

**ESTUDIO DE TECNOLOGIAS EN CONECTIVIDAD SEGURA Y
SIMULACION DE LA TECNOLOGIA IPSEC PARA REDES DE
COMUNICACIONES**

Andrés Mauricio Ramírez

Código: 0122339

**Anteproyecto de grado presentado
como requisito parcial para optar
al título de Ingeniero Electrónico**

**UNIVERSIDAD DEL VALLE
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
PROGRAMA ACADÉMICO DE INGENIERÍA ELECTRÓNICA
SANTIAGO DE CALI**

2005

**ESTUDIO DE TECNOLOGIAS EN CONECTIVIDAD SEGURA Y
SIMULACION DE LA TECNOLOGIA IPSEC PARA REDES DE
COMUNICACIONES**

Andrés Mauricio Ramírez

Código 0122339

Aprobación del director del proyecto

Ing. Oscar Polanco Sarmiento

**Ing. Fabio Guerrero, Msc
Coordinador del Área de
Telecomunicaciones**

**Ing. Carlos R. Pinedo
Director Plan de estudios
Ingeniería Electrónica**

TABLA DE CONTENIDO

1. INTRODUCCIÓN	1
2. ANTECEDENTES	2
3. FORMULACION DEL PROBLEMA	3
4. JUSTIFICACION	4
5. OBJETIVOS	5
5.1 GENERALES	5
5.2 ESPECIFICOS	5
6. MARCO TEORICO	6
6.1 ESTADO DEL ARTE	10
7. ASPECTOS METODOLOGICOS	10
8. RESULTADOS ESPERADOS	11
9. PRESUPUESTO	12
10. CRONOGRAMA DE ACTIVIDADES	12
11. GLOSARIO	13
12. REFERENCIAS	14

1. INTRODUCCIÓN

Una red es una colección de dispositivos, que interconectan a los equipos de procesamiento de información de una organización, como computadoras de escritorio y servidores. La tecnología en nuestros días avanza muy rápidamente y con ello la inseguridad en las redes, por ello surgen las tecnologías en software y hardware que nos proporcionan mayor seguridad de la información.

Como podemos apreciar, el mundo está cambiando aceleradamente en las últimas décadas y de relacionarse simplemente con asuntos a nivel local o regional, las empresas están, en este momento, pensando en mercados y negocios a nivel global. Muchas compañías tienen oficinas o instalaciones en distintos puntos del país o del mundo y hay una cosa que todas ellas necesitan: comunicaciones rápidas, seguras y confiables dondequiera que estén sus oficinas, instalaciones o empleados.

Las redes privadas virtuales (VPN¹) deben su creciente popularidad al hecho que las empresas, especialmente las PYMES², han buscado la posibilidad de utilizar una red pública, ampliamente extendida y de bajo costo como Internet para aumentar la movilidad, mejorar la productividad de los empleados y contribuir a su desarrollo. Las VPN han demostrado que pueden lograr lo anterior, cuando les permiten a los trabajadores remotos desarrollar sus actividades en la calle, en el hogar o en otras oficinas, tener acceso a una única red privada de la compañía desde cualquier parte del mundo utilizando su computadora portátil, hogareña o de oficina y el Internet público.

Básicamente, una VPN es una red privada que utiliza una red pública (generalmente Internet) para conectar varios lugares o usuarios remotos entre ellos. En vez de utilizar una conexión dedicada o líneas alquiladas, una VPN usa una "conexión virtual" a través de Internet desde la red privada de la compañía hasta el sitio o empleado remoto.

El presente trabajo de grado propone ampliar y desarrollar aún más los aspectos relacionados con la conectividad segura en las redes de comunicación, facilitando la adecuada asesoría sobre el tema a las diferentes organizaciones. También se simula el funcionamiento del protocolo IPSEC.

¹ Virtual Private Network

² Pequeñas Y Medianas Empresas

2. ANTECEDENTES

Las redes de comunicaciones y los sistemas de información se han convertido en un factor esencial del desarrollo económico y social. La informática y las redes se están convirtiendo en recursos omnipresentes, tal y como ha ocurrido con el suministro de agua y de electricidad. Por consiguiente, la seguridad de las redes de comunicación y de los sistemas de información, y en particular su disponibilidad, es un asunto que preocupa cada vez más a la sociedad, en particular, por la posibilidad de que surjan problemas en sistemas de información claves, debidos a la complejidad de los sistemas, accidentes, errores o ataques, que puedan repercutir en las infraestructuras físicas que prestan servicios esenciales para el bienestar de los ciudadanos colombianos.

El creciente número de fallos de seguridad ha causado ya importantes perjuicios económicos, ha minado la confianza de los usuarios y perjudicado el desarrollo del comercio electrónico. Los particulares, las administraciones públicas y las empresas han reaccionado implementando tecnologías de seguridad y procedimientos de gestión de la seguridad.

La encriptación usa una técnica -la criptografía- que modifica un mensaje original mediante una o varias claves, de manera que resulte totalmente ilegible para cualquier persona. Y solamente lo pueda leer quien posea la clave correspondiente para descifrar el mensaje. Junto con la firma digital y las marcas de aguas digitales (digital watermark), la encriptación es una de las posibles soluciones para proteger datos cuando son enviados a través de redes como Internet.

Un antecedente en la Universidad del Valle sobre VPN es el trabajo realizado por el ingeniero Fernando Andrés Arévalo Jiménez, para obtener su título de ingeniero. Este trabajo se titula “Cómo escoger e implementar una VPN conceptos teóricos y prácticos”; el ingeniero documentó ampliamente aspectos como enlaces privados, aparición de VPNs, autenticación y encriptamiento, tecnologías VPN y además, realizó implementaciones prácticas sobre:

- Acceso remoto PPTP, por software usando Windows 2000 server.
- LAN To LAN IPSEC, por hardware usando enrutadores CISCO 1760.
- LAN To LAN IPSEC, por software usando LINUX y free S/Wan V2.0.

En estas implementaciones se documentó sobre topologías, tecnología de túnel, plataforma y equipos utilizados.

Éste trabajo de grado se diferencia porque se enfoca principalmente en la ampliación del tema de conectividad segura y la simulación del protocolo IPSEC, para seguridad en redes.

3. FORMULACION DEL PROBLEMA

Las redes locales tradicionales son esencialmente restringidas a operar al interior de la organización de forma privada, por lo cual se puede intercambiar información entre las computadoras usualmente sin pensar en la seguridad de la información como un asunto crítico. Sin embargo, con el uso de Internet para interconectar redes privadas, la situación se vuelve preocupante debido principalmente a que Internet es intrínsecamente abierto e inseguro. Por lo tanto, las VPN se implementan usando protocolos especiales que le permiten a los usuarios comunicarse de manera segura y comprobar que la transmisión se hace desde una fuente confiable. Cuando un empleado se conecta a Internet, la configuración de las VPN les permite "perforar" la red privada de la compañía y navegar en la red como si estuvieran en su propia oficina.

Para esto, los dispositivos responsables para la implementación y administración de la red virtual, deben ser capaces de garantizar:

- La Confidencialidad de los datos, en el caso que fuesen interceptados durante la transmisión, no pueden ser decodificados. De este modo, la información no puede ser interpretada por nadie más que los destinatarios de la misma.
- Integridad de los datos, además de no ser interpretados, los datos no pueden ser modificados o alterados durante la transmisión.
- La Autenticación y Autorización, garantiza que los datos están siendo transmitidos o recibidos desde dispositivos remotos autorizados y no desde un equipo cualquiera haciéndose pasar por él. Además, administra los distintos niveles de accesos y derechos de cada uno de los usuarios que utilizan la VPN.

Este trabajo de grado busca continuar con el estudio de la conectividad segura usando las VPN e incursionar en el desarrollo de aplicaciones para asesorar a las diferentes organizaciones. Con este trabajo de grado se pretende ampliar el conocimiento de conectividad segura basado en VPNs y simular el funcionamiento de IPSEC, crear la documentación sobre la implementación de la conectividad segura para redes de comunicación, la que servirá como referente para prestar el servicio de asesoría a las diferentes organizaciones. Por último, se pretende desarrollar una presentación en formato multimedia y realizar una evaluación de los paquetes de software de distribución libre disponibles en la actualidad.

En conclusión, el problema consiste en analizar los temas fundamentales en el área de **conectividad segura**, a fin de proponer una metodología que facilite el diagnóstico, diseño e implementación de sistemas de seguridad perimetral en las redes de comunicación de cualquier organización que lo requiera.

4. JUSTIFICACION

Con la explosión del uso masivo de Internet, tanto los ordenadores personales como las redes de ordenadores, pueden ser vulnerables a diversos tipos de ataques. Internet ha pasado a ser sin ningún tipo de dudas la mayor red pública de datos, a través de la cual se facilitan comunicaciones personales y empresariales en todo el mundo. El volumen de tráfico de datos que se mueve en Internet crece exponencialmente de forma diaria. Día a día crece el número de comunicaciones vía correo electrónico, acceso a las redes corporativas de tele trabajadores o personas que se desplazan constantemente, transacciones comerciales, etc.

Conforme va aumentando el uso de la red de redes, aumentan las posibles amenazas sobre las distintas empresas y particulares que hacen uso de Internet. Entre los posibles ataques a los que puede estar sujeta una red corporativa o un particular se encuentran los virus, vándalos y troyanos; los ataques de hackers como podrían ser ataques de reconocimiento, de acceso, de negación de servicios y de interceptación de datos; e incluso una empresa debe ser capaz de estar protegida frente a los ataques desde dentro de la misma empresa, donde los mismos empleados de forma inconsciente, negligente o vengativa pueden causar daños irreparables.

Entre las principales consecuencias de estos ataques se encuentran la pérdida de datos de vital importancia, violación de la privacidad y caída de la red durante varios días.

Es importante, por parte de las empresas el establecer un sistema total de seguridad basado en sus políticas previamente definidas.

Una red privada virtual conecta los componentes y recursos de distintas redes a través de una transmisión segura sobre una red pública mediante el uso de tunnelling y encriptación para la privacidad de los datos y obtener una calidad del servicio (QoS) con el fin de lograr la fiabilidad deseada en la transmisión (ver figura 1).

Las VPNs van a ser en los próximos años el tipo de redes más utilizado, dado que mediante la utilización de redes públicas se permite de forma virtual tener redes privadas. Y con ello se consigue una disminución en los costos de comunicaciones entre la sede central de una empresa, las sucursales, los tele trabajadores, etc. permitiendo por ellas discurrir tráfico IP de voz, vídeo y datos.

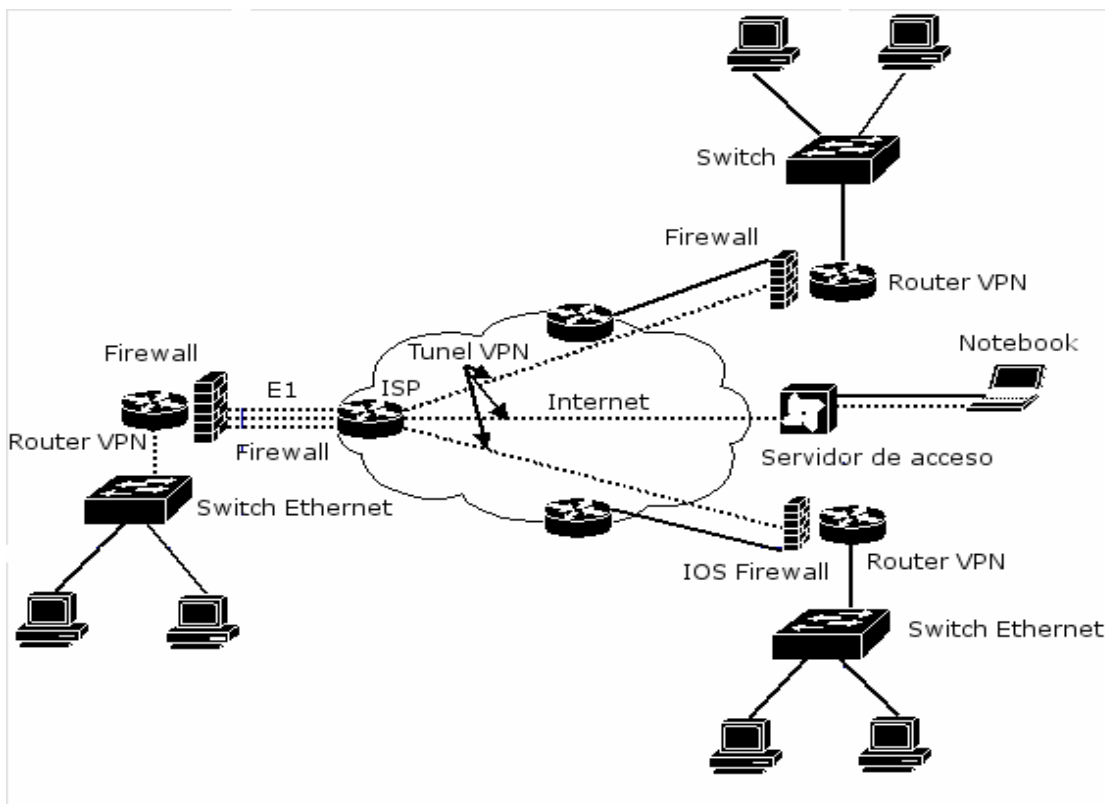


Figura 1: Esquema de una red: VPN y puntos de implementación de conectividad segura

5. OBJETIVOS

5.1 GENERALES

Desarrollar una herramienta software de simulación del algoritmo IPSEC (Seguridad IP), que permita entender el proceso base de las VPNs (Virtual Private Networks) para el aprendizaje.

5.2 ESPECIFICOS

- Desarrollar una herramienta multimedia de entrenamiento, que permita representar el funcionamiento y las soluciones basadas en VPNs en el ámbito de la conectividad segura, en Redes de Comunicaciones.
- Estudiar y evaluar las soluciones basadas en software libre para la conexión segura usando VPNs, que sean de utilidad para una organización que posea una red de 50 a 500 host, lo cual incluye:

- Evaluación de posibles soluciones.
- Evaluación de costos en la implementación.
- Evaluación de las relaciones costo/beneficio.

6. MARCO TEORICO

REDES PRIVADAS VIRTUALES [7]

En una red privada virtual todos los usuarios parecen estar en el mismo segmento de LAN³, pero en realidad están conectados por medio de varias redes (generalmente públicas).

Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas: primero, deben ser capaces de pasar paquetes IP a través de un *túnel* en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública; la solución debe agregar *encriptación*, de manera que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado; y por último, la solución debe ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación, de modo que un adversario no pueda acceder a los recursos del sistema.

Una definición simple es que se trata de una red de comunicaciones privada implementada sobre una infraestructura pública.

Las razones que impulsan al mercado en ese sentido son, fundamentalmente, de costos: es mucho más barato interconectar filiales utilizando una infraestructura pública que implementar una red físicamente privada. Por otro lado, como es lógico, es necesario exigir ciertos criterios de privacidad y seguridad, por lo que normalmente debemos recurrir al uso de la criptografía.

Una red privada virtual conecta los componentes de una red sobre otra red. Las VPN logran esto al permitir que el usuario haga un túnel a través de Internet u otra red pública, de manera que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que antes sólo estaban disponibles en las redes privadas. Las VPN permiten a los usuarios que trabajan desde el hogar o en el camino conectarse en una forma segura a un servidor corporativo remoto, mediante la infraestructura de entubamiento que proporciona una red pública (como Internet).

³ Local Area Network

Desde la perspectiva del usuario la VPN es una conexión de punto a punto entre la computadora del usuario y un servidor corporativo. Por su parte, la naturaleza de la red intermedia es irrelevante para el usuario, debido a que aparece como si los datos se estuvieran enviando sobre un enlace privado dedicado.

La tecnología VPN también permite que una compañía se conecte a las sucursales o a otras compañías (extranets) sobre una red pública (como Internet), manteniendo al mismo tiempo comunicaciones seguras.

La tecnología de la VPN está diseñada para tratar temas relacionados con la tendencia actual de negocios hacia mayores telecomunicaciones, operaciones globales ampliamente distribuidas y operaciones con una alta interdependencia de socios, donde los trabajadores deben conectarse a recursos centrales y entre sí.

Para proporcionar a los empleados la capacidad de conectarse a recursos de cómputo corporativos sin importar su ubicación, una compañía debe instalar una solución de acceso remoto que sea confiable y escalable. Por lo común, las compañías eligen una solución basada en un departamento de sistemas que está encargado de adquirir, instalar y mantener los conjuntos de módems corporativos y la infraestructura de red privada; también eligen una solución de Red de valor agregado (VAN), donde contratan a una compañía externa para adquirir, instalar y mantener los conjuntos de módems y una infraestructura de telecomunicaciones.

REQUERIMIENTOS BASICOS DE LAS VPN [8]

Por lo general, al implementar una solución de red remota, una compañía desea facilitar un acceso controlado a los recursos y a la información de la misma. La solución deberá permitir la libertad para que los clientes roaming o remotos autorizados se conecten con facilidad a los recursos corporativos de la red de área local (LAN) así como las oficinas remotas se conecten entre si para compartir recursos e información. Por último, la solución debe garantizar la privacidad y la integridad de los datos al viajar a través de Internet público. Lo mismo se aplica en el caso de datos sensibles que viajan a través de una red corporativa. Por lo tanto, como mínimo, una solución de VPN debe proporcionar lo siguiente:

Autenticación de usuario. La solución deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados. Además, deberá proporcionar registros de auditoría y contables para mostrar quién accedió a qué información y cuándo.

Administración de dirección. La solución deberá asignar una dirección al cliente en la red privada, y asegurarse de que las direcciones privadas se mantengan así.

Encriptación de datos. Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

Administración de llaves. La solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.

Soporte de protocolo múltiple. La solución deberá manejar protocolos comunes utilizados en las redes públicas; éstos incluyen Protocolo de Internet. Una solución de VPN de Internet basada en un Protocolo de túnel de punto a punto (PPTP) o un Protocolo de túnel de nivel 2 (L2TP) cumple con todos estos requerimientos básicos, y aprovecha la amplia disponibilidad de Internet a nivel mundial.

TIPOS DE REDES VIRTUALES PRIVADAS [6]

Las redes privadas virtuales se dividen en 3 categorías de acuerdo con el servicio de conectividad que brinden:

VPN de Acceso Remoto.

(Remote Access VPNs). Provee acceso remoto a la intranet o extranet corporativa a través de una infraestructura pública, conservando las mismas políticas, como seguridad y calidad de servicio, que en la red privada. Permite el uso de múltiples tecnologías como discado, ISDN, xDSL, cable, o IP para la conexión segura de usuarios móviles, *telecommuters* o sucursales remotas a los recursos corporativos.

Características:

- ▶ Outsourcing de acceso remoto
 - llamadas locales o gratuitas
 - ubicuidad del acceso
 - ▶ Instalación y soporte del PS (Proveedor de servicio)
 - ▶ Acceso único al nodo central (elimina la competencia por puertos)
 - ▶ Tecnologías de acceso RTC⁴, ISDN, xDSL
-
- ▶ Movilidad IP
 - ▶ Seguridad reforzada por el cliente
 - AAA en el ISP proporciona 1° y posiblemente 2° nivel de seguridad.

VPN de Intranet.

Vincula la oficina remota o sucursal a la red corporativa, a través de una red pública, mediante enlace dedicado al proveedor de servicio. La VPN goza de las

⁴ Run Time Checks

mismas cualidades que la red privada: seguridad, calidad de servicio y disponibilidad, entre otras.

Característica:

- ▶ Extiende el modelo IP a través de la WAN compartida.

VPN de Extranet.

Permite la conexión de clientes, proveedores, distribuidores o demás comunidades de interés a la intranet corporativa a través de una red pública.

Características:

- ▶ Extiende la conectividad a proveedores y clientes
 - sobre una infraestructura compartida
 - usando conexiones virtuales dedicadas
- ▶ Los socios tienen diferentes niveles de autorización
 - Access control lists, firewalls, filtros, según decida la empresa.

Seguridad en las VPNs [1]

Un punto fundamental es el particionamiento de las redes públicas o de uso compartido para implementar las VPN que son disjuntas. Esto se logra mediante **el uso de túneles, que son técnicas de encapsulado del tráfico**. Las técnicas que se utilizan son: **GRE**, que permite que cualquier protocolo sea transportado entre dos puntos de la red encapsulado en otro protocolo, típicamente IP; **L2TP** que permite el armado de túneles para las sesiones PPP remotas, y por último **IPSec** para la generación de túneles con autenticación y encriptado de datos.

La calidad de servicio permite la asignación eficiente de los recursos de la red pública a las distintas VPNs para que obtengan un desempeño predecible. A su vez, las VPNs asignarán distintas políticas de calidad de servicio a sus usuarios, aplicaciones o servicios. Las componentes tecnológicas básicas son:

Clasificación de Paquetes: asignación de prioridades a los paquetes basados en la política corporativa. En teoría se pueden definir hasta siete clases de prioridades utilizando el campo de *IP precedence* dentro del encabezado del paquete IP.

Committed Access Rate (CAR): garantiza un ancho de banda mínimo para aplicaciones o usuarios basándose en la política corporativa.

Weighted Fair Queuing (WFQ): determina la velocidad de salida de los paquetes en base a la prioridad asignada a éstos, mediante el encolado de los paquetes.

Weighted Random Early Detection (WRED): complementa las funciones de TCP en la prevención y manejo de la congestión de la red, mediante el descarte de paquetes de baja prioridad.

Generic Traffic Shaping (GTS): reduce la velocidad de salida de los paquetes con el fin de reducir posibles congestiones de la red que tengan como consecuencia el descarte de paquetes.

6.1 ESTADO DEL ARTE

La conectividad segura a través de Internet por medio de Redes privadas virtuales (VPNs) ofrece protección para las empresas que dependen de la conectividad a Internet. La tecnología de las VPN consiste en Concentradores de VPN, *Routers* de VPN dedicados y en los protocolos de túnel y de cifrado en los *routers* y *firewalls*. Ejemplo de soluciones de VPN extremo a extremo son los *routers* 7100 de Cisco (de terminación de extremo inicial) y 1700 y 2600 de Cisco (de terminación de extremo final). Para VPNs de acceso remoto, se tienen concentradores de VPN como el VPN 3000 concentrador de Cisco o el software *Easy VPN server* de Cisco, también existen diversas soluciones basada en software de distribución pública.

7. ASPECTOS METODOLOGICOS

Este trabajo de grado, se puede dividir en cuatro pasos fundamentales, para el logro de los objetivos:

Dar continuación a los estudios realizados en el trabajo de grado del Ingeniero Fernando Andrés Arévalo Jiménez, que se titula “Como escoger e implementar una VPN conceptos teóricos y prácticos”, pero centrándonos específicamente en el estudio del protocolo IPSEC y en las posibles soluciones actuales, basadas en VPN.

Se ampliará el conocimiento teórico que nos permitan asesorar en el tema de VPN y profundizar en el funcionamiento del algoritmo IPSEC.

Esta parte requiere de recolectar y sintetizar toda la documentación pertinente a la conectividad segura y soluciones actuales en redes de comunicación y del funcionamiento de IPSEC.

Esta documentación pretende explicar la técnica base en el desarrollo de los elementos que constituyen la conectividad segura mediante protocolo IPSEC, en las redes de comunicaciones.

También se pretende desarrollar una simulación de la técnica base. Esto incluye definir la plataforma a utilizar ya sea Matlab u otra herramienta. La escogencia de esta herramienta se hará bajo criterios de funcionalidad para la implementación de algoritmos, disponibilidad y aplicabilidad para el desarrollo de ambientes amistosos con el usuario.

Desarrollar una presentación gráfica de cada tema implicado en la conectividad segura para redes de comunicaciones que pueda servir como herramienta de entrenamiento, capacitación y asesoría en el tema.

También se debe definir la plataforma a utilizar. Esta plataforma para desarrollo de documentaciones gráficas puede ser: JAVA o Flash de Macromedia. La escogencia de esta herramienta se realizará bajo criterios de disponibilidad, acceso a la documentación, fácil manejo y pertinencia de la herramienta.

Como último paso se hará el informe correspondiente a toda la ejecución del proyecto con base en los resultados obtenidos.

8. RESULTADOS ESPERADOS

Como resultado principal se espera el desarrollo y la consecución de todos los objetivos anteriormente propuestos. El desarrollo de estos objetivos implica el desarrollo de un proyecto que permitirá:

1. Obtener un informe que facilite la asesoría a las diferentes organizaciones sobre la implementación de soluciones VPN y del funcionamiento del algoritmo IPSEC de conectividad segura en sus redes de comunicación.
2. Diseñar una documentación gráfica para poder realizar la capacitación y asesoría a cualquier entidad sobre las soluciones VPN y el algoritmo IPSEC.
3. Dotar al laboratorio de comunicaciones de una herramienta para la simulación del protocolo IPSEC.
4. Realizar un documento donde se informe sobre el análisis, valoración e implementación de software para la aplicación de conectividad en redes.

Se espera dejar un documento que sirva de base para posteriores desarrollos sobre nuevas implementaciones o distintas tecnologías aplicadas a la conectividad segura.

9. PRESUPUESTO

El trabajo de grado se financiará con recursos propios. En la tabla se presenta una relación de costos detallada.

Necesidad	Costo
Computador	3.000.000
Internet	500.000
Insumos	200.000
Material bibliográfico	500.000
Impresión	100.000
TOTAL	4.500.000

Tabla 1: Presupuesto

10. CRONOGRAMA DE ACTIVIDADES

Las actividades para el desarrollo del trabajo de grado serán divididas en los cuatro pasos mencionados en los aspectos metodológicos. El siguiente cuadro resume en tiempo el cronograma de actividades a desarrollar.

PASO	MES								
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE
	2006	2006	2006	2006	2006	2006	2006	2006	2006
PASO1									
PASO2									
PASO3									
PASO4									

Tabla 2: Cronograma de actividades

11. GLOSARIO

Autenticación: Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc).

Backbone: Enlace de gran caudal o una serie de nudos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red. Por ejemplo, NSFNET fue el backbone, la columna o el eje principal de Internet durante muchos años.

Datagramas: son paquetes de información.

Encriptación: Herramienta que permite ocultar el significado de los mensajes a otras partes que no sean el emisor y el receptor de dicha información, utilizando los distintos sistemas de cifrado.

Extranet: Una extranet es una red privada que usa los protocolos de Internet y el sistema público de telecomunicaciones para compartir, de modo seguro, parte de la información de un negocio o las operaciones con proveedores, vendedores, socios, clientes u otro tipo de negocios. Una extranet puede ser considerada como parte de la intranet de una compañía que se amplía a usuarios que están fuera de la empresa.

Hacker (del inglés *hack*, recortar), también conocidos como "*white hats*" (*sombreros blancos*) o "*black hats*" (*sombreros negros*), según una clasificación de sus *acciones* (según sean sólo destructivas o no, etc.). Es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz, etc.

PSI: Proveedores Independientes de Servicio.

Paquete: Estructura de datos con una cabecera que puede estar o no lógicamente completa. Más a menudo, se refiere a un empaquetamiento físico de datos que lógico. Se utiliza para enviar datos a través de una red conmutada de paquetes.

Red: Es una colección de estándares, basada en dispositivos que encadenan todo lo referente a la compañía, como computadoras de escritorio, servidores y recursos, sin sacrificar velocidad, costo o maniobrabilidad.

Túnel: Técnicas de encapsulado del tráfico.

Virus informático: Es un programa creado especialmente para invadir ordenadores y redes y crear el caos. El daño puede ser mínimo, como que aparezca una imagen o un mensaje en la pantalla, o puede hacer mucho daño alterando o incluso destruyendo ficheros.

12. REFERENCIAS

- [1] AVANTEL. "La importancia de las Telecomunicaciones para las PYMES"
- [2] Azara Félix de. "La información de su empresa donde la necesite" Estrategia Magazine. Edición No 55.
- [3] Caire, Ramiro J, "Introducción a las Redes Privadas Virtuales (VPN) Bajo GNU / LINUX"
- [4] Arévalo J Fernando Andrés. "Cómo Escoger e Implementar una VPN Conceptos Teóricos y Prácticos, Área de Telecomunicaciones, Universidad del Valle, 2003.
- [5] Hevia Mariano, "Virtual Private Networks", Agosto 2001,. Recuperado de Internet:<UR:<http://www.monografias.com/trabajos12/monvpn/monvpn.shtml>>.
- [6] Scott, Charly, Wolfe, Paul, Erwin, Mike. "Virtual Private Networks", 2° edición, O'Reilly & Associates, Enero 1999.
- [7] Gutiérrez González, Ma. Nieves, Sancho Buzón, Ana Rosa, Casas Cuadrado, Amadeo. "Estudio sobre las VPN (Redes Privadas Virtuales)",. Recuperado de Internet: <URL: <http://www.infor.uva.es/~jvegas/docencia/ar/seminarios/VPN.pdf>>.
- [8] Espinosa Jiménez, Ma. Margarita, Hernández García, Mónica, Jurado Quintana, Norma Ivette. "Redes Virtuales Privadas", México D.F, Mayo 28 de 2000.