gerente General .
ByPas – Comunicaciones
593 984533120
Quito – Pichicha - Ecuador

Dirección: Ruiz de Castilla Y Andagoya, ed. Expocolor , piso 2, Oficina 6-7.
Teléfono: 593 23227869

AVAL DE TRADUCCIÓN

En calidad de Docente del Centro Cultural de Idiomas de la Universidad Técnica de Cotopaxi, yo Lic. Jorge Luis Iza Pila con la C.C. 050296591-6 CERTIFICO que he realizado la respectiva revisión del Abstract; con el tema: "ANÁLISIS E IMPLEMENTACIÓN DEL PROTOCOLO DE SEGURIDAD IPSEC (INTERNET PROTOCOLO SECURITY) EN REDES DE DATOS BASADOS EN IPV6, ESTABLECIENDO CLAVES DE CIFRADO, EN LA EMPRESA BYPAS COMUNICACIONES, UBICADA EN LA CIUDAD DE QUITO, PROVINCIA DE PICHINCHA." cuya autoras son: Elvia Lucila Barahona Jami, Emma Elizabeth Oña Yánez y director de tesis Ing. Patricio Navas.

Latacunga, 25 de marzo del 2014



……
Lic. Iza Pila Jorge Luis
DOCENTE CENTRO CULTURAL DE IDIOMAS
C.I. 050296591-6

AGRADECIMIENTO

En primer lugar damos infinitamente gracias a Dios, por habernos dado fuerza y valor siempre guiándonos, con sus bendiciones en todo momento de nuestras vidas.

A nuestros padres por el gran esfuerzo realizado y brindado durante todos estos años de estudio, ese apoyo moral, económico e incondicional.

Luego a nuestro Director de Tesis Ing. Patricio Navas, un sincero agradecimiento, porque juntos estuvimos en el desafío de finalizar este proyecto.

Finalmente un agradecimiento especial a la Universidad Técnica de Cotopaxi por su gran acogida en sus aulas, impartiendo el saber, por medio de todos nuestros queridos maestros, especialmente a todos aquellos que nos han sabido brindar el apoyo y su ayuda incondicional.

Gracias a todas las personas que ayudaron directa e indirectamente en la Realización de este proyecto.

Elvia. **Emma.**

DEDICATORIA

El presente trabajo lo dedico a Dios por darme el aliento de vida cada día y no dejarme desvanecer por las dificultades encontradas en el camino del saber, después a mis padres por ser el pilar fundamental de mi vida, quienes han velado por mi bienestar y educación siendo mi apoyo en todo momento. Para ellos mi amor, obediencia y respeto.

A mi esposo Alex, a mis Hijos Alexander y Mateo por ser mi fuente de inspiración y haberme brindado su apoyo incondicional, gracias a su amor, paciencia y comprensión han hecho más fácil este trabajo.

Luego a mis hermanas y hermanos por su apoyo moral, quienes de una u otra forma con sus consejos han contribuido para ser una persona de bien.

Elvia.

DEDICATORIA

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mis padres que con su ejemplo maravilloso de amor, fe y sacrificio incomparable, me han guiado en cada momento de mi vida; siempre pendiente de mis aspiraciones e inquietudes como estudiante, y que en todo momento logran enrumbarme por el camino de la responsabilidad, para así obtener mis ideales.

Luego a mi hermana por su apoyo incondicional y por estar ahí siempre a mi lado.

Va dedicado también a mis familiares que de una u otra manera supieron comprenderme en los momentos más difíciles y que con su apoyo y comprensión e salido a delante.

Emma.

ÍNDICE CONTENIDO

CONTENIDO ***PÁGINAS***

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

ÍNDICE DE TABLAS

CONTENIDO ***PÁGINAS***

ÍNDICE DE GRÁFICOS

CONTENIDO ***PÁGINAS***

RESUMEN

Hoy en día las comunicaciones han experimentado un rápido avance y la prueba de ésta es que el mundo está interconectado; protocolos juegan un papel importante en la comunicación y en especial en la recepción de la información enviada. IPv6 es la sexta versión del Protocolo de Internet, es el encargado de dirigir y guiar a los paquetes en la red, está diseñado en los años 70 con el objetivo de las redes de interconexión. Esta nueva versión del Protocolo de Internet está destinado a sustituir el estándar IPv4, al mismo tiempo que tiene una dirección de red de límite de acceso, lo que impide la red cada vez mayor en todo el mundo. Protocolos IPSec operan en el espacio de red del modelo OSI. Otros protocolos de seguridad de Internet de uso generalizado, como SSL, TLS y SSH operan en la capa de transporte (nivel 4 del modelo OSI) hacia arriba. Esto hace que IPSec es más flexible, ya que puede ser utilizado para proteger la capa 4 de protocolos, incluidos protocolos TCP y UDP de capa de transporte utilizado. Una ventaja importante de IPSec contra SSL y otros métodos que operan en las capas superiores, es que una aplicación puede utilizar IPSec no debe realizar ningún cambio, mientras que para el uso de SSL y otros protocolos de más alto nivel, las aplicaciones tienen que ser modificado su código. La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para la construcción de las funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como llaves) que se utiliza para cifrar y autenticar a un flujo particular en una dirección. Por lo tanto, en condiciones normales de flujos bidireccionales de tráfico están asegurados por un par de SA. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) se corresponde con el administrador de IPSec.

ABSTRACT

Nowadays communications have gone through a rapid advance and proof of this one's that the worldwide is interconnected; protocols play an important role in communication and especially in the receipt of information sent. Pv6 is sixth version of the Internet Protocol, it's responsible for directing and guiding packets in the network, it's designed in the 70's with the goal of interconnect networks. This new version of the Internet Protocol is intended to replace the IPv4 standard, at the same time it has an access limit network address, which prevents network increasing worldwide. IPsec protocols operate at the network space of the OSI model. Other Internet security protocols in widespread use, such as SSL, TLS and SSH operate in the transport layer (layer 4 of the OSI model) up. This makes IPsec more flexible, as it can be used to protect layer 4 protocols, including TCP and UDP protocols used transport layer. An important advantage of IPsec against SSL and other methods that operate at higher layers, is that an application can use IPsec shouldn't make any changes, while for using SSL and other higher level protocols, applications have to be modified their code. The IP security architecture uses the concept of security association (SA) as the basis for building security functions into IP. A security association is simply the parcel of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. Thus, in normal traffic bidirectional flows are secured by a pair of SA. The final decision of the encryption and authentication algorithms (from a defined list) corresponds to the IPsec administrator.

INTRODUCCIÓN

El Internet es uno de los servicios que cada día son más utilizados, por lo mismo nos ha dado a la obligación de implementar nuevos mecanismos de seguridad para proteger uno de los recursos más importantes que es la información.

Hoy en día se tienen muchas amenazas sobre nuestra información, por lo que debemos saber cómo evitarlas y garantizar una transferencia segura de información.

Con la gran cantidad de información que se maneja en el área de redes en la actualidad se creó un nuevo protocolo, el IPv6, llamado también Internet 2. El IPv6 trabaja con distintos protocolos uno de ellos IPSec (Internet Protocolo Security) el cual sirve para implementar la seguridad. El IPSec está conformado por un conjunto de algoritmos y protocolos que habilitan un sistema para seleccionar los protocolos de seguridad, determinar los algoritmos a utilizar para cada servicio y colocar las llaves cristalográficas requeridas.

El IPSec está actualmente implementado en IPv4 y con mucha más razón en IPv6, para este último es obligatoria la implementación debido a la gran demanda que va a tener y sobre todo porque con la gran cantidad de información que se maneja a través de este protocolo se va a requerir la mayor cantidad posible. En una red de comunicaciones se encuentra con algunos problemas de seguridad dentro de los cuales son la autenticación, la integridad y la confiabilidad, por lo cual implementar el protocolo IPSec ayuda a resolver algunos de estos problemas.

En el Ecuador las empresas están adoptando nuevos estándares de seguridad ya que por medio del IPSec se puede proteger con seguridad la gran cantidad de

información que manejan a través de internet, en él envió y la recepción de la misma con mayor rapidez.

El IPSec es un estándar (norma) que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP. Los componentes principales de la arquitectura de seguridad IPSec son, protocolo y asociaciones de seguridad, manejo de claves y algoritmos de autenticación y encriptación.

Adicionalmente el IPSec ofrece un conjunto de servicios de seguridad, controles de acceso, donde se previene el uso no autorizado de recursos, integridad sin conexión, cuando se modifica un datagrama IP individual esto lo detecta, la autenticación del origen de los datos, la protección anti replay, esta detecta la integridad de una secuencia parcial, la cual también datagramas IP duplicados, encriptación y encriptación de flujo de tráfico limitado.

Es lógico que en la Empresa ByPas Comunicaciones como una Empresa de telecomunicaciones vaya con el avance de la Tecnología y también implemente este estándar de seguridad como es el IPSec logrando mayor nivel de seguridad para la información de sus clientes.

IPSec ayuda a que las aplicaciones tengan un acceso seguro y transparente, hace del comercio electrónico más seguro, permite tener una red segura principalmente sobre redes públicas, a los tele trabajadores ofrece el mismo nivel de confidencialidad que dispondría en la red local de su empresa.

Proteger la información es una de las tareas más importantes; cuando se utiliza el Internet se vuelve aún más vulnerable por lo que se necesitan mecanismos de seguridad para protegerla y mucho más cuando se trata de información altamente

confidencial o donde se juegan muchos intereses como son los bancos, los colegios o las mismas universidades.

Se necesita implementar seguridades, como también el nuevo protocolo IPv6, el cual trabaja con el protocolo IPSec para implementar seguridad y es obligatorio en él. El IPSec está formado por un conjunto de protocolos y algoritmos, que se adaptan a cada caso, pudiendo determinar qué protocolo o algoritmo, según el implementador mejor se adapte, es modular, y con esto logra una adaptación al sistema cambiante.

Este trabajo como la Universidad Técnica de Cotopaxi, lo delimita consta de tres capítulos los cuales se describen a continuación.

El capítulo I trata sobre la conceptualización de la seguridad de la información, del IPSec, de los protocolos seguros, del IPv6, como también la seguridad manejada por la capa del modelo OSI, claves de cifrado, cristología y firmas digitales.

En el Capítulo II, se presenta los resultados obtenidos en el trabajo de Campo, a través de la aplicación de la Encuesta a los técnicos, empleados y socios de la empresa ByPas Comunicaciones. Los mismos que se hallan debidamente tabulados y representados mediante gráficos circulares, como también se indica su análisis e interpretación. De igual forma con la respuesta del cuestionario de encuesta se logró la comprobación de la hipótesis.

En el Capítulo III, describe el funcionamiento de IPSec como también beneficios que se adquieren al implementarlo. La infraestructura con el certificado digital y su integración con IPSec. Como también los modos de uso de IPSec y ejemplos

de aplicaciones reales donde se maneja seguridad a base de IPSec, se muestra además un análisis de seguridad sobre el protocolo IPSec en IPv6, conclusiones y recomendaciones finales del trabajo de investigación, las mismas que se obtuvieron sobre la base del trabajo de campo realizado en la empresa ByPas Comunicaciones.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

IPSEC (INTERNET PROTOCOLO SECURITY) EN REDES DE DATOS BASADOS EN IPV6 Y HERRAMIENTAS NECESARIAS PARA EL DESARROLLO DEL SISTEMA.

1. Seguridad y Protocolos de Seguridad.

1.1 Seguridad de la Información

Según, TANENBAUM Andrew S. Redes de Computadoras, 2010 Cuarta Edición, Pearson Educación México, "En su forma más sencilla las seguridades se ocupan de garantizar que los curiosos no puedan leer, o peor aún modificar mensajes dirigidos a otros destinatarios. Tiene que ver con la gente que intenta acceder a servicios remotos no autorizados. Los problemas de seguridad de la información pueden dividirse en términos generales en cuatro áreas interrelacionadas; confidencialidad, autenticación, no repudio y control de integridad". (Pág. 721).

Según el link www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion. Obtenida 13/11/2013. "La seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen".

En base al criterio de las postulantes, podemos manifestar que la seguridad tiene mucho que ver con la confidencialidad y la integridad de la información importante dentro de un departamento de sistemas ya que el objetivo siempre va a ser el almacenamiento de la información y prevenir que no sufran alteración o pérdida alguna, además que siempre se debe tener en cuenta quienes son los empleados que pueden atentar contra la información de la empresa, hay que tomar medidas como las planteadas para proteger toda esta información.

1.2 IPSec

Según, TANENBAUM Andrew S. Redes de Computadoras, 2010 Cuarta Edición, Pearson Educación México, "El IPSec son descritos en el RFC 2401, 2402, 2406, pero no todos los usuarios desean cifrar por lo costoso, pero en lugar de hacerle opcional, se decidió requerir cifrado todo el tiempo pero permitir el uso de un algoritmo nulo. El diseño de una IPSec completo es una estructura para servicios, algoritmo y granularidades múltiples. Un aspecto ligeramente sorprendente de IPSec es que aunque se encuentra en la capa IP, es orientada a la conexión. En la actualidad esto no es tan sorprendente porque para tener seguridad se debe establecer y utilizar una clave por algún periodo, en esencia un tipo de conexión". (Pag.772).

Según, FRANCISCONI Hugo Adrián, IPSec en Ambiente IPv4 e IPv6 primera edición, Agosto 2005, ISBN 987-43.9727-6, Impreso por carril Godoy Cruz, Argentina, "IPSec proporciona servicios de seguridad en la capa IP permitiendo a un sistema seleccionar los protocolos de seguridad, determinar el/los algoritmo/s a utilizar para el/los servicio/s, e implementar cualquier algoritmo criptográfico requerido para proporcionar los servicios solicitados. IPSec se puede utilizar para proteger una o más "trayectorias" entre un par de hosts, o entre un par de security gateway, o entre un security gateway y un host. El término security gateway se utiliza en este documento para referirse a un sistema intermedio que implementa los protocolos IPSec. Por ejemplo, un router o un firewall implementando IPSec es un security gateway." (Pág. 132).

Según, http://www.ipsec-howto.org/spanish/x161.html, obtenida el 12/11/2013, "IPSec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4".

Según el criterio de las investigadoras, IPSec es una de las características que tienen los protocolos cuya función principal es de tener seguridad de la información que se envía y se recibe a través de los protocolos de internet.

1.3 Seguridad de la red

Según RAYA José Luis, TCP/IP para Windows server, Editorial Alfaomega, Impreso Colombia, 2006, "IPSec se incrementa a nivel del de la OSI y activa un nivel alto de protección no siendo necesario realizar ningún cambio de las aplicaciones existentes". (Pág. 300).

Según en link, http://www.iec.csic.es/criptonomicon/linux/introsegred.html, obtenida 12/11/2013. “La seguridad de las conexiones en red merecen en la actualidad una atención especial, incluso por medios de comunicación no especializados, por el impacto que representan los fallos ante la opinión pública”.

En base al criterio de las postulantes, la seguridad de la red proporciona protección y asegura la comunicación entre los protocolos.

1.4 Red de Computadoras

Según, TANENBAUM Andrew S. Redes de Computadoras, 2010 Cuarta Edición, Pearson Educación México, “Es la forma de designar a un conjunto de computadoras autónomas interconectadas. Se dice que dos computadoras están interconectadas si pueden intercambiar información. No es necesario que la conexión se realice mediante el cable de cobre; también se pueden utilizar las fibras ópticas, las microondas, los rayos infrarrojos y los satélites de comunicación. Las redes tienen varios tamaños, formas y figuras”. (Pág. 2).

Según, en link http://definicion.de/red-de-datos/, obtenida el 15/11/2013, “Se conoce como red de datos a la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes ha sido diseñada específicamente para satisfacer sus objetivos, con una arquitectura determinada para facilitar el intercambio de los contenidos”.

En base al criterio de las postulantes, Una red de computadoras es la forma como se comunican dos o más dispositivos electrónicos como computadores, celulares,

tablets, aunque los medios no tienen mayor importancia ya que en la actualidad lo que se trata siempre es de poder pasar información de un extremo a otro.

1.5 Protocolos

Según, COMER Douglas E, Redes Globales de Información con Internet y TCP/IP, Tercera Edición, 2009, Prentice Hall Hispanoamericana ISBN 968-880-541-6, "Son aquellos que proporcionan las reglas para las comunicaciones, contienen los detalles referentes a los formatos de los mensajes, describen cómo responde una computadora cuando llega un mensaje y especifican de qué manera una computadora maneja un error u otras condiciones anormales. Un aspecto importante es que permite reflexionar sobre las comunicaciones por computadora de manera independiente de cualquier hardware de red de cualquier marca. El hacer a un lado los detalles de bajo nivel de la comunicación nos ayuda a mejorar la productividad de muchas maneras". (Pág. 3).

Basadas en el Link: http://www.desarrolloweb.com/articulos/protocolos-red.html, obtenida el 08/11/2013, "Los protocolos son las reglas que rigen la comunicación dentro de una red, y para que haya comunicación entre dos host, por ejemplo, se requieren muchos protocolos. A este conjunto de protocolos necesarios se les llama suite de protocolos y están implementados en cada dispositivo perteneciente a la red".

En lo referente a los protocolos, podemos decir que son creados para las comunicaciones dentro de una red, para que todas las computadoras se puedan conectarse en todo el mundo a través del Internet, es necesario que tenga instalado este protocolo de comunicación.

1.6 Modelo OSI

Según RAYA José Luis, TCP/IP para Windows server, Editorial Alfaomega, Impreso Colombia, 2006, "Cuya actividad empezó a desarrollar en 1977 y llegó a construirse como estándar internacional en 1983, trata de establecer las bases para la definición de protocolos de comunicación entre sistemas informáticos.

Propone dividir en niveles todas las tareas que se llevan a cabo en una comunicación entre computadoras. Todos los niveles estarían bien definidos y no interferían con los demás. De ese modo si fuera necesario una corrección o modificación en un nivel, no afectaría al resto.

TABLA Nº 1.1

Niveles Del Modelo OSI

NIVEL	**FUNCIÓN**
7. Aplicación	Datos normalizados
6. Presentación	Interpretación de los datos
5. Sesión	Diálogos de control
4. Transporte	Integridad de los mensajes
3. Red	Encaminamiento
2. Enlace de datos	Detección de errores
1. Físico	Conexión de equipos

Fuente: RAYA José Luis, TCP/IP para Windows server

Realizado por: Grupo de investigación

En total se formarían siete niveles (los cuatro primeros tendrían la función de comunicación y los tres restantes de proceso) cada uno de los siete niveles dispondrían de los protocolos específicos para el control de dicho nivel". (Pág. 12)

Según el link, http://belarmino.galeon.com/, obtenida el 15/11/2013, "El Modelo OSI divide en 7 capas el proceso de transmisión de la información entre equipo informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global.

El modelo OSI abarca una serie de eventos importantes:

- El modo en que los datos se traducen a un formato apropiado para la arquitectura de red que se está utilizando
- El modo en que las computadoras u otro tipo de dispositivo de la red se comunican. Cuando se envíen datos tiene que existir algún tipo de mecanismo que proporcione un canal de comunicación entre el remitente y el destinatario.
- El modo en que los datos se transmiten entre los distintos dispositivos y la forma en que se resuelve la secuenciación y comprobación de errores
- El modo en que el direccionamiento lógico de los paquetes pasa a convertirse en el direccionamiento físico que proporciona la red".

En base al criterio de las postulantes, el Modelo OSI se basa en siete capas cada una de ellas con una funcionalidad específica cada capa y se encarga de ejecutar una determinada parte del proceso global.

1.7 Direccionamiento IP (Internet Protocol)

Según, GARCIA TOMAS Jesús, RAYA CABRERA José Luis, RAYA Víctor Rodrigo, Alta velocidad y Calidad de servicio en redes IP, 2002, ALFAYOMEGA Grupo Editor, México, "El protocolo IP (Internet Protocol) siempre trabaja con entregas de datagramas (sin conexión previa) que viajan de extremo a extremo de la red. No obstante, la red realiza su mejor esfuerzo para

intentar que los datagramas IP alcancen su destino. Este protocolo se encarga de seleccionar la trayectoria a seguir por los datagramas, es decir por donde se deben encaminar los datagramas salientes pudiendo llevar a cabo labores de fragmentación y re ensamblado". (Pág. 353 .354).

Según el link, http://www.marbit.es/index_ip.html, obtenida el 15/11/2013, "Una dirección IP es un número de identificación de un ordenador o de una red o (subred) – depende de la máscara que se utiliza. Dirección IP es una secuencia de unos y ceros de 32 bits expresada en cuatro octetos (4 byte) separados por puntos".

Como podemos ver, el direccionamiento IP permite conectarse a una red de internet para así comunicarse entre computadoras que utilizan diferentes sistemas operativos.

1.8 IPV6 (Protocolo de Internet versión 6)

MERIKE Kaeo, Diseño de Seguridades en redes, 2003, Impreso en España, Editorial CISCO Press, "El protocolo IP continua evolucionando, adaptándose a los requerimientos de una red en rápido crecimiento. La última versión de IP, denominada IPv6 y también IPng (IP de next generation), propone que el campo de cada dirección tenga 64bits (128 en total) de forma que pueda solucionarse el principal problema que tienen las redes IP: el agotamiento de las direcciones IP."

Las funciones más importantes que se están implementando en la actualidad son:

- **Multicast:** Las direcciones multicast (Clase D) están habilitadas para que un usuario de la red pueda enviar sus datagramas a un conjunto de usuarios que han sido configurados como miembros de un grupo multicast de varias subredes.

Un grupo multicast puede estar formado por cualquier conjunto de máquinas puede formar parte de uno o más grupos multicast en cualquier momento y no tiene que pertenecer a un grupo para enviar mensajes a miembros de un grupo.

- **RSVP:** es un protocolo de reserva de recursos para aquellas aplicaciones que requieran un ancho de banda preestablecido y asegurado como las comunicaciones de voz y la videoconferencia. Ésta especialmente indicada para aplicaciones multimedia". (Pág. 283-284).

Según, TANENBAUM Andrew S. Redes de Computadoras, 2010 Cuarta Edición, Pearson Educación México, "Por principio, y lo más importante, el IPv6 tiene direcciones más grandes que el IPv4; son de 16 bytes de longitud, lo que resuelve el problema que se buscaba resolver: proporcionar una cantidad prácticamente ilimitada de direcciones de internet. La simplificación del encabezado, que contiene solo 7 campos contra los 13 de IPv4. Este cambio permite a los enrutadores procesar con mayor rapidez los paquetes y mejorar la velocidad real de transporte. Mejor apoyo de opciones cambio que se lo hizo con un nuevo encabezado, pues campos que antes eran obligatorios ahora son opcionales, consiguiendo con esto que los enrutadores solo tomen en cuenta a los paquetes que son enviados a ellos." (Pag.464-465).

Según el link, http://es.kioskea.net/contents/268-protocolo-ipv6, obtenida el 08/11/2013, "El protocolo IPv6 responde razonablemente a los objetivos fijados. Conserva las mejores funciones de IPv4, mientras que elimina o minimiza las peores y agrega nuevas cuando es necesario.

En general, IPv6 no es compatible con IPv4, pero es compatible con todos los demás protocolos de Internet, incluyendo TCP, UDP, ICMP, IGMP, OSPF, BGP y DNS. A veces se requieren modificaciones mínimas (particularmente, cuando se trabaja con direcciones extensas)".

En base al criterio de las postulantes, el IPv6 es una nueva versión que supera al IPv4 ya que el IPv6 es de mayor capacidad, velocidad y brinda mayor seguridad.

1.8.1 Direccionamiento IPv6

Según COMER Douglas E, Redes Globales de Información con Internet y TCP/IP, Tercera Edición, 2009, Prentice Hall Hispanoamericana ISBN 968-880-541-6. "El amplio espacio de direcciones garantiza que el IPv6 puede tolerar cualquier esquema de asignación de direcciones razonable. De hecho, si los diseñadores deciden cambiar el esquema de direccionamiento más tarde, el espacio de direcciones es lo suficientemente extenso como para adaptarse a una re asignación. Es difícil comprender el tamaño del espacio de direcciones IPv6. Una forma de entenderlo es relacionando la magnitud con el tamaño de la población: el espacio de direcciones es tan grande que cada persona en el plantea puede tener direcciones suficientes como para poseer una red de redes tan grande como el internet actual. Un entero de 16 octetos puede manejar 2 exp 128 valores. Así el espacio de direcciones es mayor que 3.4 X 10exp 38. Si las direcciones se

asignaran a razón de un millón de direcciones por milisegundo, tomaría alrededor de 20 años asignar todas las direcciones posibles". (Pág. 510, 511,512).

Según el link,
http://ipv6nuevastecredes.wikispaces.com/6.+DIRECCIONES+Y+DIRECCIONAMIENTO+IPV6, obtenida el 08/11/2013, "La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo IPv6.

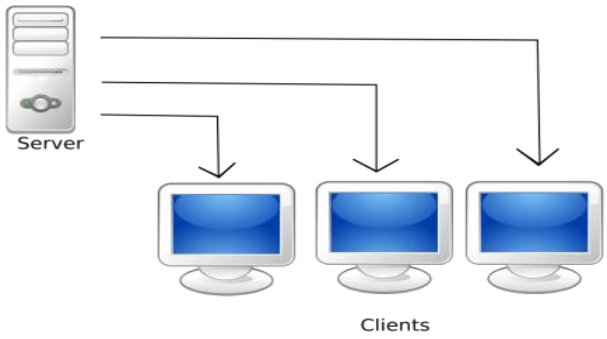
Según el criterio de las tesistas, el direccionamiento del IPv6 nos dice que son diseñadores que nos permiten cambiar un esquema para dar direccionamiento y tener un espacio suficientemente extenso dentro de una red.

1.8.2 Tipos de Direcciones en IPv6

Unicast:

Identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Este tipo de direcciones son bastante conocidas. Un paquete que se envía a una dirección unicast debería llegar a la interfaz identificada por dicha dirección.

Gráfico Nº 1.1: Representación gráfica del Unicast



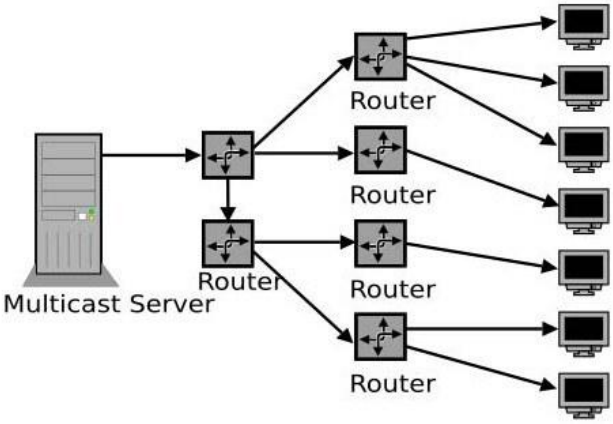
Fuente: http://naghieli.wordpress.com/about/

Realizado: Grupo de Investigación

Multicast:

Las direcciones multicast identifican un grupo de interfaces. Un paquete destinado a una dirección multicast llega a todos los interfaces que se encuentran agrupados bajo dicha dirección.

Gráfico Nº 1.2: Representación gráfica del Multicast



Fuente: http://naghieli.wordpress.com/about/

Realizado: Grupo de Investigación

Anycast:

Las direcciones anycast son sintácticamente indistinguibles de las direcciones unicast pero sirven para identificar a un conjunto de interfaces. Un paquete destinado a una dirección anycast llega a la interfaz "más cercana" (en términos de métrica de "routers"). Las direcciones anycast sólo se pueden utilizar en "routers"".

Para la opinión de las postulantes el direccionamiento IPv6 es mayor su capacidad de rendimiento ya que es cuatro veces que el tamaño de una dirección IPv4 y esta dirección IPv6 trabaja con hexadecimales y también que el multicast trabaja con un campo de 4 bits que se usa para indicar el tipo de ámbito al que pertenece la dirección

1.9 Clave de cifrado

Según el link, http://comohaceresto.info/951030, obtenida el 12/11/2013, "El cifrado es un concepto que se ha convertido en algo común con la proliferación de redes inalámbricas en casa, donde uno quiere mantener la información sea entendida por todos. En realidad, el cifrado ha existido durante siglos. Uno de los primeros ejemplos es el cifrado César, el nombre de Julio César. Este proceso de cifrado de sustitución tenía una persona tomar el alfabeto y cambiar los personajes a través de un cierto número basa apagado de un algoritmo. Por lo tanto, si el resultado era de cinco caracteres a la derecha, una "a" se trataría como "f", "c" a "h", etc. Si bien este algoritmo no esté siendo utilizada, el cifrado de clave pública y privada son dos métodos comúnmente usados ahora".

Según el link http://help.salesforce.com/apex/HTViewHelpDoc?id=security_keys_using_master.htm&language=es, obtenida 13/11/2013, "Los campos que se cifran utilizando campos personalizados cifrados, como el número de la seguridad social o el de una tarjeta de crédito utilizan una clave de cifrado principal para cifrar los datos. Esta clave se asigna automáticamente cuando activa los campos cifrados en su organización. Puede gestionar la clave principal basada en las necesidades de configuración de su organización y en sus necesidades regulatorias".

Podríamos decir que, la clave de cifrado es una secuencia de números o letras mediante la cual se transforma el texto plano en texto cifrado y así se puede proteger a la información para que no sea jaqueada.

1.10 Criptografía

TANENBAUM Andrew S. Redes de Computadoras, 2010 Cuarta Edición, Pearson Educación México, "Hasta las llegadas de las computadoras, una de las principales restricciones de la criptografía había sido la capacidad del encargado de la codificación para realizar las transformaciones necesarias con frecuencia en un campo de batalla con poco equipo. Una restricción adicional ha sido la dificultad de cambiar rápidamente de un método de criptografía a otro, debido a que esto implica volver a capacitar a una gran cantidad de personas". (Pag.724).

Basados en el Link: http://www.informatica-hoy.com.ar/seguridad-informatica/Criptografia.php, obtenida el 15/11/2013, "La criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la

escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto".

En base al criterio de las postulantes, La criptografía es importante ya que con la era digital y las computadoras todos tendemos a adoptar una técnica de encriptar la información y así poder mantener la privacidad y confidencialidad de la información por ejemplo en nuestros correos.

1.12 Criptosistemas

Basadas en el Link:

http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node306.html, obtenida el 15/11/2013, "Cuando el emisor emite un texto en claro, que es tratado por un cifrado con la ayuda de una cierta clave, creando un texto cifrado (criptograma). Este criptograma llega al descifrador a través de un canal de comunicaciones, como una red y este convierte el criptograma de nuevo en texto claro, apoyándose ahora en otra clave, esta clave puede o no ser la misma que la utilizada para cifrar.

Es obvio, a la vista de lo expuesto anteriormente, que el elemento más importante de todo el criptosistema es el cifrado, que ha de utilizar el algoritmo de cifrado para convertir el texto claro en un criptograma. Usualmente, para hacer esto, el cifrado depende de un parámetro exterior, llamado clave de cifrado (o de descifrado, si hablamos del descifrador) que es aplicado a una función matemática

irreversible, al menos, computacionalmente, no es posible invertir la función a no ser que se disponga de la clave de descifrado.

De esta forma, cualquier conocedor de la clave y por supuesto, de la función, será capaz de descifrar el criptograma, y nadie que no conozca dicha clave puede ser capaz del descifrado, aún en el caso de que se conozca la función utilizada.

La gran clasificación de los sistemas de criptografía se hace en función de la disponibilidad de la clave de cifrado/descifrado. Existen, por tanto, dos grandes grupos de criptosistemas:

- Criptosistemas de clave pública o asimétricos
- Criptosistemas de clave secreta o simétricos."

Según el link, http://cv.uoc.edu/~mat/cursoWeb/material/UW_90072_00000/web/main/m2/v3_1.html, obtenida el 15/11/2013, "Una cifra o criptosistema es un método secreto de escritura, mediante el cual un texto en claro se transforma en un texto cifrado o criptograma. El proceso de transformar un texto en claro en texto cifrado se denomina cifrado, y el proceso inverso, es decir la transformación del texto cifrado en texto en claro, se denomina descifrado. Ambos procesos son controlados por una o más claves criptográficas".

Para la opinión de las postulantes, Criptosistemas ayuda al emisor y receptor a compartir una única clave, es decir que el receptor podrá descifrar el mensaje recibido si y solo si conoce la clave con la cual el emisor ha cifrado el mensaje.

1.13 Certificado Digital

Según, TANENBAUM Andrew S., Redes de Computadoras, 2010 Cuarta Edición, Pearson Educación México, "La autenticidad de muchos documentos legales, financieros y de otros tipos se determina por la presencia o ausencia de un certificado digital autorizado. Las fotocopias no cuentan. Para que los sistemas de mensajes computarizados reemplacen el transporte físico de papel y tinta, debe encontrarse un método para que el certificado de los documentos sea infalsificable. (Pag.464-465).

Disponible en web, http://www.certsuperior.com/FirmasDigitales.aspx, obtenida el 15/11/2013, "La autenticidad de algunos documentos legales y en general, cualquier tipo de documento se determina mediante el uso de la firma manuscrita ya que ni siquiera sirve una fotocopia de la misma. Para que los documentos enviados de forma digital tengan la misma validez que un documento firmado a mano se crea la firma digital. Es un método criptográfico que asocia una identidad ya sea de una persona en particular o de un equipo a un mensaje enviado a través de transmisión por la red. Su uso puede ser diferente dependiendo de lo que queramos hacer con la firma ya que tendremos posibilidad de validar que el documento es emitido por nosotros, expresar conformidad con algún documento de tipo legal como podría ser la firma de un contrato laboral e incluso asegurar que no podrá modificarse el contenido del mensaje. La firma digital nos permitirá tener más seguridad a la hora de emitir un documento de manera íntegra a través de su sitio web. La firma digital es el resultado de aplicar a un documento, en línea, un procedimiento matemático que requiere datos que exclusivamente conoce la persona que firma, encontrándose ésta bajo su absoluto control".

Según el link,
http://www.consumer.es/web/es/tecnologia/internet/2004/01/23/94524.php,
obtenida el 15/11/2013, "El desarrollo de las redes telemáticas y de Internet ha facilitado el intercambio de mensajes de todo tipo, incluidos aquellos de contenido

contractual y administrativo, entre personas distantes geográficamente. La firma digital o electrónica viene a solventar el problema de autentificación de los mismos, ya que equivale, a todos los efectos, a la firma autógrafa, puesto que identifica fehacientemente la autoría del mensaje. Físicamente, la firma digital se basa en la criptografía y puede ser definida como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación de un algoritmo (fórmula matemática) de cifrado asimétricos o de clave pública. Estos sistemas cifran los mensajes mediante la utilización de dos claves diferentes, una privada y otra pública. La privada es conocida únicamente por la persona a quien pertenece el par de claves. La pública, por su parte, puede ser conocida por cualquiera pero no sirve para hallar matemáticamente la clave privada."

En base al criterio de las postulantes, el certificado digital nos ayuda a buscar nuevas maneras de proteger la información en la actualidad con el avance de la tecnología y que sobre todo que se requiera de cifrar la información, como las firmas digitales las mismas que van siendo de gran aporte para los documentos oficiales ya que no se requieren de enviar las firmas fotocopiadas o por empresas de transporte, sino que con un código pueden ser validadas a la distancia.

1.14 El Protocolo TCP/IP

Según RAYA CABRERA José Luis, RAYA Víctor Rodrigo, Amenaza de una red corporativa, ALFAYOMEGA Grupo Editor, México 2010, "Es un protocolo basado en paquetes, que se usa para el intercambio de datos sobre las redes de computadoras. IP gestiona el direccionamiento, la fragmentación, el reensamblado y la desmultiplexión del protocolo. Es la base sobre la que se construyen los demás protocolos IP (lo que colectivamente se denomina paquete de protocolo IP). Como protocolo de la capa de rede, IP maneja la información sobre direccionamiento y controles para permitir que los paquetes de datos se muevan por la red (lo que se suele referir como enrutamiento IP)". (PAG. 128).

En base al link http://es.kioskea.net/contents/281-protocolo-tcp, obtenida el 15/11/2013, "TCP (que significa Protocolo de Control de Transmisión) En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP).

Para el criterio de las postulantes, TCP/IP es un protocolo orientado a conexión es decir nos permite que dos máquinas que están comunicadas controlen el estado de direccionamiento de paquetes de datos que tiene una red.

1.15 Windows Server 2008

Según PÉREZ M, Windows server 2008, instalaciones, configuración y administración, Editorial RC libros, 2009, "Es el Sistema Operativo de servidor Windows más avanzado hasta el momento y cuyo predecesor es Windows server 2003 este nuevo sistema operativo está diseñado para aprovechar plenamente la nueva generación de servicios de redes, aplicaciones y web e incorporar las tecnologías de virtualización y una mayor seguridad y nuevas herramientas web y de administración. Con Windows server 2008 es posible desarrollar y gestionar aplicaciones avanzadas para el usuario, disponer de una infraestructura de red de alta seguridad e incrementar la eficiencia tecnológica y el valor de las tecnologías de información en las organizaciones.". (Pág. 5).

Según MEDIA Active, Aprende Windows 8 Consumer Preview, Editor Alfaomega, Primera edición 2012, Impreso en España, "Es un nombre de un sistema operativo de Microsoft diseñado para servidores. Es el sucesor de Windows server 2003, distribuido al público casi cinco años antes. Al igual que Windows 7, Windows Server 2008, se basa en el núcleo Windows NT 6.1. Entre

los mejores de esta edición, se destacan nuevas funcionalidades para el Active Directory, nuevas prestaciones de virtualización y administración de sistemas, la inclusión de IIS 7.5 y el soporte para más de 256 procesadores". (Pág. 3)

Podemos decir que, Windows server 2008 es una nueva versión que nos ofrece nuevas funciones, presentaciones fáciles de manipular ya que sin duda alguna es un nuevo sistema operativo con muchas ventajas ya que este sistema operativo es para servidores de red.

CAPÍTULO II

DESCRIPCIÓN, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN DE CAMPO

2. La Empresa de Soluciones Tecnológicas para las Telecomunicaciones "ByPas Comunicaciones Cia. Ltda".

2.1 Diseño de la investigación

En la actualidad las empresas de tecnología van ampliando y mejorando su portafolio de productos ya que en este mundo competitivo el que no se actualiza o mejora su calidad en servicios y productos es fácilmente absorbido por la competencia.

La empresa ByPas Comunicaciones, la cual ofrece todo tipo de soluciones en el área de las comunicaciones se ha visto en la necesidad de mejorar todos sus servicios razón por la cual ha creído conveniente aumentar a su staff de empleados un número considerable de profesionales en el área de la telemática y las seguridades principalmente en lo que tiene que ver en el área de comunicaciones ya que en la actualidad existe una gran demanda de personas que conozcan a

fondo sobre el uso y administración de ciertas aplicaciones que estén inmiscuidas en el área.

ByPas Cia. Ltda. Además de las comunicaciones se encuentra ofertando todo tipo de administración de Sistemas Operativos particularmente en lo que tiene que ver con Windows 2008 y 2012 así como clientes basados en Windows 7 y 8 esto porque las empresas consideran importante tercerizar (Outsourcing) la administración de los servidores con el fin de que sus empleados se dediquen a actividades propias del negocio y que se optimice de esta manera.

Las seguridades han ido ganando gran importancia en la actualidad ya que con el aparecimiento de nuevas herramientas informáticas ha hecho que cada día los servidores y los centros de datos se vuelvan vulnerables toda vez que los administradores no cuentan con suficientes seguridades en sus servidores principales, y más cuando sus usuarios exigen por mas principalmente en el uso del internet ya que en este mundo globalizado todos están íntimamente ligados a los correos electrónicos y a las redes sociales.

2.2 Misión

Brindar soluciones tecnológicas en el área de las telecomunicaciones con el más alto soporte técnico – tecnológico con el personal en constante capacitación y con el más variado nivel de conocimiento en distintos productos.

2.3 Visión

Ser la empresa que se encuentre siempre a la vanguardia tecnológica, con empleados con el más alto nivel de responsabilidad y conocimiento siendo un aporte para el desarrollo del buen vivir en el estado Ecuatoriano.

2.4 Metodología de la investigación aplicada

2.4.1 Método Hipotético-Deductivo:

Según ZEA, Leiva: Nociones de Metodología de Investigación Científica, quinta edición, Quito, 2001. "Es el procedimiento o camino que sigue el investigador para hacer de su actividad una práctica científica tiene varios pasos esenciales, la observación del fenómeno a estudiar, creación de una hipótesis, verificación o comprobación de la verdad". (Pág. 102).

Para poder alcanzar el objetivo y cumplir con la hipótesis planteada nosotras nos hemos puesto a realizar un estudio de las seguridades basadas en IPSec para los protocolos de alta disponibilidad basadas en IPv6, se determinará cuál es el área de influencia.

2.4.2 Método Científico:

Según ZEA, Leiva: Nociones de Metodología de Investigación Científica, quinta edición, Quito, 2001. "El método científico es el procedimiento ordenado y lógico seguido para descubrir los conocimientos verdaderos de una ciencia, o sea los medios científicos de que se vale el investigador para llegar a los fine demostrativos que se propuso inicialmente". (Pág. 102).

La utilización de este método es para garantizar que todas las ideas, información y pruebas realizadas en este proyecto de tesis para que puedan ser verificables, y que toda la información solicitada y verificada pueda contribuir a alcanzar las metas de la investigación.

Se va a tomar en cuenta la investigación en base a la falta de una seguridad que permita garantizar la información en un ambiente de trabajo y con protocolos que son nuevos en el área tecnológica como es el caso del IPv6.

Las seguridades no son suficientes cuando de información se trata y con este trataremos de resolver los problemas de seguridades que tiene el protocolo de IPv6.

2.5 Tipos de investigación

2.5.1 Investigación bibliográfica

HERNÁNDEZ Roberto, FERNÁNDEZ Carlos, BASTIDAS Piedad, Metodología de la Investigación, cuarta Edición. "La investigación bibliográfica es aquella etapa de la investigación científica donde se explora qué se ha escrito en la comunidad científica sobre un determinado tema o problema, constituye una excelente introducción a todos los otros tipos de investigación". (Pág. 35).

Este tipo de investigación se utilizó para recopilar información de la tecnología IPSec y demás aspectos que han sido necesarios establecer mediante la revisión de libros, fuentes electrónicas, textos entre otros, esta información debidamente analizada y organizada contribuyeron al desarrollo del trabajo de investigación.

2.5.2 Investigación de campo

HERNÁNDEZ Roberto, FERNÁNDEZ Carlos, BASTIDAS Piedad, Metodología de la Investigación, cuarta Edición, "La investigación de campo es el proceso que, utilizando el método científico, permite obtener nuevos conocimientos en el campo de la realidad social o bien estudiar una situación para diagnosticar necesidades y problemas a efectos de aplicar los conocimientos con fines prácticos". (Pág. 35).

Se realizó mediante visitas a la empresa ByPas Comunicaciones de la Ciudad de Quito, con el fin de poder identificar las causas que trae consigo el no disponer de un sistema de seguridad y protección para la información de la empresa y sus clientes.

2.6 Técnicas de investigación

2.6.1 Encuesta

Según GUTIERREZ, Abraham: Curso de Técnicas de Investigación, Edición Tercera, Editorial serie Didáctica A.G, Quito- Ecuador, 1992, "Es el procedimiento que consiste en preguntar, con ayuda o no de un cuestionario, a un buen número de personas sobre un tema determinado para averiguar la opinión dominante". (Pág. 46)

Las encuestas se realizó a personas conocedores del tema, de los cuales están técnicos en el área de las comunicaciones, empleados y socios de la empresa.

Teniendo como base a 36 personas encuestadas para obtener los siguientes resultados sobre el tema cuyas opiniones interesan a las investigadoras, este se realizó mediante un cuestionario de preguntas.

2.7 Diseño Metodológico

2.7.1 Población

Para el desarrollo de la tesis se enfocara de la siguiente manera a la población:

TABLA Nº 2.1

POBLACIÓN ENCUESTADA A LA EMPRESA BYPAS COMUNICACIONES

INVOLUCRADOS	CANTIDAD
Técnicos de la empresa	10
Empleados de la empresa	20
Socios de la empresa	6
Total	**36**

Fuente: Empresa ByPas comunicaciones

Realizado por: Grupo de investigación

2.7.2 Muestra

En la empresa ByPas comunicaciones de la ciudad de quito, se ha tomado en cuenta a todo el personal que labora en dicha empresa, como también a los Socios de la misma para realizar la encuesta, las cuales se las tomo para la muestra.

2.8 ANÁLISIS DE LOS RESULTADOS DE LA OBSERVACIÓN DEL OBJETO DE ESTUDIO LA INVESTIGACIÓN.

Para el desarrollo del trabajo investigativo se utilizó la técnica de la encuesta que se aplicó a los técnicos, empleados y socios de la empresa ByPas comunicaciones de la ciudad de Quito, con la finalidad de obtener información relevante que satisfaga cada una de las incógnitas planteadas.

ANALISIS DE LOS RESULTADOS DE LAS PREGUNTAS

1.- **¿Ha escuchado Ud. hablar sobre IPSec?**

TABLA Nº 2.2

Escuchó hablar sobre IPSec

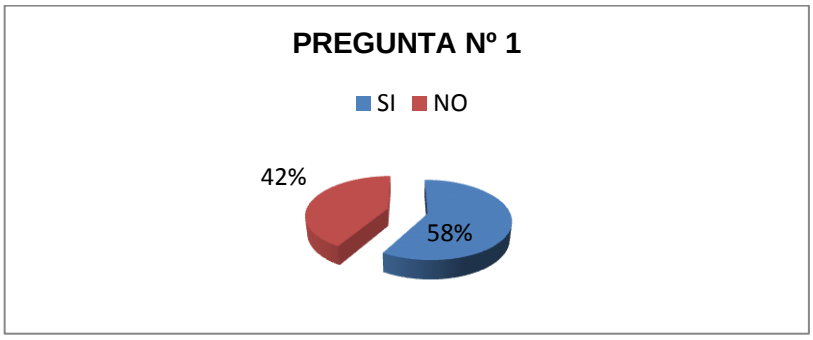
ALTERNATIVAS	F	%
SI	21	58
NO	15	42
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.1

Escucho hablar sobre IPSec



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

Como se puede observar en el grafico la respuesta SI alcanza un 58% y la respuesta NO un 42% de los encuestados, el cual indica que si han escuchado hablar sobre el IPSec y nos damos cuenta que es un tema que está incursionando en el mercado tecnológico.

2.- ¿Cree Ud. que IPv6 cuenta ya con seguridades propias?

TABLA Nº 2.3

Seguridades propias

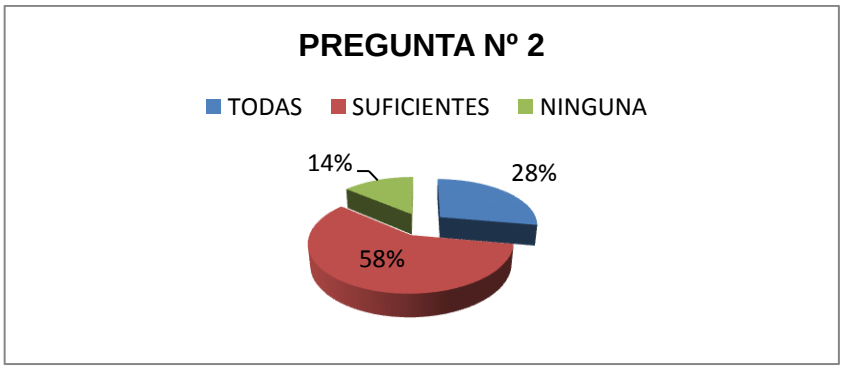
ALTERNATIVAS	**F**	**%**
TODAS	10	28
SUFICIENTES	21	58
NINGUNA	5	14
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.2

Seguridades propias



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

En lo referente a la pregunta el 28% de las personas encuestadas considera que todas las seguridades están en IPv6, el 58% piensa que las seguridades son las suficientes y el 14% considera que no tiene seguridad alguna, lo que indica que falta un poco más de investigación sobre las seguridades que tiene IPv6.

3.- ¿Considera Ud. que es oportuno implementar IPSec en IPv6?

TABLA Nº 2.4

Implementar IPSec en IPv6

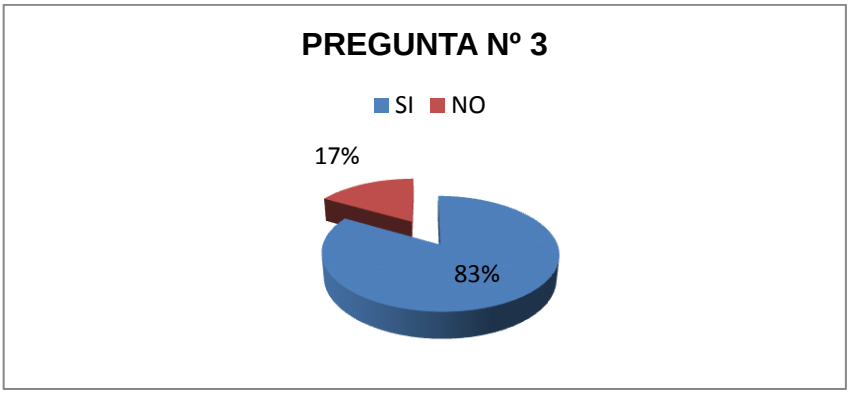
ALTERNATIVAS	F	%
SI	30	83
NO	6	17
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.3

Implementar IPSec en IPv6



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

En esta pregunta los encuestados en un amplio margen que es casi el 83% manifiesta que si es oportuno la implementación del IPSec en IPv6, mientras que un 17% manifiesta que no es todavía oportuna la implementación, con estos resultados nos indican que es factible la implementación para que obtengan más seguridades en la información que manejan.

4.- ¿A través de qué medios Ud. escucho hablar del IPv6?

TABLA Nº 2.5

Escucho hablar del IPv6

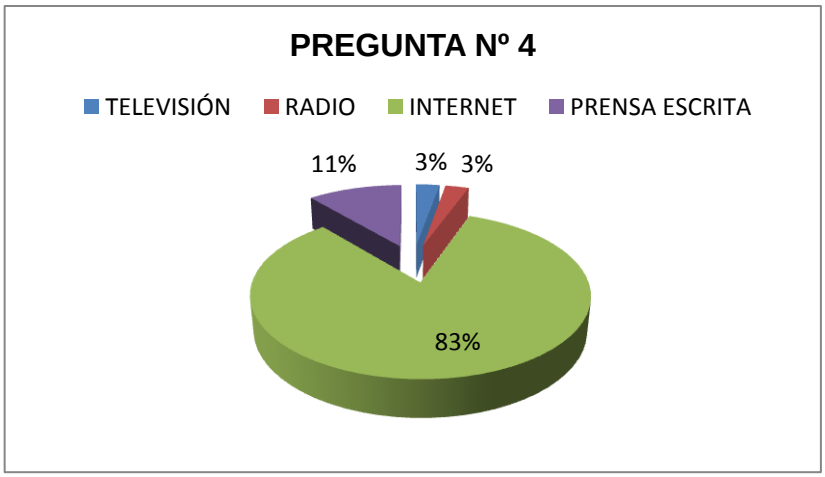
ALTERNATIVAS	F	%
TELEVISIÓN	1	3
RADIO	1	3
INTERNET	30	83
PRENSA ESCRITA	4	11
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.4

Escucho hablar del IPv6



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

El 83% ha visto en internet sobre lo que es el IPv6, mientras que un 11% ha revisado en la prensa escrita como periódicos, mientras que un 3% se ha informado en la televisión y el otro 3% ha escuchado en la radio, todas estas son fuentes de información en nuestro país y se ve que ya se habla de esta nueva tecnología que es importante para tener un poco más de conocimientos sobre el nuevo protocolo.

5.- ¿Considera Ud. que el IPSec es una seguridad que garantiza la información?

TABLA Nº 2.6

Seguridad que garantiza la información

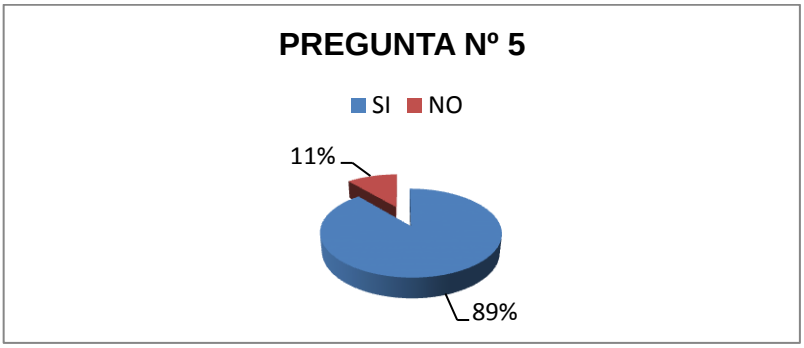
ALTERNATIVAS	**F**	**%**
SI	32	89
NO	4	11
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.5

Seguridad que garantiza la información



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

De los encuestados el 89% de personas está seguro de que el IPSec es una seguridad que presta garantías a la integridad de la información, mientras que el 11% piensa que no es prenda de garantía para la seguridad de la información, por lo que nos da a entender que es importante la implementación para poder confirmar las seguridades que tiene este protocolo de seguridad.

6.- ¿Conoce Ud. bajo qué plataforma tecnológica es más notoria la implementación de IPSec?

TABLA Nº 2.7

Implementación de IPSec

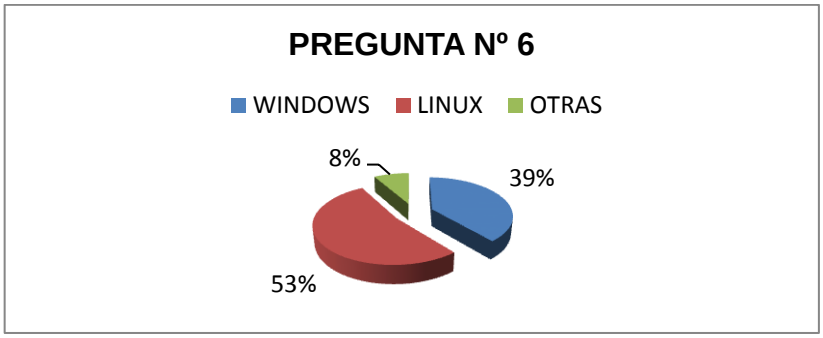
ALTERNATIVAS	**F**	**%**
WINDOWS	14	39
LINUX	19	53
OTRAS	3	8
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.6

Implementación de IPSec



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

Se puede observar según el grafico que el 53% de los encuestados piensa que Linux es más notorio en la implementación de protocolos de seguridad, un 39% piensa que Windows es más notorio, y el 8% considera que existen otras plataformas que pueden ser mejores para este tema, nos da a entender que la mejor plataforma en la que es más notorio la implementación del IPSec es en Linux ya que es un sistema operativo de software libre y que se puede obtener con facilidad.

7.- ¿Sabe Ud. de páginas web que ya tengan IPv6?

TABLA Nº 2.8

Páginas web que tengan IPv6

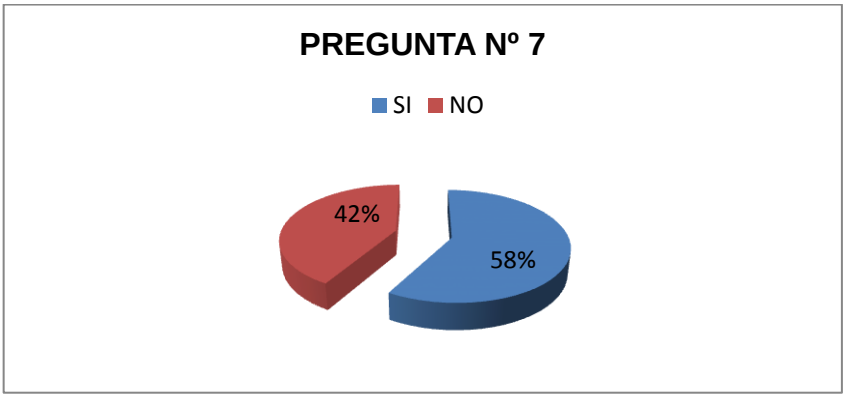
ALTERNATIVAS	F	%
SI	21	58
NO	15	42
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.7

Páginas web que ya tengan IPv6



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

El 58% de las personas encuestadas manifiestas que conoce sobre algunas páginas web que ya tienen con IPv6, mientras que el 42% de los encuestados dicen que desconoce de páginas web que tengan este servicio con IPv6, lo que indica que si conocen sobre páginas web con este nuevo protocolo ya que debe de ser más rápido en su velocidad y capacidad al utilizarlo.

8.- ¿Sabe Ud. cuantas empresas tienen IPv6 en el Ecuador?

TABLA Nº 2.9

Empresas que tienen IPv6 en el Ecuador

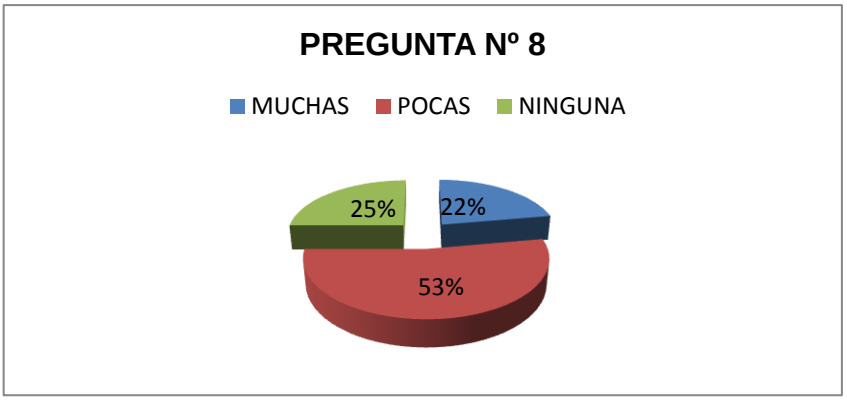
ALTERNATIVAS	F	%
MUCHAS	8	22
POCAS	19	53
NINGUNA	9	25
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº2.8

Empresas que tienen IPv6 en el Ecuador



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

En esta pregunta el 25% de las personas encuestadas manifiestan que en Ecuador muchas empresas o instituciones tienen ya IPv6, mientras que el 53% de los encuestados son pocas las que tienen IPv6 dentro de sus configuraciones, un 25% de los encuestados coincide que ninguna todavía tiene el IPv6, por lo tanto nos damos en cuenta que todavía desconoce un poco del tema.

9- ¿Cree Ud. que el IPSec del IPv6 es mejor que el de su antecesor?

TABLA Nº2.10

El IPSec del IPv6 es mejor que el de su antecesor

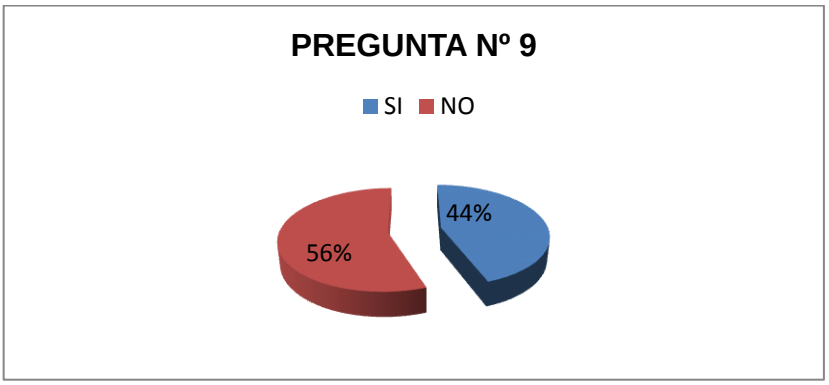
ALTERNATIVAS	**F**	**%**
SI	16	44
NO	20	56
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 9

El IPSec del IPv6 es mejor que el de su antecesor



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

Como se puede observar el 56% de las personas encuestadas considera que el IPSec del IPv6 es mejor que el de IPv4, mientras que el 44% de los encuestados dicen que el de IPv4 ha sido mejor, por lo que nos indica que es importante conocer un poco más sobre lo que es el IPv6.

10.- ¿Maneja ya bien Ud. el tema de direccionamiento IPv6?

TABLA Nº 2.11

Direccionamiento IPv6

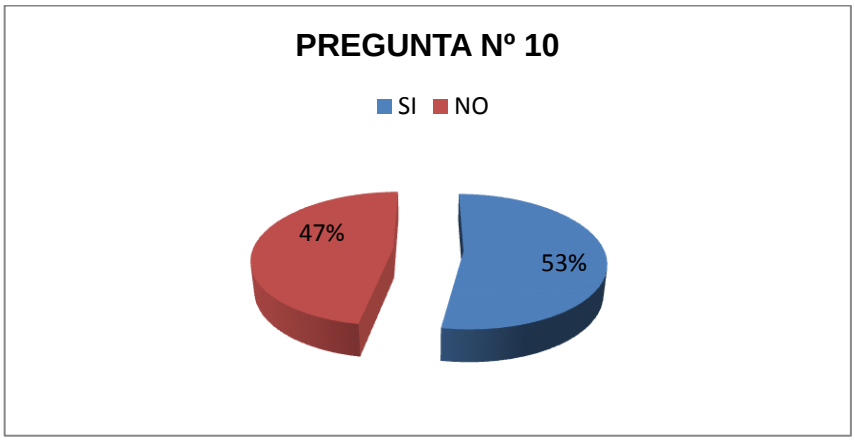
ALTERNATIVAS	F	%
SI	19	53
NO	17	47
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.10

Direccionamiento IPv6



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

Un 53% de los encuestados considera que si maneja de mejor manera el direccionamiento IPv6, mientras que por otra parte el 47% de los encuestados desconoce la forma de administración, ya que nos demuestran que un parte de la mayoría de los encuestados si está manejando este nuevo protocolo.

11.- ¿Qué dispositivos conoce Ud. que tienen seguridades para lo que es IPv6?

TABLA Nº 2.12

Seguridades para lo que es IPv6

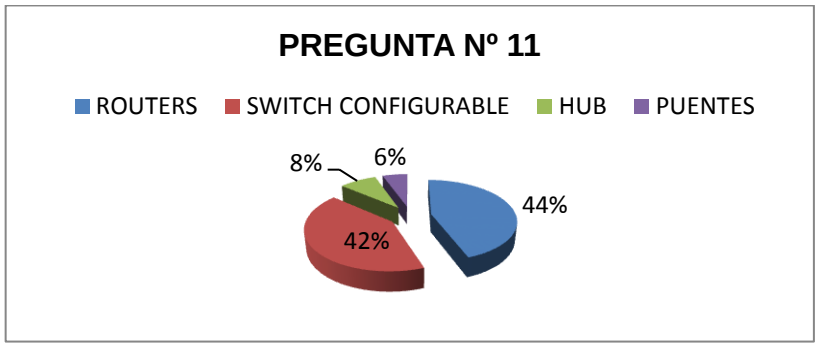
ALTERNATIVAS	**F**	**%**
ROUTERS	16	44
SWITCH CONFIGURABLE	15	42
HUB	3	8
PUENTES	2	6
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.11

Seguridades para lo que es IPv6



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

En esta pregunta el 44% de las personas encuestadas considera que los routers tienen seguridades en IPv6, el 42%de los encuestados un switch configurable, por otra parte el 8%, de los encuestados dicen que el hub, mientras que en un 6% los puentes tienen seguridades en IPv6, por lo que es necesario el routers para poder tener una conexión de red segura para poder enviar y recibir información.

12.- ¿Cree Ud. que las redes de datos están más seguras bajo una clave cifrada?

TABLA Nº 2.13

Bajo una clave cifrada

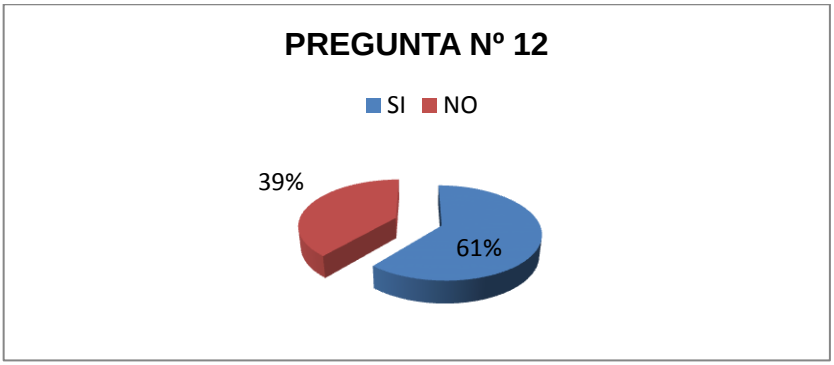
ALTERNATIVAS	F	%
SI	22	61
NO	14	39
TOTAL:	**36**	**100%**

Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

GRÁFICO Nº 2.12

Bajo una clave cifrada



Fuente: Técnicos, empleados y socios de la empresa

Realizado por: Grupo de investigación

Análisis e Interpretación

Según el grafico se puede observar que un 61% dice que si están más seguros los datos bajo una clave cifrada y un 39% que no están seguros, entonces se consideramos que si es necesario que se establezca la clave cifrada para las redes de datos.

2.9 Comprobación de la Hipótesis

Dentro de la Investigación científica la comprobación de la hipótesis se la realiza en base la determinación del cumplimiento parcial o total de los objetivos planteados o el reforzamiento de los mismos. Dicho de otra manera en el presente proyecto se pudo comprobar parcialmente la hipótesis toda vez que los protocolos de internet basados en la versión 6 todavía se encuentran en una fase de pruebas, por lo que las comunicaciones todavía son iniciales, y se desconoce de muchas seguridades principalmente por los sistemas operativos de código libre los cuales no soportan algunas medidas de seguridad basadas en estos estándares, la metodología de investigación científica nos aportó de igual manera datos relacionados a la aplicación de encuestas que fueron de aporte para la documentación del proyecto. En otras instancias se trató con la investigación experimental ya que se tenía dos maneras de presentar las configuraciones para IPSec que son mediante dispositivos de enrutamiento o de concentración y la segunda mediante servidores lo que se optó por la segunda al ser de menor costo y de mayor utilización, ya que en la actualidad existen dispositivos que se dedican a realizar este tipo de actividades.

TABLA Nº 14
VERIFICACIÓN DE LA HIPÓTESIS DE ACUERDO A LOS RESULTADOS OBTENIDOS

ALTERNATIVA	PREGUNTA 1	PREGUNTA 2	PREGUNTA 3	PREGUNTA 4	PREGUNTA 5	PREGUNTA 6	PREGUNTA 7	PREGUNTA 8	PREGUNTA 9	PREGUNTA 10	PREGUNTA 11	PREGUNTA 12
Si	58%		83%		89%		58%		44%	53%		61%
No	42%		17%		11%		42%		56%	47%		39%
Todas		28%										
Suficientes		58%										
Ninguna		14%										
Televisión				3%								
Radio				3%								
Internet				83%								
Prensa Escrita				11%								
Windows						39%						
Linux						53%						
Otras						8%						
Muchas								22%				
Pocas								53%				
Ninguna								25%				
Routers											44%	
Switch configurable											42%	
Hub											8%	

CAPÍTULO III

ANÁLISIS E IMPLEMENTACIÓN DEL PROTOCOLO DE SEGURIDAD IPSEC (INTERNET PROTOCOLO SECURITY) EN REDES DE DATOS BASADAS EN IPV6, ESTABLECIENDO CLAVES DE CIFRADO EN LA EMPRESA BYPAS COMUNICACIONES DE LA CIUDAD DE QUITO

3 Propuesta

3.1 Presentación

El Internet es un servicio cada día más utilizado, por lo mismo nos ha dado a la obligación de implementar nuevos mecanismos de seguridad para proteger uno de los recursos más importantes en él, la información.

Hoy en día existen muchas amenazas sobre nuestra información, por lo que debemos saber cómo evitarlas y asegurar una transferencia segura de información.

Dado la gran cantidad de información que se maneja en la actualidad se creó un nuevo protocolo, el IPv6, llamado también Internet 2. El IPv6 trabaja con distintos protocolos uno de ellos IPSec el cual sirve para implementar la seguridad.

El IPSec está formado por un conjunto de protocolos y algoritmos que habilitan un sistema para seleccionar los protocolos de seguridad requeridos, determinar los algoritmos a utilizar para cada servicio y colocar las llaves criptográficas requeridas.

El IPSec está actualmente implementado en IPv4 y en IPv6, para este último es obligatoria la implementación. En una red de comunicaciones nos encontramos con diferentes problemas de seguridad dentro de ellos cabe destacar la autenticación, la integridad, el repudio y la confiabilidad, por lo cual implementar el protocolo IPSec resuelve estos problemas.

El IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP. Los componentes principales de la arquitectura de seguridad IPSec son, protocolo de seguridad, asociaciones de seguridad, manejo de clave y algoritmos de autenticación y encriptación.

Además IPSec ofrece un conjunto de servicios de seguridad, control de acceso, donde en él se previene el uso no autorizado de recursos, integridad sin conexión, cuando se modifica un datagrama IP individual esto lo detecta, autenticación del origen de los datos, protección antireplay, este detecta la integridad de una secuencia parcial, como también datagramas IP duplicados, encriptación y encriptación de flujo de tráfico limitado.

IPSec posibilita a las aplicaciones un acceso seguro y transparente, hace el comercio electrónico más seguro, permite tener una red segura sobre redes

públicas, a los tele trabajadores ofrece el mismo nivel de confidencialidad que dispondría en la red local de una empresa.

3.2 Justificación

En la actualidad asegurar la información y las comunicaciones es un reto que ha empezado en todo el mundo principalmente porque día con día se ve que los usuarios investigan de mejor manera las nuevas técnicas de hacker y cracker la información de las empresas y las instituciones públicas y privadas tratando de sacar provecho de la información y las comunicaciones.

ByPas una joven empresa en el sector tecnológico, ha creído conveniente ocupar sus recursos tecnológicos y humanos en el desarrollo de nuevas tecnologías toda vez, que el protocolo de comunicaciones IPv6 va revolucionando el mercado en la actualidad. En todo lo que tiene que ver a seguridades la empresa se maneja a través de dispositivos tales como router, switch, y equipos de firewall en hardware, ya que en la empresa lo que si requiere es tener un certificado digital, ya que esta garantiza la información dentro de la empresa, hay que tener en cuenta que para realizar administración de servidores en IPv6 la empresa utiliza la metodología basada en IPv4 to IPv6**,** que en servidores se los puede configurar pero que en algunos servicios solamente funcionan o el un protocolo o el otro protocolo ya que de esta manera se estaría garantizando que todas las funciones se cumplan.

IPSec en el nuevo protocolo IPv6 es una prenda de garantía toda vez que esta forma de seguridades en el IPv4 fue de gran éxito por lo que en IPv6 viene formando parte integral del mismo. El IPSec se encarga de encriptar la

información que se envió desde una computadora hacia otra pasando siempre por un concentrador de información como son los dispositivos de enlace de datos.

El IPSec al ser un protocolo de seguridades que trabaja en la capa 3 del modelo de referencia OSI (capa de RED), por lo que una buena reestructuración de la red con dispositivo de concentración y de enlace de datos que cumpla con estas características cumplen para poder trasladar la información así como las aplicaciones SSL, SSH, VSH, entre otras que cumplen con la planificación realizada.

Los IPSec tienen por concepto la utilización de la asociación de seguridad como base para construir las seguridades en el paquete de algoritmos y parámetros, que buscan enrutar en el flujo de transportes de paquetes. El tráfico de la información se lo hace en forma bidireccional, los flujos de la información en las asociaciones de la seguridad.

Para el soporte del protocolo de IPSec está dado por la implementación del núcleo con la administración de las claves y la negociación de ISAKML/IKE, la nueva arquitectura de procesamiento de red, incluyendo procesamiento de multinucleo con cifrados íntegros, han cambiado la forma en que las IPSec son diseñadas.

Hoy en día los IPSec es una parte indispensable de IPv6 en cambio en el IPv4 es un paquete opcional. De igual manera fue planificado para proporcionar seguridad en el modo de transporte dentro de las capas del modelo OSI el cual lleva el flujo de la información de punto a punto, en modo de túnel.

3.3 Objetivos

3.3.1 Objetivo General

Analizar e Implementar el Protocolo de seguridad IPSec (Internet protocolo Security) en redes de datos basadas en IPv6, estableciendo claves de cifrado para garantizar la información que se genera en los servidores de la empresa ByPas Comunicaciones de la ciudad de Quito

3.3.2 Objetivos Específicos

- Analizar las seguridades a nivel de protocolos, para mejorar la seguridad en la información que maneja la empresa ByPas Comunicaciones.

- Diseñar las seguridades en protocolos en una red basada en IPv6, para garantizar las comunicaciones y la integridad de la información.

- Implementar y analizar las seguridades en IPv6 mediante IPSec, para salvaguardar toda la información que genera en los servidores de la empresa ByPas Comunicaciones.

3.4 IPv6

A través de un análisis en el IPv6, el IPSec es un marco de estándares abiertos (del IETF) que definen las políticas para la comunicación segura en una red. Además, estas normas también describen cómo hacer cumplir estas políticas. Uso de IPSec, participando compañeros (ordenadores o máquinas) puede lograr datos

confidencialidad, integridad de datos y autenticación de los datos en la capa de red (es decir, la capa 3 de la interconexión de sistemas abiertos de la capa 7 modelo de red). RFC 2401 especifica la arquitectura base para sistemas compatibles con IPSec".

Partiendo de este principio se tiene que para implementar el IPSec se tiene dos formas diferentes él uno que es mediante comunicaciones punto a punto (host to host). Que es la que se utiliza mediante las computadoras en comunicaciones de ad-hoc o con concentradores que no disponen de configuraciones o que no son de administración local o propia por lo que la administración se lo debe realizar a nivel de terminal o la que más se recomienda en los estándares de la RFC que son los servidores basados en algún sistema operativo de redes y comunicaciones tales como Windows Server 2008 y Linux en cualquiera de sus variantes que para nuestros casos se lo hace en Red hat para la empresa ya que esta invierten en tecnología ya que sus costos son altos, por otro lado la empresa tienen tendencia de economizar en licencias lo utilizan el Centos que son de la misma empresa y no varía mayormente porque los comandos no cambian como en la familia de servidores de Linux Debian y sus variantes como son Suse y Ubuntu.

En Microsoft su producto estrella para servidores son los Windows NT y sus variantes como el 2000, 2003, 2008 y el 2012 que en la actualidad se está promocionando, en el 2000 definitivamente no se trató lo que era el IPv6 apenas en el 2003 recién se lo hace aparecer con algunos parches con la finalidad de garantiza la información.

En el Windows server 2008 ya es lo más normal configurar como alternativa válida de protocolo de comunicaciones IPv4 ya que para redes de área local es

necesario interactuar con los dos protocolos porque algunos servicios no permiten ser administrados sino están los dos al mismo tiempo.

3.4 IPv6 y un Análisis a las Seguridades

Esta migración va a llevar un tiempo, y hasta entonces, las empresas se encontrarán en un ambiente dual de IPv4/IPv6, cada uno con su propio y específico conjunto de problemas de seguridad. Esto incrementa la carga de trabajo del personal de redes de la empresa e incrementa el número de posibilidades en que las cosas pueden salir mal. Aquí es donde la vigilancia de la seguridad es crucial; debido a este período intermedio híbrido, nos vamos a encontrar situaciones inusuales donde los delincuentes informáticos pueden tomar una ventaja potencial gracias a la interacción entre los protocolos.

Estas implementaciones de IPv6 generaran nuevas vulnerabilidades para los administradores de red ya que el internet por ejemplo debe contar ya con nuevos dispositivos de traducción los mismos que pueden ocasionar ataques distribuidos de negación de servicio o transformarse en puntos de fallas.

Las características que tienen las seguridades en el protocolo IPv6 son parecidas a las de IPv4, en la actualidad además de carecer de soporte adecuado en el ámbito de las seguridades las existentes no han sido 100%.

En el ámbito tecnológico, las pruebas de vulnerabilidades por ciertas implementaciones que en algunos casos no se tenían en IPv4, las mismas que no se tienen un aporte de cómo proteger o evitar los ataques a través de este protocolo.

En otro sentido se tiene también que los ataques denominados de fragmentación todavía son y serán un problema en el protocolo IPv6, aunque los cambios realizados con algunos soportes no existe todavía IDS que permita la forma de ingreso de los intrusos en las redes, con frecuencia.

En la red de IPv4 puede saturar una red de computadoras o un sitio web hasta volverlos inservibles y que no puedan ser utilizados en un momento determinado, aún seguirán representando una amenaza para la empresa.

Mientras que IPv6 puede ayudar a disminuir los efectos de los ataques hasta un cierto punto, pero no es una medida preventiva, dejando recursos en riesgo al punto de ser parados por completo.

IPSec es un componente obligatorio para IPv6, y por lo tanto, la seguridad IPSec se requiere modelo de ser apoyados para todas las implementaciones de IPv6. IPSec se implementa utilizando el encabezado de autenticación AH y la extensión de cabecera ESP. Dado que en el momento actual, IPv4 IPSec está disponible en casi todas las plataformas de cliente y servidor del sistema operativo, la seguridad avanzada IPSec IPv6 puede ser desplegado por los administradores de TI de inmediato, sin cambiar las aplicaciones o redes.

Los ataques de fragmentación por lo general son utilizados para evadir algunas seguridades perimetrales como los sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), y cortafuegos, a menudo son la forma en que la empresa se puede dar cuenta que está siendo atacada. Una vez dentro, todo es juego limpio: información del cliente, credenciales, correos electrónicos.

Los ataques de suplantación de identidad todavía seguirán siendo una amenaza en IPv6, pero la nueva obligación de IPSec manejará mejor esta amenaza a la

empresa en general. La suplantación de identidad permite a los delincuentes informáticos ocultar sus identidades, haciendo difícil seguirlos después de un ataque. Los ataques no están limitados a aquellos que tratan de robar información o destruir recursos, ellos realmente intentan empañar la reputación de la empresa.

3.5 IPv6 en Windows 2008

Los ataques más comunes dentro de lo que es una red con una configuración centralizada de un servidor basado en Windows server 2008, son los ataques de suplantación de identidad serán una amenaza en IPv6, por lo que es una obligación la adopción de IPSec, con la finalidad de manejar de mejor manera las amenazas en toda la institución, ya que las herramientas de active directory, lo que ayudan es a ordenar de mejor manera los usuarios dentro de un mismo departamento, proteger las seguridades que tienen cada uno de los mismos.

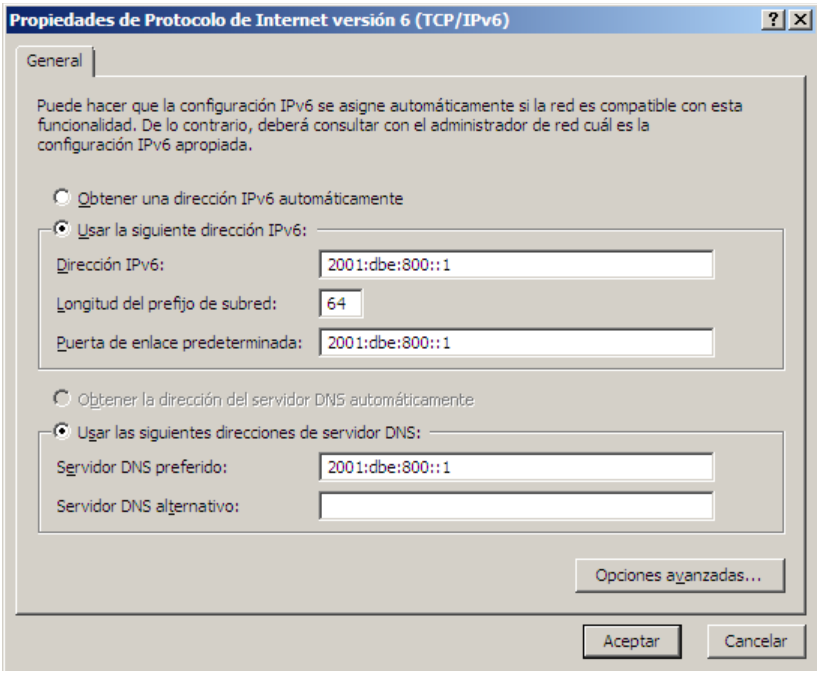
La suplantación de identidad en Windows server 2008 ayuda a los delincuentes informáticos a disfrazar sus identidades dentro de los usuarios del active directory, por lo que en ocasiones no se los puede ver en los ámbitos de administración del servidor ni en el visor de sucesos como usuario mal intencionado, y que tienen entre sus perfiles los que fueron asignados a tal o cual usuario.

Windows server 2008 en su versión R2 corrige algunas de estas desventajas frente a Linux o al mismo Solaris ya que cubre los departamentos con unidades organizativas las mismas que son las que abarcan a las áreas y estas deben estar siempre controladas por el administrador de dominio, el administrador del servidor, el controlador de dominios y el administrador de perfiles.

Los usuarios de la red o clientes de la red pueden acceder siempre y cuando valide localmente y para escritorios remotos se debe asignar un perfil en las unidades organizativas las mismas que van a otorgar las condiciones que tienen que tener los usuarios de los distintos departamentos de la empresa que considere como alternativa válida de solución.

Windows como sistema operativo de servidor, es necesario tomar en cuenta que este servidor para garantizar las seguridades a parte del sistema operativo de servidor requiere de la instalación de un paquete adicional denominado Firewall de Windows que en realidad viene incorporada pero solamente para realizarlo de forma personal o para salvaguardar las políticas propias del sistema operativo.

GRÁFICO Nº 3.1: Configuración del protocolo en la tarjeta de red IPv6



Fuente: Capturación de pantalla en Windows server 2008

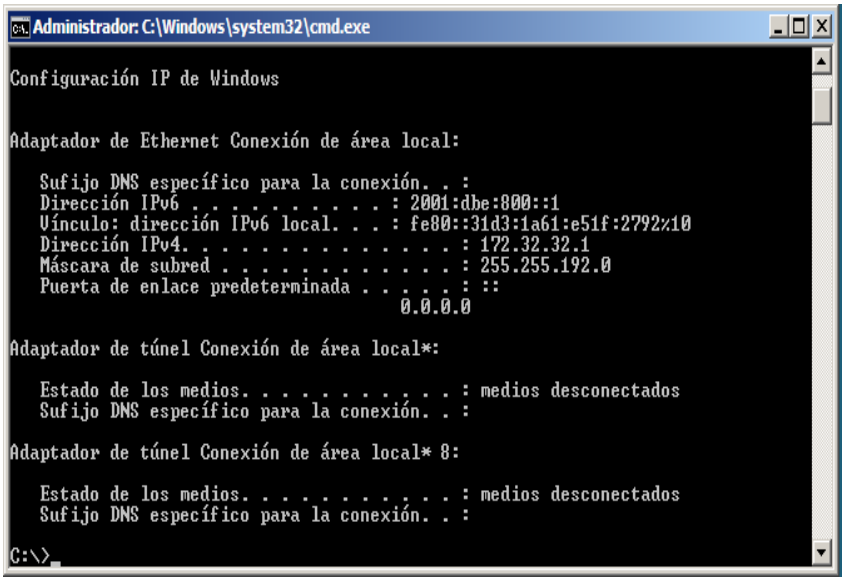
Realizado por: Grupo de Investigación

Tal y como puede verse en la pantalla anterior, el nuevo protocolo no tiene ninguna Opción de configuración (el botón de propiedades del protocolo está deshabilitado).

Para las configuraciones dentro de Windows los protocolos basados en IPv6 toman su propia vinculación automática de acuerdo a la metodología stateless. Ya que se supone una red imaginaria pre configurada así como en el caso de IPv4 las maquinas cuando no se tiene direcciones físicas ni automáticas toman una dirección ficticia basada siempre en el tipo de clase C automática en ese rango.

En el caso de nuestra red se nos pondrá una dirección de la red fe80::/64. Y el vínculo con lo que se nos autentifica seria fe80:31d3:1ª61:e51f:2792%10, lo que quiere decir que vamos a tener una dirección de clase privada en el rango de 10 bits de automatización.

GRÁFICO Nº 3.2: Configuración del protocolo en la tarjeta de red



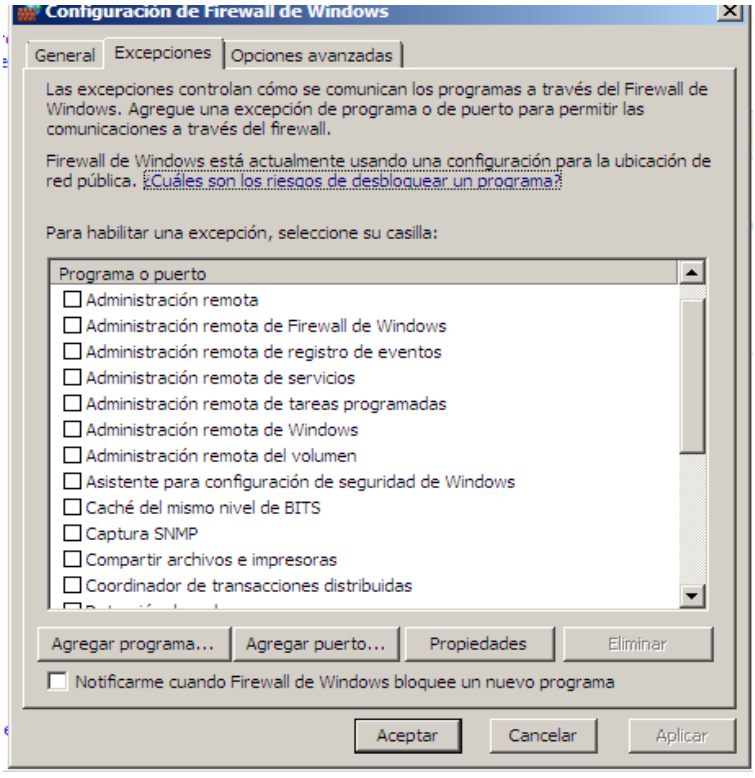
Fuente: Capturación de pantalla del administrador del Windows server 2008

Realizado por: Grupo de Investigación

Como se puede observar en la imagen que está en la parte superior se asigna una dirección IPv6 en el protocolo del mismo nombre, partiendo con el subfijo 64 para direccionamiento IP de 64 bits los mismos que nos darán como resultado una asignación de una red que pueda permitir una conexión de área local.

Las seguridades que se tienen dentro de Windows y que son propias del servidor son las que nos da el firewall de Windows los mismo que prestan una garantía pero de forma local y más no en todo el ámbito del bosque que tiene la configuración de la red.

GRÁFICO Nº 3.3: Configuración del protocolo en la tarjeta de red firewall



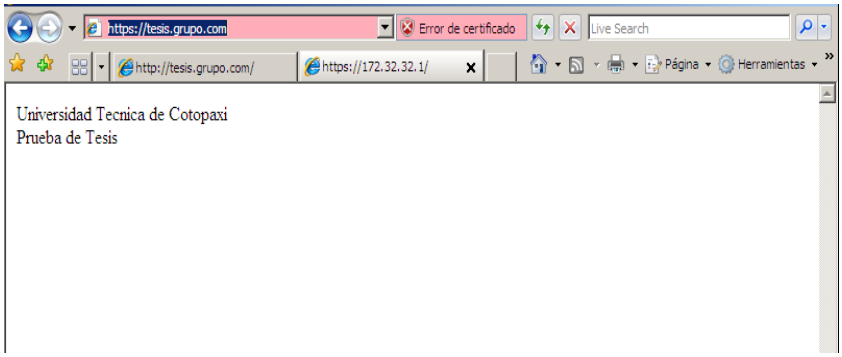
Fuente: Capturación de pantalla de la configuración Windows server 2008

Realizado por: Grupo de Investigación

Más adelante en los anexos podemos encontrar como se detalla las configuraciones de un servidor basado en Microsoft Windows server 2008, en lo que tiene que ver al firewall, pero básicamente lo que se requiere es tener mucho conocimiento con lo que tiene que ver con las configuraciones, y paso a paso vamos a tomar en cuenta como configurar las conexiones que se tienen desde los clientes hacia el servidor pasando por las configuraciones propias de un certificado digital de las maquinas que son servidores de open source es decir Linux.

Para las configuraciones del certificado digital se utilizó las configuraciones propias de Windows server 2008 el cual permite realizar el encriptamiento de lo que se envió a través de la red o en la página web de la que se desea revisar la información, toda esta encriptación se lo realiza mediante el protocolo de seguridad SSL (Security Socket Layer), que es la que nos va a brindar la garantía de la información que se requiere en el momento de abrir una página web.

GRÁFICO Nº 3.4: Configuración del protocolo en la tarjeta de red



Fuente: Capturación de pantalla del Explorer en Linux Centos 6

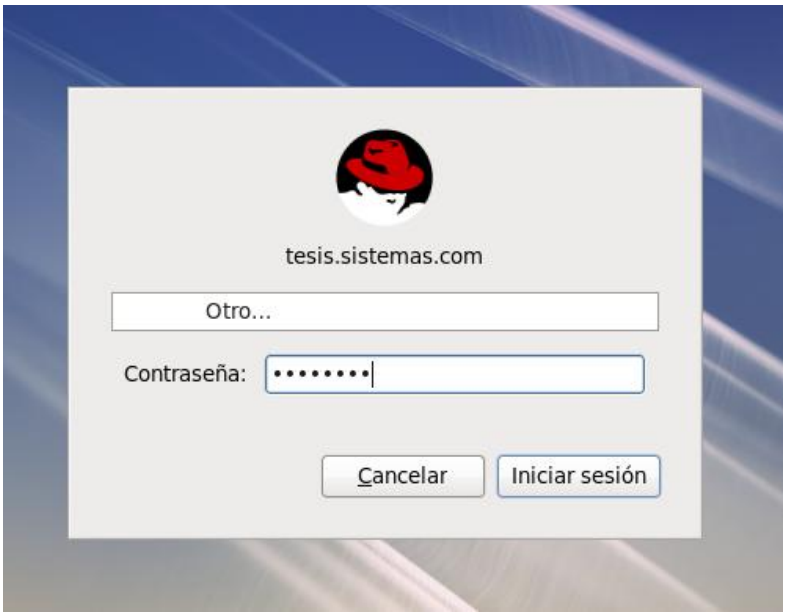
Realizado por: Grupo de Investigación

3.6 IPv6 en Linux Centos

En la actualidad el open source va ganando cada vez más adeptos a nivel mundial y más en nuestro país con las normas y decretos que ha sugerido el gobierno nacional, es por esta razón que la mayoría de las instituciones públicas han adoptado a la plataforma Linux como su modo de vida.

Enrutar en Centos es cada vez más común sobre todo, porque no se tienen limitaciones de licenciamiento y porque en el internet se puede encontrar mucha información gratuita, de igual manera los respaldos por lo que las empresas las utilizan para poder obtener el respectivo servidor de respaldos.

GRÁFICO Nº 3.5: Ingreso a Linux Centos



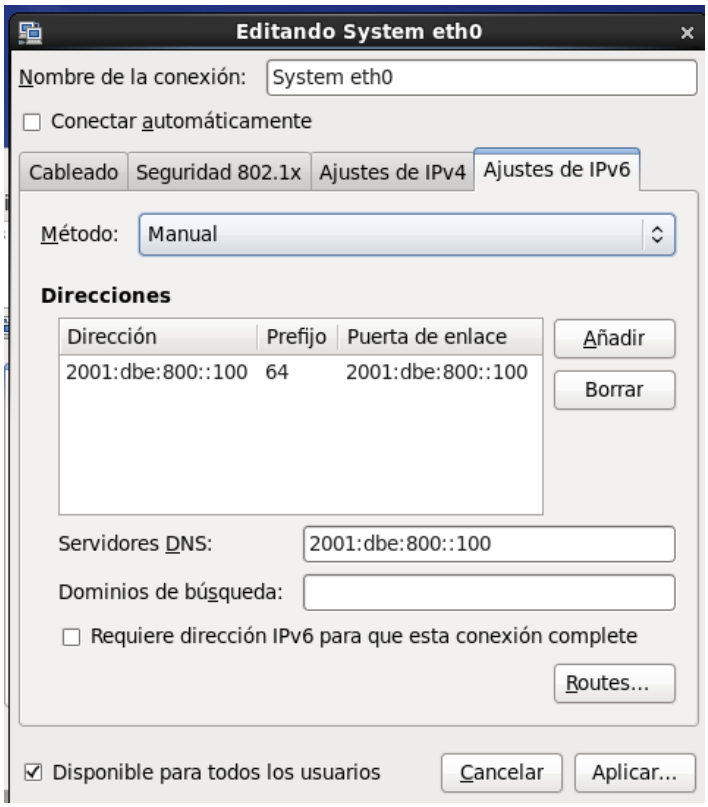
Fuente: Capturación de pantalla del Linux Centos 6

Grupo de Investigación

En esta pantalla se puede observar el control de ingreso que es una de las formas de seguridad que tiene esta plataforma, y más que todo nos asegura la información que se tienen, claro que los estándares de administración de servidores en código abierto manifiestas que no se debe tomar en cuenta al perfil del súper usuario o root porque generaría algunos inconvenientes.

Las configuraciones basadas en el nuevo estándar de IPv6 se las debe realizar siempre en el modo grafico ya que de esta manera se puede garantizar que las configuraciones pueden funcionar mientras que mediante la consola del setup.

GRÁFICO Nº 3.6: Configuración modo Gráfico IPv6



Fuente: Capturación de pantalla de la configuración de Linux Centos 6

Realizado por: Grupo de Investigación

Las configuraciones se las realizan mediante el modo grafico ya que mediante la consola del setup al IPv6 le toma como un DNS y nada más lo que genera inconvenientes, no obstante si se permite él envió de la utilización del comando del protocolo ICMP es decir el ping6 si existe replica como si se lo hubiera configurado en bajo nivel o a nivel de comandos únicamente.

Los DNS en IPv6 se los realiza de acuerdo a la IP y a la puerta de enlace las mismas que son las que justifican el desenvolvimiento de las computadoras dentro de una red de datos, más sin embargo el internet todavía no justifican la manera de asignación de IP públicas para el IPv6 y resulta un tanto complicado la designación principalmente para lo que es el LACNIC como manifiestan en su página web algunos escritores de tecnología

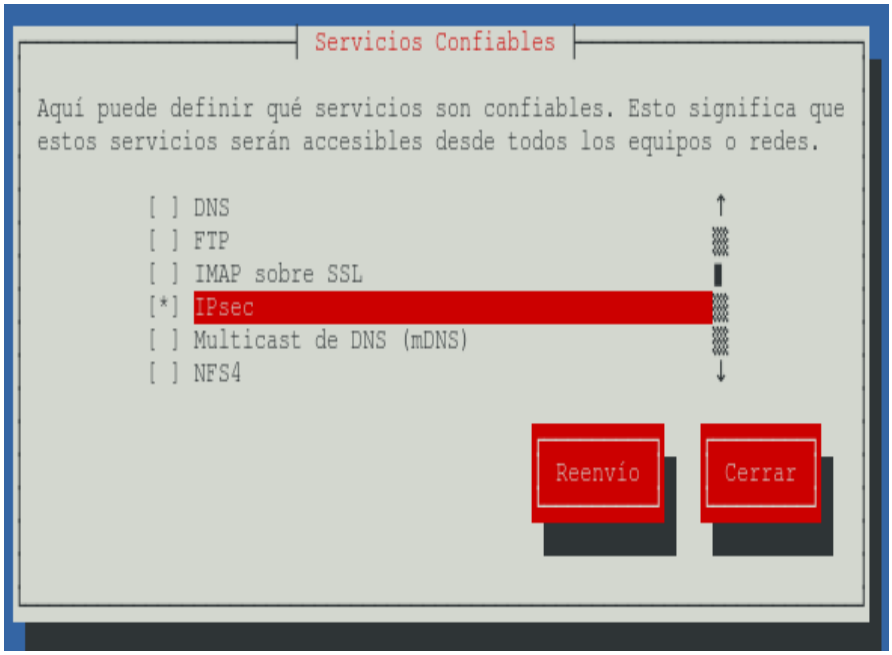
GRÁFICO Nº 3.7: IPv6 en Consola

Fuente: Capturación de pantalla de la configuración de red en Linux Centos 6

Realizado por: Grupo de Investigación

Las configuraciones para los túneles de IPSec se lo realizan en la consola de las configuraciones de Firewall ya que esta es la que nos da los privilegios para la realización de la encriptación de la información dentro de las configuraciones propias de este tipo de servicios en los protocolos.

GRÁFICO Nº 3.8: Configuración del IPSec con Firewall

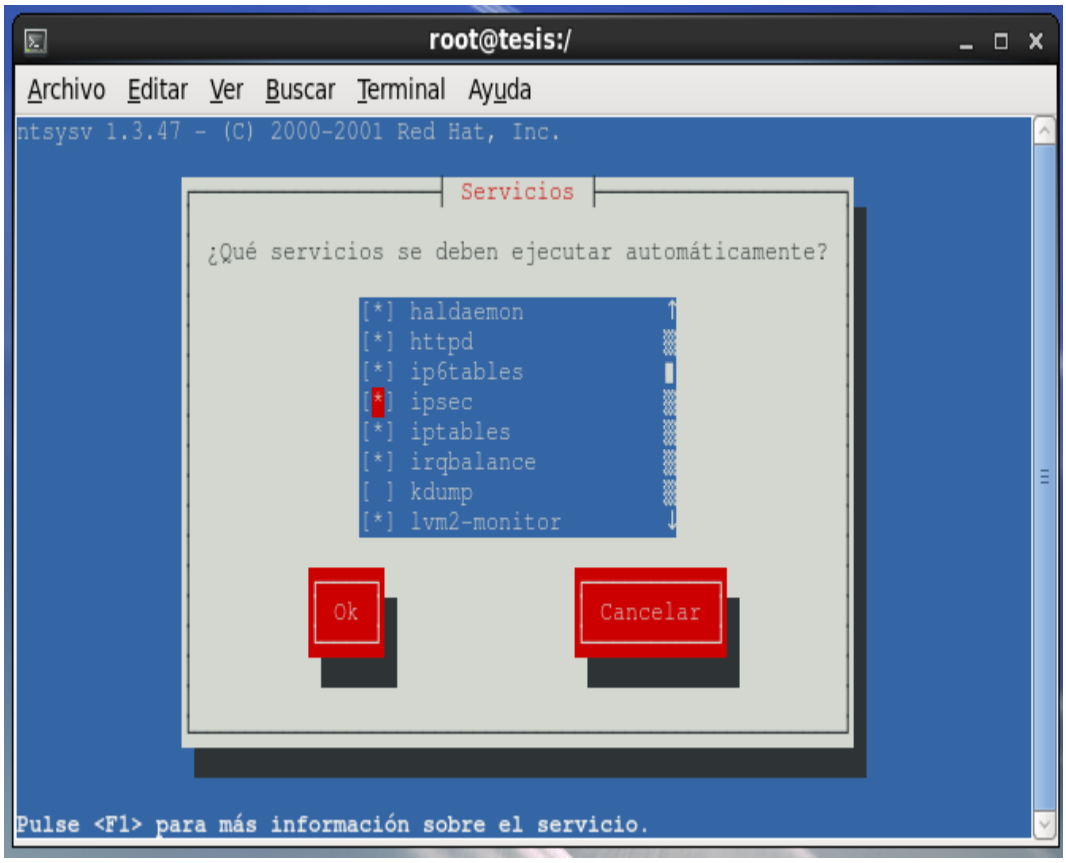


Fuente: Capturación de pantalla de la configuración del IPSec en Linux Centos 6

Realizado por: Grupo de Investigación

Previa esta configuración lo más óptimo es la configuración del IPSec, la misma que se la tiene en el ntsysv en donde se tiene que configurar o habilitar los servicios necesarios para poder alcanzar las configuraciones necesarias.

GRÁFICO Nº 3.9: Configuración del IPSec



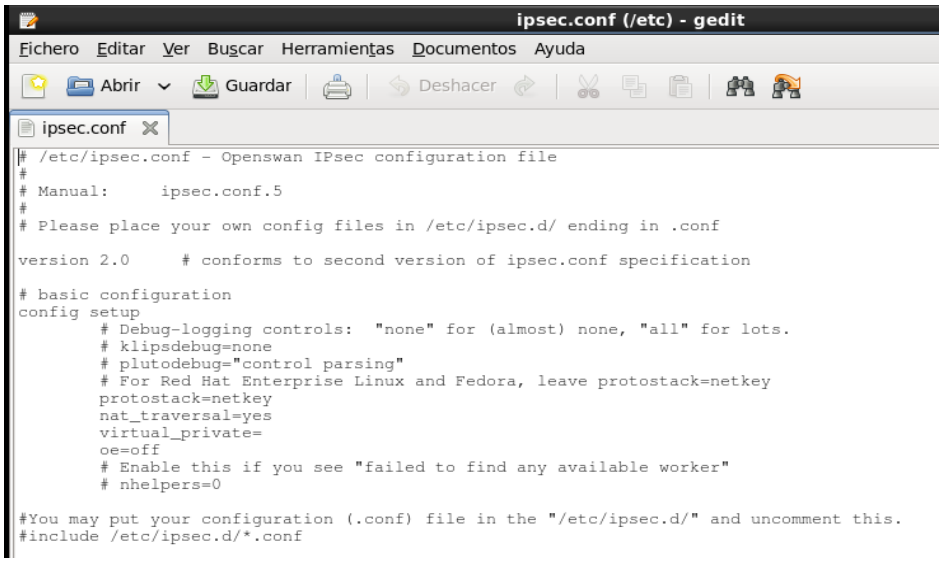
Fuente: Capturación de pantalla de la activación del IPSec en Linux Centos 6

Realizado por: Grupo de Investigación

Una vez configurada la conexión de red con la nueva dirección se procede a abrir una consola y enviar el comando de reinicio de servicio

Cuando no se dispone de conocimientos de modo gráfico y solo en modo texto, se lo debe abrir en una consola y enviar los siguientes comando que nos ayudaran a la instalación y administración de este tipo de protocolo.

GRÁFICO Nº 3.10: Configuración de IPSec

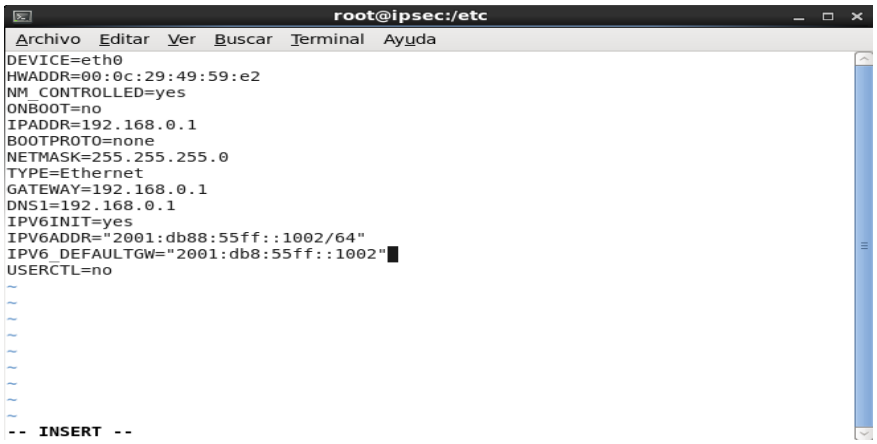


Fuente: Capturación de pantalla del resultado del IPSec en Linux Centos 6

Realizado por: Grupo de Investigación

Esta es la configuración propia del sistema para una red IPv6 pero obviamente tenemos que tener en cuenta que esto requiere de una configuración en la interfaz del eth0.

GRÁFICO Nº 3.11: Configuración de la red basada en IPv6 en Linux

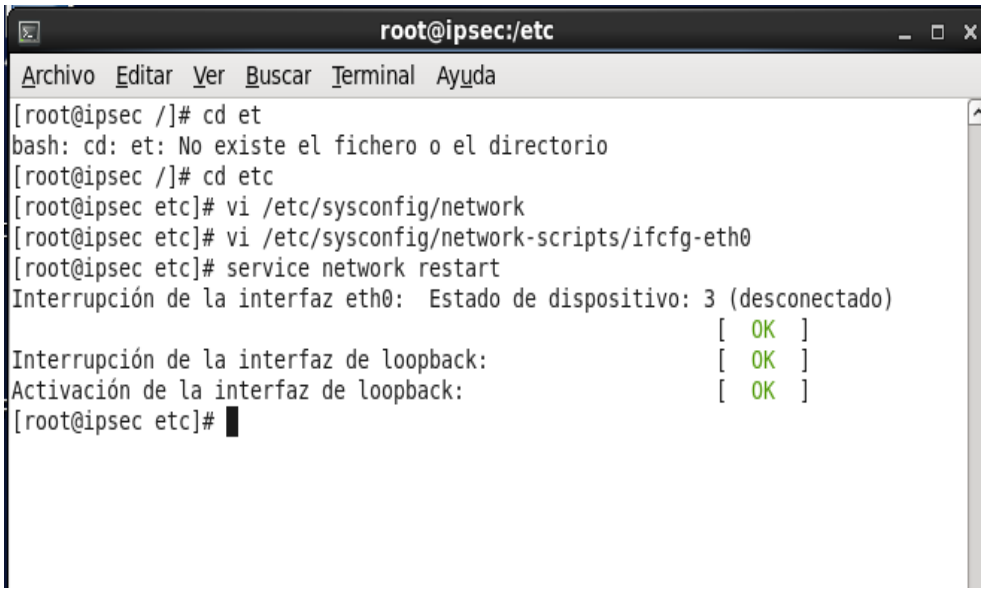


Fuente: Capturación de pantalla del root IPSec en Linux Centos 6

Realizado por: Grupo de Investigación

Una vez que se configuro todos los servicios en modo grafico procedemos a revisar de que todo lo puesto en los archivos puedan ser replicados para comprobar que se configuro de buena manera, y como se pudo observar en esta investigación el IPv6 debe garantizar las seguridades a través de IPSec y como el Linux dispone de muchas características de seguridad ponemos que solo debemos habilitar su Firewall y permitir o no las comunicaciones.

GRÁFICO Nº 3.12: Comprobación de red en IPv6



Fuente: Capturación de pantalla de la comprobación de red en Linux Centos 6
Realizado por: Grupo de Investigación

Una vez configurada las opciones de IPv6 podemos verificar que se cumple mediante la apertura de puertos y revisión de protocolos.

Una vez instalada la opción de IPSec este empieza a trabajar luego de reiniciada la computadora toda vez que el IPSec absorbe las configuraciones de los protocolos

de comunicaciones que se tengan habilitados dentro de los servidores de comunicaciones de las instituciones.

El IPSec por lo tanto quedaría configurado en IPv6 al haber sido comprobado dentro de las configuraciones del servidor. Como se puede observar es apenas de habilitación un tanto diferente al de Windows.

3.7 Adjunto Video de las Configuraciones:

- Configuración del IPSec, basado en IPv6 en Linux Centos 6

- Configuración del Active Directory, DHCP y de un Certificado Digital, basado en IPv6 en Windows Server 2008

Conclusiones y Recomendaciones

Conclusiones

- En la actualidad lo más complicado es proveer de seguridades a la información a nivel mundial, ya que día a día vemos como aparecen personas con nuevos conocimientos y con malas intenciones por lo que asegurar la información es un reto que avanza a pasos desmedidos dentro de la era tecnológica en la que se vive.

- Las configuraciones en IPSec que se plantea en esta investigación está a nivel de servidores y es como se lo debe llevar ya que en dispositivos de detección o prevención de intrusiones, tienden a ir un poco más allá y esto de acuerdo a la marca que se desee configurar

- IPv6 es un nuevo protocolo que carece todavía de seguridades por más esfuerzo que el DoD de los Estados Unidos ha invertido para garantizar la información, más sin embargo este protocolo incorporo ya el IPSec como política de privacidad a diferencia de su antecesor el cual requería de una configuración particular para su implementación.

- Los certificados digitales es más común ser implementados, lo que antes solamente se lo tenía en los bancos e instituciones financieras, por sus costos que en algunos casos eran inalcanzables.

- Windows desde su versión Server 2008 incorpora como característica la adopción de un certificado digital, el cual se lo puede configurar y todos los

servicios que aquí se tienen van ya encriptados lo que ayuda a la administración de las seguridades.

- Las configuraciones con certificados digitales y en IPv6 para lo que es Linux resulto mucho más fácil y no se requiere de mayor inversión ya que en el internet se cuenta con información y sobre todo con los paquetes propios de este tipo, tal es el caso de Open SSL.

- Muchas empresas que proveen el servicio de internet (ISP), cuentan entre sus paquetes comerciales la venta de host con el IPv6 y por lo tanto con seguridades a nivel de IPSec, para lo que son páginas web, no así el certificado digital ya que estas no cuentan en muchos casos como plataforma a Microsoft, principalmente por el licenciamiento.

Recomendaciones

- La adopción inmediata de protocolo IPv6 como fuente de comunicación dentro de la plataforma tecnológica de cualquier institución, principalmente por las seguridades que como se observó son protocolos que cuentan con seguridades propias.

- La emisión de certificados digitales resulta una de las medidas más positivas cuando se las configura para poder realizar aplicaciones web de ayuda a procesos empresariales, particularmente para la toma de decisiones oportunas.

- El open source ha trabajado mucho en lo que tiene que ver a nuevas funciones y características de los servidores pero aún son insuficientes esos esfuerzos ya que los nuevos protocolos de seguridad, como el IPSec requieren de complementación de paquetes alternativos y de configuraciones como los iptables que son medidas de seguridad necesarias en una empresa.

- El IPv6 deberá ser adoptado por una empresa cuando este cumpla con los requerimientos propios de las seguridades ya que se basa toda su infraestructura todavía en aplicaciones seguras del IPv4.

GLOSARIO

Address En redes, la palabra dirección se refiere a un distintivo único para cada nodo de la red.

Administrador Un usuario de la red con autoridad para realizar las tareas de alto nivel de cliente servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman superusuario.

Ancho de banda representa la capacidad del canal de comunicación para transportar datos

APPC Protocolo de comunicación de dos equipos donde no existe director.

ARCNet Red de computadoras y recursos compartidos creado por Datapoint muy popular en los años setenta, cuyas características eran: bajo costo, cableado en estrella y velocidad hasta 2.5 Mbps.

ARP Proceso en donde se asigna al número de la tarjeta una dirección formato TCP/IP.

ARPA Agencia militar de Estados Unidos encargada de proyectos tecnológicos como las redes computacionales militares

ARPANET	Proyecto del Departamento de Defensa de los Estados Unidos que utiliza protocolos tipo X.25 donde la cantidad e información (paquetes) no es fija. La dividieron en dos: Milnet para uso militar e Internet para uso público.
ATM	Tecnología de reciente introducción que permite la transmisión de grandes volúmenes de datos a gran velocidad, con tecnología de paquetes retrasados. Se considera la arquitectura del futuro en comunicaciones digitales.
Bridge	Puente. Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.
Broadcast	Transmisión abierta. Mensajes que se mandan sin destino
CABLE NIVEL 5	Cable tipo MIT 4 pares que soporta 100 MHZ.
CCITT	Comité Consultivo Internacional de Telegrafía y Telefonía Encargado de los estándares internacionales de comunicación.
Communication Server	Computadora destinada a dar los servicios de comunicaciones de la red.
Cocentrador	Equipo que se encarga, en primera instancia, de concentrar las señales. Algunos tienen funciones de repetir y retrasar la

señal para evitar colisiones.

Conectividad Estado que permite la transferencia de datos entre dos computadoras.

CSMA/CD Sensor de portadora de accesos múltiples con detección de colisiones. Método de transmisión de datos en donde todas as estaciones pueden mandar datos con una transmisiones simultáneas detectan las colisiones. Es la base de la topología Ethernet.

Dominio Grupo de computadoras de la red que está administrada y controlada por el mismo servidor de red. Puede tener varios servidores pero una administración única para el control de permisos, recursos y seguridad.

E1 Estándar europeo de transmisión de datos 2.048 Mbps.

E3 Cana de comunicación digital de 34 Mbps. El más veloz del mercado.

Encriptamiento Proceso basado en operaciones lógicas binarias para disfrazar un dato y evitar que sea leído por otra fuente distinta al destino.

Escalabilidad Característica de los equipos que nos permite ir aumentando velocidad y capacidad en: discos, memoria, procesadores y

tarjetas periféricas.

Ethernet Estándar de red más popular e implementado. Utiliza *CSMA/CD* con una velocidad de 10 Mbps.

Fast Ethernet Topología de transmisión digital tipo Ethernet que transmite a 100 Mbps.

Firewall Sinónimo de dispositivo de software o hardware encargado de proteger cualquier sistema de la entrada de personas o autorizadas. Regula, según las necesidades, los niveles internos de restricción a la información y autoriza el acceso a cierto tipo de datos.

FTP Servicio que permite transferir archivos entre sistemas y entre redes remotas con sistemas diversos. De uso común en Internet.

Gateway Dispositivo que permite conectra dos redes o sistemas diferentes. Es la puerta de entrada de una red hacia otra.

Hub Dispositivo inteligente que sirve de infraestructura para la red. Comúnmente asociado con un concentrador 10 base T con funciones inteligentes de retraso de señal *(retiming)*, y retransmisión de la misma *(repeating)*.

ICMP Componente de los protocolos TCP/IP que realiza las funciones de control y administración de transacciones.

IEEE-802.1	Estándar definido relativo a los algoritmos para enrutamiento de cuadros o frames (la forma en que se encuentra la dirección destino).
IEEE-802.2	Define los métodos para controlar las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI) llamado LLC.
IEEE-802.3	Define las formas de protocolos Ethernet CSMA/CD en sus diferentes medios físicos (cables).
IEEE-802.11	Estándar para redes inalámbricas con línea de vista.
Internet	Red de redes con base en TCP/IP y acceso público mundial.
Internetworking	Término usado para referirse a la interacción entre varias redes.
Interoperabilidad	Término referente a la capacidad de diferentes redes a comunicarse entre sí.
Intranet	Red de área amplia con gran infraestructura y acceso privado.
IP	Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo.

IPX	Protocolo definido para redes Netware que tienen direcciones en tres campos (nodo, red y socket), lo cual le permite mantener varios enlaces entre redes y procesos en varios servidores.
LLC	Controla las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI).
MAC	Capa de control de acceso a medios. Capa del modelo de comunicación OSI, que es la encargada del control lógico del medio físico
NetBios	Interface estándar para procesos de red. Son los servidores de software y firmware entre la tarjeta y las aplicaciones.
NFS	Sistema de archivos de red. Genéricamente es un sistema que permite el acceso a un servidor de archivos.
OSI	Estructura lógica de siete niveles para facilitar la comunicación entre diversos sistemas de computación.
Ping	Transmisión de datos de prueba para verificar la integridad de la comunicación entre dos sistemas.
Protocolo	Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.

Router	Ruteador. Dispositivo que pasa todos los mensajes entre una red y otra distinguiendo a qué red pertenece el destino del mensaje
Servidor	Equipo destinado a proveer y administrar los servicios de red, los recursos, las aplicaciones, los archivos y la seguridad de la misma.
SNMP	Protocolo parte de TCP/IP para el manejo y la administración remota de los recursos de la red.
SOLARIS	Sistema operativo UNIX desarrollado por SunSof
T1	Línea de transmisión implementada por AT&T con velocidad de 1.544 Mbps.
T3	Servicio de transmisión de datos que opera a 45 Mbps.
TCP/IP	Protocolos definidos por catedráticos en el proyecto ARPANet del Departamento de Defensa de Estados Unidos para la red universitaria Internet en los años setenta.
UNIX	Sistema operativo multiusuario desarrollado en los años setenta y que se caracteriza por ser portátil y versátil.
Usuario	Persona que trabaja con la estación de trabajo. El que realiza tareas de acceso a los recursos de la red pero no los modifica

sustancialmente. Tiene derechos de uso pero no de mantenimiento mayor.

Workstation Computadora que puede realizar procesos robustos de *front end*. Permite sacar máximo provecho a sus recursos de red.

Definición de Siglas

HSRP: Hot Standby Route Protocol.

GLBP: Gateway Load Balancing Protocol

VRRP: Virtual Router Redundancy Protocol

CARP: Common Address Redundancy Protocol

Referencias y Bibliografías

Bibliografía Consultada

- COMER Douglas E, Redes Globales de Información con Internet y TCP/IP, Tercera Edición, 2009, Prentice Hall Hispanoamericana ISBN 968-880-541-6, (Pág. 3), (Págs. 510, 511,512).

- FRANCISCONI Hugo Adrián, IPsec en Ambiente IPv4 e IPv6 primera edición, Agosto 2005, ISBN 987-43.9727-6, Impreso por carril Godoy Cruz, Argentina, (Pág. 132).

- HERNÁNDEZ Roberto, FERNÁNDEZ Carlos, BASTIDAS Piedad, Metodología de la Investigación, cuarta Edición, (Pág. 35).

- GARCIA TOMAS Jesús, RAYA CABRERA José Luis, RAYA Víctor Rodrigo, Alta velocidad y Calidad de servicio en redes IP, 2002, ALFAYOMEGA Grupo Editor, México, (Págs. 353 .354).

- GONZALES, José y otros. Diseño de redes y comunicaciones. Editor Carmelo Sánchez. 1ra. Edición. España Editorial Mc Graw-Hill, 2001. (Pág. 123 – 129).

- GUTIERREZ, Abraham: Curso de Técnicas de Investigación, Edición Tercera, Editorial serie Didáctica A.G, Quito- Ecuador, 1992, (Pág. 46).

- MEDIA Active, Aprende Windows 8 Consumer Preview, Editor Alfaomega, Primera edición 2012, Impreso en España, (Pág. 3)

- MERIKE Kaeo, Diseño de Seguridades en redes, 2003, Impreso en España, Editorial CISCO Press, (Págs. 283-284).
- PÉREZ M, Windows server 2008, instalaciones, configuración y administración, Editorial RC libros, 2009, (Pág. 5).

- RAYA José Luis, TCP/IP para Windows server, Editorial Alfaomega, Impreso Colombia, 2006. (Págs. 300, 12, 128).

- TANENBAUM Andrew S. Redes de Computadoras, 2010 Cuarta Edición, Pearson Educación México. (Págs. 721, 772, 2, 464-465, 724, 464-465).

- ZEA Leiva. Nociones de Metodología de Investigación Científica, quinta edición, Quito, 2001. (Pág. 102).

Bibliografía Virtual

- www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion.
- http://www.ipsec-howto.org/spanish/x161.html
- http://www.iec.csic.es/criptonomicon/linux/introsegred.html
- http://definicion.de/red-de-datos/
- http://www.desarrolloweb.com/articulos/protocolos-red.html
- http://belarmino.galeon.com/
- http://www.marbit.es/index_ip.html
- http://es.kioskea.net/contents/268-protocolo-ipv6.
- http://ipv6nuevastecredes.wikispaces.com/6.+DIRECCIONES+Y+DIRECCIONAMIENTO+IPV6.
- http://help.salesforce.com/apex/HTViewHelpDoc?id=security_keys_using_master.htm&language=es
- http://www.informatica-hoy.com.ar/seguridad-informatica/Criptografia.php
- http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node306.html
- http://cv.uoc.edu/~mat/cursoWeb/material/UW_90072_00000/web/main/m2/v3_1.html
- http://www.certsuperior.com/FirmasDigitales.aspx
- http://www.consumer.es/web/es/tecnologia/internet/2004/01/23/94524.php


ANEXOS

ANEXO 1

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERIA Y APLICADA

INGENIERIA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

ENCUESTA

Dirigida a los Técnicos de la empresa ByPas Comunicaciones de la Ciudad de Quito.

Objetivo: Conocer la situación actual de los protocolos de seguridad IPSec en redes de datos basadas en ipv6 de la empresa ByPas Comunicaciones de la ciudad de Quito.

Instrucciones: Sírvase responder a las siguientes preguntas con claridad.

1.- **¿Ha escuchado Ud. hablar sobre IPSec?**

Si ( )

No ( )

2.- ¿Cree Ud. que IPv6 cuenta ya con seguridades propias?

Todas ( )
Suficientes ( )
Ninguna ( )

3.- ¿Considera Ud. que es oportuno implementar IPSec en IPv6?

Si ( )
No ( )

4.- ¿A través de qué medios Ud. escucho hablar del IPv6?

Televisión ( )
Radio ( )
Internet ( )
Prensa escrita ( )

5.- ¿Considera Ud. que el IPSec es una seguridad que garantiza la información?

Si ( )
No ( )

6.- ¿Conoce Ud. bajo qué plataforma tecnológica es más notoria la implementación de IPSec?

Windows ( )

Linux ( )

Otras ( )

7.- ¿Sabe Ud. de páginas web que ya tengan IPv6?

Si ( )

No ( )

8.- ¿Sabe Ud. cuantas empresas tienen IPv6 en el Ecuador?

Muchas ( )

Pocas ( )

Ninguna ( )

9- ¿Cree Ud. que el IPSec del IPv6 es mejor que el de su antecesor?

Si ( )

No ( )

10.- ¿Maneja ya bien Ud. el tema de direccionamiento IPv6?

Si ( )

No ( )

11.- ¿Qué dispositivos conoce Ud. que tienen seguridades para lo que es IPv6?

Routers ( )

Switch configurable ( )

Hub ( )

Puentes ( )

12.- ¿Cree Ud. que las redes de datos están más seguras bajo una clave cifrada?

Si ( )

No ( )

GRACIAS POR SU COLABORACIÓN

ANEXO 2

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERIA Y APLICADA

INGENIERIA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

ENCUESTA

Dirigida a los Empleados de la empresa ByPas Comunicaciones de la Ciudad de Quito.

Objetivo: Conocer la situación actual de los protocolos de seguridad IPSec en redes de datos basadas en IPv6 de la empresa ByPas Comunicaciones de la ciudad de Quito.

Instrucciones: Sírvase responder a las siguientes preguntas con claridad.

1.- **¿Ha escuchado Ud. hablar sobre IPSec?**

Si ( )

No ( )

2.- ¿Cree Ud. que IPv6 cuenta ya con seguridades propias?

Todas ( )
Suficientes ( )
Ninguna ( )

3.- ¿Considera Ud. que es oportuno implementar IPSec en IPv6?

Si ( )
No ( )

4.- ¿A través de qué medios Ud. escucho hablar del IPv6?

Televisión ( )
Radio ( )
Internet ( )
Prensa escrita ( )

5.- ¿Considera Ud. que el IPSec es una seguridad que garantiza la información?

Si ( )
No ( )

6.- ¿Conoce Ud. bajo qué plataforma tecnológica es más notoria la implementación de IPSec?

Windows ( )

Linux ( )

Otras ( )

7.- ¿Sabe Ud. de páginas web que ya tengan IPv6?

Si ( )

No ( )

8.- ¿Sabe Ud. cuantas empresas tienen IPv6 en el Ecuador?

Muchas ( )

Pocas ( )

Ninguna ( )

9- ¿Cree Ud. que el IPSec del IPv6 es mejor que el de su antecesor?

Si ( )

No ( )

10.- ¿Maneja ya bien Ud. el tema de direccionamiento IPv6?

Si ( )

No ( )

11.- ¿Qué dispositivos conoce Ud. que tienen seguridades para lo que es IPv6?

Routers ( )

Switch configurable ( )

Hub ( )

Puentes ( )

12.- ¿Cree Ud. que las redes de datos están más seguras bajo una clave cifrada?

Si ( )

No ( )

GRACIAS POR SU COLABORACIÓN

ANEXO 3

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERIA Y APLICADA

INGENIERIA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

ENCUESTA

Dirigida a los Socios de la empresa ByPas Comunicaciones de la Ciudad de Quito.

Objetivo: Conocer la situación actual de los protocolos de seguridad Ipsec en redes de datos basadas en ipv6 de la empresa ByPas Comunicaciones de la ciudad de Quito.

Instrucciones: Sírvase responder a las siguientes preguntas con claridad.

1.- **¿Ha escuchado Ud. hablar sobre IPSec?**

Si ( )

No ( )

2.- ¿Cree Ud. que IPv6 cuenta ya con seguridades propias?

Todas ( )
Suficientes ( )
Ninguna ( )

3.- ¿Considera Ud. que es oportuno implementar IPSec en IPv6?

Si ( )
No ( )

4.- ¿A través de qué medios Ud. escucho hablar del IPv6?

Televisión ( )
Radio ( )
Internet ( )
Prensa escrita ( )

5.- ¿Considera Ud. que el IPSec es una seguridad que garantiza la información?

Si ( )
No ( )

6.- ¿Conoce Ud. bajo qué plataforma tecnológica es más notoria la implementación de IPSec?

Windows ( )

Linux ( )

Otras ( )

7.- ¿Sabe Ud. de páginas web que ya tengan IPv6?

Si ( )

No ( )

8.- ¿Sabe Ud. cuantas empresas tienen IPv6 en el Ecuador?

Muchas ( )

Pocas ( )

Ninguna ( )

9- ¿Cree Ud. que el IPSec del IPv6 es mejor que el de su antecesor?

Si ( )

No ( )

10.- ¿Maneja ya bien Ud. el tema de direccionamiento IPv6?

Si ( )

No ( )

11.- ¿Qué dispositivos conoce Ud. que tienen seguridades para lo que es IPv6?

Routers ( )

Switch configurable ( )

Hub ( )

Puentes ( )

12.- ¿Cree Ud. que las redes de datos están más seguras bajo una clave cifrada?

Si ( )

No ( )

GRACIAS POR SU COLABORACIÓN