REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSÉ ANTONIO PÁEZ

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

IMPLEMENTACIÓN DE UNA RED V.P.N. PARA INTERCONEXIÓN DE LOS DEPARTAMENTOS EN LA SEDE PRINCIPAL DE LA EMPRESA "TODO HIERRO SD C.A.", UBICADA EN SAN DIEGO, EDO. CARABOBO.

Proyecto del Trabajo de Grado presentado para optar al título de

INGENIERO DE TELECOMUNICACIONES

Autor:

Silva, Jesus

C.I 27725376

Tutor: Ing Agustin Larez

Urb. Los tamarindos, calle Nº 2. Municipio San Diego
Teléfono: (0241) 8965688 (master)

AGRADECIMIENTOS

A Dios y a la virgen del Valle, toda gratitud por darme la voluntad y sabiduría, para seguir a pesar de las dificultades, por darme salud, alegrías, coraje y paz en momentos de adversidad, te amo Señor, gracias.

A mi Compañero y amigo, por el apoyo durante la realización de este trabajo y durante nuestros estudios, gracias.

A mi preparador y gran amigo, Alexander Martinez, quien siempre estuvo presente en todo momento, en cada materia y cada semestre, gracias por siempre apoyarme. Mil gracias.

Al Profesor y tutor, Ing Agustin Larez por darme todo su apoyo durante mi crecimiento educativo, al momento de cursar las materias y durante la elaboración de esta tesis.

A mis compañeros de la universidad, gracias por estar presentes en mi camino y por tantos momentos de risas y experiencias únicas.

Agradezco cordialmente, a cada una de las personas que de una u otra manera aportaron un granito de arena para que yo pudiera alcanzar esta meta, por sus buenos sentimientos, y muestras de apoyo, a los que siempre estuvieron prestos a ayudarme de manera incondicional.

DEDICATORIA

A Dios y a la Virgen del Valle, por darme la oportunidad de crecer como persona, lograr mis metas, compartir mis logros con mis seres queridos y por darme la paciencia y sabiduría a lo largo del camino y darme la dicha de afrontar todas las adversidades que se presentaron en él, siempre acompañándome y guiándome en cada paso que doy.

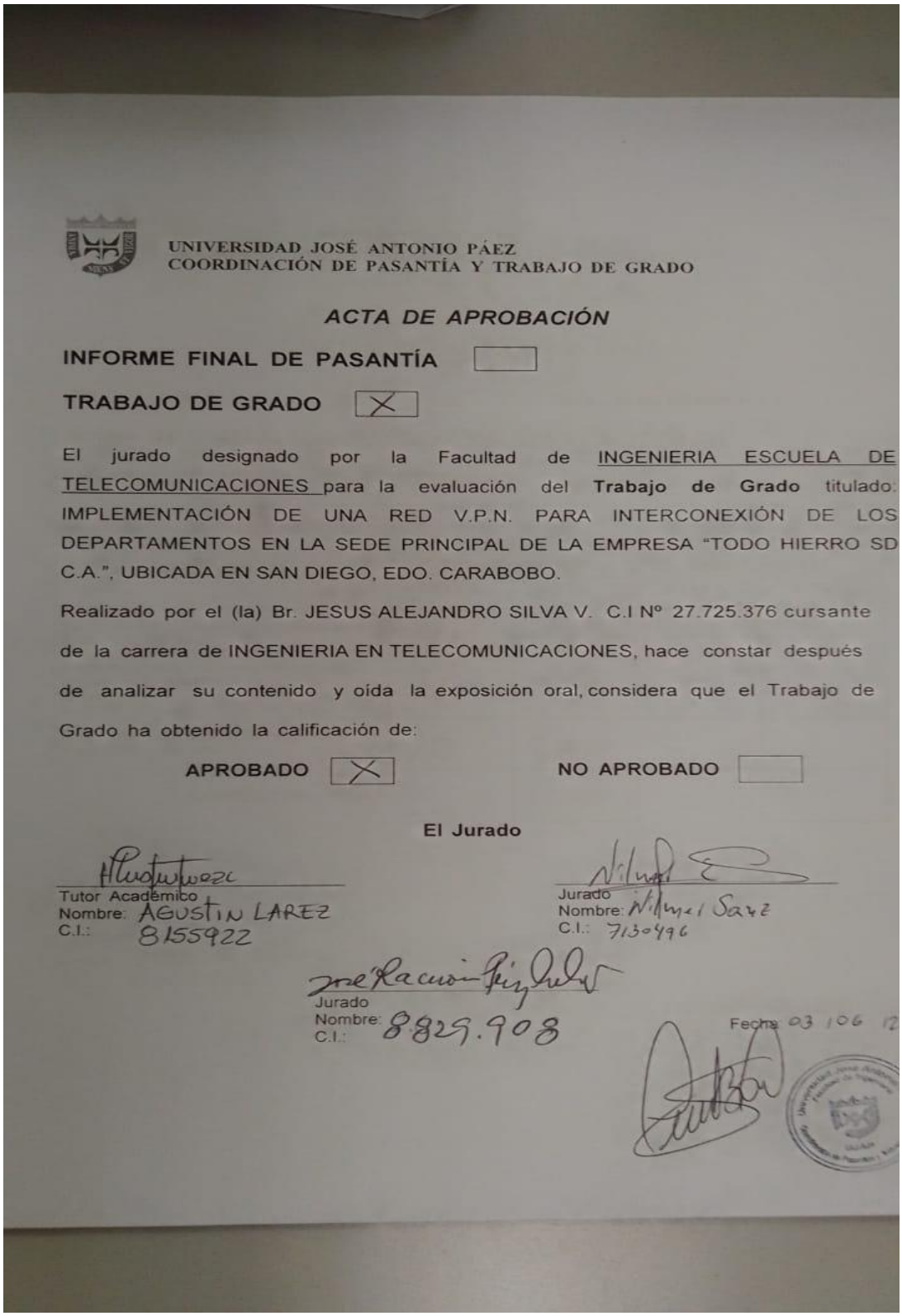
A mis padres, Carmen Yoleida Valera y Armando Rafael Paez, por ser los pilares fundamentales de mi vida, brindándome siempre su amor y su apoyo incondicional, por aconsejarme sabiamente y sobre todo por haber inculcar en mi los valores y principios que hoy en día me permiten ser quien soy, por ser ejemplos de trabajo, dedicación y amor por su familia.

A mi hermana, Maria Alejandra Silva, por siempre estar presentes, brindarme su apoyo durante 4 años de carrera, gracias por ser para mí un motivo de alegría y orgullo.

A mi pareja, Itzel Carolina Rayes, por ser también un pilar tan importante en mi vida, por apoyarme y acompañarme en este camino, siempre brindándome ánimos y amor incondicional.

A mis familiares, que desde la distancia me apoyaron y de los cuales recibí uno que otro consejo que me ayudo en tan arduo camino, por ser ejemplo de unión y apoyo incondicional.

A todos, muchísimas gracias…



UNIVERSIDAD JOSÉ ANTONIO PÁEZ
COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO

ACTA DE APROBACIÓN

INFORME FINAL DE PASANTÍA [ ]

TRABAJO DE GRADO [X]

El jurado designado por la Facultad de INGENIERIA ESCUELA DE TELECOMUNICACIONES para la evaluación del **Trabajo de Grado** titulado: IMPLEMENTACIÓN DE UNA RED V.P.N. PARA INTERCONEXIÓN DE LOS DEPARTAMENTOS EN LA SEDE PRINCIPAL DE LA EMPRESA "TODO HIERRO SD C.A.", UBICADA EN SAN DIEGO, EDO. CARABOBO.

Realizado por el (la) Br. JESUS ALEJANDRO SILVA V. C.I Nº 27.725.376 cursante de la carrera de INGENIERIA EN TELECOMUNICACIONES, hace constar después de analizar su contenido y oída la exposición oral, considera que el Trabajo de Grado ha obtenido la calificación de:

APROBADO [X] **NO APROBADO** [ ]

El Jurado

Tutor Académico
Nombre: AGUSTIN LAREZ
C.I.: 8155922

Jurado
Nombre: Nilmar Saez
C.I.: 7130496

Jurado
Nombre:
C.I.: 8.829.908

Fecha 03 / 06 / 12

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
DECANATO DE INGENIERÍA

FI T 001 2022-1CR TG

Valencia, 27 de abril de 2022

Ciudadano:
SILVA VALERA, JESUS ALEJANDRO
27.725.376

Presente -

Cumplo con informarle que la comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión **N° 3-2022** de fecha **16/02/2022** aprobó el proyecto de grado titulado:

Implementación de una red V.P.N. para la interconexión de los departamentos en la sede principal de la empresa "TODO HIERRO SD C.A.", ubicada en San Diego, Edo. Carabobo.

Presentado por usted como requisito para optar al título de Ingeniero en Telecomunicaciones

Se ratifica la designación del Tutor Académico que lo asesorará en el desarrollo de este proyecto a:
Ing. Agustín José Larez Coburuco, titular de la cédula de identidad V- 8.155.922

Atentamente

Dr. Francisco Gelanzé Sevilla.
Decano de Ingeniería

c.c. Coordinación de Pasantías y Trabajo de Grado

ANEXO N

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

CONSTANCIA DE APROBACIÓN PARA LA PRESENTACIÓN PÚBLICA DEL TRABAJO DE GRADO

Quien suscribe, Ing. Agustín José Larez Coburuco, portador(a) de la cedula de identidad N^0 V-8.155.922, en mi carácter de tutor (a) del trabajo de grado presentado por el(la) los ciudadanos(a) Jesus Alejandro Silva Valera, portador(es) de la cedula de identidad N^0 V-27.725.376, titulado **Implementación de una red V.P.N para interconexión de los departamentos en la sede principal de la empresa "TODO HIERRO SD C.A.", ubicada en San Diego, Estado Carabobo,** presentado como requisito parcial para optar al titulo de ingeniero en telecomunicaciones, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe.

En San Diego, a los 10 días del mes de mayo del año dos mil veintidós.

Ing. Agustín José Larez Coburuco
C.I. V-8.155.922

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

INSTRUMENTO DE RECOLECCIÓN DE DATOS (ENCUESTA)

OBJETIVO: Diagnosticar las debilidades de los servicios actual de telecomunicaciones en la empresa "Todo Hierro SD C.A" ubicada en San Diego, Estado Carabobo.
INSTRUMENTO: El presente formulario contiene las preguntas de la encuesta que va dirigida a los empleados de la empresa, la cual esta compuesta por 10 ítems. La información aportada por usted se utilizada solo para fines de mi investigación titulada **"IMPLEMENTACIÓN DE UNA RED V.P.N. PARA INTERCONEXIÓN DE LOS DEPARTAMENTOS EN LA SEDE PRINCIPAL DE LA EMPRESA "TODO HIERRO SD C.A.", UBICADA EN SAN DIEGO, EDO. CARABOBO"**, y será utilizada de manera confidencial.

1. ¿Tiene usted algún proveedor de servicios de Telecomunicaciones por fibra óptica?
2. ¿Cuenta usted con algún proveedor de servicios de Telecomunicaciones por enlace inalámbrico?
3. ¿Posee usted intermitencias de señal con su actual proveedor de servicios de internet?
4. ¿Está usted conforme con la velocidad en la que navega actualmente con su proveedor de servicios de internet?
5. ¿Se ve usted afectado por problemas de conectividad en otras áreas?
6. ¿Conoce usted otro sistema de Telecomunicaciones distinto al que utiliza actualmente?
7. ¿Sabe usted que es una red VPN?
8. ¿Conoce usted para que sirve una Red VPN?
9. ¿Estima usted que una implementación de una red de VPN beneficie la calidad de interconexión en la empresa TODO HIERRO en el sector Macomaco de San Diego?
10. ¿Estaría usted dispuesto a adquirir y cancelar mensualmente los planes que se ofrecen para el disfrute de esta red VPN?

INDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

ÍNDICE DE GRAFICOS

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

IMPLEMENTACIÓN DE UNA RED V.P.N. PARA INTERCONEXIÓN DE LOS DEPARTAMENTOS EN LA SEDE PRINCIPAL DE LA EMPRESA "TODO HIERRO SD C.A.", UBICADA EN SAN DIEGO, EDO. CARABOBO.

Autores: Silva, Jesus.
Tutor: Ing. Agustín Lares
Fecha: Noviembre 2021.

RESUMEN

Hoy en día un gran número de estudiantes, profesionales e investigadores en el área de la Ingeniería Telecomunicaciones se ven en la necesidad de cómo extender el marco de las comunicaciones creando radioenlaces con el fin de poder interconectar gente para que estas mismas aprovechen de estas nuevas tecnologías. Sin embargo, no todas las empresas tienen acceso a estas tecnologías es por esto que se pensó Diseñar una Red Privada Virtual para dar acceso a Internet entre la sede principal de la empresa "TODO HIERRO SD C, A", ubicada en San Diego estado Carabobo. La cual es de gran ayuda ya que esta empresa se encuentra en total desconexión entre las otras sedes actuales, ya que no puede ser conectada a un servicio de Internet por su ubicación geográfica, y es de necesario este servicio ya que la empresa se encuentra en ascenso y necesita de este primordial servicio para poder cumplir con sus labores. Por otro la incorporación de una Red Virtual Privada (V.P.N), también es necesaria ya que las personas o trabajadores afuera de la empresa podrían ingresar a la red y monitorear todos sus enlaces y operadores. Por otro lado, el proyecto de investigación está enmarcado dentro de la modalidad de investigación de proyecto factible especial, bajo los lineamientos de la investigación de campo, con un nivel descriptivo siguiendo la línea de investigación ciencias cognitivas y aplicadas.

Descriptores: red virtual privada, radioenlace, internet.

INTRODUCCIÓN

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

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

Este conjunto se conoce actualmente como configuración VPN de redes, y muchas empresas comienzan a utilizarlo, ya sea para interconectar sub-redes como teletrabajadores. Cuando un empleado se conecta a Internet, la configuración de las VPN les permite "perforar" la red privada de la compañía y navegar en la red como si estuvieran en la oficina. En la actualidad existen dispositivos especiales que otorgan niveles de seguridad esenciales para realizar enlaces remotos entre empresas, a estos equipos se les conoce como equipos VPN.

Por otro lado, los sistemas de radioenlace digitales se han convertido en muchos aspectos en un elemento central del proceso evolutivo. En las telecomunicaciones

móviles su uso está muy extendido, pues la interconexión de las estaciones bases resulta ser muy interesante desde el punto de vista económico. Se prevee una utilización similar en el caso de las redes personales inalámbricas. Los radioenlaces digitales se utilizan para conectar islas de redes de áreas locales a las líneas principales, tanto para integrarlas en redes privadas nacionales o internacionales como para permitir el acceso a las redes públicas con conmutación. También es gratificante como ver el despliegue de los sistemas de radioenlace digitales en todo el país en desarrollo y en las regiones de población escasa, poniendo al alcance de mucha gente los medios de telecomunicaciones, como es el caso de nuestro país y sobre todo en algunos estados.

Es por esto que el objetivo principal del trabajo de grado es implementar de una red V.P.N. para interconexión de los departamentos en la sede principal de la empresa "TODO HIERRO SD C.A.", ubicada en san diego, edo. Carabobo.

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

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

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

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

Capítulo IV: este capítulo se hablará de los recursos utilizados para por realizar este proyecto.

CAPÍTULO I
EL PROBLEMA

1.1 Planteamiento del problema

Tras el surgimiento de la pandemia llamada COVID-19 las empresas se han visto afectadas por el confinamiento, generando pérdidas en la productividad y seguridad de sus empleados. Dada esta problemática algunas empresas se han visto en la obligación de implementar este tipo de tecnologia; la cual permite crear una red local sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet de forma remota. Por consiguiente, Obtienes un modo más seguro de proteger los datos de tu empresa y cuidar tu red de fugas de privacidad, cibercrimen y malware.

Es por esto, que una red de este tipo consiste en una tecnología que permite el acceso de los usuarios, trabajar desde otros países y hacer uso de servicios que en ese país no están disponibles, este proceso disfraza su dirección IP cuando utiliza internet, lo que vuelve invisible su ubicación para todos.

Sin embargo, en la actualidad es necesario que las instituciones, empresas o microempresas estén actualizadas al avance tecnológico, para así poder tener un mejor control de la información y la comunicación entre los usuarios y empleados que conforma la institución o empresas.

Actualmente en la empresa Todo Hierro SD C.A, ubicada en San Diego, Estado Carabobo, en el Sector Macomaco, cuenta de 02 locales, con planta alta de aproximadamente 288 m^2. Esta empresa se encarga de la distribución de materiales de construcción, ferretería en general al mayor y detal.

Por otra parte, en la empresa Todo Hierro SD C.A no cuenta con un sistema de red para interconectar los departamentos de ventas, administración, sistema, marketing, gerencia entre otros. Por ende, los empleados no pueden realizar las actividades laborales fuera de las instalaciones, al momento del confinamiento, trayendo como inconvenientes retrasos en el crecimiento tecnológico. Es importante que en la empresa se logre un sistema de red que permita mantener comunicación con los servidores de la misma ya que los empleados y administrativos requieren de información para poder realizar sus labores diarias en momentos de pandemia.

Por lo tanto, es importante llevar de la mano una red de internet con la tecnología Virtual Private Network (VPN) ya que esta surge como un medio para utilizar el canal público de Internet para comunicar datos privados utilizando llamadas locales, proporcionando además seguridad a través de técnicas de encriptación y encapsulamiento.

Con la implementación de la red privada virtual que cuente con un servidor privado y otorgue el acceso de los empleados fuera de las instalaciones, es decir, de forma remota a la empresa Todo Hierro SD C.A ayudando a su progreso y ampliación en el ámbito tecnológico.

1.2 Formulación del problema

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

¿Cómo se puede mejorar los servicios de telecomunicaciones entre los departamentos en la sede principal de la empresa “Todo Hierro SD C, A”?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

Implementar una Red Privada Virtual para interconectar todos los departamentos de “Todo Hierro SD C.A” ubicada en San Diego, Estado Carabobo.

1.3.2 Objetivo Específicos

- Diagnosticar las debilidades de los servicios actual de telecomunicaciones en la empresa “Todo Hierro SD C.A” ubicada en San Diego, Estado Carabobo.
- Identificar los parámetros, dispositivos, entornos para el cálculo del radioenlace y para el diseño de la Red Virtual Privada (VPN) en la empresa “Todo Hierro SD C.A” ubicada en San Diego, Estado Carabobo.
- Implementar el sistema de la red privada virtual VPN en la empresa “TODO HIERRO SD C, A”, ubicada en San Diego estado Carabobo.
- Realizar un estudio de viabilidad social, ambiental y de costos que tiene el presente proyecto en la empresa “TODO HIERRO SD C, A”, ubicada en San Diego estado Carabobo.

1.4 Justificación

El presente trabajo de investigación tiene como objetivo Realizar una Red Privada Virtual para interconectar todos los departamentos de “Todo Hierro SD C.A” ubicada en San Diego, Estado Carabobo.

Se observa que es necesario el diseño de un sistema de red privada virtual (V.P.N) ya que se estaría brindado la comunicación a la empresa Todo Hierro SD C.A y esto mejoraría los procesos de envío y recepción de información, así como también mejorando la comunicación entre sus diferentes departamentos, a través de una forma remota bien sea fuera o dentro de la empresa.

Asimismo, la investigación ofrece a la Universidad José Antonio Páez el incentivo a los demás estudiantes a investigar más en el área de las telecomunicaciones y conexiones, ya que esta propuesta puede impulsar y ser implementada no solo en la empresa, si no en otras empresas que estén alejadas de esta tecnología, puesto que la realización de una red privada virtual genera e impulsa a la empresa.

1.5 Alcance de la Investigación

Con la investigación se pretende llegar a la realización una Red Privada Virtual para interconectar todos los departamentos de “Todo Hierro SD C.A” ubicada en San

Diego, Estado Carabobo. El cual permita a la empresa dar a sus empleados acceso remoto a la sede ubicada en San Diego, Edo Carabobo desde otra parte del país sin necesidad de estar en las instalaciones y solucionar problemas inesperados.

1.6 Limitaciones

Al implementar una solución de Red Privada Virtual, se desea facilitar un acceso controlado a los recursos informáticos dentro de la empresa. La conexión deberá permitir a los usuarios autorizados conectarse fácilmente a los recursos corporativos de la red e igualmente debe garantizar la privacidad. Las imitaciones en este tipo de proyectos presentan diferentes particularidades, en este caso, es el tiempo un factor limitante al desarrollo del trabajo, puesto que este pudiera no ser suficiente para la mayor profundización en el periodo evaluado. Así mismo, en cuanto al factor económico, es importante considerar el estudio de factibilidad de los equipos para poder desarrollar la red privada de alta calidad.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes

González, G. (2019) en su trabajo de grado **"Diseño de un Sistema de Radioenlace para comunicaciones en el ámbito Industrial".** Presentado en la Universidad Oberta de Catalunya para optar por el título de Grado en Tecnologías de Telecomunicación. España. La investigación tuvo como propósito aportar el estudio necesario sobre el diseño a realizar en una comunicación de radioenlace entre dos plantas de la misma empresa, que se sitúan en pueblos contiguos y con línea de visión directa. Para ello, se han realizado los análisis teóricos y prácticos imprescindibles de un sistema de radiocomunicación, puesto que dan la información necesaria para poder observar la viabilidad de este trabajo. Por otro lado, se analizan las especificaciones de los elementos principales y relevantes del sistema, como son las antenas, el cableado o el mástil, de modo que permitan conseguir la mejor comunicación y transmisión de la señal entre ambos edificios. De esta manera, y tras la búsqueda detallada en el mercado, se definen los componentes adecuados para el enlace.

Finalmente, mediante el uso de software como Google Earth y Radio Mobile, se realiza una simulación del sistema de radiocomunicación que permite visualizar los diferentes parámetros que se obtendrán en la antena receptora, teniendo en cuenta las características obtenidas en los análisis. Con ello, se consigue un diseño satisfactorio donde se cumplen los mínimos necesarios para la correcta recepción de la señal.

El proyecto se vincula con el actual en función de la selección del software Google Earth y Radio Mobile, la cual es necesaria para el cálculo de este Radioenlace ya que permite la visualización de ciertos parámetros necesarios para el desarrollo de este trabajo de grado.

De la misma manera 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 otra parte, Villares, C (2017), en su investigación denominada: **"Sistema de comunicación para la transmisión de la información entre la matriz y la sucursal de la distribuidora de material de construcción "FREVI" en la Ciudad de Ambato"** para optar por el título de Ingeniero Electrónica y Comunicaciones presentado en la Universidad Técnica de Ambato en la Facultad de Ingeniería en Sistemas Electrónicas e Industrial, Ecuador (Ambato). El presente trabajo explica el problema real de la empresa; el cual se procedió a investigar y se concluyó que la misma presenta deficiencia en la comunicación de datos entre la oficina matriz y la

sucursal de la Distribuidora de Materiales de Construcción “FREVI”, por este motivo se realizó un diseño de sistema de comunicación que servirá para alcanzar los objetivos y metas deseadas en el presente proyecto, teniendo como resultado el mejoramiento de la transferencia de información, coadyuvando al incremento en el nivel de ventas y la rentabilidad de la empresa.

Sin embargo el proyecto efectuado está basado en fundamentos tecnológicos, además que el objetivo primordial es transmitir datos desde la matriz hacia la sucursal de la empresa; teniendo en cuenta estos antecedentes se realizó el enlace Radio eléctrico, pues con la existencia de un sistema de comunicación la empresa comenzaría a tener eficacia y eficiencia en prestar sus servicios, donde los beneficiados serían los clientes externos y principalmente los clientes internos pues tendrán mejor accesibilidad a los datos de la empresa.

La investigación citada, se vincula con la actual en función de cómo desarrollar los requerimientos y criterio técnicos para el diseño del cálculo del radioenlace, el cual explica cómo se puede determinar el ancho de banda necesario para las distintas aplicaciones a usar, como calcular los enlaces, la zona de Fresnell, línea de vista entro otros factores muy importantes para el desarrollo de este trabajo de grado.

2.2 Bases teóricas

2.2.1 Telecomunicaciones

Las Telecomunicaciones para la Unión Internacional de Telecomunicaciones, con su primer estándar ITU 1932, “Es toda transmisión, emisión o recepción de signos, señales, datos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de cables, medios ópticos, físicos u otros sistemas electromagnéticos.” Las telecomunicaciones, es el intercambio de señales que pueden llevar cualquier clase de información como datos, voz video, etc., emitidas desde un transmisor a un receptor a cualquier tipo de distancia mediante procedimientos electromagnéticos por un medio guiado o no guiado.

2.2.2 Sistema de Comunicación

Los Sistemas de Comunicación, es el conjunto de medios (transmisión y conmutación), tecnologías (procesado, multiplexación, modulación), protocolos y facilidades en general, por el cual se transmite una o varias señales para el intercambio de información en una extensión territorial y que abarcan diversos servicios entre el transmisor y el receptor.

2.2.2.1 Clasificación de los Sistemas de Comunicaciones

La clasificación de las telecomunicaciones es la siguiente:

a) **Las Telecomunicaciones Terrestres**: las telecomunicaciones terrestres son aquellas cuyo medio de propagación son líneas físicas, estas pueden ser cables de cobre, cable coaxial, fibra óptica, par trenzado, etc.

b) **Las Telecomunicaciones Radioeléctricas:** las telecomunicaciones radioeléctricas son aquellas que utilizan como medio de propagación la atmósfera terrestre, transmitiendo las señales en ondas electromagnéticas, ondas de radio, microondas, etc. dependiendo de la frecuencia a la cual se transmite.

c) **Las Telecomunicaciones Satelitales:** las telecomunicaciones satelitales son aquellas comunicaciones radiales que se realizan entre estaciones espaciales, entre estaciones terrenas con espaciales o entre estaciones terrenas (mediante retransmisión en una estación espacial). Las estaciones espaciales se encuentran a distintas alturas fuera de la atmósfera.

2.2.2.2 Caracterización de los Sistemas de Comunicaciones

La Caracterización de los Sistemas de Comunicación se basan en:

- ✓ **Direccionalidad.**

a) Redes de comunicaciones unidireccionales: Las redes de comunicaciones unidireccionales son cuando la información viaja desde un emisor a un receptor, no existiendo camino de retorno para la comunicación inversa. Este tipo de comunicaciones se suele encontrar en las redes de difusión o distribución.

b) **Redes de comunicaciones bidireccionales o interactivas:** Las redes de comunicaciones bidireccionales dícese a la información que viaja en los dos sentidos entre sus extremos, típicamente por el mismo camino, aunque también existen redes en que no tiene porque coincidir los caminos de ida y vuelta. Algunos ejemplos son las redes de telefonía y de datos.

c) **Redes híbridas: las** redes hibridas son las que se integran diferentes tipos de redes; por ejemplo, una red unidireccional para un sentido de la comunicación es combinada con otra red para el camino de retorno. Estas soluciones fragmentarias permiten tener, por ejemplo, servicios interactivos de televisión, en la que ésta es recibida por la red de difusión terrestre o por satélite, mientras que las selecciones del usuario y sus peticiones de vídeo bajo demanda (VoD), se envían por Internet (sobre la red telefónica).

2.2.3 Ancho de Banda

El ancho de banda de un sistema de comunicaciones es la banda de paso mínima (rango de frecuencias) requerida para propagar la información de la fuente a través del sistema. El ancho de banda de un sistema de comunicaciones debe ser lo suficientemente grande (ancho) para pasar todas las frecuencias significativas de la información.

En cuanto al ancho de banda, hay que señalar que los tipos de información que pueden circular por las redes son muy variados, en cuanto a su naturaleza, tratamiento, degradación y, particularmente de muy distinto ancho de banda. Dentro del ancho de banda de una señal quedan recogidas todas las frecuencias distintas que incorpora la señal. Las variaciones de frecuencia de una señal de voz son muy inferiores a las de una imagen movimiento (vídeo). La tecnología requerida en cada caso es muy distinta; la frecuencia es la variable fundamental del diseño de sistemas de comunicaciones, en sus aspectos de transporte de señal. De aquí, se puede hablar de redes de banda ancha cuando la información que manejan ocupa un rango de frecuencias elevado y de banda estrecha en caso contrario. Además, en determinados usos de las redes de comunicaciones, uno de los extremos genera mucha más información que el otro, lo

que tiene implicaciones relativas a la ubicación de las infraestructuras de mayor ancho de banda, en el sentido emisor-receptor o en el inverso.

2.2.4 Red

Las redes y en general el uso de ordenadores en las organizaciones, empresas o industrias hoy en día se han incorporado de una manera creciente, y constituyen parte importante de la producción. Una red corresponde a dos o más PC interconectados entre sí para lograr una comunicación, intercambio de datos y a la vez poder compartir recursos. Debe estar configurada de tal forma que sea compatible a estándares de conectividad preestablecidos. En la actualidad existen varios tipos de redes, es decir están confeccionadas de maneras diferentes según normativas, topologías o equipos que hacen posible la interconexión.

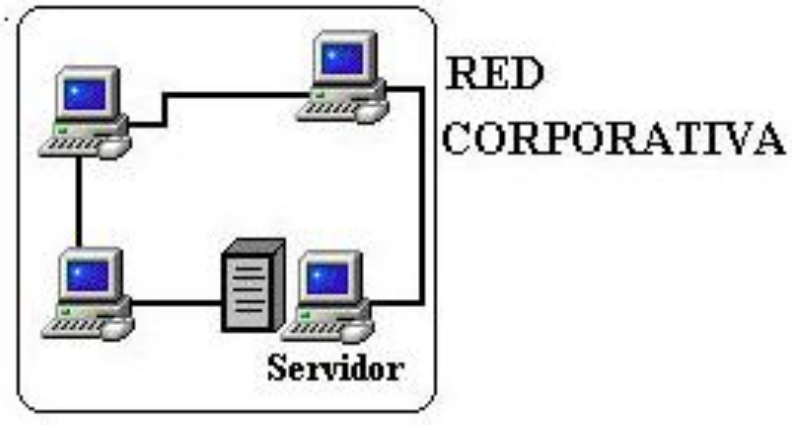


Figura 1. Estructura básica de una RED
Fuente:http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf

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

2.2.4.1 Tipos de Redes de Comunicación

Existen Redes de Comunicación en función de que la información se reciba por un usuario determinado, un conjunto determinado de ellos, o un número indeterminado de los mismos, las cuales se clasifican en:

- **Redes de difusión:** las redes de difusión, es cuando la información enviada se recibe en cualquier terminal conectado, recibiendo todos los usuarios la misma información y a la vez. El ejemplo típico son las redes de televisión convencionales en cualquiera de sus formas de transporte, cable, satélite o terrenal.
- **Redes conmutadas:** las redes conmutadas consisten en que cualquier usuario conectado a la red puede intercambiar información con otro conectado a la misma, mediante el establecimiento de la conexión entre los terminales extremos. El ejemplo más conocido son las redes de telefonía. El uso del correo electrónico sobre Internet es otro ejemplo de comportamiento punto a punto.

Las Redes de Comunicación en función a los flujos de información con respecto a su origen y destino y es prácticamente paralela con la anterior, se clasifican en:

- **Redes punto a punto:** las redes punto a punto, es un extremo (usuario) que entabla comunicación con otro, y la arquitectura de la red mantiene separados y diferenciados estos flujos de información. Ejemplos típicos son la telefonía (fija o móvil).
- **Redes punto a multipunto:** las redes punto a multipunto, es cuando un usuario o terminal mantiene un flujo de información simultáneamente con varios terminales. En caso de que los "usuarios multipunto" puedan generar información, la información que transmiten cada uno de ellos es recibida exclusivamente por el "usuario punto", quién a su discreción la hará visible al resto de "usuarios multipunto". Un ejemplo típico es la difusión de TV, o las aplicaciones de teleeducación por videoconferencia.

- **Redes multipunto a multipunto:** las redes multipunto a multipunto se dice a todos los usuarios que pueden comunicarse simultáneamente con el resto. Un esquema de este tipo se encuentra en los sistemas de chat o también en los de juego en red.

Las redes de comunicación según su alcance o tamaño se clasifican en:

- **Red de Área Local (LAN):** Una red LAN consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre dispositivos y el medio y regular el orden de acceso al mismo, para lograr velocidades de transmisión de datos altas en distancias relativamente cortas.
- **Red de Área Metropolitana (MAN):** Las redes de área metropolitanas están diseñadas para la conexión de equipos a lo largo de una ciudad entera. Una red MAN puede ser una única red que interconecte varias redes de área local LAN resultando en una red mayor. Por ello, una MAN puede ser propiedad exclusivamente de una misma compañía privada, o puede ser una red de servicio público que conecte redes públicas y privadas.
- **Red de Área Extensa (WAN):** Las Redes de área extensa son aquellas que proporcionen un medio de transmisión a lo largo de grandes extensiones geográficas (regional, nacional e incluso internacional). Una red WAN generalmente utiliza redes de servicio público y redes privadas y que pueden extenderse alrededor del globo.

2.2.5 Red Privada

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

2.2.6 Red Privada Virtual (VPN)

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

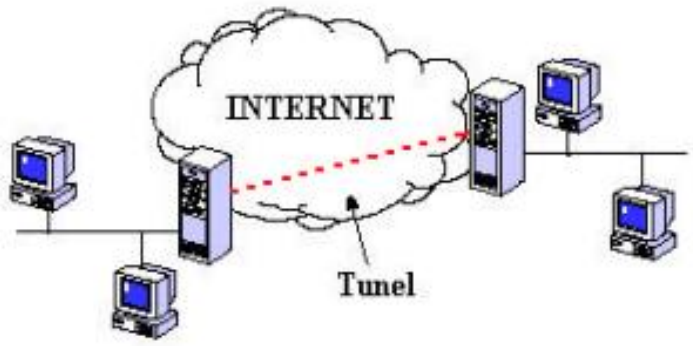


Figura 2. Red Virtual Privada VPN.
Fuente:http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf

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

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

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

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

2.2.6.1 Requisitos para una Red VPN

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

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

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

2.2.6.2 Razones por las cuales es recomendable implementar una VPN

- **Reducción de Costos:** Para una implementación de red que abarque empresas alejadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto) de muy alto costo que caracterizaron a muchas empresas privadas, siendo reemplazadas por ejemplo, por acceso ADSL de un ancho de banda alto y bajo costo, disponible por lo general en la mayoría de las zonas urbanas sin mayores problemas. Los usuarios remotos móviles podrán ahorrar altos costos de llamadas telefónicas de larga distancia, bastando con que disque un proveedor de acceso local a la Internet (no IP fija).
- **Alta Seguridad:** Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, dando un resultado comparable a una red punto a punto. Protocolos como 3DES (Triple data encryption Standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP

Security) para manejo de los túneles mediante software brindan una alto nivel en seguridad al sistema. Además se utilizan varios niveles de autentificación de usuarios para el acceso a la red privada mediante llaves de ingreso, para la asegurar que el usuario es el original y no un tercero que percibe el password de autentificación.

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

2.2.6.3 Ventajas y Desventajas de una Red VPN

Ventajas

- Como tecnología de acceso avanzada ofrece múltiples posibilidades. Las opciones para la conectividad se adaptan a los requisitos de cada empresa. Los beneficios de las VPN son conocidos y además útiles para pequeñas y grandes empresas.
- Las VPN tradicionales son fáciles de implementar tanto del lado del ISP como por el del cliente. El proveedor no participa en los procesos de enrutamiento.

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

Desventajas

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

2.2.6.4 Componentes de una Red VPN

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

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

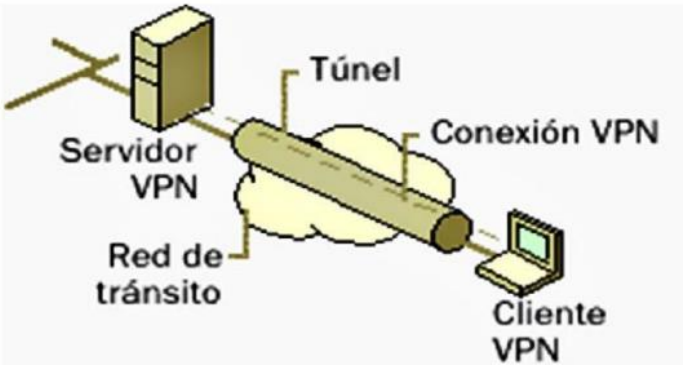


Figura 3. Componentes de una Red VPN
Fuente:http://www.equitek.com.mx/f/ERM-Conversore-Señales-Analògicas.jpg

2.2.6.5 Topologías de una Red VPN

Hay dos tipos básicos de redes VPN:

1) De Sitio a Sitio

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

conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN.

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

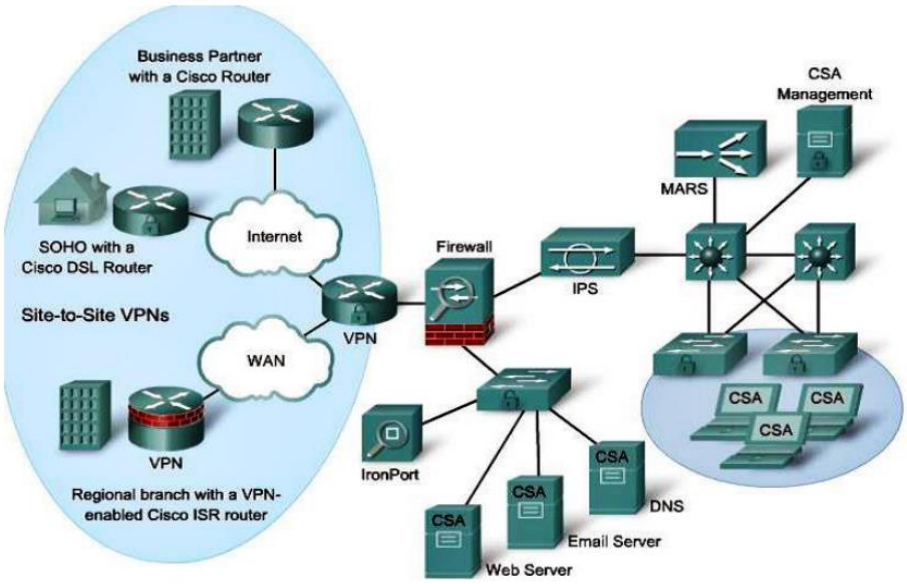


Figura 4. VPN sitio a sitio
Fuente:https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%20Jorge.pdf

2) De acceso remoto

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

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

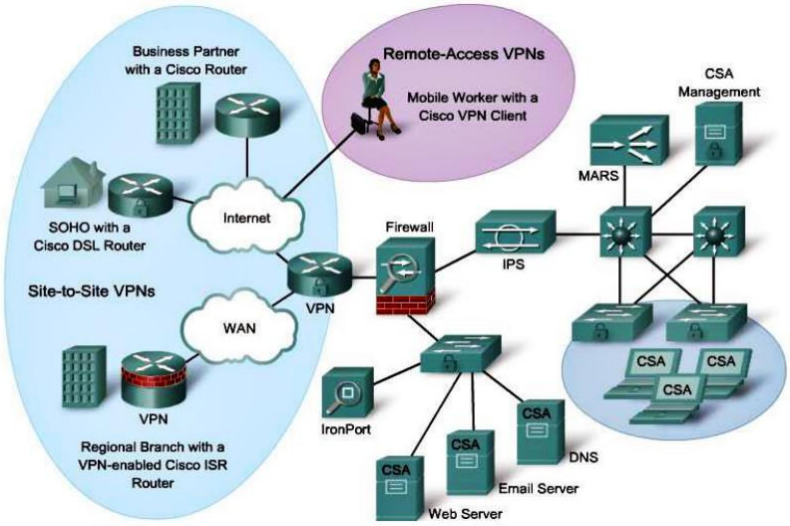


Figura 5. VPN de acceso remoto
Fuente:https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%Selector.pdf

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

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

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

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

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

Figura 6. Ventana del Software VPN Client

Fuente:https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%Selector.pdf

2.2.7 Tipos de VPN

2.2.7.1 Sistemas basados en Hardware

Las VPN basadas en Hardware poseen en el extremo del Servidor de la organización un “router” o “enrutador” dedicado el cual tiene la misión de encriptar los datos, además de abrir y cerrar los túneles VPN cuando funciona como receptor. Estos proporcionan facilidades al usuario que administra la implementación VPN, ya que son seguros, rápidos, de fácil instalación y fáciles de usar. Ofrecen un gran rendimiento ya

que no malgastan ciclos en forma tan significativa de procesamiento de operación ya que no requiere un sistema operativo, ya que este es configurado para las operaciones que requiera el servicio VPN.

2.2.7.2 Sistemas basados en Firewall

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

2.2.7.3 Sistemas basados en Software

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

2.2.8 Modelo OSI

El modelo OSI (Open System Interconnection) es el comienzo de cualquier estudio de redes. Es un modelo idealizado de 7 capas o niveles que representa la subdivisión de tareas teórica que se recomienda tener en cuenta para el estudio o diseño de un sistema. Esto no significa que todas las redes cumplan o deban cumplir exactamente con este modelo pero se recomienda siempre tener en cuenta el modelo OSI como referencia, ya que conocimiento del mismo posibilita la correcta

comprensión de cualquier red e inclusive facilita el poder realizar la comparación entre sistemas diferentes.

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

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

Las 7 capas son las siguientes:

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

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

2.2.9 Radioenlace

Una comunicación radioenlace se define como cualquier interconexión realizada entre los terminales de telecomunicación mediante ondas electromagnéticas, a través de un medio no guiado, también llamadas STL, Studio Transmitter Link (Enlace Estudio Transmisor). La frecuencia en la que trabajan estas ondas, se sitúan en el rango de microondas, es decir, en el espectro de las altas frecuencias (de 300 MHz a 300 GHz) con una longitud de onda de entre 1 m a 1 mm, aunque lo más común es el uso de frecuencias súper elevadas (SFH, Super High Frequency) donde se superan los 3 GHz. Sobre esta información, se definen las dos frecuencias que se utilizan para la comunicación, siendo una para la portadora modulada de transmisión y otra para la otra portadora de recepción. Este concepto de comunicación, se define como comunicación de tipo dúplex, donde las frecuencias de emisión y recepción constituyen el radio canal. (Ver figura 7)

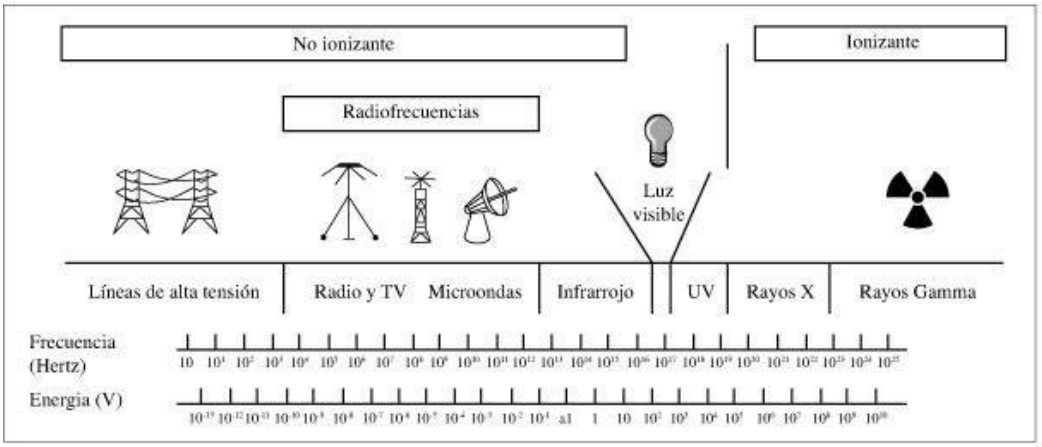


Figura 7. Frecuencias de las Telecomunicaciones.
Fuente https://es.slideshare.net/iqoscarhernandez/msho-salud- ocupacional-radiaciones-no-ionizantes-equipo-tec-generacion-72

En cuanto a la definición de un sistema de radiocomunicación, varía según las especificaciones utilizadas para los elementos en curso, esto es, existen diferentes tipos de comunicaciones según los terminales utilizados y la señal emitida.

Teniendo en cuenta la ubicación del terminal:

- **Terrestre**: todos los terminales se sitúan en la tierra, por lo tanto, se crean radioenlaces terrenales.
- **Satélite**: mínimo uno de los repetidores se encuentra en satélite. Con ello, se generan radioenlaces espaciales o por satélite.

Conforme al terminal:

- **Radioenlace de servicio móvil**: comunicaciones realizadas mediante terminales móviles.
- **Radioenlace de servicio fijo**: enlace creada entre puntos fijos situados sobre la superficie terrestre. Este sistema de comunicación realizada entre los 800 MHz y 42 GHz, facilita una capacidad de información con características de calidad y disponibilidad determinadas.

Dependiendo de la señal emitida:

- **Analógica**: fueron las primeras señales que se emitían y se consiguen con la modulación en frecuencia.
- **Digital**: son más actuales que las analógicas y se crean mediante la modulación por conmutación de fase o por amplitud en cuadratura. Este tipo se señales permiten la regeneración de los datos y constan de una mayor tolerancia frente a ruidos e interferencias.

2.2.9.1 Elementos de un Radioenlace

Los elementos principales de un sistema de radioenlace punto a punto son las antenas, sobre todo las transmisoras y las receptoras; ya que, son las encargadas de emitir y captar, respectivamente, la señal a enviar. Pero en una comunicación en radiofrecuencia también pueden existir otros dispositivos de apoyo, cuales ayudarán en aquellos casos en los que la señal no cumple con las condiciones mínimas establecidas para una correcta recuperación de datos. Estos elementos, se definen como estaciones intermedias y pueden ser de dos tipos. Por un lado, se encuentran los repetidores, cuáles pueden ser activos o pasivos según las especificaciones de los mismos. Los activos, bajan la frecuencia de la portadora recibida a una frecuencia intermedia (FI) para poder amplificar la señal y volver a retransmitirlo. En caso de los pasivos, reflejan la señal obtenida, como si de unos espejos se tratasen. Por otro lado, se encuentran las estaciones nodales, que se tratan de una sección de conmutación, la entidad de control, protección y supervisión. En estas estaciones, se demodula la señal recibida y se baja a la frecuencia de banda base, ya que, desde este punto, permiten adjuntar o eliminar diferentes canales (drop-in).

En cuanto a la estructura del sistema de radiocomunicación, está definida mediante enlaces en serie, por lo que, en caso de fallo de algún elemento, esta comunicación se detiene, es decir, el enlace se corta. Es por ello, la necesidad de equipos de alta disponibilidad y confiabilidad con redundancias frente a las averías y desvanecimientos que puedan surgir. Para ello, y teniendo en cuenta que las estaciones funcionan de forma no atendida, también son necesarios los sistemas de supervisión y

control automático que realicen dichas técnicas, cuales obtendrán información mediante las señales auxiliares de telemando y telesupervisión enviadas junto a la información útil de la señal. De esta manera, se pueden obtener los datos del estado del radio enlace en un momento determinado y así facilitar las operaciones de mantenimiento. En caso de avería, esta información deberá permitir localizar con exactitud el equipo dañado y poder comunicarse con él por telemando, enviando señales desde la central.

Propagación de la Señal

El método de propagación de la señal según Pedraza y col. (2009), la clasificación de los modelos de pérdida por propagación, puede hacerse según el ambiente de propagación, la cobertura y el origen de los datos, para una correcta transmisión de información, datos y/o voz, debe cumplir una de las condiciones más importantes en las comunicaciones inalámbricas, la línea de visión entre las antenas receptoras y transmisoras. Para ello, es necesaria la definición correcta del rango de frecuencias a utilizar en el radioenlace. Esto es debido a que, las ondas emitidas pueden ser difractadas, refractadas, reflejadas o absorbidas por la atmosfera y los diferentes obstáculos que se encuentran en el recorrido que llevan los rayos desde el emisor hasta el receptor. Por lo tanto, ha de cumplir unas especificaciones mínimas establecidas para la propagación, cuales, en caso necesario, hagan posible la correcta recuperación de la señal.

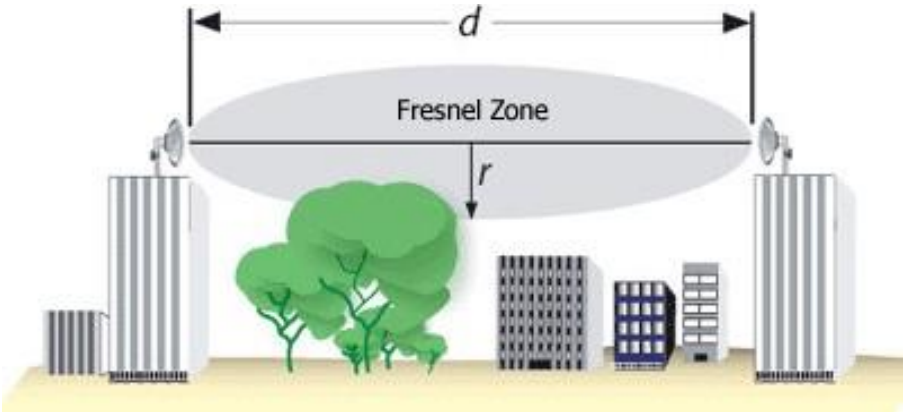


Figura 8. Zona de Fresnel 1

Fuente http://mundotelecomunicaciones1.blogspot.com/

Las ondas de radio no viajan en una línea recta entre un punto y el otro, sino en una espiral llamada Fresnel. Por este motivo, se crean dos grupos según las frecuencias de las ondas a emitir. Por un lado, se encuentran las VHF, Very High Frequency (30 MHz a 300 MHz) y UHF, Ultra High Frequency (3 MHz a 3 GHz), cuales presentan mayor tolerancia a los obstáculos y hacen posible los enlaces nLOS, Near Line of Sight (casi con línea de visión), lo cual define un trayecto parcialmente obstruido entre el emisor y el receptor de la señal. (Ver figura 8).

En cambio, para los radioenlaces superiores a 900 MHz, es necesario realizar una propagación LOS, Line of Sight (en línea de visión o visión directa); es decir, sin obstáculos en la zona Fresnel (Ver figura 9)

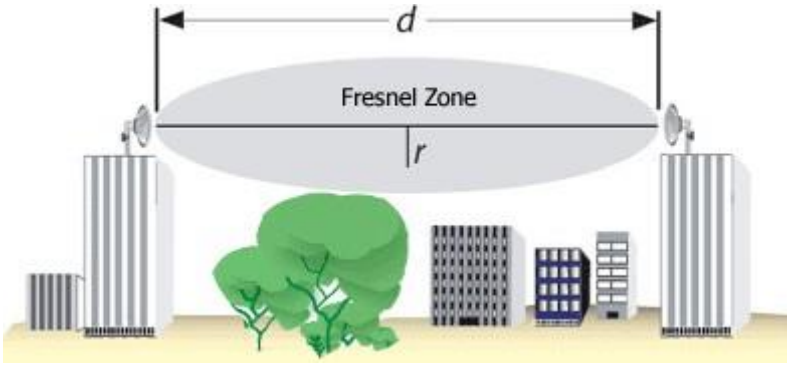


Figura 9. Zona de Fresnel 2
Fuente http://mundotelecomunicaciones1.blogspot.com/

Por lo tanto, los pasos a seguir para definir un radioenlace de una manera satisfactoria son:

- Selección del lugar de instalación de los elementos. Se debe determinar, sobre todo, la ubicación de las antenas de transmisión y de recepción. Así como en caso necesario, las estaciones intermediarias.
- Verificación del perfil del terreno en el que se va a configurar el sistema de comunicación. Es decir, se debe tener en cuenta el territorio donde se quiere

realizar el radioenlace, ya que debe cumplir la línea de visión entre las dos antenas, así como la distancia de separación entre ambas.

- Cálculos de la colocación del mástil de la antena, así como de la altura a la que instalar el elemento, con el fin de una correcta visualización.
- Cálculos completos del radioenlace, teniendo en cuenta la trayectoria que van a llevar las ondas y los efectos a los que se exponen las mismas, ya sean consecuencias naturales o producidos por el ser humano (atenuación, interferencias…)
- Pruebas posteriores a la instalación del sistema radioenlace, cuales verificarán la correcta implantación del sistema y puesta en marcha del mismo.

2.2.10 Internet

Según, Snell (1995) es una red masiva de redes, infraestructura de redes que conecta a millones de computadoras unidas de forma global; formando una sola red en la que una computadora puede comunicarse con otra siempre y cuando estén las dos computadoras conectadas a Internet. Este conecta decenas de millones de computadoras en todo el mundo, permitiéndoles comunicarse entre sí y compartir recursos. Internet es una colección de redes organizada en una estructura multinivel las cuales usan toda una variedad de tecnologías para interconectarse. En el nivel más bajo se encuentra algunas decenas o cientos de computadoras conectadas a un router, formando una LAN. Otras computadoras se conectarán a un router a través de la red telefónica usando un módem. Una empresa o universidad podrá tener varios routers enlazados a un router principal. Estos routers se encuentran conectados mediante líneas alquiladas a un router de un Proveedor de Servicios de Internet (ISP, Internet Service Provider). A su vez, el proveedor conecta sus routers a una WAN de alta velocidad llamada backbone. Un país puede tener varios backbones que conectan a todos los ISP. Finalmente, los backbones de todos los países se interconectan en una malla usando líneas internacionales. Todo esto es lo que finalmente forma Internet.

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

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

2.2.7.2 Intranet

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

2.2.7.3 Extranet

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

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

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

2.2.7.5 Acceso Remoto

Según Douglas da Silva (2021) Conectarse a una red desde una ubicación distante es lo que se denomina acceso remoto. El acceso remoto a una red ha sido algo de gran importancia en el mundo de las redes, ya que muchas compañías que promueven viajes de trabajo de sus empleados o el trabajo desde el hogar o desde una pequeña oficina remota. Y estos empleados necesitan conectarse a la red privada de la compañía para consultar ciertos archivos o correo electrónico. La necesidad del acceso remoto ha sido la causa principal del auge de las redes privadas virtuales, por lo que es preciso analizarlo un poco antes de verlo desde el punto de vista de las VPN.

2.2.8 Windows Server 2012

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

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

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

- Servicio de enrutamiento y acceso remoto: utiliza una red privada virtual (VPN) para admitir la conectividad.

- Direct Access: 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. (Ver figura 10).

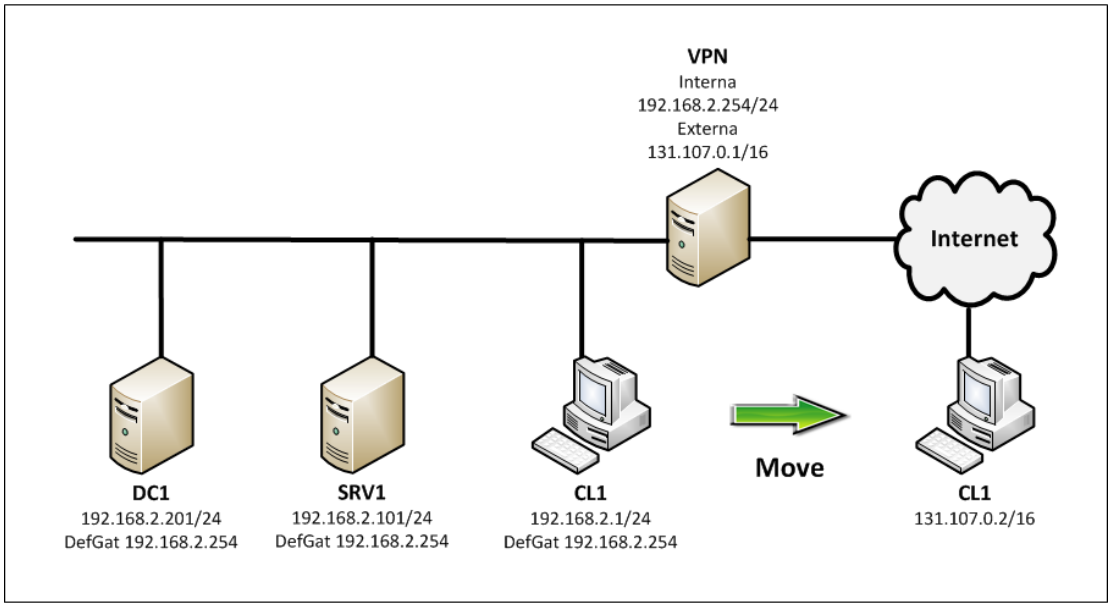


Figura 10. Modelo para Windows Server 2012
Fuente:https://tesis.ipn.mx/jspui/bitstream/1/Osciloscopio%20Karina%20y%Selector.pdf

2.3 Definición de términos básicos

Banda ancha: Capacidad para transmitir datos un canal compartido.

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

Firewall: Según (Ran95), un firewall o cortafuegos es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre dos redes. Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o

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

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

Interfaz: Es el mecanismo o herramienta que posibilita esta comunicación mediante la representación de un conjunto de objetos, iconos y elementos gráficos que vienen a funcionar como metáforas o símbolos de las acciones o tareas que el usuario puede realizar en la computadora (Bonsiepe, 1998).

Internet: Red informática de nivel mundial que utiliza la línea telefónica para transmitir la información.

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

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

Radioenlace: interconexión entre los terminales de telecomunicaciones efectuados por ondas electromagnéticas.

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

Software: Según la definición del IEEE, "software es la suma total de los programas de ordenador, procedimientos, reglas, la documentación asociada y los datos que pertenecen a un sistema de cómputo" y "un producto de software es un producto diseñado para un usuario".

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

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

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

Zona Fresnel: volumen de energía finito entre un emisor y un receptor.

CAPÍTULO III
MARCO METODOLÓGICO

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

3.1 Tipo de investigación

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

En relación con lo expresado anteriormente, se dice que la presente investigación se puede calificar como documental – descriptiva, ya que la misma, constituye un estudio sistemático de investigaciones previas ya comprobadas, y a su vez, se realiza bajo el esquema de un proyecto factible, cuyo enfoque se centra en la posibilidad de llevar teorías generales al ámbito práctico, y cuyo esfuerzo se destina a
la implantación de propuestas, que pueden materializarse y brindar soluciones a problemas que se plantean en la sociedad, lo cual en este caso es respaldo de energía eléctrica.

3.2. Nivel de la Investigación

De acuerdo al nivel investigativo, se considera una investigación descriptiva, debido a que según Arias (2006)

> "La investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere" (página 24).

Considerando lo ya expuesto, se puede clasificar que la investigación es una investigación descriptiva, debido a que se hizo apoyo de investigaciones existentes de redes VPN, pudiendo establecer un comportamiento sobre el funcionamiento y estabilidad de las señales.

3.3. Diseño de la Investigación

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

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

3.4 Población y Muestra

3.4.1. Población

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

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

La presente investigación tiene como población las redes de comunicaciones, en este caso se escogió la red privada.

3.4.2. Muestra

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

3.5 Técnicas e Instrumentos de recolección de datos

3.5.1. Técnicas de recolección de datos

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

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

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

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

Por ello, es importante destacar que los investigadores utilizarán la encuesta descriptiva debido a que se creará un registro sobre las actitudes de los empleados con respecto a sus sistemas de servicios de telecomunicaciones, y de respuesta cerrada ya que presenta dos alternativas de respuesta de forma tal que se obtenga una tendencia en el sentimiento de conformidad de los empleados con el servicio.

En esta oportunidad en consenso con el tutor asignado se redactó la siguiente serie de preguntas que ayudaron al diagnóstico de la situación actual de la empresa.

Tabla1. Encuesta realizada en la empresa de estudio

Preguntas	**Si**	**No**
1) ¿Tiene usted algún proveedor de servicios de Telecomunicaciones por fibra óptica?		
2) ¿Cuenta usted con algún proveedor de servicios de Telecomunicaciones por enlace inalámbrico?		
3) ¿Posee usted intermitencias de señal con su actual proveedor de servicios de internet?		
4) ¿Está usted conforme con la velocidad en la que navega actualmente con su proveedor de servicios de internet?		
5) ¿Se ve usted afectado por problemas de conectividad en otras áreas?		
6) ¿Conoce usted otro sistema de Telecomunicaciones distinto al que utiliza actualmente?		
7) ¿Sabe usted que es una red VPN?		
8) ¿Conoce usted para que sirve una Red VPN?		
9) ¿Estima usted que una implementación de una red de VPN beneficie la calidad de interconexión en la empresa TODO HIERRO en el sector Macomaco de San Diego?		
10) ¿Estaría usted dispuesto a adquirir y cancelar mensualmente los planes que se ofrecen para el disfrute de esta red VPN?		

De igual forma, la observación directa es un método por el cual el investigador se vale para obtener, tal y como lo dice su nombre, la información directa del análisis que se desea desarrollar. Hurtado, J. (2010) cita: “La observación directa y natural de los hechos es el punto de partida del método del empirismo. Según Bacon esta

observación debe hacerse dejando de lado los prejuicios, a los que este autor llamó ídolo". (pág. 112).

3.5.2. Instrumentos de recolección de datos

Un instrumento sirve como recurso material que se relaciona con el individuo al cual se le hace el análisis. Para Arias, F. (2012), los instrumentos: "Son los medios materiales que se emplean para recoger y almacenar la información. Ejemplo: fichas, formatos de cuestionario, guía de entrevista, lista de cotejo, escalas de actitudes u opinión, grabador, cámara fotográfica o de video, etc.". (pág. 111)

En la presente investigación, tiene como instrumento de recolección de datos la cámara fotográfica. Evidenciando la muestra finita antes propuesta, para asi destinar la misma, logrando entonces los resultados que se desean alcanzar.

Por otra parte, la lista de cotejo representa otro instrumento de recolección de datos de la presente investigación para determinar la presencia o ausencia de una serie de indicadores.

3.6 Fases de la Investigación

Fase I: "Diagnosticar la situación actual de telecomunicaciones en la empresa "TODO HIERRO SD C, A", ubicada en San Diego estado Carabobo."

- Se realizará el diagnóstico de la operatividad de la situación actual de telecomunicaciones en la empresa "TODO HIERRO SD C, A", por otro lado, se estará evaluando su situación actual de la red y se estarán realizando encuestas a los empleados de tal manera para ver qué importancia puede llegar a tener este cambio en la empresa "TODO HIERRO SD C, A".

Fase II: "Identificar los parámetros, dispositivos, entornos para el cálculo del Radioenlace y para el diseño de la Red Virtual Privada (VPN)".

- Se procederá a identificar los parámetros que conformar el diseño del cálculo del radioenlace, así como el diseño de la Red Virtual Privada (V.P.N). Se estarán evaluando que dispositivos son los mejores y necesarios para el desarrollo de este trabajo de grado. Luego se procederá a realizar los cálculos

de los parámetros necesarios para el radioenlace, se estará evaluando la zona de fresnel, la línea de vista, ganancia, diagramas de radiación entre otros de tal manera que cumplan con el diseño adecuado de un radioenlace optimo.

Fase III: "Implementar el sistema de la red privada virtual (VPN en la empresa "TODO HIERRO SD C, A", ubicada en San Diego estado Carabobo.

- Luego de haber realizado el estudio del radioenlace se estará diseñando la Red Virtual Privada (V.P.N) como paso ultimo para el desarrollo de este trabajo de grado, realizando la Comprobar la dirección IP, Comprobar posibles fugas de DNS, hacer un test de velocidad y Optimizar la conexión.

Fase IV: "Realizar un estudio técnico, social, ambiental y de costos que tiene el presente proyecto en la empresa "TODO HIERRO SD C, A", ubicada en San Diego estado Carabobo."

- Finalmente, se estudió la factibilidad del proyecto**.** En el aspecto social, se captó la receptividad de los empleados ante el proyecto planteado y las mejoras que ofrece. En el aspecto ambiental, se determinó el impacto ambiental del desarrollo de este proyecto. En el aspecto técnico, se planteó la capacidad de expansión y mejoras operativas que presento la red VPN, ante los sistemas utilizados actualmente y finalmente se realizó un estudio de costos de inversión y retorno del proyecto

CAPÍTULO IV

RESULTADOS

En lo que respecta a las técnicas de análisis y presentación de resultados, el autor Tamayo y Tamayo (2007), expresa lo siguiente: “los datos tienen su significado únicamente en función de las interpretaciones que les da el investigador. De nada servirá una abundante información si no se somete a un adecuado tratamiento analítico; pueden utilizarse técnicas lógicas y estadísticas”. (p 123).

En este capítulo se describen los resultados obtenidos durante el desarrollo de la investigación mediante la aplicación de las técnicas de recolección de datos descritas en las fases expuestas anteriormente. Finalmente, el investigador se apoya en los resultados obtenidos para plantear estrategias de solución viables, así como lo es la propuesta de la red para la mejora de las comunicaciones en el sector de estudio.

La presente investigación tuvo como propósito diseñar una propuesta que permita mejorar el acceso a la red y la comunicación entre varios departamentos de la empresa TODO HIERRO SD C,A en San Diego. Se aplicó inicialmente una revisión documental que permitió apoyar teóricamente el estudio. Posteriormente se llevó a cabo la investigación de campo para realizar el diagnostico que sustente los resultados en función a los objetivos específicos planteados. Cada uno de los resultados obtenidos se explica a continuación.

4.1 Fase I: Diagnosticar la situación actual de telecomunicaciones en la empresa “TODO HIERRO SD C, A”, ubicada en San Diego estado Carabobo.

Con la finalidad de identificar la situación problemática actual de los servicios de comunicación dentro de la empresa TODO HIERRO SD C,A en San Diego, se presenta esta sección, en la cual se utilizaron técnicas de recolección de datos, tales como la observación directa, y encuestas descriptivas de respuestas cerradas la cual fue realizada a una muestra de 23 personas a las cuales se les aclararon las dudas que surgieron en el momento.

La empresa TODO HIERRO SD C,A del estado Carabobo, en el municipio San Diego. Dicha empresa cuenta con 5 departamentos entre ellos administración, cobranza, recursos humanos, atención al cliente y ventas. Dicha empresa en promedio cuenta con una construcción de $288mts^2$.

Los principales proveedores de internet en la zona son: CANTV, Movistar y Digitel (a través de datos móviles).

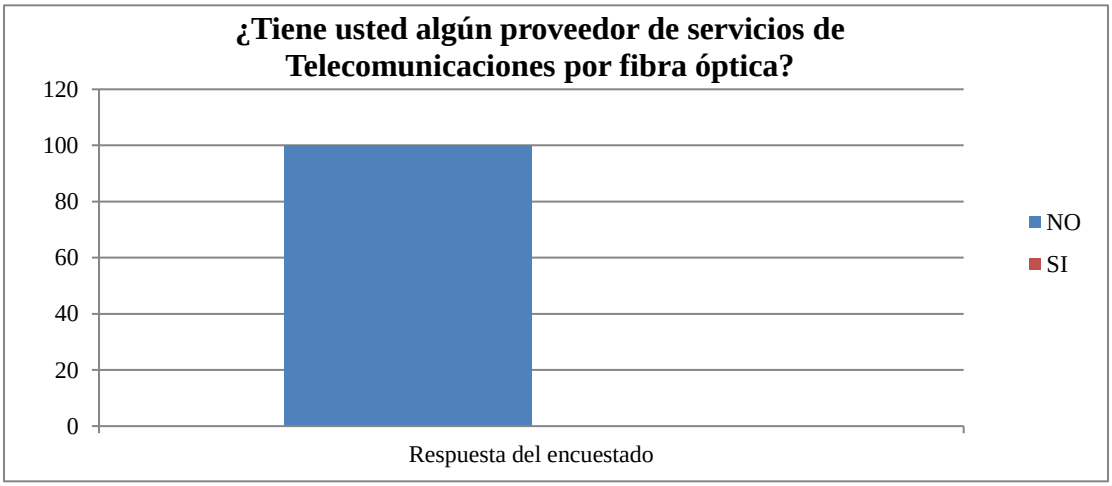
La actual red de cobre de CANTV llega desde un poste, el cual pasa a cada vivienda de manera aérea, conducido hasta un punto óptimo dentro de la empresa, donde se coloca la acometida ADSL de CANTV, la cual es una tecnología que cuenta con la capacidad de permitir la conexión y transmisión de datos a través de la red de telefonía básica.

En cuanto a las comunicaciones mediante operadoras de telefonía celular, hay diferentes tipos de conexiones, por ejemplo, 3G y 4G LTE de las empresas Movistar y Digitel. Este tipo de conexiones termina siendo muy cara porque la cantidad de datos que pueden descargar y transferir es muy baja y se consume muy rápido. Además, los precios por transferencias extras son muy elevados. Digitel y Movistar ofrecen un ancho de banda el cual varía dependiendo de las condiciones climáticas, lo cual trae como consecuencia un servicio inestable, (Ver figura 11 y 12).

Estar conectado desde un servicio de telefonía celular 3G o 4G no les da acceso a los empleados a todas las posibilidades de internet.

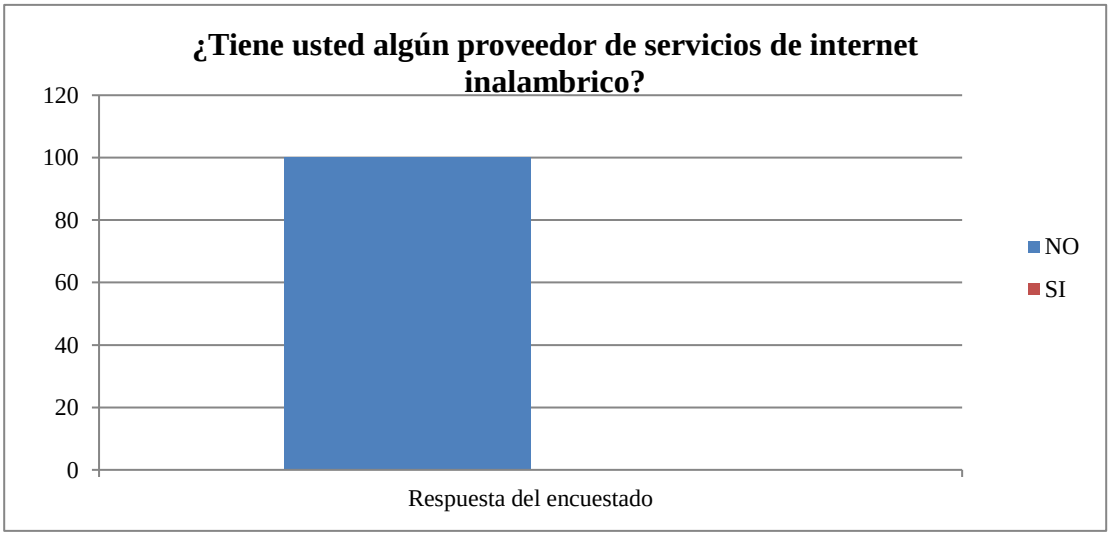
A continuación, presentamos algunas de las fallas más comunes, según los resultados arrojados por la encuesta, en las cuales los empleados de TODO HIERRO SD C,A de San Diego se han visto afectados:

Grafico 1. Representación de los Resultados de la Encuesta (Pregunta 1)



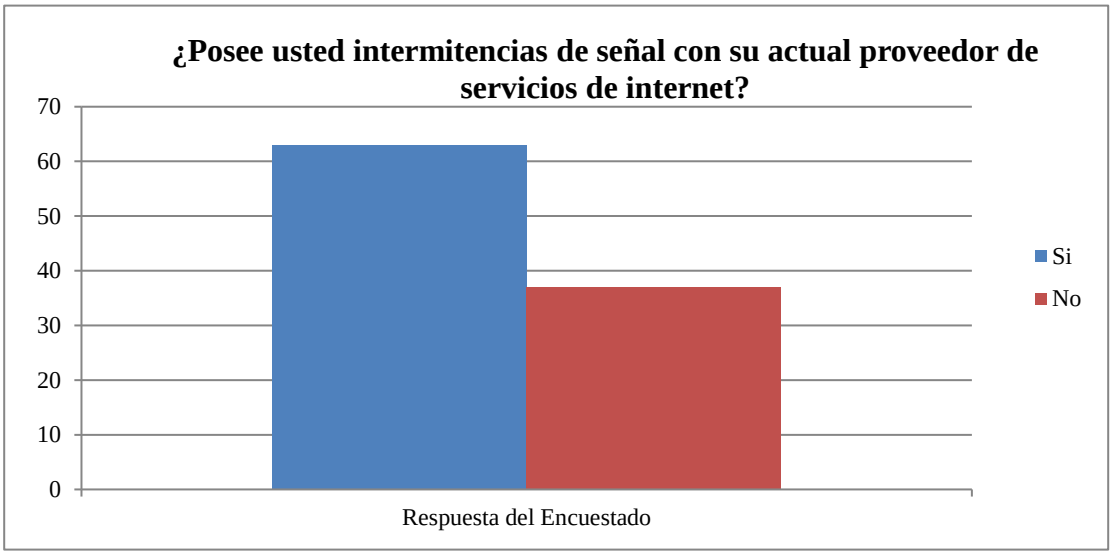
Según lo observado en el gráfico 1, el 100% de los encuestados manifiesta no poseer servicio de telecomunicaciones por fibra óptica por lo que los problemas que presenta la comunidad, son atribuibles a otro tipo de servicio de internet (ADLS de CANTV, datos móviles de Movistar y Digitel).

Gráfico2. Representación de los Resultados de la Encuesta (Pregunta 2)



Al analizar los resultados del gráfico 2, se observa que el 100% de la muestra afirma no contar con este tipo de servicio, este resultado en conjunto con el anterior delimita los proveedores de internet y a su vez las responsabilidades en cuanto a las deficiencias del servicio en la zona.

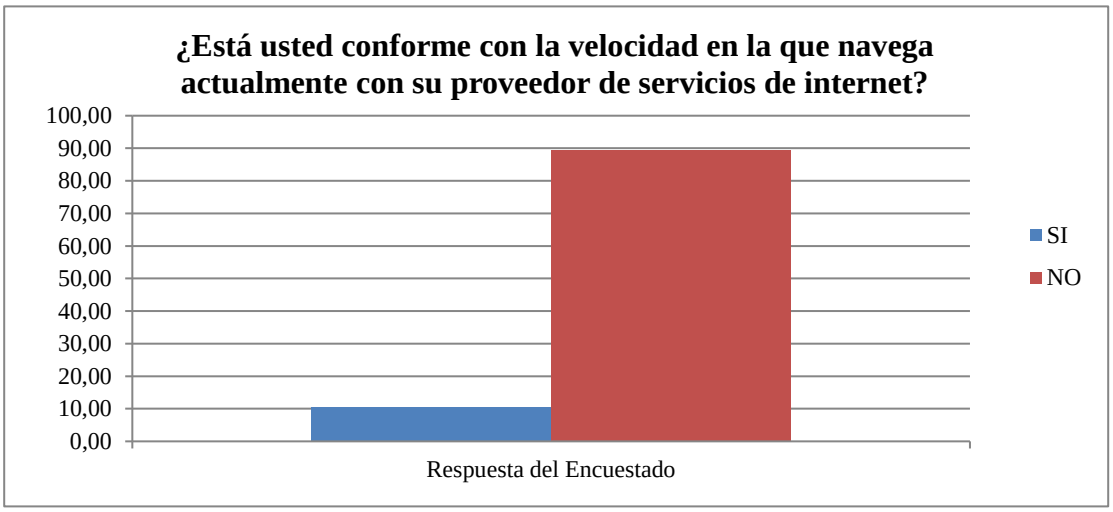
Gráfico 3. Representación de los Resultados de la Encuesta (Pregunta 3)



Partiendo de los resultados anteriores, al preguntar sobre la intermitencia de los servicios de telecomunicaciones, se observa cómo el 63% de los encuestados manifiesta sufrir de constantes caídas o colapsos en el servicio, corroborando su descontento con la eficiencia de la conectividad.

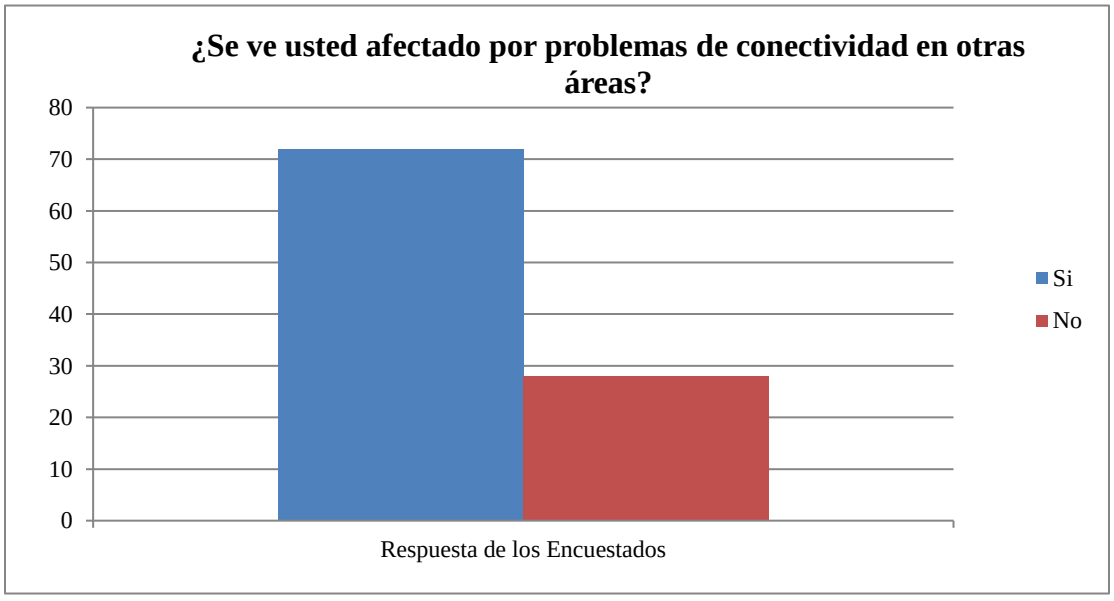
En cuanto a este particular las compañías que prestan el servicio en la empresa, presentan fallas en la prestación de sus servicios debido a que por ejemplo, las instalaciones de la empresa CANTV se en encuentran en un estado deplorable, al observarse postes doblados y con presencia de corrosión en su estructura, además de esto se visualiza ciertas irregularidades en cuanto al número de conexiones y de cables presentes en algunos de ellos, con respecto a las otras dos compañías de telecomunicaciones Movistar y Digitel que prestan los servicios de conexión 3G o 4G, no les brinda acceso a los habitantes del sector a todas las posibilidades de internet ya algunos sitios en internet no están diseñados para ser vistos en dispositivos móviles y la velocidad de datos celulares dificulta la carga de páginas que requieren cierta velocidad de descarga para funcionar eficientemente, por lo que la experiencia navegando en estos sitios se ve afectada.

Gráfico 4. Representación de los Resultados de la Encuesta (Pregunta 4)



Según lo observado en el gráfico 4, solo 10% de los consumidores están conformes con el servicio, la mayor parte de la población ha manifestado que las situaciones anteriores son las causas más comunes de su descontento.

Gráfico 5. Representación de los Resultados de la Encuesta (Pregunta 5)

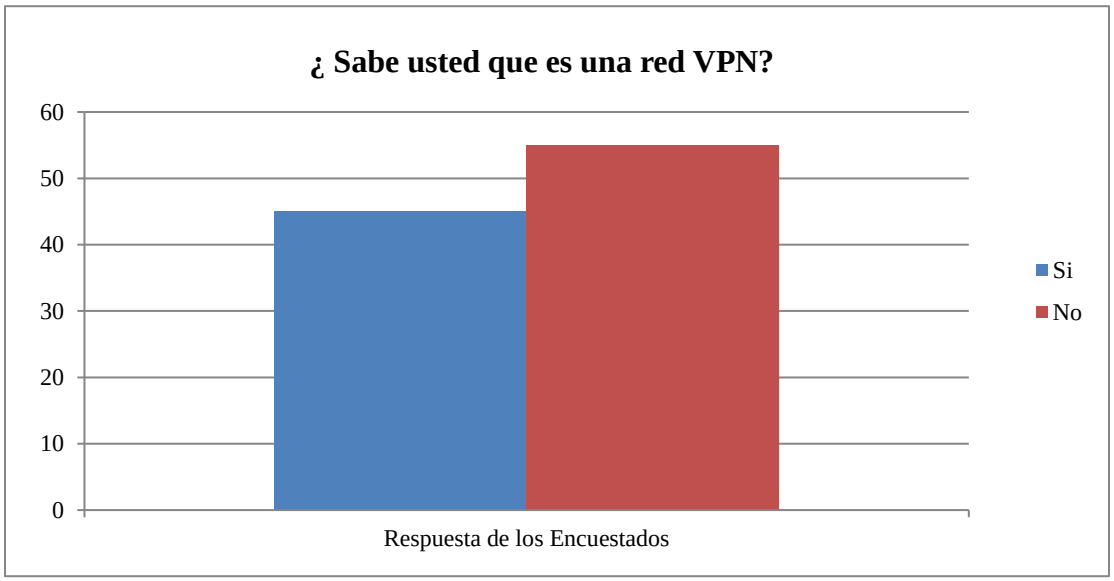


El 72% de los encuestados ha respondido de forma afirmativa a esta interrogante indicando inmediatamente que se ven afectados en el área laboral, ya que necesitan tener acceso a una computadora e internet para realizar asignaciones, investigaciones, entre otras actividades. Por otra parte, debido a las nuevas modalidades implementadas por la actual pandemia del Covid-19 hoy en día muchos trabajos se han llevado a distancia y se han vuelto cada vez más indispensables conexiones estables las cuales no están disponibles en este momento en la empresa.

Gráfico 6. Representación de los Resultados de la Encuesta (Pregunta 6)

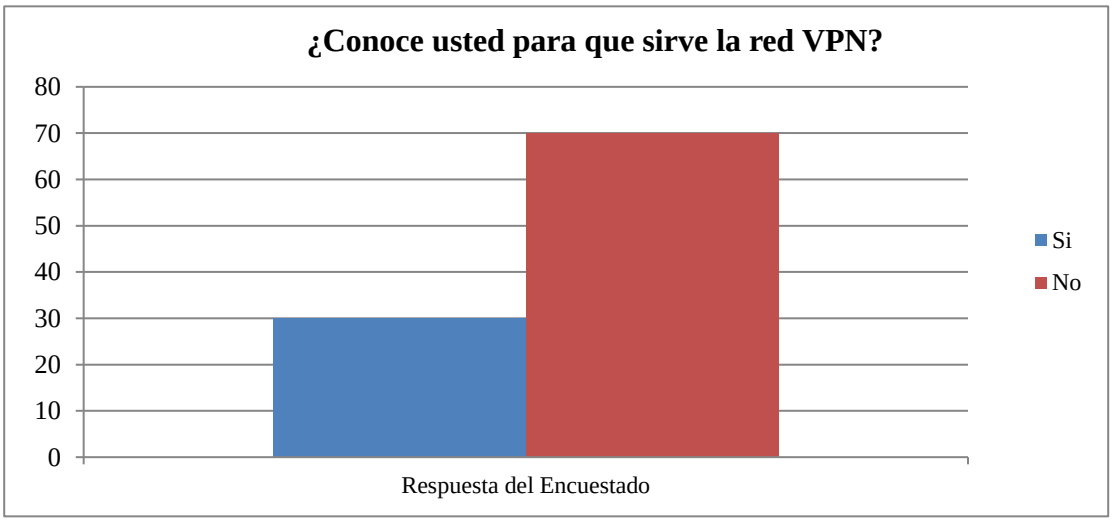
Al analizar el gráfico 6, se puede llegar a la conclusión que el 57% de los encuestados si conoce de otros tipos de servicios de telecomunicaciones distinto al que utiliza.

Gráfico 7. Representación de los Resultados de la Encuesta (Pregunta 7)



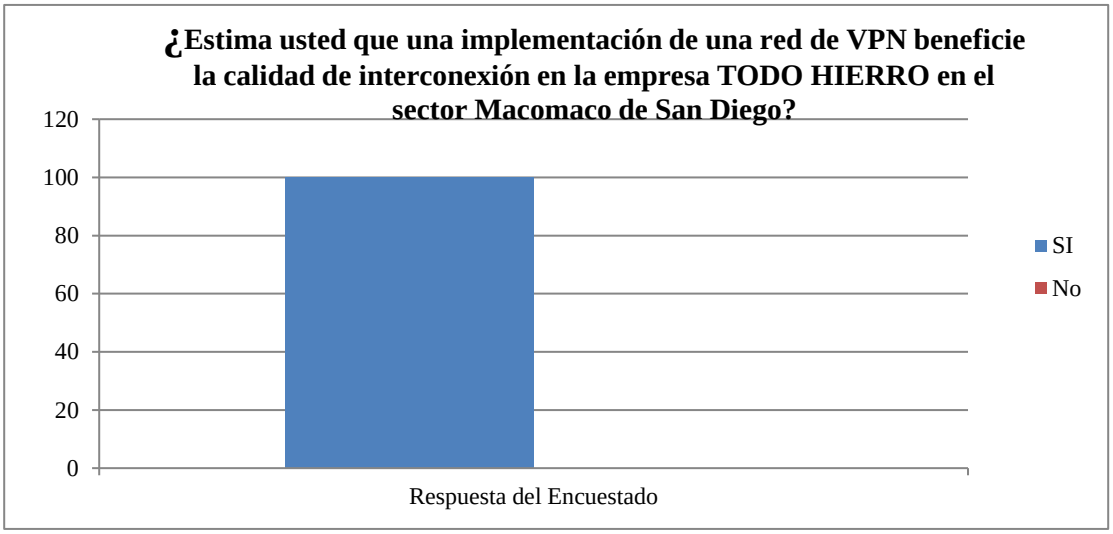
Los encuestados al responder esta pregunta afirman en un 45% conocer la red VPN.

Gráfico 8. Representación de los Resultados de la Encuesta (Pregunta 8)



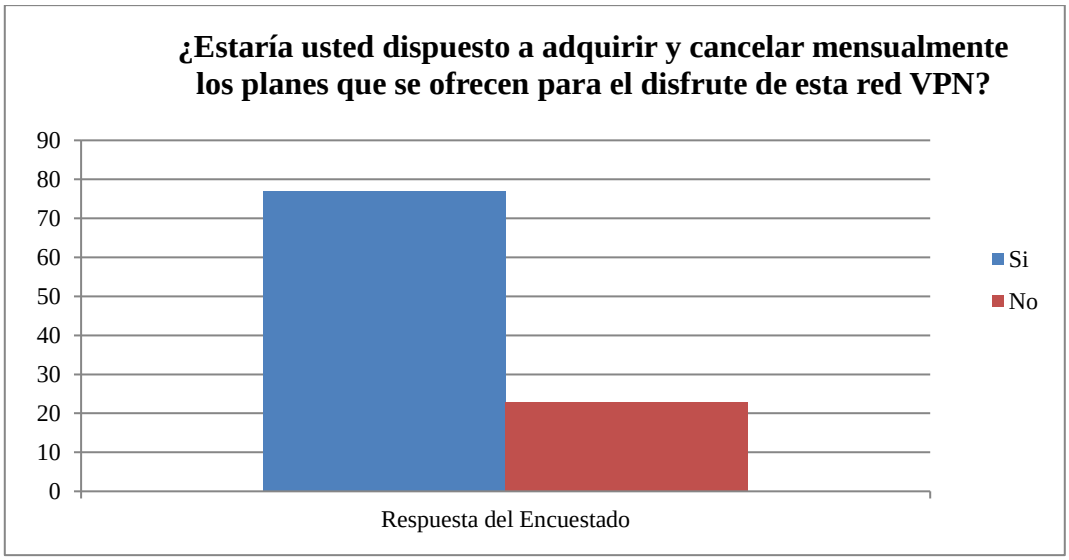
El 70% de las personas afirma no conocer este tipo de red, mientras que el 30% restante si conoce de la existencia de este tipo de redes en el área de las telecomunicaciones.

Grafico 9. Representación de los Resultados de la Encuesta (Pregunta 9)



La interpretación en general, afirma con un rotundo SI por lo que se debe implementar un nuevo servicio más actualizado como lo es la red VPN.

Grafico 10. Representación de los Resultados de la Encuesta (Pregunta 10)



El 77% de los encuestados si están de acuerdo en cancelar el servicio tal y como es ofrecido dentro de esta propuesta.

Al analizar la información obtenida a través de los recursos utilizados se puede demostrar la ausencia de calidad de servicios, en los cuales se encuentra el mal estado de las instalaciones e infraestructura de la empresa CANTV, las caídas y alta latencia del ABA en la zona, mientras que si se habla de las empresas de telefonía celular se concluye que no son suficientes para satisfacer las necesidades de conectividad de los empleados debido a la poca cobertura y velocidad de los mismos, otro punto observado en este diagnóstico y que vale la pena mencionar es que de la muestra de la encuesta, nadie cuenta con un servicio diferente a la tecnología ADLS de CANTV o de telefonía celular (Movistar, Digitel).

4.1.1 Lista de cotejo

Para dar un diagnóstico más amplio acerca del estado actual en el que se encuentran las instalaciones en la que se desarrollara el proyecto de la red VPN para la empresa TODO HIERRO SD C,A en San Diego, se ha recolectado mediante una lista de cotejo la siguiente información.

Tabla 2. Lista de cotejo utilizada en el diagnóstico

Fuente: Silva, Jesus (2022)

Aspectos a evaluar	Cantidad	Observación
Computadoras	20	Se contabilizaron 10 computadoras
Computadoras en uso	12	Computadoras actas para el uso de los empleados
Computadoras en mal estado	8	Computadoras con problemas que no están actas para el uso.
Repetidores de señal inalámbrica	0	No se encontraron repetidores en el recorrido de las instalaciones de la empresa
Distancia entre departamentos	8mts	Todos cuentan con una distancia de 8 mts aproximadamente

4.2 Fase II. Identificar los parámetros, dispositivos, entornos para el cálculo del Radioenlace y para el diseño de la Red Virtual Privada (VPN).

En esta fase se seleccionaron los componentes, materiales y equipos de acuerdo a la información recolectada en la Fase I, se llevó a cabo una comparación de las características, ventajas y desventajas que estos ofrecen, y se determinó la que ofreció mejores soluciones para utilizar en la empresa TODO HIERRO SD C,A en San Diego, además de los cálculos necesarios para su implementación.

Por otra parte, en las siguientes secciones se hace mención a los diferentes equipos que se sugieren utilizar para la implementación del diseño propuesto. Cabe indicar que para la red de acceso VPN se utilizarán equipos disponibles en la empresa asi como equipos en el mercado, como son: splitters ópticos, cajas de dispersión y conectores, antenas.

4.2.1 Fibra Óptica

La fibra seleccionada es de tipo monomodo ADSS (single mode o SM), específicamente de 12 hilos, que debe cumplir con el estándar G.652, pues este permite trabajar en un rango de 1310 nm a 1625 nm. Dentro de las subcategorías de la norma G.652, se sugiere la de tipo D, en este tipo de fibra se reduce el pico de dispersión por iones de hidroxilo (OH-), aumentando de esta manera las velocidades de transmisión (ITU-T, 2001). En ese mismo sentido, se determinó usar este tipo de fibra y con capacidad de 12 hilos primeramente porque la fibra monomodo puede llegar a cubrir distancias de 40 km o más, sin dañar la señal, siendo ideal para aplicaciones de largo alcance lo que puede proporcionar, así como la cantidad elegida de hilos una escalabilidad en la red.

Por otra parte, la utilización de usar fibra ADSS frente a una plana con guía es la cantidad de herrajes que necesita para así poder conservar el tendido logrando ser más seguro y confiable frente agentes externos como (Fuertes vientos o lluvias), además de su comodidad de instalación en la elaboración de las mangas o cajas nap y su implementación sobre postes.

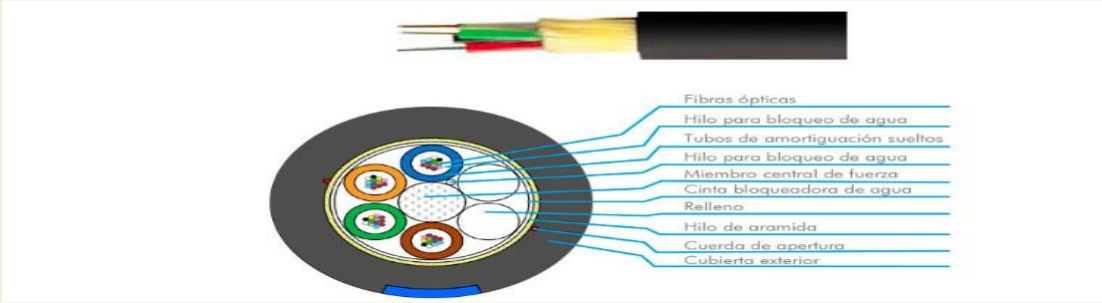


Figura 11. Cable ADSS - 12 Fibras Monomodo OS2 (9/125)
Fuente: https://www.fibramarket.com/p/cable-adss-autosoportado-12-fibras-monomodo-os2-9-125-span-120m/

4.2.2 Herraje helicoidal o preformado

Es un herraje consistente en alambre con forma helicoidal que proporciona la fuerza necesaria para tenar el cable de fibra óptica por su propio apriete. Se determinó usar este herraje en particular porque es ideal para ser utilizado en sujeción de cables exteriores dieléctricos tipo ADSS y el interior del remate cuenta con abrasivo para garantizar la retención del cable.

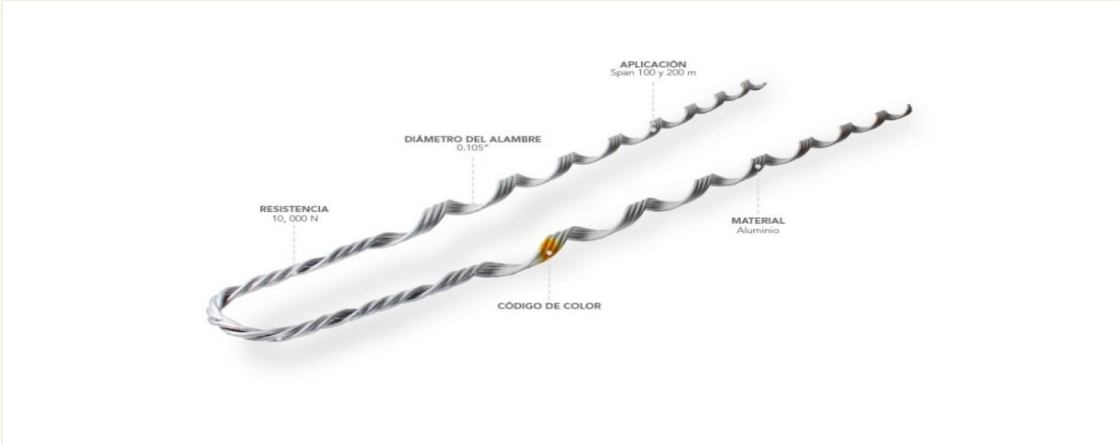


Figura 12. Preformado de Aluminio para Cable ADSS 12.0-12.8 mm

Fuente:https://optronics.com.mx/conectividad/views/producto/h4XB6S4SLA52j9GzXf45fMmWjnHt5UA0TfchnbE4TKrXxSe4ufl0cDKgEQQEQQ#1

4.2.3 Trompeta de suspensión

Este tipo de herraje es utilizado para soportar cables tipo ADSS de 5 a 20mm. De diámetro. El herraje es fabricado en acero galvanizado y en neopreno resistente a rayos UV. Su diseño hace más sencilla la instalación al poste, ya sea por medio del fleje o atornillado a la punta de un brazo de extensión. Este herraje frente a los demás tipos como (herraje tipo B, FAS o mini FAS) posee una ventaja en cuanto al sujetar el cable debido a lo suave pero firme que lo sujeta, evitando la fatiga y el daño del cable.

Figura 13. Herraje Tipo J
Fuente:https://optronics.com.mx/conectividad/views/producto/h4XB6S4SLA52icgxXF4TRDQMHPLUS1C9JPLUSFC16ehLQ1PfurMEQQ#4

4.2.4 Trompoplatina

Es un herraje de sujeción a poste que garantiza total inmovilidad, gracias a su doble ranura para inserción de flejes de acero que proporciona una mejor sujeción. Se usará un herraje tipo A y la ventaja que presenta este tipo de herraje es su capacidad de minimizar costos en cuanto a la utilización de fleje y hebillas ya que mientras un herraje tipo D puede consumir aproximadamente 1m de fleje para abrazar al poste y 2 hebillas

este con tan solo 0.5m aproximadamente de fleje y 1 hebilla cumple con la misma función.

Figura 14. Herraje tipo A ADSS
Fuente: https://www.grupoosi.com/producto/herraje-tipo-a-

4.2.5 Fleje

Los flejes funcionan como una abrazadera que se fija sobre un poste y son una parte esencial de toda solución aérea en planta externa, pues sirven como base para la instalación de otros elementos, como herrajes y remates, indispensables en el tendido de cualquier tipo de cable de fibra óptica. Se determinó usar fleje de ¾ por su mayor capacidad de resistencia a la abrasión del poste.

Figura 15. Fleje ¾.
Fuente: https://www.inflegra.com/productosinflegra/p/34-x-022

4.2.6 Hebilla

Son el complemento esencial para la instalación, utilizado como abrazadera para fijar los herrajes a los postes en conjunto con los flejes. Además, es importante aclarar que se usara hebilla de ¾ por su compatibilidad con el fleje de ¾.

Figura 16. Hebilla de acero inoxidable ¾
Fuente:https://optronics.com.mx/conectividad/views/producto/h4XB6S4SLA52jUpCXqCh0aF7bPLUSBVdEycE5e87vi53T7y0EQQ#4

4.2.7 Requerimientos básicos de una VPN:

1. **Identificación de usuario:**

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien accedió, que información y cuando.

2. **Administración de direcciones:**

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

3. **Codificación de datos:**

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

4. **Administración de claves:**

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

5. **Soporte a protocolos múltiples:**

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet (IP), el intercambio de paquete de internet (IPX) entre otros.

4.2.8 Equipo para el radio enlace punto a punto

Entre los equipos para hacer radioenlace en el mercado se sugiere utilizar la antena DAP-3711 que es de la marca D-Link con un servicio completo y tamaño pequeño, que además proporciona tecnología TDMA. Su determinación radica por lo comercial y económica que es a comparación con las antenas Ubiquiti y por permitir la escalabilidad de la red.

Por otra parte, esta antena posee una ventaja frente a la antena Ubiquiti basada en que la antena es compatible con diferentes ONT como por ejemplo ONT de las marcas (ZTE, TP-LINK, ADC, entre otros) mientras que el Ubiquiti solo es compatible con sí mismo.

Figura 17. Antena D-Link DAP-3711
Fuente:https://www.google.com/url?sa=i&url=https%3A%2F%2Feu.dlink.com%2Fes%2Fes%2Fproducts%2Fdap-3711-punto-acceso-enlaces-bridge-larga-distancia

4.2.9 Equipo ONT, Optical Network Terminal

Entre los tipos de ONT sugeridos se determinó usar el de la marca ZXHN F660 que es un terminal de red óptica GPON diseñado para el escenario FTTH. Admite la función L3 para ayudar al suscriptor a construir una red doméstica inteligente. Brinda a los suscriptores servicios ricos, coloridos, individualizados, convenientes y cómodos que incluyen voz, video (IPTV) y acceso a Internet de alta velocidad. Además, por el simple hecho de ser un modelo presentado por la empresa ZTE su compatibilidad con el OLT es garantizada y es por esto en primer lugar se determinó implementarlo dentro del diseño.

Igualmente, este modelo actúa como ONT router, es decir, puede cumplir con la función de ONT y ofrecer wi-fi simultáneamente dándole así un valor agregado para los usuarios

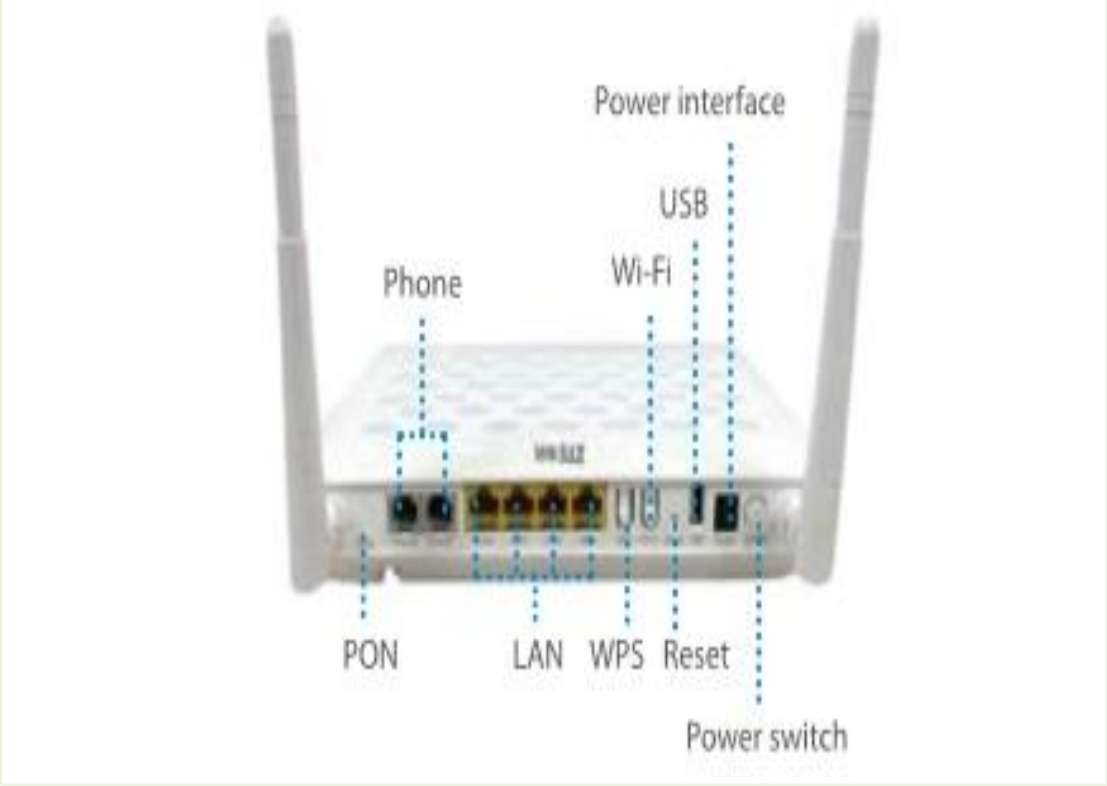


Figura 18. ONT ZTE-ZXHN F660
Fuente: https://www.batna24.com/en/p/zte-zxhn-f660-ont-rmmpk\

4.2.10 Convertidor multimedia

El MC111CS es un conversor de medios diseñado para convertir el cable de fibra 100BASE-FX a cable de cobre 100Base-TX o viceversa. El MC111CS incorpora la tecnología WDM mediante la cual únicamente es necesario un solo cable de fibra para transmitir y recibir datos, lo que permite ahorrar la mitad del coste en cables. El MC111CS está diseñado siguiendo los estándares IEEE 802.3u 10/100Base-TX y 100Base-FX y utiliza cable de fibra monomodo provisto de un conector tipo SC. El MC111CS soporta la especificación de láser de onda larga (LX) a la máxima velocidad de transmisión. Funciona a 1550 nm en el envío de datos y a 1310 nm en la recepción. De este modo, el dispositivo que funciona en conjunto con el MC111CS debe trabajar a 1310 nm en el envío de datos y 1550 nm en la recepción. El conversor de medios MC112CS de TP-LINK es sólo uno de los dispositivos que pueden funcionar en conjunto con el MC111CS.

Otras de las ventajas de este módulo es la posibilidad de utilizarlo de forma independiente (sin necesidad de carcasa) o con un chasis de 19" de TP-LINK. Además, detecta automáticamente tanto el modo MDI/MDI-X como el modo Duplex en el puerto TX e incluye leds de estado en su panel frontal. El MC111CS amplía el rango de distancia de la transmisión óptica hasta 15 kilómetros utilizando fibra monomodo.

Figura 19. Convertidor MC111CS
Fuente: https://www.pngwing.com/es/free-png-mrmwd

4.2.11 Cantidad de Materiales, equipos y componentes a utilizar

Tabla 3. Lista de materiales para el radioenlace.

Materiales	Cantidad	Observación
Antena D-Link DAP-3711	2 und	Enlace punto a punto
Fibra óptica monomodo	10 mts	Incluidas reservas.
Trompoplatinas	2 und	Una por cada antena
Computadoras	1 und	Para realizar la programación de la red
Hebillas	2 und	Una hebilla por poste con trompoplatina.

Tabla 4. Lista de equipos de la red de acceso VPN

Equipos	Cantidad	Observación
Antena D-Link	2	Punto-Punto
Convertidor MC111CS	1	Convertir fibra óptica a cable de cobre
computadoras	12	Red VPN
ONU ZTE	1	GPON

4.2.12 Calculo del radioenlace

4.2.12.1 FSL Ecuación 1. Silva, Jesus (2022)

Fsl(dB)=(20log(Dist.Km))+(20log(Frec.Mhz))-148

Fsl(dB)=(20log(1))+(20log(5800))-148

Fsl(dB)=-72.73

4.2.12.2 Enlace Ecuación 2. Silva, Jesus (2022)

Enlace=**(**PotenciaTX)+(-PerdidaTX)+(ganancia)+(-Fsl)+(gananciaRX)+(-PerdidaRX)

Enlace(dB)=**(**27)+(-1)+(15)+(-72)+(15)+(-1)

Enlace(dB)=-17

4.2.12.3 Margen Ecuación 3. Silva, Jesus (2022)

Margen(dB)=Enlace-(-Sensibilidad)

Margen(dB)=-17-(-93)

Margen(dB)=76

4.2.12.4 Pire Ecuación 4. Silva, Jesus (2022)

Pire(dB)=(PotenciaTX)+(-PerdidaTX)+(GananciaTX)

Pire(dB)=(27)+(-1)+(15)

Pire(dB)=41

4.2.12.5 Zona de Fresnel Ecuación 5. Silva, Jesus (2022)

R(mts)=17,32√((d1*d2)/(d*f))

R(mts)=17,32√((0,5*0,5)/(1,1*5,8))

R(mts)=3,77

4.2.13 Cálculos de los componentes de la red de acceso VPN

Tomando en cuenta que la empresa TODO HIERRO SD C,A solo tiene hasta el momento 5 departamentos, solo se necesitara un servidor para crear la red VPN donde todos los dispositivos se conectaran a la red realizada a través del radio enlace. Usando para esto un ONT también conocido como Router/Wifi. Teniendo un límite de 100 dispositivos según el fabricante.

4.2.14 Diagrama de Radiación

En la empresa TODO HIERRO SD C,A se utilizó una antena isotrópica para realizar una conexión a internet a través de un radioenlace, donde según el fabricante esta debe cumplir ciertos parámetros de funcionamiento, a continuación se muestra su diagrama de radiación:

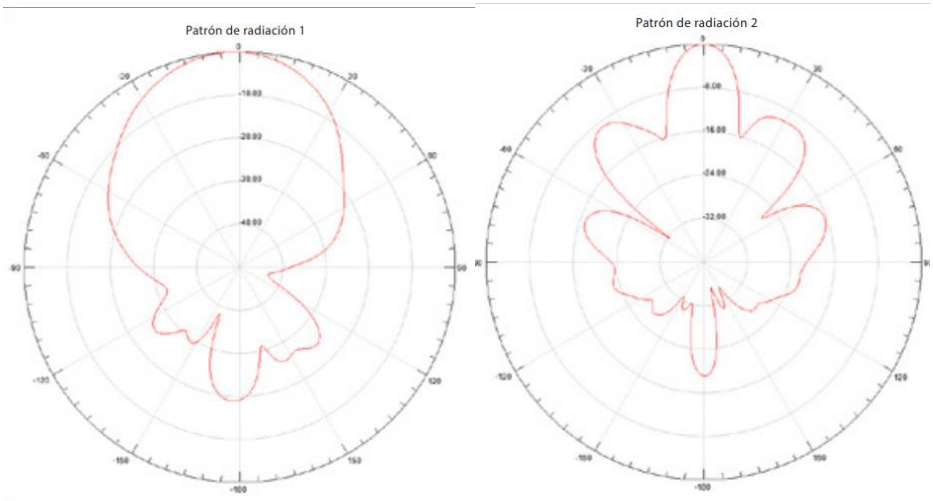


Figura20: Diagrama de radiación antena DAP 3711

Fuente: https://eu.dlink.com/es/es//media/business_products/dap/dap3711/datasheet/dap3711-dap3712-datasheet-en-es.pdf

4.3 Fase III: "Implementar el sistema de la red privada virtual VPN en la empresa "TODO HIERRO SD C, A", ubicada en San Diego estado Carabobo.

Cuando hablamos de VPN o redes privadas virtuales, automáticamente se nos viene a la cabeza una de sus funciones más extendidas en estos tiempos, que es la de conectarse a Internet como si estuvieras navegando desde otro país. Pues bien, crear una red VPN doméstica no te va a servir para esto. O por lo menos no en todos los casos, ya que, si creas una VPN en Venezuela, al usarla para navegar las páginas verán que eres de Venezuela.

Una VPN doméstica es algo más centrado en la privacidad cuando navegas. Se encargará de crear un túnel para tus datos, ya que todas las peticiones que hagas, como búsquedas, correos electrónicos y demás, se cifrarán y pasarán por el servidor VPN para enviarse a Internet.

Con esto, lo que vas a conseguir es enmascarar la dirección IP de tu ordenador, evitando que aplicaciones y empresas puedan rastrearte cuando navegas por Internet.

Las páginas no sabrán la dirección IP de tu router cuando te conectas, sino que, en vez de eso, solo sabrán la de tu VPN.

Además de esto, un servidor VPN también te permite crear una red local sin necesidad que tus dispositivos estén físicamente conectados entre sí, aunque en este caso sí vas a necesitar que estén conectados a la misma red. En cualquier caso, puede ser útil para ahorrarse algunos cables.

4.3.1 Montaje de la red VPN

Lo primero que tienes que hacer es entrar en la Configuración de Windows. Una vez dentro, entra en la sección de Red e Internet, que es donde se encuentran las configuraciones relacionadas con Internet. Aquí dentro, en Windows 10 tienes que ir a la sección de Estado y pulsar en el botón de Cambiar opciones del adaptador. En Windows 11 es diferente se entra en el apartado Configuración de red avanzada, y pulsas en la opción Más opciones del adaptador de red.

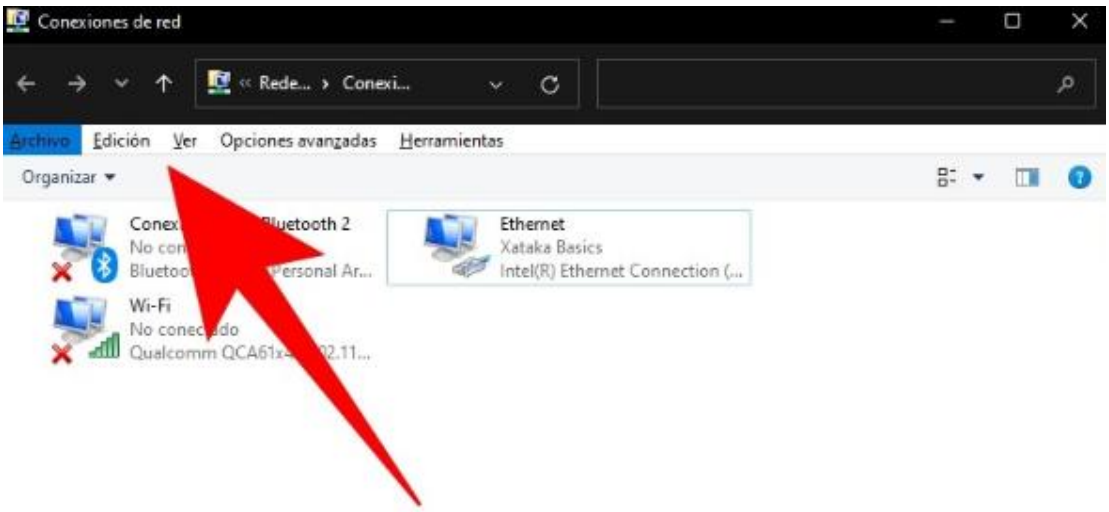


Figura 21: Cambio de adaptador

Fuente: Silva, Jesus (2022)

Se abrirá una ventana del antiguo Panel de control de Windows 7 y versiones anteriores, que sigue estando escondido dentro de Windows 10 y Windows 11. En esta

ventana te aparecerán las conexiones que tengas, por ejemplo, Ethernet si estás conectado a través de cable al router. En esta ventana, pulsa F10 para mostrar un menú oculto con más opciones que te aparecerá en una barra en la parte de arriba.

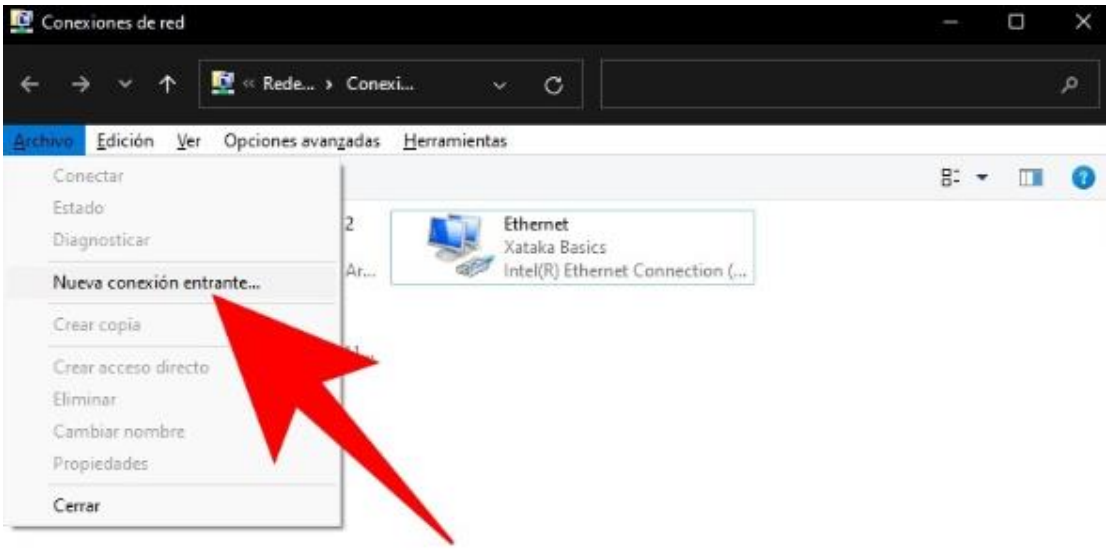


Figura 22: Nueva conexión

Fuente: Silva, Jesus (2022)

En este menú oculto, se tiene que hacer clic en Archivo, y se abrirá un menú en el que debes pulsar sobre la opción de Nueva conexión entrante. Con esto, le estarás diciendo a Windows que quieres crear una nueva conexión, que en este caso va a ser la VPN.

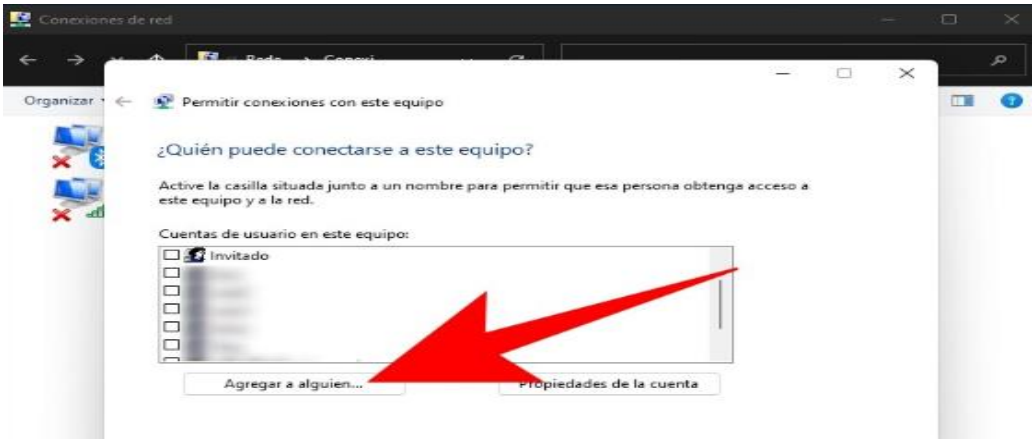


Figura 23: Agregar Conexión

Fuente: Silva, Jesus (2022)

Se abrirá una pantalla en la que van a poder ver cuentas de usuario que pueden agregar al ordenador. Estarán tanto las que tengas creada para inicio de sesión de Windows como las de tu grupo familiar de Microsoft si lo quisieras, y se tiene que elegir qué cuentas quieren que puedan acceder a la VPN. Lo mejor es crear uno nuevo pulsando en el botón de Agregar a alguien, y que así ese usuario y contraseña los utilices después.

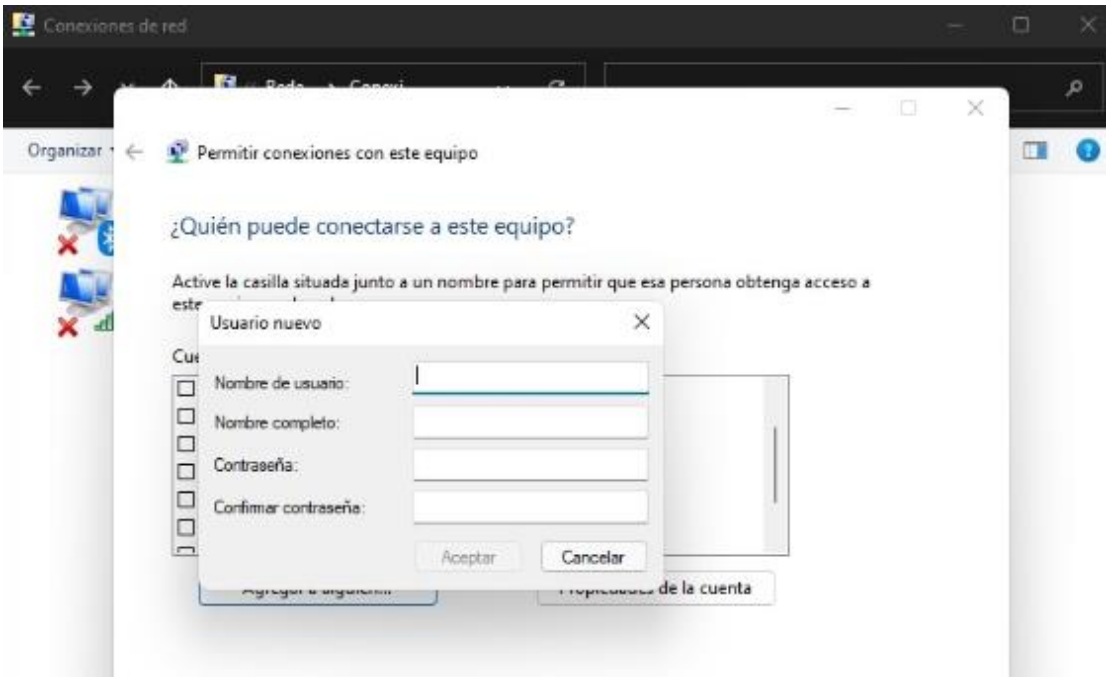


Figura 24: Nuevo usuario

Fuente: Silva, Jesus (2022)

Se abrirá una ventana en la que tienes que escribir un nombre de usuario y la contraseña. Aquí pueden poner el nombre que quieran, pero recuerda que lo tendrán que utilizar después para acceder a la VPN, serán el usuario y contraseña de esta red.

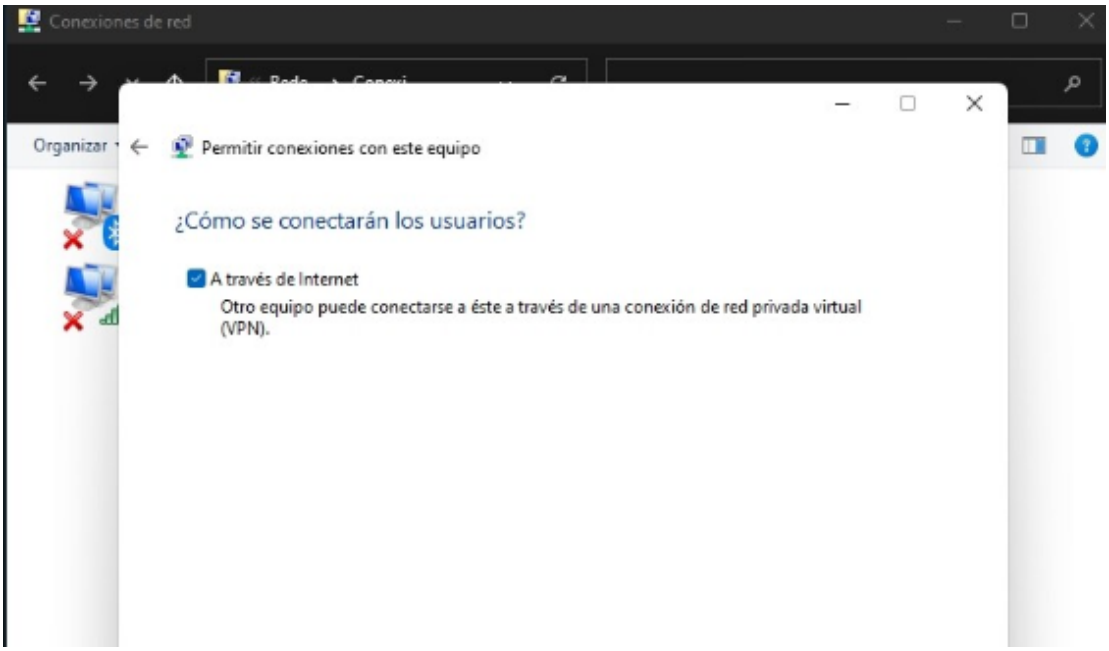


Figura 25: Tipo de conexión

Fuente: Silva, Jesus (2022)

Saldrá una pantalla en la que se te va a preguntar cómo se va a conectar este usuario a tu red, y en ella tienen que dejar seleccionada la opción de A través de Internet. Así, el nombre de usuario que has creado será para conectarse a la red formando una VPN, ya que te conectarás con este usuario a través de Internet a tu red.

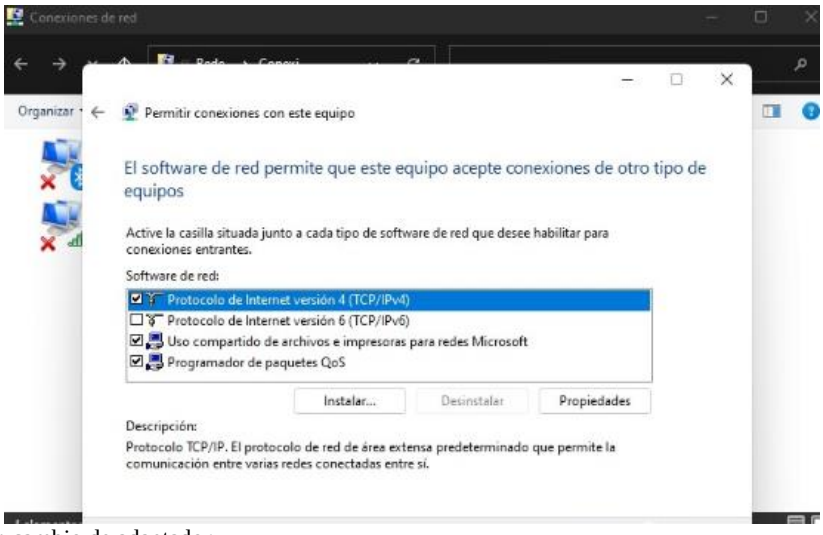


Figura 26: cambio de adaptador

Fuente: Silva, Jesus (2022)

Ahora, entrarás a otra pantalla en la que puedes configurar los protocolos y software de red que quieres utilizar. Aquí, tienes que seleccionar la opción Protocolo de Internet versión 4 y pulsar en Propiedades. Aquí, lo que tienes que saber es que por defecto este usuario va a utilizar tu IP, y que vamos a cambiarlo para asignarle un rango de IPs diferentes, y que así sea una VPN.

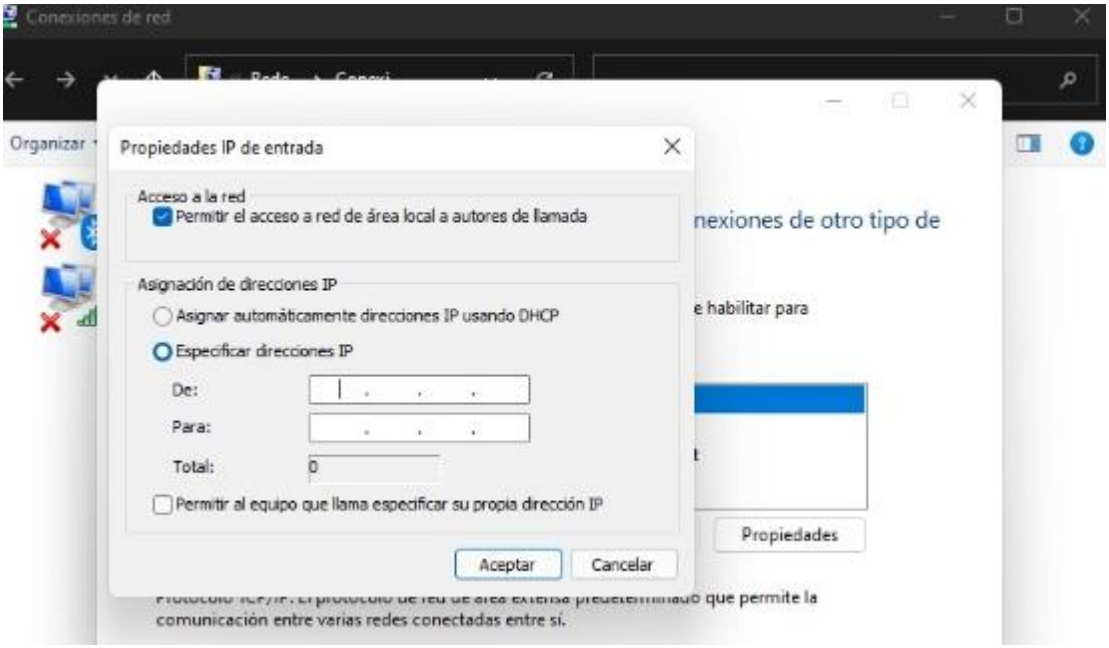


Figura 27: Cambio de IPs

Fuente: Silva, Jesus (2022)

Aquí, vamos a llegar a una parte un poco compleja. Llegarás a una ventana en la que tienes que seleccionar la opción de Esperar direcciones IP. Aquí, vas a tener que especificar un rango de IPs que estén dentro de tu dirección IP. Esto suena muy complejo, pero te vamos a decir cómo verlo.

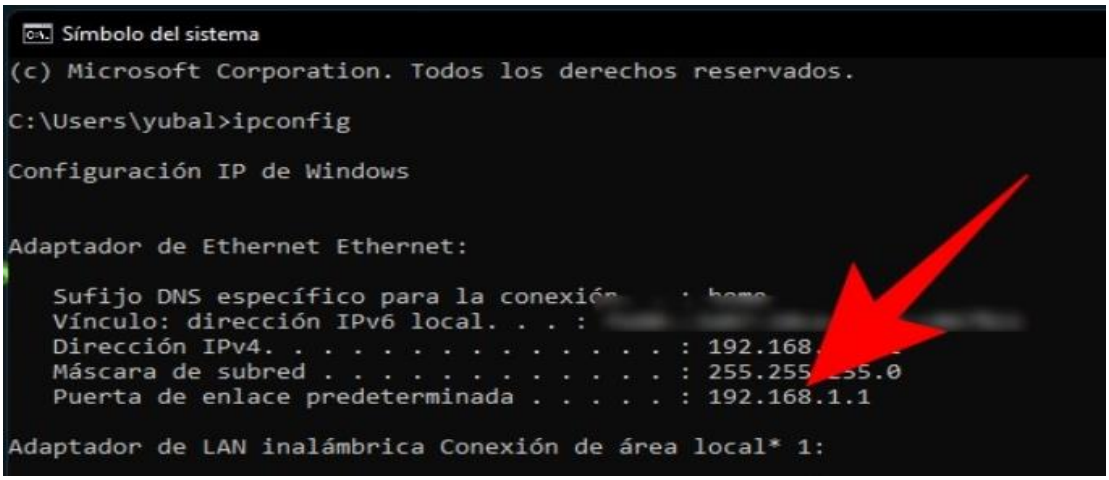


Figura 28: Como ver la dirección IPs

Fuente: Silva, Jesus (2022)

Para hacer esto, primero tienes que saber tu dirección IP. Para ello, abre la aplicación de Símbolo de sistema de Windows y escribe el comando ipconfig. Te aparecerá un texto con varias direcciones IP, y lo que tienes que hacer es quedarte con la IP de Puerta de enlace predeterminada, ya que es la dirección IP de tu router.

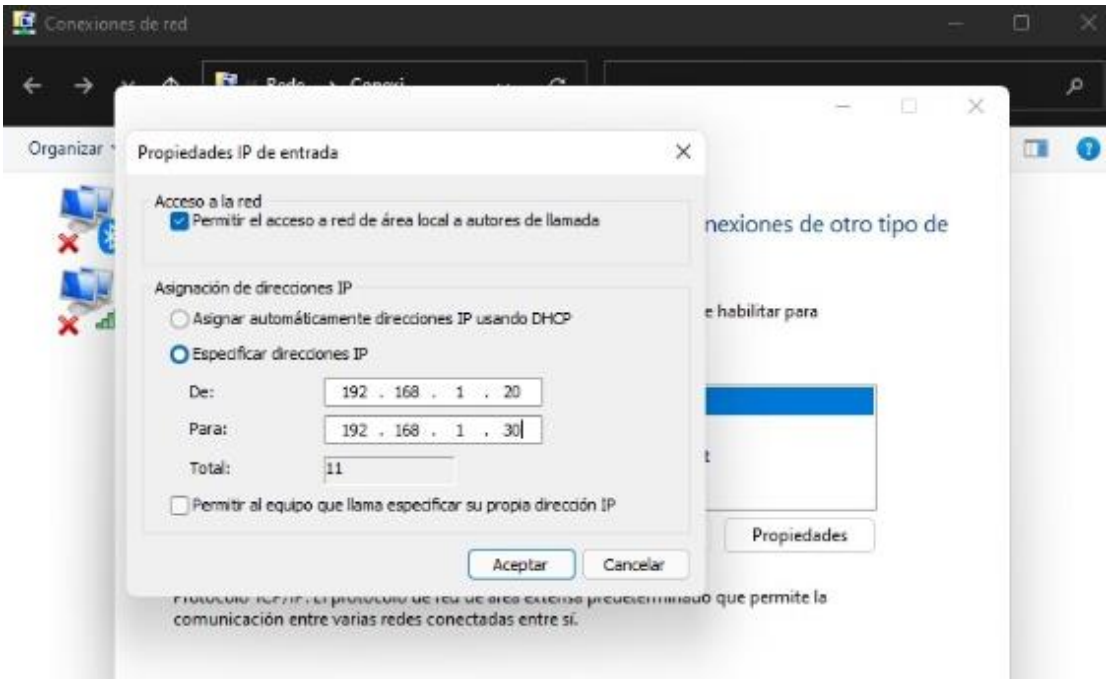


Figura 29: Selección de rango de dispositivos

Fuente: Silva, Jesus (2022)

Volviendo a la pantalla anterior, para escribir un rango de números dentro de tu IP, las primeras tres series de números deben ser las mismas que las de tu router. Por ejemplo, si la IP de mi router es 192.168.1.1, entonces las IPs del rango que tienes que escribir deben empezar con 192.168.1, y luego los últimos números pues poner los que quieras dependiendo del número de IPs que quieras darle a la VPN. Por ejemplo, puedes poner que sea de 192.168.1.20 a 192.168.1.120 para darle 100 direcciones IP.

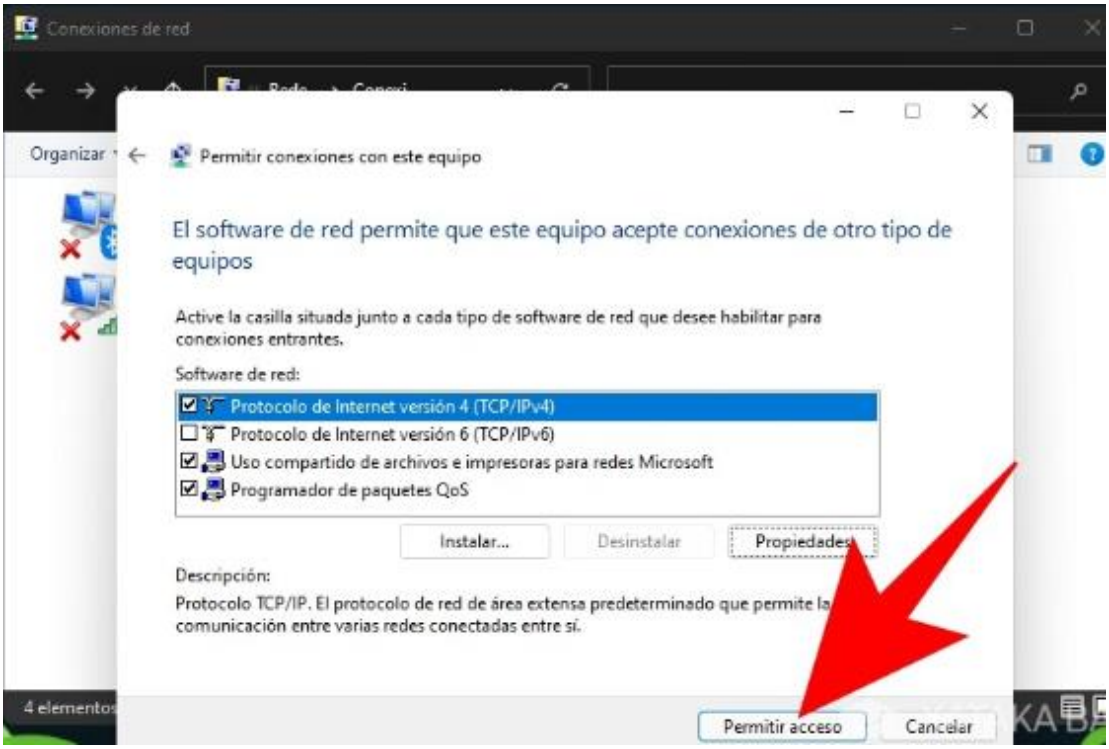


Figura 30: Permitir los cambios en la Red

Fuente: Silva, Jesus (2022)

Una vez escrito el rango de IPs, pulsa en Aceptar, y volverás a la pantalla de software de red. Aquí ya habrás terminado de configurarlo todo, por lo que solo te queda pulsar en el botón de Permitir acceso, y Windows procederá a crear tu servidor VPN.

4.3.2 Abrir puertos en el router y da permisos en el firewall

Ahora tienes que dar dos pasos más. Primero tienes que abrir el puerto para VPNs de tu router. Para esto, tienes que entrar en la configuración de tu

router utilizando la IP de Puerta de enlace predeterminada, que suele ser 192.168.1.1 o 192.168.0.1 y escribiéndola en el navegador. La contraseña viene en tu router, aunque es recomendable cambiarla. Dentro, tienes que abrir el puerto 1723 en tu router. Para esto, tienes que escribir la dirección de tu router en el navegador, y acceder a su configuración. El puerto en Windows siempre es el 1723.

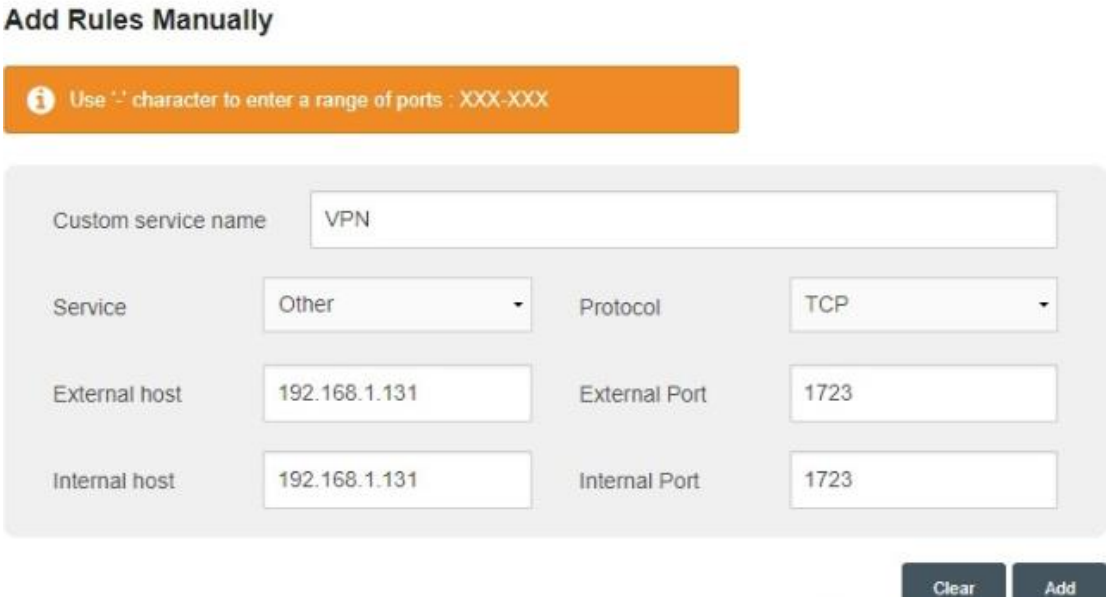


Figura 31: Configuración del router

Fuente: Silva, Jesus (2022)

La pantalla de configuración será diferente en cada router. Aquí, tendrás que añadir una regla escribiendo la IP de tu ordenador y el puerto 1723 para que lo abra. La IP de tu ordenador no es la misma que la del router. Volviendo al Símbolo de sistema con el comando ipconfig, la de tu ordenador será donde pone Dirección IPv4. Aquí, tendrás que buscar por tu cuenta en la configuración de tu router un término relacionado con los puertos del router o ports.

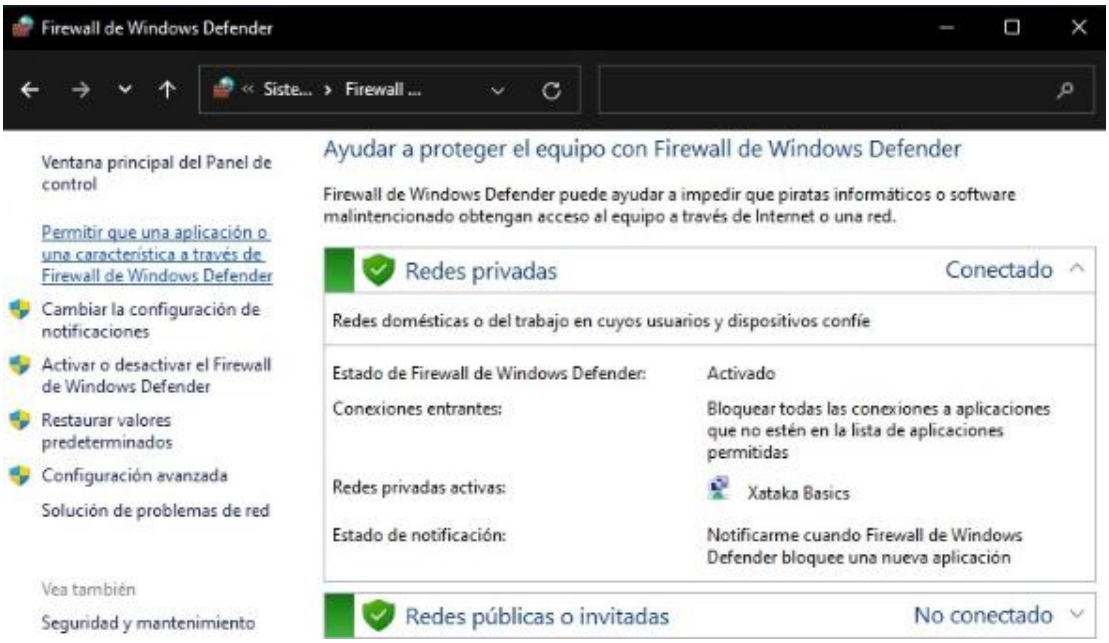


Figura 32: Configurar el Firewall

Fuente: Silva, Jesus (2022)

Ahora, tienes que abrir la aplicación Panel de control de Windows otra vez. Estando en su índice principal, tienes que pulsar en Sistema y seguridad y luego en Firewall de Windows Defender. Cuando entrés en esta ventana de configuración, que es la de la captura, pulsa en Permitir que una aplicación o una característica a través de Firewall de Windows Defender, que es una opción que tienes en la columna de la izquierda.

Figura 33: Cambiar la configuración del Firewall

Fuente: Silva, Jesus (2022)

Entrarás en la ventana de Permitir a las aplicaciones comunicarse a través de Firewall de Windows Defender. Aquí, tienes que pulsar en el botón de Cambiar la configuración y darle permisos de administrador para poder hacer camios en la lista inferior.

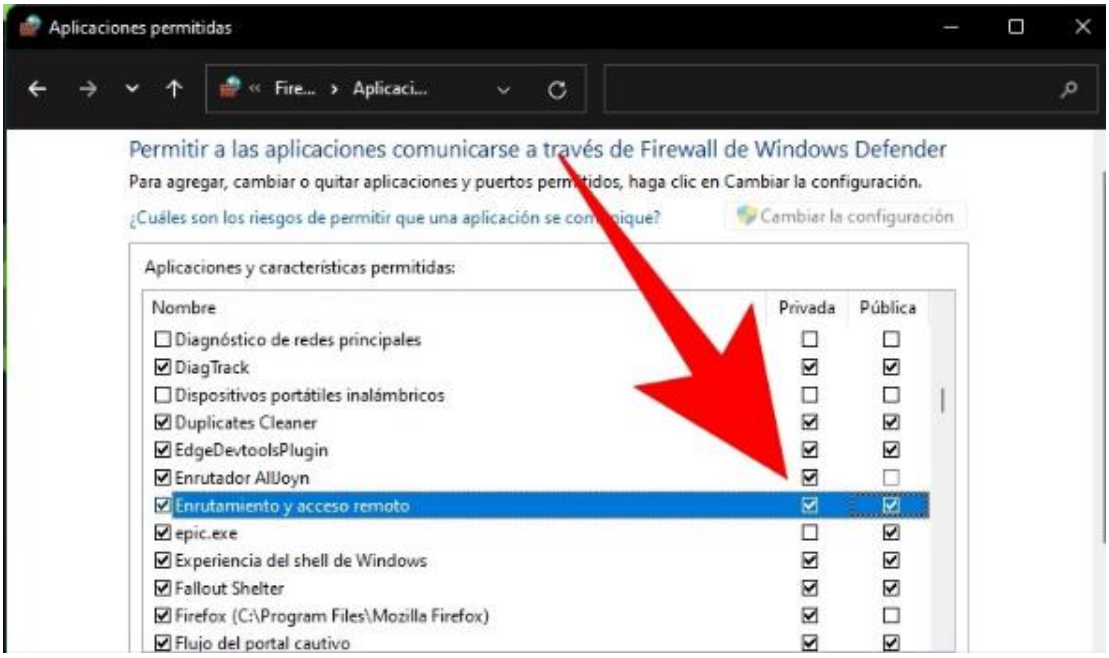


Figura 34: Cambio de enrutamiento y acceso remoto

Fuente: Silva, Jesus (2022)

Aquí, tienes que activar las casillas Privada y Pública de la opción de Enrutamiento y acceso remoto, que aparece en la lista. Las opciones van en orden alfabético, o sea que tendrás que ir bajando hasta encontrarlo, y activar sus dos casillas. Una vez lo hagas, pulsa en Aceptar para que se apliquen los cambios.

4.3.3 Conectar la VPN

Y una vez hayas hecho esto, ya está, tienes tu red VPN creada. Ahora ya solo te queda conectarte a ella desde tus diferentes dispositivos, como desde Android o desde iOS. En este caso, para conectarte tienes que volver a utilizar el comando ipconfig en el símbolo de sistema, y utilizar la IP que aparece en Dirección IPv4 como el nombre de servidor de la VPN.

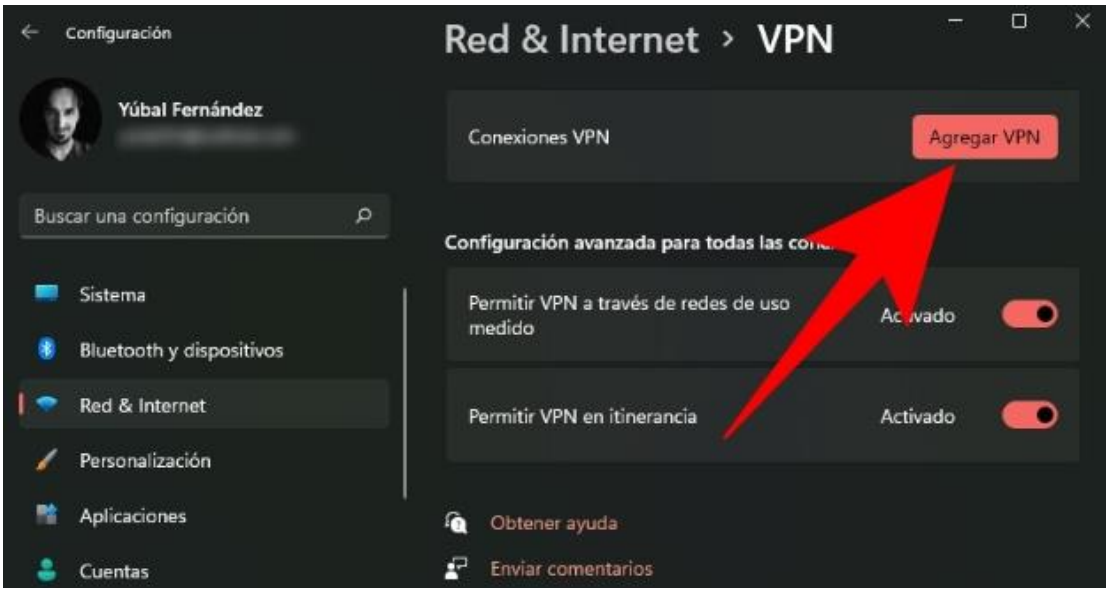


Figura 35: Agregar VPN a la PC

Fuente: Silva, Jesus (2022)

Para conectarte a la VPN desde Windows, tienes que ir a la configuración y entrar en Red e Internet. Allí ve a la sección VPN. Tendrás la lista de redes VPN que hayas configurado, que en mi caso está vacía por no tener ninguna. Aquí, pulsa en la opción de Agregar VPN para proceder a añadir la que has configurado.

Figura 36: Configurar la VPN a la PC

Fuente: Silva, Jesus (2022)

Se abrirá una ventana de configuración. En ella, en Proveedor de VPN tienes que elegir la opción Windows. Luego, debes ponerle el nombre que quieras a la configuración para que se identifique en Windows, y en Nombre de servidor o dirección escribir la IP que te aparecía como Dirección IPv4 dos pasos atrás. Al final, también tendrás que escribir un nombre y contraseña, que serán del usuario al que le hayas dado acceso.

Figura 37: VPN activa en la red

Fuente: Silva, Jesus (2022)

Y ya está. Con estas credenciales, ya te podrás conectar desde un ordenador que esté en la misma red que estés utilizando. Puedes dejar conectada la VPN para utilizarla todas las veces que quieras.

4.4 Fase IV: Realizar un estudio ambiental, social, y de costos que tiene el presente proyecto en la empresa "TODO HIERRO SD C, A", ubicada en San Diego estado Carabobo.

4.4.1 Factibilidad Ambiental

En distintas circunstancias el ambiente se ve afectado por las nuevas tecnologías e innovaciones que día por día se hacen presentes en nuestra vida. Por este motivo las

empresas de telecomunicaciones buscan reemplazar los antiguos cables cobre con tecnología de fibra óptica para entrar en un enfoque más ecológico.

El medio de comunicación por fibra óptica reduce mucha más energía a diferencia del medio de comunicación a través de cobre. Según datos proporcionados por la Agencia de Protección Ambiental, los cables de cobre consumen 3,5 W por cada 100 metros, contra apenas 1 W de consumo estimado con el uso de cables de fibra óptica para conducir haces de luz en una mayor distancia recorrida de 300 metros y si pensamos en el medio ambiente al usar menos energía significa menor generación de calor lo que le da un valor agregado a la fibra óptica como medio de comunicación eficiente para ser implementado en lugar del cobre.

En ese mismo sentido, ahorrar energía es un elemento fundamental para el aprovechamiento de los recursos energéticos y de la misma forma estamos evitando la emisión de gases que contaminan nuestra atmósfera, por lo que la fibra óptica solo libera 7 gramos de CO2 por cada Gigabit de datos transmitidos. Además, la fibra óptica radica en el alta resistencia de sus materiales porque los hilos de vidrio tienen el espesor de un cabello en el interior del cable, duran muchos años, mientras que los de cobre sufren oxidación y recalentamiento por los cambios de temperatura que sufre este metal, dentro o fuera de la tierra.

Posteriormente, la transmisión de luz por la fibra óptica no genera ruidos de ningún tipo. Las actividades periódicas de mantención, reposición o retiro de elementos del tendido no suponen la generación de ruidos que pudieran generar efectos dañinos en la población o el medio ambiente

Finalmente, el presente trabajo de investigación no causa ningún tipo de deterioro capaz de ser perjudicial para el medio ambiente, de manera que el nivel de contaminación que el propio produce es considerado insignificante, en virtud de lo cual el presente trabajo de investigación vence en lo absoluto con las condiciones o factores necesarios que certifiquen su factibilidad ambiental.

4.4.2 Factibilidad Social

Esta investigación evidencio en los resultados y por la implementación de las herramientas de recolección de datos, apoyado en encuestas cerradas de respuestas de SI y NO, se corrobora en una pluralidad el control de información sobre las Redes VPN y que a diferencia con la red de cobre, esta red VPN es ejemplar por sus valiosas utilidades, donde los consumidores en esta ocasión buscan velocidad, un servicio que vista sus expectativas y sirva de avance para la sociedad en general promocionando otras actividades sociales y beneficiosas. La obtención de las redes inalambricas en su conjunto hasta el hogar va en crecimiento, considerando a NETUNO o INTER en primer lugar y otras empresas para su posible implementación.

4.4.3 Factores para medir la viabilidad del proyecto

- **Emergencia:** Venezuela es otro país. Es radicalmente diferente lo que ocurrió en el año 2020 a lo que paso en 2021, la manera de adaptarse y reaccionar ante la pandemia para poder vivir mejor y realizar todas nuestras actividades laborales desde casa se ha vuelto algo muy común, en ese sentido el uso del internet se ha convertido en un elemento tan fundamental como el agua, aire, comida e incluso tener un techo donde vivir. De allí nace la importancia de trabajar en proyectos que busquen brindar soluciones a las necesidades de las personas en materia de sistemas de telecomunicaciones.
- **Número de beneficiarios directos:** El proyecto de la red de acceso VPN con tecnología de radioenlace para la empresa TODO HIERRO SD C,A en San Diego del presente trabajo de investigación se verían beneficiadas un total de 23 personas, sin embargo la red está diseñada para ser escalable a largo plazo teniendo una capacidad de 1024 personas a lo cual presentarían mejoras representativas en su calidad de vida por contar con un servicio de Internet fiable.

- **Soluciones:** El presente trabajo de investigación posee las soluciones eficaces y oportunas para dar garantía de ser exitoso y supone la solución a un objetivo concreto o que, al menos, cubre la necesidad para la que será ejecutada.
- **Sostenibilidad:** Los aportes de los recursos, la financiación, su gestión y mantenimiento, entre otras cuestiones quedara bajo la decisión y responsabilidad del estado o de las empresas proveedoras de servicios de internet (ISP) si estas lo consideran pertinente.

4.4.4 Estudio de Costos de la instalación de la red VPN

A continuación, se muestra un desglose de los costos asociados a los materiales y equipos requeridos en la instalación de cada una de las etapas de la red, considerando que los insumos y la mano de obra corresponden a una fracción el total del costo de los materiales y equipos.

Cuadro.5 de Costos de materiales para el radioenlace

Material	Cantidad	Unidad	P. unt ($)	Precio ($)
Antena D-Link DAP-3711	2	und	100	200
Fibra óptica monomodo	10	mts	1.5	15
Trompoplatinas	2	und	4.19	8.38
Computadora	1	und	400	400
Hebillas	2	und	0.32	0.64
Total, costos del Troncal Principal				**624.02**

Cuadro 6. De Costos de Equipos de la Red de Acceso

Equipos	Cantidad	Unidad	P. unt ($)	Precio ($)
Antena D-Link DAP-3711	2	und	100	100
Convertidor MC111CS	1	und	26	26
Computadora	12	und	500	6000
ONU ZTE	1	und	70	70
Total costos de Equipos para la Red de Acceso				**6196**

Cuadro 7. Costo Total de la Instalación

Descripción	Precio ($)
Materiales para el radioenlace	624.02
Equipos de la Red de Acceso	6196
Total de la Instalación	**6820.02**

CONCLUSIÓN

En primer lugar, se pudo demostrar la baja calidad con respecto a las instalaciones e infraestructura que presenta actualmente la empresa CANTV en la empresa TODO HIERRO SD C,A en San Diego, donde se encuentran en mal estado, sufren frecuentes caídas y alta intermitencia, por otro lado, Movistar y Digitel se concluye que no son suficientes para satisfacer las necesidades de conectividad de los empleados debido a la poca cobertura y velocidad de los mismos, finalmente al observar las respuestas de las encuestas cerradas de SI y NO se concluye que existe la necesidad de proponer una red de acceso FTTH con tecnología GPON para dicha empresa.

En segundo lugar, se logró evidenciar la cantidad requerida de materiales, equipos y componentes siendo esta una cantidad exacta e inigualable para este proyecto, se concluye que las características de cada uno de ellos anteriormente mencionadas son las ideales para el diseño de la red de acceso VPN para la empresa en cuestión.

En tercer lugar, se implementó la red de acceso VPN donde se concluye que los pasos para realizarla son claros y concisos, además las características de las antenas, la distribución de los equipos, las conexiones internas en cada una de los departamentos y la potencia de recepción en la ONT es viable, segura y eficiente.

Finalmente, el presente trabajo de investigación supera en su totalidad las condiciones o factores inexcusables que certifiquen su factibilidad ambiental, social y de costos para la empresa TODO HIERRO SD C, A ubicada en el sector Macomaco municipio San Diego, Valencia, Edo. Carabobo.

RECOMENDACIONES

- La ubicación de las antenas debe ubicarse a una distancia no mayor a la recomendada para que funcionen de una forma óptima.
- Se recomienda tomar los procedimientos realizados en el diseño de la red de acceso VPN para la empresa TODO HIERRO SD C, A en el diseño de otras redes.
- La extensión de fibra requerida para el proyecto no debe exceder los 20km, pasado esta distancia se presentan pérdidas de información por las distintas atenuaciones presentes en la fibra óptica.
- Se recomienda no alterar el número de antenas al recomendado para tener que evitar alterar el diseño de la red de radioenlace.
- Se recomienda contar con anticipación con los permisos pertinentes por parte de los entes que regulan las normas de Telecomunicaciones en el país para así darle más provecho en tiempo al proyecto.
- El personal técnico destacado para la instalación y administración de la red VPN deberá cumplir mínimamente con un perfil especifico que es de contar con conocimiento sólidos en el manejo y operación de este estándar lo asegura que a futuros se presenten inconvenientes en su rendimiento y normal funcionamiento.
- Para los futuros cálculos de presupuesto de pérdidas ópticas se deben de considerar los valores más altos posibles en referencia a la atenuación en la distancia de los enlaces, fusiones, conectorizaciones, y splitter a emplearse para contar con una conectividad fiable.
- Se recomienda tener los cuidados propios de la manipulación y operación de fibra óptica, por ejemplo, limpieza de conectores, cortes de fibra compatible y empalmes. Para no introducir más perdidas de las deseadas

REFERENCIAS

Bibliográficas

Aguilera, P (2002). **Estructura básica del PLC**. Recuperado en: http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf

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

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

González, G. (2019) .**Diseño de un Sistema de Radioenlace para comunicaciones en el ámbito Industrial.** Recuperado en: https://cicsa-maxon.com.mx/media/Diseño-Sistema-Rdioenlace-Cicsa-1.pdf

Hurtado, J. (2010). **El proyecto de investigación.** Caracas: Editorial Quirón. http://dspace.espoch.edu.ec/bitstream/123456789/1335/1/108T0005.pdf

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

Peña, V. (2019) .**Diseño e implementación de un Red Privada Virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada.** Recuperado en: http://repositorio.uncp.edu.pe/handle/20.500.12894/6628

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

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

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

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

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

Villares, C (2017). **Sistema de comunicación para la transmisión de la información entre la matriz y la sucursal de la distribuidora de material de construcción "FREVI" en la Ciudad de Ambato.** Recuperado en: Http://repositorio.espe.edu.ec/xmlui/handle/21000/12402?locale-attribute=de

Mendillo, V (2011). **Requisitos para las Redes VPN.** Recuperado en: http://repositorio.uncp.edu.pe/handle/20.500.12894/6628