UNIVERSIDAD JOSÉ ANTONIO PÁEZ

RED PRIVADA VIRTUAL (VPN) DE ACCESO REMOTO A LA RED LOCAL EMPRESARIAL DE AXE TELECOM

Autor:
Jorge Luis Malpica Perez

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

RED PRIVADA VIRTUAL (VPN) DE ACCESO REMOTO A LA RED LOCAL EMPRESARIAL DE AXE TELECOM

Trabajo de grado presentado como requisito para optar al título de

INGENIERO TELECOMUNICACIONES.

Autor:
Jorge Luis Malpica Perez
CI: 18.913.618
Tutor: Ing. Wilmer Mendoza

San Diego, Febrero 2020

FI-T -002-2020-1CR (TG)

Valencia, 08 de junio de 2020

Ciudadano:
Malpica P, Jorge L.
18.913.618
Presente-

Cumplo con informarle que la Comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión **Nº 01-2020** de fecha **10-02-2020** aprobó el proyecto de trabajo de grado titulado ***RED PRIVADA VIRTUAL (VPN) DE ACCESO REMOTO A LA RED LOCAL EMPRESARIAL DE AXE TELECOM*** presentado por usted (es) como requisito para optar al título de Ingeniero en Telecomunicaciones.

Se ratifica la designación del Ing. Wilmer Mendoza C.I: 22.225.097 como Tutor Académico que lo asesorara en el desarrollo de este proyecto.

Atentamente,

Decano de la Facultad de Ingeniería

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

Ll/a.a.

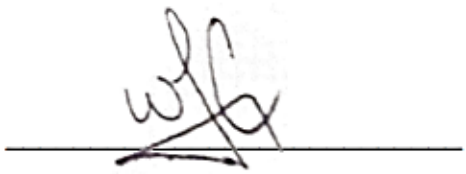
REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE TELECOMUNICACIONES

San Diego, 30/06/2020

APROBACIÓN DEL TUTOR

Quien suscribe, Ingeniero Wilmer Mendoza portador de la cedula de identidad Nº V-22.225.097, en mi carácter de tutor del trabajo de grado presentado por el ciudadano Jorge Luis Malpica Perez, portador de la cedula de identidad Nº V-18.913.618, titulado **RED PRIVADA VIRTUAL (VPN) DE ACCESO REMOTO A LA RED LOCAL EMPRESARIAL DE AXE TELECOM**, presentado como requisito parcial para optar al título de Ingeniero en Telecomunicaciones, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a presentación pública y evaluación por parte del jurado examinador que se designe.

En San Diego, a los treinta (30) días del mes de junio del año dos mil veinte (2020).



Ing. Wilmer Mendoza
C.I.: 22.225.097

DEDICATORIA

Dedicado este Trabajo Especial de Grado a los docentes los cuales han entregado sus esfuerzos, conocimientos y buenos deseos para hacer de nosotros unos profesionales preparados y aptos para enfrentar un largo camino profesional. Dedicado especialmente a mis Padres Tomas Malpica y Nubia Perez a mi esposa Marbely Morales a mi hijo Mathias Malpica a mi hermano Israel Malpica y a Dios, los cuales han sido un gran apoyo para luchar y seguir adelante en esta ardua labor superando los obstáculos que vivimos durante todo el proceso académico, dándome fuerza y animo cada día para lograr y cumplir el objetivo.

AGRADECIMIENTOS

Ante todo, agradezco a Dios por darme fuerza, valor, sabiduría y herramientas necesarias para cumplir mis objetivos.

Agradezco a José Gregorio Hernandez y la Virgen del Valle por brindarme protección y salud en cada momento y escucharme en cada situación.

Agradezco a la Universidad José Antonio Páez (UJAP), por haberme brindado la oportunidad de cursar y adquirir conocimientos a lo largo de la carrera.

A los profesores y tutor por haberme orientado y apoyado durante el desarrollo de Trabajo Especial de Grado.

A mi familia y amigos que de una u otra manera están presentes en mi crecimiento personal y profesional.

Muchas gracias a todos por haberme brindado durante todo este tiempo su confianza, amor y apoyo en mis años de carrera.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

Tablas **Pág.**

ÍNDICE DE FIGURAS

FIGURAS **Pág.**

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

RED PRIVADA VIRTUAL (VPN) DE ACCESO REMOTO A LA RED LOCAL EMPRESARIAL DE AXE TELECOM

Autor: Jorge Luis Malpica Perez
Tutor: Ing. Wilmer Mendoza
Fecha: marzo 2020.

RESUMEN

En las telecomunicaciones vía red, el internet brinda la posibilidad de enviar y recibir información bien sea en diferentes formatos de video, audio o imágenes a través de una red pública, logrando el libre tráfico pero esta información es vulnerable ya que terceros pueden interceptarla y no se garantiza la seguridad sobre el internet, por tal surge la idea de utilizar la misma plataforma del internet como medio para usuarios y empresas de enviar y recibir dicha información de manera segura, con la idea de las redes (VPN) la información puede viajar sin ningún tipo de inconvenientes bien sea por que esta es interceptada o modificada ya que las (VPN) brindan todas estas características de seguridad como ser encriptadas y además de trabajar con servidores de control asignando direcciones IP y brindando acceso y autentificación, con esta red atractivamente más económica que otros servicios como enlaces punto a punto o líneas dedicadas, podemos disfrutar la misma privacidad a un menor costo; con el diseño de la red (VPN) para la empresa Axe Telecom sus empleados pueden conectarse de manera remota continuando con sus funciones, gracias a el desarrollo de ese servicio tecnológico de comunicación a nivel de redes de telecomunicaciones.

La empresa Axe Telecom requiere que sus empleados estén conectados vía remota de la manera más segura y menos costosa posible y que cumplan sus labores y sigan interactuando con los clientes desde cualquier lugar, con el diseño de esta red VPN la cual mediante protocolos de seguridad encriptaran la información antes de esta ser enviada a la red y dará acceso mediante autentificación a los usuarios que se le permita acceder, además de acceder a carpetas o documentos dentro del servidor principal; entre las modalidades de investigación a utilizar esta la del tipo de proyecto que es factible con un nivel de tipo descriptivo y un diseño de tipo documental y de campo ya que con la ayuda de programas de simulación y diseño de redes como Packet Tracer se realizó toda la topología que en este caso será tipo estrella con lo cual todos los terminales estarán en la red interna conectados vía ethernet además de la configuración del servidor de la empresa con Windows Server 2012 R2 el cual brindara las funciones de conexión y autentificación a los usuarios y clientes externos a la red interna.

Descriptores: Tecnología, Servidor, red, internet, terminales, topología.

INTRODUCCIÓN

Desde que al mundo han incursionado las computadoras o dispositivos electrónicos las telecomunicaciones se han venido desarrollando a grandes pasos viéndose beneficiada también la rama de las redes las cuales permiten la comunicaciones entre diferentes puntos transportando información de cualquier usuario o persona; tanto ha sido el desarrollo que en esta época las empresas que prestan el servicio de telecomunicaciones se ven obligados a ofrecer un mayor ancho de banda o velocidades que permitan a los usuarios excelente calidad a la hora de enviar información a través de sus plataformas.

Gracias al uso de las redes locales muchas empresas u organismos se han beneficiado de esta tecnología la cual permite el libre tráfico de archivos, documentos, carpetas y que ofrece una seguridad a nivel interno de la información ya que se mantiene resguardada en una red cerrada pero con el desarrollo de las empresas estas se ven en la necesidad de enviar y compartir información mucho más allá de una red local y que esta información viaje a lugares remotos, otros estados, países o continentes los cuales el emisor necesita que dicha información este protegida, segura sin alterar y mucho menos que llegue a un destino equivocado.

Para esto se ha utilizado como medio las redes que gracias a la plataforma del internet la cual es la principal y más extensa red a nivel mundial ha permitido el intercambio de datos por muchos años y lo seguirá haciendo pero existe la desventaja que esta plataforma no brinda la seguridad por si sola de que la información enviada por su estructura este protegida ya que por ser la principal red a nivel mundial es la más congestionada y vulnerable lo cual puede ocasionar que manos inescrupulosas o terceros manipulen el mensaje y quizás no llegue a su destino.

Por este motivo surge el desarrollo de las redes virtuales privadas (VPN) las cuales si bien es cierto trabajan sobre la misma plataforma del internet esta con el uso de diferentes protocolos y servidores de acceso o autentificación permiten crear un

túnel entre dos sedes (emisor-receptor) logrando que el mensaje viaje de manera segura, confiable y sin que esta haya sido alterada, además de esto otra característica de las (VPN) es la manera en que esta encriptada la información.

Existen otros medios para establecer la comunicación mediante las redes, los diferentes puntos o sedes de una empresa o usuarios que deseen conectarse vía remota como líneas dedicadas, pero con el uso de las VPN mediante la plataforma del internet el costo es mucho más reducido ahorrando a las empresas capital y disfrutando de la misma seguridad que ofrecen otros servicios de telecomunicación.

Seguidamente se presentan cada uno de los 4 capítulos en los cuales se expone lo investigado, indicando su estructura y la finalidad de cada uno.

Capítulo I: Esta referido al planteamiento del problema y cuáles son las posibilidades de obtener una solución satisfactoria, realizando un diagnostico a la situación actual para determinar las causas que producen el problema y como objetivo general se tendrá, Proponer el diseño de una Red Virtual Privada (VPN) de acceso remoto.

Capítulo II: Este capítulo constituye un aspecto de mucha importancia dentro de la investigación. En términos generales, representa la "explicación" teórica para comprender la naturaleza del hecho investigado, o lo que es lo mismo, sustentar teóricamente el estudio. Con la investigación de los antecedentes también se tendrá una idea o apoyo para la solución del problema.

Capítulo III: se planteará 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 este capítulo veremos los resultados obtenidos luego de diagnosticar, analizar, investigar y diseñar la red VPN con la ayuda del programa de simulación Packet Tracer 7.2.2 y de Windows Server para prestar el servicio a los usuarios, y cuál fue la inversión y costo del proyecto.

CAPÍTULO I
EL PROBLEMA

1.1 Planteamiento del problema

A continuación, se presentan breves citas

Según Ackoff (2012) … **“**Un problema bien planteado constituye la mitad de la solución.” (p. 37)

En términos generales, problema es un asunto que requiere solución.

Independientemente de su naturaleza, un problema es todo aquello que amerita ser resuelto. Si no hay necesidad de encontrar una solución, entonces no existe tal problema.

Según Arias (2012) … “El planteamiento del problema consiste en describir de manera amplia la situación objeto de estudio, ubicándola en un contexto que permita comprender su origen, relaciones e incógnitas por responder”.

Si bien es sabido hoy en día las empresas a nivel mundial están conectadas internamente mediante redes locales (LAN) las cuales permiten compartir archivos, documentos, información que tienen un gran valor para la institución o empresa, mediante el uso de esta red local (LAN) diferentes departamentos de una misma empresa mantienen la comunicación entre ellos y con otros dispositivos gracias a la conexión vía red mediante sus equipos de escritorio logrando así sus funciones y realizar sus trabajos todo esto de una manera cercana; la problemática surge cuando estas empresas envían documentos fuera de la red local (LAN) utilizando como plataforma el internet apoyándose de correos o cargando la información a medios de almacenamiento como las “nubes”, esta información valiosa la cual es vulnerable sobre el internet puede ser interceptada por terceros y manos inescrupulosas permitiendo a

estos aprovecharse de la misma, si estos archivos no están protegidos o encriptados pueden ocasionar dependiendo del tipo de información que contenga, perdidas económicas, de tiempo, de confidencialidad.

En la empresa AXE TELECOM C.A en la cual tengo el gusto y privilegio de trabajar ubicada en Santa Mónica, Caracas, la empresa internamente tiene su estructura de red local con la cual los diferentes departamentos (Administración, RRHH, Ingeniería, Gerencia e Implementación) comparten información de gran valor de manera segura, con el transcurso de los años la empresa ha venido presentando problemas de seguridad en la red con información que se realiza internamente debido a que Axe realiza trabajos de ingeniería los cuales se redactan documentos y realizan propuestas sobre planificación, cálculos, instalación y configuración de equipos de Telecomunicaciones y luego esta información es enviada por correo a los clientes, información la cual no está protegida ni encriptada y puede ser interceptada por terceros permitiendo visualizar lo que hay internamente en el documento y de alguna manera ser robado todo el esfuerzo y tiempo que se invirtió.

Además el departamento de administración de igual manera maneja información en cuanto a pagos, montos, presupuestos o transacciones que siguen siendo vulnerables sobre el internet, esta información solo debería ser visualizada a quien interese a la empresa por otro lado existe la problemática de que se realizan proyectos en horarios fuera de horario de oficina y dicha información esta almacenada en el servidor interno de Axe la cual estando fuera los empleados les es imposible conseguir, ocasionando pérdida de tiempo, recursos y dinero, esto conlleva retrasos en los trabajos dejando en una mala posición a la empresa.

Entre otros problemas se lleva una gran cantidad de inventario de herramientas y esta información hoy en día esta almacenada en una nube permitiendo que esta sea visualizada por la empresa que presta el servicio lo cual no es de mucho agrado para Axe. Por otra parte, Axe cuenta con empleados que laboran fuera de la oficina ubicados en diferentes países y con estos de igual manera hay un constante intercambio de información de alto valor que se necesita este protegido y estos puedan trabajar de

manera confiable. Con la idea de la red VPN, esta información viajaría mediante internet de manera segura permitiendo a los empleados trabajar desde sus hogares u otros lugares, logrando tranquilidad en la empresa sabiendo que su información está completamente protegida.

Según Arias (2012) … "Formulación del problema es la concreción del planteamiento en una pregunta precisa y delimitada en cuanto a espacio, tiempo y población (si fuera el caso)."

1.2 Formulación del problema

Del planteamiento del problema redactado anteriormente podemos formularnos la siguiente interrogante.

¿Cómo establecer una comunicación de manera segura que permita el flujo de información entre la red de área local de Axe Telecom con los diferentes usuarios externos y clientes?

1.3 Objetivos de la investigación

Según Arias (2012) …" El objetivo de una investigación es un enunciado que expresa lo que se desea indagar y conocer para responder a un problema planteado."

1.3.1 Objetivo General

- Proponer el diseño de una red privada virtual (VPN) de acceso remoto a la red local de la empresa Axe Telecom ubicada en Santa Mónica, Caracas.

1.3.2 Objetivos Específicos

- Diagnosticar la condición actual en que se encuentra la red de comunicación de Axe Telecom.
- Identificar fallas y puntos críticos de la red de comunicación de la empresa Axe Telecom.
- Diseñar la red privada virtual (VPN) de acceso remoto a la red local empresarial de Axe Telecom.
- Realizar el estudio de factibilidad técnica, económica, social y ambiental para la implementación de la propuesta.

1.4 Justificación del problema

Estamos en una época donde el avance de la tecnología evoluciona cada día drásticamente, siempre hay innovaciones, creaciones sorprendentes que nos facilitan la vida o entretienen, las empresas hoy en día tienen que seguir ese mismo camino ya que la alta competencia entre ellas las obliga a tener las últimas actualizaciones o lo más reciente en el mercado, si estas no van a la par de la tecnología quedaran prácticamente obsoletas o en el olvido, es el caso de muchas empresas que no quisieron arriesgarse al cambio y por ende sufren la perdida de lo que por muchos años les costó construir.

Modernizar y mantener al día las empresas esto las coloca en una posición favorable lo cual se ven beneficiadas tanto la misma empresa como sus empleados lo cual es la idea que se tiene con la empresa de AXE TELECOM y diseñar la red VPN la cual todos se verán beneficiados permitiendo que cualquier empleado pueda trabajar desde manera remota o desde sus hogares, la razón es que cada empleado tendrá la facilidad de conectarse desde cualquier lugar a cualquier hora a su trabajo de una manera segura sin que esta red sea vulnerable a terceros ya que debido a problemas como el transporte público o el simple hecho de conseguir efectivo o que a tempranas o altas horas sea imposible llegar al trabajo u oficina debido a la inseguridad, cualquier empleado podrá tener la información que necesite sin que este se encuentre en dicho lugar, además de mentalmente crear una sensación de comodidad ya que no se retrasarían ciertos trabajos debido a los percances mencionados anteriormente.

Con el desarrollo de esta nueva red la empresa tendrá otra puerta o facilidad que los empleados tendrán para seguir trabajando además de estar actualizados ya que la red VPN brinda la misma seguridad que una red local y evita que manos inescrupulosas accedan a información de alto valor de la empresa sin importar que esta viaje mediante el internet, la información estará encriptada y estará protegida solo con acceso a personal autorizado, evitara el retraso de trabajo a ciertos empleados además de que para su implementación es mucho más económica que otras tecnologías como frame relay y firewall y los equipos a nivel de hardware implican menos cantidad, lo único

para mantener esta comunicación seria tener un proveedor de internet que nos garantice el buen servicio de internet.

1.5 Alcance de la investigación

Con el siguiente Trabajo Especial de Grado se tiene como finalidad el diseño de una red VPN la cual permita ampliar la red interna de la empresa y lograr que la comunicación entre los empleados y la compañía de manera remota sea completamente segura y confiable, facilitando que todo lo que viaje por la red en este caso el internet este protegido evitando retrasos laborales y acceso a cualquier hora y brindando así otra herramienta de comunicación actualizada con la cual los empleados poniendo en práctica se verán beneficiados.

1.6 Limitaciones

Entre las limitaciones podemos quizás tener problemas con los proveedores de internet (ISP) ya que entre ellos esta CANTV y por tal su calidad de servicio no es la más ideal ya que es intermitente y quizás por momentos el servicio se vea interrumpido además las fallas eléctricas en el país viéndose afectado tanto el servidor VPN o donde esté conectado el empleado de manera remota, otras de las limitantes es la económica ya que la implementación de los equipos entre ellos el servidor puede ser costoso.

CAPÍTULO II
MARCO TEÓRICO

Según Mijares y García (2007) … "El marco teórico constituye un aspecto de mucha importancia dentro de la investigación. En términos generales, representa la "explicación" teórica para comprender la naturaleza del hecho investigado, o lo que es lo mismo, sustentar teóricamente el estudio." (p. 12).

Según Arias (2012) … "El marco teórico o marco referencial, es el producto de la revisión documental–bibliográfica, y consiste en una recopilación de ideas, posturas de autores, conceptos y definiciones, que sirven de base a la investigación por realizar." (p.106).

2.1 Antecedentes

Según Arias (2012) … "Los antecedentes reflejan los avances y el estado actual del conocimiento en un área determinada y sirven de modelo o ejemplo para futuras investigaciones." (p. 106).

Ortega, V. (2003) en su trabajo de grado **"Metodología para la implementación de redes privadas virtuales, con internet como red de enlace"** presento en la universidad Técnica del Norte para optar por el título de ingeniero en sistemas computacionales. Ecuador. La presente investigación tuvo como finalidad dar a conocer una nueva tecnología para aquella época que aún hasta el día de hoy de encuentra en evolución, tecnología que nos permitirá conectar redes distantes geográficamente de manera segura y a bajos costos, utilizando redes públicas como medio de enlace o transmisión, dicho termino VPN el cual es muy común en las telecomunicaciones; esta investigación nos representa los aspectos más importantes referente a VPN empezando por una breve introducción a las redes privadas virtuales,

además, se estudia los diferentes elementos que se utilizan para implementar un sistema de red privada virtual, donde se revisara los implementos comunes, los requisitos y beneficios de esta tecnología.

El proyecto se vincula con el actual en función de la selección del software Windows server 2000 el cual tendrá relación con dicho trabajo ya que será utilizada una versión más reciente Windows server 2012, Ortega indica que "espera que esta investigación sirva para afianzar en los lectores los conocimientos sobre redes y VPN y despertar en ellos la curiosidad por esta tecnología que poco a poco va creciendo y posesionándose en el mercado de las telecomunicaciones."

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.

Por ultimo 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 OSI, 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 los desarrollos de estas capas pudieron realizar la implementación de la Red Privada Virtual VPN. 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 OSI. 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.

2.2 Bases Teóricas

Según Mijares y García (2007) … "En esta sección, el investigador se da a la tarea de analizar y explicar el problema, su naturaleza, interrelaciones, así como el planteamiento por parte del investigador de sus propias ideas y exposiciones relacionadas con el tema investigado. Resulta conveniente acudir a bancos de datos, ya sea de consulta manual o por medios electrónicos, indagar en revistas científicas y arbitradas que suelan tratar el tema que interesa, revisar trabajos de grado y conferencias sobre el tópico, consultar a expertos en la materia y cualquier otra fuente que pudiera considerarse provechosa para el desarrollo de la investigación." (p. 14).

Según Arias (2012) … “las bases teóricas implican un desarrollo amplio de los conceptos y proposiciones que conforman el punto de vista o enfoque adaptado, para sustentar o explicar el problema planteado.” (p. 108)

2.2.1 Concepto de 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).

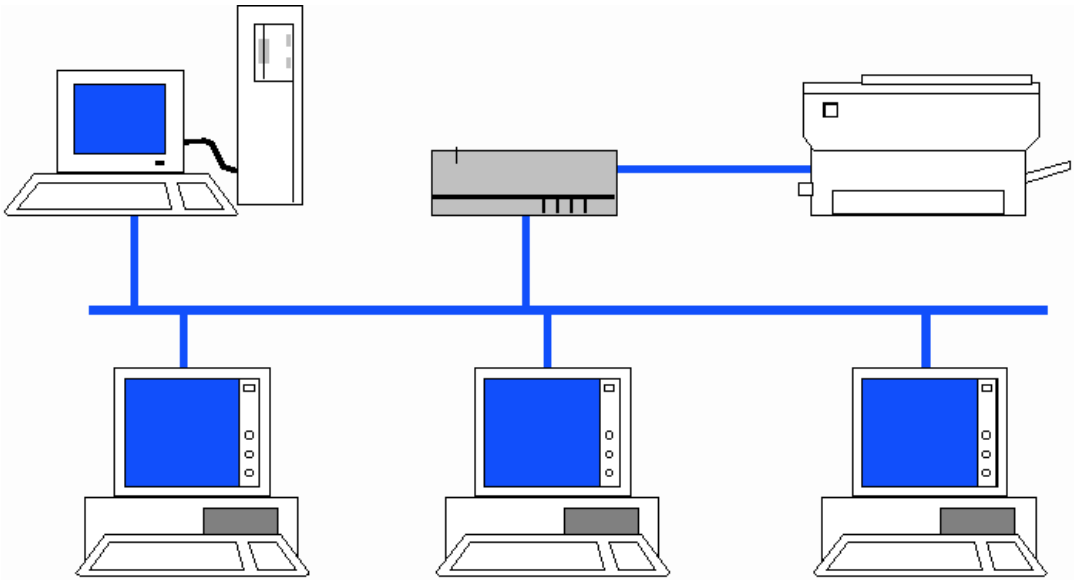


Figura 1. Estructura de una red

Fuente: El autor

2.2.1.1 Red de Computadoras

Las red de computadoras (también llamadas redes de ordenadores, red de comunicaciones de datos o red informática) es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

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

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP utilizado como base para el modelo de referencia OSI. Este último, concibe cada red como estructurada en siete capas con funciones concretas pero relacionadas entre sí (en TCP/IP se habla de cuatro capas). Debe recordarse que el modelo de referencia OSI es una abstracción teórica, que facilita la comprensión del tema, si bien se permiten ciertos desvíos respecto a dicho modelo.

El primer indicio de redes de comunicación fue de tecnología telefónica y telegráfica. En 1940 se transmitieron datos desde la Universidad de Darmouth, en Nuevo Hampshire, a Nueva York. A finales de la década de 1960 y en los posteriores 70 fueron creados los miniordenadores. En 1976, Apple introduce el Apple I, uno de los primeros ordenadores personales. En 1981, IBM introduce su primer PC. A mitad de la década de 1980 los PC comienzan a usar los módem para compartir archivos con otros ordenadores, en un rango de velocidades que comenzó en 1200 bps y llegó a los

56 kbps (comunicación punto a punto o dial-up), cuando empezaron a ser sustituidos por sistema de mayor velocidad, especialmente ADSL en el 1980

2.2.1.2 Red de Telecomunicaciones

Se entiende por red de telecomunicación al conjunto de medios, tecnologías, protocolos y facilidades en general, necesarios para el intercambio de información y archivos entre los usuarios de una red. La red es una estructura, que, para su estudio suele dividirse en los siguientes componentes:

- Red de acceso
- Red de tránsito o núcleo de red
- Servidor
- Estaciones de trabajo
- Recursos Periféricos y Compartidos

Los siguientes son ejemplos de redes de telecomunicaciones:

- las redes de computadoras
- Internet
- la red Telefonica

2.2.2 Red Privada Virtual (VPN)

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

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda

acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

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

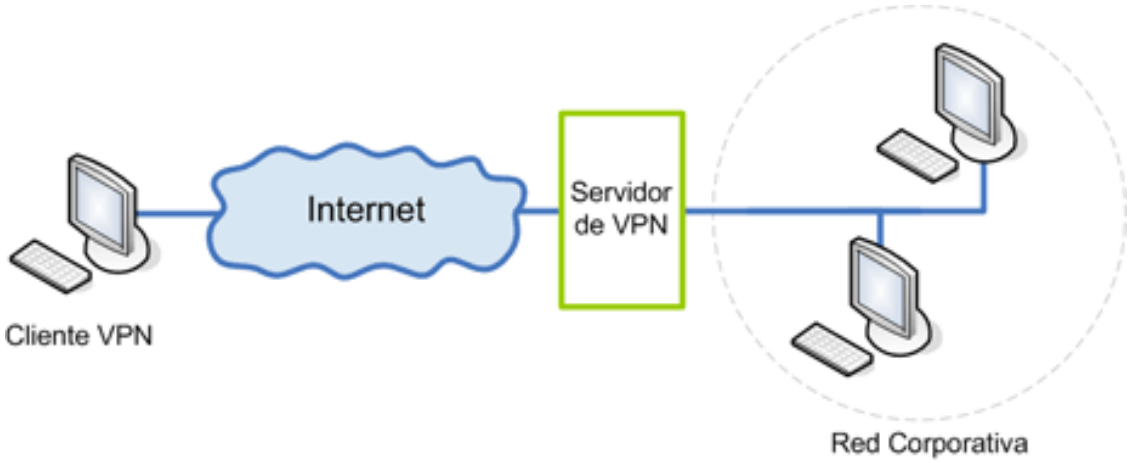


Figura 2. Estructura de red VPN

Fuente: El autor

2.2.2.1 Características básicas de seguridad

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

- Autentificación y autorización: ¿quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: de que los datos enviados no han sido alterados. Para ello se utilizan funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

- Confidencialidad/Privacidad: dado que solamente puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).
- No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.
- Control de acceso: se trata de asegurar que los participantes autentificados tienen acceso únicamente a los datos a los que están autorizados.
- Auditoría y registro de actividades: se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.
- Calidad del servicio: se trata de asegurar un buen rendimiento, que no haya una degradación poco aceptable en la velocidad de transmisión.

2.2.2.2 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. 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.

2.2.2.3 Tipos de VPN

VPN de acceso remoto: Es quizás el modelo más usado actualmente, y consiste en usuarios 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).

VPN punto a punto: Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los

servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales.

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

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

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil. Se maneja de manera remota.

VPN over LAN: Este esquema es el menos difundido, pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta

capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

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

Otro ejemplo es la conexión a redes Wi-Fi haciendo uso de túneles cifrados IPSec o SSL que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

2.2.2.4 Razones por las cuales es recomendable implementar una red 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.

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.

2.2.2.5 Tipos de conexión VPN

- **Conexión de acceso remoto**

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

- **Conexión VPN router a router**

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

- **Conexión VPN firewall a firewall**

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

- **VPN en entornos móviles**

La VPN móvil se establece cuando el punto de terminación de la VPN no está fijo a una única dirección IP, sino que se mueve entre varias redes como pueden ser las redes de datos de operadores móviles o distintos puntos de acceso de una red Wifi. Las VPNs móviles se han utilizado en seguridad pública dando acceso a las fuerzas de orden público a aplicaciones críticas tales como bases de datos con datos de identificación de criminales, mientras que la conexión se mueve entre distintas subredes de una red móvil. También se utilizan en la gestión de equipos de técnico y en organizaciones sanitarias entre otras industrias. Cada vez más, las VPNs móviles están siendo adaptadas por profesionales que necesitan conexiones fiables. Se utilizan para moverse entre redes sin perder la sesión de aplicación o perder la sesión segura en la VPN. En una VPN tradicional no se pueden soportar tales situaciones porque se produce la desconexión de la aplicación, time outs o fallos, o incluso causar fallos en el dispositivo.

2.2.2.6 Implementaciones

El protocolo estándar de facto es el IPSEC, pero también están PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

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

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

de esta familia tenemos a los productos de Fortinet, SonicWALL, SaiWALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen (Juniper Networks), Symantec, Nokia, U.S. Robotics, D-link, Mikrotik, etc.

Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperabilidad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, GNU/Linux y los Unix en general. Por ejemplo productos de código abierto como OpenSSH, OpenVPN y FreeS/Wan.

En ambos casos se pueden utilizar soluciones de firewall («cortafuegos» o «barrera de fuego»), obteniendo un nivel de seguridad alto por la protección que brinda.

2.2.3 IPsec

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

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de aplicación (capa 7 del modelo OSI). Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP.

2.2.4 Seguridad de la capa de transporte (TLS)

Es un protocolo criptográficos, que proporciona comunicaciones seguras por una red, comúnmente Internet.

Se usan certificados X.509 y por lo tanto criptografía asimétrica para autentificar a la contraparte con quien se están comunicando, y para intercambiar una llave simétrica. Esta sesión es luego usada para cifrar el flujo de datos entre las partes. Esto permite la confidencialidad del dato/mensaje, códigos de autenticación de mensajes para integridad y como un producto lateral, autenticación del mensaje. Varias versiones del

protocolo están en aplicaciones ampliamente utilizadas como navegación web, correo electrónico, fax por Internet, mensajería instantánea y voz-sobre-IP (VoIP). Una propiedad importante en este contexto es forward secrecy, para que la clave de corta vida de la sesión no pueda ser descubierta a partir de la clave asimétrica de largo plazo.

2.2.5 Secure SHell (SSH)

Es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada. Además de la conexión a otros dispositivos, SSH permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir contraseñas al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH y también puede redirigir el tráfico del (Sistema de Ventanas X) para poder ejecutar programas gráficos remotamente. El puerto TCP asignado es el 22.

2.2.6 Layer 2 Tunneling Protocol (L2TP)

Es un protocolo utilizado por redes privadas virtuales que 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 de datos, incluyendo X.25, Frame Relay y ATM.

2.2.7 MODELO OSI

Es un modelo de referencia para los protocolos de la red (no es una arquitectura de red), creado en el año 1980 por la Organización Internacional de Normalización (ISO). Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones

(UIT) y, desde 1984, la Organización Internacional de Normalización (ISO) también lo publicó con estándar. Su desarrollo comenzó en 1977.

Es un estándar que tiene por objetivo conseguir interconectar sistemas de procedencia distinta para que estos pudieran intercambiar información sin ningún tipo de impedimentos debido a los protocolos con los que estos operaban de forma propia según su fabricante.

Para mediados de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones no podían intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de conexiones propietarias. Una tecnología es llamada “propietaria” cuando su implementación, (ya sea de software o hardware) está sujeta a un copyright. Esto supone que una empresa controla esta tecnología y las empresas que quieran utilizarla en sus sistemas tienen que pagar derechos por su uso. Las tecnologías de conexión que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes e incluso con las que usen reglas de conexión copyleft.

Para enfrentar el problema de incompatibilidad de redes, la ISO investigó modelos de conexión como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (Systems Network Architecture, SNA) y TCP/IP, a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

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. (Ver Figura 3).

Figura 3. Modelo OSI

Fuente: El autor

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.

2.2.7.2 Modelo de referencia OSI

Es un estándar desarrollado en 1980 por la ISO, una federación global de organizaciones que representa aproximadamente a 160 países. El núcleo de este estándar es el modelo de referencia OSI, una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.

El modelo especifica el protocolo que debe usarse en cada capa, y suele hablarse de modelo de referencia ya que se usa como una gran herramienta para la enseñanza de comunicación de redes.

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

Este modelo está dividido en siete (7) capas o niveles.

2.2.7.3 Capa Física – Capa 1

Es la capa más baja del modelo OSI. Es la que se encarga de la topología de red y de las conexiones globales de la computadora hacia la red, se refiere tanto al medio físico como a la forma en la que se transmite la información.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), cable coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.

- Manejar las señales eléctricas del medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de dicha conexión).

2.2.7.4 Capa de enlace de datos – Capa 2

Esta capa se ocupa del direccionamiento físico, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo.

Es uno de los aspectos más importantes que revisar en el momento de conectar dos ordenadores, ya que está entre la capa 1 y 3 como parte esencial para la creación de sus protocolos básicos (MAC, IP), para regular la forma de la conexión entre computadoras, determinando el paso de tramas (unidad de medida de la información en esta capa, que no es más que la segmentación de los datos trasladándolos por medio de paquetes), verificando su integridad, y corrigiendo errores.

Por lo cual es importante mantener una excelente adecuación al medio físico (los más usados son el cable UTP, par trenzado o de 8 hilos), con el medio de red que redirecciona las conexiones mediante un router.

Dadas estas situaciones cabe recalcar que el dispositivo que usa la capa de enlace es el Switch que se encarga de recibir los datos del router y enviar cada uno de estos a sus respectivos destinatarios (servidor - computador cliente o algún otro dispositivo que reciba información como teléfonos móviles, tabletas y diferentes dispositivos con acceso a la red, etc.), dada esta situación se determina como el medio que se encarga de la corrección de errores, manejo de tramas, protocolización de datos (se llaman protocolos a las "reglas de cortesía" o convenciones que debe seguir cualquier capa del modelo OSI).

2.2.7.5 Capa de red – capa 3

Se encarga de identificar el enrutamiento existente entre una o más redes. Las unidades de datos se denominan paquetes, y se pueden clasificar en protocolos enrutables y protocolos de enrutamiento.

- Enrutables: viajan con los paquetes (IP, IPX, APPLETALK)

- Enrutamiento: permiten seleccionar las rutas (RIP, IGRP, EIGRP, OSPF, BGP)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente, sino que utilicen dispositivos intermedios. Los dispositivos que facilitan tal tarea se denominan encaminadores o enrutadores, aunque es más frecuente encontrarlo con el nombre en inglés routers. Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de determinadas máquinas o limitar el acceso a ciertas de ellas.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

2.2.7.6 Capa de Transporte – Capa 4

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independientemente del tipo de red física que esté utilizando.

La PDU (unidad de información) de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP, el primero orientado a conexión (transmisión verificada, eventualmente retransmitida) y el otro sin conexión (pueden perderse algunos datos por el camino). Trabajan, por lo tanto, con puertos lógicos y junto con la capa red dan forma a los conocidos como Sockets IP:Puerto (ejemplo: 191.16.200.54:80).

2.2.7.7Capa de Sesión – Capa 5

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones

definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

2.2.7.8 Capa de Presentación – Capa 6

El objetivo es encargarse de la representación de la información, de manera que, aunque distintos equipos puedan tener diferentes representaciones internas de caracteres, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. Por ejemplo, un mismo sitio web puede adecuar la presentación de sus datos según se acceda desde un computador convencional, una tableta, o un teléfono inteligente.

Esta capa también permite cifrar los datos y comprimirlos. Por lo tanto, podría decirse que esta capa actúa como un traductor.

2.2.7.9 Capa de Aplicación – Capa 7

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (Post Office Protocol y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación, pero ocultando la complejidad subyacente.

2.2.7.10 Unidad de Datos en modelo OSI

El intercambio de información entre dos capas OSI consiste en que cada capa en el sistema fuente le agrega información de control a los datos, y cada capa en el sistema de destino analiza y quita la información de control de los datos como sigue:

Si una computadora (A) desea enviar datos a otra (B), en primer término, los datos deben empaquetarse a través de un proceso denominado encapsulamiento, es decir, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.

N-PDU

La unidad de datos de protocolo (N-PDU) es la información intercambiada entre entidades pares, es decir, dos entidades pertenecientes a la misma capa pero en dos sistemas diferentes, utilizando una conexión N-1. Está compuesta por:

- N-SDU (Unidad de Datos del Servicio): son los datos que necesitan la entidades N para realizar funciones del servicio pedido por la entidad N+1.
- N-PCI (Información de Control del Protocolo): información intercambiada entre entidades N utilizando una conexión N-1 para coordinar su operación conjunta.

N-IDU

La Unidad de Datos de Interfaz (N-IDU): es la información transferida entre dos niveles adyacentes, es decir, dos capas contiguas. Está compuesta por:

- N-ICI (Información de Control de Interfaz): información intercambiada entre una entidad N+1 y una entidad N para coordinar su operación conjunta.
- Datos de Interfaz-(N): información transferida entre una entidad-(N+1) y una entidad-(N) y que normalmente coincide con la (N+1)-PDU.

2.2.7.11 Transmisión de Datos en modelo OSI

La capa de aplicación recibe el mensaje del usuario y le añade una cabecera constituyendo así la PDU de la capa de aplicación. La PDU se transfiere a la capa de aplicación del modo destino, este elimina la cabecera y entrega el mensaje al usuario. (Ver figura 4).

Para ello ha sido necesario todo este proceso:

- Ahora hay que entregar la PDU a la capa de presentación para ello hay que añadirle la correspondiente cabecera ICI y transformarla así en una IDU, la cual se transmite a dicha capa.
- La capa de presentación recibe la IDU, le quita la cabecera y extrae la información, es decir, la SDU, a esta le añade su propia cabecera (PCI) constituyendo así la PDU de la capa de presentación.
- Esta PDU es transferida a su vez a la capa de sesión mediante el mismo proceso, repitiéndose así para todas las capas.
- Al llegar al nivel físico se envían los datos que son recibidos por la capa física del receptor.
- Cada capa del receptor se ocupa de extraer la cabecera, que anteriormente había añadido su capa homóloga, interpretarla y entregar la PDU a la capa superior.
- Finalmente, llegará a la capa de aplicación, la cual entregará el mensaje al usuario.

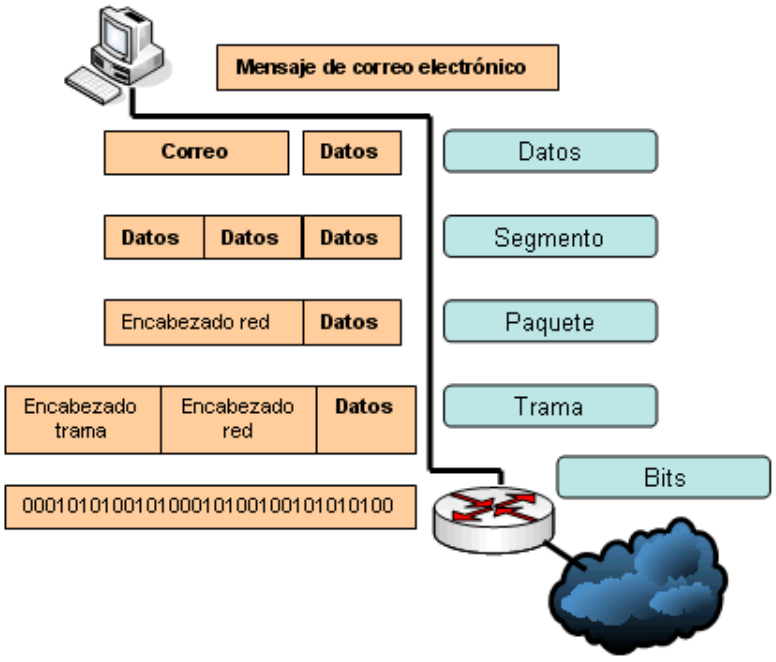


Figura 4. Transferencia de datos en modelo OSI

Fuente: El autor

2.2.8 Windows Server 2012

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. (Ver Figura 5).

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

El acceso remoto se puede instalar utilizando el Asistente para agregar roles y características. El rol del servidor agrupa tres tecnologías involucradas en el acceso a la red: el Servicio de enrutamiento y acceso remoto, DirectAccess y el Proxy de aplicación web.

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

Figura 5. Logo Windows Server 2012

Fuente: El autor

2.2.9 Remote Authentication Dial-In User Service (RADIUS)

Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, 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 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. (Ver Figura 6).

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuándo 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. A menudo se utiliza SNMP para monitorear remotamente el servicio. 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).

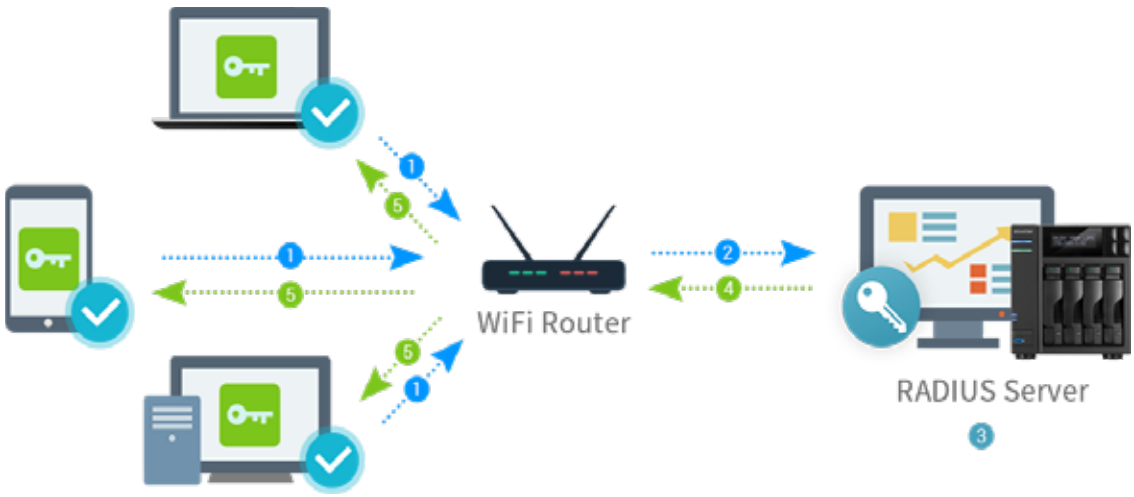


Figura 6. Esquema Servidor RADIUS

Fuente: El autor

2.3 Definiciones de términos básicos

Internet: es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen, constituyan una red lógica única de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California (Estados Unidos).

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW o la Web), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Esta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión.

Dirección IP: es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits expresado en código hexadecimal, para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado en la red.

La dirección IP puede cambiar muy a menudo debido a cambios en la red, o porque el dispositivo encargado dentro de la red de asignar las direcciones IP, decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se le denomina también dirección IP dinámica (normalmente abreviado como IP dinámica).

Modelo TCP/IP: es una descripción de protocolos de red desarrollado por Vinton Cerf y Robert E. Kahn, en la década de 1970. Fue implantado en la red ARPANET, la primera red de área amplia (WAN), desarrollada por encargo de DARPA, una agencia del Departamento de Defensa de los Estados Unidos, y

predecesora de Internet; por esta razón, a veces también se le llama modelo DoD o modelo DARPA.

El modelo TCP/IP es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

El modelo TCP/IP y los protocolos relacionados son mantenidos por la Internet Engineering Task Force.

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.

Ejemplos de interfaces en informática son las interfaces de usuario (entre computadora y persona) como sería una pantalla o un ratón (si hablamos de hardware) o la ventana gráfica de un programa con la que interactuamos (si hablamos de software); las interfaces físicas (entre dos dispositivos) como el SCSI o el USB; o las interfaces lógicas (entre dos programas) como la API o el DOM.

Ancho de banda: es la medida de datos y recursos de comunicación disponible o consumida expresados en bit/s o múltiplos de él como serían los Kbit/s,Mbit/s y Gigabit/s. Ancho de banda puede referirse a la capacidad de ancho de banda o ancho de banda disponible en bit/s, lo cual típicamente significa el rango neto de bits o la máxima salida de una huella de comunicación lógico o físico en un sistema de comunicación digital. También en telecomunicaciones, se conoce como banda ancha a cualquier tipo de red con elevada capacidad para transportar información que incide en la velocidad de transmisión de esta. Así entonces, es la transmisión de datos simétricos

por la cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva.

Velocidad de Transmisión: La velocidad de transmisión de datos es un promedio del número de bits, caracteres o bloques que se transfieren entre dos dispositivos, por una unidad de tiempo, usualmente segundos.

Otros nombres: data transfer rate, transfer rate, radio de transferencia de datos.

En otras palabras, es la cantidad de datos digitales que son movidos de un lugar a otro en un determinado tiempo. En general, mientras más grande sea el ancho de banda de un determinado canal o camino, más elevada será la velocidad de transmisión de datos.

La unidad de tiempo puede ser en milisegundos en ciertos casos como cuando se miden velocidades de transferencia de datos en el microprocesador o en la memoria RAM.

Velocidad de transmisión de datos en telecomunicaciones.

En telecomunicaciones, la tasa de transmisión de datos es usualmente medida en bits por segundo y sus múltiplos. Por ejemplo, una conexión de baja velocidad a internet puede ser de 33,6 kilobits por segundo (kbps). En una red de área local, la velocidad de transferencia puede ser de 100 megabits por segundo (mbps). Esto significa que se transfieren 33600 bits en un segundo y 100 millones de bits en un segundo, respectivamente. En sistemas de telecomunicaciones antiguos, la tasa de transferencia era a veces medida en caracteres o bloques (de cierto tamaño) por segundo.

Frame Relay: es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos.

La técnica Frame Relay se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.

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

Según Mijares y Garcia (2007) … “La metodología es una creación personal, cuyas técnicas e instrumentos a utilizar para la recopilación de datos, pueden resultar convenientes a los objetivos que se persiguen; las conformaciones de los mismos tienen que estar en perfecta concordancia con los objetivos de la investigación.” (p. 14).

Según Arias (2012) … “La metodología del proyecto incluye el tipo o tipos de investigación, las técnicas y los instrumentos que serán utilizados para llevar a cabo la indagación. Es el cómo se realizará el estudio para responder al problema planteado.” (p. 111).

Por ende, se presenta en el siguiente capítulo el abordaje metodológico llevado a cabo para cubrir el problema planteado de como Proponer el diseño de la red privada virtual de acceso remoto para la empresa Axe Telecom. 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 los cuales serán de gran apoyo para la elaboración de dicho trabajo y lograr diseñar la red VPN para beneficio de los empleados, clientes y de la empresa.

3.1 Tipo de Investigación

La investigación seleccionada para el siguiente trabajo de grado es de tipo factible.

Según Mijares y García (2007) …La investigación de proyectos factibles “Consistirá en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organización o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos.” (p. 6)

3.2 Nivel de la Investigación

Según Arias (2012) …" En esta sección se indica el tipo de investigación según el nivel o grado de profundidad con el que se realizara el estudio. En este sentido la investigación podrá ser exploratoria, descriptiva o explicativa. En cualquiera de los casos es recomendable justificar el nivel adoptado." (p. 110).

Según Arias (2012) … "El nivel de investigación se refiere al grado de profundidad con que se aborda un fenómeno u objeto de estudio." (p. 23)

El tipo de investigación seleccionada para el trabajo especial de grado sobre el diseño de red VPN de acceso remoto para la empresa Axe Telecom es la investigación descriptiva; a continuación, una cita de Fidias Arias.

Según Arias (2012) … "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."

3.3 Diseño de la investigación

El diseño de la investigación seleccionado en este caso es el documental y de campo ya que con la ayuda de trabajos previos y con el desarrollo de dicha red y las tecnologías que estas lo acompañan se diseñara la red VPN.

Según Arias (2012) … "El diseño de la investigación es la estrategia general que adopta el investigador para responder al problema planteado. En atención al diseño, la investigación de documental, de campo y experimental." (p. 27).

3.4 Población y Muestra

El termino Población Según Balestrini (2001) **se** refiere a …" cualquier conjunto de elementos de los que se quiere conocer o investigar alguna o alguna de sus características." (p. 110).

Según Arias (2012) ... "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. Esta queda delimitada por el problema y los objetivos de estudio." (p. 81).

En este caso el conjunto de todos los departamentos que conforman el grupo de trabajo de Axe Telecom será la población a estudiar. De manera que cuando se tome de manera aleatoria usuarios conectados vía remota o algunos físicamente dentro de la empresa serán parte de nuestra muestra.

Según Morales (1994) la Muestra es un…" subconjunto representativo de un universo o población." (p. 54).

3.5 Técnicas e Instrumentos de Recolección de Datos.

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

En el presente trabajo se utilizará la técnica de revisión documental con información que nos suministre la investigación, la observación directa utilizando lista de cotejo y check list y la encuesta de tipo escrita.

Según Arias, F. (2012, P.68), "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."

En el presente trabajo contaremos con el apoyo de instrumentos electrónicos como laptops, cámaras fotográficas, teléfonos celulares y libretas de nota.

3.6 Técnicas de Procesamiento y Análisis de Datos.

En este punto se describen las distintas operaciones a las que serán sometidos los datos que se obtengan: clasificación, registro, tabulación y codificación si fuere el caso. En lo referente al análisis, se definirán las técnicas lógicas (inducción, deducción, análisis-síntesis), o estadísticas (descriptivas o inferenciales), que serán empleadas para descifrar lo que revelan los datos recolectados.

3.7 Fases de la investigación

3.7.1 Fase I "Diagnostico de condición actual de la red de comunicación de la empresa Axe Telecom."

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.

3.7.2 Fase II "Identificación fallas y puntos críticos de la red de comunicación de la empresa Axe Telecom."

En este punto se identificarán los puntos más vulnerables de la red, en cuanto a su seguridad y que protocolos se deberían aplicar para el resguardo de la información y de quienes mediante Windows server tendrán acceso o no a la red VPN.

3.7.3 Fase III "Diseño de la red privada virtual (VPN) de acceso remoto a la red de local empresarial de Axe Telecom."

En esta fase se realizará 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 cualquiera de los departamentos de la empresa, la cual estará basada en un modelo de cliente servidor, que recopilará la información del software y hardware del diseño.

3.7.4 Fase IV "Estudio de factibilidad técnica, económica, social y ambiental para la implementación de la propuesta."

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 Axe Telecom 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 VPN. 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 de métodos, procedimientos y funciones requeridas para el desarrollo e implantación del proyecto. Factibilidad 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

En este capítulo se presenta de manera detallada cada una de las fases las cuales con la información recolectada se indica cómo lograr de manera exitosa la culminación del trabajo de grado, comenzando por la condición actual de la red de comunicación de la empresa donde se aprecian fotos del cuarto de servidor como evidencia, además de la tabla de cotejo donde indica los requerimientos necesarios para la elaboración del trabajo y del diseño de la red local con el programa Packet Tracer.

4.1 Fase I: Diagnostico de condición actual de la red de comunicación de la empresa Axe Telecom.

Para determinar la situación actual en la que se encuentra la infraestructura de red de comunicaciones, se realiza una inspección del cuarto de servidor (Figura 8) donde observamos y detallamos los parámetros y condiciones en la cual trabaja esta infraestructura.

Se observa en la (Figura 7) el rack donde están instalados los diferentes equipos de la red interna como switch, router y Servidor, el cual en conjunto hacen vida a la red.

Axe desea comunicar todos sus usuarios externos y clientes mediante una red de recursos de carácter público, manteniendo el mismo sistema y mismas políticas de acceso que se usan en las redes privadas.

Para el diseño de la Red Privada Virtual (VPN) tendremos en cuenta la estructura de la red LAN de la empresa, es decir, cuantos equipos estarán conectados, que protocolos se implementarán para la comunicación y seguridad de la información, dispositivos empleados y direccionamiento. Con base a la información obtenida, se

realizarán ajustes a la red LAN y se configurara la Red Privada Virtual en los equipos locales y remotos.

Figura 7. Rack de Servidor y Equipos

Fuente: El Autor

Figura 8. Cuarto de Servidor

Fuente: El Autor

Figura 9. Instalaciones de la empresa

Fuente: El Autor

Figura 10. Cubiculo Administracion

Fuente: El Autor

Figura 11. Gerencia

Fuente: El Autor

Figura 12. RRHH

Fuente: El Autor

Con el presente trabajo la empresa también se beneficiará ya que esta ampliará y unificará su red privada más allá de su área geográfica, empleando una red pública como internet, reduciendo los costos frente a las conexiones WAN y obteniendo las mismas ventajas en seguridad, productividad y oportunidades en comunicación adicionales. Con el fin de recopilar, analizar y verificar las necesidades del cliente, se tendrá en cuenta el manejo de las funciones que sistema será capaz de realizar y las limitantes que se puedan presentar en la implementación tales como fiabilidad, rendimiento, mantenimiento, portabilidad, en otras.

Los requerimientos que se tendrán en cuenta para el diseño se especifican en la Tabla 1.

Los involucrados en el desarrollo del sistema son:

- Usuarios Internos
- Usuarios Externos
- Red LAN
- Red VPN
- Clientes

4.1.1 Requerimientos Funcionales

Red LAN

- Determinar cuántos equipos estarán conectados en la red LAN mediante recopilación de información, con el fin de realizar el direccionamiento IP a cada subred, permitiendo que cada equipo sea identificado dentro de la red, para la identificación y diseño de la red será utilizado el programa de simulación de redes Packet Tracer 7.2.2.
- Identificar los dispositivos (Switch, Router, Tarjetas Ethernet NIC) a utilizar en la red.
- Configurar las tarjetas de red de cada uno de los equipos, teniendo en cuenta el direccionamiento IP en cada subred.

Red VPN

- Identificación de usuarios, es decir, que la VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a los no autorizados mediante el servidor VPN que realiza la autentificación de acceso.
- Establecer una dirección del cliente en la Red Privada y que esta se conserve
- Encriptar los datos a través de los túneles VPN para que no puedan ser leídos
- Generar y renovar claves para el cliente y el servidor
- Intercambio de información en tiempo real y disponibilidad de esta sin importar la ubicación de usuario.
- Interconexión total a la red de todos los usuarios tanto internos como externos de forma segura a través de una infraestructura pública.
- Flexibilidad y facilidad de uso en el ingreso remoto a los aplicativos de la empresa.

4.1.2 Requerimientos No Funcionales

- La Red LAN y VPN deben funcionar en los sistemas operativos Windows 7,8,10 ya que los equipos de la empresa cuentan con Windows.

- Los usuarios deben ser capaces de utilizar todas las funciones de la red VPN, tras un entrenamiento que se les dará a los empleados.
- El sistema controlara la valides y coherencia de los datos ingresados en la conexión VPN.

Tabla 1. Lista de Cotejo de los requerimientos en el cuarto de Servidor.

Lista de Cotejo de los requerimientos principales	
Área Física	
Área 4x3 m^2	ok
Conexión de red	ok
Techo falso	ok
Recubriendo de suelo con goma anti golpe	ok
Salida de emergencia	ok
Rack Bastidor 2,13m 19”	ok
Suministro de energía eléctrica	
Diferentes puntos de tomacorriente	ok
UPS	ok
Planta electica	ok
Control de Clima	
Aire Acondicionado 18000BTU	ok
Deshumificador	ok
Control Preventivo	
Aspersores	ok
Extintor	ok
Desagües	ok

Con base a la formulación y recopilación de información obtenida al principio del trabajo de grado se obtuvo la siguiente información sobre la estructura física de la empresa.

Tabla 2. Distribución de los departamentos de la empresa.

Departamento	Numero de Host
Gerencia	1
Ingeniería	3
Implementación	2
Administración	1
RRHH	1
Total	**8**

Mediante la investigación se realiza una comparación (tabla 3) en la cual se podrá ver un conjunto de opciones para el obtener acceso vía remota a la red LAN y usuarios externos en la cual se detallan sus características, ventajas y desventajas una con respecto a la otras para determinar la mejor opción a elegir para el problema que presenta la empresa y establecer una comunicación de manera confiable, segura y privada.

Tabla 3. Comparación de características y diferentes de conexiones remotas

Conexiones Vía Remota Ventajas y Desventajas			
VPN	**Escritorio Remoto**	**Frame Relay**	**Punto a Punto**
Permite acceder a otra Red	Permite acceder a otra dispositivo o sistema	Permite acceder a otra red LAN	Acceso a otra equipo
Servicio de Cifrado	No cuenta con Cifrado de datos	No garantiza entrega de datos	Fáciles de configurar
Conexión simultanea de varios usuarios	Conexión de un solo Usuario	Conexión entre usuarios a través de red publica	No son escalables
Acceso mediante Internet	Acceso mediante Internet	Acceso mediante red publica	Línea Dedicada
Seguridad de que terceros no intercedan	No garantiza la confidencialidad	Viaja por canales dedicados	No son muy seguras
Costo de implementación bajo	Costo de implementación bajo	Costo de implementación bajo	Los cotos de cableado dependen del número de enlaces entre estaciones
Funciona en múltiples dispositivos ya que no hace falta instalar o descargar app	El programa de escritorio remoto viene instalado en los equipos llamado (RDP) o se puede instalar otros programas (Teamviewer-Anydesk)	Protocolo que se configura en router, switch para trabajar en una misma red	Los dispositivos actúan como cliente y servidor y disminuye el funcionamiento

Entre la comparación de todos estos accesos vía remota podemos destacar que la mejor opción para el trabajo de grado que beneficie a la empresa y su comunicación entre otras sedes, clientes o usuarios remotos es la red VPN ya que la misma ofrece seguridad, cifrado, autentificación, fiabilidad, rapidez en el transporte de datos y a un bajo costo de implementación.

Configuración LAN de la empresa

En la conexión de la red de área local de la empresa, se emplean dos arquitecturas de red:

- La tecnología Ethernet también conocido como estándar IEEE 802.3, el cual se basa en que todos los equipos en una red Ethernet están conectados a la misma línea de comunicación compuesta por cables de red cilíndricos. Con esta arquitectura se tendrá en cuenta el cableado, infraestructura física y direccionamiento local de cada uno de los terminales y equipos intermediarios.

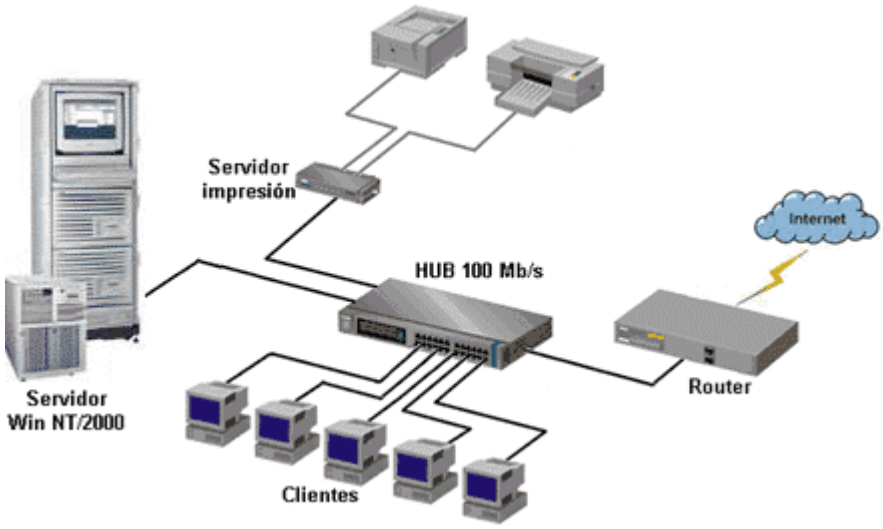


Figura 13. Tecnología Ethernet

Fuente: El Autor

· Tecnología WIFI o especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de la red de área local inalámbrica (WLAN), con base en esta tecnología se tendrá en cuenta las características de señalización para la transmisión de datos.

  En la empresa se empleará tanto la red Ethernet como la red WIFI para empleados que requieran de una oficina móvil local que permita al igual que la tecnología Ethernet transmitir y recibir datos, compartir periféricos, acceso a un servidor, navegar a través de internet a velocidades de 54 Mbps o hasta 300 Mbps.

Figura 14. Tecnología WIFI

Fuente. El Autor

4.2 Fase II: Identificación de fallas y puntos críticos de la red de comunicación de la empresa Axe Telecom.

Al desarrollar la Red Privada Virtual (VPN) se debe detectar las vulnerabilidades que se pueden presentar en la red de la empresa, entre las fallas se encuentran:

4.2.1 La autentificación del usuario y restringir el acceso a los usuarios no autorizados. Si no se contara con este requerimiento, cualquier persona malintencionada podría conectarse a los recursos e información de la red local. Con la ayuda de Windows Server 2012 R2 se podrá crear y permitir el acceso a los usuarios tanto internos como externos, incluyendo a los clientes para que estos puedan ingresar mediante la red VPN, los cuales con el proceso de autentificación se comprobara que realmente tienen los permisos de conexión, actualmente la empresa no cuenta con ese sistema de autentificación.

4.2.2 Otro factor importante a tener en cuenta es la red local (LAN), ya que, a partir del buen funcionamiento, su correcto direccionamiento ip de los terminales tanto los PC como las impresoras, router, switch y servidores y adecuada distribución de esta, se puede lograr un balance de cargas entre los usuarios internos como externos, de lo contrario podrían generarse colisiones entre los paquetes y por ende perdida de información, generando problemas de interconectividad tanto en la red LAN con WAN, con una tabla de direccionamiento se tendrá un control de qué dirección ip tiene asignado cada equipo y cuales servirán para los clientes externos.

4.2.3 Al momento de conectar la red LAN y lo usuarios remotos, se debe implementar el mismo protocolo para evitar incompatibilidad en la conexión o comunicación en él envió y recepción de los mensajes ya que actualmente la empresa no cuenta con ningún protocolo de seguridad, al realizar el diseño la red VPN cuenta con diferentes protocolos de seguridad entre los que están SSL, TTL, PPTP e IPSec.

4.2.4 Otros factores que se tendrán en cuenta y que generarían fallos a la red son la configuración inadecuada del servidor, más adelante se verá la configuración del servidor; también alguna falla del cableado estructurado generando demoras e interferencias en la transmisión de los datos lo cual siempre es recomendable verificar

la conexión del cable de red en todos sus puntos tanto en la PC como la conexión del punto de la pared o de las conexiones a los switch y router.

4.2.5 Proveedor de servicios de internet, la empresa cuenta de momento solamente con un proveedor de internet, en este caso CANTV lo cual es un punto crítico vulnerable ya que no se cuenta con un respaldo del servicio, permitiendo una posible falla latente a la hora de ser interrumpido este servicio, siempre es recomendable contar con un segundo proveedor de servicios para garantizar la conexión cuando alguno de los 2 servicios sufra una caída repentina.

Una vez identificados los puntos vulnerables para la implementación de la Red Privada Virtual (VPN) en la empresa, se tendrán en cuenta y se trabajara principalmente en ellos para evitar inconsistencias en la red. Como la red VPN emplea una infraestructura pública, se emplearán un sistema de encriptación y autentificación mediante túneles virtuales entre la empresa y usuarios externos, asegurando la confidencialidad e integridad de los datos transmitidos a través de internet, también se tendrá el protocolo de túnel de VPN a implementar en la red, el cual debe ser compatible con la configuración WAN y LAN.

4.3 Fase III: Diseño de la red privada virtual (VPN) de acceso remoto a la red local empresarial de Axe Telecom.

Se realizo el diseño de la red empresarial para establecer la normativa del cableado dependiendo de los dispositivos a conectar, también se establecerá el direccionamiento LAN y WAN, configuración de los equipos para que estos trabajen con la red VPN.

Con base a la información obtenida al comienzo del trabajo de grado sobre la cantidad de equipos necesarios, se realizará la división de las subredes a partir de la dirección de red 192.168.0.0.

El diseño LAN se realizó de la siguiente manera:

La empresa está conformada por cinco departamentos: Gerencia, Ingeniería, Implementación, Administración, Recursos Humanos, en la cual se maneja todo referente a la parte administrativa la realización de trabajos de ingeniería y el

departamento de implementación encargado de la instalación de todo lo planificado por Ingeniería.

El diseño de la red de esta se tendrá en cuenta la escalabilidad para que la red local pueda expandir y admitir nuevos usuarios y aplicaciones sin que se afecte el rendimiento del servicio. Cada host conectado debe contar con una dirección IP para poderse identificar y localizar dentro o fuera de la red y así lograr un punto de conexión.

Estos hosts tendrán una dirección IP lógica única que identifican la ubicación ya sea en la red local u otra diferente. Esta dirección IP es conocida como notación decimal conformada por 32 bits la cual está divida en dos partes, una parte corresponde a la red y otra a los host.

Con lo mencionado anteriormente podremos determinar que la red tendrá un segmento de red conformado por 10 host primeramente, en la red se tendrá en cuenta a los usuarios a futuro para no limitar la red local. El tipo de clase que se implementará será la clase C, la cual permite un máximo de 254 host con lo cual se trabajará por debajo de esa cantidad de host.

La red será simulada con el programa Packet Tracer versión 7.2.2, el cual nos permitirá configurar los dispositivos, realizar pruebas de conectividad, implementar protocolos de comunicación, entre otras actividades.

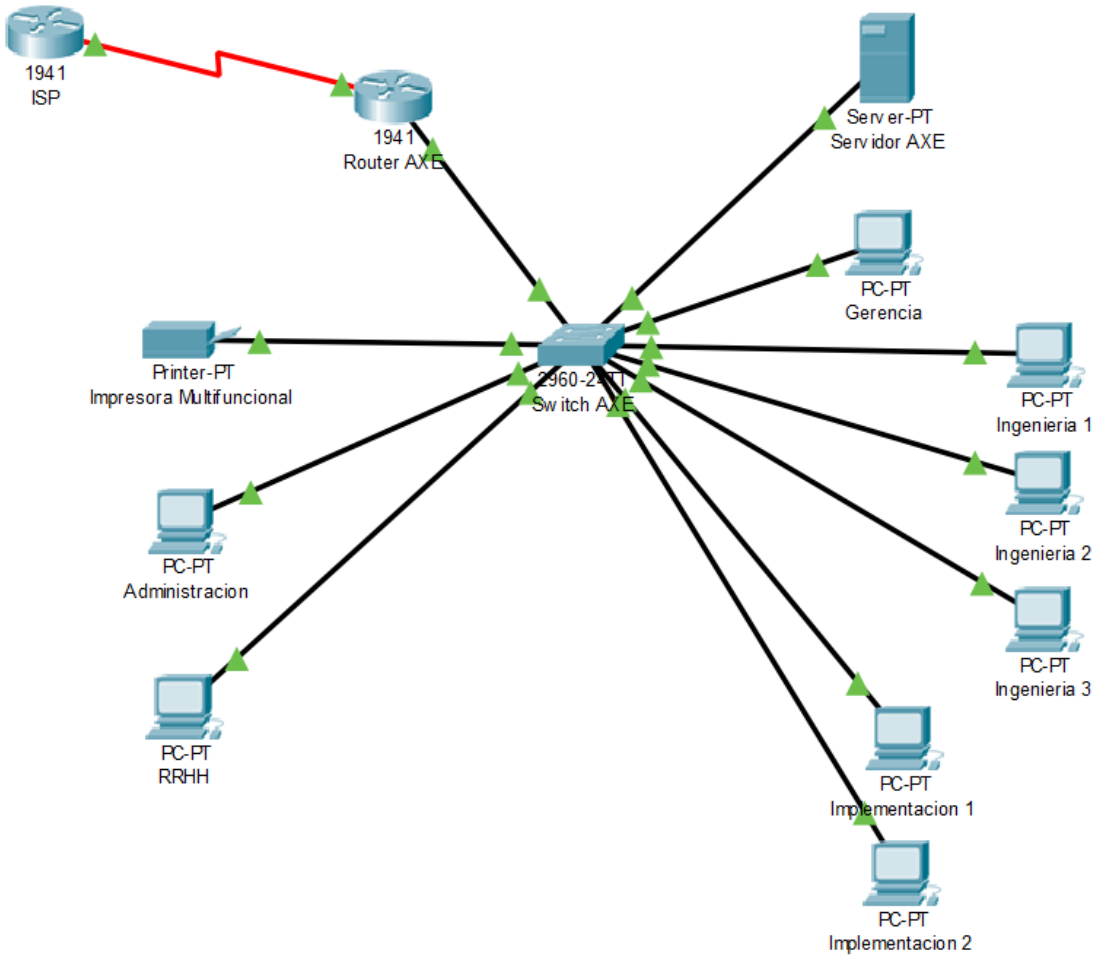


Figura 15. Topología de Red Local de la empresa

Fuente. El Autor

Tabla 4. Direccionamiento de red LAN de Axe Telecom.

Descripción	Interfaz	Dirección IP	Mascara Subred	Gateway
Router AXE	G0/0	192.168.0.1	255.255.255.224	N.A
	S0/0/0	201.210.70.244	255.255.255.252	N.A
Switch AXE	VLAN	192.168.0.30	255.255.255.224	192.168.0.1
Servidor AXE	F0/1	192.168.0.2	255.255.255.224	192.168.0.1
Gerencia	F0/2	192.168.0.5	255.255.255.224	192.168.0.1
Ingeniería 1	F0/3	192.168.0.10	255.255.255.224	192.168.0.1
Ingeniería 2	F0/4	192.168.0.11	255.255.255.224	192.168.0.1
Ingeniería 3	F0/5	192.168.0.12	255.255.255.224	192.168.0.1
Implementación 1	F0/6	192.168.0.15	255.255.255.224	192.168.0.1
Implementación 2	F0/7	192.168.0.16	255.255.255.224	192.168.0.1
Impresora	F0/8	192.168.0.3	255.255.255.224	192.168.0.1
Administración	F0/9	192.168.0.20	255.255.255.224	192.168.0.1
RRHH	F0/10	192.168.0.25	255.255.255.224	192.168.0.1

Tabla 5. Direccionamiento características secundarias

Dirección de Red	192.168.0.0
Broadcast	192.168.0.31
Mascara de subred	255.255.255.224
Prefijo	/27
Host Utilizables	30
Host Usados	10
Ampliable	20
1er IP valida	192.168.0.1
Ultima IP valida	192.168.0.30
Gateway	192.168.0.1
Descripción	RED AXE TLECOM

Realizada la tabla de direccionamiento IP se observa que la misma cuenta con una cantidad máxima de 30 host para lo cual se tiene en cuenta la escalabilidad en la red ya que solo se estarán utilizando primeramente 10 host, en un futuro la empresa podrá tener la opción de seguir ingresando más usuarios a la red local.

En el diseño de la red de la empresa Axe Telecom, se encuentra un Router Axe, enlazado al proveedor de servicios ISP y la red LAN. La red LAN corresponde a la estructura física, en ella encontramos un Switch llamado Switch Axe que está conectado directamente al Router Axe, por medio de un cable directo es decir con sus dos extremos iguales. Este switch está conectado finalmente a los host de los usuarios finales, como equipos, servidores, e impresoras, por cables directos de red. Cada uno de estos dispositivos están configurados con una dirección IP como se muestra en la Tabla 4, partiendo de la dirección de red 192.168.0.0 con mascara de subred /27 o 255.255.255.224. La simulación se realiza a través del programa Packet Tracer versión 7.2.2.

Una vez estructuradas las conexiones LAN y WAN en todas las sucursales de la empresa, se configura las VPNs a los equipos de la red local y usuarios remotos.

4.3.1 Configuración de Red VPN

En la configuración de la VPN se debe contar con:

- Conexión a internet rápida tanto para el servidor como para los equipos locales y remotos.
- Una dirección IP para los recursos a compartir.
- Una dirección IP para el servidor.
- El firewall debe estar inactivo en todo los PC que se van a conectar.

Elementos principales de la configuración de una red con VPN

- AXE TELECOM utiliza su red privada, con dirección IP 192.168.0.0 con mascara de subred 255.255.255.224.

- La dirección IP WAN en internet asignada por el proveedor de servicios de internet (ISP) de AXE con conexión ADSL, la dirección IP es 201.210.70.244.
- El servidor VPN que estará ubicado en la oficina, cuarto de servidor, el cual proporciona el enrutamiento de paquetes hacia ubicaciones en intranet o internet.

AXE desea comunicar sus usuarios internos y externos sin invertir mucho dinero en infraestructura como se ha mencionado anteriormente, por lo tanto, se quiere realizar una convergencia del modelo actual de la red diseñando y ofreciendo una tecnología que no requiera conexiones costosas y que sea confiable, estable y segura, además que garantice la calidad de los servicios de voz, video y datos sin que estos sean afectados entre sí.

Actualmente la red de AXE cuenta con la configuración LAN como se mostró anteriormente en el trabajo, pero el objetivo a lograr es permitir la comunicación sin necesidad de emplear canales dedicados, empleando la tecnología VPN.

La red VPN funciona sobre un canal público internet y reemplazando los canales dedicados por un protocolo de túnel, el cual cifra los datos que se transmiten desde un lado de la VPN a otra, impidiendo que la información sea comprensible para cualquiera que no se encuentre en los extremos de las VPNs

4.3.2 Direccionamiento del Servidor VPN

Para la configuración del servidor VPN y el cliente VPN, utilizaremos el siguiente direccionamiento en las tarjetas de red ethernet del servidor y el PC del cliente. El cliente entrara a la red por la IP del servidor.

Tabla 6. Direccionamiento IP del Servidor VPN

Direccionamiento del Servidor				
Dirección Red	Dirección IP	Mascara	Gateway	Descripción
192.168.0.0	192.168.0.2	255.255.255.224	192.168.0.1	Servidor AXE
192.168.0.0	192.168.0.29	255.255.255.224	192.168.0.2	Cliente VPN

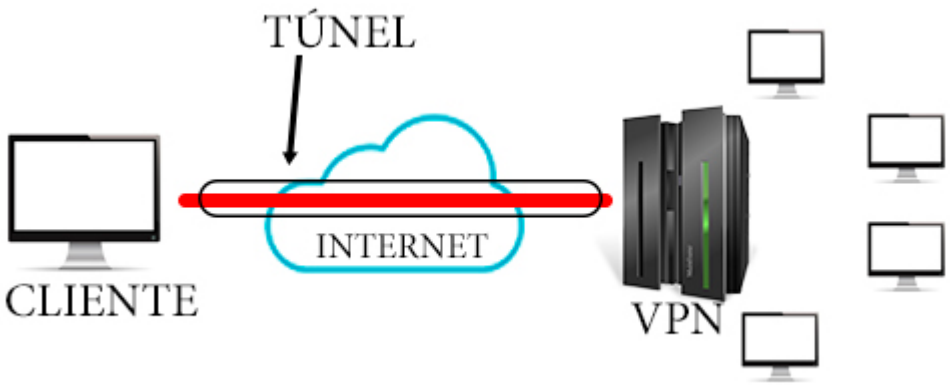


Figura 16. Esquema de Red VPN

Fuente: El Autor

Con la Red Privada Virtual (VPN), los datos se encapsulan o se envuelven con un encabezado que proporciona información de enrutamiento, lo que permite que los datos atraviesen la red compartida o publica hasta llegar a su punto de destino, de esta forma, los datos se cifran para conservar la confidencialidad, por lo tanto, los paquetes interceptados en la red compartida o publica no se pueden descifrar sin las claves de cifrado.

En la configuración del Servidor VPN tendremos dos opciones:

Si el equipo no es Servidor ni miembro de un dominio, las conexiones entrantes se configuran en Windows con el asistente para conexión de red que se utiliza para las conexiones salientes.

Si el equipo es Servidor y miembro de un dominio, para configurar conexiones entrantes las realizaremos mediante Server 2012 R2 a través de herramientas, enrutamiento y acceso remoto. El uso de esta herramienta puede ayudar a configurar redes privadas virtuales y conjuntos de módems en un servidor de acceso remoto.

Por medio del Servidor VPN los equipos remotos podrán interactuar con la Red LAN como si estuvieran dentro de esta, este Servidor será la puerta de enlace para comunicar los usuarios remotos con los locales.

4.3.3 Pasos para la configuración del Servidor VPN en Windows Server 2012 R2

1 –Para la configuración del Servidor VPN primero debemos habilitarlo, vamos a Inicio y click en Administrador del servidor y luego en agregar roles y características (Figuras 17 y 18).

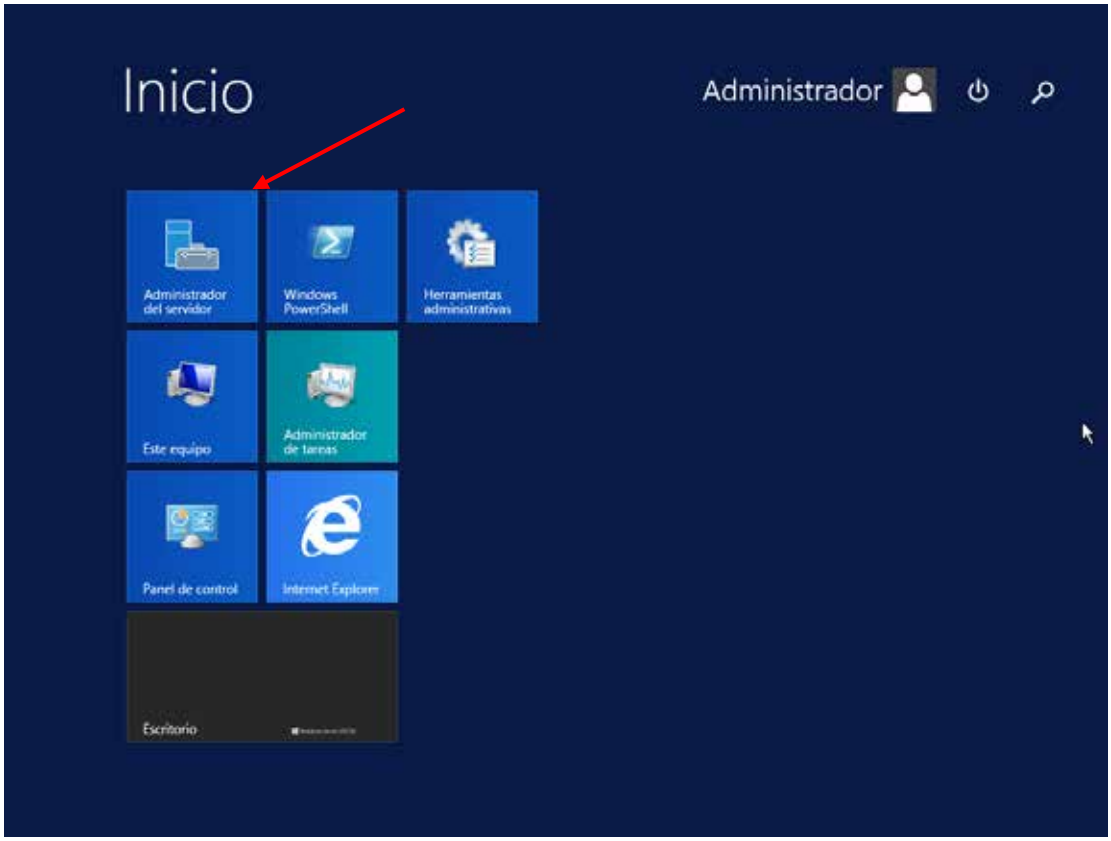


Figura 17. Menú Inicio- administrador del Servidor

Fuente: El Autor

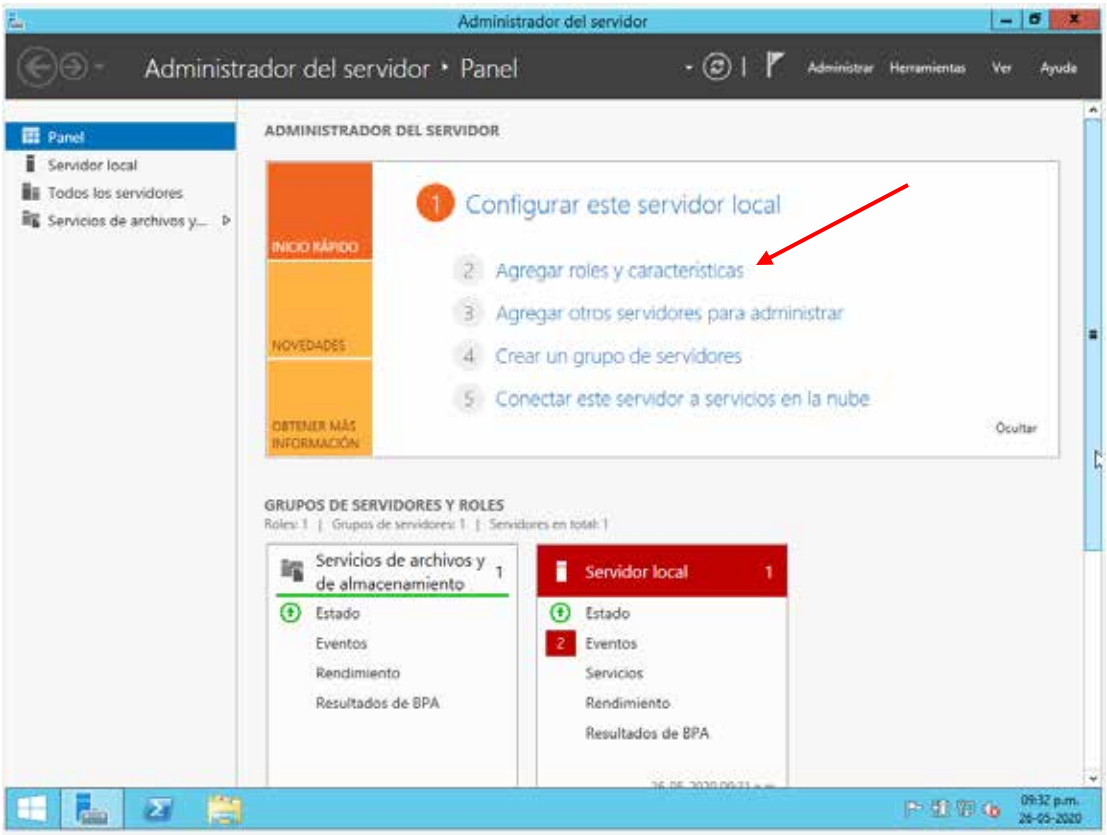


Figura 18. Agregar roles y características

Fuente: El Autor

Seguidamente en la pestaña **“Tipo de Instalación”**, verificamos que está marcada la opción **“Instalación basada en características o en roles”** y siguiente.

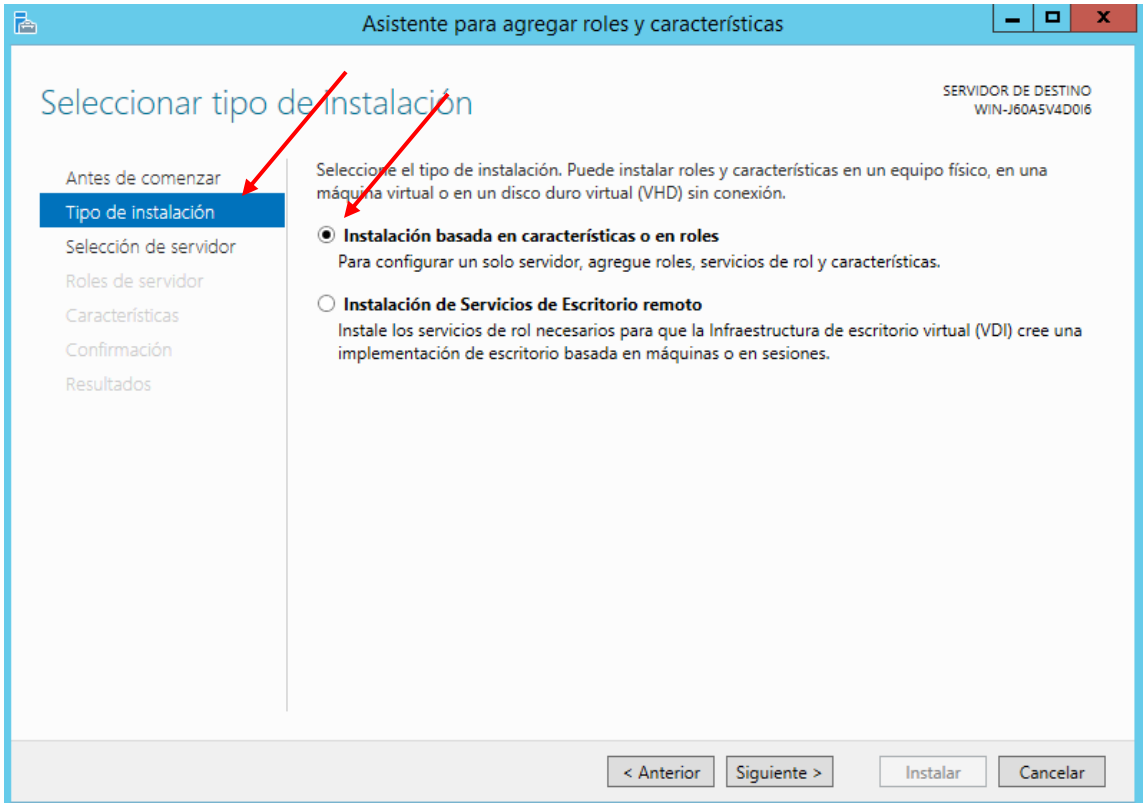


Figura 19. Pestaña Tipo de Instalación

Fuente: El Autor

.

En la pestaña de “Selección Servidor” verificamos que este marcado “Seleccionar un Servidor del grupo de Servidores” y corroboramos que este seleccionado nuestro Servidor, luego siguiente.

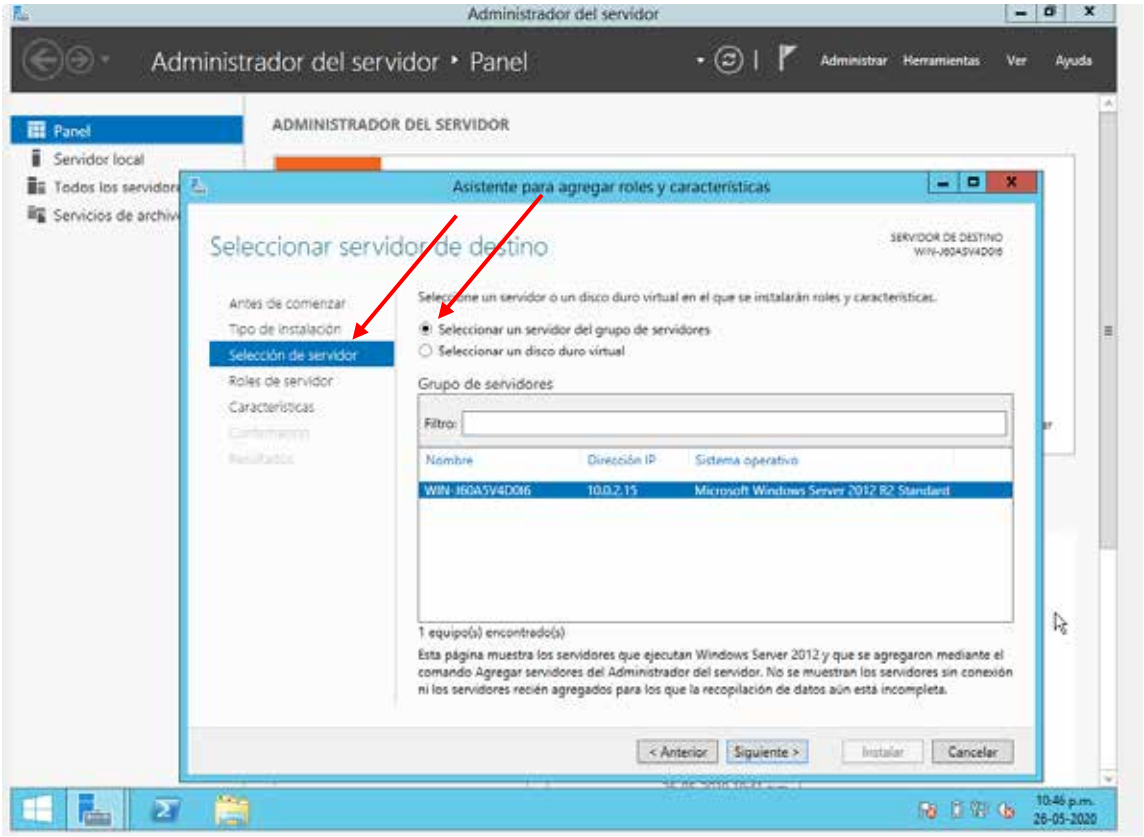


Figura 20. Pestaña Selección del Servidor

Fuente: El Autor

Seguidamente en la pestaña “Roles de Servidor” marcamos la opción de “Acceso Remoto” y siguiente.

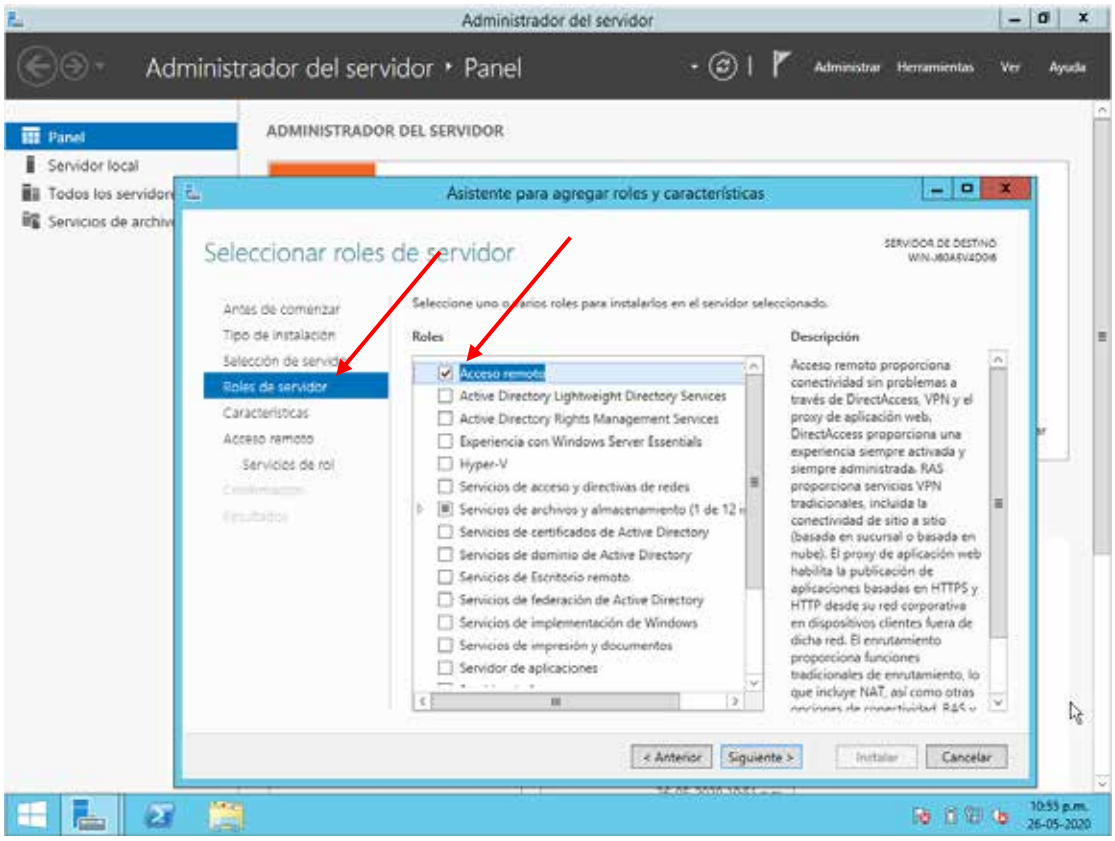


Figura 21. Pestaña Roles de Servidor

Fuente: El Autor

En **“Servicios de Rol”** tildamos la opción de **“Directaccess y VPN (RAS)”** nos aparece otra ventana y damos click a agregar esta característica marcamos la opción de **“Enrutamiento”** y siguiente hasta que nos de la opción de marcar Instalar. Ver (Figuras 22 y 23).

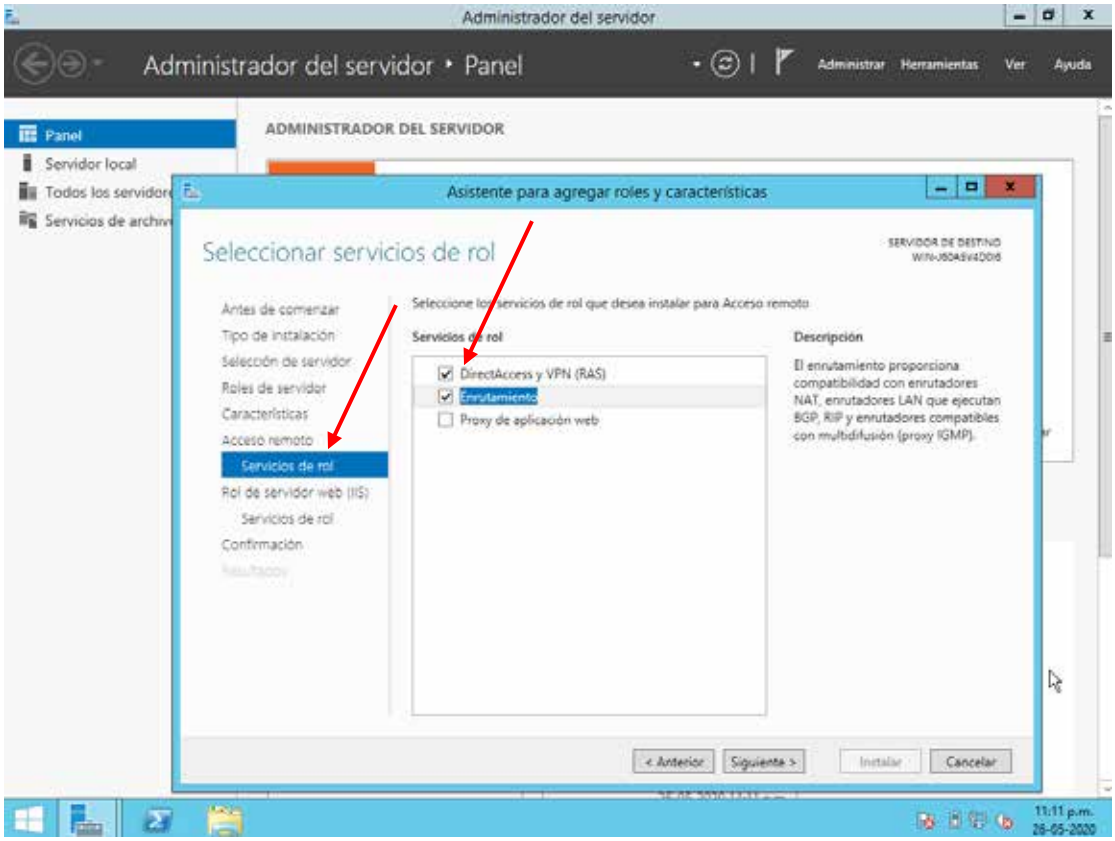


Figura 22. Pestaña Servicios de Rol

Fuente: El Autor

Marcamos la opción de Instalar y esperamos que se instale el Servidor VPN.

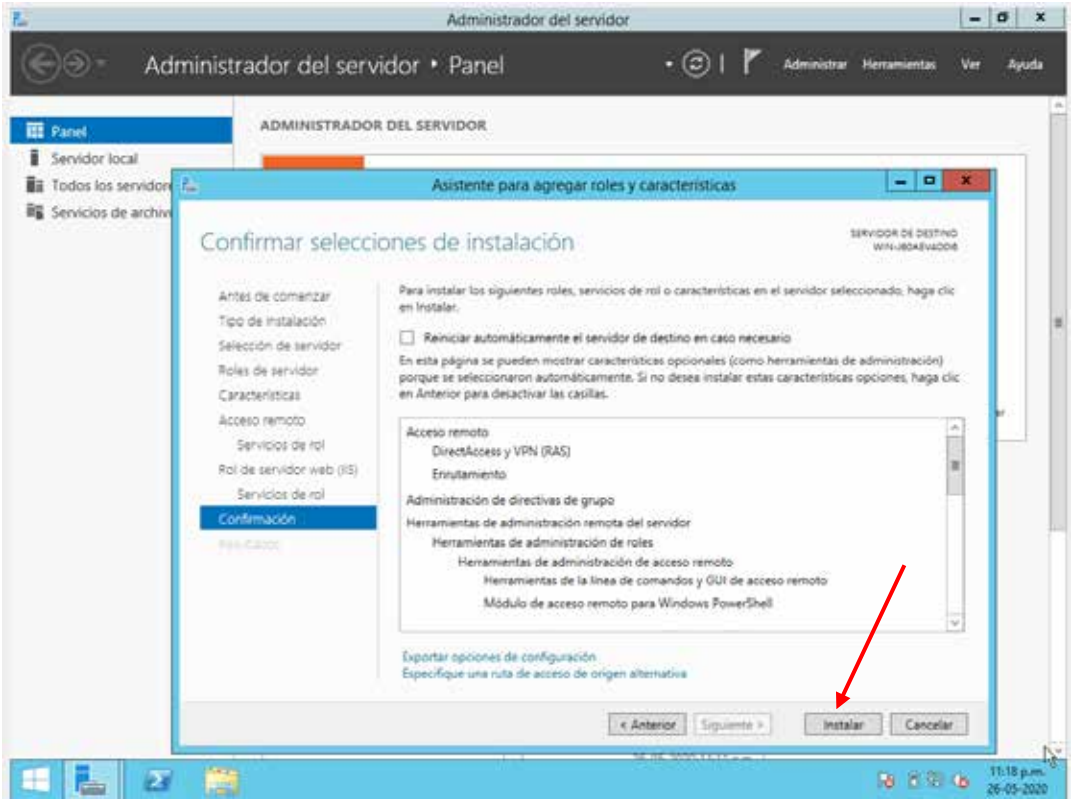


Figura 23. Instalar Servidor VPN

Fuente: El Autor

A continuación, damos click a “Abrir el asistente para introducción”

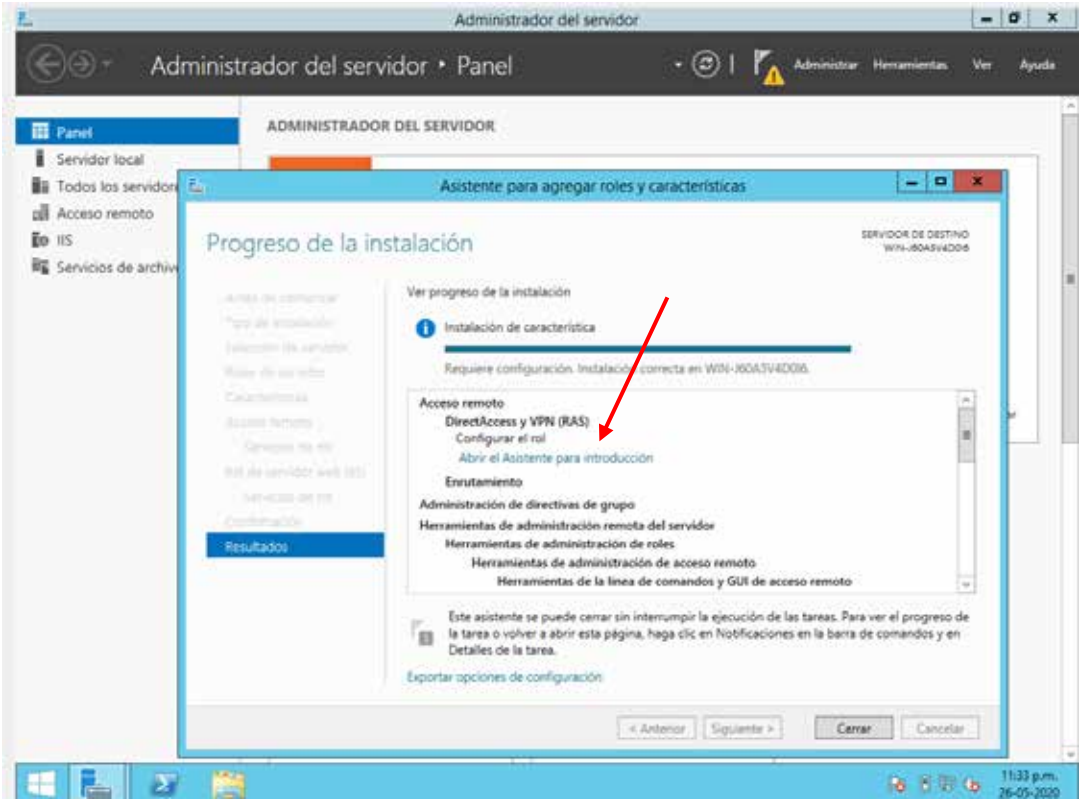


Figura 24. Abrir el Asistente para Introducción.

Fuente: El Autor

Nos aparece otra ventana en la cual marcaremos “Implementar solo VPN”, lo cual es exactamente lo que queremos.

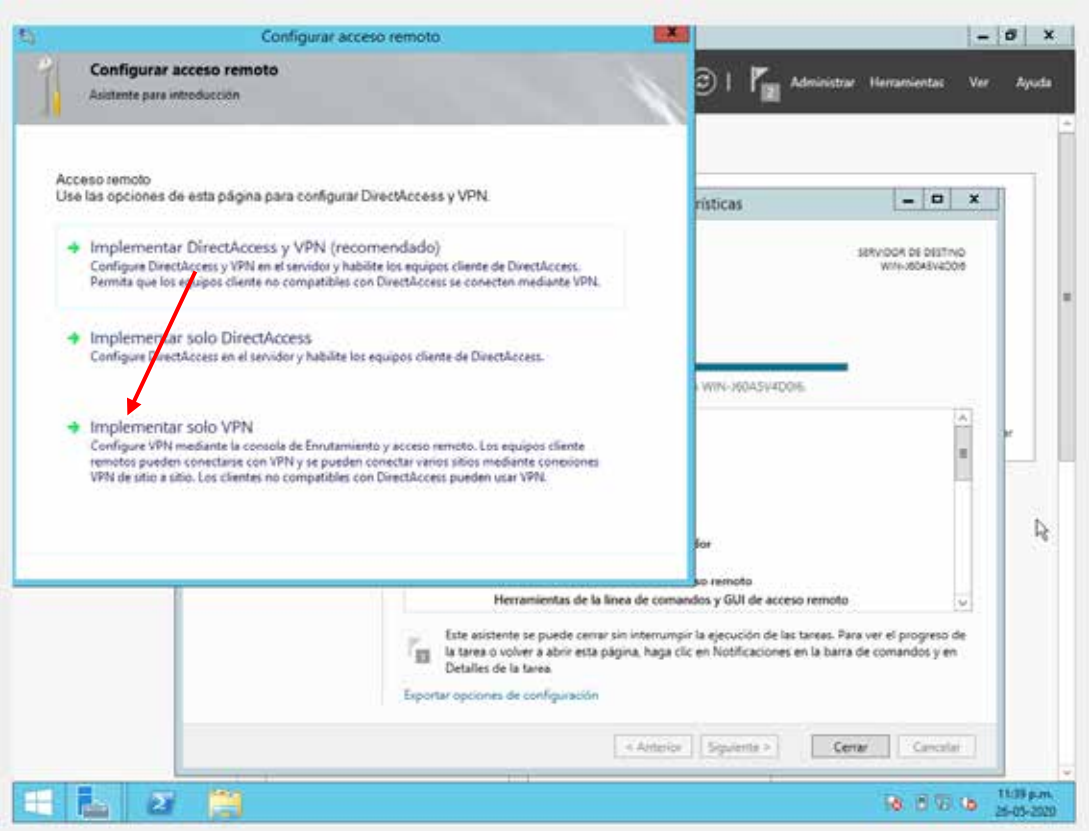


Figura 25. Implementar solo VPN

Fuente: El Autor

Seguidamente se observa nuestro servidor, en la barra del lado izquierdo el cual esta Down, marcado con una flecha roja hacia abajo lo que indica que no está configurado completamente.

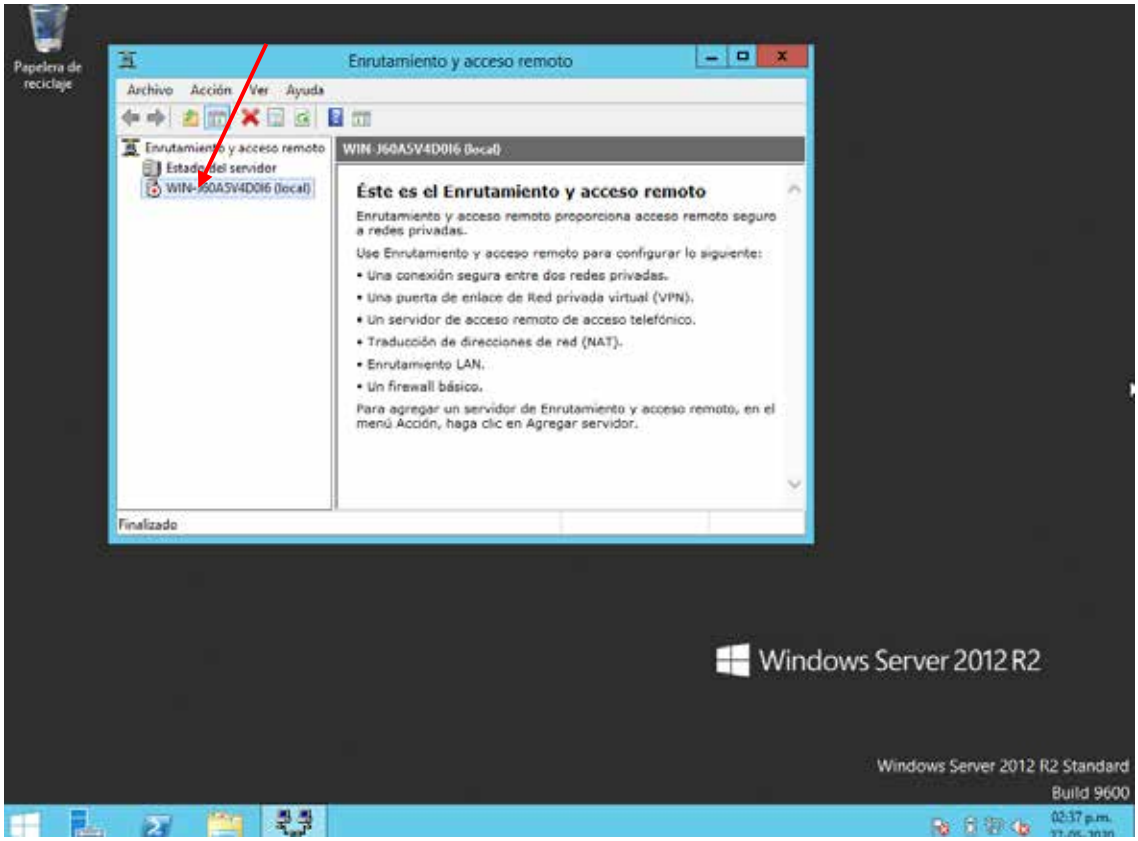


Figura 26. Servidor Local

Fuente: El Autor

El siguiente paso es dar click derecho al Servidor y se marca la opción de "**Configurar y habilitar enrutamiento y acceso remoto"**, se abre una ventana de asistente y damos siguiente, en esta nueva ventana se da click a la opción de **"Configuración Personalizada".** Ver (Figura 27).

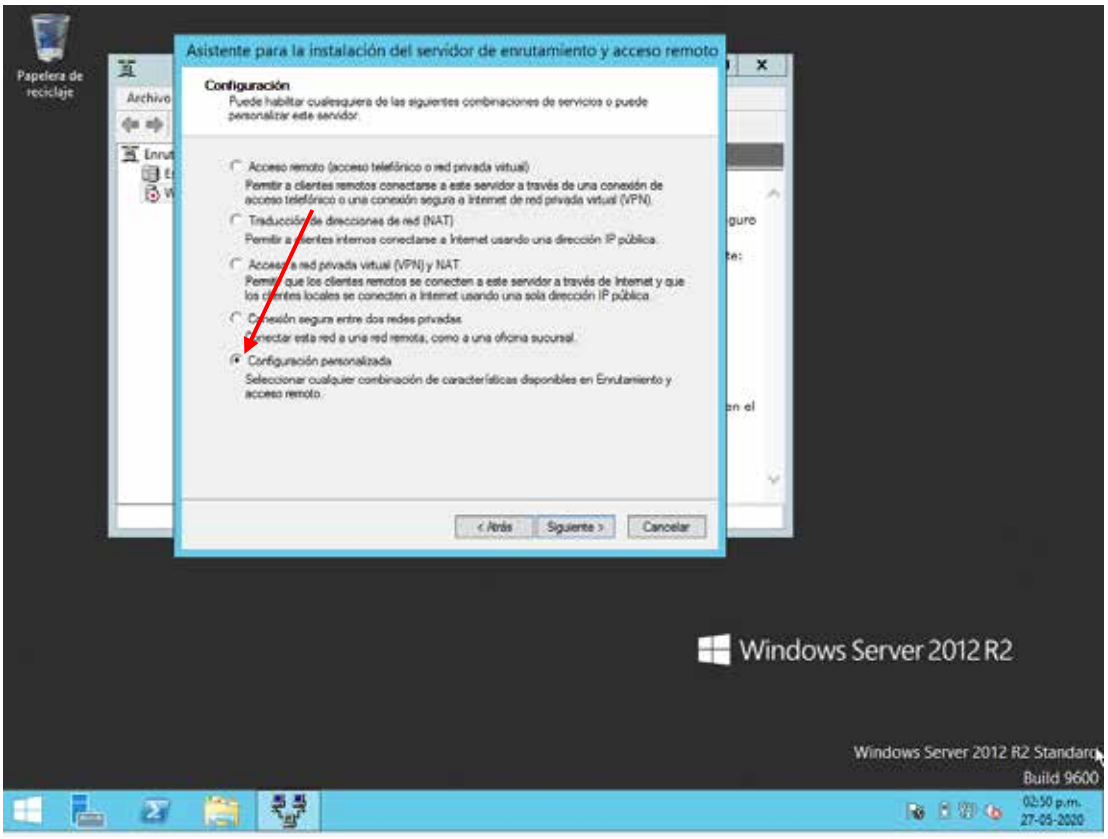


Figura 27. Configuración Personalizada.

Fuente: El Autor.

En Configuración Personalizada tildamos **"Acceso a VPN"** y vamos a siguiente, aparece una ventana y se marca **Finalizar**. Ver (Figura 28).

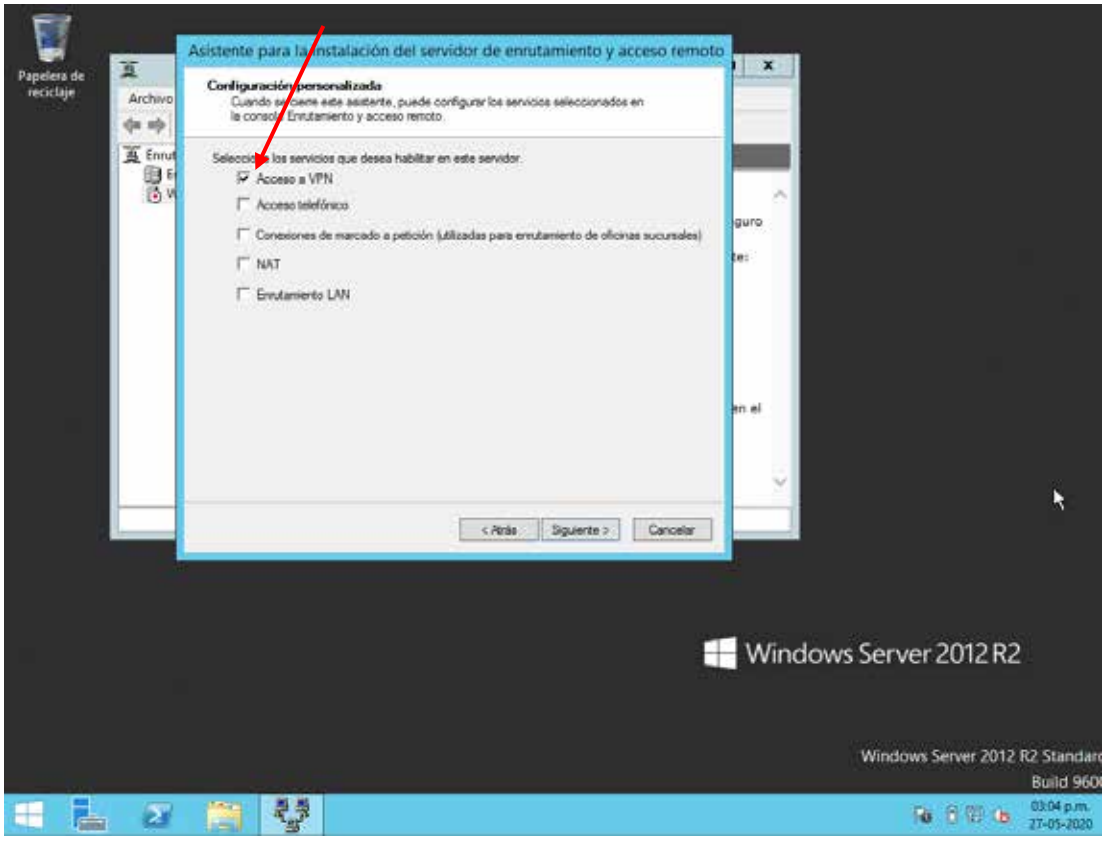


Figura 28. Acceso a VPN

Fuente: El Autor

Luego de marcar **“Finalizar”** damos click a **“Iniciar Servicio”**, esperamos unos pocos segundos mientras se carga el servicio de enrutamiento y acceso remoto. Ver (Figura 29).

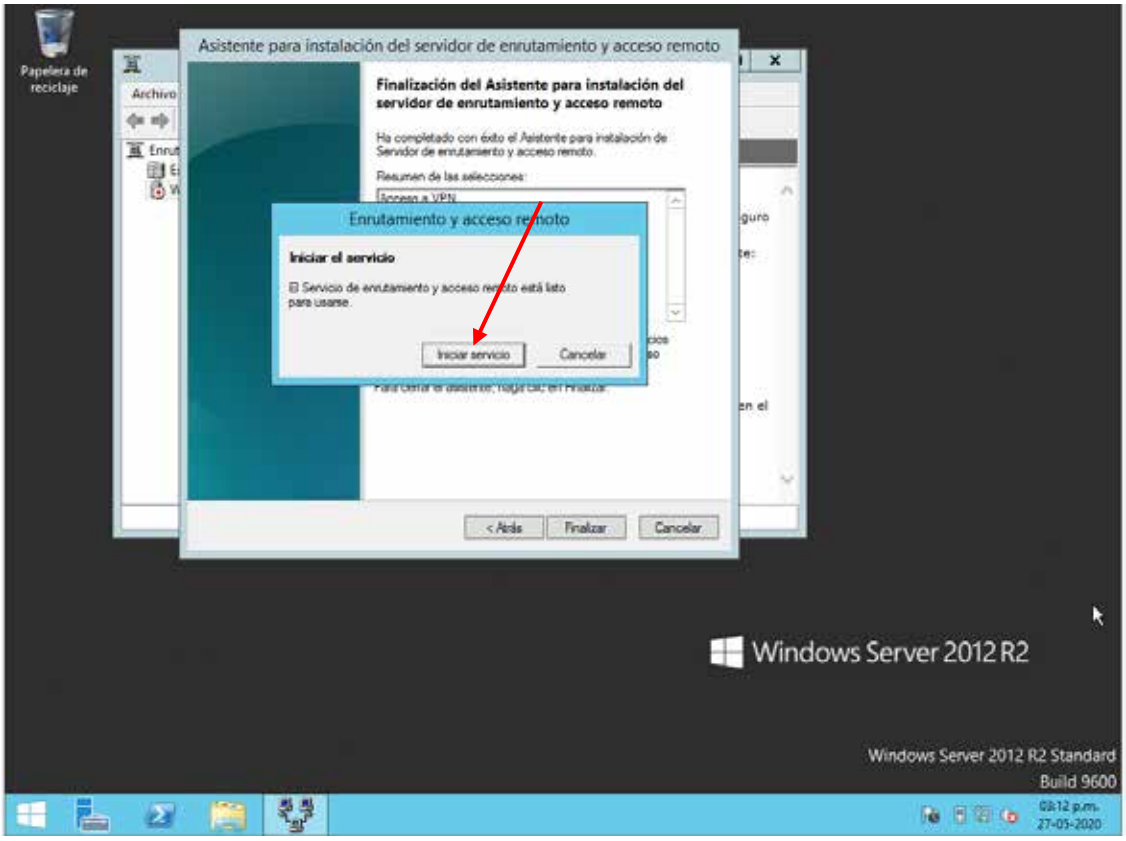


Figura 29. Iniciar Servicio

Fuente: El Autor

Ahora observamos que nuestro Servidor está operando, se aprecia las Interfaces de red, Puertos donde se conectaran distintos clientes, los Clientes que se conectaran vía remota y diferentes características. Ver (Figura 30).

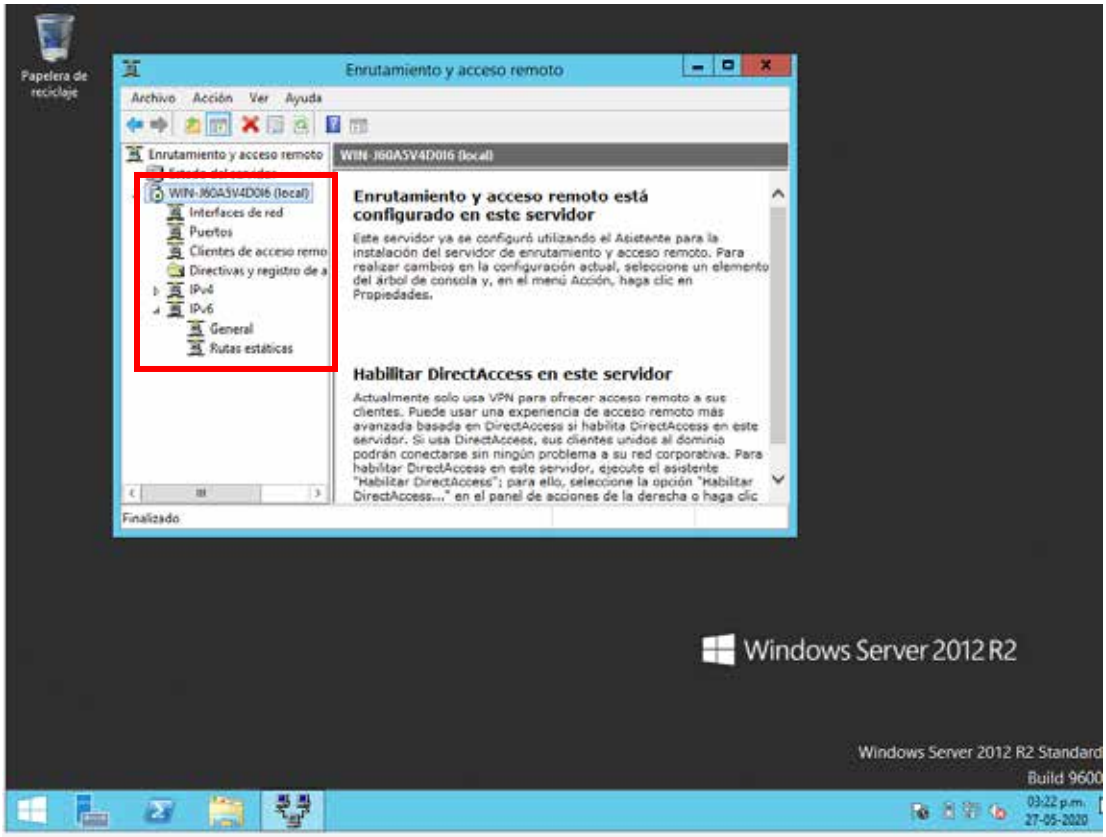


Figura 30. Servidor Local Operando.

Fuente: El Autor.

El siguiente paso es en el Servidor marcar click derecho y “Propiedades” luego marcamos la pestaña **SEGURIDAD**, y en la opción **Proveedor de autenticación** se tilda **Autenticación de Windows** y luego tildamos abajo para permitir el protocolo IPSsec. Ver (figura 31).

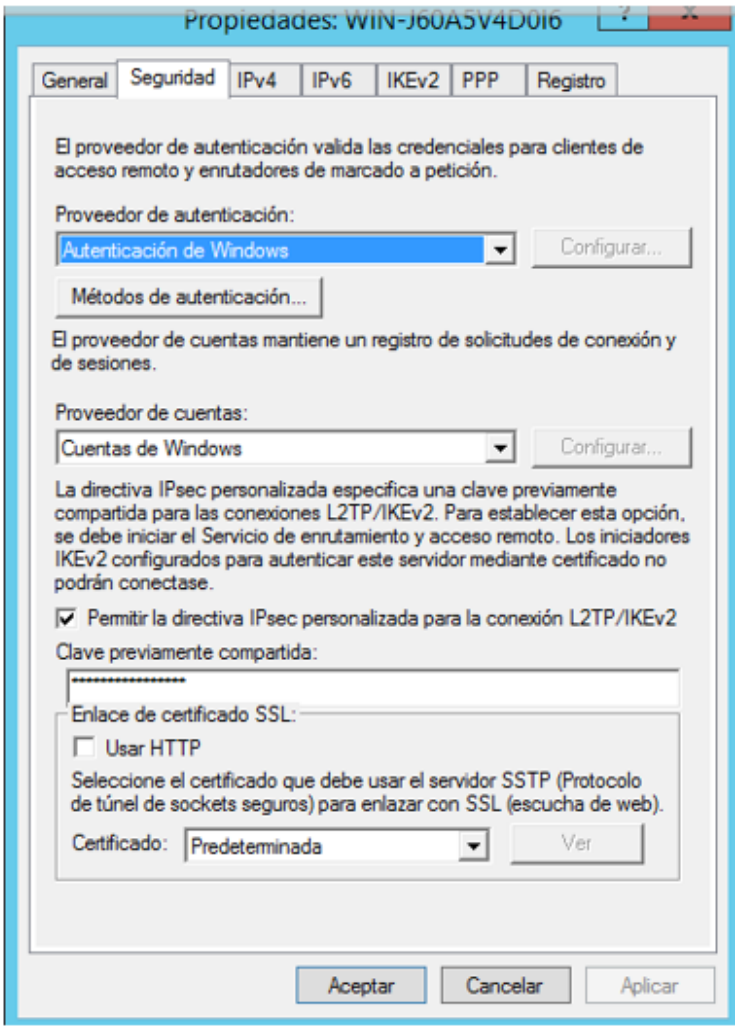


Figura 31. Autenticación y Protocolo.

Fuente: El Autor.

En la pestaña IPV4, ahí asignaremos el rango de direcciones IP las cuales se va a permitir el acceso vía remota. En este caso verificando la tabla de direccionamiento IP se escogió el rango entre 192.168.0.26 a 192.168.0.29. Ver (Figura 32).

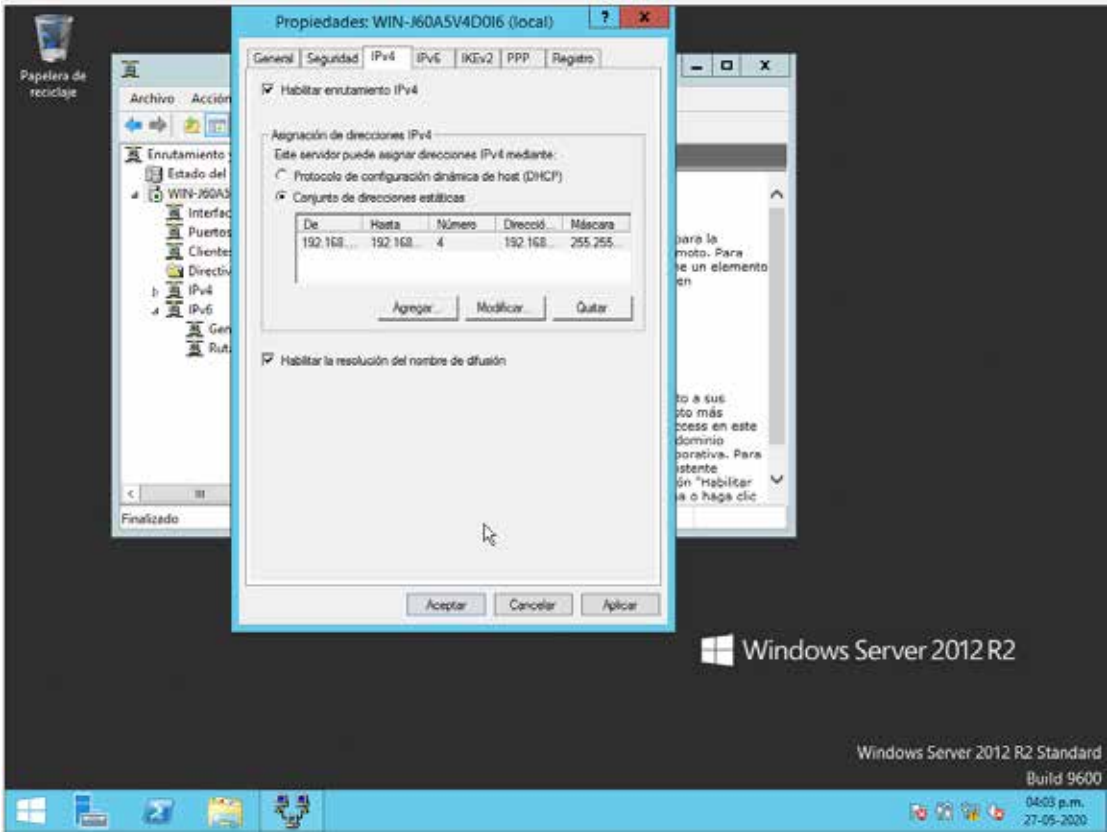


Figura 32. Agregar conjunto de direcciones estáticas.

Fuente: El Autor.

En este paso se procede a crear el Dominio del Servidor el cual lo identificará en la red y será el de referencia para la conexión de usuarios remotos. En el Administrador del Servidor se marca en el menú derecho la pestaña AD DS. Aparece otra ventana y vamos a marcar **"MAS"**, la cual se ve arriba a la derecha. Ver (Figura 33).

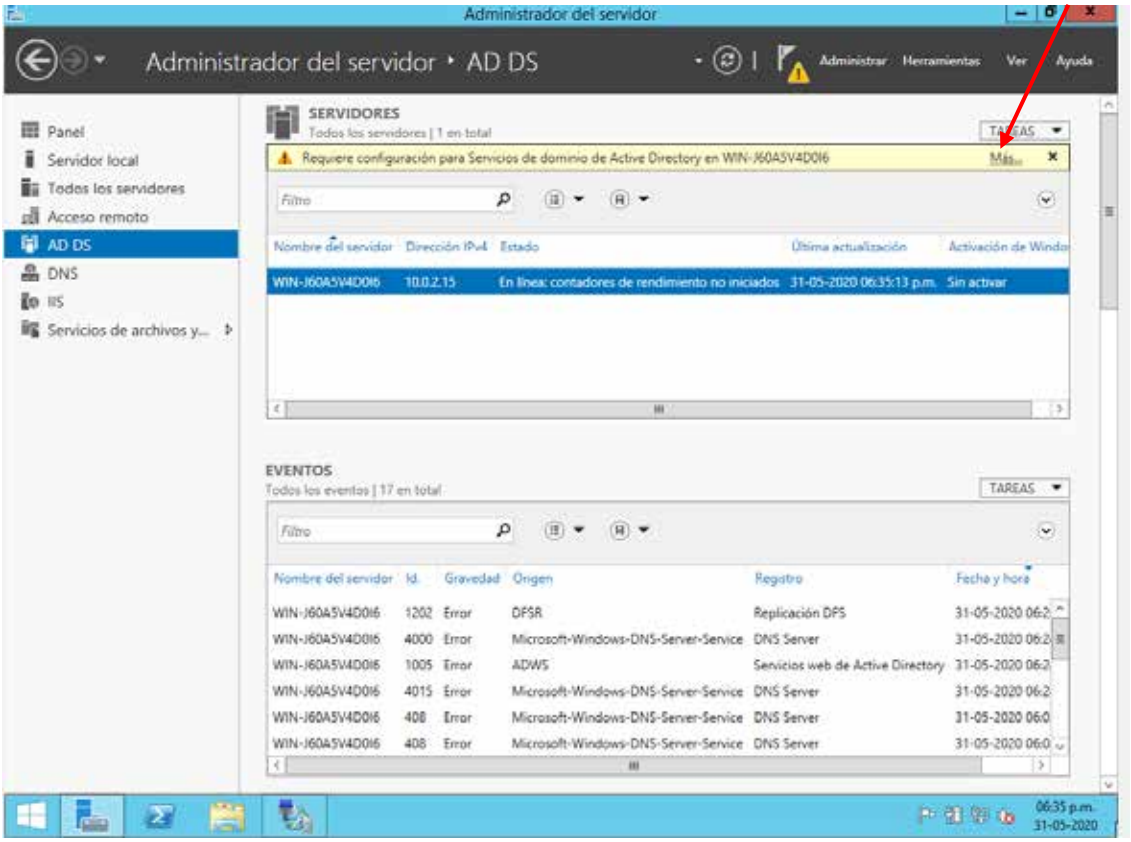


Figura 33. Creación de Dominio.

Fuente: El Autor.

En esta ventana se marca “Promover este servidor”. Ver (Figura 34).

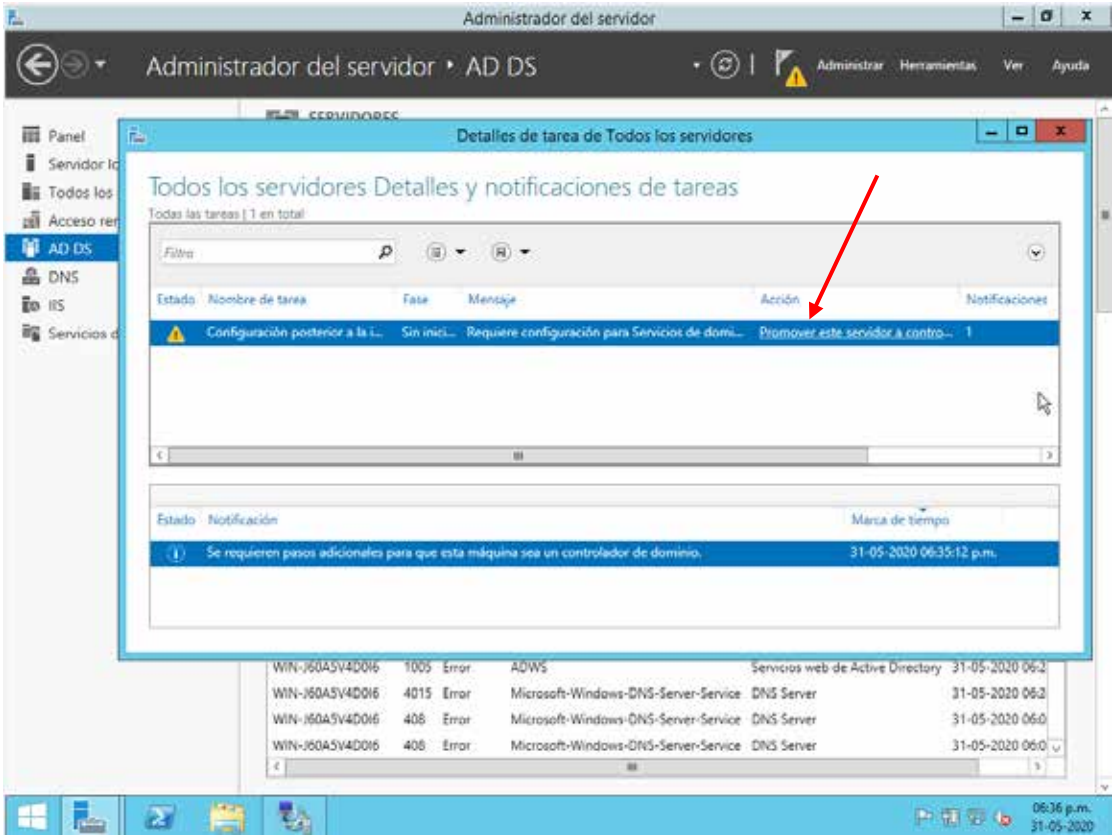


Figura 34. Promover este Servidor

Fuente: El Autor.

En la siguiente ventana entre las diferentes opciones marcaremos **“Agregar un nuevo bosque”.** Ver (Figura 35).

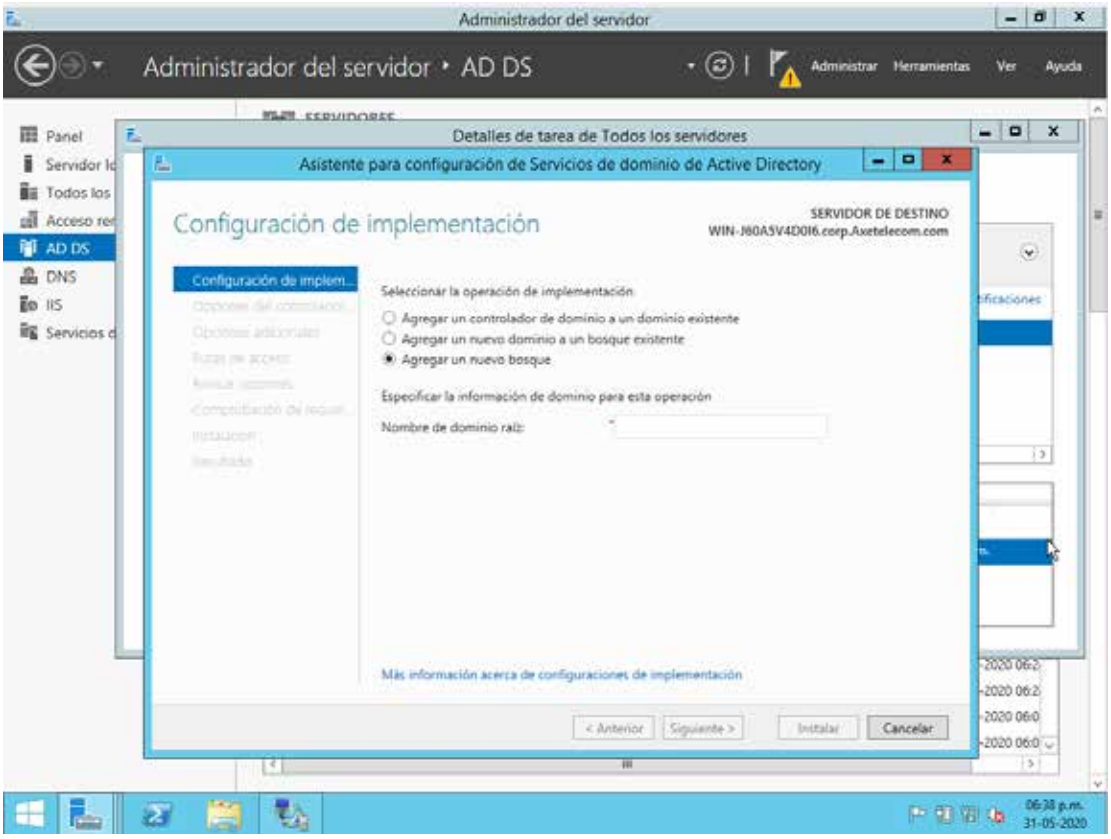


Figura 35. Agregar un nuevo bosque.

Fuente: El Autor.

Seguidamente se indica el Nombre de Usuario que vamos a utilizar en este caso será: **corp.Axetelecom.com.** Ver (Figura 36).

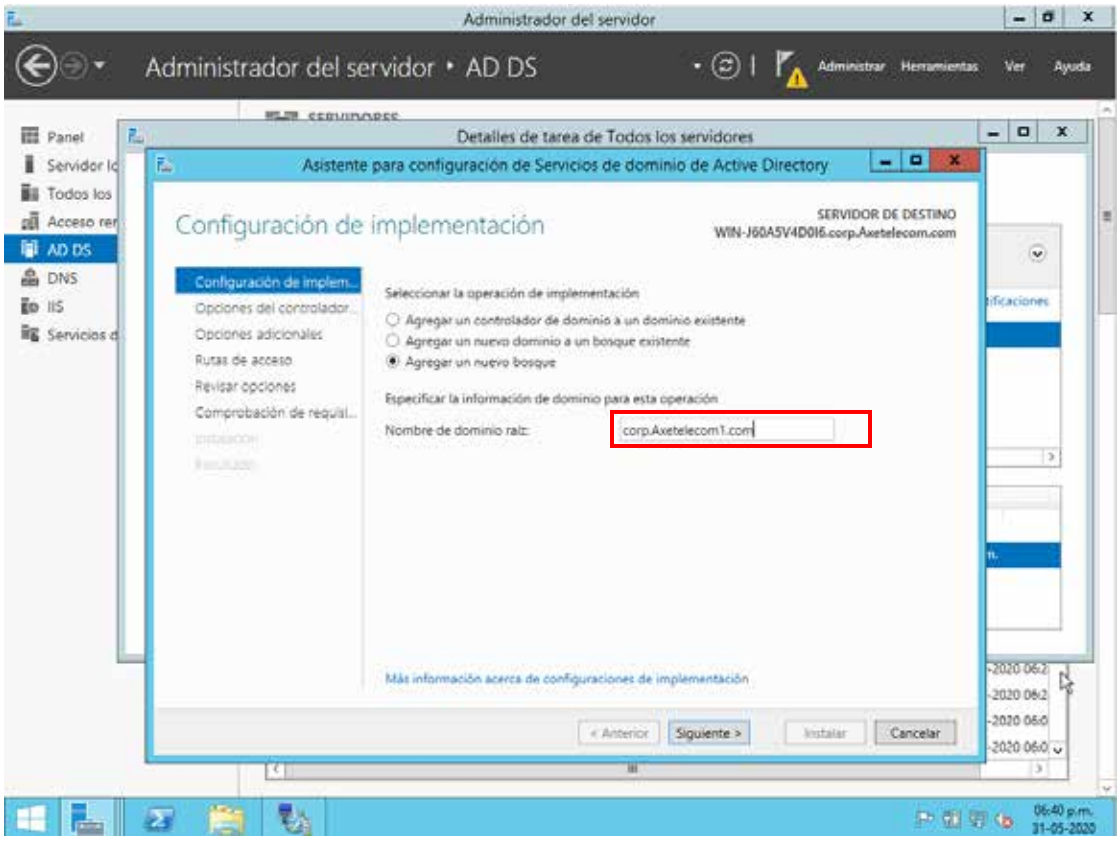


Figura 36. Nombre de Dominio.

Fuente: El Autor.

En la nueva ventana ingresamos la clave que será utilizada. Ver (Figura 37).

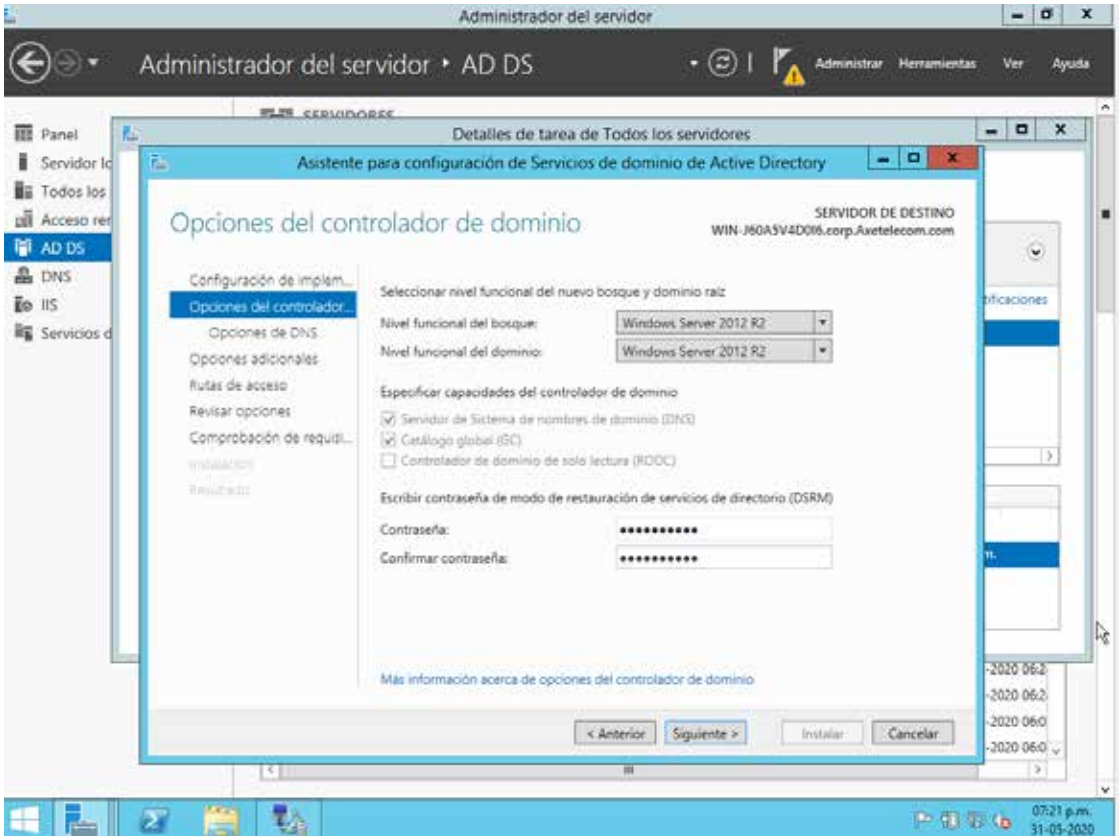


Figura 37. Contraseña de Dominio.

Fuente: El Autor.

En la próxima ventana damos click en siguiente y aparece un recuadro donde vamos a indicar el nombre de dominio Netbios: colocaremos “CORP”. Ver (Figura 38).

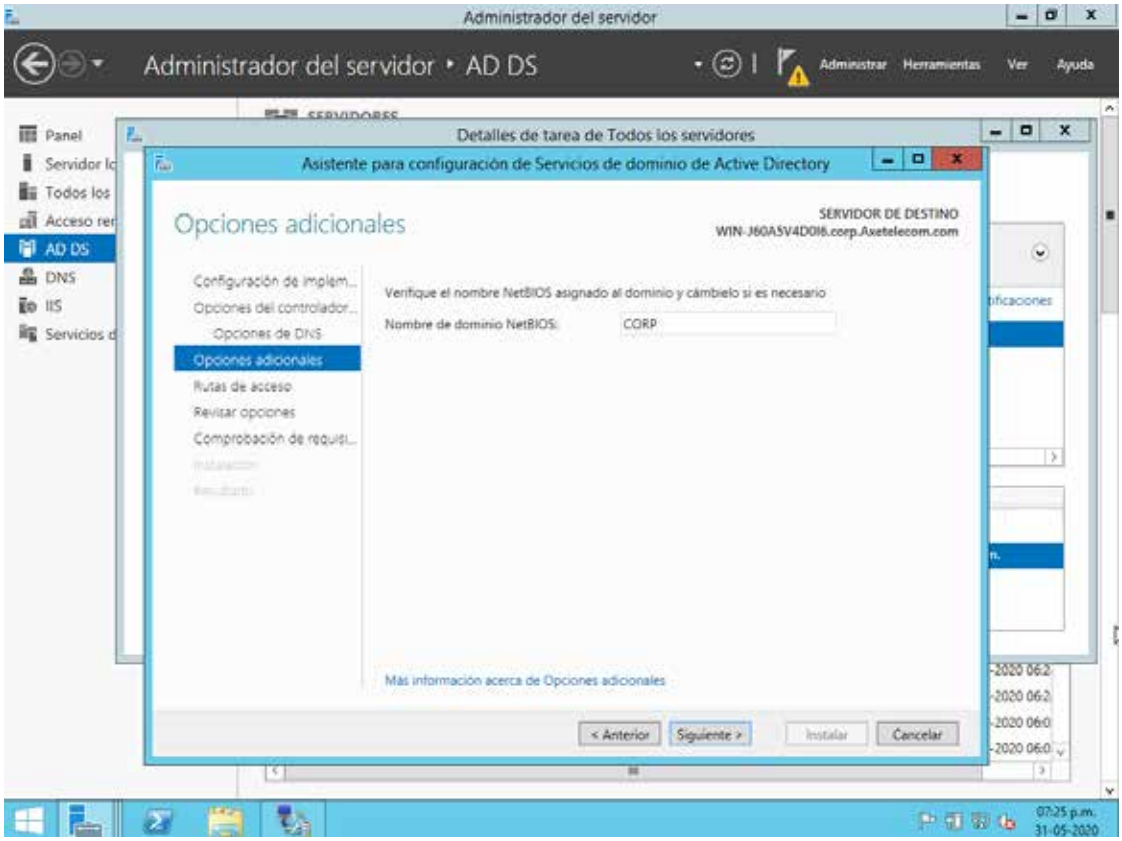


Figura 38. Netbios.

Fuente: El Autor.

Aparece otra ventana en la cual se marca siguiente, podemos ver el script de la configuración, marcamos siguiente y procedemos a Instalar. Ver (Figura 39).

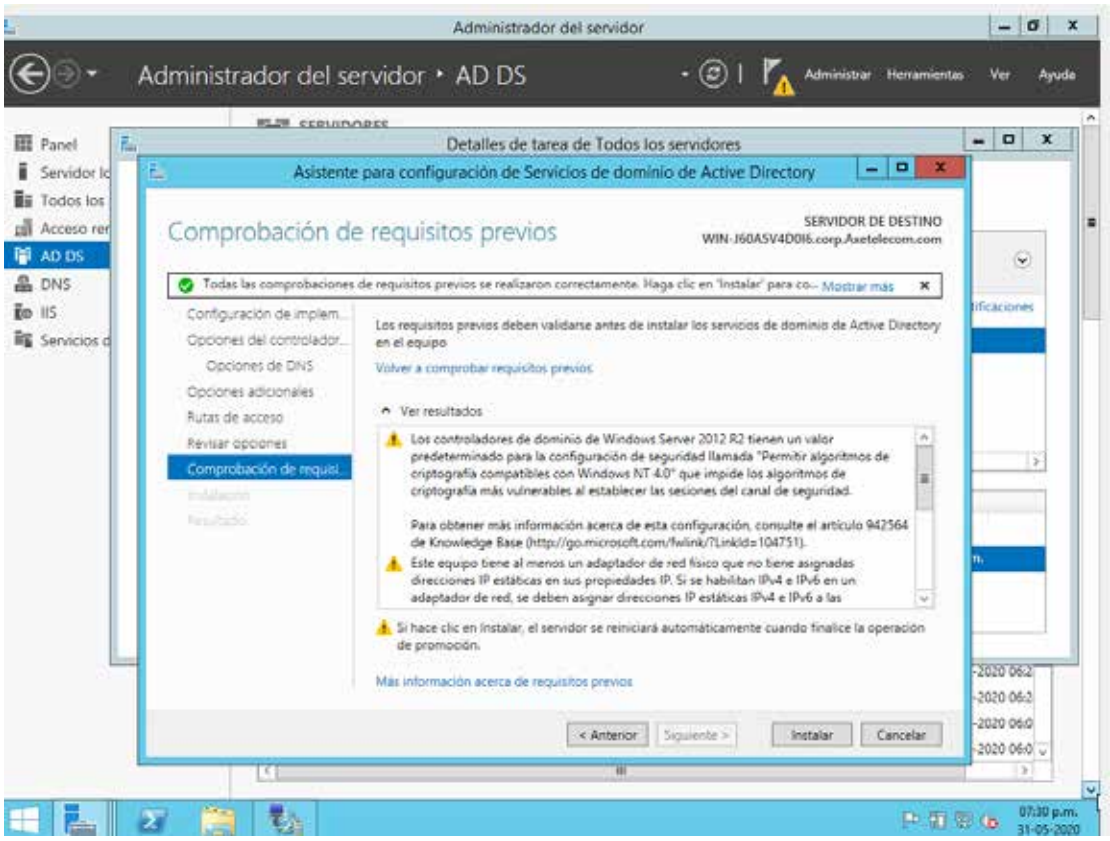


Figura 39. Instalar Dominio.

Fuente: El Autor.

Esperamos unos segundos mientras ocurre el proceso de instalación y verificamos la creación del Dominio. Ver (Figura 40).

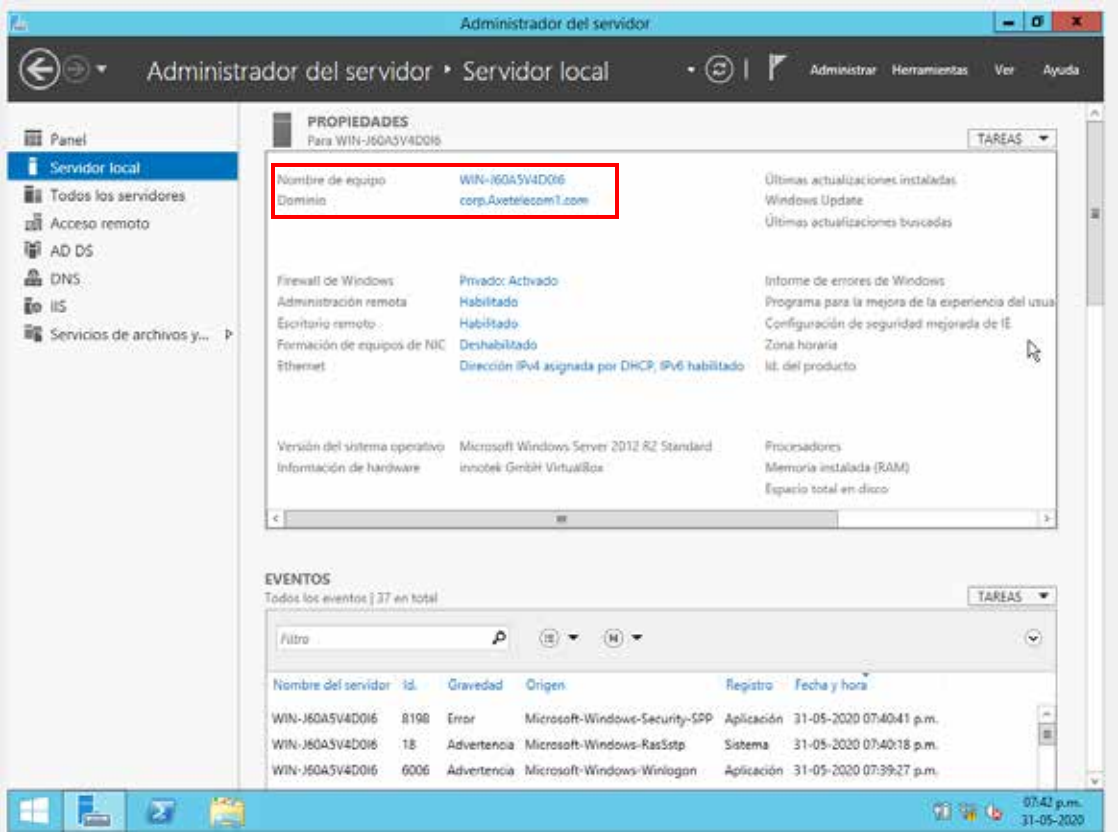


Figura 40. Verificación de nombre de Dominio

Fuente: El Autor.

Se procede a habilitar el Permiso al Servidor para la conexión VPN con los clientes remotos. En el administrador del Servidor arriba en la parte derecha marcamos la pestaña **Herramientas**, se despliegan las opciones y marcamos **"Administración de equipos".** Ver (Figura 41).

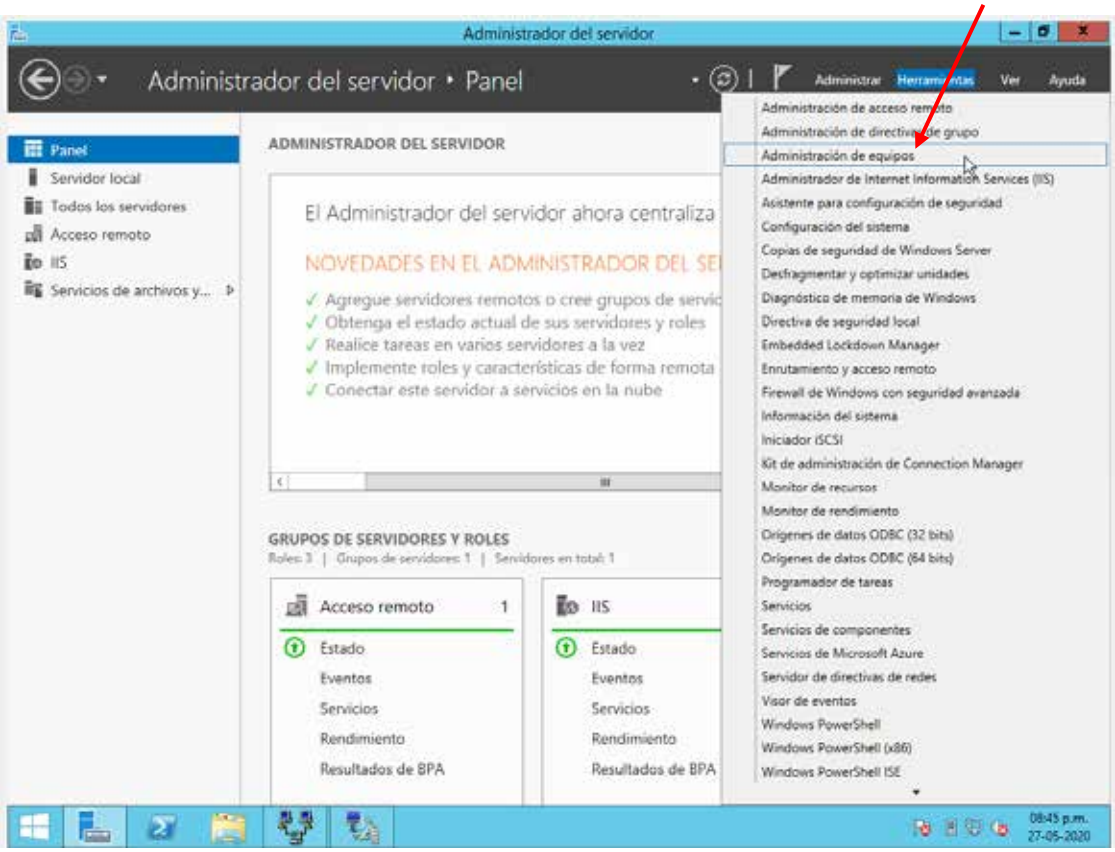


Figura 41. Administración de equipos.

Fuente: El Autor.

Del lado izquierdo en la barra marcamos **Usuarios y grupos locales**, luego **Usuarios** y en el **Administrador** click derecho **Propiedades.** Ver (Figura 42).

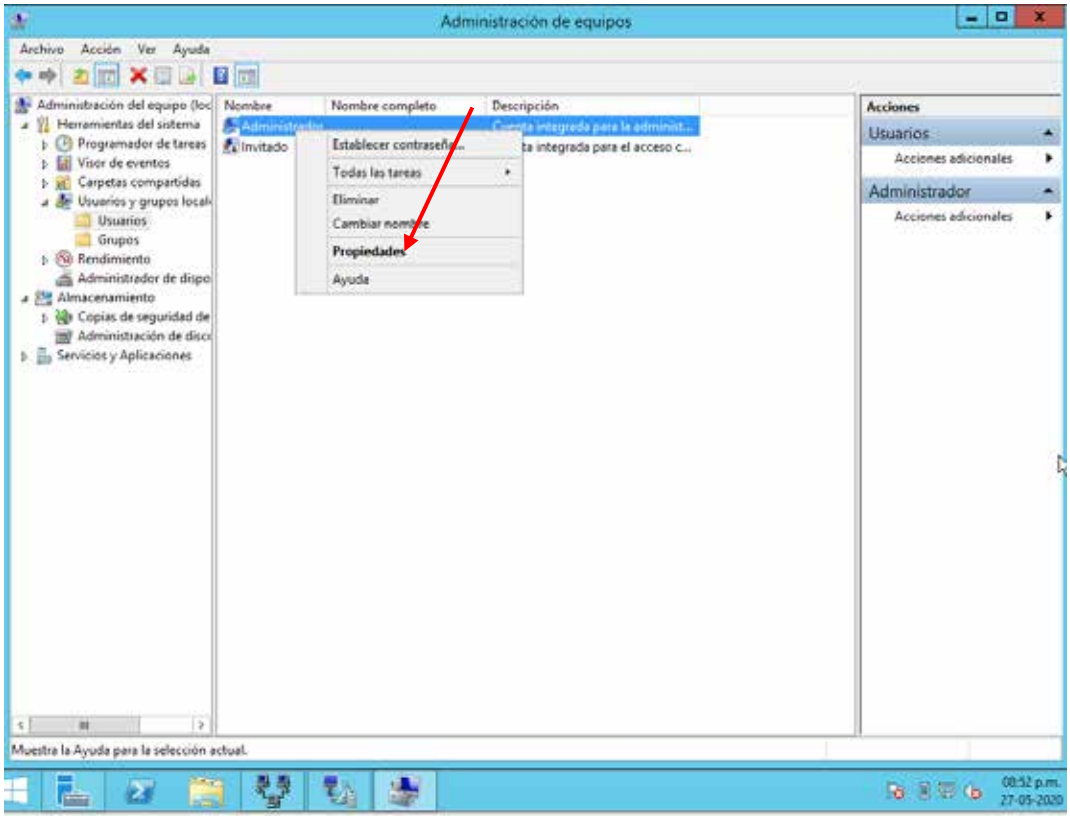


Figura 42. Propiedades de administrador.

Fuente: El Autor.

Al aparecer la ventana de Propiedades administrador, se da click derecho a la pestaña **“Marcado”** y tildamos **“Permitir acceso”**. Ver (Figura 43).

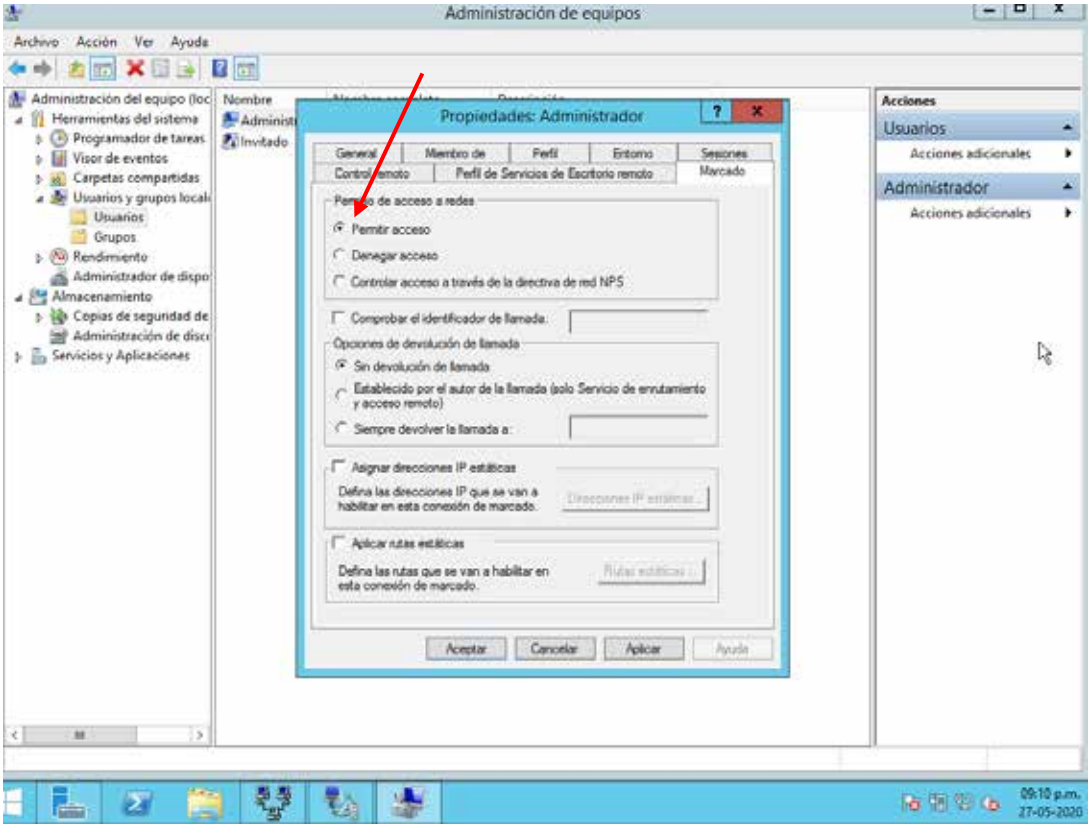


Figura 43. Permitir acceso a administrador.

Fuente: El Autor.

En consola verificamos que aparezca la conexión o IP del servidor; y con esto concluiríamos la configuración del Servidor VPN. Ver (Figura 44).

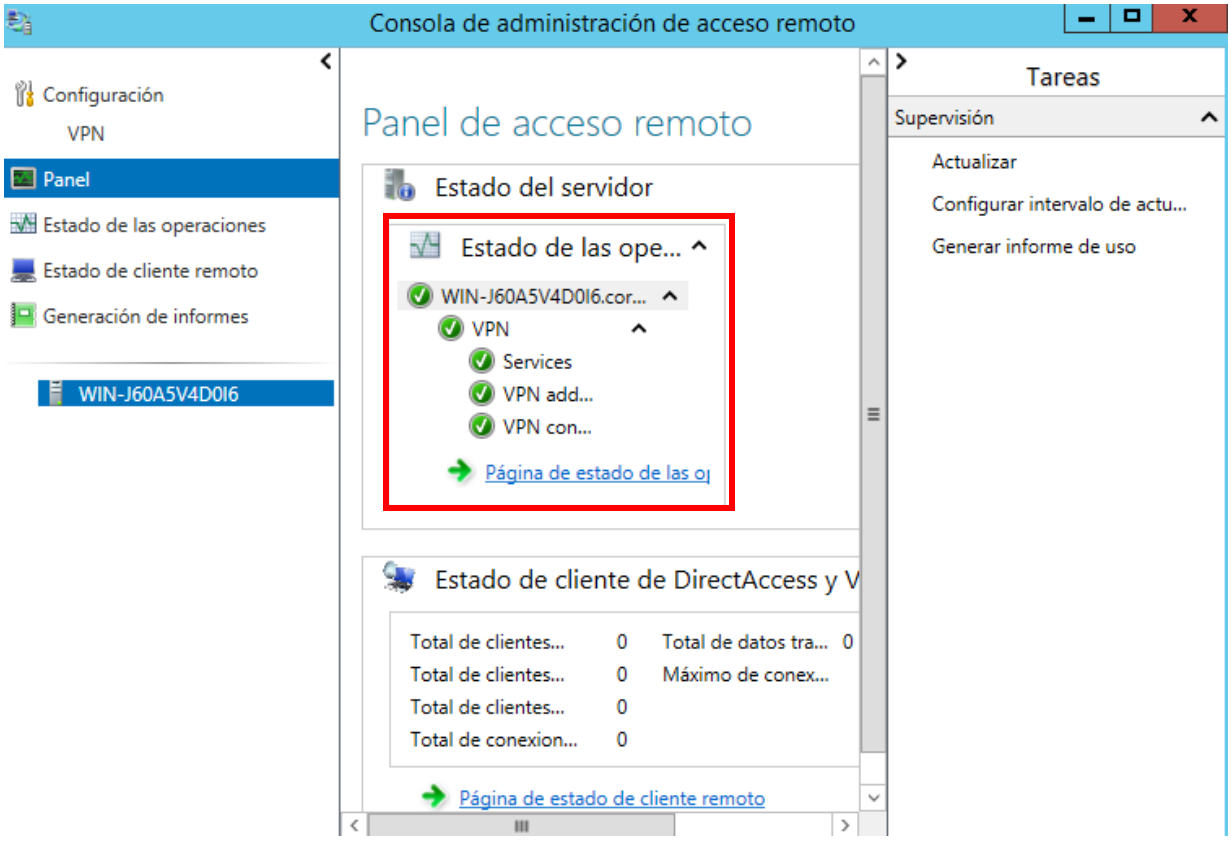


Figura 44. Cuadro de configuración de VPN

Fuente: El Autor.

Verificación en Consola de administración de acceso remoto. Ver Figura 45.

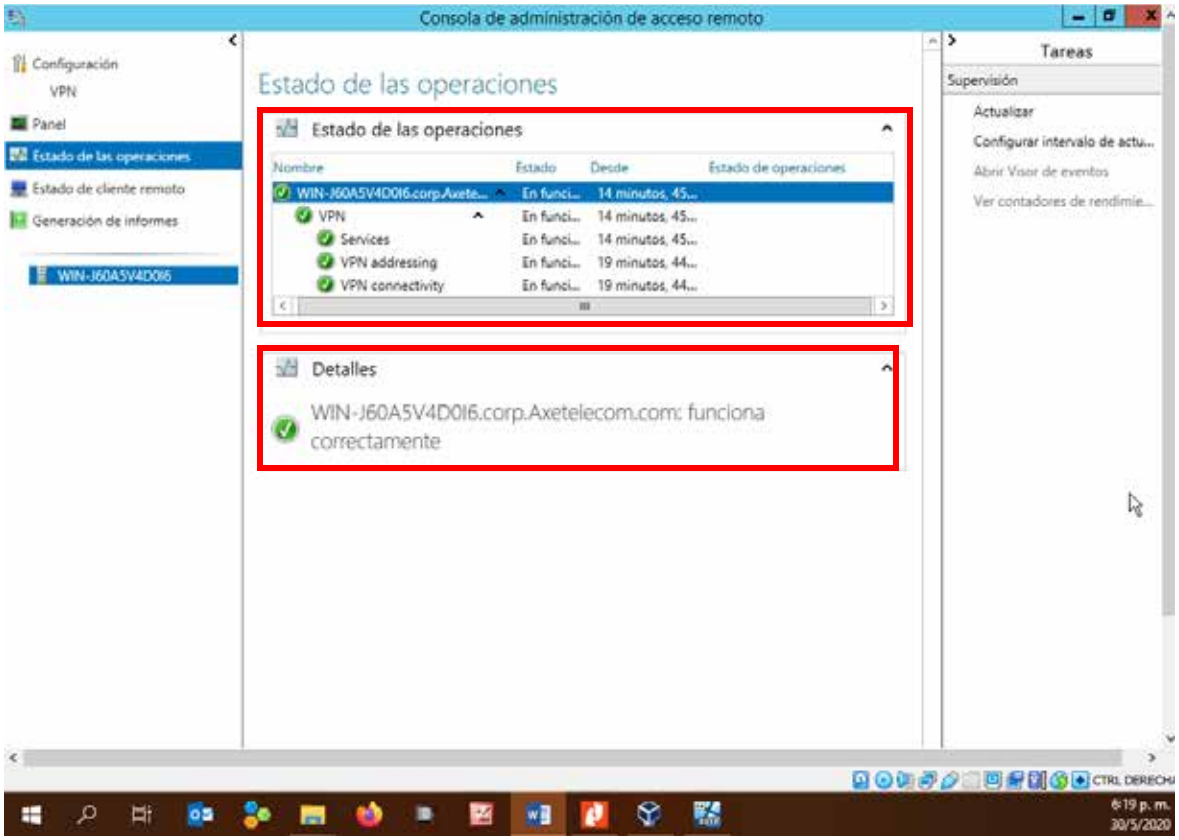


Figura 45. Estado de las operaciones.

Fuente: El Autor.

Se verifica en la consola que esté incluida la dirección IP del Servidor. Ver (Figura 46).

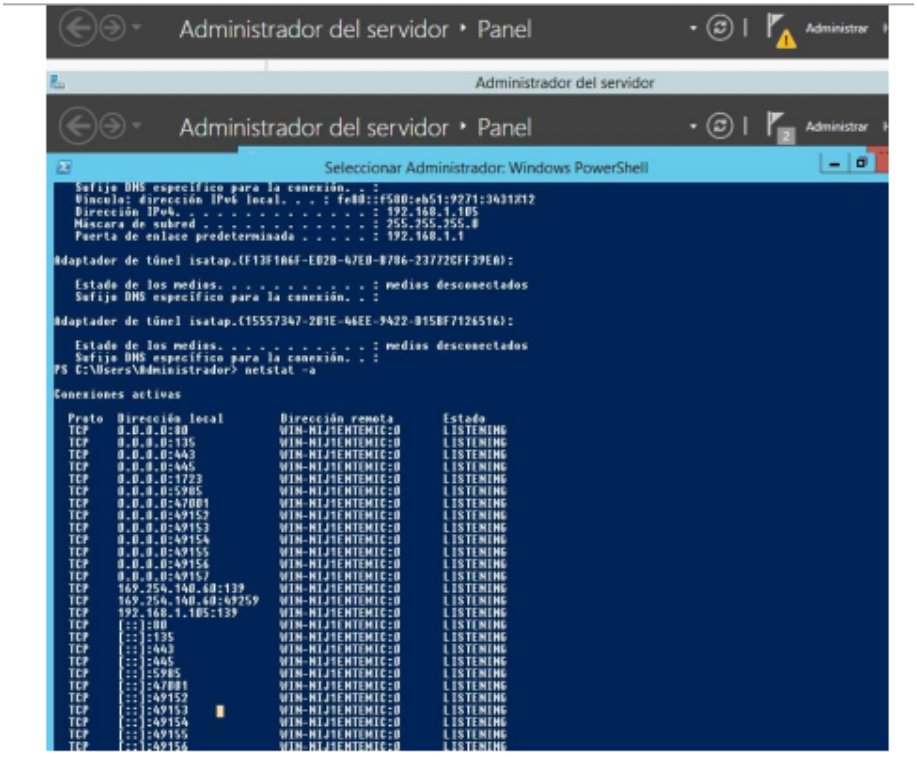


Figura 46. Verificación en consola.

Fuente: El Autor

Creación de Usuario Ej. María Perez; se creó en las propiedades del Servidor (Usuarios y Equipos de active Directory). Ver (Figura 47).

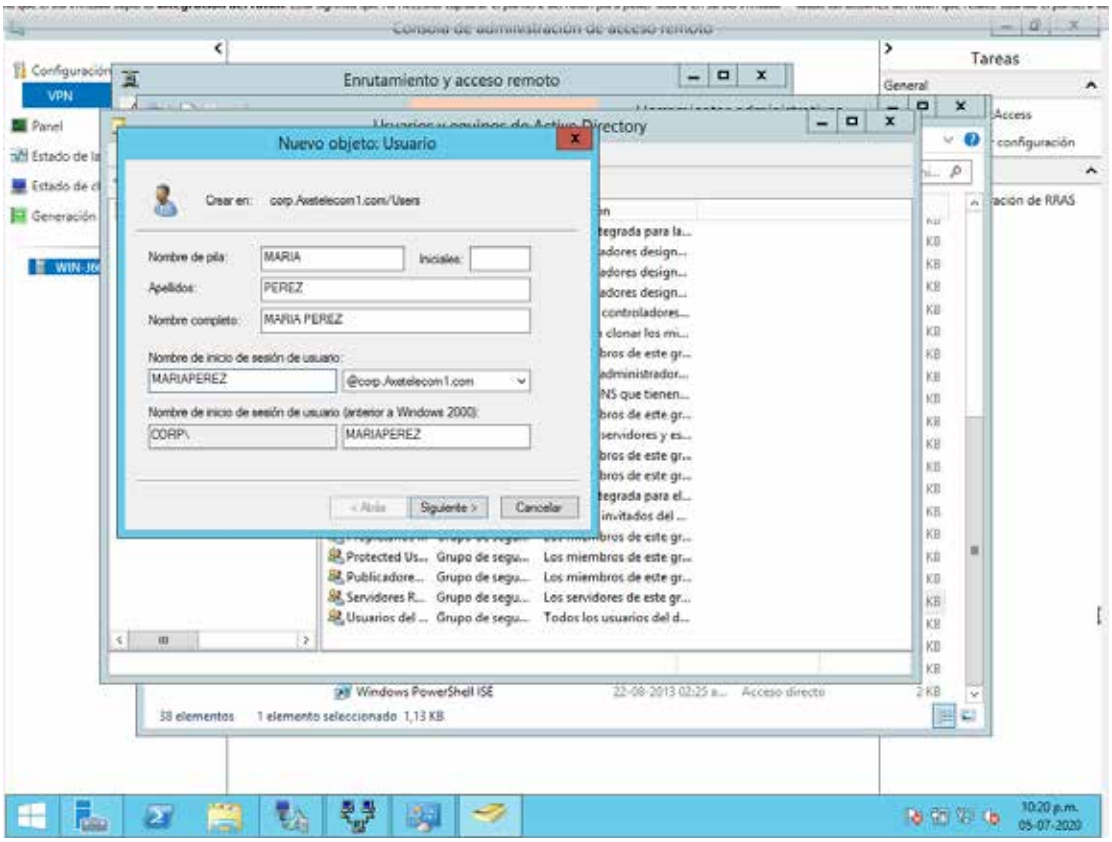


Figura 47. Creación de Usuario.

Fuente: El Autor.

En la siguiente ventana se colocó la contraseña y abajo hay varias opciones para otorgar al Usuario. Marcamos Siguiente y en la próxima ventana Finalizar. Ver (Figura 48).

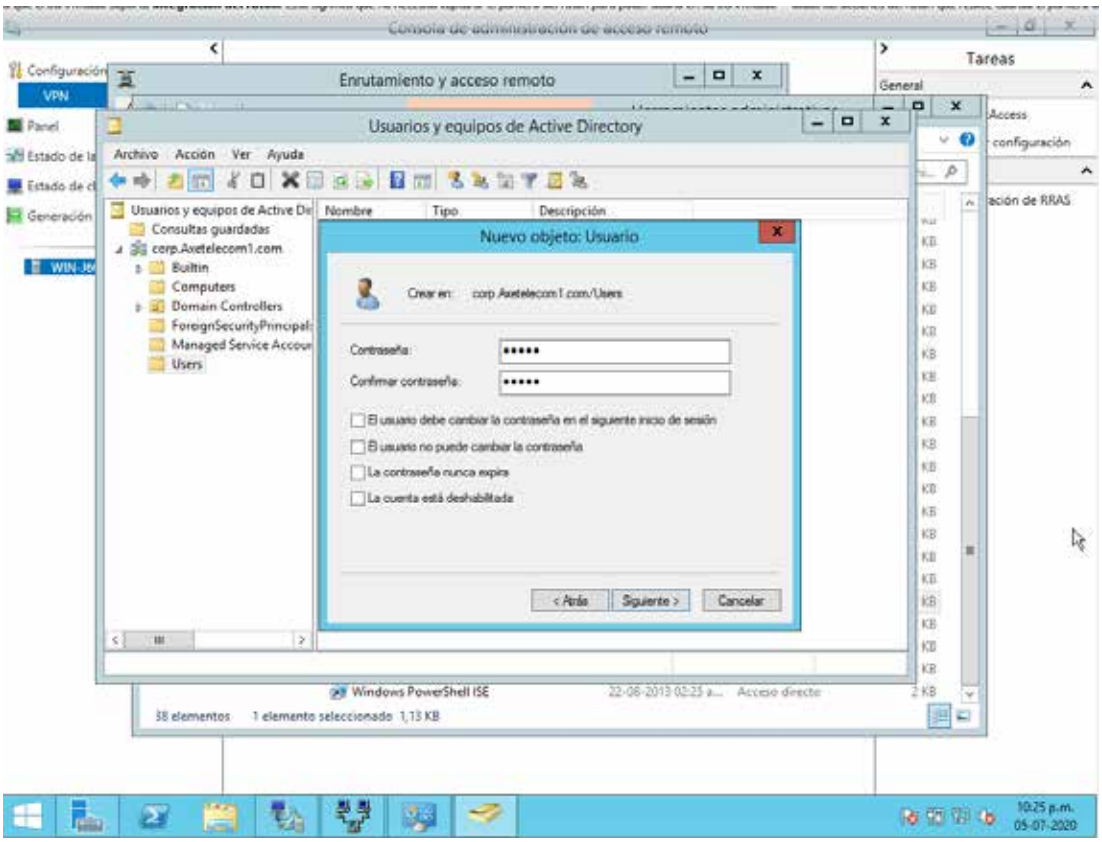


Figura 48. Contraseña de Usuario.

Fuente: El Usuario.

Abrimos el Usuario María Perez, damos click a la pestaña Marcado y tildamos la opción Permitir Acceso. Ver (Figura 49).

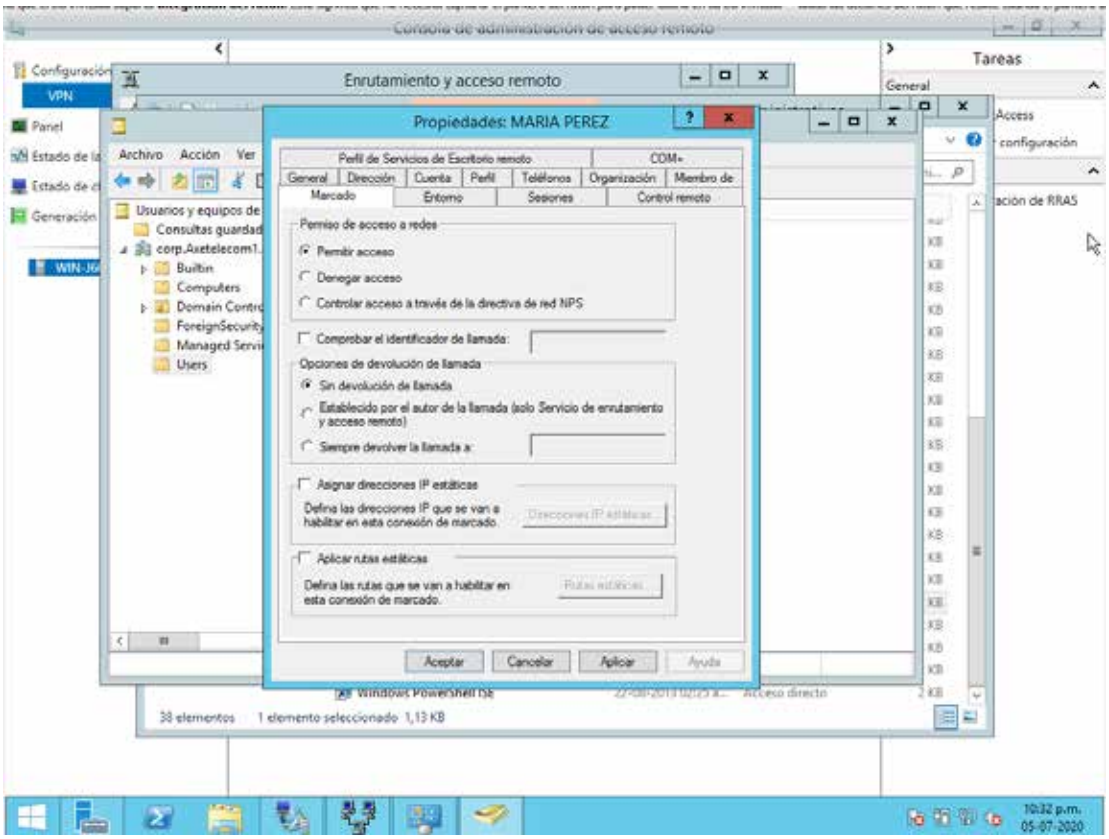


Figura 49. Permitir acceso a usuario María Perez.

Fuente: El Autor.

4.3.4 Configuración VPN cliente

Con el fin de comunicar los equipos remotos con la red LAN de la empresa, se configurará en estos la VPN cliente, la cual permitirá la conexión con el Servidor para ingresar a la red local y trabajar como si se encontrara en la empresa.

En la configuración de los equipos realizaremos los siguientes pasos.

- Para Windows 10

1-Primeramente, ubicamos en la PC **"Panel de Control"** y se marca la opción **"Centro de redes y recursos compartidos".** En esa nueva ventana damos click a **"Configurar una nueva conexión o red".** Ver (Figura 50).

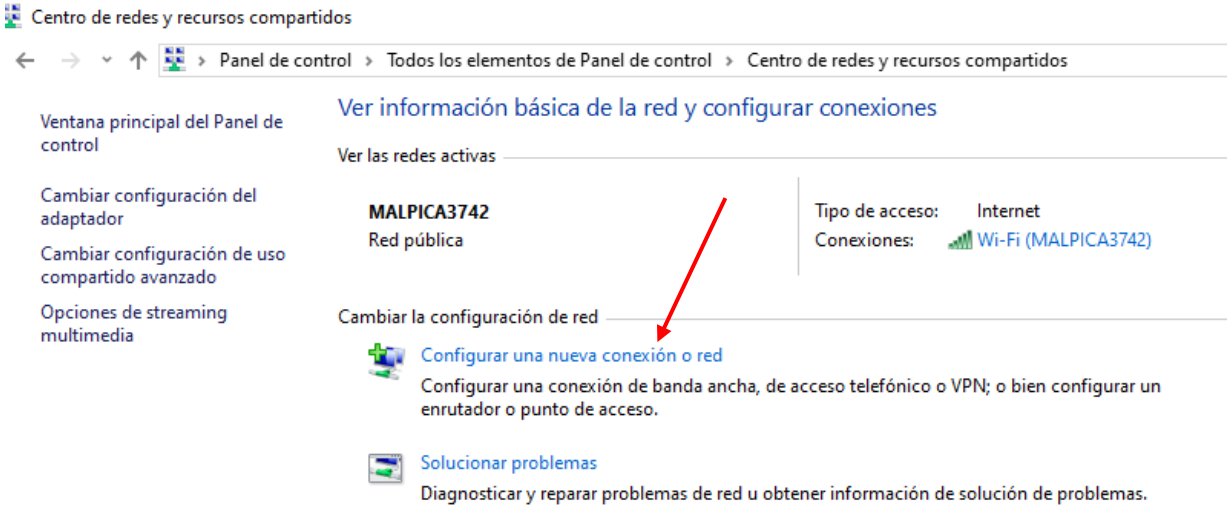


Figura 50. Configurar una nueva conexión o red.

Fuente: El Autor

En la próxima ventana marcamos la opción **“Conectarse a un área de trabajo”.** Ver (Figura 51).

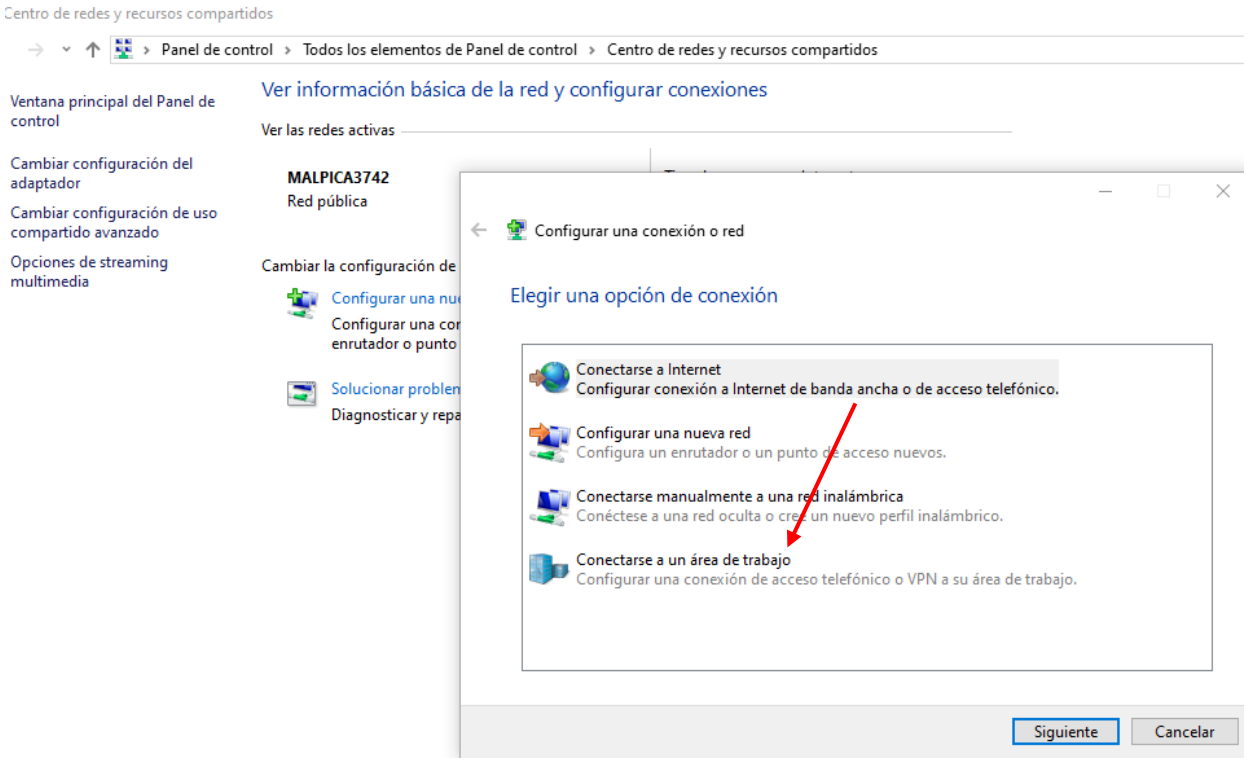


Figura 51. Conectarse a un área de trabajo.

Fuente: El Autor.

Seguidamente se marca la opción de **“Usar mi conexión a Internet VPN”**. Ver (Figura 52).

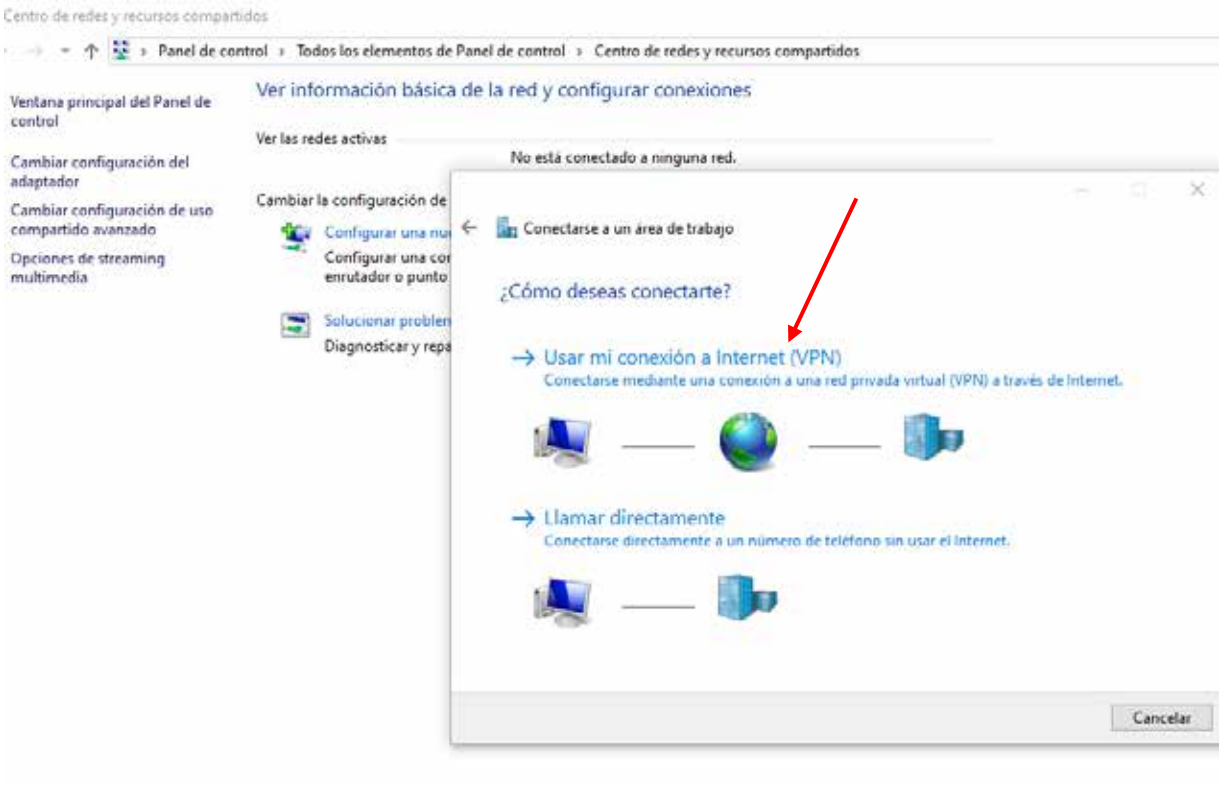


Figura 52. Usar mi conexión a Internet VPN.

Fuente: El Autor.

En esta nueva ventana se coloca en el primer recuadro la Dirección de Internet, bien sea el (Dominio de la empresa o la IP publica donde está el Servidor de la empresa), En el segundo recuadro Nombre de destino se puede dejar el nombre que sale por defecto (Conexión VPN) damos click a crear. Ver (Figura 53).

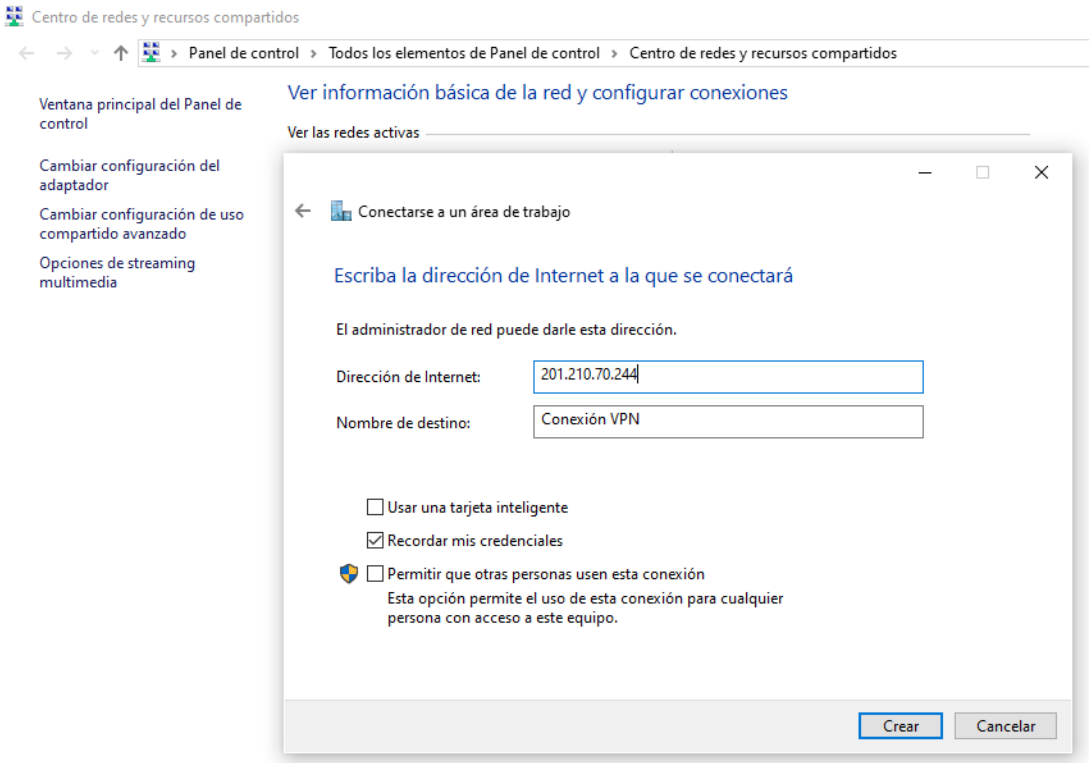


Figura 53. Ingresar Datos de Servidor.

Fuente: El Autor.

El próximo paso es dar click en el símbolo de wifi o ethernet que se ve en la barra inferior de Windows “Acceso a internet”, se despliega un menú y en la parte superior damos click a **“Conexión VPN”** y marcamos conectar; otra manera en ubicar en el buscador de Inicio colocando VPN y marcamos “Configuración de VPN”, nos aparece la opción de “Conexión VPN” y damos conectar. Ver (Figura 54).

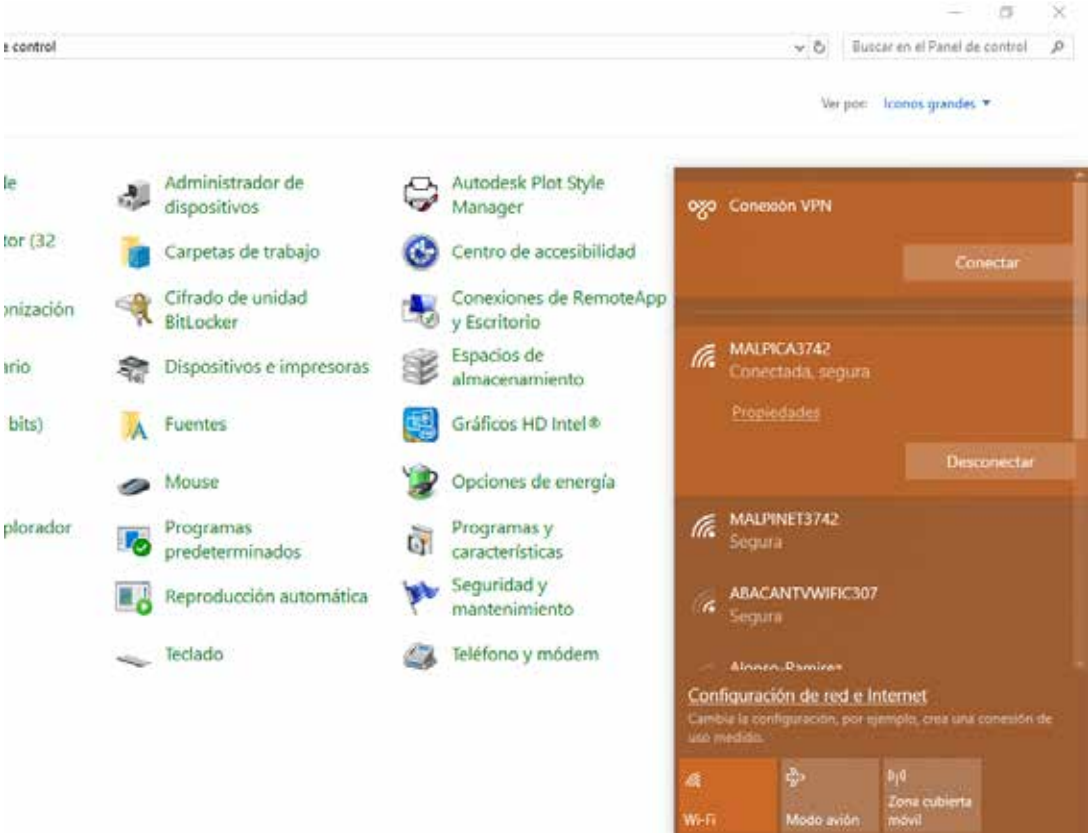


Figura 54. Conexión VPN.

Fuente: El Autor.

Se ingresa el Usuario y contraseña que tendrá acceso a la red VPN el cual se creó en el Servidor y damos aceptar. Ver (Figura 55).

Figura 55. Ingresar Datos en PC usuario.

Fuente: El Autor.

Luego de unos segundos la PC estará conectada al Servidor VPN. Ver (Figura 56).

Figura 56. Conectado a red VPN

Fuente: El Autor.

4.4 Fase IV: Estudio de factibilidad técnica, económica, social y ambiental para la implementación de la propuesta.

Luego de desarrollar técnicas y análisis para que el Trabajo de grado se lleve a cabo, es necesario realizar un estudio de factibilidad. Esta herramienta nos va a facilitar la toma de decisiones para la evaluación del proyecto, la cual nos ayudara a determinar e identificar las posibilidades de que el proyecto sea un éxito o fracaso. De esta manera, se podrá decidir si se procede o no a la implementación.

4.4.1 Factibilidad Técnica

En el desarrollo del diseño de la red VPN se cuenta con los recursos necesarios como conocimientos, habilidades a nivel de red, manejo de SO, PC y diseño básicos de red, además de que se les brinda técnicas a los usuarios para el manejo y uso de la red VPN. Con la continua practica se verá el desenvolvimiento de los empleados en el uso de esta alternativa de trabajo a nivel remoto.

4.4.2 Factibilidad Económica

Con el diseño de la red VPN habrá un beneficio económico significativo ya que primeramente los empleados serán los primeros beneficiados además de la empresa obviamente, ya que se está ampliando la red local hasta cualquier lugar geográfico reduciendo el costo de tránsito, tiempo y permitirá el teletrabajo y se mantendrá la productividad de la empresa, con lo cual también ofrece a la empresa más oportunidades de trabajo ya que tendrá el acceso de diferentes clientes a una conexión segura, sin que estos se dirijan a la oficina a entregar documentos confidenciales. Además de esta ser la opción más rentable comparada con la implementación de enlaces dedicados punto a punto. Además de que la empresa cuenta ya con su Servidor y equipos de red los cuales solo se realiza la respectiva configuración y mantenimiento. Cabe destacar que los equipos instalados actualmente son de otras marcas y el diseño se realizó con Packet Tracer, programa de la marca reconocida CISCO, a continuación, se muestra la Tabla 7. Con los precios en el mercado de quipos de la marca CISCO los cuales permitiría la configuración a nivel de software tal cual como el diseño realizado en Packet Tracer, entre los que destacan (Router, Switch). Ver (Tabla 7).

Tabla 7. Costo de equipos

Descripción	Modelo	Costo
Router Cisco	Serie 1941	350$
Switch Cisco	Catalyst 2960 / 24 Puertos	300$
Total		650$

4.4.3 Factibilidad Social

Otra de las bondades que se desea lograr con este trabajo de grado es la de mejorar la experiencia de la red VPN para los usuarios que interactúan diariamente con este servicio y que estos se desenvuelvan cada día más con esta tecnología y que se beneficien de ingresar o tener acceso a documentos de manera remota, además de interactuar en tiempo real y de manera segura con los clientes.

4.4.4 Factibilidad Ambiental

El presente trabajo de grado no genera impactos ambientales negativos ya que el mismo no genera ninguna caracteriza que afecte el medio ambiente ni la vida natural, bien sea contaminando de diferentes maneras, como punto positivo deja de producir en este caso el dióxido de carbono que produciría el vehículo con el cual se trasladaría el empleado a la oficina, además del ruido que generaría el vehículo ya que la persona o usuario estaría realizando sus funciones vía teletrabajo desde un lugar remoto.

4.4.5 Factibilidad Operativa

En este punto los empleados tendrán una capacitación o explicación de cómo realizar la debida conexión a la red privada virtual y que estos logren hacer uso del servicio y trabajar de manera ideal, además de capacitar al personal que seguirá dándole seguimiento y continuidad al mantenimiento de la red.

4.5 Encuesta

Luego de culminado el diseño de la red VPN se realizó la técnica de la encuesta con lo cual se pretende obtener información suministrada por los empleados en cuanto

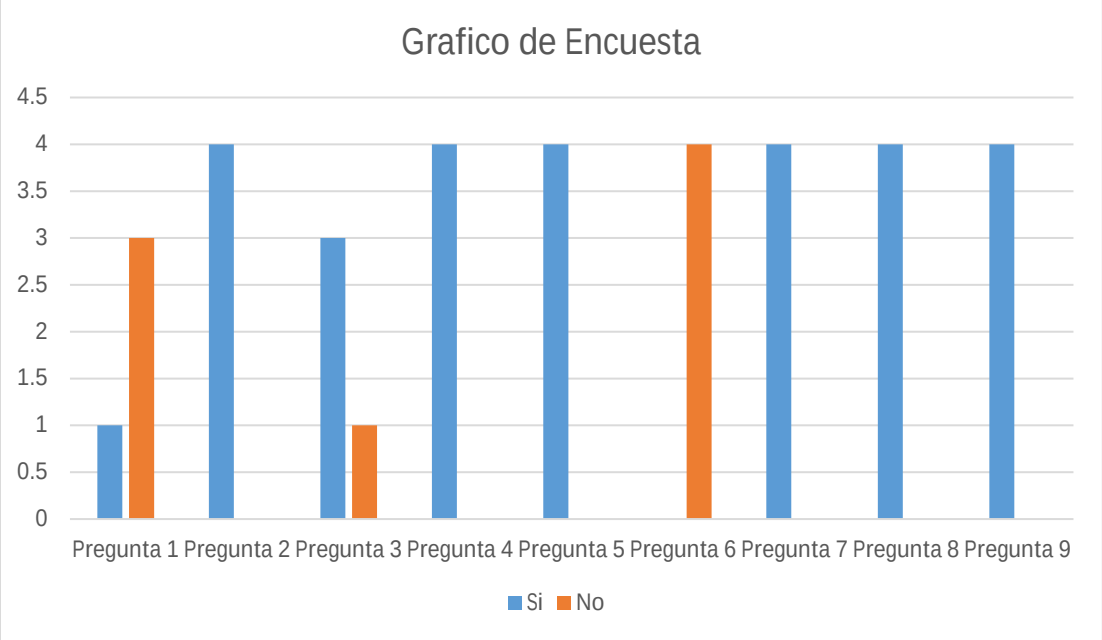
a su parecer con esta herramienta de trabajo. La encuesta se realiza de manera oral, vía telefónica con un total de 9 preguntas. Ver (Tabla 8).

Tabla 8. Encuesta a personal de la empresa.

Numero	Preguntas	Respuestas	
		Si	No
1	¿Conoce usted que es una red VPN?	1	3
2	¿Estaría de acuerdo en participar en una capacitación de red VPN?	4	0
3	¿Realiza trabajos de la empresa en su hogar?	3	1
4	¿Utilizaría la herramienta VPN para trabajar desde su hogar?	4	0
5	¿Cuenta con laptop o PC en su hogar?	4	0
6	¿Ha utilizado otra herramienta diferente de acceso remoto alguna vez?	0	4
7	¿Cuenta con servicio de internet en su hogar?	4	0
8	¿Cree que se beneficiara utilizando la red VPN?	4	0
9	¿Estaría de acuerdo con la implementación de la red VPN?	4	0

Luego de obtener cada una de las respuestas de la muestra del equipo de trabajo de la empresa, se realiza un grafica con la cual se detalla de manera visual los resultados obtenidos.

Tabla 9. Gráfico de la encuesta.



Se observa que luego de la encuesta la mayor parte de la muestra de los empleados desconoce lo que es una red VPN, pero también están de acuerdo en participar en una capacitación y hacer uso de esta desde sus hogares para seguir con la continuidad de sus trabajos de manera remota y segura, además de que cuentan con equipos como laptops o PC y servicio de internet.

CONCLUSIONES Y RECOMENDACIONES

Luego de culminar el Trabajo de grado, se puede concluir que con el cumplimiento de cada una de las fases la red privada virtual puede trabajar para el beneficio de los usuarios y empresa. El diseño de la VPN en la organización, permite ofrecer movilidad, garantiza la integridad, confidencialidad y seguridad de los datos, reducir costos de implementación y lo más importante, permitir a los usuarios y clientes conectarse desde cualquier ubicación geográfica de forma segura ante cualquier evento que se pueda presentar en el país mediante la creación de un túnel. Con el diseño y posible implementación, se garantiza la continuidad del negocio siempre y cuando el usuario posea acceso a internet sin la necesidad de estar físicamente en las instalaciones de la organización.

El montaje de la red se realizó con Packet Tracer para configurar los dispositivos de manera simulada además de permitir crear el diseño de la red, permitiendo el comportamiento y funcionamiento de los dispositivos al configurarlos y evitando inconsistencias a futuro.

El direccionamiento IP que se realizó para Axe a partir de una dirección IP privada, permitirá la escalabilidad y rendimiento de la red, en un futuro cuando la red siga ampliando esta tendrá disponible direcciones IP que asignar a los nuevos usuarios.

Dicha VPN representa 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.

Es recomendable el mantenimiento continuo cada 3 meses aproximadamente a nivel de hardware y software para lograr el mejor desempeño de la red.

El diseño de la red permite a los usuarios trabajar de manera óptima, efectiva y segura, generando su continua productividad y permitiendo el acceso a los datos de la empresa.

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

Crear un manual donde estén definidos cada uno de los pasos que deben seguir lo empleados para lograr la conexión a la Red Privada Virtual.

REFERENCIAS

Bibliográficas

Arias, F. (1999). **El proyecto de investigación - introducción a la metodología científica** (Tercera Edición). Caracas: Episteme.

Arias, F. (2012). **El proyecto de investigación - introducción a la metodología científica** (Sexta Edición). Caracas: Episteme.

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

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

Mijares, H. García, L. (2007). **Normas para la elaboración y presentación de los anteproyectos, proyectos y trabajos de grado.** Valencia: Autores.

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

Tesis en Línea

Ortega, C. (2003) **Metodología para la implementación de redes privadas virtuales, con internet como red de enlace** [Tesis en línea]. Universidad Técnica del Norte, Ibarra, Ecuador. Consultada el 02 de Febrero de 2020 en: https://www.academia.edu/9016546/tesis_de_grado_vpn

Electrónicas

Aguiar, M (2012). **Configuración de una Red en telecomunicaciones.** Consultada el 02 de febrero de 2020 en: http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf

González, A. (2017). **Red Privada Virtual**. Consultada el 02 de febrero de 2020 en:

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

Mackenzie J. (2015). **Tipos de Redes Privadas** Consultada el 03 de febrero de 2020 https://repository.DiseñoyconstruccióndeunGPONa.pdf;jsessionid=8B8F6719F0983D83E2EA5922851F8A89?sequence=2

Osorio, A. (2016). **Redes Privadas.** Consultada el 04 de febrero de 2020 en: https://repositorio.espe.edu.ec/bitstream/21000/11329/1/AC-ESPEL-EMI-0295.pdf

García, M. (2019). **Cuál es la diferencia entre una conexión VPN y una conexión de escritorio remoto.** Consultada el 20 de mayo de 2020 en: https://www.nettix.com.pe/documentacion/administracion/vpn/cual-es-la-diferencia-entre-una-conexion-vpn-y-una-conexion-de-escritorio-remoto

Tecnozero (2019). **Escritorio remoto vs red privada virtual.** Consultada el 20 de mayo de 2020 en: https://www.tecnozero.com/blog/escritorio-remoto-vs-red-privada-virtual/

ANEXO 1 (CONFIGURACIÓN DEL ROUTER AXE)

```
R1#show running-config
Building configuration...
Current configuration : 1355 bytes
version 15.1
service password-encryption
security passwords min-length 10
hostname R1
login block-for 120 attempts 3 within 120
enable secret 5 $1$mERr$858QIme1tjEe7KvlcaK9Z.
username axe privilege 15 secret 5 $1$mERr$h0yfa86jrotowS/Mg.4Dl.
license udi pid CISCO1941/K9 sn FTX15243OD4-
no ip domain-lookup
ip domain-name axetelecom
spanning-tree mode pvst
interface GigabitEthernet0/0
 description LAN AXE TELECOM
 ip address 192.168.0.1 255.255.255.224
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 description WAN AXE
 ip address 200.200.200.1 255.255.255.252
```

```
banner motd ^CProhibido el acceso a la red, sin autorizacion^C
line con 0
 exec-timeout 5 0
 password 7 0820544B
 login
line vty 0 4
 exec-timeout 5 0
 password 7 0820544B
 login local
 transport input ssh
end
```

ANEXO 2 ENRRUTAMIENTO, INTERFACES DEL ROUTER

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.0.1     YES manual up                    up
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial0/0/0                200.200.200.1   YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
Vlan1                      unassigned      YES unset  administratively down down
R1#
```

ANEXO 3 CONFIGURACION DEL SWITCH AXE

```
S1#show running-config
Building configuration...
Current configuration : 1533 bytes
version 12.2
service password-encryption
hostname S1
enable secret 5 $1$mERr$858QIme1tjEe7KvlcaK9Z.
no ip domain-lookup
ip domain-name axe.com
username telecom secret 5 $1$mERr$x5sJ0mbl6OpAdMDZ.mBdx0
interface Vlan1
 description LAN Local
 ip address 192.168.0.30 255.255.255.224
ip default-gateway 192.168.0.1
banner motd ^CProhibido el acceso a la red, sin autorizacion^C
line con 0
 password 7 0820544B
 login
 exec-timeout 5 0
line vty 0 4
 exec-timeout 5 0
 password 7 0820544B
 login local
 transport input ssh
line vty 5 15
 exec-timeout 5 0
 password 7 0820544B
 login local
```

```
 transport input ssh
end
```

ANEXO 4 ENRRUTAMIENTO, INTERFACE DEL SWITCH

S1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	up	up
FastEthernet0/3	unassigned	YES	manual	up	up
FastEthernet0/4	unassigned	YES	manual	up	up
FastEthernet0/5	unassigned	YES	manual	up	up
FastEthernet0/6	unassigned	YES	manual	up	up
FastEthernet0/7	unassigned	YES	manual	up	up
FastEthernet0/8	unassigned	YES	manual	up	up
FastEthernet0/9	unassigned	YES	manual	up	up
FastEthernet0/10	unassigned	YES	manual	up	up
FastEthernet0/11	unassigned	YES	manual	down	down
FastEthernet0/12	unassigned	YES	manual	down	down
GigabitEthernet0/1	unassigned	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	manual	down	down
Vlan1	192.168.0.30	YES	manual	up	up