UNIVERSIDAD JOSÉ ANTONIO PÁEZ

SISTEMA DE ACCESO REMOTO
A LA RED CORPORATIVA DE LA
EMPRESA RADIO AMERICA
EN VALENCIA, ESTADO CARABOBO

Autores:
Pulido Narlesky
Velásquez Miguel.

Urb. Yuma II, calle Nº 3. Municipio San Diego
Teléfono: (0241) 8714240 (máster) – Fax: (0241) 8712394

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

SISTEMA DE ACCESO REMOTO A LA RED CORPORATIVA DE LA EMPRESA RADIO AMERICA EN VALENCIA, ESTADO CARABOBO

Trabajo de grado presentado como requisito para optar al título de

INGENIERO TELECOMUNICACIONES.

Autores:
Pulido Narlesky
CI: .21.663.611
Velásquez Miguel.
C.I.: 18.097.129
Tutor: Ing. Oliger Mendoza

San Diego, Agos

Universidad José Antonio Páez
Decanato de Ingeniería

FI-T -003 -2019-2CE

Valencia, 18 de Julio de 2019

Ciudadanos:
Narlesky Pulido
C.I:21.663.611
Miguel Velásquez
C.I:18.097.129
Presente-

Cumplo con informarle que la Comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión **N° 01-2019** de fecha **18-07-2019** aprobó el proyecto de trabajo de grado titulado **SISTEMA DE ACCESO REMOTO A LA RED CORPORATIVA DE LA EMPRESA RADIO AMÉRICA EN VALENCIA, ESTADO CARABOBO** Presentado por usted como requisitos para optar al título de Ingeniero en Telecomunicaciones.

Se ratifica la designación del Ing. Oliver Mendoza C.I:11.556.607 y la Ing. Alicia De Pizzela C.I: 4.598.880 como Tutores Académicos y Metodológicos que los asesoraran en el desarrollo de este proyecto.

Atentamente,

Prof. Luis Lira
Decano de la Facultad de Ingeniería

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

LL/le

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

ACEPTACIÓN DEL TUTOR

Quien suscribe, Ing. Oliger Mendoza, portador de la cédula de identidad N°11.556.607, en mi carácter de tutor del trabajo de grado presentado por la ciudadana Narlesky Pulido, portadora de la cédula de identidad N° 21.663.611 y el ciudadano Miguel Velásquez portador de la cedula de identidad N° 18.097.129, titulado **SISTEMA DE ACCESO REMOTO A LA RED CORPORATIVA DE LA EMPRESA RADIO AMÉRICA EN VALENCIA, 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, a los 15 de Agosto del año 2019

Ing. Oliger Mendoza.
C.I.: 11.556.607

ÍNDICE GENERAL

LISTA DE TABLAS

TABLA **Pp.**

LISTA DE FIGURAS

FIGURA **Pp.**

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

Autores: Pulido Narlesky
Velásquez Miguel.
Tutor: Ing. Oliger Mendoza.
Fecha: Agosto 2019.

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. Los datos transmitidos a través de Internet son mucho más vulnerables que cuando viajan por una red interna de una organización, están expuestos ante cualquier usuario. 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 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.

Descriptores: Red privada, sistema, acceso remoto.

INTRODUCCIÓN

Como es sabido, las telecomunicaciones son de vital importancia para comunicarnos a diario, esto ha hecho que el acceso al ancho de banda y a las velocidades de transmisión, sean parámetros exigidos al momento de solicitar los servicios de telecomunicación. Es por ello, que ha surgido una variedad de alternativas para los sistemas de red privada.

Las formas de comunicación computacionales en el mundo entero que se aplican en estos momentos como necesidad primordial, han sufrido evoluciones a medida que crece la tecnología. Y ya a estas alturas toda organización tendrá la necesidad de estar comunicada ya sea localmente como con el mundo entero. Por este motivo surgen las redes organizacionales donde entre los nodos terminales se realizan diferentes operaciones e intercambio de datos, los cuales han requerido contar con normas de seguridad para no sufrir modificaciones o pérdidas de información. Para las redes locales no existe mayor riesgo debido a que el organizador de la red dará los permisos a cada usuario. Pero cuando se realizan enlaces punto a punto sobre un medio público las empresas necesitaran resguardar de una mejor forma sus bases de datos para transportarlos. Luego de costosos modelos de transporte físico nacen las redes privadas virtuales, que básicamente realizan túneles a través de la plataforma pública.

Por lo que en la actualidad, las organizaciones han incrementado las implementaciones de la VPN-SSL, dicha implementación se encarga de conectar usuarios remotos a la LAN de la Organización. La conexión vía VPN-SSL, se establece mediante una infraestructura pública (Internet) de manera segura, ya que los datos se establecen a través de un canal cifrado. La conexión a través de esta infraestructura pública, permite la reducción de costos en la implementación y se puede establecer la conexión segura desde cualquier ubicación geográfica.

A través de cuatro (4) capítulos, se expone el desarrollo del trabajo de grado, seguidamente se presenta la estructura general de cada capítulo y se comenta brevemente la finalidad de cada uno:

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, como objetivo principal del trabajo de grado se tiene “Proponer el diseño de la red privada virtual mediante acceso remoto para la empresa Radio América”.

Capítulo II: se hace hincapié en los antecedentes, se establecerán las bases teóricas que sustentan la realización del proyecto, al igual que los antecedentes existentes que aportan a la posible solución del mismo.

Capítulo III: se planteara 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 sirvió de guía para el desarrollo del trabajo de grado.

Capítulo IV: en el último capítulo se dará a conocer los recursos económicos que serán necesarios para el desarrollo del proyecto y los resultados del mismo.

CAPÍTULO I
EL PROBLEMA

1.1 Planteamiento del problema

Las necesidades de las diferentes corporaciones motivan la creación de redes LAN, WAN, intranet, extranet y claro, el Internet. Las empresas conectan sus sucursales con la oficina central a través de redes WAN. También se puede instalar infraestructura para permitir el acceso remoto. Pero surge una problemática al tratar de mantener una red privada en estas condiciones: resulta ser en la mayoría de las ocasiones costosa y poco segura.

A pesar de la evolución de las tecnologías de seguridad, que están para suplir las necesidades generadas por el advenimiento de Internet, la red mundial de ordenadores todavía se utiliza como medio, y herramienta, para la actuación de usuarios malintencionados, que tienen como objetivo fraudar o capturar información crítica de empresas y personas.

Actualmente, en la empresa Radio América Valencia Edo Carabobo, los empleados necesitan ingresar a la red interna de manera remota para acceder al sistema en búsqueda de soluciones de problemas fuera del horario laboral, también existen personal que trabaja desde casa o de manera móvil, se requiere fomentar la interrelación entre los trabajadores y reducir procesos burocráticos para compartir información los más rápido posible. Por lo indicado anteriormente, la empresa debe contar con un mecanismo de acceso remoto seguro como la VPN (Virtual Prívate Network).

Debido a esto, resulta necesario buscar maneras de cómo garantizar conectividad a la red para los trabajadores de la empresa Radio América, que sea capaz de satisfacer la demanda de peticiones al servidor, mantener la seguridad y la privacidad mientras nos conectamos a internet y que permita ahorrar costos de instalación y servicio.

1.2 Formulación del problema

Del planteamiento del problema descrito anteriormente se deriva la siguiente interrogante:

¿De qué forma se puede contribuir para mejorar el sistema de acceso remoto entre los trabajadores y la red interna de la empresa Radio América de tal forma que se garantice la seguridad de la información?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

Proponer el diseño del sistema de acceso remoto a la red corporativa de la empresa Radio América.

1.3.2 Objetivos Específicos

- Diagnosticar el estado actual de la red interna de la empresa Radio América
- Análisis de las alternativas para acceder de manera remota y segura a la red interna.
- Diseñar el sistema de red privada virtual para dar conectividad remota de manera segura a los departamentos de recursos humanos y administración.
- Realizar un estudio de factibilidad económica, ambiental operativa y social.

1.4 Justificación

A medida que la empresa crece con el tiempo, requiere cambios drásticos que brinden seguridad, eficiencia, calidad y economía para satisfacer y mejorar las necesidades operativas que se presenta a diario; van a la mano las exigencias de las redes las cuales deben adaptarse a los cambios que se puedan presentar. Uno de estos cambios es optimizar las redes de área global a redes que tengan una distancia mayor a la local, permitiendo la conectividad de su personal y oficinas de otros edificios con la sede central y disponer de los mismos servicios sin importar su ubicación.

Tecnológica:

Las ventajas tecnológicas que brinda una VPN a la Radio, es la escalabilidad que tiene esta tecnología ya que puede adaptarse a más usuarios y muchos más lugares a diferencia de las líneas dedicadas, la instalación de esta en cualquier PC Windows es muy sencilla, evita altos costos de actualizaciones y mantenimiento de las PC´s remotas, control de acceso según políticas de la empresa, ya que la empresa podrá gozar de una conexión a una red con las características de una red privada.

El constante volumen de información que genera la empresa sumado a las constantes innovaciones tecnológicas, hace que sea posible elaborar sistemas de información con un mayor grado de adaptabilidad y flexibilidad ante las diferentes problemáticas que se presentan.

Económica:

El diseño de una VPN para la empresa Radio América CA, es una forma económica en la comunicación entre oficinas, trabajadores externos, clientes, proveedores, mediante acceso remoto a los servidores, intranet y aplicativos de la empresa, reemplazando las costosas conexiones permanentes como Frame Relay, Punto a Punto, Firewall ASA, o RDSI. La Radio estaría reduciendo costos en inversiones de hardware y servicios de telecomunicaciones costosas y proporcionales a la distancia implicada en la conexión de las oficinas. Con el uso de VPNs mediante Internet, la inversión en hardware es pequeña y la distancia no influiría en costos adicionales**.** Además, la implementación de dicha VPN utilizaría hardware y software ya disponible en la empresa.

1.5 Alcance de la Investigación

El proyecto de grado se enfoca en el diseño e implementación de una VPN y se aprovechará la disponibilidad del directorio activo de la organización. Para culminar exitosamente la implementación se debe realizar las siguientes actividades:

- Definir una política de acceso remoto a la red.
- Definir la arquitectura a utilizar en la implementación de la VPN

- Configurar e implementar los protocolos de seguridad para la conectividad de los usuarios VPN.
- Desarrollar actividades de capacitación a los empleados para correcto uso del sistema de acceso remoto a través VPN.

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 pudo 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 una investigación más profunda, es importante destacar que anqué se consiguió información relevante para la investigación, la misma fue limitada.

CAPÍTULO II
MARCO TEÓRICO

Según Méndez (2005) se define el Marco Teórico como, una descripción detallada de cada uno de los elementos de la teoría que serán directamente utilizados en el desarrollo de la investigación. También incluyen las relaciones más significativas que se dan entre estos elementos teóricos.

A continuación, se presentan varios proyectos o trabajos integradores efectuados en los últimos años, y tomando aportes valiosos para la investigación que pueda brindar cada uno de ellos.

2.1 Antecedentes

Peña, V. (2019) 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.

De la misma manera González, A. (2017) en su trabajo de grado **"Red Privada Virtual".** Presentado en la Institución Universitaria Politécnico Gran Colombiano para optar por el título Ingeniero en Telecomunicaciones y Electrónica. Colombia. La investigación tuvo como propósito el desarrollo de una Red VPN bajo el modelo OIS, el cual se desarrolla en distintas capas, específicamente contiene 7 capas las cuales son: capa física, capa de enlace de datos, capa de red, capa de transporte, capa de sesión, capa de presentación y capa de aplicación, las cuales el desarrollo de estas capas pudieron realizar la implementación de la Red Privada Virtual VNP. En este proyecto se llevó a cabo la conexión vía SSL-VPN, la cual garantiza la continuidad del negocio permitiendo establecer conexión desde cualquier ubicación geográfica y al utilizar el protocolo LDAP en la VPN-SSL.

El proyecto se vincula con el actual para la realización del modelo, ya que para este trabajo de grado se escogió el modelo OIS. Este trabajo de grado ofrece toda la documentación necesaria para el diseño de una Red VPN por capas. Por otro lado ofrece como realizar una conexión vía SSL-VPN.

Por último, Ramírez M. (2015) contribuye en su trabajo de grado **"Protocolos de Seguridad para Redes Privadas Virtuales (VPN)".** Presentado en la Universidad Austral de Chile para optar por el título de Ingeniero en Telecomunicaciones. Chile. El presente trabajo de grado tuvo como el propósito de indagar sobre las redes locales no existe mayor riesgo debido a que el organizador de la red dará los permisos a cada usuario. Pero cuando se realizan enlaces punto a punto sobre un medio público las empresas necesitaran resguardar de una mejor forma sus bases de datos para transportarlos. Luego de costosos modelos de transporte físico nacen las redes privadas virtuales, que básicamente realizan túneles a través de la plataforma pública. Por lo que este trabajo de grado analiza las diferentes formas que

hacen posible crear túneles a través de estos medios considerados como poco seguro para quien necesite que sus datos no sean dañados, leídos o tergiversados.

El proyecto se vincula con el actual ya que se necesita estudiar la seguridad de enlaces punto a punto sobre un medio público, ya que las empresas necesitaran resguardar de una mejor forma sus bases de datos para transportarlos. Por lo que es importante tener a la disposición todos los modelos y estructurar que se adoptan a todos tipos de seguridad para un Red Privada Virtual (VPN).

2.2 Bases teóricas

2.2.1 Concepto de VPN

VPN significa literalmente VIRTUAL PRIVATE NETWORK, en español RED PRIVADA VIRTUAL.

2.2.1.2 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. (ver figura 1).

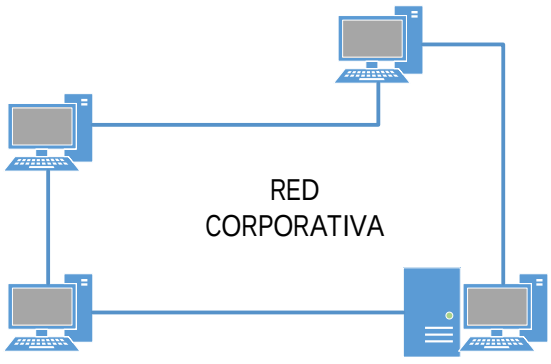

Figura 1. Estructura básica de una RED
Fuente: los autores

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, es un modelo bastante sencillo.

2.2.1.3 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.

2.2.2 RED VPN

Una VPN (Virtual Private Network), es una red privada virtual que utiliza una red pública (Internet) para conectar sitios remotos o usuarios. En vez de utilizar una conexión dedicada como enlace WAN, una VPN utiliza conexiones "virtuales" que se enrutan a través de Internet desde la red privada de la empresa hasta el sitio remoto o viceversa.(Ver figura 2).

Una 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.
- Servir de apoyo al trabajador que está desplazándose.

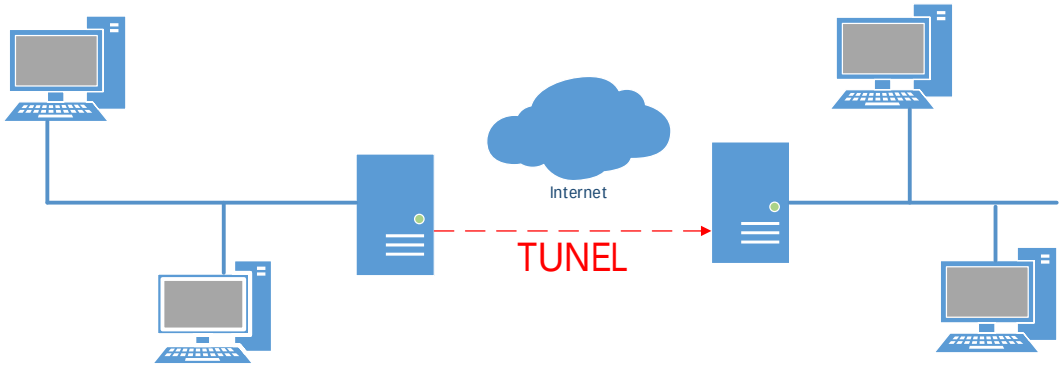

Figura 2. RED VPN.

- **Fuente:** los autores

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. 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.

2.2.2.1 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.

2.2.2.2 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 Acceso remoto del usuario sobre una Red publica

Las VPN proporcionan acceso remoto a recursos corporativos sobre la red Internet pública, manteniendo al mismo tiempo privacidad y seguridad de la información.

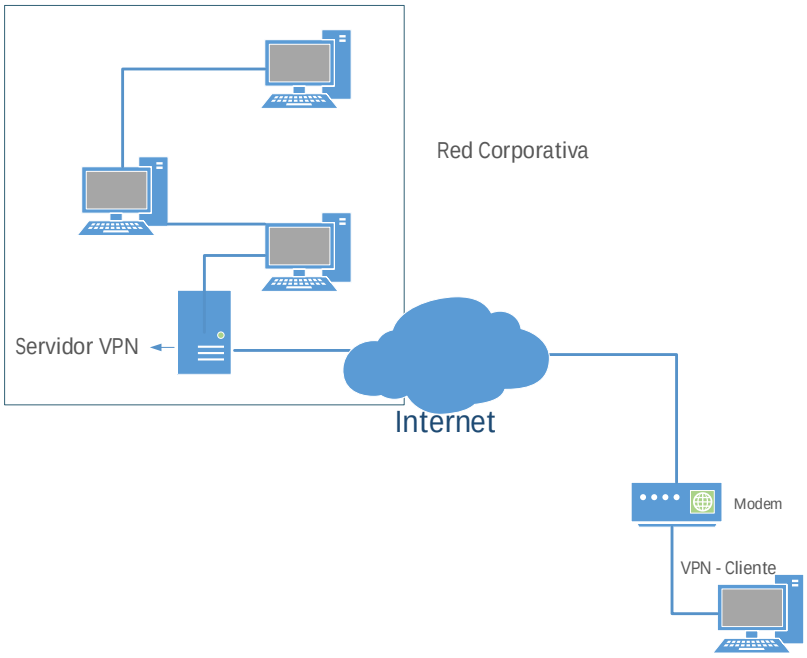

Figura 3. Acceso Remoto de un usuario a un VPN

- **Fuente:** los autores

Este tipo de conexión se establece cuando un usuario de la red corporativa se encuentra realizando un trabajo geográficamente lejos o algún cliente de la empresa necesita obtener datos en forma remota de las bases para futuras transacciones. Luego de la configuración VPN previa del equipo remoto que va a ser conectado a la red, se debe adquirir un servicio de Internet al ISP local. Utilizando la infraestructura de la Internet de esta manera se realiza un túnel de comunicación del equipo con el servidor VPN de la organización de manera confiable donde se puede asegurar que los datos serán tan confidenciales como si se tratase de una red privada o dedicada. Además la gran ventaja de esta alternativa es que decrecen significativamente los costos de conexión debido que no es necesario establecer la comunicación mediante llamada de larga distancia a un servidor de acceso de red (NAS), lo cual implica un gasto adicional mucho más elevado para el logro del objetivo.

2.2.4 VPN Cliente-Servidor

Existe el caso del usuario que forme parte de un ambiente laboral dentro de un edificio donde se implementa una LAN (red de área local), pero este usuario desea comunicarse confidencialmente de manera específica con solo un departamento de dicha LAN, sin que terceros miembros intercepten la información en cuestión. Entonces se utilizaran los servicio de encaminamiento de datos de la Internet o los de la misma impuesta por la LAN para realizar un túnel con encriptación y se logre la seguridad y confidencialidad que se requiere. Algunos de los problemas que surgen si no se toman medidas de seguridad en el tráfico de datos adecuadas son:

- Cualquier usuario conectado a la red tendrá acceso libre a servicios críticos.
- La información que viaja por la red queda sensible a sniffing (visualización por parte de terceros)
- Importación de usuarios validos con datos obtenidos del medio de transmisión.

Y para el caso en que la organización haya implementado un sistema que exija autentificación del usuario que entra al departamento de la red:

- Captura de password por sniffing y posterior importación de usuario.

La alternativa de solución de estos problemas de seguridad es la incorporación del servidor VPN para la RED o departamento dedicado que necesite resguardar datos y requiera la comunicación con usuarios que se encuentre físicamente situados en la RED común para todos. Es decir con esta implementación se configuran tanto el servidor VPN como los equipos que auténticamente tendrán acceso a la información confidencial, de manera tal que se lograra crear un túnel de comunicación privada entre estas dos partes, sin que terceros puedan captar o capturar los datos de intercambio.

Las ventajas que se obtienen al poner en marcha el sistema VPN dentro de una LAN son:

- **Implementación transparente a las aplicaciones:** Una vez configurado mediante un simple cambio de rutas, todo el tráfico es automáticamente encriptado y validado sin necesidad de cambio alguno en la operatoria. ·
- **Alta seguridad:** al encriptar no solo los datos sino también las direcciones destino, se evita que terceras personas tengan acceso a la información.
- **Distintos niveles de seguridad:** según la necesidad, se puede operar con password preconfigurados o para mayor seguridad con certificados para firmas digitales de RSA 1024/2048 bits para la autentificación de los extremos.

La figura 4 permite visualizar en forma global los niveles de seguridad que se puede lograr al implementar un enlace VPN dentro de una organización:

- Línea Roja: Camino Inseguro
- Línea Negra: Camino Seguro
- Línea Azul: Camino seguro protegido por modelo VPN

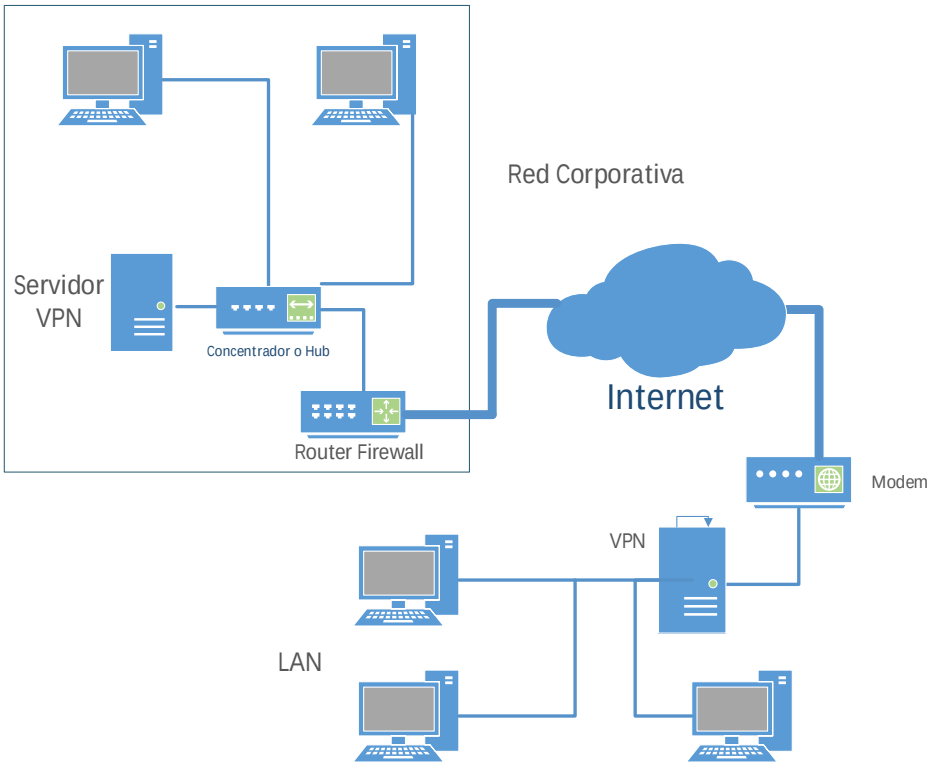

Figura 4. Acceso privado de un cliente dentro una red cooperativa
Fuente: los autores

2.2.5 VPN Servidor-Servidor

Este es el caso en que dos oficinas de una misma organización las cuales poseen un equipamiento de infraestructura lo bastante robusto como para soportar ordenadores creando redes corporativas, las cuales requieran comunicarse remotamente mediante alguna red pública. Si estas sucursales no mantienen las medidas de seguridad para resguardas los paquetes que viajan por la red tendrán el riesgo de que su información privada sea captada o se pueda tener acceso al sistema con fines perjudiciales. Si se desea optar a una forma de interconexión más segura se deberá inve rtir en un enlace punto a punto lo cual podría generar altos costos de instalación. Los problemas que podría generar el modelo en el cual se realiza una interconexión mediante red pública son los que se citan a continuación:

- Cualquier usuario conectado a la red pública podrá tener libre acceso a servicios críticos e información confidencial.
- Información viajando sensible a sniffing (visualización por parte de terceros).
- Importación de usuarios validos con datos obtenidos del medio de transmisión.

Para dar una alternativa solución a este tipo de problemas ambas redes tendrán que incorporar a los terminales de acceso al medio publico barreras de protección mediante un Servidor VPN las cuales administran los equipos tales como Router (enrutador) y Firewall que hacen posible la creación y disposición Off / On de túneles para que la información viaje encriptada y no sea visualizada por terceros. El esquema que refleja la solución VPN para dos Servidores que administran redes corporativas es el siguiente:

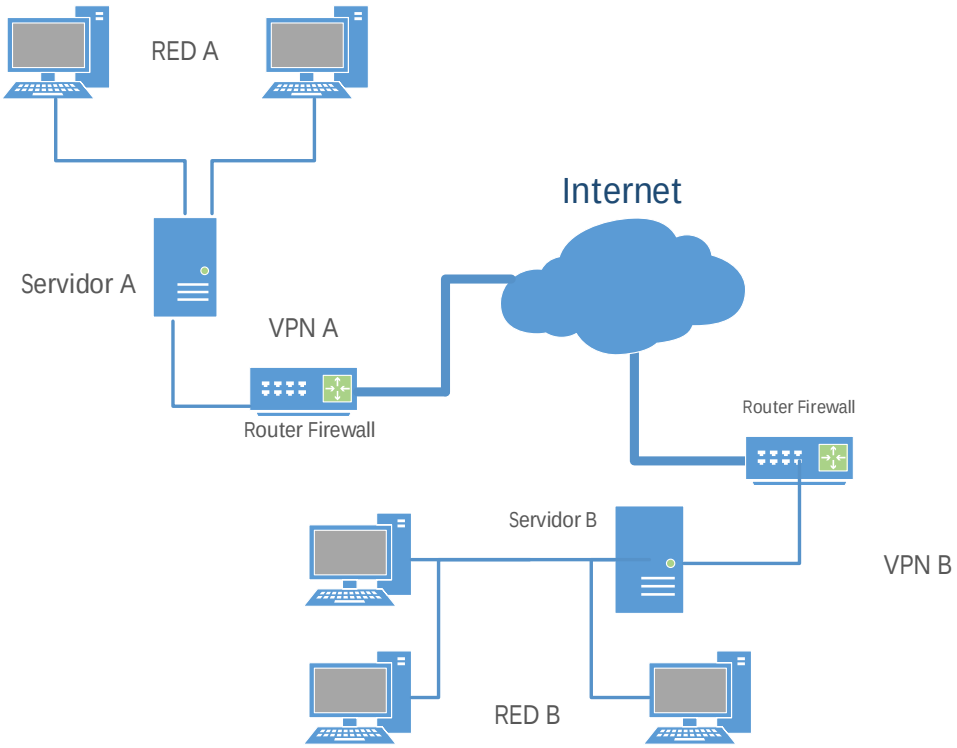

Figura 5. VPN entre dos redes corporativas.
Fuente: los autores

Se puede establecer en la figura anterior que el tramo comprendido a la salida de los equipos terminales que están caracterizados con líneas azules que contienen protocolos de encriptación que contribuyen a la seguridad de la red en el medio en que se está transmitiendo en esta caso la INTERNET.

Dentro de cada red visto con líneas negras no hay peligro que haya accesos no deseados o captura de información ya que el equipo FIREWALL (cortafuego) es el encargado de cerrar el acceso a terceros no autorizados. Las ventajas que se pueden citar luego de la implementación de un enlace VPN entre dos redes corporativas mediante una vía pública son:

- **Alta seguridad:** Al encriptar no solo los datos sino también las direcciones destino, evita que un usuario de la red publica ajeno al autorizado para el manejo de la información capture o lea los datos que están siendo enviados. La información viaja indescriptible entonces no es posible la captura de los datos y la impostación de usuarios.
- **Distintos Niveles de Seguridad:** Según las necesidades, se puede trabajar con claves pre-configuradas o con certificados de llaves para la autentificación de los extremos.

2.2.6 Tipos de VPN

2.2.6.1 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.

2.2.6.2 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.

2.2.6.3 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.

2.2.7 Modelo OSI

El modelo OSI lo desarrolló allá por 1984 la organización ISO (International Organization for Standarization). Este estándar perseguía el ambicioso objetivo de conseguir interconectar sistema de procedencia distinta para que esto pudieran intercambiar información sin ningún tipo de impedimentos debido a los protocolos con los que estos operaban de forma propia según su fabricante.

El modelo OSI está conformado por 7 capas o niveles de abstracción. Cada uno de estos niveles tendrá sus propias funciones para que en conjunto sean capaces de poder alcanzar su objetivo final. Precisamente esta separación en niveles hace

posible la intercomunicación de protocolos distintos al concentrar funciones específicas en cada nivel de operación.

Figura 6. Modelo OSI
Fuente: los autores

2.2.7.1 Niveles OSI orientados a redes

Estos niveles se encargan de gestionar el apartado físico de la conexión, como el establecimiento de la comunicación, el enrutamiento de ésta y el envío

- **Capa 1: Física**

Este nivel se encarga directamente de los elementos físicos de la conexión. Gestiona los procedimientos a nivel electrónico para que la cadena de bits de información viaje desde el transmisor al receptor sin alteración alguna.

Define el medio físico de transmisión: cables de pares trenzados, cable coaxial, ondas y fibra óptica. Maneja las señales eléctricas y transmite el flujo de bits. Define las características de los materiales, como conectores y niveles de tensión

Algunas normas relativas a este nivel son: ISO 2110, EIA-232, V.35, X.24, V24, V.28

- **Capa 2: Enlace de datos**

Este nivel se encarga de proporcionar los medios funcionales para establecer la comunicación de los elementos físicos. Se ocupa del direccionamiento físico de los datos, el acceso al medio y especialmente de la detección de errores en la transmisión. Esta capa construye las tramas de bits con la información y además otros elementos para controlar que la transmisión se haga de forma correcta. El elemento típico que realiza las funciones de esta capa es el switch o también el router, que se encarga de recibir y enviar datos desde un transmisor a un receptor. Los protocolos más conocidos de este enlace son los IEEE 802 para las conexiones LAN y IEEE 802.11 para las conexiones WiFi.

- **Capa 3: Red**

Esta capa se encarga de la identificación del enrutamiento entre dos o más redes conectadas. Este nivel hará que los datos puedan llegar desde el transmisor al receptor siendo capaz de hacer las conmutaciones y encaminamientos necesarios para que el mensaje llegue. Debido a esto es necesario que esta capa conozca la topología de la red en la que opera. El protocolo más conocido que se encarga de esto es el IP. También encontramos otros como IPX, APPLETALK o ISO 9542.

- **Capa 4: Transporte**

Este nivel se encarga de realizar el transporte de los datos que se encuentran dentro del paquete de transmisión desde el origen al destino. Esto se realiza de forma independiente al tipo de red que haya detectado el nivel inferior. La unidad de información o PDU antes vista, también le llamamos Datagrama si trabaja con el protocolo UPD orientado al envío sin conexión, o Segmento, si trabaja con el protocolo TCP orientado a la conexión. Esta capa trabaja con los puertos lógicos como son el 80, 443, etc. Además, es la capa principal en donde se debe proporcionar la calidad suficiente para que la transmisión del mensaje se realice correctamente y con las exigencias del usuario.

- **Capa 5: Sesión**

Mediante este nivel se podrá controlar y mantener activo el enlace entre las máquinas que están transmitiendo información. De esta forma se asegurará que una vez establecida la conexión, esta e mantengas hasta que finalice la transmisión. Se encargará del mapeo de la dirección de sesión que introduce el usuario para pasarlas a direcciones de transporte con las que trabajan los niveles inferiores.

- **Capa 6: Presentación**

Como su propio nombre intuye, esta capa se encarga de la representación de la información transmitida. Asegurará que los datos que nos llegan a los usuarios sean entendibles a pesar de los distintos protocolos utilizados tanto en un receptor como en un transmisor. Traducen una cadena de caracteres en algo entendible, por así decirlo.
En esta capa no se trabaja con direccionamiento de mensajes ni enlaces, sino que es la encargada de trabajar con el contenido útil que nosotros queremos ver.

- **Capa 7: Aplicación**

Este es el último nivel, y en encargado de permitir a los usuarios ejecutar acciones y comandos en sus propias aplicaciones como por ejemplo un botón para enviar un email o un programa para enviar archivos mediante FTP. Permite también la comunicación entre el resto de capas inferiores. Un ejemplo de la capa de aplicación puede ser el protocolo SMTP para el envío de correos electrónicos, programas de transmisión de ficheros por FTP, etc.

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.(ver figura 7)

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.

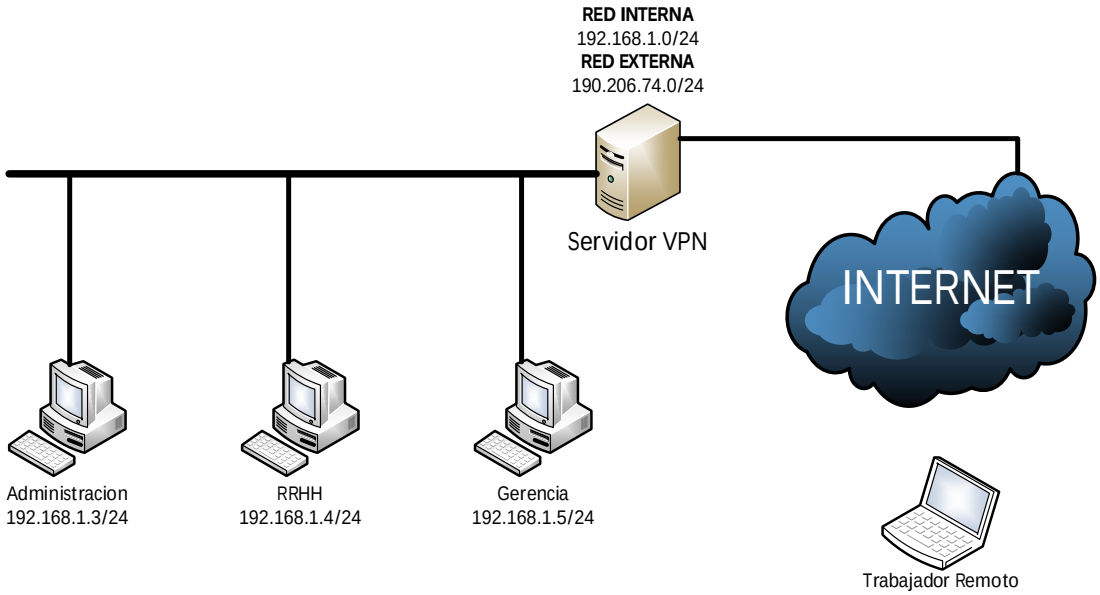

Figura 7. Modelo para Windows Server 2012

- **Fuente:** los autores

2.2.9 VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

2.2.10 VPN punto a punto

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

2.2.11 Tunneling.

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

2.2.12 PDU Unidades de Datos de Protocolo.

Se utiliza para el intercambio entre unidades parejas, dentro de una capa del modelo OSI. Existen dos clases de PDUs: PDU de datos, que contiene los datos del

usuario final (en el caso de la capa de aplicación) o la PDU del nivel inmediatamente superior. PDU de control, que sirven para gobernar el comportamiento completo del protocolo en sus funciones de establecimiento y ruptura de la conexión, control de flujo, control de errores, etc. No contienen información alguna proveniente del nivel N+1. Cada capa del modelo OSI en el origen debe comunicarse con capa igual en el lugar destino. Esta forma de comunicación se conoce como comunicación de para-par. Durante este proceso, cada protocolo de capa intercambia información en lo que se conoce como unidades de datos de protocolo (PDU), entre capas iguales.

Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino.

2.2.13 IPsec (Abreviatura de Internet Protocol security).

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

2.2.14 PPTP (Point to Point Tunneling Protocol).

Es un protocolo desarrollado para implementar redes privadas virtuales o VPN. Point-To-Point Tunneling Protocol (PPTP) permite el seguro intercambio de datos de un cliente a un servidor formando una Red Privada Virtual (VPN por el anglicismo Virtual Private Network), basado en una red de trabajo vía TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET. Esta habilidad permitirá a una compañía usar Internet para establecer una red privada virtual (VPN) sin el gasto de una línea alquilada. Esta tecnología que hace posible el PPTP es una extensión del acceso remoto del PPP (point-to-point-protocol. La tecnología PPTP encapsula los paquetes ppp en Communications, 3com / Primary Access, ECI Telematics y US Robotics. Datagramas IP para su transmisión bajo redes basadas en TCP/IP. PPTP y VPN: El Protocolo Point-To-Point Tunneling Protocol viene incluido con WindowsNT 4.0 Server y Workstation.

Los PC’s que tienen corriendo dentro de ellos este protocolo pueden usarlo para conectar con toda seguridad a una red privada como un cliente de acceso remoto usando una red pública como Internet. Una característica importante en el uso del PPTP es su soporte para VPN. La mejor parte de esta característica es que soporta VPNs sobre public-switched telephone networks (PSTNs) que son los comúnmente llamados accesos telefónicos a redes.

Usando PPTP una compañía puede reducir en un gran porcentaje el coste de distribución de una red extensa, la solución del acceso remoto para usuarios en continuo desplazamiento porque proporciona seguridad y comunicaciones cifradas sobre estructuras de área de trabajo existentes como PSTNs o Internet.

2.2.16 L2TP (Layer 2 Tunneling Protocol)

Fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661). L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM. Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo: Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel. Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente. L2TP no cifra en principio

el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos. A pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos. A causa de estos inconvenientes, el grupo del IETF que trabaja en el desarrollo de PPP consideró la forma de solventarlos. Ante la opción de crear un nuevo conjunto de protocolos para L2TP del mismo estilo de los que se están realizando para IPSec, y dado la duplicación del trabajo respecto al propio grupo de desarrollo de IPSec que supondría, se tomó la decisión de utilizar los propios protocolos IPSec para proteger los datos que viajan por un túnel L2TP. 39 L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

2.2.17 Radius (Remote Authentication Dial-In User Server).

Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones. Cuando se realiza la conexión con un ISP mediante módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red o Network Access Server (NAS)) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS.

El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una

dirección IP, y otros parámetros como L2TP, etc. Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos. RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores de Acceso a la Red(NAS), más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes).

2.3 Definición de términos básicos

Banda ancha: Capacidad para transmitir datos un canal compartido.
configuración de cables, computadoras y otros periféricos.

Dirección IP: Número exclusivo que utilizan los dispositivos a fin de identificarse y comunicarse entre ellos en una red de computadoras utilizando el estándar de protocolo de Internet (IP).
enviar los datos.

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. Es un dispositivo de networking que guarda un registro de las rutas a destinos particulares de la red.

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.

SSTP: Secure Socket Tunneling es un protocolo VPN creado y desarrollado por Microsoft que ofrece un túnel cifrado mediante el protocolo SSL/TLS, es una mejora actualizada del ya existente PPTP o Point to Point Tunneling Protocol. Se considera una de los protocolos mas seguros para tunelizacion VPN.

Tabla de Enrutamiento: Tabla almacenada en la memoria de un router o algún

Topología Física: La topología física de una red hace referencia a la

Túnel: Se conoce como túnel o tunneling a la técnica que consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel de información dentro de una red de computadoras.

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.

Frame Relay: es una tecnología de conmutación rápida de paquetes de datos, llamados tramas, que puede utilizarse como un protocolo de transporte y acceso en redes públicas o privadas, a fin de brindar servicios de telecomunicaciones. Frame Relay ha sido especialmente adaptado para velocidades de hasta 2 Mbps, aunque nada le impide superarlas. La tecnología Frame Relay está basada en el concepto de uso de Circuitos Virtuales (Virtual Circuit). Un Circuito Virtual son dos vías, definidas por software, de un trayecto entre dos puertos que actúa como una línea privada en la red.

Escritorio remoto: Tecnología que permite a un usuario trabajar en una computadora a través de su escritorio grafico desde otro dispositivo terminal ubicado en otro lugar.

Firewall ASA: Es un dispositivo de alto rendimiento creado por la compañía CISCO SYSTEM, que proporciona seguridad web sólida en sitio o en la nube, y completa protección de amenazas y malware avanzado con acceso remoto sumamente seguro.

CAPÍTULO III
MARCO METODOLÓGICO

Para Arias, F. (2012, pág. 110): “La metodología del proyecto incluye el tipo o tipos de investigación, las técnicas y los instrumentos que fueron utilizados para llevar a cabo la indagación. Es el “cómo” se realizó el estudio para responder al problema planteado. Es así, como se da a conocer entonces en el presente capítulo, el abordaje metodológico llevado a cabo para cubrir el problema planteado de como Proponer el diseño de la red privada virtual mediante acceso remoto para la empresa Radio América. En este orden de ideas, el capítulo comprende todo lo referente al tipo, nivel y diseño de la investigación, así como técnicas e instrumentos de recolección de datos. La modalidad del presente proyecto es especial.

3.1. Tipo de Investigación

La investigación descriptiva, para Arias, F. (2012, pág. 24), “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”. Siendo el objetivo de la presente investigación.

3.2. Diseño de la Investigación

El estudio se sustentó en una investigación documental y de campo, ya que se estudió un problema con el propósito de ampliarlo con apoyo, principalmente de trabajos previos, es decir, en la evolución histórica del objeto en estudio. Arias, F. (2012, pág. 27), plantea la investigación documental de la siguiente forma:

> Documental: "La investigación documental es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas.

> Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos".

3.3. 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.

3.4. Técnica e Instrumentos de Investigación

Según Arias, F. (2012, pág. 67), “Se entenderá por técnica de investigación, el procedimiento o forma particular de obtener datos o información.”.

Las técnicas de recolección de datos utilizadas en la presente investigación fueron la observación directa y Recolección de datos.

Cabe destacar que el uso de este instrumento responde a lo planteado por Arias, F. (2012, pág. 68), quien define que: “Un instrumento de recolección de datos es

cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información.”.

3.4.1. Técnicas empleadas

3.4.1.1. Revisión Documental

La revisión documental es hacer una recopilación de información sobre textos e investigaciones generados por otros investigadores que tienen relación directa o indirecta con la problemática que es razón de estudio. Hurtado (2007) define este concepto como:

> “… es una técnica en la cual se recurre a información escrita, ya sea bajo la toma de datos que pueden haber sido producto de mediciones hechas por otros como texto en sí mismo constituyen los eventos de estudio” (p.427).

3.4.1.2. Observación directa

La observación directa es el proceso en el cual el investigador recolecta datos directamente desde el medio ambiente del fenómeno a estudiar, por otro lado Hurtado (2007) la define como:"… un proceso de atención, recopilación, selección y registro de información para el cual el investigador se apoya en sus sentidos” (p.459).

3.4.3. Instrumentos empleados

3.4.3.1. Instrumento de registro

Permite poseer un soporte de la información en periodos de tiempo relativamente largos de modo que el investigador pueda recuperar la información cuando lo necesite. En el presente trabajo se utilizó lista de cotejos, tablas de direccionamiento IP, topologías de red.

3.4.3.2. Análisis de observación técnicamente asistida

Principalmente se contara con el empleo de un cuarto de servidores en donde se concentra todos los datos de la organización y en donde se presente las experiencias del investigador con el fenómeno a estudiar. En el actual trabajo contamos con herramientas de simulación como Packet Tracer y Visio Office para

simular la Red Privada Virtual y el OS Windows Server en donde se realizara el diseño de la VPN.

3.5. Población y Muestra

La población es un conjunto de individuos de la misma clase, limitada por el estudio, enfocado en desarrollo del proyecto la población estudiada es el departamento de RRHH de la empresa entre los demás departamentos que son administración, Recursos humanos,. Arias, F. (2012, pág. 81) define este concepto de la siguiente manera:

"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.

… La muestra es un subconjunto representativo y finito que se extrae de la población accesible"

Por consiguiente la muestra nos indica s el grupo de individuos que se toma de la población como lo es un computador en el cual un empleado va acceder de manera remota.

3.6. Fases de la Investigación

3.6.1. Fase I: "Diagnostico de la situación actual de la red corporativa de Radio América."

En esta fase del trabajo de grado se realizará la inspección y diagnóstico del área destinada al control, resguardo e interacción de la información que será accesible mediante el recurso asociado a la plataforma tecnológica de Windows Server 2012

.

3.6.2 Fase II: "Análisis de las alternativas para acceder de manera remota y segura a la red interna"

De la fase I se tomara el diagnóstico y toda la documentación investigada para poder seleccionar todas las opciones de trabajo conjunto a los dispositivos involucrados que sean aplicables al diseño del acceso remoto. Aun así se deben

identificar todos los parámetros necesarios mediante un cuadro comparativo para continuar con el desarrollo del proyecto, y de esta manera se puede minimizar los gastos operativos. Entre los parámetros se indagara:

- Servidor de dominio.
- Marca y modelo de firewall.
- Topología de red

3.6.3. Fase III: "Diseño del sistema de la red privada virtual (VPN) para dar conectividad remota de manera segura a los departamentos de recursos humanos y administración.".

En esta fase se realizara el diseño para una red privada virtual (VPN), ya habiendo identificado los parámetros y dispositivo a utilizar es importante realizar la conectividad de manera remota a los departamentos de recursos humanos y administración, la cual estará basada en un modelo de cliente servidor, que recopilara la información del software y hardware del diseño.

3.6.4. Fase IV: "Realizar un estudio de factibilidad económica, operativa, legal y técnica".

En la siguiente fase requiere un estudio sobre la disponibilidad de los recursos necesario para llevar a cabo el proyecto como lo es la factibilidad económica el cual se basa en el financiamiento de la empresa Radio América para el desarrollo de software que suministre mayor seguridad y velocidad de conexión. La factibilidad ambiental es un estudio que busca identificar, cuantificar y valorar los distintos impactos del proyecto sobre las especies vivas y especies físicas del entorno a corto y a largo plazo, este factor no aplica en este proyecto de investigación. La Factibilidad Legal estudia los requerimientos legales del Proyecto para su operación y aprobación. Como también las licencias para el software a emplearse en la implantación de un sistema informático de manera auténtica, con la finalidad de no tener inconvenientes legales a futuro. Factibilidad operativa se refiere a que debe existir el personal

capacitado requerido para darle continuidad al proyecto y así mismo, deben existir usuarios finales como lo son los empleados dispuestos a emplear el acceso remoto mediante la red virtual privada. Factibilidad tiempo indica el cumplimiento de los plazos entre lo planificado y la realidad en donde se desenvuelve el proyecto. Factibilidad técnica Indica si se dispone de los conocimientos y habilidades en el manejo métodos, procedimientos y funciones requeridas para el desarrollo e implantación del proyecto. Factibilidad de social consiste en la evaluación dirigida al bienestar de la sociedad en donde se desenvuelve el proyecto, es decir el impacto social generado en los trabajadores de la empresa en cuanto al desarrollo del acceso remoto.

CAPÍTULO IV

RESULTADOS

4.1. Diagnóstico de la situación actual de la radio

Para esta fase se realiza el estudio del estado de la red iniciando por el cuarto de servidores en donde estará ubicada la conexión física, el cual se encuentra en pleno desarrollo, ya que la empresa aborda cambios en cuanto a las instalaciones e infraestructura. La tabla n°1 muestra la lista de cotejo con los aspectos a observar y los resultados obtenidos de esta observación.

Posteriormente se documenta a través material fotográfico las condiciones de las conexiones a la red de la empresa y la creación de la sala de servidores.

Cabe destacar que no interfiere en el diseño del acceso remoto la habilitación del espacio destinado a la red física conjunto a los servidores, aunque no se apreciaría del todo el proyecto a realizar.

Figura 9. Personal instalando tablero eléctrico cuarto de comunicaciones.
Fuente: los autores

Figura 8. Vista del cuarto de comunicaciones donde se instalara servidor VPN.
Fuente: los autores

Figura 11. Otra vista de cuarto de comunicaciones de la radio.
Fuente: Los autores

Figura 10. Rack de Comunicaciones donde se instalará Servidor VPN
Fuente: los autores

Figura 12. Cuarto actual de comunicaciones
Fuente: los autores

Tabla 1. Lista de cotejo de los aspectos más importantes sobre la sala de servidores

Lista de cotejo de los requerimientos necesarios sobre la sala de servidores	
Espacio Físico	
Espacio Físico de 4X4 m	ü
Conexión de red	ü
Recubrimiento de paredes y baldosas anti polvo	
Techo falso	ü
Acceso controlado	ü
Rack Bastidor de 2, 10 m de aluminio	ü
Control de climatización y humedad	
Aire acondicionado de 12000 BTU	ü
Sensores de temperatura y humedad	
Deshumidificador	ü
Suministro de energía eléctrica	
Varias tomacorrientes	ü
Protectores y UPS	ü
Planta eléctrica	
Control de ruido	
Carcasa de insonoracion	
Transmisión de ruido	ü
Bloque anti-vibraciones	
Control preventivo	
Aspersores	ü
Extintor	ü
Desagües	ü

4.2. Análisis de las alternativas

Mediante a la investigación desarrollada se optó por la selección de un cuadro comparativo como lo muestra la tabla n°2, tomando en cuenta los requerimientos necesarios para escoger la mejor solución a la problemática que presenta la empresa.

Tabla 2. Cuadro comparativo entre el acceso remoto, una red VPN, Firewall ASA, Frame Relay

Escritorio Remoto	**Servidor VPN**	**Firewall ASA**	**Frame Relay**
En general los Sistemas operativos vienen con el paquete de escritorio remoto	Funciona en múltiples dispositivos móviles sin necesidad de descargar una aplicación	El cliente solo puede tener acceso a la red LAN.	Proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada punto a punto.
La experiencia es generalmente lenta y depende de la velocidad de la conexión a Internet.	Si tu servidor VPN está muy lejos, experimentarás mucha latencia a la hora de navegar por la red.	Trabaja en entornos de ultra baja latencia.	Sólo ha sido definido para velocidades de hasta 1,544/2,048 Mbps. Y no garantiza la entrega de los datos.
Bajo costos de implementación	Bajo costos de implementación	Altos costos de implementación	Se reduce las necesidades de “hardware” y el procesamiento simplificado ofrece un menor coste.

Con soporte de conexión simultanea uno a uno.	Con soporte de conexión simultanea para 20 empleados	Soporta múltiples conexiones simultáneamente , y con VPN de 25 a 750 empleados	El límite máximo viene marcado por el tráfico en exceso.

Las VPN y los escritorios remotos no están necesariamente enfrentados entre sí. De hecho, si se usan juntos, brindan mayor seguridad y facilidad a cualquier individuo o compañía. Al usar los dos en conjunto, puede disfrutar de una experiencia RDP muy segura. Al conectarse al Escritorio remoto mediante una VPN, elimina todas las posibilidades de que una entidad externa pueda acceder a su red. Además, las empresas con empleados internos pueden implementar el sistema fácilmente para mantener una mejor seguridad en todos los dominios del negocio. Por otro lado los firewalls serian la opción más recomendada, proporcionan la visibilidad de red, además de protección superior contra amenazas y malware avanzado, y mayor automatización para la configuración redes privadas virtuales (VPN) que proporcionen a los trabajadores remotos y móviles un acceso seguro a los recursos de la compañía o establezca VPN entre partners. Aunque el costo de hardware y actualizaciones del software son elevadas por lo que no es factible para el proyecto en desarrollo.

Sin embargo, convenientemente para el proyecto de investigación la mejor alternativa es el acceso mediante VPN ya que brinda una conexión segura, rápida y eficaz en comparación con el escritorio remoto.

4.3. Topología del sistema de la red privada virtual (VPN) para dar conectividad remota de manera segura a los departamentos de RRHH y administración".

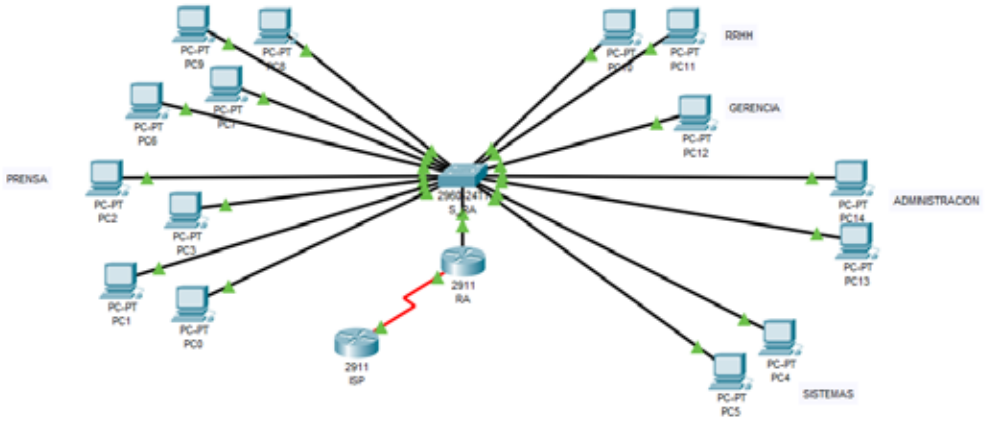

Figura 13. Topología de la red de la empresa diseñado en el programa Packet Tracer.
Fuente: los autores

Tabla 3. Direccionamiento Red General Radio America

ID	Dirección de red	Mascara	Gateway	Descripción
1	192.168.1.20	255.255.255.0	192.168.1.1	Administracion_1
2	192.168.1.21	255.255.255.0	192.168.1.1	Administracion_2
3	192.168.1.30	255.255.255.0	192.168.1.1	Gerencia
4	192.168.40	255.255.255.0	192.168.1.1	RRHH_1
5	192.168.41	255.255.255.0	192.168.1.1	RRHH_2
6	192.168.50	255.255.255.0	192.168.1.1	Sistemas_1
7	192.168.51	255.255.255.0	192.168.1.1	Sistemas_2
8	192.168.1.60	255.255.255.0	192.168.1.1	Prensa_1
9	192.168.1.61	255.255.255.0	192.168.1.1	Prensa_2
10	192.168.1.62	255.255.255.0	192.168.1.1	Prensa_3

11	192.168.1.63	255.255.255.0	192.168.1.1	Prensa_4
13	192.168.1.64	255.255.255.0	192.168.1.1	Prensa_5
14	192.168.1.65	255.255.255.0	192.168.1.1	Prensa_6
15	192.168.66	255.255.255.0	192.168.1.1	Prensa_7
16	192.168.67	255.255.255.0	192.168.1.1	Prensa_8

Tabla 4. Distribución de la red por áreas de Radio America

Área	**Numero de host**
Gerencia	1
Recursos Humanos	2
Sistemas	2
Administración	2
Prensa	8
TOTAL	15

4.4. Pasos para la configuración del Servidor de VPN en Windows Server 2012

Primero se debió iniciar sesión en el servidor a través del Escritorio remoto en el que se instalo la VPN y luego se abrio el **Administrador del servidor** y se hizo click en Agregar roles y características como se puede observar en la figura 14.

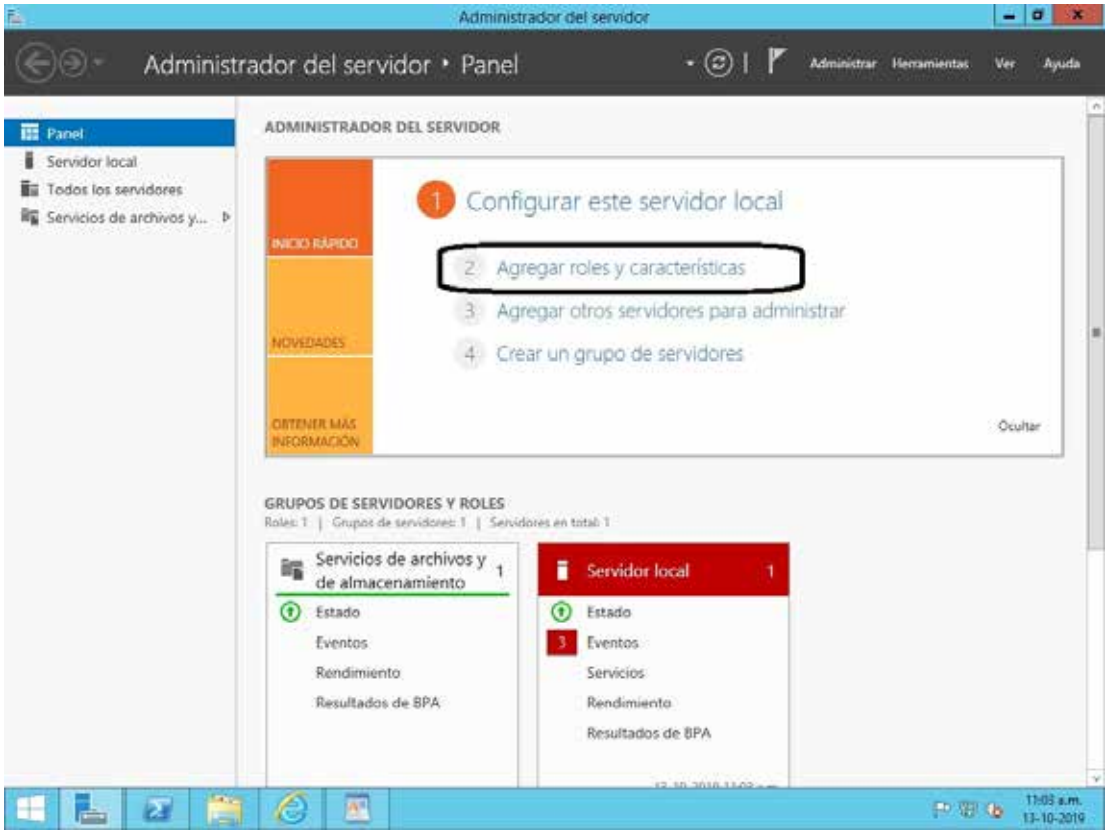

Figura 14. Configuración VPN en Windows Server 2012: Agregando Roles
Fuente: los autores

Se hizo la selección del tipo de **instalación**: Instalación **basada en roles o características** como puede verse en la figura 15, y luego en el campo de selección del servidor, se marco **Seleccionar un servidor del grupo de servidores** tal como se muestra en la figura 16. Se pudo observar el servidor con el nombre de la computadora en el grupo de servidores.

Figura 15. Configuración VPN en Windows Server 2012: Agregando Roles
Fuente: los autores

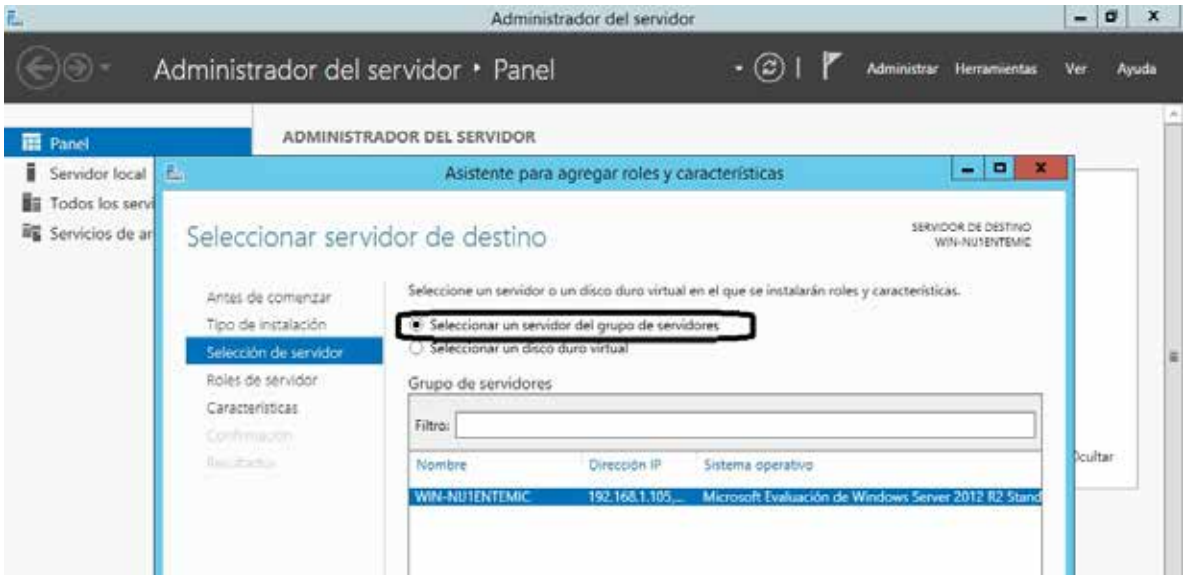

Figura 16. Configuración VPN en Windows Server 2012: Selección servidor de destino
Fuente: los autores

En esta sección se marcó la función " **Acceso remoto** " en **Roles** de servidor. No se realizó algún otro cambio. Figura 17

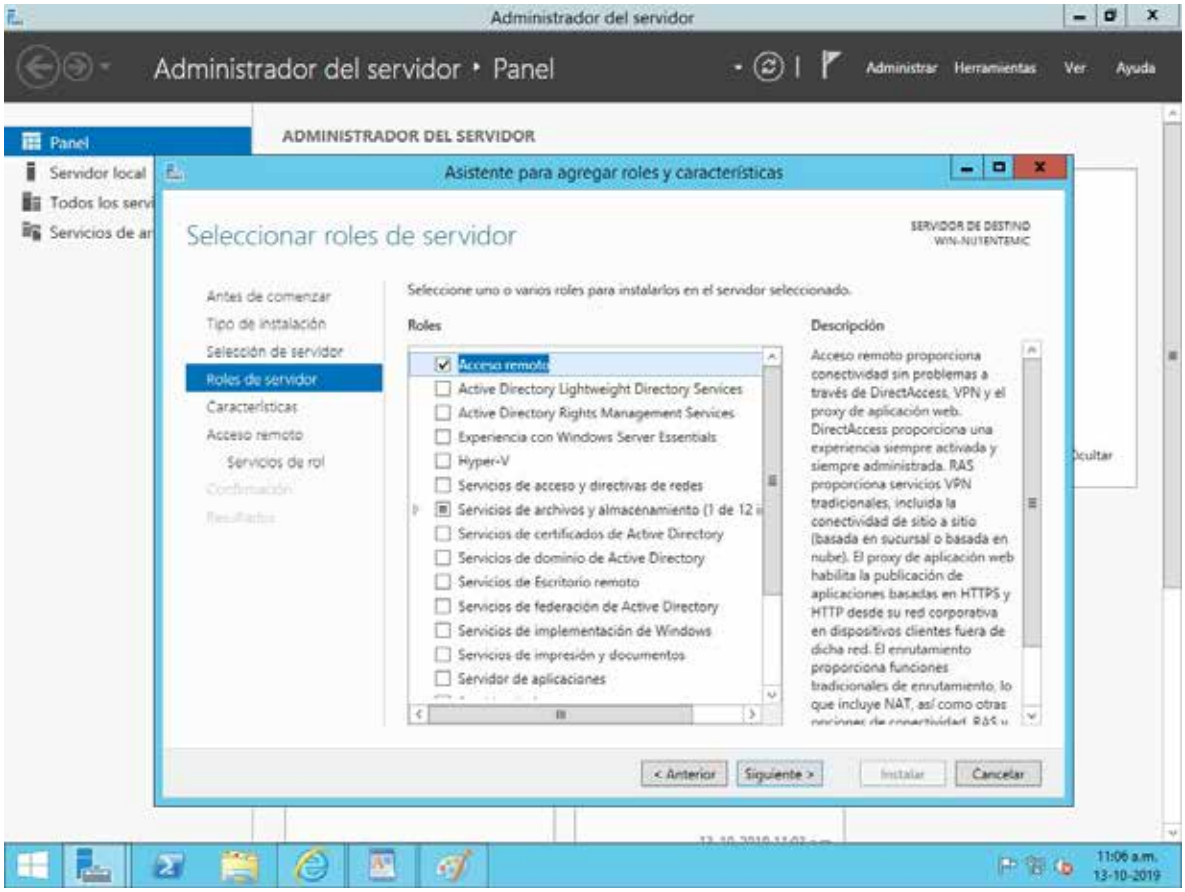

Figura 17. Configuración VPN en Windows Server 2012: Selección del rol para el servidor de destino.

Fuente: los autores

En Servicios de rol, se realizó la selección de los servicios de enrutamiento **DirectAccess y VPN.** Observe la figura 18.

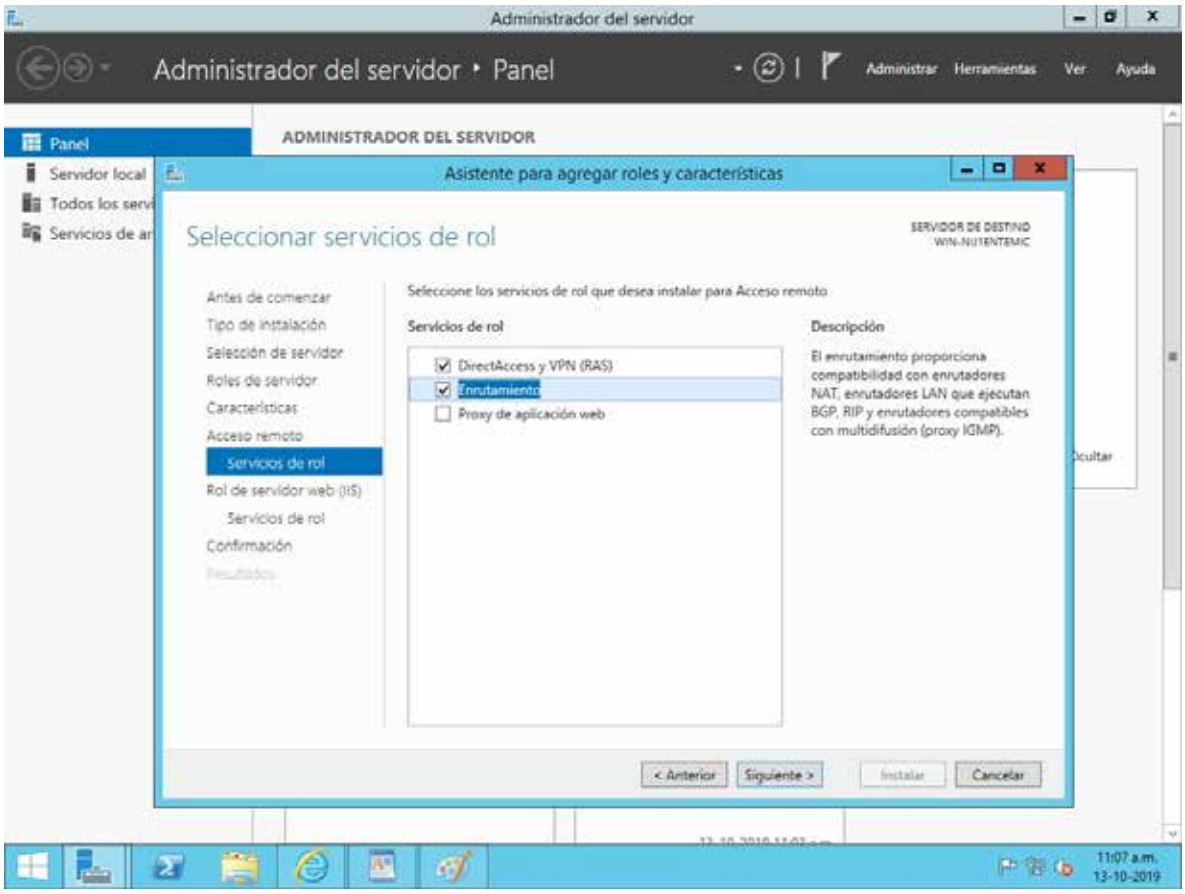

Figura 18. Configuración VPN en Windows Server 2012: Selección de los servicios de rol.

Fuente: los autores

En la página de instalación se marcó la opción de instalar, una vez se completó esta se hizo click en la opción de **Abrir el Asistente de Introducción** como se puede ver en la figura 19.

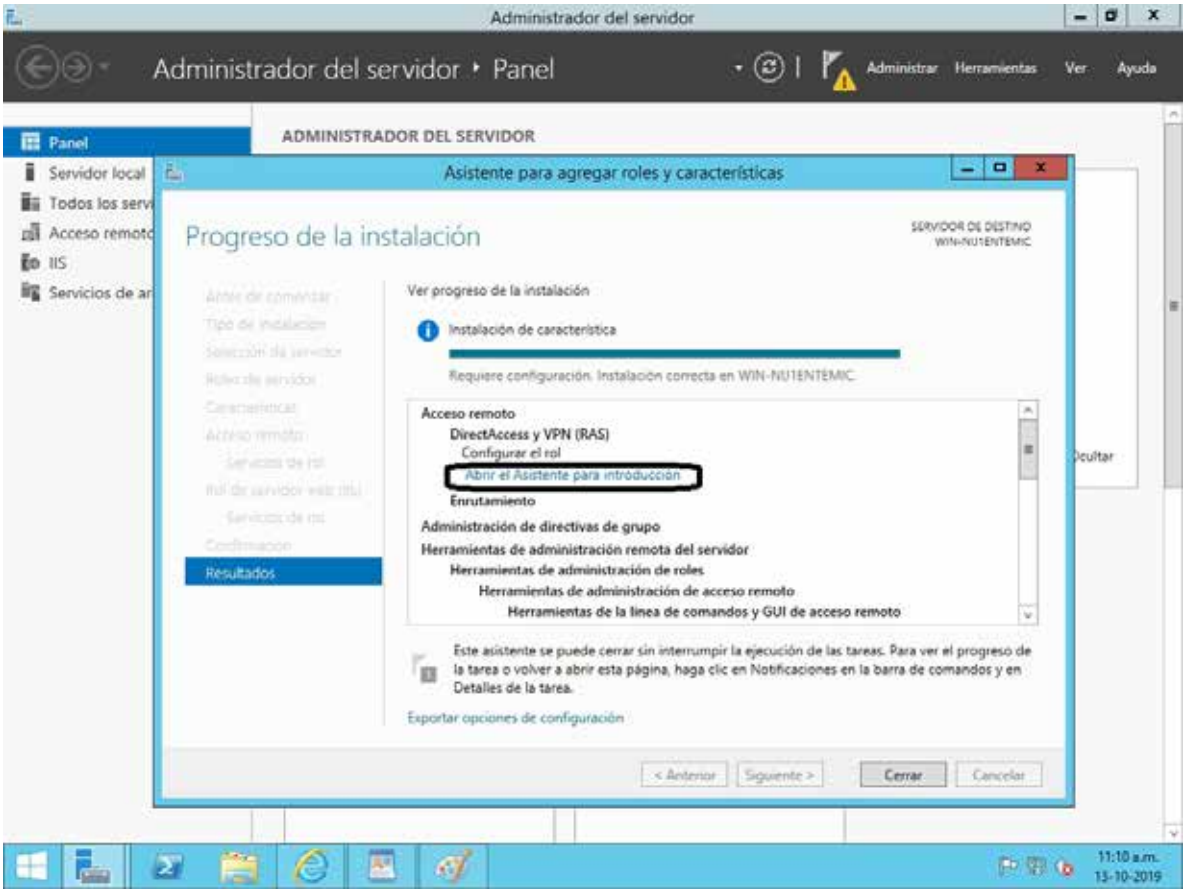

Figura 19. Configuración VPN en Windows Server 2012: Instalación de los roles y selección del asistente para introduccion.
Fuente: los autores

Se pudo observar que se abre la venta del asistente para **Configurar acceso remoto**. En este paso se marco la opción de **Implementar solo VPN** como se observa en la figura 20.

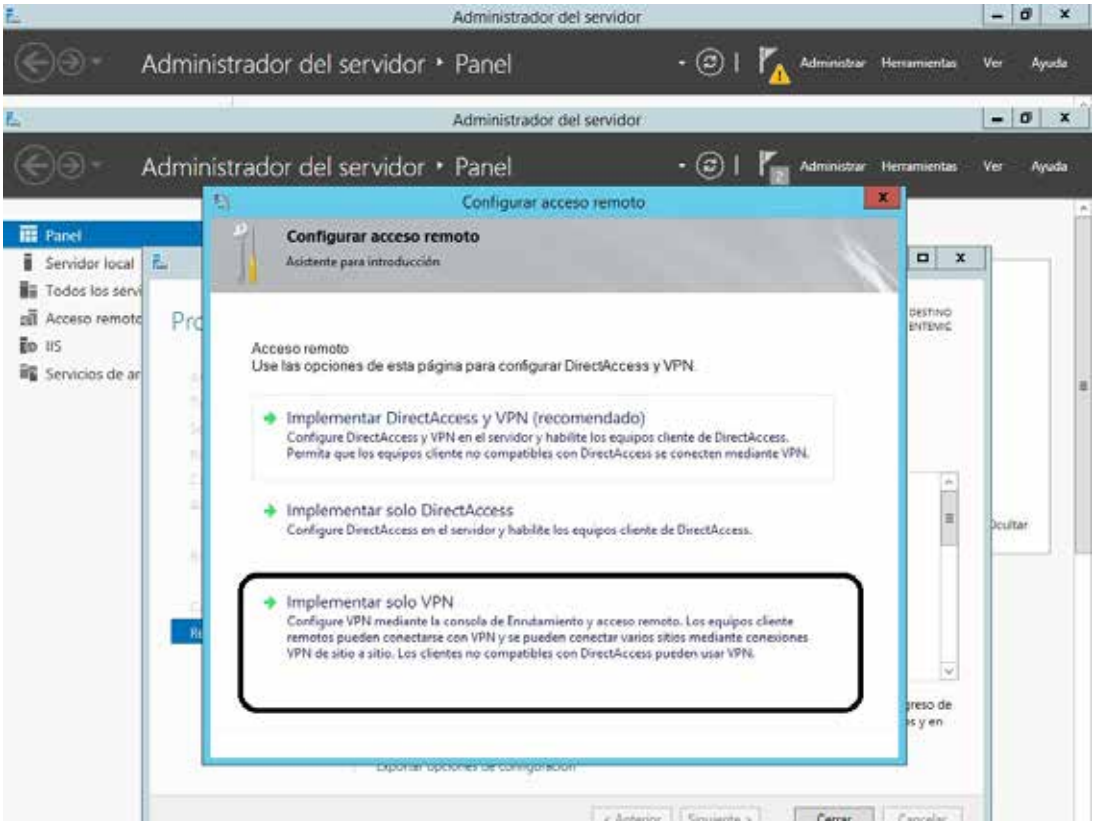

Figura 20. Configuración VPN en Windows Server 2012: Selección del tipo de Acceso remoto a través de únicamente VPN.

· **Fuente:** los autores

Posteriormente se presento una ventana con el titulo de **Enrutamiento y acceso remoto**. Alli se realizó click con el botón derecho del mouse en nuestro servidor como se puede observar en la figura 21.

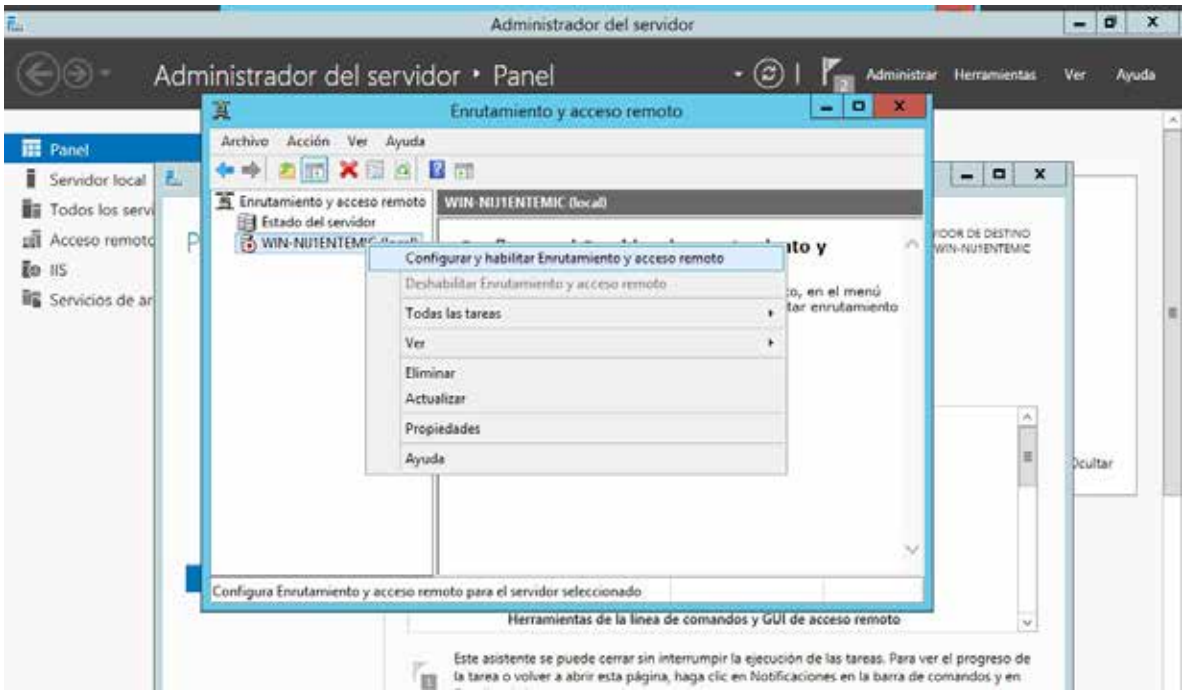

Figura 21. Configuración VPN en Windows Server 2012: Habilitación del enrutamiento y acceso remoto.

· **Fuente:** los autores

En la ventana del **Asistente para la instalación del servidor de enrutamiento y acceso remoto** que apareció se hizo clic en Siguiente. Figura 22

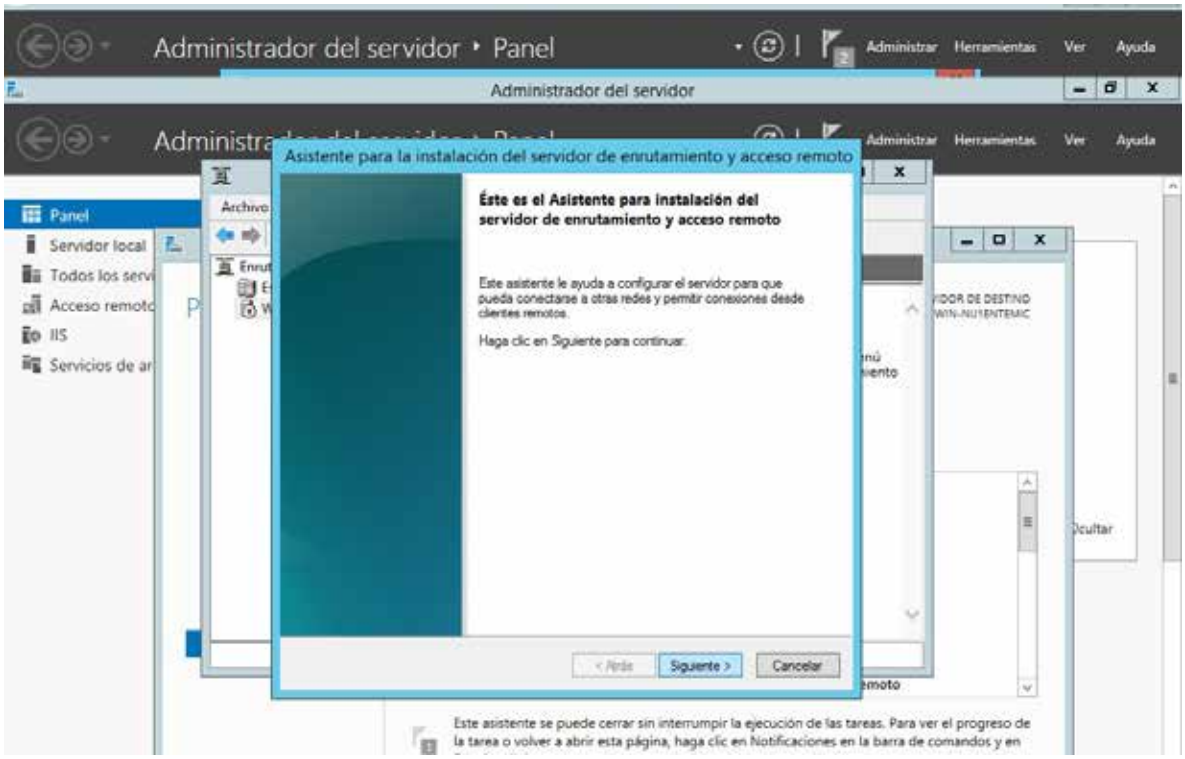

Figura 22. Configuración VPN en Windows Server 2012: Habilitación del enrutamiento y acceso remoto.

· **Fuente:** los autores

En el asistente de configuración, se realizo la seleccion de **Acceso a red privada virtual (VPN) y NAT** ' y luego se hizo click en siguiente. Figura 23.

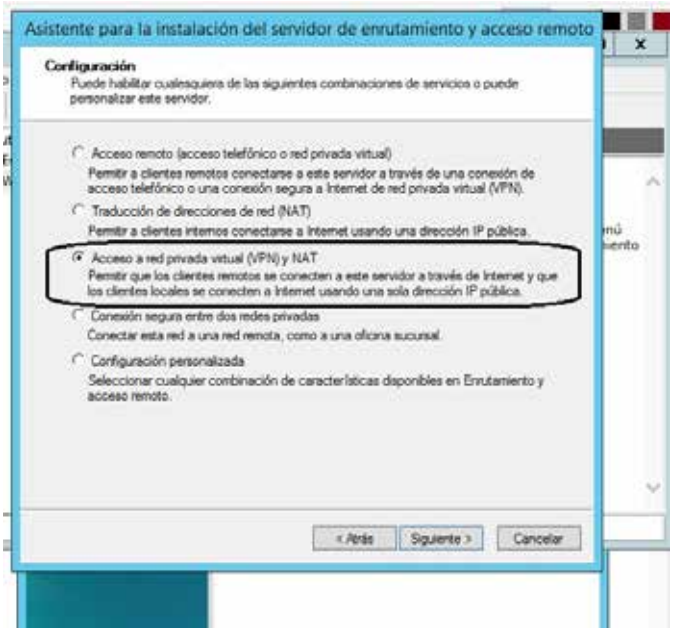

Figura 23. Habilitación del acceso a red privada virtual (VPN) y NAT

· **Fuente:** los autores

En Conexión VPN, se marcó la opción de la **interfaz de red** que tiene una dirección IP pública con **una conexión a Internet adecuada**. Luego se hizo click en siguiente. Figura 24.

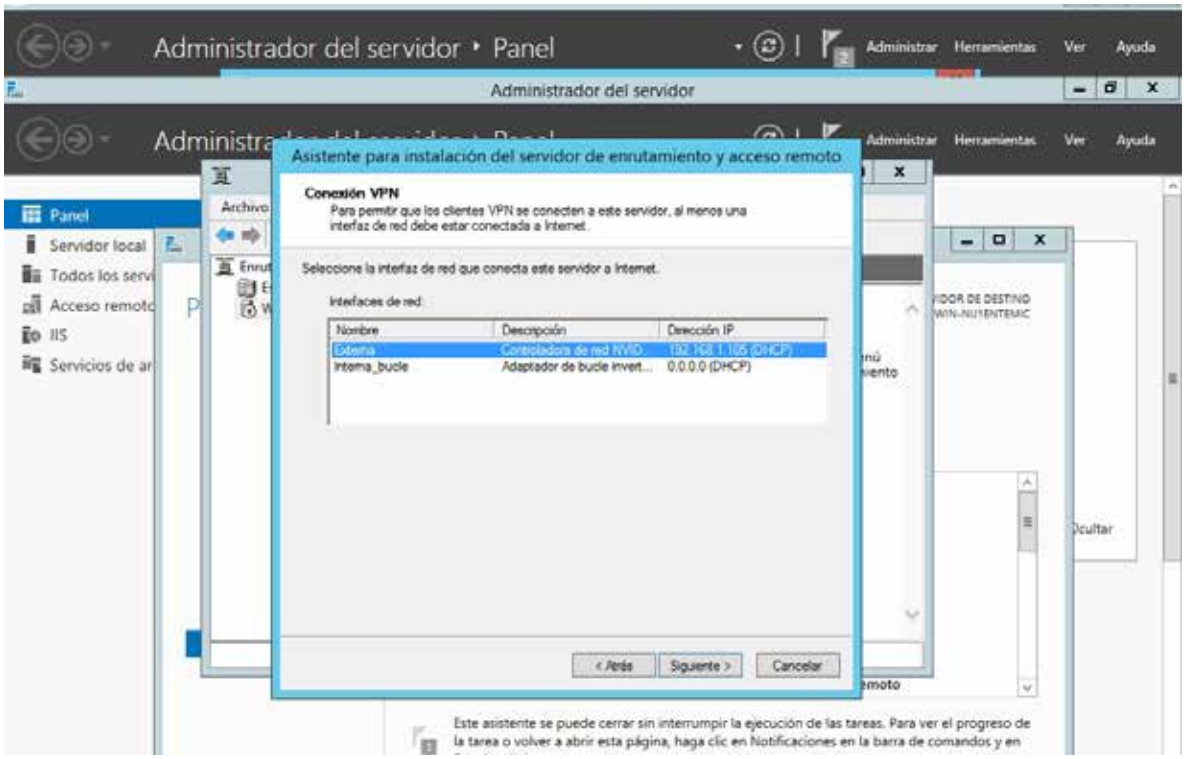

Figura 24. Windows Server 2012: Eleccion red Externa para VPN

- **Fuente:** los autores

En Asignación de dirección IP, se marcó la opción **De un intervalo de direcciones especificado**. Figura 25.

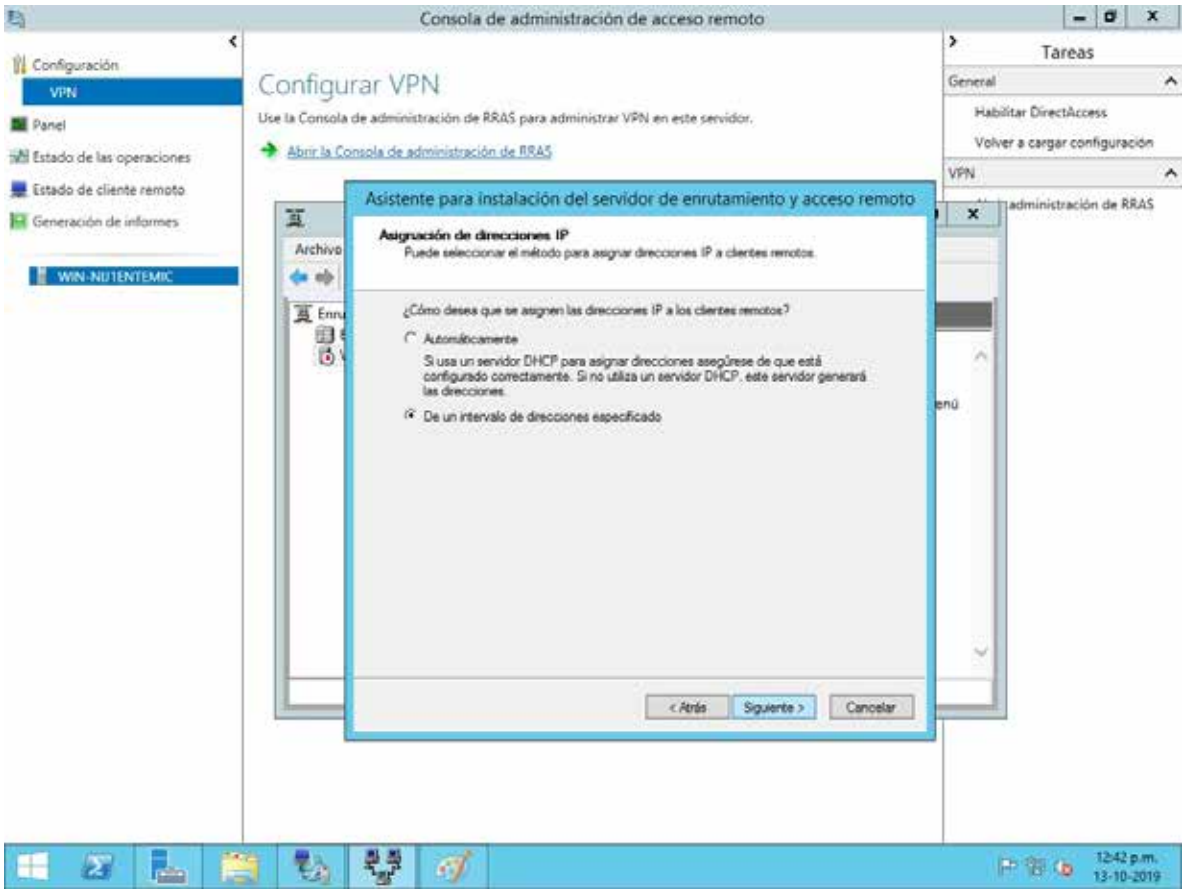

Figura 25. Windows Server 2012: Selección de un intervalo de direcciones.

· **Fuente:** los autores

En la ventana de **Editar intervalo de direcciones IPv4** se agregó **el rango de dirección IP local** (aquí se realizó la verificación de que la dirección IP de inicio fuera la misma que la dirección IP principal de nuestra red interna). Esto se usará para asignar la dirección IP a clientes remotos que se conectan a este servidor VPN. Una vez que haya agregado el rango de IP, haga clic en Siguiente para continuar. Vease figura 26.

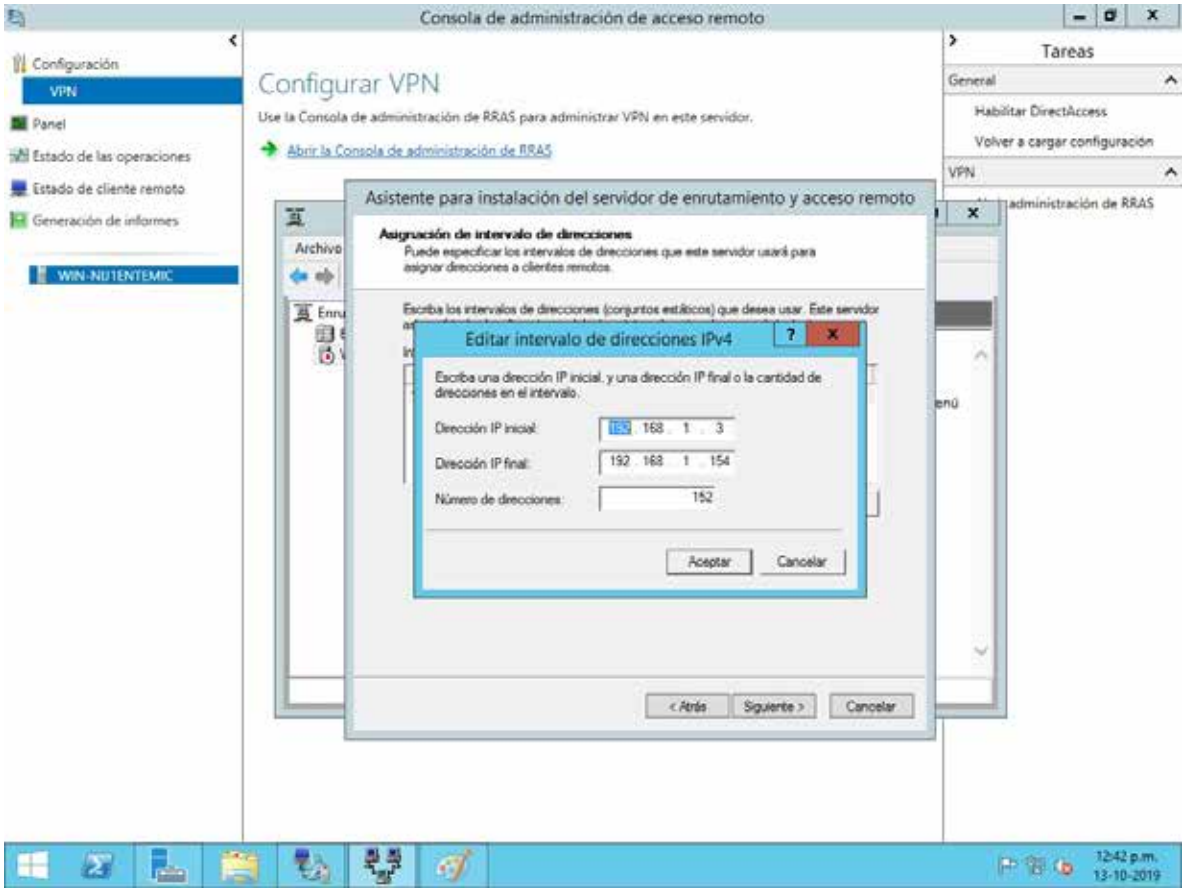

Figura 26. Configuración VPN en Windows Server 2012: Selección de la red externa

· **Fuente:** los autores

En Administración del servidor de acceso remoto múltiple, se realizo marco la opcion de '**No, usar Enrutamiento y acceso remoto para autenticar las solicitudes de conexión**' y se hizo click Siguiente. Vease figura 27.

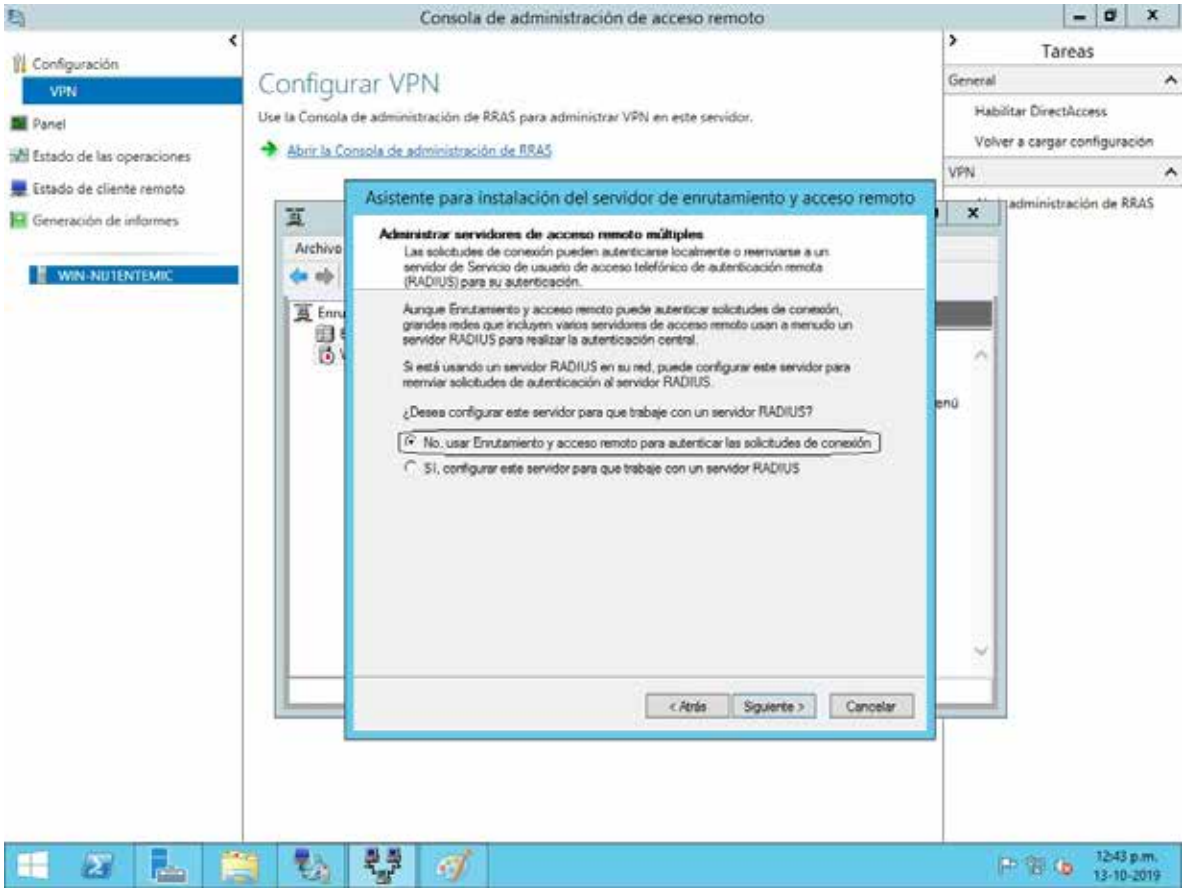

Figura 27. Configuración VPN en Windows Server 2012: Selección de enrutamiento remoto para autenticación de las solicitudes de conexión.

· **Fuente:** los autores

Al completar el asistente se solicitó un mensaje para el agente de retransmisión DHCP, se marco la opcion Aceptar para este mensaje y posteriormente se permitio al **puerto RDP** del servidor en **los servicios y puertos NAT** . Vease figura 28.

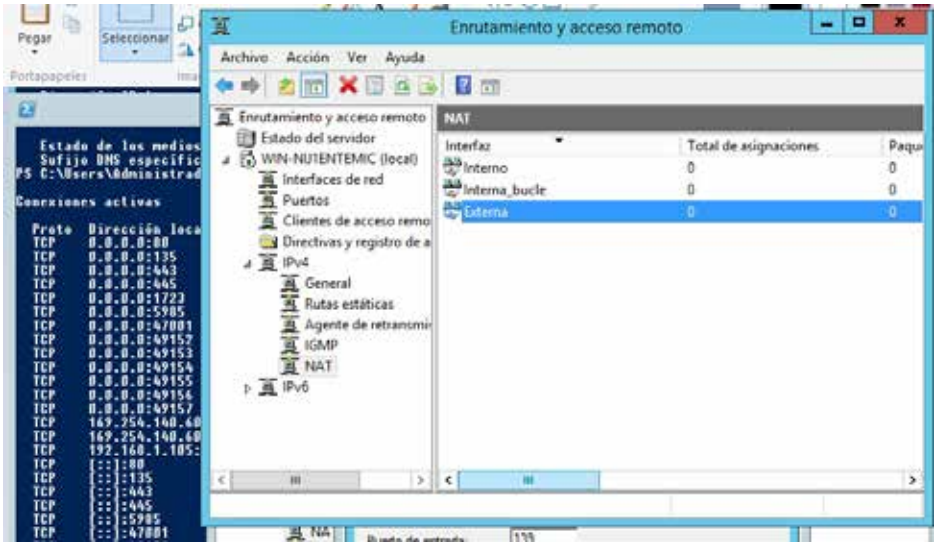

Figura 28. Configuración VPN en Windows Server 2012: Configuracion servicios NAT

· **Fuente:** los autores

En Enrutamiento y acceso remoto se hizo clic en el icono del servidor para expandir las opciones, luego en IPV4 y posteriormente en **NAT.** Una vez allí se hizo click derecho en Red externa, y luego en propiedades, **Servicios y puertos.** Observe la figura 29.

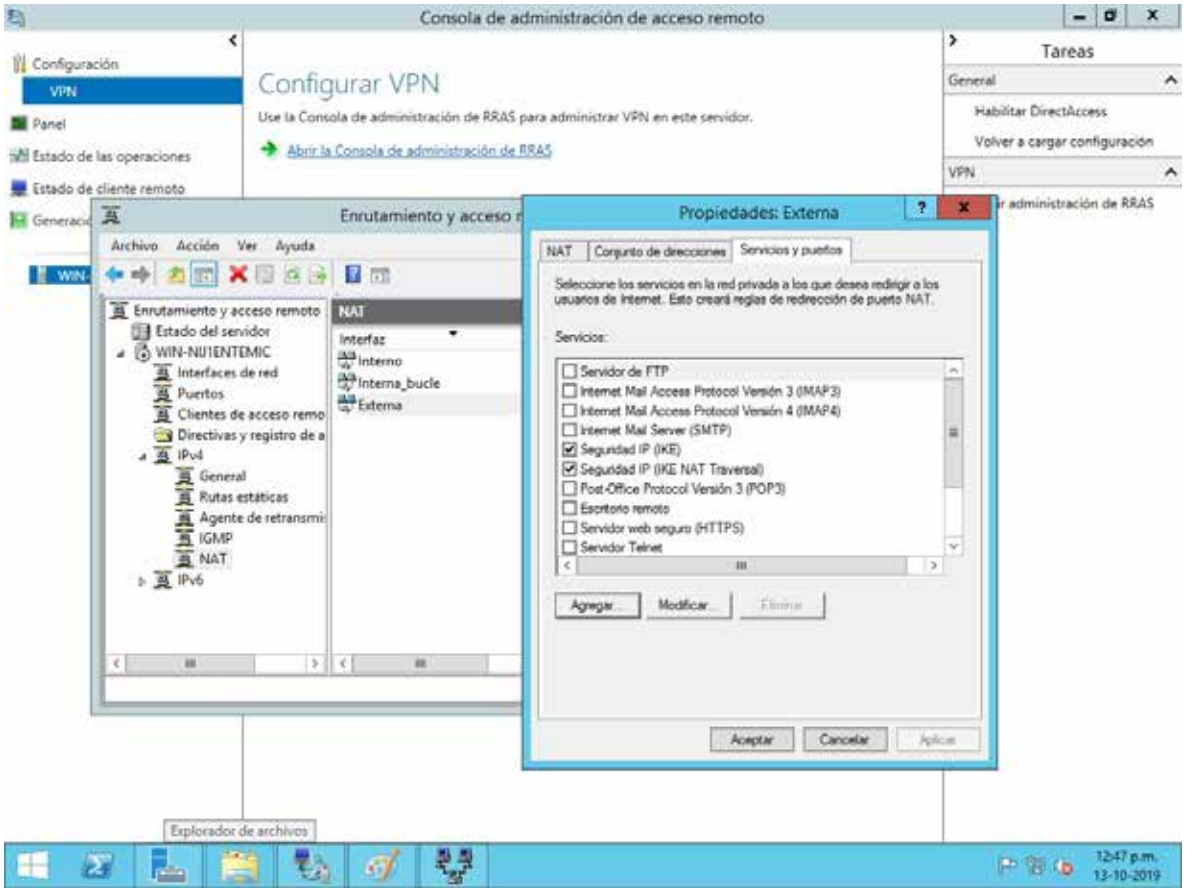

Figura 29. Configuración VPN en Windows Server 2012: Selección de la red externa

- **Fuente:** los autores

En la ventana de **Editar Servicio** se ingresó la descripción de este servicio y luego el **puerto RDP** y **la dirección IP** del VPS. Ver figura 30.

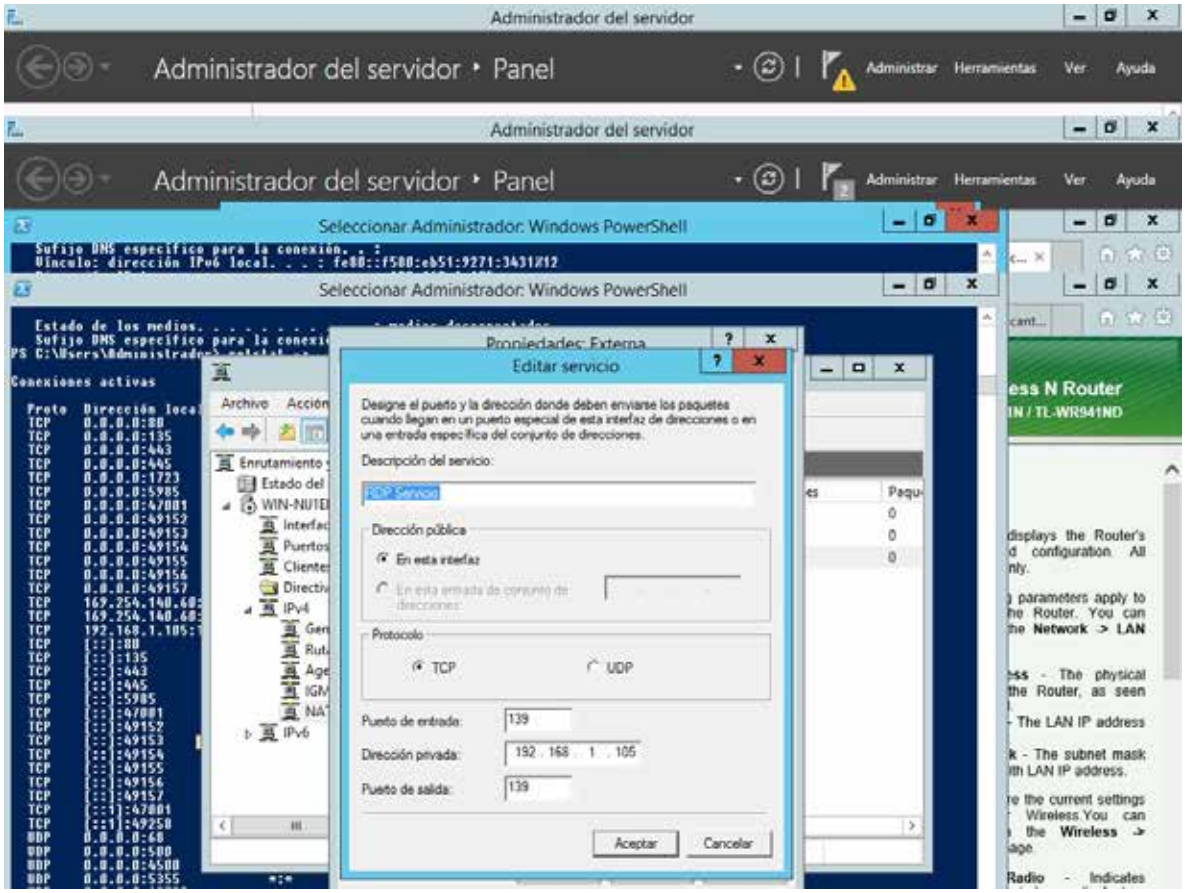

Figura 30. Configuración VPN en Windows Server 2012: Configurando el Servicio RDP

· **Fuente:** los autores

En la siguiente ventana se modificó la configuración del usuario para hacer la conexión VPN desde el cliente o máquina remota.

En **Propiedades de Administrador** se seleccionó la pestaña **Acceso** telefónico, y luego se marcó **Permitir acceso** en la opción Permiso de acceso a la red. Ver figura 32.

Con esto finalizamos la configuración en el servidor VPN el cual quedo habilitado para conexiones cliente / remotas.

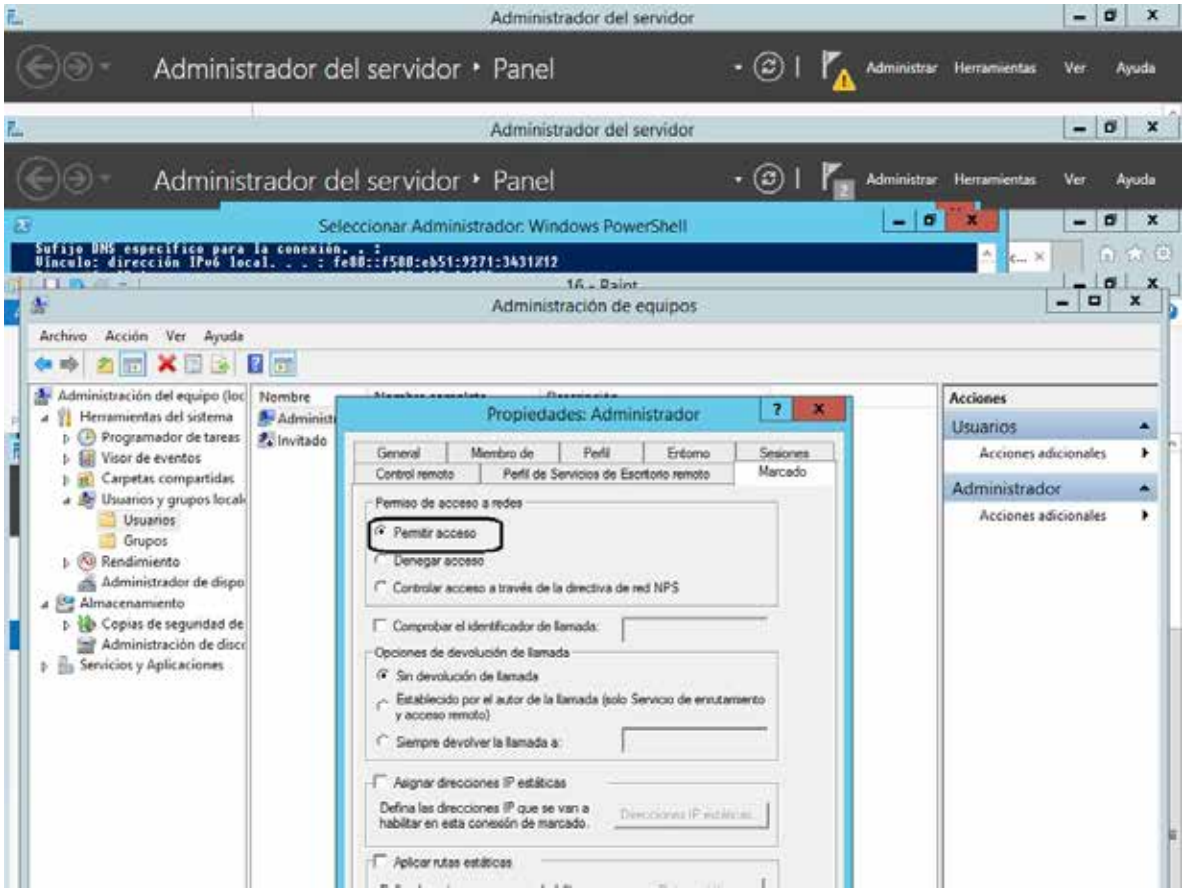

Figura 32. Configuración VPN en Windows Server 2012: Estableciendo permisos de Acceso al usuario Administrador.

Fuente: los autores

- En Consola de Windows se pudo verificar la conectividad junto con las direcciones IPs asignadas a cada uno de los adaptadores, incluyendo el de VPN. Ver figura 33.

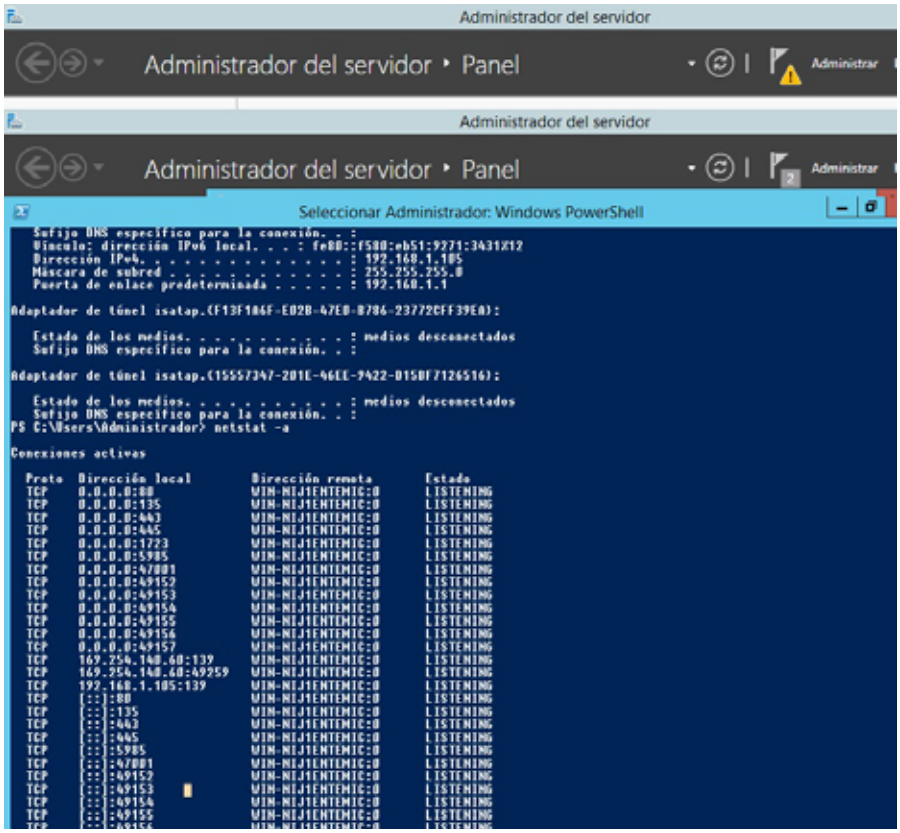

Figura 33. Configuración VPN en Windows Server 2012: Probando en consola el comando netstat –a para observar puertos habilitados y direcciones ip en el servidor.

- **Fuente:** los autores

4.5. Pasos a seguir para la configuración máquina cliente para la conexión al servidor VPN.

La siguiente explicación está basada en Windows 10 pero es aplicable a otros sistemas operativos, entre ellos, Windows 8,7,Vista y XP.

Se realizó el ingreso a Panel de Control y luego al Centro de redes y recursos compartidos del sistema local. Se hizo click en **Configurar una nueva conexión o red**. Vease figura 34.

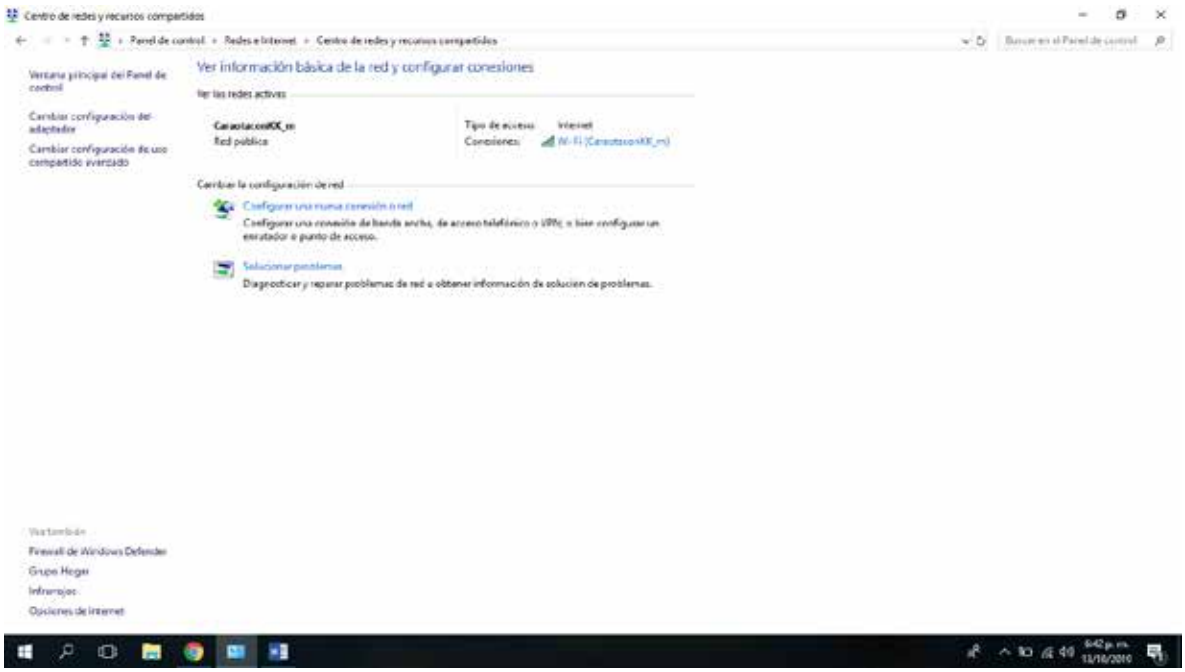

Figura 34. . Configuración máquina cliente para la conexion al servidor VPN en Windows 10: Configuracion de una nueva conexión de red.

Fuente: **los autores**

En la ventana de la figura 35 se marcó la opción de **Conectar a un lugar de trabajo**

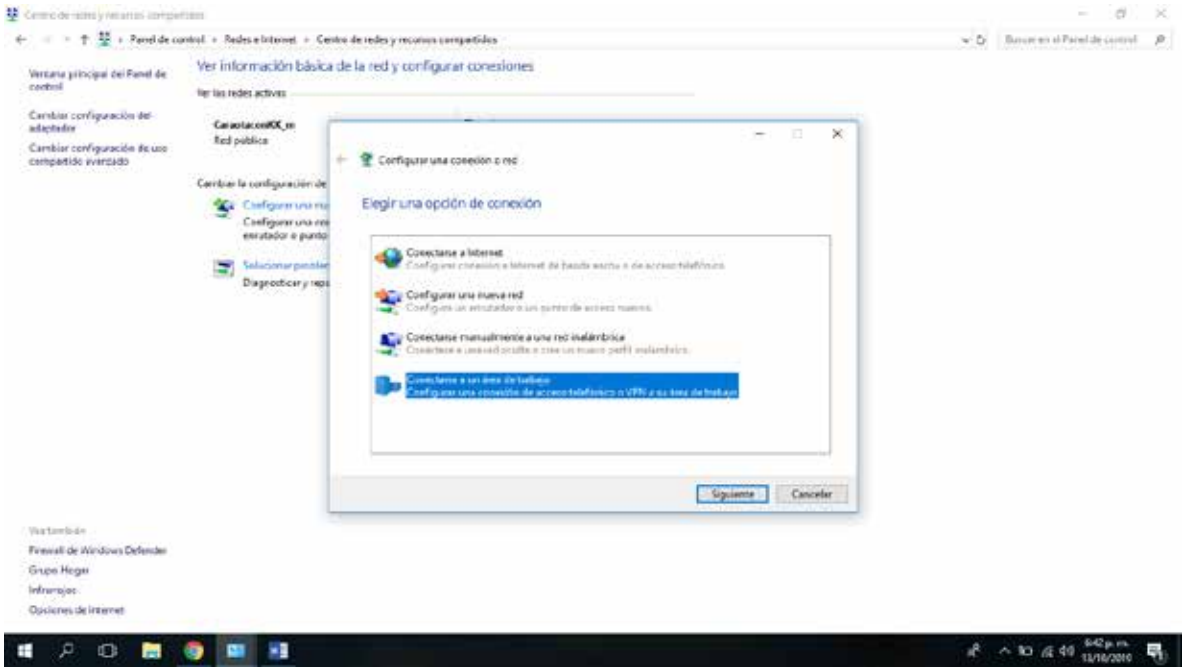

Figura 35. Configuración máquina cliente para la conexión al servidor VPN en Windows 10: Configuración de una nueva conexión de red de trabajo.

· **Fuente:** los autores

En la ventana que aparece se marcó la opción de **mi conexión a Internet** (**VPN**). Ver figura 36

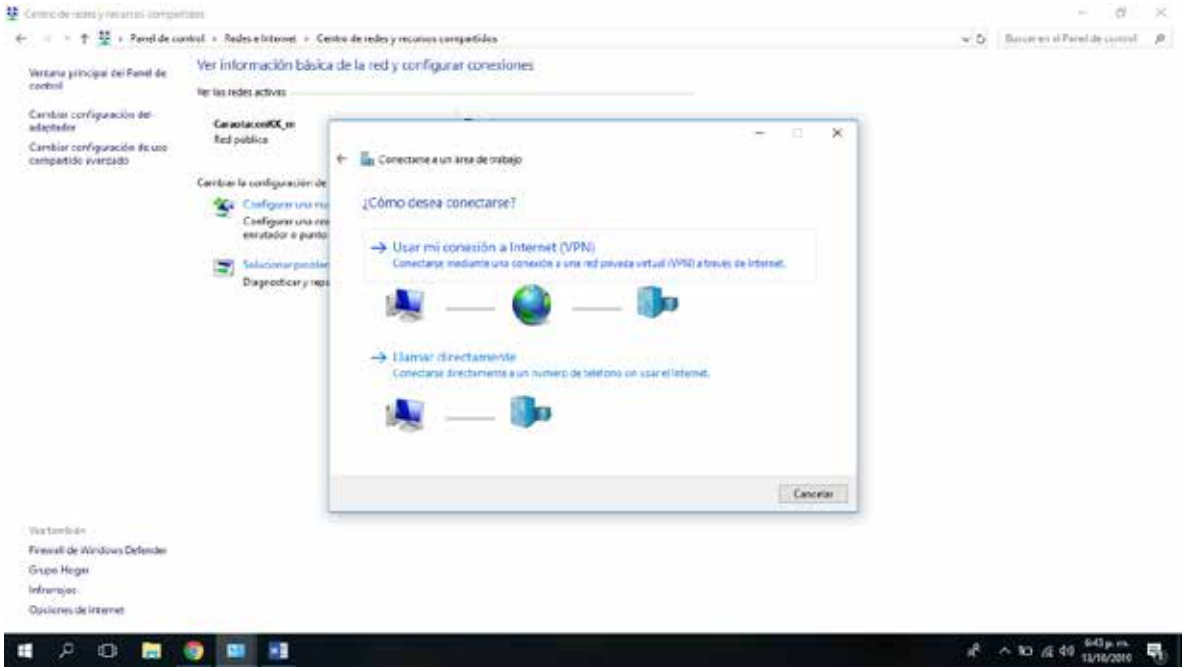

Figura 36. Configuración máquina cliente para la conexión al servidor VPN en Windows 10: Selección de VPN como conexión.

Fuente: **los autores**

En la siguiente venta se realizó el ingreso de la dirección IP del servidor VPN (IP primaria / estática de la red externa que tiene conexión a Internet) . Ver figura 37.

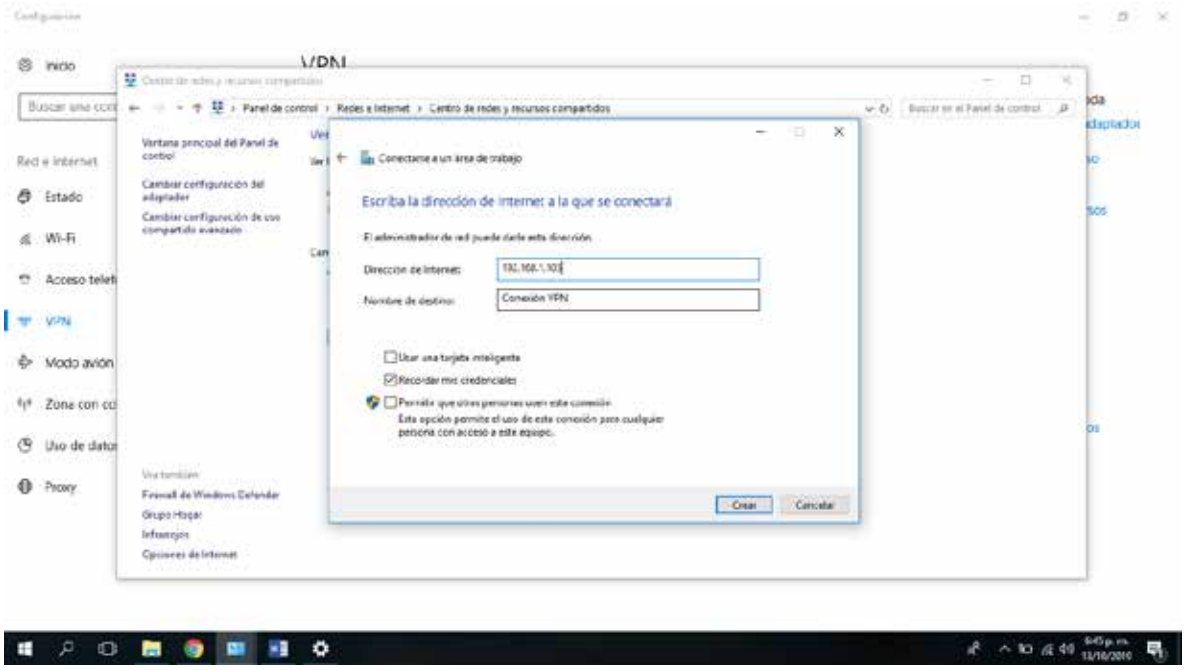

Figura 37. Configuración máquina cliente para la conexion al servidor VPN en Windows 10: Ingreso de la dirección IP del servidor.

Fuente: **los autores**

En la ventana de **Editar conexión VPN** se ingresó los detalles de inicio de sesión del servidor VPN y luego se hizo click en Guardar. Ver figura38.

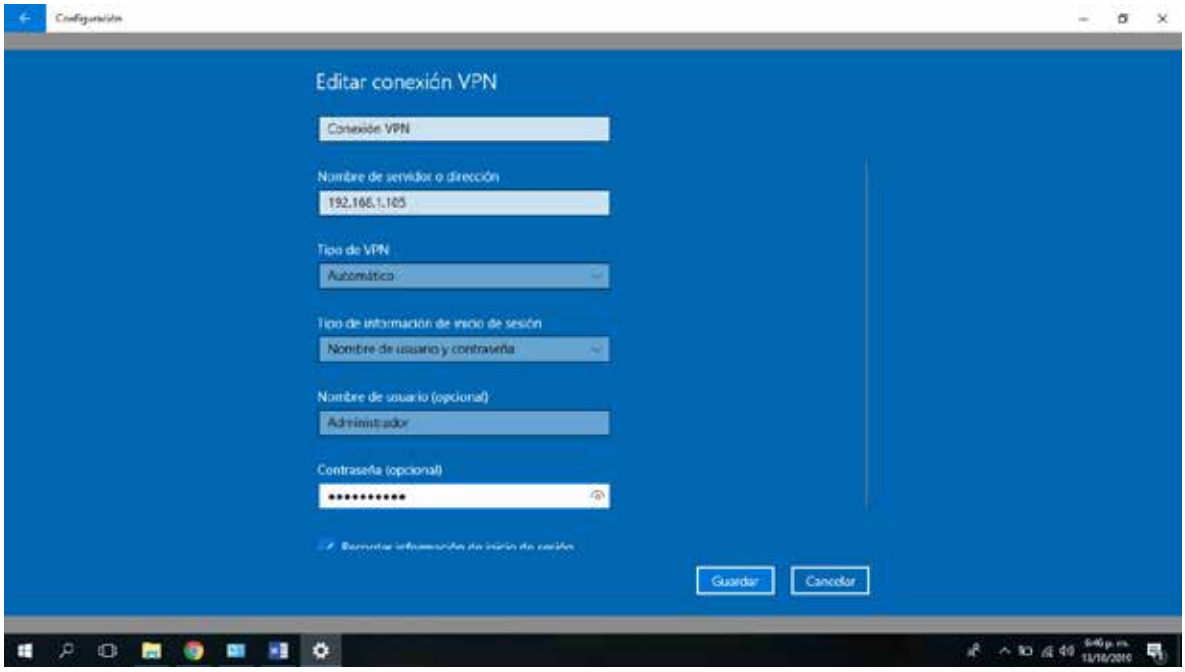

Figura 38. Configuración máquina cliente para la conexión al servidor VPN en Windows 10: Ingreso de la dirección IP del servidor Configuración VPN.

- **Fuente:** los autores

En este punto la maquina local está conectada al servidor VPN, como se puede observar en la figura 39. Se pudo verificar la dirección IP desde una herramienta en línea, y se observó que la dirección IP era del servidor VPN y no del ISP local.

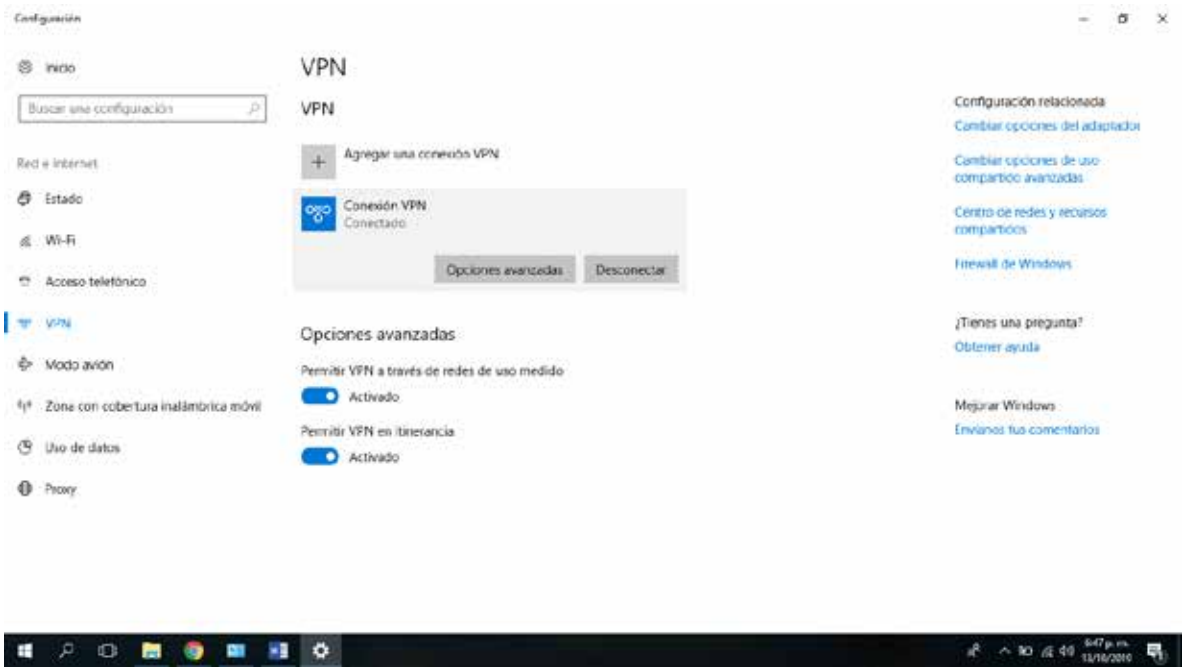

Figura 39. Configuración máquina cliente para la conexión al servidor VPN en Windows 10: Verificación de la conectividad de la VPN.

- **Fuente:** los autores

En Consola de Windows se pudo verificar la conectividad junto con las direcciones IPs asignadas a cada uno de los adaptadores, incluyendo el de VPN. Ver figura 40.

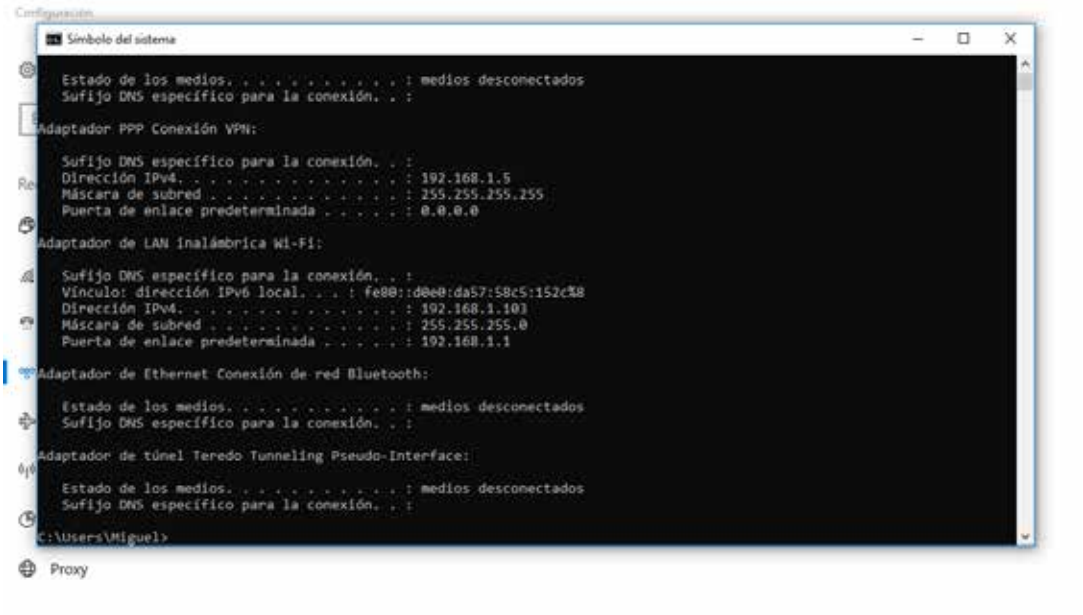

Figura 40. Configuración máquina cliente para la conexión al servidor VPN en Windows 10: Verificación de la conectividad de la VPN a través de Consola de Windows

Fuente: **los autores**

4.6. Equipamiento a utilizar para la creación de la VPN

- Servidor Dell PowerEdge R610 | 2x2.66GHz 12 núcleos | 32GB |

Figura 41. Servidor Dell PowerEdge R610

- **Fuente: página web de la empresa** Amazon

- Router de servicios integrados con Firewall Cisco 2911

Figura 42. Router de servicios integrados con Firewall Cisco 2911

- **Fuente: página web de la empresa** Amazon

4.7. Estudio de factibilidad

4.7.1. Ambiental

Este estudio fue de gran impacto para el autor ya que se desconocía de los grandes beneficios que caracteriza la utilización de una VPN en el aspecto ambiental

ya que solo se conocía el aspecto tecnológico que tiene ventajas ya descritas en todo el trabajo de grado.

Las compañías que apuestan por el uso un sistema de acceso remoto a su red 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, según la segunda edición del Libro Blanco Más allá del Teletrabajo: Una nueva forma flexible de trabajar, publicado por la Fundación Másfamilia, en colaboración con BICG, AXA España.

Según cálculos realizados por Fundación Másfamilia 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 teletrabajar), se obtendría una reducción de 332.843 ton CO2/año o unas 336.171 ton de GEI/año (GEI - gases de efecto invernadero).

Por otro lado, 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.

4.7.2. Económica

Factibilidad económica en cuanto el diseño e implementación del acceso remoto a través de una red VPN, lo que quiere decir que la inversión que la empresa está aportando es justificada por las ganancias generadas, los costos mediante la adquisición de hardware como se indica en la tabla n°3.

La aplicación del acceso remoto a través de una red VPN incrementa un beneficio económico a los trabajadores por no gastar en transporte público para llegar hasta su puesto de trabajo este tipo de acceso garantiza mayor seguridad al gestionar datos y

documentos importantes a distancia ya que con una conexión de forma rápida y segura desde su domicilio. De los trabajadores actuales son 16 en total de los cuales solo el 50% cuenta con vehículo propio y el resto debe tomar el servicio de transporte público.

Tabla n° 3 Cuadro de costos en equipamiento, instalación y soporte técnico

ID	Descripción	Precio(USD)
1	Router de servicios integrados con Firewall Cisco 2911	455
2	Servidor Dell Power Edge R610 | 2x2.66GHz 12 núcleos | 32GB | FOB (Free on board)	280
3	Instalación, programacion y soporte técnico por un año de Router Cisco 2911	700
	TOTAL	**1435**

*Nota: La instalación y soporte técnico del servidor Dell Power Edge lo llevara a cabo personal técnico de la radio. / Todos los precios incluyen IVA.

Fuente: los autores

4.7.3. Operativa

La adecuación de una Red Privada Virtual en la empresa Radio América es un sistema de fácil uso para los usuarios locales y externos, ya que solo requiere de una autenticación y validación de datos para poder ingresar a la información de la empresa, lo cual no generaría un mal uso o fallas en el sistema. Al momento de implementar esta tecnología debemos establecer si es aceptable por los empleados, que resultados producirá para la empresa y los usuarios externos, la productividad de los empleados mejorara y se beneficiaran de trabajar desde casa o desde otra ciudad, producirá efectos positivos en algunas o todas las áreas de Radio América.

4.7.4. Técnica

Mediante la implementación de la Red Privada Virtual brindar los recursos necesarios como conocimientos, habilidades, experiencia, manejo y especificaciones técnicas de esta tecnología a los usuarios, la cual permitirá que la utilización sea fácil y compresible para ellos. Mejora del sistema actual.

4.7.5. Legal

- En relación con las implicaciones legales pertinentes para el uso de una RED VPN se adquieren las licencias de software para Windows Server 2012 el cual se encuentra integrado en el servidor Servidor Dell PowerEdge R610. Con el cual se cuenta para la implementación del acceso remoto a la empresa Radio América.
- Es factible en el ámbito legislativo ya que no existe ninguna ley o reglamento que regule la aplicación, creación y usos de una red VPN, según CONATEL. Cabe destacar que la empresa CANTV ofrece servicios de acceso remoto a través VPN a Clientes Jurídicos.

4.7.6. Social

En siguiente estudio demostró que los análisis de los resultados por medio de la técnica de recolección de datos, basadas en encuesta cerradas de respuestas de SI y NO, el desconocimiento de la red, sus beneficios y aplicaciones. Dicha encuesta fue aplicada a los departamentos de RRHH y Administración.

4.8. Encuestas

En el siguiente orden se definieron las preguntas:

Instrucciones:

Mediante la presente encuesta se busca conocer la necesidad para acceder de manera remota a la red corporativa.

Lea detenidamente cada uno de los Ítems

Marque con una (X) la respuesta que considere correcta

Ítems	**Alternativas**	
	Si	**No**
1- ¿Ud. ha utilizado en algún momento una red VPN?	0	4
2- ¿Conoce Ud. acerca de las ventajas de utilizar una red VPN?	1	3
3- ¿Ud. estaría de acuerdo con la implementación de una VPN en su área de trabajo?	4	0
4- ¿Participaría Ud. en la capacitación para el uso de la red VPN?	4	0
5- ¿Conoce Ud. otros sistemas de acceso remoto que no estén basados en VPN?	1	4
6- ¿Cree Ud. que sea necesario reemplazar el modo de acceso a la red actual?	3	1
7-¿Ud. posee algún ordenador y conexión a internet desde casa?	4	0

Tabla nº 4. Encuesta realizada a los trabadores del departamento de RRHH y Administración de Radio América

Fuente: los autores

4.8.1. Resultados de las Encuestas

Luego de haber practicado las encuestas a la población definida en el departamento de Administración y RRHH donde la muestra obtenida fue de seis empleados (4), se describen los resultados por los ítems propuestos.

Ítem 1-. ¿Ud. ha utilizado en algún momento una red VPN?

La respuesta a la siguiente interrogante se caracteriza por desconocimiento total al sistema de acceso remoto seleccionado.

Ítem 2- ¿Conoce Ud. acerca de las ventajas de utilizar una red VPN?

El resultado a esta interrogante denota la falta de conocimiento en su gran mayoría de los trabajadores acerca de los beneficios que nos brinda una red privada virtual

Ítem 3- ¿Ud. estaría de acuerdo con la implementación de una VPN en su área de trabajo?

Queda demostrado con la siguiente repuesta, que la población desea que el diseño se culmine en implementación luego que se explicara de manera sencilla y dinámica las preguntas anteriores

Ítem 4- ¿Participaría Ud. en la capacitación para el uso de la red VPN?

Con una aprobación rotunda ante la siguiente interrogante, de manera que los empleados pueden interpretar la información suministrada por el inductor.

Ítem 5- ¿Conoce Ud. otros sistemas de acceso remoto que no estén basados en VPN?

Como se puede apreciar solo un empleado se encuentra familiarizado con los que son los accesos remotos por lo que la mayoría queda a la expectativa antes esta interrogante.

Ítem 6- ¿Cree Ud. que sea necesario reemplazar el modo de acceso a la red actual?

Las respuestas ante la siguiente interrogante demuestran la confianza que ofrecen los empleados para poder acceder desde cualquier sitio sin tener que estar presente en su lugar de trabajo.

Ítem 7- ¿Ud. posee algún ordenador y conexión a internet desde casa?

Actualmente tener un computador forman de nuestra vida cotidiana y lo que implica la conexión a internet mediante un ISP, por lo cual es totalmente positiva la respuesta ante la pregunta planteada.

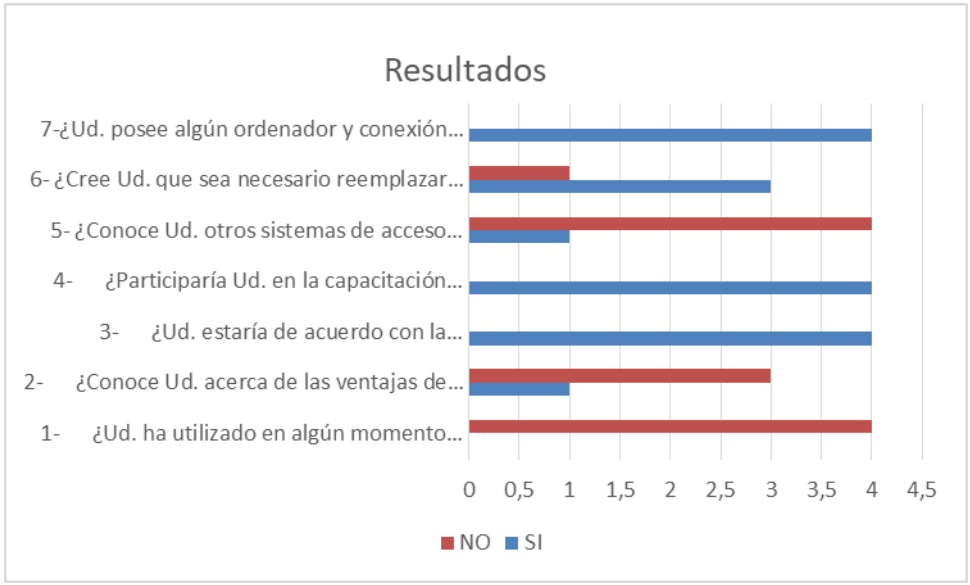

Figura 43. Resultados encuesta.
Fuente: los autores

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

De la presente investigación se concluye que la problemática en el acceso remoto a la oficina de la empresa Radio América requiere una solución oportuna, como es la red VPN se encarga de establecer un túnel, es decir un canal de comunicación seguro a través de Internet para oficinas remotas, usuarios móviles y socios comerciales, con respecto a el diseño de la red de Radio América CA inicia desde cero, en consideración con el sistema actual, con el fin de evitar inconsistencias a futuro. El montaje de la red se realizará mediante Packet Tracer y Visio Office 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 realizó para Radio América CA 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 Radio América CA, 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.

- Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos, reduciendo significativamente el costo de la transferencia de datos de un lugar a otro.

- 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

- La seguridad en las redes es una necesidad, dadas las características de la información que por ellas se transmite, permitiendo la confidencialidad e integridad de dicha información mediante protocolos de encriptación que eviten la manipulación de terceros. Por consiguiente, la utilidad de la red VPN para trabajar a distancia o desde casa es un beneficio fundamental tanto para la empresa como para el trabajador incrementando su productividad de forma veraz y segura, como por ejemplo las noticias, vivencias y opiniones relatadas por los periodistas de la empresa Radio a través de sus diferentes redes sociales.

- Informar a los empleados de los servicios y beneficios de la red, así como de su funcionamiento; además solicitar que se enmarquen en las políticas de seguridad establecidas.

Recomendaciones

- Otorgar el acceso VPN a los usuarios claves de la Organización, ya que esto garantiza la optimización de los recursos y la continuidad al intercambio de información.

- Mantener el firmware actualizado para evitar posibles vulnerabilidades o bugs asociados a la versión.

- Renovar el licenciamiento del Firewall, Windows, antivirus de la organización.

- Activar protocolos de seguridad suficientemente confiables como IPSec, L2PT, Open VPN entre otros para mayor seguridad criptográfica, ya que por el factor tiempo no se han habilitado a la programación del servidor.

- Realizar auditorías de hardware y software trimestralmente como conexiones en la red VPN para un mayor control y registro.

- Crear un manual que defina los pasos que deben seguir los trabajadores para obtener la conexión a la red VPN.

REFERENCIAS

Bibliográficas

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

Balestrini, M. (2006). **Como se Elabora el Proyecto de Investigación.** Caracas. Editorial: BL Consultores Asociados.

Dubs de Moya, R. (2002). **El Proyecto Factible: una modalidad de investigación.** Caracas, Venezuela.

Forouzan, B. (2007). **Transmisión de Datos y Redes de Comunicaciones.** España: Editorial: McGraw-Hill

Hurtado, J. (2007). **El proyecto de investigación.** Caracas: Editorial Quirón.

Mijares, H y García, L. (2007). **Normas para la Elaboración y Presentación de los Anteproyectos, Proyectos y Trabajos de Grado**. Carabobo: Editorial UJAP .Caracas: Editorial Fedupel.

Editorial Limusa.

Pérez. M. (2012). **Configuración de una RED VPN.** México. Editorial BMJ.

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

Tamayo, M. (1998). **El proceso de la investigación científica.** 3ra edición. México:

Electrónicas

Aguiar, M (2012). **Configuración de una Red en telecomunicaciones**. Recuperado en:

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

Aguilera, P (2016)**. Sistemas de telecomunicaciones.** Recuperado en:

https://repository.unimilitar.edu.co/bitstream/handle/10654/9294/ContrerasHurtadoJuanJose2013.pdf;jsessionid=8B8F6719F0983D83E2EA5922851F8A89?sequence=2

González, A. (2017). **Red Privada Virtual.** Recuperado en: **http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf**

Mackenzie J. (2015). **Tipos de Redes Privadas** Recuperado: **https://repository.DiseñoyconstrucciondeunGPONa.pdf;jsessionid=8B8F6719F0983D83E2EA5922851F8A89?sequence=2**

Osorio, A. (2016). **Redes Privadas.** Recuperado en: **https://repositorio.espe.edu.ec/bitstream/21000/11329/1/AC-ESPEL-EMI-0295.pdf**

Peña, V. (2019) Diseño **e implementación de un Red Privada Virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada** Recuperado en: **https://repository.DiseñoyconstrucciondeunGPONa.pdf;jsessionid=8B8F6719F0983D83E2EA5922851F8A89?sequence=2**

Ramírez M. (2015). Protocolos de Seguridad para Redes Privadas Virtuales (VPN). **Recuperado en: https://repository.DiseñoyconstrucciondeunGPONa.pdf;jsessionid=8B8F6719F0983D83E2EA5922851F8A89?sequence=2**