UNIVERSIDAD JOSÉ ANTONIO PÁEZ

DISEÑO DE UNA RED VIRTUAL PRIVADA PARA LA EMPRESA TELEINTER 2009 C.A. EN NAGUANAGUA, ESTADO CARABOBO

Autores:
Flores, Carlos
Reyes, Andrés

Urb. Yuma II, calle Nº 3. Municipio San Diego
Teléfono: (0241) 8714240 (master)

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA TELECOMUNICACIONES

DISEÑO DE UNA RED VIRTUAL PRIVADA PARA LA EMPRESA TELEINTER 2009 C.A. EN NAGUANAGUA, ESTADO CARABOBO

Trabajo de grado presentado como requisito para optar al título de

INGENIERO TELECOMUNICACIONES.

Autores: Flores, Carlos
C.I.: 20.181.789
Reyes, Andrés
C.I: 24.209.877
Tutor: Ing. Oliger V Mendoza

San Diego, Marzo 2021

FI-T-002-2020-3CR (TG)

Valencia, 26 de marzo de 2021

Ciudadanos:
Flores Alvarado, Carlos Guillermo.
CI. 20.181.789
Reyes Bolívar, Andrés José.
CI. 24.209.877
Presente-

Cumplo con informarle que la Comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión **Nº 05-2021** de fecha **22-01-2021** aprobó el proyecto de trabajo de grado titulado ***DISEÑO DE UNA RED VIRTUAL PRIVADA PARA LA EMPRESA TELEINTER 2009 C.A. UBICADA EN NAGUANAGUA, ESTADO CARABOBO*** presentado por usted (es) como requisito para optar al título de Ingeniero en Telecomunicaciones.

Se ratifica la designación de la Ing. Oliger Mendoza C.I: 16.775.513 como Tutora Académica que lo asesorara en el desarrollo de este proyecto.

Atentamente,

Dr. Francisco Gelanzé Sevilla.
Decano

c.c. Coordinación de Pasantías y Trabajo de Grado (1).

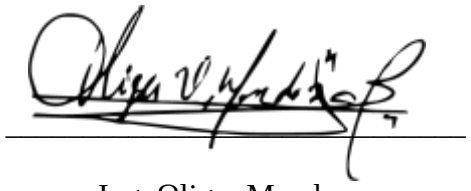
GF/aa

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA TELECOMUNICACIONES

ACEPTACIÓN DEL TUTOR

Quien suscribe, Ingeniero Oliger Mendoza, titular de la cédula de identidad Nº 16.775.513, en mi carácter de tutor del trabajo de grado presentado por los ciudadanos Carlos Flores titular de la cédula de identidad N.º 20.181.789, e Andrés Reyes titular de la cédula de identidad N.º 24.209.877 titulado "**DISEÑO DE UNA RED VIRTUAL PRIVADA PARA LA EMPRESA TELEINTER 2009 C.A. EN NAGUANAGUA, ESTADO CARABOBO"**, presentado como requisito parcial para optar al título de Ingeniero de Telecomunicaciones, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe.

En San Diego, al 02 de abril del año 2021



Ing. Oliger Mendoza.
C.I.: 16.775.513

INDICE GENERAL

IV RESULTADOS

ÍNDICE DE FIGURAS

FIGURA **Pp.**

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA TELECOMUNICACIONES

DISEÑO DE UNA RED VIRTUAL PRIVADA PARA LA EMPRESA TELEINTER 2009 C.A. EN NAGUANAGUA, ESTADO CARABOBO

Autores: Flores, Carlos.
Reyes, Andrés.
Tutor: Ing. Oliger Mendoza
Fecha: Marzo 2020.

RESUMEN

El mundo ha cambiado últimamente y ya no solo interesa tratar asuntos locales o regionales, ahora muchas empresas tienen que lidiar con mercados de logística globales, pero siempre hay algo que necesitan: comunicación segura, confiable y rápida sin importar dónde estén sus oficinas. Una solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas, sin embargo, el costo es alto. Para esto se crean las Redes Privadas Virtuales (VPN). Redes artificiales que utilizan Internet como medio de transmisión junto a un protocolo de túnel garantizando confidencialidad, bajo costo, autenticación y que la información recibida sea la enviada son algunas de las características de VPN, además de su sistema de cifrado de mensajes. El sistema propuesto se basa en el diseño de la red privada virtual para la empresa Teleinter 2009 C.A por la cual se puedan conectar todos sus trabajadores por acceso remoto a las redes. Por otro lado, el proyecto de investigación está enmarcado dentro de la modalidad de investigación de proyecto factible, bajo los lineamientos de la investigación de campo, con un nivel descriptivo y documental.

Descriptores: diseño, red virtual privada, VPN, empresa.

INTRODUCCIÓN

Hace unos años con el surgimiento masivo de las estructuras de red locales a niveles empresariales no era aún significativo la conexión de usuarios a Internet para asuntos laborales, pero a medida que ha pasado el tiempo las compañías han requerido que sus redes locales trasciendan más allá del ámbito de la oficina e incluyeran a los trabajadores y centros de información de otros edificios, ciudades, estados o incluso otros países. Para esta causa tenían que invertir en hardware y servicios de telecomunicaciones costosos para crear redes amplias de servicio, además de líneas dedicadas para el acceso WAN. Sin embargo ya con la llegada y popularización de Internet, las compañías tienen la posibilidad de crear enlaces virtuales que demandan una inversión relativamente pequeña de hardware, ya que utilizan la infraestructura ya establecida como publica para la conexión entre los puntos de la red.

Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras usualmente sin pensar en la seguridad de la información o preocuparse mucho por ella y verdaderamente cuán importante es esta ya que Internet no es un medio de difusión seguro, nacieron una serie de normas y protocolos especiales que permiten encriptar información y permitir únicamente a la persona autorizada desencriptar esta información con un identificador que comprueba que la transmisión se ha hecho desde una fuente confiable.

Este conjunto se conoce actualmente como configuración VPN de redes, y muchas empresas comienzan a utilizarlo, ya sea para interconectar sub-redes como teletrabajadores. 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 la oficina. En la actualidad existen dispositivos especiales que otorgan niveles de seguridad esenciales para realizar enlaces remotos entre empresas, a estos equipos se les conoce como equipos VPN. Es por esto que la empresa TeleInter 2009 C.A debido a la pandemia del CodVid-19 hace necesario la conexión por acceso

remoto, y así conectar a sus trabajadores con las redes de la empresa para poder solucionar cualquier falla o avería que se presente.

Es por esto que el presente proyecto busca de un modo de integrar a los trabajadores de la empresa a través de una Red Privada Virtual VPN, para poder lograr sus funciones de trabajo desde su hogar y no exponiéndose a la pandemia del CodVid-19.

Por lo tanto, el objetivo principal del trabajo de grado es Diseñar una Red Virtual Privada para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo.

El presente trabajo de investigación está estructurado en cuatro capítulos, con el fin de cumplir las normativas establecidas por la Universidad José Antonio Páez, dichos capítulos se describen a continuación:

Capítulo I: referido al problema, su planteamiento el cual se trata de comprobar durante todo el curso de la investigación por medio de los objetivos generales y específicos, así como la justificación del estudio y su alcance.

Capítulo II: se hace hincapié en los antecedentes y bases teóricas.

Capítulo III: Marco Metodológico se plantea la naturaleza de la investigación, la cual por sus características, se trata de una investigación documental con carácter descriptivo, de modo que la estrategia metodológica seleccionada servirá de guía para el desarrollo del trabajo de grado.

Capítulo IV: este capítulo se hablará de los resultados que fueron desarrollados en cada una de las fases para llegar al objetivo principal de este proyecto de grado.

CAPÍTULO I
EL PROBLEMA

1.1 Planteamiento del problema

El ser humano se encuentra en la llamada era de la Información. Mientras que en el pasado las únicas tecnologías para realizar comunicaciones eran el telégrafo y más tarde el teléfono, a partir de la segunda mitad del siglo XX, la computadora se ha convertido en el medio favorito para poder comunicarse. Hoy en día, la información se ha convertido en el elemento más importante en una organización, sobre todo para aquellas que poseen sucursales, clientes y socios comerciales distribuidos a lo largo de la ciudad, país, e incluso a nivel internacional, los cuales necesitan tener acceso a las bases de datos y procesos en línea que reflejen la situación real de la misma.

Sin embargo todo tipo de organizaciones, ya sea empresas grandes y pequeñas, universidades, institutos, gobierno, etc., requieren de métodos para poder transmitir información de forma rápida, eficiente, segura y a un precio razonable. Esto lleva al desarrollo continuo de tecnologías de la información y actualización de las ya existentes con el fin de satisfacer las necesidades de dichas organizaciones en este mundo globalizado. Entonces las empresas no cuentan con estas conexiones ya que resultan muy costosas, sobre todo cuando se trata de grandes distancias, y muchas veces el enlace no se encuentra disponible en el lugar de destino cual agrava la situación. Por esta razón la información llega con retardos y corre el riesgo de ser alterada en el camino, lo cual afecta los procesos de la corporación.

Es por esto que mantener esta situación disminuye la eficiencia y la productividad de las empresas en las operaciones de negocio, debido a que la información se encuentra en forma aislada y resulta difícil ubicarla rápidamente. Por tal motivo, se requiere la interconexión de los clientes, socios y oficinas que la conforman de manera que los usuarios remotos se consideren parte de la Red de Área

Local (LAN) empresarial. Todo esto debe ser realizado sin afectar la seguridad de la empresa, al garantizar que la información relacionada a los procesos claves de la organización solo pueda ser solicitada por los miembros autorizados para tales fines; y que además presente costos competitivos que representen una opción atractiva desde el punto de vista económico.

En tal sentido, la tecnología de Virtual Private Network (VPN) surge como un medio para utilizar el canal público de Internet para comunicar datos privados utilizando llamadas locales, proporcionando además seguridad a través de técnicas de encriptación y encapsulamiento.

Actualmente los trabajadores de la empresa TeleInter 2009 C.A requieren conexión externa para acceder al sistema, esto debido a la pandemia del covid-19 es el principal motivo, ya que millones de personas en Venezuela se encuentren ahora en cuarentena, no pasando por alto una de las principales estados del país siendo este Carabobo se ha visto afectado por dicho virus y con ello las empresas, ya que los trabajadores deben ausentarse de sus puestos de trabajo para evitar la propagación del virus. Esto conlleva que la empresa TeleInter 2009 C.A se haya visto impactada a nivel de productividad y economía en el proceso de sus operaciones, para llevar a cabo sus objetivos , ya que sus empleados no tienen acceso controlado, eficiente y seguro a la red de área local,

Es por esto que los trabajadores requieren conexión externa constantemente para acceder al sistema y solucionar problemas inesperados, pero realizar este tipo de conexión además de ser beneficioso puede generar un riesgo o un ataque a la seguridad del sistema por lo cual la empresa debe contar con un mecanismo de acceso remoto como es la VPN; manteniendo la seguridad de sistema, ya que esta proporciona un canal de comunicación seguro a través de internet para oficinas remotas, usuarios móviles y socios comerciales disminuyendo costos asociados a enlaces dedicados como se trabajaba anteriormente.

Entorno a esto el diseño de una Red Privada Virtual como una alternativa para el acceso remoto, es una necesidad que se hace evidente en el momento para la

empresa Teleinter 2009 C.A.

1.2 Formulación del problema

Del planteamiento del problema descrito anteriormente se deriva las siguientes interrogantes:

¿Cómo se puede mejorar la conexión externa para acceder al sistema de la empresa Teleinter 2009 C.A. que sea segura y confiable?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

Diseñar una Red Virtual Privada para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo.

1.3.2 Objetivos Específicos

- Diagnosticar la situación actual de la red corporativa de la empresa Teleinter 2009 C.A
- Identificar los parámetros, dispositivos y entornos para el diseño de la red virtual privada (VPN).
- Diseñar el sistema de la red privada virtual (VPN) para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo.
- Realizar un estudio de factibilidad, económico, técnico y ambiental para la red privada virtual (VPN) para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo.

1.4 Justificación

El presente trabajo de grado tiene como principal objetivo la propuesta de diseño de una Red Virtual Privada para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo. Este trabajo es de gran importancia ya que a través del diseño de una Red Privada virtual se puede conectar todos los empleados de la empresa en una red corporativa ancha a través de Internet, disminuyendo los costos de largas distancias.

Además, al utilizar ciertos protocolos permite una conexión segura similar a la existente en una red privada tradicional; por lo cual representa una opción atractiva para establecer conexiones remotas en una organización. Al igual, proporciona conocimientos acerca de una nueva forma de establecer conexiones remotas económicas y seguras: las Redes Privadas Virtuales, y los resultados servirán de guía para que las empresas la consideren como alternativa en el momento de adquirir u optimizar sus conexiones remotas, facilitando así la toma de decisiones.

Por otro lado con este diseño de red privada virtual (VPN) se puede aprovechar las tecnologías que implementen seguridad, ya que estas tecnologías son utilizadas en la mayoría de dispositivos empleados en redes de internet.

Así mismo la investigación ofrece a la Universidad José Antonio Páez el incentivo a los demás estudiantes a investigar más en el área de las telecomunicaciones y conexiones externas a sistemas remotos ya que esta propuesta puede impulsar y ser implementada en distintas universidades para proporcionar una conexión segura a todos sus empleados.

1.5 Alcance de la Investigación

Con la investigación se pretende llegar al diseño de una Red Virtual Privada para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo, el cual permita a todos los empleados de la empresa el acceso remoto para acceder al sistema y solucionar problemas inesperados.

1.6 Limitaciones

Todos los casos de estudio no poseen las mismas limitaciones, cada una de estas prestaran diferentes particularidades, es el tiempo un factor limitante al desarrollo del trabajo, puesto que este no pudiera haber sido suficiente para la mayor profundización en el periodo evaluado. Así mismo, pudo haber limitaciones en cuanto a los recursos especialmente financieros para poder desarrollar un dispositivo con alta calidad, es importante destacar que, aunque se consiguió información relevante para la investigación, la misma fue limitada.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes

Mendoza, A. (2017) en su trabajo de grado **"Diseño e implementación de un prototipo de red privada virtual en capa 3 utilizando Cisco IOS para la Universidad Nacional del Altiplano".** Presentado en la Universidad Nacional del Altiplano para optar por el título de Ingeniero Electrónico, Perú (Puno). El presente trabajo explica que en la Universidad Nacional del Altiplano cuenta con un sistema de intercambio de información primordial para el trabajo de dicha institución. Mediante esta red se intercambian los datos de exámenes de admisión, ingresantes a esta casa superior de estudios, datos de los estudiantes, tales como notas, datos de los docentes, entre otros. Es así, que siendo esta red el eje principal para el trabajo de la Universidad Nacional del Altiplano, se encuentra expuesta a ataques cibernéticos y a riesgos de perdida de información que se envía entre las diferentes oficinas.

Siendo la finalidad proteger esta información y sobre todo evitar la vulnerabilidad de estos datos una vez subidos a la Internet, es que se ha realizado el diseño y posterior implementación de un prototipo de Red Privada Virtual en la capa de Red, utilizando protocolos de enrutamiento óptimos para el tipo de información que se requiera enviar y protocolos de encriptación para el cifrado de estos datos, acoplándolos a CISCO IOS. Para lograr que la utilización de éste prototipo sea factible en la institución, se realizaron diferentes diseños que permitan la implementación real de la red privada virtual; además los resultados obtenidos en la pruebas del prototipo mostraron que nuestra red transmite los datos de un punto a otro encriptándolos y encapsulándolos con el conjunto de protocolos IPsec que trabaja en la capa 3 o capa de red configurada con Cisco IOS.

Los resultados fueron obtenidos con los programas Packet Tracer y Wireshark siendo estos satisfactorios. De esta manera se comprobó que nuestro prototipo de Red Privada Virtual brinda la autenticación, integridad y confidencialidad a los paquetes transmitidos entre la Oficina de Tecnología e Informática y las coordinaciones académicas de la institución, teniendo como resultado una Red segura y confiable protegida en LAN y WAN con un rendimiento mínimo de 89.29% de los 56 datos transmitidos a partir de las pruebas realizadas, y fue implementada dentro del Laboratorio Cisco de la Universidad Nacional del Altiplano demostrando que esta red puede ser aplicada en equipos reales a todas las oficinas de la institución.

El proyecto se vincula con el actual en función de cómo usar los programas de Packet Trace para poder realizar el diseño de la Red Virtual Privada (VPN), para la empresa Teleinter 2009 C.A..

Por otra parte, Peña, V. (2017) en su trabajo de grado **"Diseño e implementación de un Red Privada Virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada".** Presentado en la Universidad Nacional para optar por el título Especialista en Comunicaciones y Redes de Comunicaciones de Datos. Ecuador. La investigación tuvo como propósito diseñar e implementar una Red Privada Virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada, con el objetivo de proteger las conexiones de acceso remoto hacia la organización a través del contenido cifrado, garantizando la integridad, confidencialidad y seguridad de los datos. En su desarrollo, se abordaron aspectos teóricos de una VPN, seguridad y documentación de los protocolos que se utilizan actualmente para las conexiones seguras de acceso remoto. En base a ello se llevaron a cabo cada una de las fases planificadas, logrando la implementación de una VPN-SSL integrada con el protocolo LDAP. Se realizaron una serie de adecuaciones y configuraciones en la empresa privada en el que se definió la política de acceso remoto a la red.

El proyecto se vincula con el actual en función de la selección del software Windows Server 2012 que será propuesto en este trabajo de grado, por otro lado la

elección del software correcta para la realización del proyecto es esencial, en este trabajo de grado ya que es la base para la propuesta y desarrollo de la Red Privada Virtual (VPN), por lo que es necesario considerar toda la información disponible y herramientas empleadas para el desarrollo de este proyecto.

Por último, Pulido y Velázquez (2019) en su trabajo de grado **"Sistema de una Red Privada Virtual para Radio América en Valencia, Estado Carabobo"** para optar por el título de Ingeniero en Telecomunicaciones presentado en la Universidad José Antonio Páez. Facultad de Ingeniería Telecomunicaciones, Venezuela (Carabobo). El presente trabajo de grado ofrece una solución para satisfacer la necesidad de comunicación segura que implica conectar redes remotas mediante líneas dedicadas, por medio de Redes Privadas Virtuales (VPN) a los empleados de la empresa Radio América. Estas redes artificiales que utilizan Internet como medio de transmisión junto a un protocolo de túnel garantizando confidencialidad, bajo costo, autenticación y que la información recibida sea la enviada son algunas de las características de VPN, además de su sistema de cifrado de mensajes. El sistema propuesto se basa en la implementación de la red privada virtual para la empresa Radio América y para ello es necesario una base con las políticas de seguridad, servidor de acceso y autenticación, administración de direcciones y soporte para múltiples protocolos, para poder compartir datos, aplicaciones y recursos.

El proyecto se vincula con el actual en función de la como está estructurado una la Red Virtual Privada (VPN), a través de distintas capas, y el uso del establecimiento para el modelo IOS y sus distintos niveles orientados a redes ya que es la base teórica para la propuesta y desarrollo de este trabajo de grado.

2.2 Bases teóricas

2.2.1 Red

Las redes y en general el uso de ordenadores en las organizaciones, empresas o industrias hoy en día se han incorporado de una manera creciente, y constituyen parte importante de la producción. Una red corresponde a dos o más PC interconectados entre sí para lograr una comunicación, intercambio de datos y a la vez poder

compartir recursos. Debe estar configurada de tal forma que sea compatible a estándares de conectividad preestablecidos. En la actualidad existen varios tipos de redes, es decir están confeccionadas de maneras diferentes según normativas, topologías o equipos que hacen posible la interconexión.

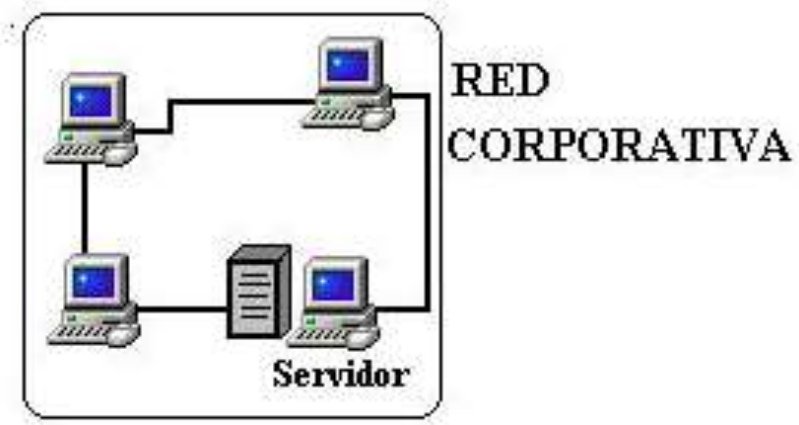


Figura 1. Estructura básica de una RED
Fuente: http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf

Una red no la componen solo los PC, existen equipos conectados al conjunto que cumplen roles diversos en el sistema, por ejemplo: Servidores, Hubs, Switches, Routers, Concentradores, Firewalls, Gateways, etc. Los cuales se incorporan de acuerdo a las necesidades, tamaño y topología de la red, es decir una red de PC de gran envergadura requerirá equipos que soporten las tareas y exigencias. Un modelo bastante sencillo se puede apreciar en la figura 1.

2.2.2 Red Privada

Una red privada se establece luego de presentarse la necesidad de resguardar la información, es decir existen empresas u organizaciones que deben transmitir sus datos de forma confidencial. Las redes corporativas que manejan tantos antecedentes de fondos y bases de datos tienen carácter de privadas ya que tienen una arquitectura cerrada y para terceros es difícil acceder. Esto se lograra con equipos especiales que bloquean la entrada a terceros, o simplemente estas redes no están conectadas a un medio de difusión pública.

2.2.3 Red Privada Virtual (VPN)

Una red privada virtual (VPN) es en esencia una estructura de red la cual tiene la capacidad de establecer un canal de comunicación privado sobre una infraestructura de red pública. Entonces con VPN es posible establecer una comunicación vía infraestructura pública entre dos estaciones de trabajo remotas sin correr el riesgo que terceras personas ajenas a la organización pueda acceder a dicha información ni al sistema de interconexión. Esta tecnología permite crear un túnel de encriptación a través de la Internet u otra red pública de tal forma que permita a los usuarios que se encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles solo en redes privadas. (Observar figura 2).

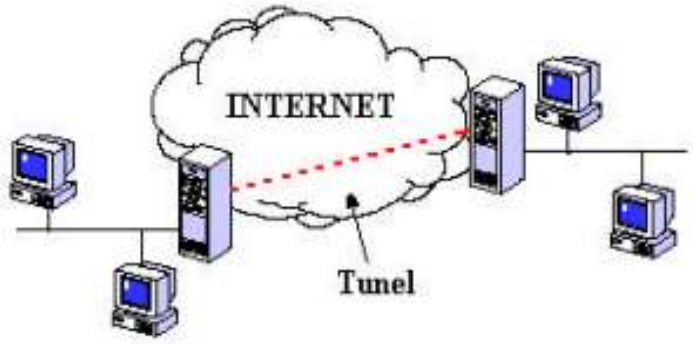


Figura 2. Red ViRtual Privada VPN.
Fuente: http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf

Una Red Virtual Privada (VPN) bien diseñada puede aportar grandes beneficios a una empresa. Por ejemplo, puede:

- Ampliar la conectividad geográfica.
- Reducir los costos de funcionamiento en comparación con las WAN tradicionales.
- Reducir el tiempo de tránsito y los gastos de viaje de los usuarios remotos.
- Mejorar la productividad.

- Simplificar la topología de red.
- Proporcionar oportunidades de trabajo en red global.

El equivalente lógico a esta red VPN corresponde a un enlace privado punto a punto, lo que implica una inversión bastante costosa si se desea realizar una extensión de la red a una distancia considerable. Es decir, se debe realizar una arquitectura de cableados y equipos de conectividad que abarque la zona a la cual se desee llegar

2.2.3.1 Requisitos para una Red VPN

Vincenzo Mendillo (2011), indicó los requisitos para la Red Privada Virtual (VPN), dichos requisitos se pueden agrupar en cuatro áreas principales: compatibilidad, seguridad, disponibilidad e interoperabilidad.

- **Compatibilidad:** para que una VPN pueda utilizar Internet, debe ser compatible con el protocolo de Internet (IP). Resulta obvia esta consideración con el fin de poder asignar y, posteriormente, utilizar conjuntos de direcciones IP. Sin embargo, la mayoría de redes privadas emplean direcciones IP privadas o no-oficiales, provocando que únicamente unas pocas puedan ser empleadas en la interacción con Internet. La razón por la que sucede esto es simple, la obtención de un bloque de direcciones IP oficiales suficientemente grande como para facilitar un subnetting resulta imposible. Las subredes simplifican la administración de direcciones así como la gestión de los routers y conmutadores, pero malgastan direcciones muy preciadas. Actualmente existen varias técnicas con las que se puede obtener la compatibilidad deseada entre las redes privadas e Internet, por ejemplo la conversión a 29 direcciones Internet mediante NAT (Network Address Traslation) y el empleo de túneles para encapsulamiento. En la primera de estas técnicas, las direcciones Internet oficiales coexistirán con las redes IP privadas en el interior de la infraestructura de routers y conmutadores de las organizaciones. De este modo, un usuario con una dirección IP privada puede acceder al exterior por medio de un servidor de direcciones IP públicas mediante la infraestructura local y sin necesidad de emplear ningún tipo de acción especial.

- **Seguridad:** debe considerarse seriamente la seguridad cuando se usa Internet. Las comunicaciones ya no van a estar confinadas a circuitos privados, sino que van a viajar a través de Internet, que es considerada una red "demasiado pública" para realizar comunicaciones privadas. Aunque puede parecer poco probable que alguien monitoreando una línea con un sniffer consiga capturar información y hacer uso de ella, ya que está encriptada, la posibilidad existe. Cuando la información está encriptada, se requieren claves para cifrar y descifrar. Los usuarios en cada extremo deben tener las claves adecuadas. Si se está configurando una conexión con una sucursal es fácil administrar este intercambio de claves. Sin embargo, si un usuario remoto accede a la red corporativa, se necesita un modo de verificar quién es y un modo de intercambiar las claves para la encriptación. Las claves públicas basadas en certificados digitales y PKI son los que más de utilizan para este propósito.
- **Disponibilidad:** la disponibilidad viene motivada principalmente por dos variables: una accesibilidad plena e independiente del momento y del lugar, y un rendimiento óptimo que garantice la calidad de servicio ofrecida al usuario final. 30 La calidad de servicio (QoS – Quality of Service), hace referencia a la capacidad que dispone una red para asegurar un cierto grado de operación de extremo a extremo. La QoS puede venir dada como una cierta cantidad de ancho de banda o un retardo que no debe sobrepasarse, o bien como una combinación de ambas. Actualmente, la entrega de datos en Internet es realizada de acuerdo al mejor esfuerzo (best effort), lo cual no garantiza la calidad de servicio demandada. No obstante, en el futuro Internet será capaz de suplir esta carencia ofreciendo un soporte para la QoS a través de un conjunto de protocolos emergentes entre los que cabe destacar DiffServ (Differential Services), RSVP (Resource ReSerVation Protocol) y RTP (Real Time Protocol). Pero por ahora, los proveedores sólo proporcionan la QoS de las VPNs haciendo uso del tráfico

CIR (Committed Information Rate) en Frame Relay u otras técnicas (ejemplo MPLS).

- **Interoperabilidad:** las implementaciones de los tres primeros requisitos han provocado la aparición de un cuarto: la interoperabilidad. Los estándares sobre tunneling, autenticación, encriptación y modo de operación ya mencionados anteriormente son de reciente aparición o bien se encuentran en proceso de desarrollo. Por esta razón, previamente a la adquisición de una tecnología VPN, se debe prestar una cuidadosa atención a la interoperabilidad de extremo a extremo. Esta responsabilidad puede residir tanto en el usuario final como en el proveedor de red, dependiendo de la implementación deseada. Una manera de asegurar una correcta interoperabilidad radica en la elección de una solución completa ofrecida por un mismo fabricante. En el caso de que dicho fabricante no sea capaz de satisfacer todos los requisitos, se deberán limitar los aspectos inter operacionales a un subconjunto que englobe aquellos que sean esenciales, además de utilizar únicamente aquel equipamiento que haya sido probado en laboratorios o bien sometido a pruebas.

2.2.3.2 Razones por las cuales es recomendable implementar una VPN

- **Reducción de Costos:** Para una implementación de red que abarque empresas alejadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto) de muy alto costo que caracterizaron a muchas empresas privadas, siendo reemplazadas por ejemplo, por acceso ADSL de un ancho de banda alto y bajo costo, disponible por lo general en la mayoría de las zonas urbanas sin mayores problemas. Los usuarios remotos móviles podrán ahorrar altos costos de llamadas telefónicas de larga distancia, bastando con que disque un proveedor de acceso local a la Internet (no IP fija).
- **Alta Seguridad:** Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, dando un resultado comparable a una red punto a punto.

Protocolos como 3DES (Triple data encryption Standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindan una alto nivel en seguridad al sistema. Además se utilizan varios niveles de autentificación de usuarios para el acceso a la red privada mediante llaves de ingreso, para la asegurar que el usuario es el original y no un tercero que percibe el password de autentificación.

- **Escalabilidad:** Para agregar usuarios a la red no es preciso realizar inversiones adicionales. La provisión de servicios se hace con dispositivos y equipos fáciles de configurar y manejar. Se usa la infraestructura de alto nivel establecida ya por los proveedores de Internet y no realizar un enlace físico que puede significar una gran inversión monetaria y de tiempo. 4 · Compatibilidad con tecnologías de banda ancha: Una red VPN puede aprovechar infraestructura existente de banda ancha inalámbrica, TV cable o conexiones de alta velocidad del tipo ADSL o ISDN, lo que implica un alto grado de flexibilidad y reducción de costos al momento de configurar la red. Incluso es posible usar voz sobre IP usando la implementación VPN, y esto implica un significativo ahorro en telefonía de larga distancia.
- **Mayor Productividad:** Debido a un mejor nivel de acceso durante mayor tiempo se podría probar que se obtendría una mayor productividad de los usuarios de la RED. Además se fomenta el teletrabajo con la consecutiva reducción en las necesidades de espacio físico.

2.2.3.3 Ventajas y Desventajas de una Red VPN

Ventajas

- Como tecnología de acceso avanzada ofrece múltiples posibilidades. Las opciones para la conectividad se adaptan a los requisitos de cada empresa. Los beneficios de las VPN son conocidos y además útiles para pequeñas y grandes empresas.

- Las VPN tradicionales son fáciles de implementar tanto del lado del ISP como por el del cliente. El proveedor no participa en los procesos de enrutamiento.
- Las VPN peer to peer proporcionan una solución óptima en los procesos de enrutamiento empleando topologías de malla completa proporcionando redundancias entre todos los sitios, sin necesidad de implementar cambios desde el punto de vista del cliente.
- Agregar sitios nuevos es tan simple como el agregado de nuevos routers e interconectarlos a un nuevo bucle local. La configuración no requiere múltiples circuitos para proporcionar capacidades de malla completa.

Desventajas

- El coste y las tareas administrativas asociadas en grandes empresas con las topologías de malla completa pueden ser enormes. Para reducir el número de circuitos virtuales requeridos se deben sacrificar posibles rutas redundantes.
- Las VPN tradicionales también tienen problemas de sobrecarga cuando se utiliza IPsec o GRE. Los principales beneficios de las VPN peer to peer pueden ser también su principal desventaja, como por ejemplo en la participación del enrutamiento del cliente.
- La información de enrutamiento de las distintas redes es redistribuida entre el CE y el PE. Deben aplicarse filtros de enrutamiento en las interfaces de los routers para proteger ambas partes de flujos de rutas no deseadas. El cliente debe confiar en la capacidad del ISP para configurar y mantener la infraestructura de enrutamiento.

2.2.3.4 Componentes de una Red VPN

Los componentes básicos de una VPN aparecen en la figura 3 y son:

- Servidor VPN.
- Túnel.
- Conexión VPN.
- Red pública de tránsito.

- Cliente VPN

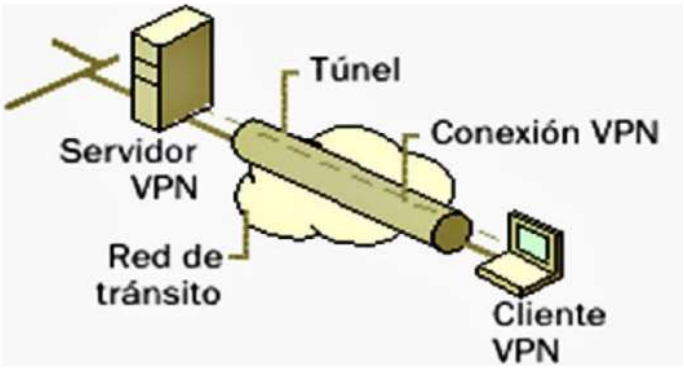


Figura 3. Componentes de una Red VPN
Fuente: http://www.equitek.com.mx/f/ERM-Conversore-Señales-Analògicas.jpg

2.2.3.5 Topologías de una Red VPN

Hay dos tipos básicos de redes VPN:

1) De Sitio a Sitio

Una VPN sitio a sitio se crea cuando los dispositivos de conexión en ambos lados de la conexión VPN son conscientes de la configuración de la VPN. La "VPN permanece estática, y los Host internos no tienen conocimiento de que existe una VPN. Frame Relay, ATM, GRE y VPN MPLS son ejemplos de VPNs sitio a sitio. En una VPN sitio a sitio, los Host envían y reciben tráfico TCP/IP normal a través de un Gateway VPN, lo que puede ser un router, firewall, Concentrador VPN de Cisco, o Cisco ASA 5500 Series Adaptive Security Appliance. El Gateway VPN se encarga de encapsular y encriptar el tráfico de salida de un sitio específico y enviarlo a través de un túnel VPN sobre Internet a otro Gateway VPN en el lugar de destino. Tras la recepción, el Gateway VPN destino retira las cabeceras, descifra el contenido, y reenvía el paquete hacia el host de destino dentro de su red privada. En base a los problemas comerciales que resuelven, las VPN de sitio a sitio pueden subdividirse a su vez en VPN intranet y VPN extranet. VPN intranet. Las VPN intranet se utilizan para la comunicación interna de una compañía, como aparece en la figura 4. Enlazan una oficina central con todas sus sucursales. Se disfrutan de las mismas normas que

en cualquier red privada. Un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN.

VPN extranet. Estas VPN enlazan clientes, proveedores, socios o comunidades de interés con una intranet corporativa, como se muestra en la figura 4. Se puede implementar una VPN extranet mediante acuerdo entre miembros de distintas organizaciones. Las empresas disfrutan de las mismas normas que las de una red privada. Sin embargo, las amenazas a la seguridad en una extranet son mayores que en una intranet, por lo que una VPN extranet debe ser cuidadosamente diseñada con muchas pólizas de control de acceso y acuerdos de seguridad entre los miembros de la extranet. (Observar figura 4).

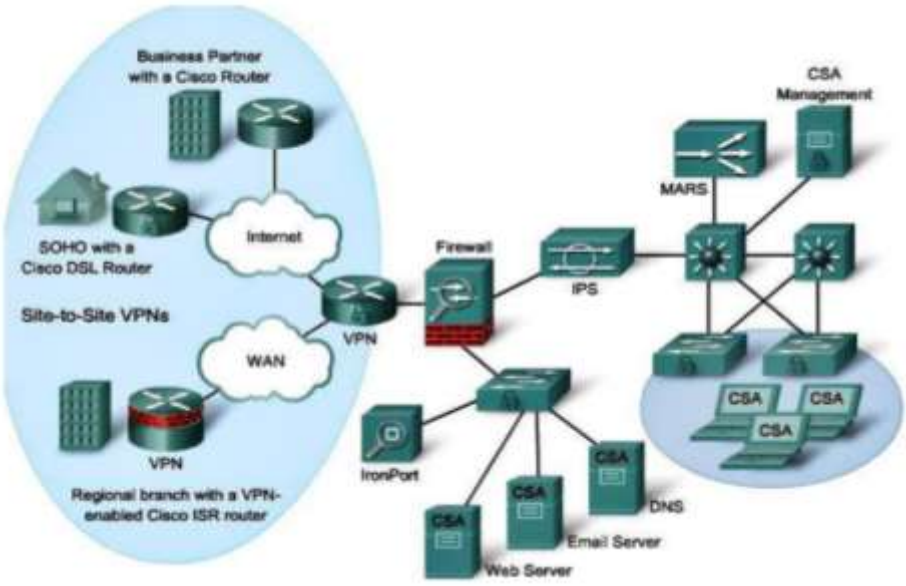


Figura 4. VPN sitio a sitio
Fuente: https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%20Jorge.pdf

2) De acceso remoto

Una VPN de acceso remoto se crea cuando la información no es creada estáticamente, sino que permite cambiar dinámicamente la información y puede ser activado y desactivado. Considere la posibilidad de un teletrabajador que necesita VPN de acceso a los datos corporativos a través de la Internet. El teletrabajador no

tiene necesariamente que configurar la conexión VPN a cada momento. La PC del teletrabajador es responsable de establecer la conexión VPN. La información necesaria para establecer la conexión VPN, tales como la dirección IP de los teletrabajadores y los cambios de forma dinámica dependiendo de la ubicación de cada teletrabajador. VPN de acceso remoto son una evolución de las redes de conmutación de circuitos, como lo era el servicio telefónico antiguo (POTS) o RDSI. Las VPN de acceso remoto puede apoyar las necesidades de los teletrabajadores, los usuarios móviles, y de los consumidores de extranet para el tráfico de negocios. Las VPN de acceso remoto tienen una arquitectura cliente / servidor en el que un cliente VPN (Host remoto) requiere un acceso seguro a la red de la empresa a través de un dispositivo de servidor de VPN en el borde de la red. (Ver figura 5).

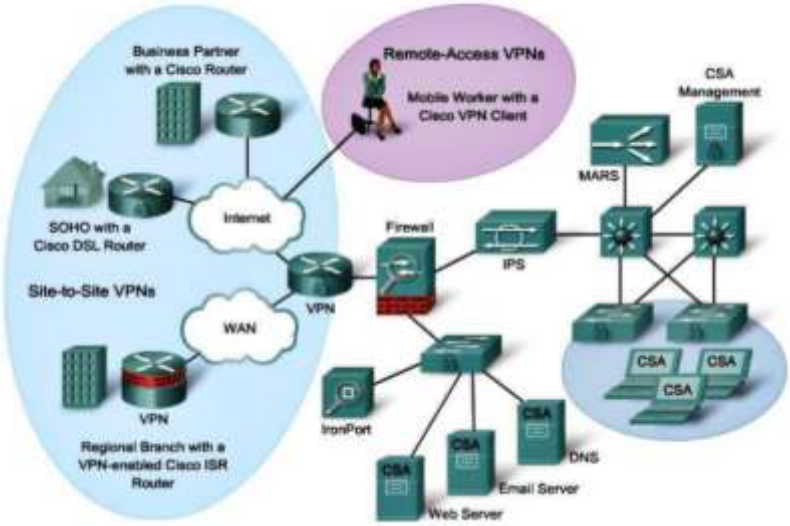


Figura 5. VPN de acceso remoto
Fuente: https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%Selector.pdf

De acuerdo a la tecnología utilizada para establecer la conexión, las VPN de acceso remoto se puede dividir en VPN dial-up y VPN directas:

- VPN dial-up. En esta VPN, el usuario realiza una llamada local al ISP utilizando un módem. Aunque se trata de una conexión lenta es todavía muy común. El uso de este tipo de VPN se da más entre los usuarios móviles, ya

que no en todos los lugares a donde se viaja se pueden tener disponibles conexiones de alta velocidad.

- VPN directa. En esta VPN, se utilizan las tecnologías de conexión a Internet de alta velocidad, tales como DSL y módem de cable las cuales ya ofrecen muchos ISP. Este tipo de VPN se puede encontrar principalmente entre los teletrabajadores. Actualmente se pueden obtener conexiones a Internet desde el hogar utilizando estas tecnologías.

En un acceso remoto VPN, cada Host tiene típicamente un software de cliente VPN de Cisco. Cada vez que el Host intenta enviar tráfico destinado a la VPN, el software Cisco VPN Client encapsula y cifra el tráfico antes de enviarlo por Internet a la puerta de enlace VPN en el borde de la red de destino. Tras la recepción, la puerta de enlace VPN se comporta como lo hace para de una VPN sitio a sitio. (Ver figura 6).

Figura 6. Ventana del Software VPN Client
Fuente: https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%Selector.pdf

2.2.4 Tipos de VPN

2.2.4.1 Sistemas basados en Hardware

Las VPN basadas en Hardware poseen en el extremo del Servidor de la organización un “router” o “enrutador” dedicado el cual tiene la misión de encriptar los datos, además de abrir y cerrar los túneles VPN cuando funciona como receptor.

Estos proporcionan facilidades al usuario que administra la implementación VPN, ya que son seguros, rápidos, de fácil instalación y fáciles de usar. Ofrecen un gran rendimiento ya que no malgastan ciclos en forma tan significativa de procesamiento de operación ya que no requiere un sistema operativo, ya que este es configurado para las operaciones que requiera el servicio VPN.

2.2.4.2 Sistemas basados en Firewall

Estos sistemas aprovechan las ventajas del "Firewall" o "cortafuego" como la restricción de acceso a la red o generación de registros de posibles amenazas, y ofrecen además otras opciones como traducción de direcciones o facilidades de autentificación fuerte. La desventaja de un sistema basado en Firewall afecta en mayor o menor medida al rendimiento del sistema general, lo que puede ser un problema para la organización dependiendo de las necesidades que se requieran. Algunos fabricantes de Firewalls ofrecen en sus productos procesadores dedicados a encriptación para minimizar el efecto del servicio VPN en el sistema.

2.2.4.3 Sistemas basados en Software

Estos sistemas basados en software son ideales en el caso en que los dos extremos que deseen comunicarse en forma remota y privada no pertenezcan a la misma organización. Esta solución permite mayor flexibilidad en cuanto a la decisión de que trafico enviar por el túnel seguro VPN, pudiendo decidir por protocolo y dirección donde en un sistema basado en hardware solo se puede decidir por dirección. Existen desventajas para un sistema basado en software, las cuales consisten en que estos sistemas son difíciles de administrar, ya que necesitan estar familiarizados con el sistema operativo Cliente, la aplicación VPN y los mecanismos de seguridad adecuados.

2.2.5 Modelo OSI

El modelo OSI (Open System Interconnection) es el comienzo de cualquier estudio de redes. Es un modelo idealizado de 7 capas o niveles que representa la subdivisión de tareas teórica que se recomienda tener en cuenta para el estudio o diseño de un sistema. Esto no significa que todas las redes cumplan o deban cumplir

exactamente con este modelo pero se recomienda siempre tener en cuenta el modelo OSI como referencia, ya que conocimiento del mismo posibilita la correcta comprensión de cualquier red e inclusive facilita el poder realizar la comparación entre sistemas diferentes.

A cada capa se le asigna una función específica y las mismas se apilan desde la inferior a la superior de forma que cada una depende de la inmediata inferior para su funcionamiento. Cada capa dialoga con la capa de arriba, y con su par en el otro equipo accesando la capa de abajo, este diálogo se le llama protocolo: conjunto de reglas que gobiernan el intercambio de datos entre entidades de un mismo nivel. La unidad de información que intercambian las entidades de cada capa se le denomina PDU (Protocol Data Unit), cada capa o nivel tiene una misión distinta y no se preocupa de lo que debe hacer otro nivel.

Inicialmente, el modelo OSI fue diseñado por la ISO para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas exclusivos. El modelo OSI proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él. Si bien el contenido de este curso está estructurado en torno al modelo de referencia OSI, el análisis se centra en los protocolos identificados en el modelo de protocolo TCP/IP.

Las 7 capas son las siguientes:

1) Física.: los protocolos de capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia un dispositivo de red y desde él.
2) Enlace de Datos: los protocolos de capa de enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.

3) Red: la capa de red proporciona servicios para intercambiar los datos individuales en la red entre dispositivos finales identificados.
4) Transporte: la capa de transporte define los servicios para segmentar, transferir y rearmar los datos para las comunicaciones individuales entre dispositivos finales.
5) Sesión: la capa de sesión proporciona servicios a la capa de presentación para organizar su diálogo y administrar el intercambio de datos.
6) Presentación: la capa de presentación proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.
7) Aplicación: la capa de aplicación proporciona los medios para la conectividad de extremo a extremo entre individuos de la red humana mediante redes de datos.

En la figura se muestra las 7 capas del modelo IOS

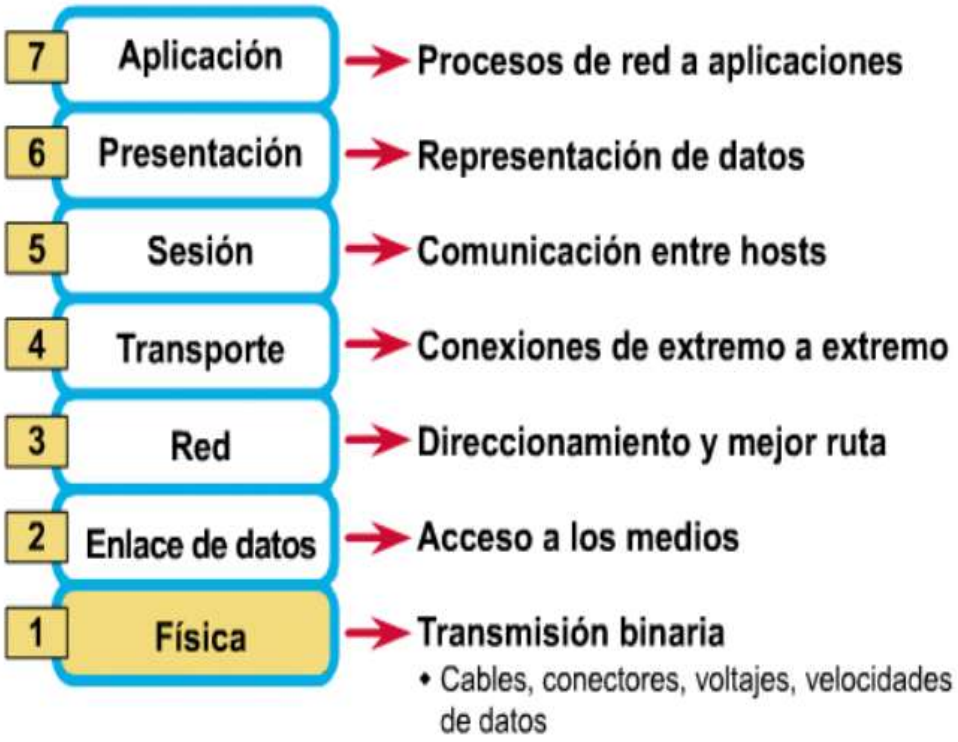


Figura 7. Capas de Modelo IOS
Fuente: https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%Selector.pdf

2.2.5.1 Capa de Red del Modelo OSI

La capa de red (capa 3 OSI) define el enrutamiento y el envío de paquetes entre redes. Su función es transferir datos desde el host que origina los datos hacia el host que los usa, a través de varias redes separadas si fuera necesario. “La capa de red del modelo OSI proporciona el enrutamiento de mensajes y determina si el destino de estos es la capa 4 (Transporte) o la capa 2 (Enlace de Datos)”. Esta capa provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa de red utiliza cuatro procesos básicos:

- ✓ Direccionamiento.
- ✓ Encapsulamiento.
- ✓ Enrutamiento.
- ✓ Desencapsulamiento.

Durante la encapsulación en el host origen, un paquete IP se construye en la Capa de red para transportar el PDU de la Capa 4. Gracias a esto, el paquete puede llevar una PDU a través de muchas redes y muchos routers. Para ello, las decisiones de envío están basadas en la información del encabezado del paquete IP.

2.2.6 Protocolo TCP/IP

El Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP, Transmission Control Protocol/Internet Protocol) es un conjunto de protocolos que permiten la comunicación a través de varias redes diferentes. TCP/IP fue creado por el Departamento de Defensa de Estados Unidos y se diseñó porque se quería un protocolo que fuera capaz de transmitir información en cualquier momento y bajo cualquier condición. Este protocolo tan popular dio origen a Internet, el cual ha posibilitado la interconexión de toda clase de redes a nivel mundial.

2.2.6.1 Modelo TCP/IP

TCP/IP fue diseñado en base un modelo de cuatro capas. Este modelo precedió al modelo OSI y fue muy importante. Aunque los nombres de algunas capas del

modelo TCP/IP son iguales a las del modelo OSI no se debe confundirlas. Las funciones que realizan son diferentes. Estas capas se muestran en la figura 8.

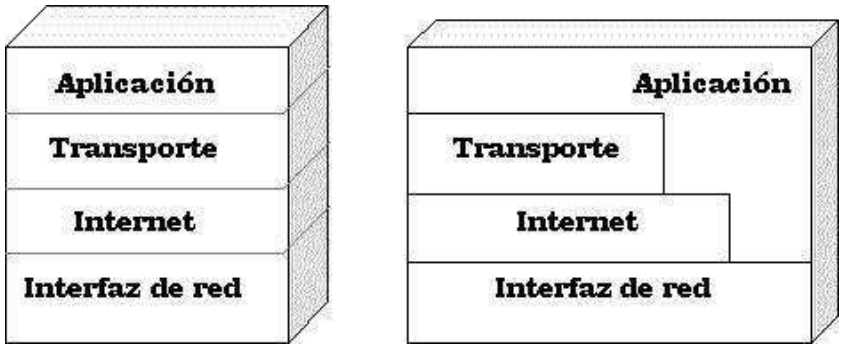


Figura 8. Las 4 capas de Modelo TCP/IP
Fuente: https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%Selector.pdf

1) **Capa de aplicación.** Esta capa proporciona servicios que pueden ser utilizados por otras aplicaciones utilizadas para acceso remoto, correo electrónico, transferencia de archivos y administración de la red. La capa de aplicación de TCP/IP utiliza servicios de las tres capas superiores del modelo OSI (aplicación, presentación y sesión). Como podemos apreciar en la figura 1.7, TCP/IP no utiliza una estructura de capas rígida, ya que la capa de aplicación puede operar directamente sobre las capas de transporte, Internet y red. Los protocolos de la capa de aplicación son los siguientes:
    - Protocolo de Transferencia de Hipertexto (HTTP, HyperText Transfer Protocol)
    - Protocolo Trivial de Transferencia de Archivos (TFTP, Trivial File Transfer Protocol)
    - Protocolo de Transferencia de Archivos (FTP, File Transfer Protocol)
    - Sistema de Archivos de Red (NFS, Network File System)
    - Protocolo Simple de Transferencia de Correo (SMTP, Simple Mail Transfer Protocol)
    - Emulación de Terminal (Telnet)

- Protocolo Simple de Administración de Redes (SNMP, Simple Network Management Protocol)
- Sistema de Nombres de Dominio (DNS, Domain Name System)

2) **Capa de transporte.** La capa de transporte se encarga de controlar las conexiones lógicas entre las computadoras o hosts. Los protocolos de esta capa segmentan y reensamblan los datos que las aplicaciones de la capa superior envían. Los protocolos de la capa de transporte son los siguientes:
   - Protocolo de Control de Transmisión (TCP, Transmission Control Protocol).
   - Protocolo de Datagrama de Usuario (UDP, User Datagram Protocol).
3) **Capa de Internet.** Gestiona la transferencia de información a lo largo de varias redes mediante el uso de routers. La capa de Internet de TCP/IP es equivalente a la capa de red del modelo OSI, ya que se encarga de la transferencia de paquetes entre computadoras conectadas a distintas redes. En esta capa se determina la mejor ruta a seguir y la conmutación de paquetes. Los protocolos de la capa de Internet son los siguientes:
   - Protocolo de Internet (IP, Internet Protocol)
   - Protocolo de Mensajes de Control en Internet (ICMP, Internet Control Message Protocol)
   - Protocolo de Resolución de Direcciones (ARP, Addres Resolution Protocol)
   - Protocolo de Resolución Inversa de Direcciones (RARP, Reverse Address Resolution Protocol)

IP es un protocolo que funciona en la capa de red del modelo OSI el cual define la forma en que se asignan las direcciones a los datos que van del origen hasta el destino y la secuencia en que los datos deben ser reensamblados en el otro extremo de la transmisión.

4) **Capa de interfaz de red.** Se encarga de todo lo relacionado con la

transferencia de paquetes dependientes de la red. Realiza funciones que pertenecen a parte de la capa de enlace de datos y la capa física del modelo OSI. Se ocupa de los métodos utilizados para que un paquete IP pueda obtener un enlace físico con el medio de red. Los protocolos de la capa de interfaz de red son:

- Tecnologías LAN (Ethernet, Fast Ethernet, FDDI)
- Tecnologías WAN (ATM, Frame Relay)
- Protocolo Punto a Punto (PPP, Point-to-Point Protocol)
- ARP y RARP.

2.2.7 Acceso Remoto y Conexiones WAN

Internet, intranets y extranets

Internet es una red de redes que ha proporcionado muchas ventajas a toda clase de organizaciones. A las empresas les aporta muchos beneficios económicos el hecho de conectarse a Internet y poder realizar ahí toda clase de negocios. Las corporaciones han descubierto también que llevar la tecnología sobre la cual se basa Internet a sus propias redes privadas les trae muchos beneficios a todos sus usuarios, de ahí el surgimiento de las intranets. Finalmente, las empresas requieren estar conectadas con sus socios y clientes, por lo que pronto surgen las extranets. Internet, intranet y extranet son conceptos muy importantes en el mundo de las VPN y no puede hablarse de una VPN sin antes conocer en qué consisten dichos conceptos.

2.2.7.1 Internet

Internet conecta decenas de millones de computadoras en todo el mundo, permitiéndoles comunicarse entre sí y compartir recursos. Internet es una colección de redes organizada en una estructura multinivel las cuales usan toda una variedad de tecnologías para interconectarse. En el nivel más bajo se encuentra algunas decenas o cientos de computadoras conectadas a un router, formando una LAN. Otras computadoras se conectarán a un router a través de la red telefónica usando un módem. Una empresa o universidad podrá tener varios routers enlazados a un router principal. Estos routers se encuentran conectados mediante líneas alquiladas a un

router de un Proveedor de Servicios de Internet (ISP, Internet Service Provider). A su vez, el proveedor conecta sus routers a una WAN de alta velocidad llamada backbone. Un país puede tener varios backbones que conectan a todos los ISP. Finalmente, los backbones de todos los países se interconectan en una malla usando líneas internacionales. Todo esto es lo que finalmente forma Internet.

La base de Internet es TCP/IP. El éxito de las redes basadas en IP se debe precisamente a Internet. Dos conceptos definen la tecnología de Internet: los paquetes y la forma de direccionamiento.

- **Paquetes.** Internet transporta toda la información en unidades llamadas paquetes. Un paquete consta de dos partes: la información que contiene, la cual se llama carga útil y la información acerca de la información, llamada cabecera. La cabecera contiene información acerca de las direcciones origen y destino, longitud de los datos y tipo de éstos.
- **Direccionamiento.** Las direcciones de la cabecera permiten el envío de la información a través de Internet. Los routers se encargan de realizar esto. Los paquetes recorren diferentes caminos para llegar a su destino y eventualmente pueden ser almacenados dentro del router.

2.2.7.2 Intranet

Una intranet es una Internet orientada a una organización en particular. Los servidores web intranet difieren de los servidores web públicos en que estos últimos no tienen acceso a la intranet de la empresa sin los permisos y las contraseñas adecuadas. Una intranet está diseñada para que accedan a ellas sólo los usuarios con los debidos permisos de acceso a una red interna de una empresa. Una intranet reside dentro de un firewall y éste impide el acceso a los usuarios no autorizados.

2.2.7.3 Extranet

Una extranet es una intranet orientada a las personas u organizaciones que son externas a su empresa, pero necesitan acceder a alguna información, así se les permite el acceso a este contenido adicional, siempre bajo un sistema de

autenticación y control de acceso.

La diferencia entre una intranet y una extranet es el método de acceso, siendo similares en cuanto a las facilidades y funciones, el tipo de recurso que utiliza y su filosofía general, de proporcionar acceso fácil, rápido y seguro a la información requerida.

El concepto extranet nace cuando una empresa quiere dar acceso a unas determinadas personas o grupos de personas a una determinada información de su intranet. Sin hacerla pública, la hace accesible a otras personas que puedan necesitarla o con quien mantienen relaciones comerciales. El ejemplo más claro es la accesibilidad que una empresa da a una parte de sus clientes o proveedores.

2.2.7.5 Acceso Remoto

Conectarse a una red desde una ubicación distante es lo que se denomina acceso remoto. El acceso remoto a una red ha sido algo de gran importancia en el mundo de las redes, ya que muchas compañías que promueven viajes de trabajo de sus empleados o el trabajo desde el hogar o desde una pequeña oficina remota. Y estos empleados necesitan conectarse a la red privada de la compañía para consultar ciertos archivos o correo electrónico. La necesidad del acceso remoto ha sido la causa principal del auge de las redes privadas virtuales, por lo que es preciso analizarlo un poco antes de verlo desde el punto de vista de las VPN.

2.2.8 Windows Server 2012

Es un sistema operativo destinado a servidores lanzado por Microsoft. Es la versión para servidores de Windows 8 y es el sucesor de Windows Server 2008 R2. El software está disponible para los consumidores desde el 4 de septiembre de 2012.
Función de servidor de acceso remoto en Windows Server 2012.

El acceso remoto es una función del servidor en Microsoft Windows Server 2012 y Windows Server 2012 R2 que proporciona a los administradores un panel para administrar, configurar y monitorear el acceso a la red.

El acceso remoto se puede instalar utilizando el Asistente para agregar roles y características. El rol del servidor agrupa tres tecnologías involucradas en el acceso a

la red: el Servicio de enrutamiento y acceso remoto, DirectAccess y el Proxy de aplicación web.

- Servicio de enrutamiento y acceso remoto: utiliza una red privada virtual (VPN) para admitir la conectividad.
- DirectAccess: permite a los usuarios finales remotos dentro de una organización un acceso seguro a archivos, documentos y otros recursos sin la necesidad de una VPN.
- Proxy de aplicación web: admite el acceso de los usuarios finales a aplicaciones desde fuera de una red corporativa mediante el uso de autenticación de proxy inverso.

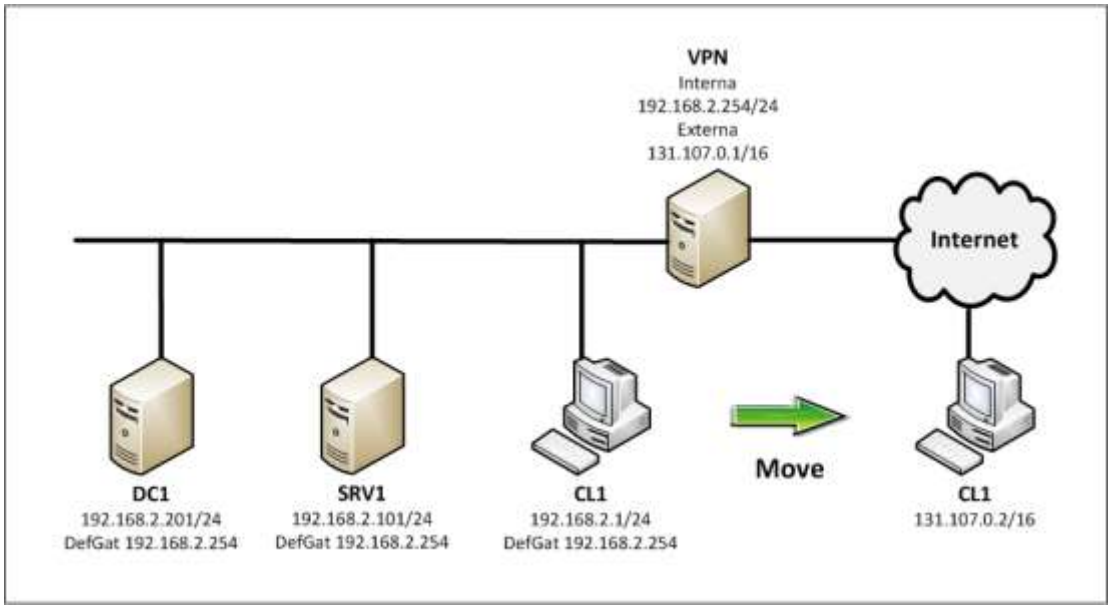


Figura 9. Modelo para Windows Server 2012
Fuente: https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%Selector.pdf

2.3 Definición de términos básicos

Banda ancha: Capacidad para transmitir datos un canal compartido.

Estándar: Es un proceso, protocolo o técnica utilizada para hacer algo concreto.

Firewall: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones

autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Gateway: Es una "puerta de enlace" (equipo para interconectar redes).

Interfaz: Es el mecanismo o herramienta que posibilita esta comunicación mediante la representación de un conjunto de objetos, iconos y elementos gráficos que vienen a funcionar como metáforas o símbolos de las acciones o tareas que el usuario puede realizar en la computadora.

LAN (Local Area Network): Red de área local, es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios)

Protocolo TCP/IP: TCP/IP es un conjunto de protocolos. La sigla TCP/IP significa "Protocolo de control de transmisión/Protocolo de Internet.

Red de acceso: Hace mención a aquella parte de la red de comunicaciones que conecta a los usuarios finales con algún proveedor de servicios y es complementaria al núcleo de red.

Secure Sockets Layer: Es un protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet. SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.

Software: está compuesto por un conjunto de programas que son diseñados para cumplir una determinada función dentro de un sistema, ya sean estos realizados por parte de los usuarios o por las mismas corporaciones dedicadas a la informática.

Telecomunicaciones: sistema de comunicación a distancia que se realiza por medios eléctricos o electromagnéticos.

UDP: Es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el

propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

VPN: Permite crear una conexión segura a una red remota a través del Internet. Cuando se conecta cualquier dispositivo a un concentrador VPN, esta conexión actúa como una extensión de la LAN y todo el tráfico de datos se envía de forma segura a través del túnel VPN.

CAPÍTULO III
MARCO METODOLÓGICO

El marco metodológico de la investigación se puede definir como la explicación de los mecanismos que se utilizan para analizar la problemática que se presente en una investigación. Arias, F. (2012), según el marco metodológico expresa que: "La metodología del proyecto incluye el tipo o tipos de investigación, las técnicas y los instrumentos que serán utilizados para llevar a cabo la indagación. Es el "cómo" se realizará el estudio para responder al problema planteado." (pág. 110).

3.1 Tipo de investigación

Con lo que respecta al tipo de investigación, Tamayo, M (2003) expresa que una investigación descriptiva "Comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o procesos de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre cómo una persona, grupo o cosa se conduce o funciona en el presente. La investigación descriptiva trabaja sobre realidades de hecho, y su característica fundamental es la de presentarnos una interpretación correcta."

El autor Arias, F. (2012) afirma que: "La investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere". (pag.24).

En relación con lo expresado anteriormente, se dice que la presente investigación se puede calificar como documental – descriptiva, ya que la misma, constituye un estudio sistemático de investigaciones previas ya comprobadas, y a su vez, se realiza bajo el esquema de un proyecto factible, cuyo enfoque se centra en la posibilidad de llevar teorías generales al ámbito práctico, y cuyo esfuerzo se destina a

la implantación de propuestas, que pueden materializarse y brindar soluciones a problemas que se plantean en la sociedad, lo cual en este caso es respaldo de energía eléctrica.

3.2. Nivel de la Investigación

Según Arias, F. (2012, pág. 23), el nivel de investigación puede definirse como "el grado de profundidad con que se aborda un fenómenos u objeto de estudio". "El tipo de investigación según el nivel o grado de profundidad con el que se realizará el estudio" (pág. 110).

Este trabajo se ha considerado de tipo descriptivo el cual es definido por Sabino, C. (1996, pág. 54) como "Las investigaciones descriptivas utilizan criterios sistemáticos que permiten poner de manifiesto la estructura o el comportamiento de los fenómenos en estudio, proporcionando de ese modo información sistemática y comparable con la de otras fuentes". "También deben clasificarse como investigaciones descriptivas los diagnósticos que realizan consultores y planificadores: ellos parten de una descripción organizada y lo más completa posible de una cierta situación, lo que luego les permite en otra fase distinta del trabajo trazar proyecciones u ofrecer recomendaciones específicas.". Este nivel de investigación consiste, fundamentalmente, en caracterizar un fenómeno o situación concreta indicando sus aspectos más importantes, es decir, en si el objetivo de este nivel de investigación es el de conocer las situaciones frente a un tema en particular, no quedándose solo en la recolección de datos sino también en ayudar a predecir e identificar la relación que existe entre dos o más variables.

3.3. Diseño de la Investigación

El diseño de la investigación es el conjunto de directrices que toma el investigador con el fin de observar, analizar y plantear una solución de ser posible a la problemática objeto de la investigación. Según el autor Palella y Martins (2010), define:

> "El diseño experimental es aquel según el cual el investigador manipula una variable experimental no comprobada, bajo condiciones

> estrictamente controladas. Su objetivo es describir de qué modo y porque causa se produce o puede producirse un fenómeno. Busca predecir el futuro, elaborar pronósticos que una vez confirmados, se convierten en leyes y generalizaciones tendentes a incrementar el cúmulo de conocimientos pedagógicos y el mejoramiento de la acción educativa". (pag.86).

Según el autor Palella y Martins (2010), define: La Investigación de campo consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar las variables. Estudia los fenómenos sociales en su ambiente natural. El investigador no manipula variables debido a que esto hace perder el ambiente de naturalidad en el cual se manifiesta. (pag.88)

3.4 Población y Muestra

3.4.1. Población

La población es todo individuo de características considerables en las estadísticas de una investigación. Arias, F. (2012), realiza la siguiente definición:

> "La población, o en términos más precisos población objetivo, es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Ésta queda delimitada por el problema y por los objetivos del estudio." (pág. 81).

En la población del siguiente trabajo de grado se tomara de los usuarios involucrados directamente en la interconexión de redes VPN y acceso remoto.

3.4.2. Muestra

La muestra es todo aquel subconjunto considerado en una determinada población, a la cual se aplicará la posterior técnica de recolección de datos. Según Arias, F. (2012), expresa que: "La muestra es un subconjunto representativo y finito que se extrae de la población accesible". (pág. 83).

3.5 Técnicas e Instrumentos de recolección de datos

3.5.1. Técnicas de recolección de datos

Es el medio por el cual el investigador facilita la recolección de datos, valiéndose del mismo para obtener la información necesaria. Hurtado, J. (2010), concluye que:

> "Los aspectos metodológicos se desarrollan a lo largo del marco metodológico y se evidencian en las técnicas utilizadas para la recolección de datos y para el análisis de resultados... Las técnicas son modos específicos de hacer algo. Por ejemplo, algunas técnicas de recolección de datos son la entrevista y la observación". (pág. 105 y 110).

La presente investigación, tiene como técnica la entrevista estructurada, la cual, según Arias, F. (2012) define que:

> "Es la que se realiza a partir de una guía prediseñada que contiene las preguntas que serán formuladas al entrevistado. En este caso, la misma guía de entrevista puede servir como instrumento para registrar las respuestas, aunque también puede emplearse el grabador o la cámara de video". (pág. 73).

Por ello, es importante destacar que los investigadores utilizarán la entrevista estructurada como técnica de recolección de datos, seleccionando la muestra finita antes planteada, para así aplicar la misma, obteniendo entonces los resultados que se desean lograr.

De igual forma, la observación directa es un método por el cual el investigador se vale para obtener, tal y como lo dice su nombre, la información directa del análisis que se desea desarrollar. Hurtado, J. (2010) cita: "La observación directa y natural de los hechos es el punto de partida del método del empirismo. Según Bacon esta observación debe hacerse dejando de lado los prejuicios, a los que este autor llamó ídolo". (pág. 112).

3.5.2. Instrumentos de recolección de datos

Un instrumento sirve como recurso material que se relaciona con el individuo al cual se le hace el análisis. Para Arias, F. (2012), los instrumentos: "Son los medios

materiales que se emplean para recoger y almacenar la información. Ejemplo: fichas, formatos de cuestionario, guía de entrevista, lista de cotejo, escalas de actitudes u opinión, grabador, cámara fotográfica o de video, etc.". (pág. 111)

En la presente investigación, tiene como instrumento de recolección de datos la ficha de registro de información que será diseñada por los autores. Esta ficha será diseñada tomando en consideración los objetivos de la investigación, a su vez estará constituida por preguntas cerradas, dicotómicas. Cabe destacar que dicho instrumento será empleado a la muestra determinada.

3.6 Fases de la Investigación

Fase I: "Diagnosticar la situación actual de la red corporativa de la empresa Teleinter 2009 C.A"

Actividades:

- Se realizo el diagnóstico de la situación actual de la empresa, el cual llevo a una observación directa para ver con cuantos departamentos trabaja la empresa. Por otro lado se revisaron las estructuras de redes y date center.

Fase II: "Identificar los parámetros, dispositivos y entornos para el diseño de la red virtual privada (VPN)"

Actividades:

- Se procederá a identificar los parámetros que conformar el diseño de la red virtual privada (VPN).

Fase III: "Diseñar el sistema de la red privada virtual (VPN) para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo"

Actividades:

- Siguiendo el estudio anteriormente se procederá a realizar el diseño de la red privada virtual VPN para la empresa Teleinter 2009 C.A.

Fase IV: "Realizar un estudio de factibilidad, económico, técnico y ambiental para la red privada virtual (VPN) para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo"

Actividades:

- Se evaluará la factibilidad económica, social y ambiental sobre el diseño de la red privada virtual (VPN) para la empresa Teleinter 2009 C.A a utilizar para que sea posible su futuro desarrollo.

CAPÍTULO IV
RESULTADOS

Basado en esto se presentan a continuación el desarrollo de las fases establecidas en el actual trabajo de investigación, con el fin de dar cumplimiento a los objetivos específicos presentados inicialmente, y así suministrar una solución al problema que acontece dentro de la empresa Teleinter 2009 C.A.

4.1 Fase I: Diagnosticar de la situación actual la red corporativa de la empresa Teleinter 2009 C.A.

4.1.1 Observación directa

La empresa Teleinter 2009 C.A. es una empresa venezolana, proveedora de servicio de Internet inalámbrico, dedicado, simétrico y asimétrico, brindando estabilidad y un alto nivel de conexión y de comunicaciones. El cual esta tiene una visón de expandir la cobertura a nivel nacional, y su misión es brindar conexión segura y confiable del Internet. La cual su sede se ubica la en Naguanagua, las Trincheras, Edif. Cumaná, piso 2, apartamento. 2-2D en Valencia. En esta sede es donde se realizan todas las funciones de gerencia, administrativas, centro de control, operaciones, almacén entre otras, las cuales se estarán especificando con más detalle.

- **Gerencia:** es el área considerada la cabeza de la empresa. Establece los objetivos y la dirige hacia ellos. Está relacionada con el resto de áreas funcionales, ya que es quien las controla.
- **Área de Finanzas:** es el área que se encarga del óptimo control, manejo de recursos económicos y financieros de la empresa, esto incluye la obtención de recursos financieros tanto internos como externos, necesarios para alcanzar los objetivos y metas empresariales.
- **Recursos Humanos:** es el área encargada de la dirección eficiente y efectiva del recurso humano de la empresa. Dentro de las principales funciones de esta

área, se pueden mencionar: Reclutamiento y selección de personal capaz, responsable y adecuado a los puestos de la empresa, la motivación, capacitación y evaluación del personal; el establecimiento de un medio ambiente agradable para el desarrollo de las actividades.

- **Centro de control:** es el área encargada del monitoreo de la flota mediante GPS; los encargados de esta área trabajan 24/7 pues es indispensable saber la ubicación de las unidades que se encuentran en ruta para poder dar un mejor servicio a los clientes.
- **Logística:** es el área encargada de obtener y buscar los recursos, económicos y materiales (herramientas y maquinaria) necesarios para el funcionamiento de la empresa. Entre las principales funciones del área de operaciones y centro de control, el mantenimiento y reparación de maquinaria o equipo, el almacenamiento de equipos necesarios para darle un buen servicio al cliente.
- **Contabilidad:** registra y clasifica las operaciones de la empresa en términos monetarios utilizando diferentes herramientas de registro como la Balanza General, Estado de Resultados y Balances de Comprobación.
- **Almacén:** el área de almacén tiene la función de proveer de equipos a todos los técnicos que se encargan de la instalación sobre las antenas para darle un buen servicio al cliente, en este departamento se encuentran las antenas, routers, fuentes como otros equipos necesarios.
- **Sistemas:** se encarga de mantener siempre en buen estado el funcionamiento técnico y tecnológico de la empresa para evitar que aquellas tareas que se realizan por medio de los servidores y dispositivos de la red estén en mal estado y no se lleven a cabo los objetivos de la empresa.

Siguiendo con nuestro diagnóstico se hizo conteo por todas las áreas que pertenecen a la empresa de manera que en la siguiente tabla se especifica cuantas computadoras se encuentran por cada departamento y qué tipo de software trabaja cada máquina sacando así las siguientes conclusiones:

- La Empresa está conformada por nueve (9) oficinas, las cuales fueron especificadas anteriormente.
- Se hizo un conteo total de treinta (30) computadoras operativas.
- Entre las treinta (30) computadoras, diez (10) de ellas cuentan con Core I5 y veinte (20) de ellas cuenta con Core I7.
- Todas las treinta (30) computadoras cuentan con Windows 7.

Tabla 1. Diagnostico de Hardware y Software de las computadoras de los departamentos.

OFICINAS	Nº PC	Hardware			Software		
		CORE 2 DUO	CORE I5	CORE I7	WINDOWS 7	WINDOWS 8	WINDOWS 10
FINANZAS	2	-	-	2	2	-	-
CENTRO DE CONTROL	10	-	5	5	10	-	-
GERENCIA	2	-	-	2	2	-	-
RR. HH	1	-	-	1	1	-	-
LOGISTICA	5	-	3	2	5	-	-
ALMACEN	4	-	2	2	4	-	-
SISTEMAS	4	-	-	4	4	-	-
ADMINISTRACIÒN	2	-	-	2	2	-	-
TOTAL DE PC	30						

Autor: Flores, Reyes (2021)

4.1.1.1 1nfraestructura del data center

Un datacenter convencional es un centro de procesamiento de datos, una instalación empleada para albergar un sistema de información de componentes asociados de telecomunicaciones y equipos de almacenamientos donde generalmente incluyen fuentes de alimentación redundante en un ambiente controlado, como por ejemplo acondicionando el espacio con aire acondicionado, sistema de extinción de

incendios UPS y diferentes dispositivos de seguridad para permitir que los equipos tengan la posibilidad de almacenar y gestionar toda la información de sus clientes, sus empleados, y sus proveedores y la comunicación por internet sea de manera optima. En la figura 10 se puede observar algunos componentes que se encuentran en el data center de la empresa.

Figura 10. Infraestructura básica del data center.
Autor: Flores, Reyes (2021)

La empresa cuenta con un Data Center ubicada en un segundo piso de la casa. Este ambiente cuenta con los requisitos mínimos de seguridad que debe tener un Data Center. El área de este ambiente es muy pequeña, lo que ocasiona que el diseño de red no sea escalable. En la tabla dos (2) se puede observar una lista de cotejo del data

center el cual se realizo para ver que componentes existían físicamente y se realizaron algunas observaciones de mejora.

Tabla 2. Lista de cotejo para la infraestructura del Data Center

Punto a Observar	Si	No	Observaciones
Espacio Físico de 4X4 m	x		Posiblemente se va aumentar el espacio físico
Conexión de red	x		
Acceso controlado	x		
Rack Bastidor	x		
Recubrimiento de paredes anti polvo		x	
Aire acondicionado de 24000 BTU	x		Necesita mantenimiento
Sensores de temperatura y humedad	x		
Existe buena iluminación	x		Necesita algunos cambio de focos
Deshumidificador	x		
UPS	x		
Planta eléctrica	x		
Extintor	x		
PDU	x		
Bloqueo anti-vibraciones		x	

Autor: Flores, Reyes (2021)

La empresa cuenta con un rack bastidor el cual en la siguiente tabla se especifican los componentes que están conformados el rack, el cual ese se especifica como el cuarto de telecomunicaciones.

Tabla 3. Lista de equipos en el cuarto de Telecomunicaciones

Equipos		
Cantidad	**Modelo**	**Marca**
2	Switch (core)	Catalyst 4506
2	Monitor	LG
2	Teclado y mouse	LG
4	UPS	Elise

4	Router serie	Cisco
4	Modem óptico	Cisco
4	Modem ADSL	Tp-link
2	Servidores System	IBM

Autor: Flores, Reyes (2021)

4.1.1.2 Cable Estructurado

Actualmente la Empresa cuenta con un cableado horizontal lo cual interconecta todas las oficinas de la empresa. Se tiene instaladas 02 Access-Point distribuidos en el área de esparcimiento, en la oficina de finanzas.

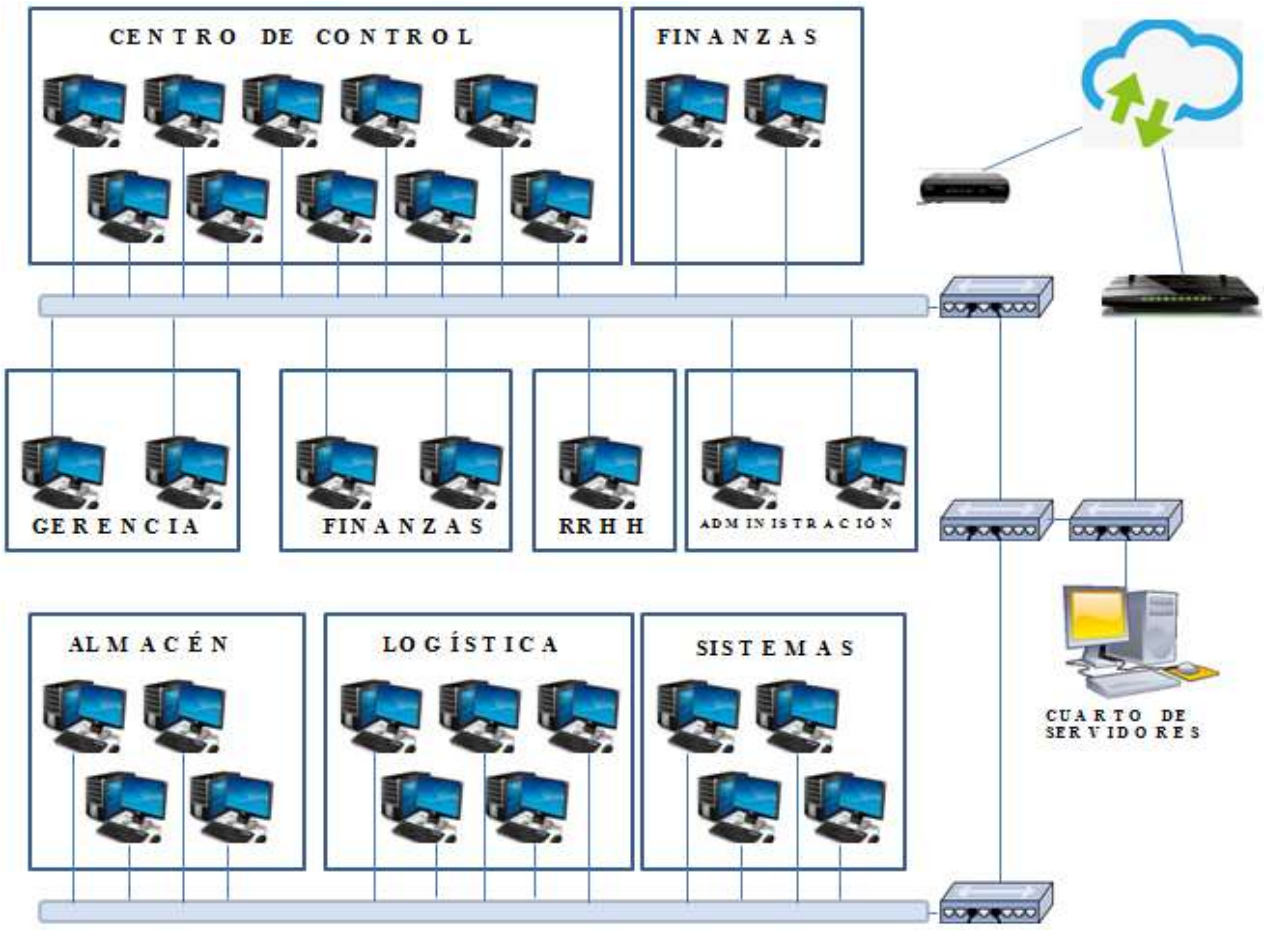


Figura 11. Estructura de las Redes LAN de la empresa Teleinter
Autor: Flores, Reyes (2021)

Para el diseño de la Red Privada Virtual (VPN) tendremos en cuenta la estructura de la red LAN en cada una de las áreas de la empresa, es decir, cuantos equipos estarán conectados, que protocolos se implementaran para la comunicación y seguridad de la información, dispositivos empleados, direccionamiento y cableado como fue explicado anteriormente.

Para los servicios de internet la empresa cuenta con lo siguiente:

Tabla 4. Servicio de Internet

Sucursal	Servicio	Velocidad Mb/s
Teleinter	Internet Fibra óptica Línea dedicada	20
Teleinter	Internet Fibra óptica Línea dedicada	40
Teleinter	Internet ADSL Línea Comercial	20

Autor: Flores, Reyes (2021)

Por último para terminar con nuestro diagnóstico en la empresa Teleinter se propone algunos requisitos de mejora para el diseño de la Red VPN.

- Hardware y software apropiados para el diseño.
- Hardware y software para brindar la seguridad de la información
- Servicio de internet, con velocidad adecuada para un funcionamiento rápido.
- Equipos de respaldo para evitar caídas en el servidor VPN y brindar la confiabilidad necesaria en la operación.

Sin embargo para concluir con esta primera fase es bueno tener en cuenta algunos riesgos que se puedan presentar al diseñar la Red Privada Virtual (VPN), se deben detectar las vulnerabilidades que se pueden presentar a nivel de seguridad, la cual debe proporcionar como mínimo la autenticación del usuario y restringir el acceso a los usuarios no autorizados. Si no se contara con ese requerimiento,

cualquier persona malintencionada podría conectarse a los recursos e información de la red local.

- Un factor importante a tener en cuenta es la red local (LAN), ya que a partir del buen funcionamiento y adecuada distribución de esta, se puede lograr un balance de cargas entre los usuarios internos como externos, de lo contrario podrían generarse colisiones de paquetes y por ende perdida de la información, generando problemas de interconectividad tanto en la red LAN como WAN.
- Al momento de conectar las redes LAN de las sucursales y los usuarios remotos, se debe implementar el mismo protocolo para evitar incompatibilidad en la conexión o comunicación en el envió y recepción de los mensajes; otros factores que se tendrán en cuenta y que generarían fallos a la red son la configuración inadecuada de los servidores o la mala elección del cableado estructurado generando demoras e interferencias en la transmisión de los datos.
- Una vez identificados los puntos vulnerables para el diseño de la Red Privada Virtual en Teleinter 2009 C.A., se tendrán en cuenta y se trabajara principalmente en ellos para evitar inconsistencias en la red. Como la VPN emplea una infraestructura pública, se emplearan un sistema de encriptación y autenticación mediante túneles virtuales entre las sedes, asegurando la confidencialidad e integridad de los datos transmitidos a través de internet, también se tendrá el protocolo de túnel de VPN a implementar en la red, el cual debe ser compatible con la configuración WAN y LAN.

4.2 Fase II: Identificar los parámetros, dispositivos y entornos para el diseño de la red virtual privada (VPN).

4.2.1. Análisis de Requerimientos

Los requerimientos que se tendrán en cuenta para la especificación del sistema y el modelo de análisis son los siguientes:

1 **Identificar los Skateholders**: las personas involucradas en el desarrollo del sistema son:

- Usuarios Internos.
- Usuarios Externos.
- Red LAN.
- Red VPN.

2 **Identificar los requerimientos**:

✓ **Requerimientos Funcionales**

Red LAN

- Determinar cuántos equipos estarán conectados en cada sucursal mediante la recopilación de información, con el fin de realizar el direccionamiento IP a cada subred de Teleinter 2009 C.A., permitiendo que cada equipo sea identificado dentro de la red. o Establecer los dispositivos (switch, router, tarjetas Ethernet), cableado (conector RJ45, Cable par trenzado) a utilizar en la red.
- Configurar las tarjetas de red de cada uno de los equipos de las sucursales, teniendo en cuenta el direccionamiento IP de cada subred.

Red VPN

- Identificación de usuarios, es decir, que la VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a los no autorizados mediante el servidor VPN que real iza la autenticación de acceso.
- Establecer una dirección del cliente en la red Privada y que esta se conserve.
- Encriptar los datos a través de túneles VPN para que no puedan ser leídos.
- Generar y renovar claves para el cliente y el Servidor.
- Conexión de las sedes y los usuarios Remotos, mediante una conexión permanente a internet y una dirección IP fija, la cual usaran los usuarios remotos para conectarse a la VPN.

- Intercambio de información en tiempo real y disponibilidad de esta sin importar la ubicación del usuario.
- Conexión del servidor a través del router que estará conectado al ISP continuamente y la configuración del protocolo VPN que se utilizara para la conexión.
- Interconexión total a la red de todos los usuarios tanto internos como externos de forma segura a través de una infraestructura pública.
- Flexibilidad y facilidad de uso en el ingreso remoto a los aplicativos de la empresa.

✓ **Requerimientos Funcionales**

- La Red LAN y VPN deben funcionar en los Sistemas Operativos XP y Vista, ya que los equipos de la empresa cuenta con Windows.
- Los usuarios deben ser capaces de utilizar todas las funciones de la red VPN, tras un entrenamiento que se le dará los empleados.
- El sistema controlara la validez y coherencia de los datos ingresados en la conexión VPN.

4.2.2 Resultados de los Análisis

Actualmente la empresa se está comunicando mediante correo electrónico y llamadas telefónicas para mantenerse informada una sede de la otra sobre las ventas, actualización de mercancía, entre otras tareas, lo cual hace que los datos no se efectúen en tiempo real, generando retrasos en las respuestas a los clientes y procesos internos de la empresa. Con el fin de evitar estos medios de comunicación, se pensó en una reestructuración total en el modo de acceder a los datos, mediante la creación de una red que interconecta tanto la red LAN como la WAN con la posibilidad de tener un acceso total a los equipos y aplicativos independientemente del lugar donde se encuentre.

Teleinter 2009 C.A. cuenta con 40 empleados, ubicados en los distintos departamentos que conforman la empresa, a cada uno de ellos se le asigno un computador con las siguientes características:

- Sistema Operativo Windows Server 2012.
- Paquete Office.
- Cuentas en Outlook para los empleados.
- Aplicativos Internos de la empresa (Software para el manejo de inventarios, Contabilidad, Ventas). Instalados exclusivamente en los equipos que lo requieran.
- Otros Software (Navegador, Java, Fhash Player, Acrobet, Real Player, etc).

Por petición del Gerente, los computadores de los empleados tendrán acceso limitado a internet, es decir, no podrán ingresar a Redes Sociales (Facebook, Twitter, Instagram, etc), paginas de ocio, entretenimiento entre otras. El servicio de internet se empleara principalmente para revisar correos y la intranet.

4.2.3 Alternativas de Soluciones

Las formas en que pueden implementar las VPN pueden ser basadas en hardware o a través de Software, pero lo más importante es el protocolo que se utilice para el diseño, por eso es que es importante identificar algunas alternativas de soluciones para un posible diseño optimo.

4.2.3.1 Alternativas de Soluciones a nivel de Hardware

Son equipos de red dedicada exclusivamente a la finalidad de VPN. Aunque por lo general más caros que el software VPN, hardware VPN puede ofrecer el mejor rendimiento para las organizaciones y empresas que dependen en gran medida de VPN. Hay consideraciones sobre topología de la red a pesar, como un hardware VPN es un aparato adicional y pueden requerir una amplia formación de un departamento de TI.

Hardware VPN Beneficios: Hardware dispositivos VPN se construyen específicamente para el propósito de VPN y pueden proporcionar la capacidad de

VPN más eficiente para una organización o empresa. El uso de hardware de VPN se asegura de que otros equipos de la red puede centrarse en sus tareas previstas en lugar de proporcionar recursos para fines VPN. Un ejemplo es un router que se espera para reenviar el tráfico de la red a una velocidad determinada, y si sus recursos se destinan en parte a VPN, puede enviar los datos de red más lenta.

- **VPN Cisco**

Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad IP (IPsec) cifrada o túneles VPN de Secure Sockets Layer (SSL) y tecnologías de autenticación. Estas tecnologías protegen los datos que pasan por la red privada virtual contra accesos no autorizados. Las empresas pueden aprovechar la infraestructura estilo Internet de la red privada virtual, cuya sencillez de abastecimiento permite agregar rápidamente nuevos sitios o usuarios. También pueden aumentar drásticamente el alcance de la red privada virtual sin expandir significativamente la infraestructura.

- **VPN O-LINK**

Los routers de servicios unificados O-Link ofrecen soluciones en red seguras y de alto rendimiento para satisfacer las necesidades crecientes de las empresas. Estos routers están repletos de funciones avanzadas de seguridad y administración, como lEE 802.11 n, acceso inalámbrico seguro, redundancia WAN 3G, 1Pv6 y completas funciones VPN que también pueden integrarse con facilidad en su infraestructura actual. Estos routers proporcionan a los trabajadores que tienen que desplazarse un acceso remoto en cualquier momento y lugar usando el potente motor VPN que permite establecer conexiones seguras con los recursos de la empresa. O-link ofrece un rendimiento comparable a las redes tradicionales de cable pero con menos limitaciones. La optima seguridad de red se obtiene por medio de características como túneles de red privada virtual (VPN), IPSec (IP Security), PPT (Point-to- Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), y SSL Secure Sockets

Layer, que lo convierten en ideal para Pymes y delegaciones que necesitan una conexión segura y fiable a recursos remotos.

- VPN MICROTIK

Mikrotik proporciona VPN para unir redes distantes, haciendo un túnel de conexiones seguras a través de redes abiertas o internet, o conectar lugares remotos con conexiones cifradas; router OS soporta varios métodos y protocolos de túnel VPN.

- ✓ IPSec: El modo de túnel y de transporte, certificado o PSK, protocolos de seguridad AH y ESP.
- ✓ Túneles punto a punto (OpenVPN, PPTP, PPPoE, L2TP).
- ✓ Características avanzadas de PPP (MLPPP, BCP).
- ✓ Túneles básicos (IPIP, EoiP).
- ✓ Soporte de túneles 6 a 4 (1Pv6 sobre 1Pv4 red).
- ✓ Soporte VLAN -IEEE802.1q Virtual LAN, Q-in-Q.
- ✓ MPLS basado en VPN

Esto significa que se puede interconectar de forma segura las redes de banca, utilizar sus recursos de trabajo durante el viaje, conectarse a su red doméstica local, o aumentar la seguridad de su enlace de backbone inalámbrico. Incluso puede interconectar dos redes de sucursales de oficinas y que serían capaces de utilizar los recursos del otro, como si las computadoras estarían en el mismo lugar, todo seguro y encriptado

4.2.3.2 Alternativas de Soluciones a nivel de Software

Software tecnología VPN está disponible en varias formas. Una forma es una aplicación añadido a un servidor existente en una red. Otra es una actualización de software para una pieza existente de equipos de red. Un proveedor de hardware puede ofrecer mayor funcionalidad de un dispositivo de red, como un router, como una actualización de software. Software VPN.

Beneficios: Software VPN tiene una ventaja de ser de bajo costo en relación con los dispositivos de hardware VPN. Dado que el software puede ser instalado en el equipo existente, puede haber también menos formación necesaria para el personal de TI de una organización porque el mismo proveedor puede mantener una interfaz de aplicación similar. Software VPN es también una manera de mantener una topología de hardware más simple para una red.

- **OPEN VPN (LINUX)**

OpenVPN es una solución de conectividad basada en software libre: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas IEEE 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo la licencia GPL, de software libre. OpenVPN, es un producto de software creado por James Yonan en el año 2001 y que ha estado mejorando desde entonces. Ofrece una combinación de seguridad a nivel empresarial, seguridad, facilidad de uso y riqueza de características. Es una solución multiplataforma que ha simplificado la configuración de VPN's frente a otras soluciones más antiguas y difíciles de configurar como IPsec y haciéndola más accesible para gente inexperta en este tipo de tecnología.

- **MICROSOFT FOREFRONT TMG VPN SERVER**

Con una red privada virtual puede conectar componentes de red a través de otra red, por ejemplo Internet. Puede convertir un equipo basado en Windows Server 2012 en un servidor de acceso remoto de forma que otros usuarios puedan conectarse a él mediante VPN y, a continuación, puedan iniciar sesión en la red y tener acceso a los recursos compartidos. Las VPN implementan "túneles" a través de Internet o de otra red pública de manera que proporcionan la misma seguridad y funcionalidad que una red privada. Los datos se envían a través de la red pública utilizando su infraestructura de enrutamiento, pero para el usuario parece como si los datos se

enviaran a través de un vínculo privado dedicado. Una VPN en servidores que ejecutan Windows Server 2012 consiste en un servidor VPN, un cliente VPN, una conexión VPN (la parte de la conexión en la que los datos están cifrados) y el túnel (la parte de la conexión en la que los datos están encapsulados). Los túneles se realizan a través de uno de los protocolos de túnel que se incluyen con los servidores que ejecutan Windows Server 2012, los cuales se instalan con el servicio Enrutamiento y acceso remoto. El servicio Enrutamiento y acceso remoto se instala automáticamente durante la instalación de Windows Server 2012. Sin embargo, de forma predeterminada, el servicio Enrutamiento y acceso remoto está desactivado.

Los dos protocolos de túnel que se incluyen con Windows son:

a) **Protocolo de túnel punto a punto (PPTP):** Proporciona cifrado de datos mediante el cifrado punto a punto de Microsoft.
b) **Protocolo de túnel de capa 2 (l2TP):** Proporciona cifrado de datos, autenticación e integridad mediante IPSec.

La conexión a internet debe utilizar una línea dedicada como T1, T1 fracciona! o Frame Relay, El adaptador WAN debe ser configurado con la dirección IP y la máscara de subred asignadas al dominio o proporcionadas por un proveedor de servicios de internet (ISP). El adaptador WAN también debe estar configurado como puerta de enlace predeterminada del enrutador de ISP.

Para terminar en base a las alternativas se determinaron los parámetros para el diseño de la Red VPN.

- La homogeneidad del sistema, dado que el servidor y equipos actualmente en funcionamiento usan Microsoft Windows.
- La empresa cuenta con licencias para Windows server 2012 R2 Microsoft, esto genera un ahorro significativo para la misma.
- La interfaz de Windows es amigable y sencilla de configurar a diferencia de las otras alternativas, nos permite una administración sencilla en la red de la empresa.

- Dada las necesidades de la empresa, Windows Server es una alternativa de solución VPN adecuada para los requerimientos técnicos.

4.2.4 Determinar los equipos para el diseño de la Red VPN

4.2.4.1 Servidores

Los servidores operan a través de una arquitectura cliente-servidor. Los servidores son programas de computadora en ejecución que atienden las peticiones de otros programas, los clientes. Por tanto, el servidor realiza otras tareas para beneficio de los clientes.

- **Servidor Intel Xeon(R) CPU E3-1240 v3.**

Características:

Procesador: lntel Xeon 3.40 GHz.

Memoria Ram: 8GB

Disco Duro: 2TB

- **Servidor System x 3 500 E5506**

Procesador: lntel Xeon 2.13 GHz.

Memoria Ram: 28GB

Disco Duro: 500GB

- **Servidor Core I5 2 400**

Procesador: lntel Core i5 3.1 O GHz.

Memoria Ram: 04GB

Disco Duro: 500GB

4.2.4.2 Switch.

Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red.

Switch 3com: Baseline 2928 Pwr

Modelo: 24

Número de puertos: 01

Puerto Giga Ethernet: 01

Cantidad: 1

Switch 3com: Baseline 2928 Pwr

Modelo: 4226T

Número de puertos: 24

Puerto Giga Ethernet: 02

Cantidad: 02

4.2.4.3 Routers

También conocido como enrutador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes.

- **Router Cisco**

Modelo: 1921

Número de puertos: 02

Puerto Giga Ethernet: 02

Cantidad: 01

4.2.4.4 Modem

Es un dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (demodulación), y permite así la comunicación entre computadoras a través de la línea telefónica o del cable módem. Sirve para enviar la señal moduladora mediante otra señal llamada portadora.

- **Modem Tp-Link adsl2**

Modelo: TD-W8970B

Número de puertos: 04

Puerto Giga Ethernet: 01

Cantidad: 01

4.2.4.5 UPS

Sistema de alimentación ininterrumpida, es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados. Otras de las funciones que se pueden adicionar a estos equipos es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Modelo: Apc Su a 1

Número de tomas: 08

Capacidad: 1 000 kw

Cantidad: 02

4.2.4.5 Servidor VPN

Debido a que se cuenta con licencias vigentes de Windows Server 2012 R2 y porque se utiliza este mismo sistema operativo para el servidor SAP, es la razón por el cual se podrá utilizar en los servidores de la empresa de VPN y Active Directory.

- **Servidor VPN (Forefront)**

Como ya se menciono anteriormente tiene como sistema operativo Windows Server 2012 R2 pero para poder configurar el servidor VPN es posible utilizar una herramienta de Microsoft denominada Forefront TMG.

✓ **Microsoft Forefront Threat Management Gateway (TMG)**

Microsoft Forefront Client Security (antes conocido como Microsoft Client Protection) brinda una protección unificada contra malware para sistemas operativos de escritorios empresariales, laptops y servidores que es más fácil de administrar y controlar. Basada· en la misma tecnología de protección de Microsoft altamente exitosa y ya utilizada por millones de personas en todo el mundo, Forefront Client Security ayuda a proteger contra amenazas emergentes como spyware y rootkits, como también contra amenazas tradicionales como virus, gusanos y Trojan horses y

VPN. Proporcionando una administración simplificada a través de la administración central y brindando visibilidad crítica de .las amenazas y vulnerabilidades, Forefront Client Security lo ayuda a proteger su empresa con mayor confianza y eficiencia. Forefront Client Security se integra con su software de infraestructura existente, como Active Directory, y complementa otras tecnologías de seguridad para una mayor protección y mejor control.

Microsoft Forefront TMG puede actuar como un router, un gateway de Internet, un servidor de red privada virtual (VPN), un servidor de traducción de direcciones de red (NAT) y un servidor proxy.

- ✓ **Servidor Active Directory**

Función Servicios de dominio de Active Directory

Servicios de dominio de Active Oirectory (AO OS) del sistema operativo Windows Server® 2008) almacena información acerca de los usuarios, equipos y otros dispositivos de la red. AO OS ayuda a los administradores a administrar esta información con seguridad y simplifica el uso compartido de recursos y la colaboración entre usuarios. AO OS debe estar instalado en la red para poder instalar aplicaciones habilitadas para el uso de directorios, como Microsoft® Exchange Server, y para aplicar otras tecnologías de Windows Server, como la directiva de grupo.

4.3 Fase III: Diseñar el sistema de la red privada virtual (VPN) para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo.

4.3.1 Topología de la Red VPN

Con base a la formulación y recopilación de información obtenida en la fase I y II de este trabajo de grado se obtuvo la siguiente información sobre la estructura física de la empresa Teleinter 2009 C.A.

Tabla 5. Distribución de las Redes en la Empresa Teleinter 2099 C.A

Departamento	Numero de host
Gerencia	2

Recursos Humanos	1
Sistemas	4
Administración	2
Centro de control	10
Finanzas	2
Almacén	4
Logística	5
TOTAL	**30**

Autor: Flores, Reyes (2021)

Para el diseño de red de la empresa, se cuenta un router el cual esta enlazado al proveedor de servicios ISP y a la red LAN. La red LAN corresponde la estructura física, en ella encontramos un switch, que está conectado directamente al router, por medio de un cable directo es decir con sus dos extremos iguales. Este Switch estaría conectado finalmente a los host de los usuarios finales, como equipos, servidores e impresoras, por cables directos. Cada uno de estos dispositivos están configurados con una dirección IP partiendo de la 192.168.1.0 con máscara de subred /24 ó 255.255.255.0 En la siguiente tabla se puede observar el direccionamiento general de la empresa Teleinter.

Tabla 6. Direccionamiento general del al Empresa Teleinter 2099 C.A

ID	Dirección de red	Mascara	Gateway	Descripción
1	192.168.1.2	255.255.255.0	192.168.1.1	Administracion_1
2	192.168.1.3	255.255.255.0	192.168.1.1	Administracion_2
3	192.168.1.40	255.255.255.0	192.168.1.1	Gerencia_1
4	192.168.1.41	255.255.255.0	192.168.1.1	Gerencia_2
5	192.168.1.50	255.255.255.0	192.168.1.1	RRHH_1
6	192.168.1.60	255.255.255.0	192.168.1.1	Sistemas_1
7	192.168.1.61	255.255.255.0	192.168.1.1	Sistemas_2

8	192.168.1.62	255.255.255.0	192.168.1.1	Sistemas_3
9	192.168.1.63	255.255.255.0	192.168.1.1	Sistemas_4
10	192.168.1.70	255.255.255.0	192.168.1.1	Almacen_1
11	192.168.1.71	255.255.255.0	192.168.1.1	Almacen _2
12	192.168.1.72	255.255.255.0	192.168.1.1	Almacen _3
13	192.168.1.73	255.255.255.0	192.168.1.1	Almacen _4
14	192.168.1.74	255.255.255.0	192.168.1.1	Finanzas_1
15	192.168.1.75	255.255.255.0	192.168.1.1	Finanzas_2
16	192.168.1.10	255.255.255.0	192.168.1.1	CControl_1
17	192.168.1.11	255.255.255.0	192.168.1.1	CControl_2
18	192.168.1.12	255.255.255.0	192.168.1.1	CControl_3
19	192.168.1.13	255.255.255.0	192.168.1.1	CControl_4
20	192.168.1.14	255.255.255.0	192.168.1.1	CControl_5
21	192.168.1.15	255.255.255.0	192.168.1.1	CControl_6
22	192.168.1.16	255.255.255.0	192.168.1.1	CControl_7
23	192.168.1.17	255.255.255.0	192.168.1.1	CControl_8
24	192.168.1.18	255.255.255.0	192.168.1.1	CControl_9
25	192.168.1.19	255.255.255.0	192.168.1.1	CControl_10
26	192.168.1.30	255.255.255.0	192.168.1.1	Logistica_1
27	192.168.1.31	255.255.255.0	192.168.1.1	Logistica_2
28	192.168.1.32	255.255.255.0	192.168.1.1	Logistica_3
29	192.168.1.33	255.255.255.0	192.168.1.1	Logistica_4
30	192.168.1.34	255.255.255.0	192.168.1.1	Logistica_5

Autor: Flores, Reyes (2021)

En la siguiente figura se puede observar el diseño de la Red Privada Virtual (VPN) para dar la conectividad remota a los departamentos que están en la empresa.

4.3.2 Pasos para la configuración del Servidor VPN con Windows Server 2012

Primeramente antes de hacer la configuración de servidor VPN con el Windows Server 2012, es bueno establecer los requisitos para el sistema.

Tabla 7. Requisitos mínimos necesarios para la utilización del Windows Server 2012

Componentes	Requisitos
Procesador	**Mínimo:** 1 GHz **Recomendado:** 2 GHz **Óptimo:** 3 GHz o más
Memoria	**Mínimo:** 512 MB de RAM **Recomendado:** 1 GB de RAM **Óptimo:** 2GB de RAM (instalación completa) o 1 GB de **RAM**: (instalación de Server Core) o más Máximo (sistemas de 32 bits): 4GB (Standard) o 64GB.
Espacio en disco disponible	**Mínimo:** 8 GB **Recomendado:** 40 GB (instalación completa) o 1 O GB (instalación de Server Core) **Óptimo:** 80GB (instalación completa) o 40GB (instalación de Server Core) o más.
Pantalla y Periféricos	Súper VGA (800 x 600) o monitor con una resolución mayor. Teclado. Mouse de Microsoft o dispositivo señalador compatible.

Autor: Flores, Reyes (2021)

Luego de definir los requisitos mínimos necesario para la utilización del Windows Server 2012, se realizaron los siguientes pasos para la configuración del Servidor VPN.

1) Instalar el rol de acceso remoto, para esto se abre el administrador del servidor y se hace clic en administrar. Luego se selecciona agregar roles y características. (Observar figura 12).

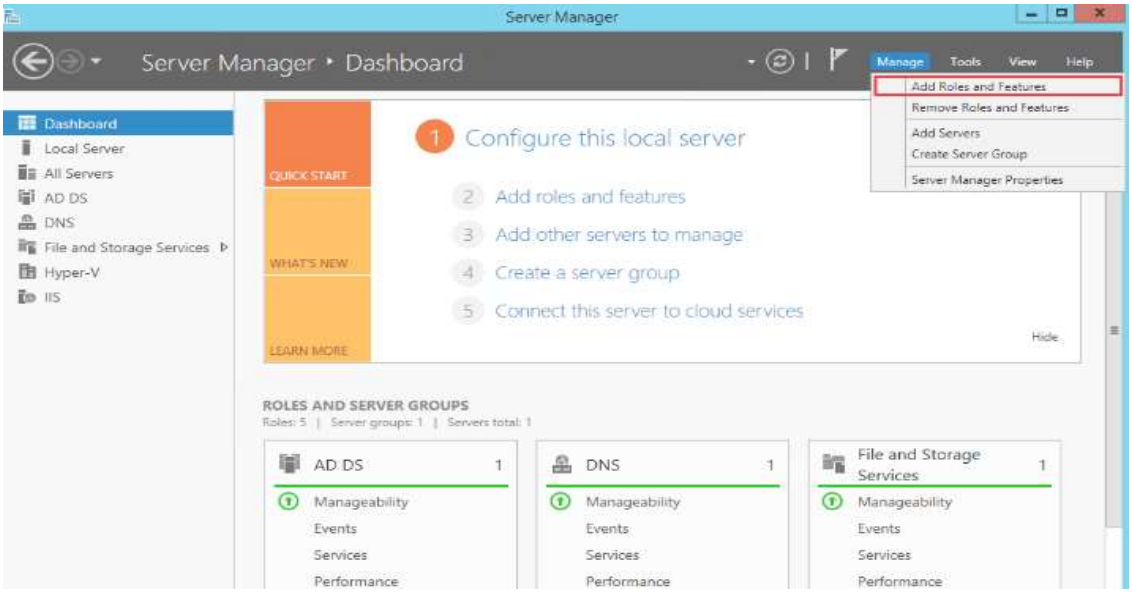


Figura 12. Paso 1 para la Configuración del Servidor VPN
Autor: Flores, Reyes (2021)

2) Se selecciona los Roles (Observar figura 13 y 14).

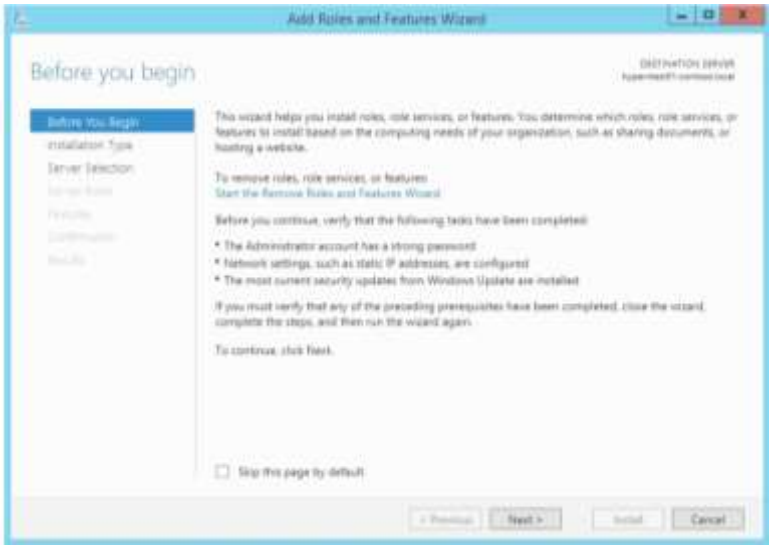


Figura 13. Paso 2 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

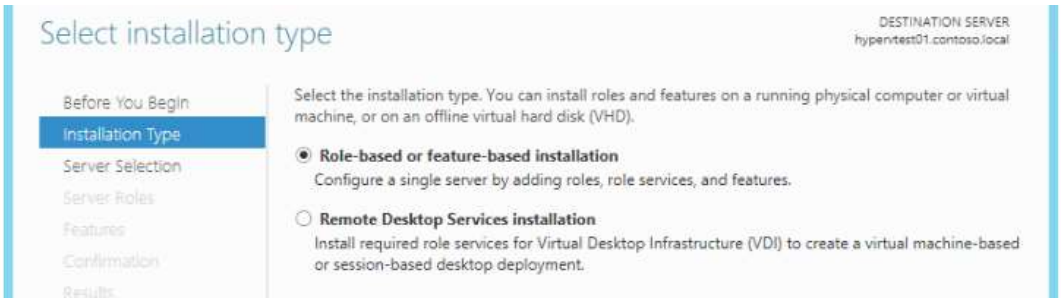


Figura 14. Paso 2.1 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

3) Luego selecciónanos un servidor de grupo de servidores. (Observar figura 14)

Figura 15. Paso 3 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

4) Y en el siguiente paso seleccionamos Acceso Remoto (Observar figura 13)

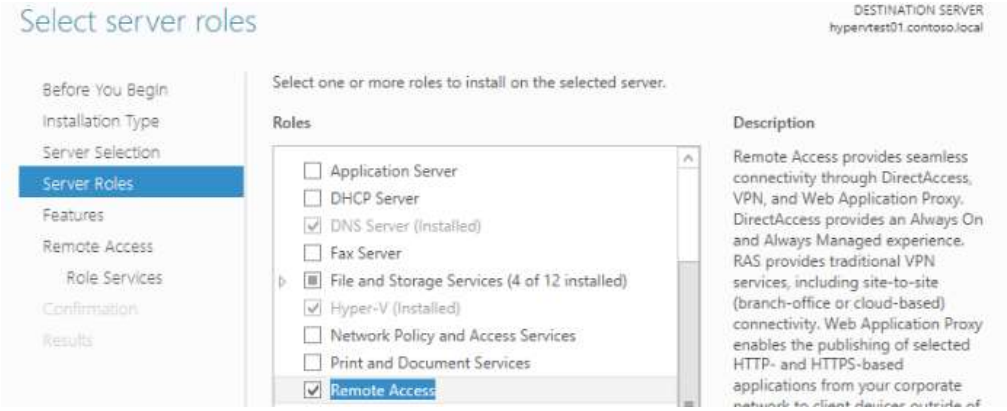


Figura 16. Paso 3 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

5) Luego no se selecciona ninguna característica y se le da clic en siguiente, hasta llegar a la instalación del rol acceso remoto. (Observar figura 17)

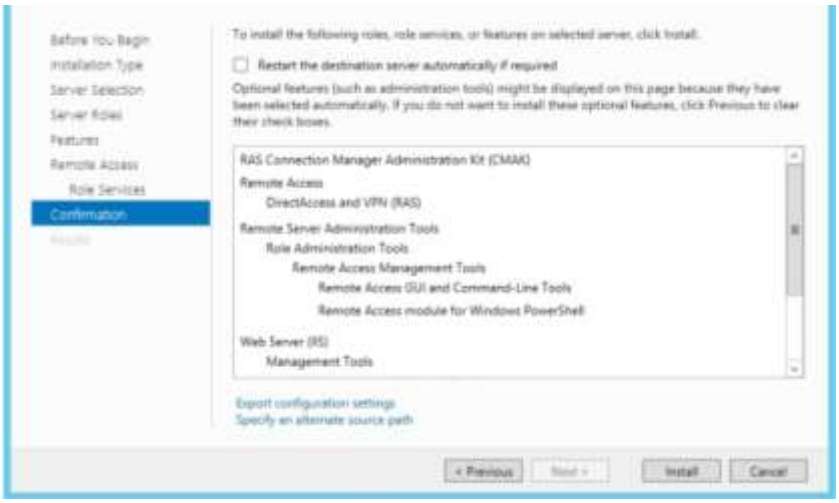


Figura 17. Paso 5 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

6) Luego después de haber hecho la instalación volvemos al Administrador del servidor y hacemos clic en Acceso Remoto. Seleccionamos el servidor y hacemos clic con el botón derecho, pulsando en Administración de acceso remoto y seleccionamos solo VPN. (Observar figura 18 y 19).

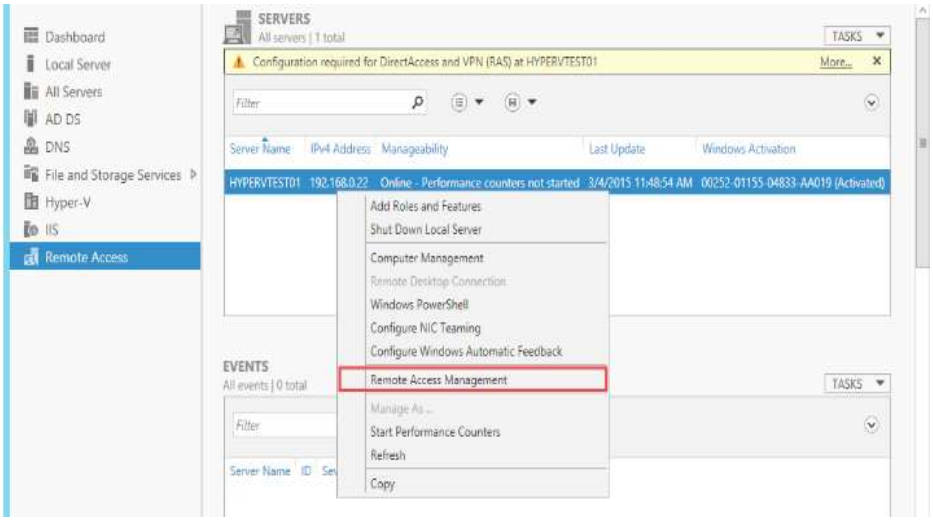


Figura 18. Paso 6 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

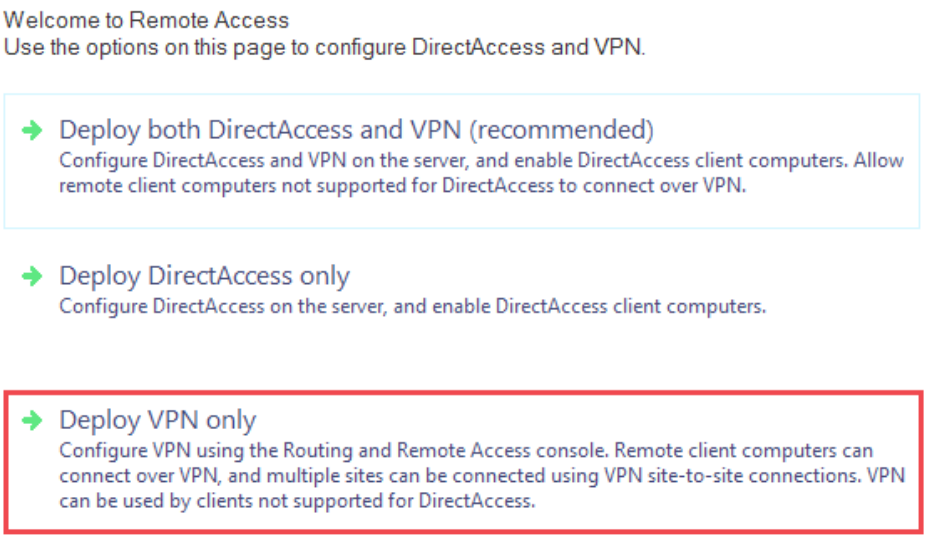


Figura 19. Paso 6.1 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

7) Luego seleccionamos nuestro servidor ya creado y configuramos y habilitamos el enrutamiento y acceso remoto. (Observar figura 20)

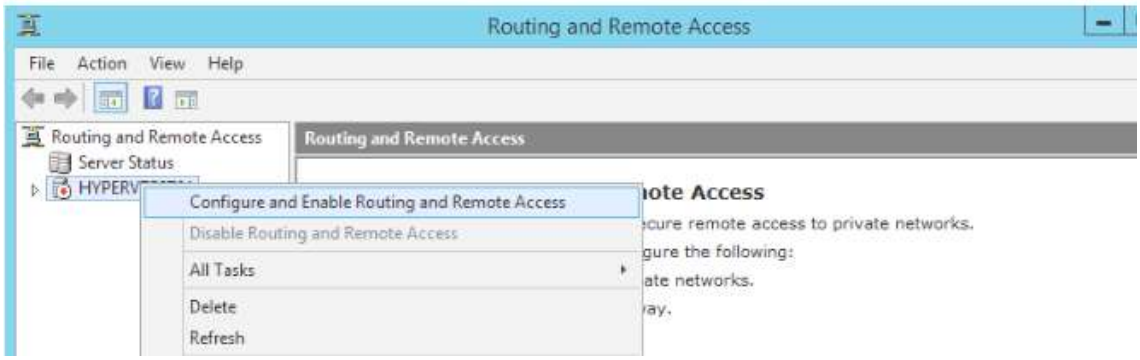


Figura 20. Paso 7 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

8) Luego nos vamos a la asignaciones de direcciones IP, en la que se marca la opción de un intervalo de direcciones especificados, debidamente en la ventana editar se agrega el rango de dirección de IP local con la finalidad de asignar IP a posibles trabajadores remotos que se puedan conectar a este servidor VPN. (Observar figura 21)

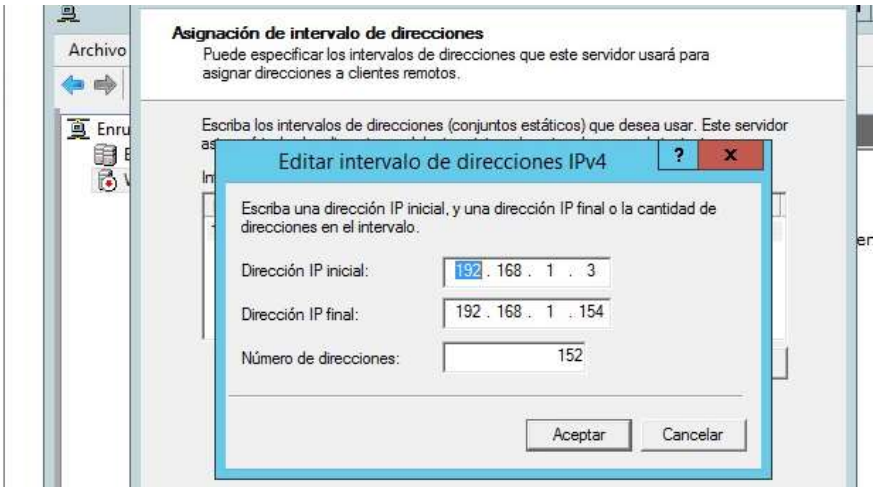


Figura 21. Paso 8 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

9) Estos paso explicados fueron algunos que se realizaron para la configuración del servidor VPN. Por último en consola Windows se verifico la conectividad junto con las direcciones IP asignadas a cada uno de los adaptadores de la empresa.

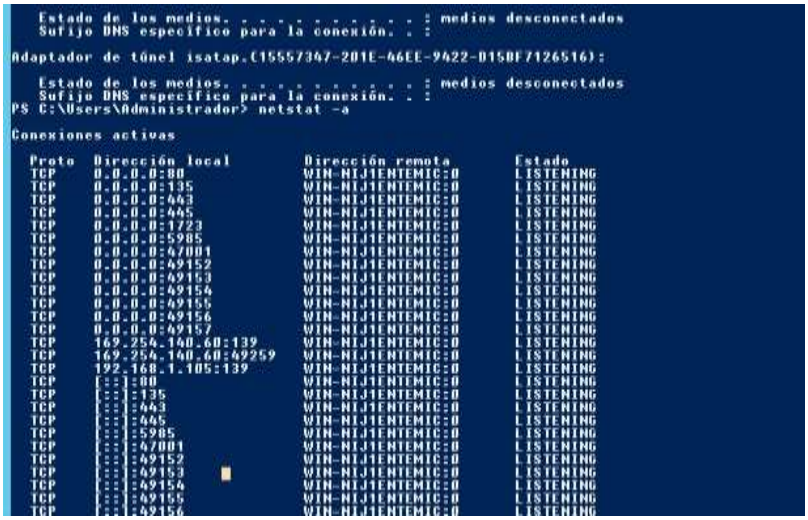


Figura 22. Paso 8 para la Configuración del Servidor VPN.
Autor: Flores, Reyes (2021)

Por último se ingresa al panel de control y luego al centro de redes y recursos compartidos del sistema local. Todo esto se realiza para hacer una verificación de un

cliente externo al servidor VPN, haciendo ingreso también de la dirección IP del servidor VPN, la cual anteriormente fue explicado cual era y en las ventanas conexiones se ingresan los detalles para el inicio de sesión del servidor VPN. (Ver figura 22).

Figura 23. Conexión al servidor de un posible cliente externo.
Autor: Flores, Reyes (2021)

Después en la consola de Windows se puedo verificar la conectividad y de las direcciones IP asignadas a cada uno de los adaptadores, incluyendo el de VPN.

4.4 Fase IV: Realizar un estudio de factibilidad, económico, técnico y ambiental para la red privada virtual (VPN) para la empresa Teleinter 2009 C.A, en Naguanagua, estado Carabobo.

4.4.1 Factibilidad Económica

El diseño de una Red Privada Virtual en la empresa Teleinter 2009 C.A es una alternativa económica para el acceso remoto en ambiente corporativo donde empleados, clientes y gerentes pueda intercambiar información de forma segura desde cualquier lugar del mundo a través de internet sin la necesidad de utilizar canales dedicados que son muy costosos.

Las principales razones para optar por esta solución son fundamentalmente los costos en cuanto a la infraestructura, mantenimiento y seguridad de la información para permitir la comunicación de los usuarios remotos (clientes, empleados externos, entre otros) desde cualquier lugar del mundo.

- **Infraestructura:** Resulta más económico emplear una infraestructura pública que desplegar una red físicamente privada. Si empleamos una conexión publica estaríamos reduciendo notablemente costos en cuanto facturas a Proveedores de Internet (ISP), cableado, enrutadores.
- **Mantenimiento:** Para un optimo funcionamiento de las redes se debe efectuar frecuentemente mantenimiento a los elementos que conforman la red, por ejemplo las conexiones locales, WIFI, conexión con el proveedor, hardware y software, en el caso de una red privada los costos serian mayores ya que se debe hacer una revisión.

Tabla 8. Costos de los Equipos para la red VPN

Implemento	Descripción	P. Unitario	Cantidad	TOTAL
Cable UTP	CAT. 5: Ancho de Banda de 100 MHz, distancia de hasta 100 Estándares: UL444/UL1581, TIA/EIA 568B.2	5	20mtrs	100
Router	Router Modular: Permiten la conexión a redes de cualquier tipo (ADSL2+, VDSL2, Gigabit, E1/T1, Wifi, 3G, etc.), conexión a redes públicas analógicas o digitales (BRI/PRI)).	40	2	80

	Interfaces Ethernet 10/100/1000. Seguridad (WEP/WPA/WPA2).			
Switch	Modular. Velocidad de 10/100/1000. 0 puertos 10BASE-T/100BASE-TX/1000BASE-T; puerto de alimentación RPS (-48 VDC); puerto de consola RJ-45; 2 puertos de apilamiento dedicados; 1 ranura para módulo opcional. Seguridad: RADIUS; autenticación PAP/CHAP/EAPoL (EAP sobre LAN)	80	2	160
Servidor	Dell: Intel® Xeon® X3440 (8MB Caché, 2.53 GHz, Turbo, HT), Memoria de 16GB (4X4GB), 1333Mhz, Dual RankedUDIMM, RAID 5 - PERC S100 (SATA Software RAID Integrado) soporta 3 a 4 Disco Duros , Disco duro SATA	500	1	500

	250GB 7.2K RPM 3Gbps 3.5 pulgadas Cabled, Broadcom® 5709 de puerto doble, Gigabit Ethernet, con TOE/iSCSI, PCIe x4 ,			
	TOTAL			**840**

Autor: Flores, Reyes (2021)

Costos de Implementación

Tabla 9. Costos de Implementación

Detalle	**Tiempo de implementación**	**Precio Total en $**
Instalación y configuración de protocolo y servidor VPN	4 días	700
Capacitación de usuarios para instalación de cliente VPN en máquinas remotas	2 días	250
Capacitación de personal encargado de IT para poder ofrecer soporte y mantenimiento a servidor y servicios VPN	2 días	400
	TOTAL	1350

Autor: Flores, Reyes (2021)

Resumen de costos

Detalle	Precio Total en $
Costos de los equipos	840
Costos por implementación	1350
TOTAL	2190

El costo total de de implementación de una Red VPN para la empresa Teleinter 2009 C.A es de aproximadamente 2190 $ por lo que resulta ser una solución económicamente factible.

4.4.2 Factibilidad Técnica

Gracias a los avances de las telecomunicaciones y de la tecnología en general, los sistemas se han ido simplificando y ofreciendo mejores respuestas ante las constantes demandas del mundo actual. En este caso concreto, la implementación y configuración de esta nueva tecnología no representa alta complejidad. Cualquier persona con conocimientos técnicos en redes es capaz de configura el sistema sin problema. Y por otro lado en cuanto a los usuarios involucrados y empleados este nuevo sistema será de gran ayuda para poder realizar un trabajo eficaz por teletrabajo, con lo que de esta manera no se para ni la empresa ni los empleados por esta afección que está ocurriendo debido a la pandemia.

4.4.3 Factibilidad Ambiental

Para la factibilidad ambiental este proyecto de grado ofrece grandes beneficios que caracteriza la utilización de una VPN en el aspecto ambiental. Puesto que las compañías que apuestan por el uso un sistema de acceso remoto a su red (VPN) para fomentar el teletrabajo también conocido como trabajo a distancia contribuyen a reducir la huella de carbono, así como de otros contaminantes atmosféricos con efecto invernadero o sobre el cambio climático.

Por otro lado según los cálculos realizados por Fundación Más familia basados en la encuesta de movilidad en día laboral (realizada en Barcelona en 2017, bajo la hipótesis de teletrabajo de 2 días/semana (40%) que es la opción preferida y con una estimación del 40% de la población susceptible de teletrabajo), se obtendría una reducción de 332.843 ton CO2/año o unas 336.171 ton de GEI/año (GEI - gases de efecto invernadero).Sin embargo el libro blanco destaca que, según las estadísticas del Instituto Nacional de Seguridad e Higiene en el Trabajo (INSHY), en 2017 se produjeron 49.289 accidentes de tráfico durante el viaje hasta o desde el trabajo, con baja laboral, un 3% más con respecto al ejercicio anterior.

CONCLUSIONES

- Debido a las ventajas económicas que ofrecen las Redes Privadas Virtuales se puede concluir que se trata de una excelente tecnología para el acceso remoto, puesto que el uso de una VPN constituye un sustituto indispensable a los métodos tradicionales caros como es la transmisión de datos a través de fibra óptica punto a punto. Además, constituye una buena solución alterna a los métodos de implementación de redes WAN tradicionales.
- El diseño de la red VPN de la empresa Teleinter 2009 C.A inicia desde cero, teniendo en cuenta el sistema actual, con el fin de evitar inconsistencias a futuro. El montaje de la red puede realizarse mediante Packet Tracer para configurar los dispositivos de forma real, permitiendo el comportamiento y funcionamiento de los dispositivos al configurarlos y evitando inconsistencias a futuro.
- El direccionamiento IP que se realizo para la empresa Teleinter 2009 C.A a partir de una dirección IP, permitirá la escalabilidad y rendimiento de la red, es decir, que si la empresa sigue creciendo no tendrá inconveniente con la asignación de direcciones a equipos nuevos.
- El diseño de la red para la empresa la empresa Teleinter 2009 C.A permite a los usuarios trabajar de una forma sencilla, efectiva y segura, generando mayor productividad, reflejándose en la facilidad y rapidez, para la obtención de información.
- En cuestión de la seguridad en una VPN es muy importante. La gran mayoría de las organizaciones podrán ver satisfechas sus necesidades de seguridad con las tecnologías de seguridad existentes, pero siempre será necesario llevar un control estricto de la seguridad y mantener actualizada la VPN con los últimos avances en tecnología.

- Una VPN podrá ser aplicada en todo tipo de entornos, desde las grandes empresas con sucursales en diversas partes del país o del mundo y varios trabajadores móviles hasta las pequeñas empresas que tengan dos o más sucursales en una sola ciudad; así como también las diversas dependencias del gobierno que necesiten intercambiar información entre ellas; e instituciones educativas como universidades y en general cualquiera que necesite acceder a sus archivos desde una ubicación remota de manera segura podrá obtener beneficios con esta tecnología.
- Las VPN permiten brindar servicios a los clientes de la empresa en cualquier lugar del mundo, con lo que los clientes obtendrán la información que el necesita al instante, lo que generará una mayor productividad de la empresa.

RECOMENDACIONES

- Continuar con el estudio de la tecnología de VPN, ya que es una tecnología que va creciendo y que necesita de una constante actualización de conocimientos debido a las constantes actualizaciones en el software de soporte que se implementan en los sistemas operativos especialmente en Windows.
- Cabe anotar que la metodología expuesta, puede ser no acoplable para determinada situación o empresa, por lo que se recomienda plantear nuevas metodologías de acuerdo a las necesidades particulares que se presenten en cada empresa.
- Realizar mantenimiento periódico a nivel de hardware y software, a los equipos para evitar inconvenientes con el funcionamiento de la red tanto local como externa.
- Se deben tener en cuenta los requerimientos mínimos para el servidor en el caso del SO Windows server 2012 es RAM 512, 1GB recomendada procesador P IV o superior y disco duro de 40 GB mínimos.
- Crear un manual que defina los pasos que deben seguir los trabajadores para obtener la conexión a la red VPN.

REFERENCIAS

Bibliográficas

Aguiar, M (2012). **Configuración de una Red en telecomunicaciones**. Recuperado en: **http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf**

Arias, F. (2010). **El proyecto de investigación: Introducción a la metodología científica.** 3ra Edición. Caracas: Editorial Episteme.

Arias, F. (2012). **El proyecto de investigación. Introducción a la metodología científica.** Caracas: Editorial Episteme.

Hurtado, J. (2010). **El proyecto de investigación.** Caracas: Editorial Quirón.

León, P. (2015). Redes de Comunicación. Editorial: Mc Graw- Hill. España.

Mendoza, A. (2017) .**Diseño e implementación de un prototipo de red privada virtual en capa 3 utilizando Cisco IOS para la Universidad Nacional del Altiplano.** Quito, Perú. Editorial Politécnica Nacional.

Microsoft Corporation. (2010). **Windows Server 2000.** Recuperado en: **www. Microsoft.com/windows2000/server/default.asp**

Mora, M (2010). **Estructura básica de los osciloscopios analógicos y digitales**. Recuperado en: http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf

Palella y Martins (2010). **Metodología de la investigación cualitativa.** Caracas: Editorial Fedupel. Segunda Edición.

Peña, V (2017) . **Diseño e implementación de un Red Privada Virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada.** Recuperado en: **http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf**

Pulido y Velázquez (2019).**Sistema de una Red Privada Virtual para Radio América en Valencia, Estado Carabobo.** Carabobo. Editorial UJAP

Ramírez M. (2015). Protocolos de Seguridad para Redes Privadas Virtuales (VPN). Recuperado en:

https://repository.DiseñoyconstrucciondeunGPONa.pdf;jsessionid=8B8F6719F0983D83E2EA5922851F8A89?sequence=2

Sabino, C. (1996). **Introducción a la Metodología de Investigación**. Caracas: Editorial: Panapo.

Stallings, W. (2004). Comunicaciones y redes de computadoras. Editorial: Prentice-Hall. México.

Tamayo, M. (2003). **El proceso de la investigación científica.** 3ra edición. México: Editorial Limusa.

http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf