UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN

"Implementación de una Red VPN "Virtual Private Network para la mejora de la seguridad dentro de la red local inalámbrica de la Empresa de distribución de material de Construcción y Ferretero "Distribuidora Gómez, mediante el uso de protocolos Ipsec y Tcp/Ip."

Proyecto de titulación previo a la obtención del título de Ingeniero en Informática y Sistemas Computacionales

AUTORES

Andaluz Guerrero Alex Agustín

Guanoluisa Guanoluisa Jessica Alexandra

TUTOR ACADÉMICO

Ing. Rubio Peñaherrera Jorge Bladimir

Latacunga – Ecuador

2022

DECLARACIÓN DE AUTORÍA

Nosotros, **Andaluz Guerrero Alex Agustin con C.I.: 1724441645 y Guanoluisa Guanoluisa Jessica Alexandra con C.I.: 0504415431**, declaramos ser los autores del proyecto de investigación: **"IMPLEMENTACIÓN DE UNA RED VPN "VIRTUAL PRIVATE NETWORK" PARA LA MEJORA DE LA SEGURIDAD DENTRO DE LA RED LOCAL INALÁMBRICA DE LA EMPRESA DE DISTRIBUCIÓN DE MATERIAL DE CONSTRUCCIÓN Y FERRETERO "DISTRIBUIDORA GÓMEZ", MEDIANTE EL USO DE PROTOCOLOS IPSEC Y TCP/IP."**, siendo el **Ing. Rubio Peñaherrera Jorge Bladimir con C.I: 0502222292,** tutor del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certificamos que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de nuestra exclusiva responsabilidad.

Atentamente,

Andaluz Guerrero Alex Agustin
C.I: 1724441645

Guanoluisa Guanoluisa Jessica Alexandra
C.I: 0504415431

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título:

"IMPLEMENTACIÓN DE UNA RED VPN "VIRTUAL PRIVATE NETWORK" PARA LA MEJORA DE LA SEGURIDAD DENTRO DE LA RED LOCAL INALÁMBRICA DE LA EMPRESA DE DISTRIBUCIÓN DE MATERIAL DE CONSTRUCCIÓN Y FERRETERO "DISTRIBUIDORA GÓMEZ", MEDIANTE EL USO DE PROTOCOLOS IPSEC Y TCP/IP", de los Estudiantes : Andaluz Guerrero Alex Agustin y Guanoluisa Guanoluisa Jessica Alexandra de la carrera **INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES**, considero que dicho proyecto de Investigación cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la **FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS** de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, 29 de agosto 2022

Atentamente.

Ing. Rubio Peñaherrera Jorge Bladimir

Tutor de Titulación/Proyecto de investigación

C.I: 050222229-2

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la FACULTAD de Ciencias de la Ingeniería y Aplicadas; por cuanto, el o los postulantes: Andaluz Guerrero Alex Agustín, Guanoluisa Guanoluisa Jessica Alexandra, con el título de Proyecto de titulación: "IMPLEMENTACIÓN DE UNA RED VPN "VIRTUAL PRIVATE NETWORK" PARA LA MEJORA DE LA SEGURIDAD DENTRO DE LA RED LOCAL INALÁMBRICA DE LA EMPRESA DE DISTRIBUCIÓN DE MATERIAL DE CONSTRUCCIÓN Y FERRETERO "DISTRIBUIDORA GÓMEZ", MEDIANTE EL USO DE PROTOCOLOS IPSEC Y TCP/IP", han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, 30 de agosto de 2022

Para constancia firman:

Ing. Manuel William Villa Quishpe
Lector1 "Presidente"
CC: 180338695-0

Ing. Segundo Humberto Corrales Beltran
Lector 2
CC: 050240928-7

Ing. Víctor Hugo Medina Matute
Lector 3
C.C: 050137395-5

EMPRESA DE DISTRIBUCIÓN DE MATERIAL DE CONST
FERRETERO "DISTRIBUIDORA GÓMEZ"

AVAL DE IMPLEMENTACIÓN

Mediante el presente pongo a consideración que los señores estudiantes:

ANDALUZ GUERRERO ALEX AGUSTÍN Y GUANOLUISA GUANOLUISA JESSICA ALEXANDRA, realizaron su tesis a beneficio de la **EMPRESA DE DISTRIBUCIÓN DE MATERIAL DE CONSTRUCCIÓN Y FERRETERO "DISTRIBUIDORA GÓMEZ"** con el tema: **"IMPLEMENTACIÓN DE UNA RED VPN "VIRTUAL PRIVATE NETWORK" PARA LA MEJORA DE LA SEGURIDAD DENTRO DE LAED LOCAL INALÁMBRICA DE LA EMPRESA DE DISTRIBUCIÓN DE MATERIAL DE CONSTRUCCIÓN Y FERRETERO "DISTRIBUIDORA GÓMEZ", MEDIANTE EL USO DE PROTOCOLOS IPSEC Y TCP/IP"**, trabajo que fue presentado y probado de manera satisfactoria.

Quito, Agosto 2022

GOMEZ MAZABANDA

Gerente General

Ing. Jackeline Gomez

DISTRIBUIDORA GÓMEZ
RUC: 1712045093001

Parroquia "Alangasí" Av. Italo s5-87 y Rio Corrientes Esq. Distribuidora de Material de Construcción y Ferretero "Distribuidora Gómez".

AGRADECIMIENTO

Agradezco a mis padres y hermanos por ser los pilares fundamentales durante todo mi proceso académico ya que gracias a su apoyo y motivación eh logrado completar mis metas y objetivos propuestos al igual que han sido mi alegría en momentos difíciles gracias a ellos eh podido obtener un muy valioso regalo para mi vida el cual se ve reflejado tanto en mi vida personal como profesional.

Al Ing. Jorge Rubio, por ser un excelente docente el cual mediante su conocimiento a logrado plantar una semilla de inquietud por el estudio de las redes informáticas y al igual por el apoyo y guía brindada durante el proceso de desarrollo del proyecto de investigación el cual se ve reflejado en el trabajo académico de titulación elaborado.

De igual manera agradezco a mi querida Universidad Técnica de Cotopaxi y a sus docentes por brindarme la oportunidad de potenciar mis capacidades académicas, ya que gracias a ellos y a su amplio conocimiento eh podido conocer y comprender conceptos informáticos que servirán para futuro profesional, conocimientos que me abrirán camino en un amplio campo laboral.

Finalmente me agradezco a mi por tener la fuerza para sobrellevar las vueltas de la vida y levantarme con fuerza sabiendo que todo es posible, motivándome y creyendo en que este gran esfuerzo al final tendrá una gran recompensa que alegrará mi vida, la de mis padres y familia.

ANDALUZ GUERRERO ALEX AGUSTIN

DEDICATORIA

Quiero dedicar el logro de esta meta, a mis padres Victoria Guerrero y Julio Andaluz quienes con su esfuerzo y perseverancia han guiado mi vida formando mi carácter y creando en mí una persona responsable y decidida, siendo ellos mi principal ejemplo y fortaleza a seguir enseñándome a ser una persona trabajadora y valiente para afrontar cualquier situación por más compleja que esta sea.

A mis hermanos y familia quienes con su apoyo me han ayudado durante mi proceso académico les dedico este título, el cual me permite culminar una importante etapa de mi formación académica.

Dedicó también este triunfo a una amiga muy importante que creyó en mí y vio mis momentos difíciles tanto académicos como personales, siendo ella una fuente de motivación para superarme y creer en mis habilidades informáticas a ti mi amiga 17.

ANDALUZ GUERRERO ALEX AGUSTIN

AGRADECIMIENTO

Primero Agradecer a Dios por permitirme culminar mis Estudios Universitarios a la vez, agradecer a la Universidad Técnica de Cotopaxi por abrirme las puertas para seguir mis estudios Superiores, Agradecer también al Ingeniero Jorge Rubio por ser un gran docente y tutor de nuestro proyecto de investigación, sobre todo demostrándonos paciencia y Amabilidad, pues nos brindó sus mejores conocimientos y guía en todas las etapas del proyecto para que al final lleguemos a la meta deseada.

A mi Familia por estar siempre a mi lado en todo momento siempre pendientes de se cumpla cada uno de mis objetivos y metas trazadas.

A Nuestros Docentes de la Carrera que fueron parte de la formación académica los cuales con paciencia y esmero nos enseñaron conocimientos necesarios para que podamos desenvolvernos y desarrollar habilidades en el campo laboral.

GUANOLUISA GUANOLUISA JESSICA ALEXANDRA

DEDICATORIA

A mi Madre Marina Guanoluisa quien me brindo su confianza infinita para llegar a cumplir una meta más en la vida pues ella fue la persona quien me inculco muchos valores desde pequeña y quien estuvo al tanto de toda mi formación académica haciendo de mi una persona responsable, motivándome a conseguir mi título y nunca darme por Vencida.

Finalmente quiero dedicar este proyecto a mi Esposo Luis Aymacaña, a mis niñas Antonella y Sherezade quienes son parte fundamental en mi vida, siendo la principal motivación para no darme por vencida.

GUANOLUISA GUANOLUISA JESSICA ALEXANDRA

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TITULO: "**IMPLEMENTACIÓN DE UNA RED VPN "VIRTUAL PRIVATE NETWORK" PARA LA MEJORA DE LA SEGURIDAD DENTRO DE LA RED LOCAL INALÁMBRICA DE LA EMPRESA DE DISTRIBUCIÓN DE MATERIAL DE CONSTRUCCIÓN Y FERRETERO "DISTRIBUIDORA GÓMEZ", MEDIANTE EL USO DE PROTOCOLOS IPSEC Y TCP/IP**"

Autores:

Andaluz Guerrero Alex Agustín

Guanoluisa Guanoluisa Jessica Alexandra

RESUMEN

La presente investigación tipo como objetivo Implementar Una red VPN VIRTUAL PRIVATE NETWORK mediante el uso de protocolos IPSEC y TCP/IP , siendo así que la implementación de una red VPN en la empresa permitirá la integración de los datos mejorando su control y protección mediante la aplicación de protocolos de seguridad, y autenticaciones de usuario, para mayor privacidad de la empresa y de los equipos informáticos con los que cuenta la oficina principal. Pues La VPN será capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos que no estén autorizados, la VPN implementada deberá dar dirección al cliente en la red privada esperando que las direcciones privadas se conserven entre sí, generando y renovando claves de codificación tanto para el cliente como para el Servidor .Al realizar la implementación de la VPN nos basaremos de su disponibilidad,control,Compatibilidad,Seguridad,Confiabilidad,Autenticacion de Datos y Usuarios que se conecten ala VPN, esperando de esta Manera que se integren Elementos como el Servidor VPN, cliente VPN ,Túnel para datos Encriptados.

Palabras Claves: Vpn, cliente, servidor, túnel, Ipsec, Tcp, Ip, implementar

TOPIC: IMPLEMENTATION OF A "VIRTUAL PRIVATE NETWORK" VPN NETWORK TO IMPROVE SECURITY WITHIN THE WIRELESS LOCAL NETWORK OF THE "DISTRIBUIDORA GÓMEZ" CONSTRUCTION MATERIAL AND HARDWARE DISTRIBUTION COMPANY THROUGH THE USE OF IPSEC AND TCP/IP PROTOCOLS.

Authors:

Andaluz Guerrero Alex Agustín

Guanoluisa Guanoluisa Jessica Alexandra

ABSTRACT

The objective of this research is to implement a VIRTUAL PRIVATE NETWORK VPN network through the use of IPSEC and TCP / IP protocols, being that the implementation of a VPN network in the company will allow the integration of data, improving its control and protection through the application of security protocols, and user authentications, for greater privacy of the company and of the computer equipment that the main office has. Well, the VPN will be able to verify the identity of the users and restrict access to the VPN to those who are not authorized, the implemented VPN must give the client an address in the private network, hoping that the private addresses will keep each other, generating and renewing encryption keys for both the client and the Server. When implementing the VPN we will base it on its availability, control, compatibility, security, reliability, data authentication and users who connect to the VPN. Hoping in this way that Elements such as VPN Server, VPN client, Tunnel for Encrypted data are integrated.

keywords: Vpn, client, server, tunnel, IPsec, Tcp, Ip, implement.

UNIVERSIDAD TÉCNICA DE COTOPAXI

CENTRO DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi, en forma legal **CERTIFICO** que:

La traducción del resumen al idioma Inglés del proyecto de investigación cuyo titulo versa: **IMPLEMENTACIÓN DE UNA RED VPN "VIRTUAL PRIVATE NETWORK" PARA LA MEJORA DE LA SEGURIDAD DENTRO DE LA RED LOCAL INALÁMBRICA DE LA EMPRESA DE DISTRIBUCIÓN DE MATERIAL DE CONSTRUCCIÓN Y FERRETERO "DISTRIBUIDORA GÓMEZ", MEDIANTE EL USO DE PROTOCOLOS IPSEC Y TCP/IP"**, presentado por: **Andaluz Guerrero Alex Agustín y Guanoluisa Guanoluisa Jessica Alexandra** egresados de la Carrera de Ingeniería en Sistemas perteneciente a la **Facultad de Ciencias de la Ingeniería y Aplicadas** lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a los peticionarios hacer uso del presente aval para los fines académicos legales.

Latacunga, septiembre del 2022

Atentamente,

CENTRO DE IDIOMAS

MSc. Alison Mena Barthelotty
DOCENTE CENTRO DE IDIOMAS-UTC
CI: 0501801252

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

1. INFORMACIÓN GENERAL

Título del Proyecto:

Implementación de una Red VPN “Virtual Private Network” para la mejora de la seguridad dentro de la red local inalámbrica de la Empresa de distribución de material de Construcción y Ferretero “Distribuidora Gómez”, mediante el uso de protocolos Ipsec y Tcp/Ip.

Fecha de inicio:

Abril 2022

Fecha de finalización:

Agosto 2022

Lugar de ejecución:

Cantón “Quito” Parroquia “Alangasi” Av. Ilalo s5-87 y Rio Corrientes Esq. Distribuidora de Material de Construcción y Ferretero “Distribuidora Gómez”.

Facultad que auspicia:

Facultad de Ciencias de la Ingeniería y Aplicadas

Carrera que auspicia:

Ingeniería en Informática y Sistemas Computacionales

Proyecto de investigación vinculado:

Transformación Digital y Nuevas Tecnologías

Equipo de Trabajo:

Tutor (Anexo A)

Apellidos y Nombres: Ing.: Rubio Peñaherrera Jorge Bladimir

Cédula de ciudadanía: 0502222292

Estado civil: Casado

Email institucional: Jorge.rubio@utc.edu.ec

Teléfono: 0995220308

Investigador I (Anexo B)

Apellidos y Nombres: Andaluz Guerrero Alex Agustín

Cédula de ciudadanía: 1724441564-5

Fecha de nacimiento: 18-11-1995

Estado civil: Soltero

Email institucional: alex.andaluz1645@utc.edu.ec

Teléfono: 0992791749

Investigador II (Anexo C)

Apellidos y Nombres: Guanoluisa Jessica Alexandra.

Cédula de ciudadanía: 050441543-1

Fecha de nacimiento: 16-08-1994

Estado civil: Casado

Email institucional: jessica.guanoluisag1@utc.edu.ec

Teléfono: 0979166662

Área de Conocimiento:

Información, Comunicación, Tics

Ciencias, 48 Informática (Unesco),

Línea de investigación:

Tecnologías de la Información y comunicación

Sublíneas de investigación de la Carrera:

Sublínea 1.- Diseño, implementación y configuración de redes y Seguridad Computacional, aplicando normas y estándares internacionales.

2. INTRODUCCIÓN

2.1. EL PROBLEMA:

En la actualidad la empresa "Distribuidora Gómez" cuentan con una infraestructura de red en la cual todos los empleados pueden ingresar a los datos existentes en las máquinas de la oficina principal, por lo que se conoce que existe una configuración de red local en la empresa a la que no deben tener acceso las personas que no se encuentren verificadas.

Actualmente la empresa realiza sus procesos de monitoreo y transmisión de información, por medio de correo electrónico, medios de almacenamiento externo, o aplicaciones de acceso remoto con el fin de precautelar la información que maneja la oficina principal. Al utilizar este tipo de medios para el manejo de la información, se cuenta con un alto riesgo de que la misma pueda sufrir alteraciones o pueda perderse, por lo que la implementación de una red VPN en la empresa permitirá la integración de los datos mejorando su control y protección mediante la aplicación de protocolos de seguridad, y autenticaciones de usuario, para mayor privacidad de la empresa y de los equipos informáticos con los que cuenta la oficina principal.

2.1.1 Situación Problemática

La empresa en la actualidad cuenta una sede principal, la cual cuenta con su propio proveedor para el acceso a internet independiente de la red local del hogar, a su vez cuenta con servidor localizado en la oficina principal del establecimiento: el mismo es un servidor de base de datos el cual cumple la función de almacenar los registros del stock del almacén, el registro de ventas, y el inventario del mismo, así como también controla y gestiona un sistema de cámaras de vigilancia con acceso remoto, el que actúa como proxy para el control de accesos.

De esta manera se conoce que solo la oficina principal y los administradores de la empresa tienen acceso al uso de estos recursos, debido a esto se considera importante el control del registro de la información desde cualquier ubicación. Siendo así que el acceso a la información y datos más relevantes de la empresa como son el registro del stock o inventario de los productos de la sucursal, el registro de las ventas y control diario de caja sólo es accesible desde la sede principal, por lo que el administrador solo se puede acceder a la información vía correo electrónico, comunicación telefónica o de forma manual mediante los equipos informáticos de la oficina principal.

Siendo que el servidor principal de Active Directory se encuentra ubicado físicamente en la sede principal la misma que cuenta con una red local interna (LAN), y conociendo que este es único punto de acceso con controles de seguridad, siendo que al no contar con un control para la comunicación de la sede principal con el hogar del Administrador, los empleados tienen el acceso libre y sin restricción a chats y páginas web, y demás información de la empresa, lo que representa un bajo nivel de desempeño laboral por parte del empleado.

2.1.2 Formulación del problema:

¿Cómo se establecería una comunicación con los equipos físicos de la empresa mediante una red VPN con el fin de brindar seguridad y confianza al momento de monitorear o transferir datos?

2.2 REVISIÓN BIBLIOGRÁFICA Y DOCUMENTAL

En la Referencia [16] ALEJANDRO ROBINSON MOREIRA sobre DISEÑO DE UNA VPN (VIRTUAL PRIVATE NETWORK) PARA ACCEDER VÍA WI-FI A LA RED INALÁMBRICA DE LA FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS PARA LA CARRERA DE NETWORKING Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE GUAYAQUIL" **Manifiesta:** "La presente investigación tiene como objetivo diseñar una Red Privada Virtual, VPN por sus siglas en inglés, para acceder vía Wi-Fi a la red inalámbrica de la Facultad de Ciencias Matemáticas y Físicas para la carrera de ingeniería en Sistemas y Networking de la Universidad de Guayaquil. Se muestra una investigación descriptiva que permitió elaborar un perfil sobre el diseño de la VPN que se implementó, sirviendo de apoyo una encuesta que contribuyó a analizar las expectativas de la comunidad universitaria. La VPN

diseñada posibilita el acceso seguro a la red de la Universidad de Guayaquil empleando protocolos de seguridad que garantizan la confidencialidad y disponibilidad de los datos.**”**

JARAMILLO ZAMORA ALEX WLADIMIR en la referencia [17] se explica como la TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA;TELECOMUNICACIONES;REDES DE COMUNICACIÓN;SEGURIDAD PROTOCOLO INTERNET (IPSEC);RED PRIVADA VIRTUAL MULTIPUNTO DINÁMICA (DMVPN);RED PRIVADA VIRTUAL (VPN);RETARDO DE PAQUETES;VARIANZA DEL TIEMPO (JITTER);INTERNET nos **menciona que:** “Se realizó el análisis comparativo entre Red privada virtual Protocolo de Internet Seguro (VPN IPSEC) y red privada virtual multipunto dinámica (DMVPN) para mejorar el desempeño de redes privadas sobre Internet. La solución tradicional de VPN se basa en IPsec punto a punto, la cual no permite una comunicación directa entre cada sitio y depende del estado de su concentrador para garantizar la comunicación. Se evaluó una nueva técnica que elimina las conexiones punto a punto y permite la convergencia de las aplicaciones, se analiza DMVPN como una solución que permitirá mejorar el desempeño de las VPN sobre Internet. Se implementó una red de un HUB y cuatro SPOKE para la transmisión y evaluación de paquetes de datos, voz y video”.

En la Referencia [18] **Según Oña LLumitasig Diego** sobre: ANÁLISIS E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL VPN CON TÚNELES DE SEGURIDAD EN EL TRANSPORTE DE DATOS CON UN SERVIDOR CENTOS LINUX: CASO PRÁCTICO: PROPUESTA DE IMPLEMENTACIÓN EN LA UNIDAD DE ADMISION Y NIVELACION DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI. **se refiere a** “En este proyecto se analiza y se implementa un modelo de seguridad de red y datos que ayudan a la protección de la información de intrusos no deseados que podrían perjudicar de una u otra manera la integridad de cada institución , por ende se ha puesto interés en el tema de seguridades ya que forman parte de un una nueva tecnología formada por certificados de autenticación, llaves de seguridad tanto como del servidor y los clientes y a la vez la incorporación de túneles que permiten el traslado del tráfico de datos e información segura en la nube y que forman parte fundamental de una Red Privada Virtual VPN. ”

AGUILAR FERNANDEZ LUIS en la referencia [19] nos habla sobre la: IMPLEMENTACIÓN DE UNA VIRTUAL PRIVATE NETWORK PARA LA INTERCONEXIÓN DE LA EMPRESA ALBIS S.A. CON SUS SUCURSALES EN PROVINCIAS-CHICLAYO DICE: "El presente trabajo denominado "Implementación de una Virtual Private Network para la Interconexión de la Empresa Albis S.A. con sus sucursales en Provincias", mostrará el uso del software que permita racionalizar y administrar los recursos en una red privada. La investigación realizada surge a raíz que en todo el ámbito empresarial un sistema de teléfono análogo que presenta fallas en su normal desempeño genera incomodidad al carecer de este importante servicio de comunicación. El objetivo principal de este proyecto encamina a dotar a LA EMPRESA ALBIS S.A de una Central de telefonía IP con servidor Asterisk que permite brindar un servicio confiable y eficiente, haciendo usos de los múltiples recursos. El proyecto está dividido en diferentes capítulos que me permitirá desarrollar cada punto en cuestión que se ha considerado para el desarrollo de la misma En el Capítulo I, se describe a la Institución en estudio considerando su misión, visión, objetivos y funciones básicas como su estructura organizativa. En el Capítulo II, se tiene en cuenta para el análisis del problema, la situación problemática, como su formulación del problema, su justificación e importancia, el objetivo general y específico del proyecto. Este punto nos permitirá identificar cuáles son las variables e indicadores. En el Capítulo III, se considera todo lo referente a Antecedentes Teóricos sobre Proyectos y trabajos de investigación ya realizados en base a este proyecto que se desea realizar."

2.3 OBJETIVOS Y CAMPO DE ACCIÓN

Objeto de estudio: Distribuidora de material de construcción y ferretero "Distribuidora Gómez".

La empresa "Distribuidora Gomez" se verá beneficiada con la implementación del proyecto, ya que permitirá que la misma potencia sus procesos de ventas, de artículos de construcción y material ferretero, motivo por el que la empresa decide mejorar los procesos de control y gestión de la información de su oficina principal optimizando los recursos existentes y agilizando los procesos de transacciones diarias de la empresa, de esta manera se proyecta un proceso de

interconexión de redes la cual permita al gerente acceder a los datos de forma remota desde su hogar hacia la oficina principal de la empresa y sus demás departamentos.

Actualmente dentro de la empresa “Distribuidora Gomez” se conoce que los distintos procesos administrativos que se realizan en la oficina principal presentan un estado de potencial riesgo de pérdida y daño de la información, por lo que la gerencia de la empresa requiere un sistema de comunicación remoto el cual permita la gestión de la información desde un punto A un punto

B, de manera rápida, segura y en tiempo real, siendo el campo de acción para el presente proyecto el área de informática y finanzas, impactando con la solución a estos departamentos permitiendo la interconexión entre la empresa y el hogar del gerente.

2.4 BENEFICIARIOS

Se determina como beneficiarios a los 3 actores principales, para la ejecución y funcionamiento del aplicativo, tales como la Gerente propietaria de la Empresa de Distribución de material de Construcción y Ferretero “Distribuidora Gómez”, la secretaria y encargada de Caja, el Administrador general de la “Distribuidora Gómez”, y 3 personas que colaboraran dentro de la empresa en actividades varias.

Tabla 1. Beneficiarios

Beneficiarios Directos	**Responsable**	**Beneficiarios Indirectos**
Ing. Jacqueline Gómez	Gerente Propietario	10
Ing. Santiago Andaluz	Administrador General	8
Lic. Lidia Gualichico	Trabajadora	3

Fuente: los investigadores

2.5 JUSTIFICACIÓN

La implementación de una red VPN dentro de la empresa presenta una solución en cuanto a la seguridad y protección de la información, beneficiando en el gasto en cuanto a transferencia de información entre los equipos informáticos de la oficina principal.

Con el uso de una VPN se logra la conexión de los equipos dentro de una red LAN interna en la empresa, a través de medios de autenticación los cuales proporcionen una seguridad extra en el cifrado de esta información

Para la empresa es de vital importancia contar con las seguridades necesarias para la protección de este tipo de información con el fin de precautelar los datos que se manejan dentro del servidor principal de la empresa, razón por la cual se recomienda la implementación de una VPN para la integración de los equipos informáticos y sus redes internas mediante el uso de red "LAN" usando los recursos públicos disponibles.

La implementación de una red privada virtual dentro de la empresa "Distribuidora Gómez" permitirá a la misma contar con una mejor relación costo/beneficio dado que una VPN representa un menor gasto económico con respecto a los gastos actuales de la empresa sobre la seguridad de la información.

2.6 HIPÓTESIS

Con la implementación de una Red Privada Virtual "VPN" en la empresa "Distribuidora Gómez", se verá una mejorará la seguridad y transmisión de los datos de la sede principal con equipos Informáticos del propietario y administradores encargados de la empresa mejorando el tráfico de red interna al igual que la privacidad en red.

Variable Dependiente

- Implementación de una red VPN
- Análisis de protocolos Ipsec
- Valoración de equipos y recursos conectados a la red

Variable Independiente

- Aplicación de protocolos de seguridad Ipsec
- Creación de un canal punto a punto dentro de una red privada virtual
- Implementación de la Red VPN en la empresa solicitante.

2.7 OBJETIVOS

2.7.1 General

Implementar una red VPN que proporcione confianza y seguridad en el manejo de la información, mediante la utilización de los protocolos IPsec y TCP/IP como una alternativa para el acceso remoto a los datos de la Empresa de Distribución de material de Construcción y Ferretero "Distribuidora Gómez".

2.7.2 Específicos

- Definir las bases teóricas para la elaboración de una propuesta mediante diagramas lógicos de red para estructurar un proceso de diseño de la VPN
- Determinar la metodología más adecuada para la implementación de los protocolos Ipsec para la VPN con la finalidad de mejorar la seguridad en la misma.
- Implementar en la red VPN en la Empresa de Distribución de material de Construcción y Ferretero "Distribuidora Gómez" para la conexión de usuarios de forma remota.

2.8. SISTEMA DE TAREAS

Tabla 2. Sistema de Tareas

Objetivos específicos	Actividades (Tareas)	Resultados Esperados	Técnicas, Medios e Instrumentos
Definir las bases teóricas para la elaboración de una propuesta mediante diagramas lógicos de red para estructurar un proceso de diseño de la VPN	Recolección de información sobre el estado del equipo informático - Análisis y diagnóstico del equipo informático y soporte de red. - Determinar protocolos y estándares para el uso de VPN de acuerdo con los equipos informáticos.	- Determinar las características necesarias para la implementación de una red VPN - Obtener resultados sobre el uso de Vpn locales confiables.	-Observación, diagnostico técnico, pruebas de red, revistas, artículos científicos
Determinar la metodología más adecuada para la implementación de los protocolos Ipsec para la VPN	- Recolección de información sobre las VPN en redes locales	- Obtener una estructura básica para la implementación de una VPN	-Revistas, Artículos científicos, Videos Tutoriales.

con la finalidad de mejorar la seguridad en la misma.	- Clasificación de los datos encontrados sobre las VPN en redes locales - Delinear referencias y citas bibliográficas más relevantes	- Obtención de un software adecuado para que permita una VPN	
Implementar en la red VPN en la Empresa de Distribución de material de Construcción y Ferretero "Distribuidora Gómez" para la conexión de usuarios de forma remota.	- Aplicación de un software análisis para la red local - Determinar medios de comunicación para la red local de la empresa - Recolección de información sobre validaciones y cifrado de datos para conexión remota	- Informe sobre los recursos necesarios para la VPN - Obtención de herramienta s confiables para el manejo de redes VPN - Obtención y análisis de los protocolos de seguridad necesarios para VPN en redes locales	-Artículos Científicos, Repositorios digitales, publicaciones de internet. Google Meet, Cisco Packer Traer.

Fuente: los investigadores

3. FUNDAMENTACIÓN TEÓRICA

3.1 ANTECEDENTES

El concepto de una VPN se hace presente hace algunos años atrás en todas las redes. En 1960 se dice que fueron grandes portadores llamados VPN utilizados para servicios de voz, esto funcionaba de la siguiente manera. Las empresas tenían una red privada de voz mientras se iba compartiendo los recursos de red, actualmente se los llamaría voz para datos. Creándose así el primer sistema de redes de la historia donde también a la VPN se le llamaba Arpanet.

Arpanet fue creada para reducir fallos en la red es considerada como los primeros pasos de seguridad de Internet donde se avanzaba con distintos avances técnicos, gracias a Arpanet se pudo ejecutar programas en computadores remotos, pero en aquel entonces permitían que los

usuarios de Arpanet envíen y reciban mensajes electrónicos desarrollándose en los programas de red-email.

Sobre los años 80 se crea los protocolos TCP/IP siendo este un estándar para este tipo de comunicación, pero este intercambio de comunicación causó muchos problemas, interviniendo muchos hackers ante este problema los cuales intentaban compartir datos por esta vía. En los años 90 iniciaron la creación de software IP dando un mejor rendimiento de seguridad y sobre todo mejorando todos los protocolos Ip. El servicio de las VPN contiene acceso privado a internet fue creado para las grandes empresas u organizaciones las cuales son expuestas a una serie de amenazas que pudieran vulnerar la confidencialidad de la información.

Siendo así que también las VPN es una subred privada donde se comparte los recursos de una red de información, en donde Internet es la plataforma ideal para la creación de un VPN.

En la construcción de las redes se fueron construyendo elementos de encriptación o VPN seguras para transmitir información segura por medio de internet. VPN podía ser complementaria y confiable y segura cumpliendo:

- VPN debe estar encriptada y autenticada pues las propiedades de seguridad deber ser guardadas por todas las redes VPN.
- Las propiedades de las VPN confiables aseguran el canal de servicio brindando seguridad ante los atacantes de red.

La encriptación se convierte en un código secreto que permite ocultar los datos que se envíe o que se reciben o guarda lo que se sigue almacenando ,tomando en cuenta la información importante que tiene una empresa es la encriptación de los datos pues ya que esta es una de las formas de mantener datos importantes de la empresa protegida de amenazas y de seguridad cibernética pues la encriptación empieza desde cuando navegas por internet, en la encriptación se evita el acceso no autorizado de tus datos pues con tal solo enviamos un mensaje a través de internet estamos enviando un mensaje ya encriptado y a su vez llegara a su destino.

Desde el punto de vista de una empresa es importante observar que muchos dispositivos ofrecen encriptación como un estándar como por ejemplo Windows que ofrece funciones de encriptación si se desea encriptar los correos electrónicos existen diversas herramientas incorporadas de encriptación.

3.2 FUNDAMENTOS DE UNA VPN

3.2.1 ¿Cómo funciona una red privada virtual (VPN)?

[1]¿Una VPN extiende la red corporativa a través de conexiones cifradas por Internet. Debido a que el tráfico está cifrado entre el dispositivo y la red, el tráfico sigue siendo privado durante el recorrido. Un empleado puede trabajar fuera de la oficina y, aun así, conectarse de manera segura a la red corporativa. Incluso se pueden conectar smartphones y tablets mediante la VPN.

3.2.2¿Qué es el acceso remoto seguro?

Secure Remote Access proporciona una forma segura y protegida de conectar a los usuarios y sus dispositivos de forma remota a una red corporativa. Incluye la tecnología de VPN que usa formas sólidas de autenticar el usuario o dispositivo. La tecnología de VPN está disponible para verificar si un dispositivo cumple determinados requisitos, lo que también se denomina estado del dispositivo, antes de que pueda conectarse de forma remota.

3.2.3 REQUERIMIENTOS BÁSICOS DE UNA VPN

[2]Para implementar la VPN tener en cuenta lo siguiente:

- **IDENTIFICACIÓN DEL USUARIO**

La VPN será capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos que no estén autorizados.

- **ADMINISTRACIÓN DE DIRECCIONES**

La VPN debe dar dirección al cliente en la red privada y deber esperar que las direcciones privadas se conserven entre sí.

- **CODIFICACIÓN DE DATOS**

Los datos que se transmitan en la red pública deben ser previamente encriptados para que no puedan ser leídos por los clientes no autorizados en la red.

- **ADMINISTRACIÓN DE CLAVES**

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

3.3 TIPOS DE REDES PRIVADAS VIRTUALES

3.3.1 VPN basada en hardware

- [2] Utilizan básicamente equipos dedicados (routers).
- Son seguras y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red.

3.3.2 VPN basada en firewall

- El rendimiento en este tipo de VPN decrece, ya que no se tiene hardware especializado de encriptación.
- Utilizan equipos firewall dedicados.
- Tienen un alto costo económico.

3.3.3 VPN basada en software

- Permiten que el tráfico de túnel sea dependiendo de la dirección o protocolo, a diferencia de los productos basados en hardware.[3]
- Ofrecen mayor flexibilidad en cómo se gestiona el tráfico de red
- Tienen un bajo costo económico.

3.3.4 VPN Intranet:

Este tipo de red es creado entre una oficina central y una o varias o

Se crea entre las oficinas centrales y los usuarios situados remotamente, ya sea a través de dispositivos móviles o terminales fijas. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa donde se encuentre. [4]

3.3.5 VPN Extranet:

[5]Se forma entre dos organizaciones diferentes, o bien entre una corporación y sus proveedores o clientes. Se puede implementar una VPN Extranet mediante acuerdo entre miembros de distintas organizaciones.

3.3.6 VPN Internas:

Con la migración hacia redes inalámbricas, como 802.11, es necesario incrementar las medidas de seguridad en una corporación. Actualmente se puede implementar una VPN interna cuando se tiene una LAN inalámbrica. En este caso la red pública es el espectro de frecuencia que se ocupa para comunicar un punto de acceso (AP) y un dispositivo 22 móvil. Muchos de los

ataques son ejecutados desde el interior de las corporaciones, por los que una VPN interna elimina la posibilidad de que un usuario malintencionado logre acceder al servidor principal sin tener los permisos necesarios.[6]

3.4 COMPONENTES QUE CONFORMAN UNA VPN

[7] Las VPN consisten hardware y software, y además requieren otro conjunto de componentes. Estos componentes son simples requisitos que garantizan que la red sea segura, este disponible y sea fácil de mantener. Son necesarios ya sea que un PSI proporcione la VPN o que usted haya decidido instalar una por sí mismo.

- ✔ **Disponibilidad**

  Se aplica tanto al tiempo de actualización como al de acceso.

- ✔ **Control**

  [8]Suministra capacitación, experiencia, supervisión meticulosa y funciones de alerta que ofrece algunos proveedores de servicios administrados. Una consideración significativa es que sin importar que tan grande sea la organización, es probable que solo cuente con una VPN; puede tener otros puntos de acceso, pero seguirá siendo una VPN corporativa.

- ✔ **Compatibilidad**

  [9] Para utilizar tecnología VPN e Internet como medio de transporte, la arquitectura interna del protocolo de red de una compañía debe ser compatible con el IP nativo de Internet.

- ✔ **Seguridad**

  [9] Lo es todo en una VPN, desde el proceso de cifrado que implementa y los servicios de autenticación que usted elige hasta las firmas digitales y las autoridades emisoras de certificados que utilizan. Abarca el software que implementa los algoritmos de cifrado en el dispositivo de la VPN.

✔ **Confiabilidad**

[9] Cuando una compañía decide instalar el producto VPN de un PSI, está a merced de este.

✔ **Autenticación de Datos y Usuarios**

[10] Datos: Reafirma que el mensaje ha sido enviado completamente y que no ha sido alterado de ninguna forma.

Usuarios: clientes que se conectan a la VPN.

✔ **Sobrecarga de tráfico**

[10] En todo tipo de tecnologías existen sacrificios: velocidad contra desempeño, seguridad contra flexibilidad. Las VPN caben en la misma categoría cuando se hablan de tamaño de paquetes cifrados la sobrecarga está en juego, ya que si mandamos varios paquetes se incrementa el tamaño de estos y por lo tanto se afecta la utilización del ancho de banda.

3.5 CARACTERÍSTICAS DE UNA VPN

[11]Existe la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde casa

o algún usuario que pueda acceder a su equipo doméstico desde un sitio remoto, siempre y cuando utilizando la infraestructura de internet utilizando autenticación, integridad y confidencialidad

de la comunicación

- ✔ **Autenticación**: El emisor y el receptor son capaces de determinar las entidades.
- ✔ **Integridad:** Se da la garantía de que los datos que llegan al receptor sean exactamente los que el emisor transmite por el canal [12]
- ✔ C**onfidencialidad**: La información no debe poder ser interpretada por nadie más que los destinatarios de la misma la manera de conseguir esto mediante Técnicas de Encriptación [13]

3.6 REQUISITOS BÁSICOS DE UNA VPN

[14]Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

- ✔ **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, se debe proporcionar registros estadísticos que muestren quien acceso, que información es la que introdujo, actualizo, utilizo y cuando.
- ✔ **[12] 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.
- ✔ **[13] 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.

3.6.1 ELEMENTOS DE UNA VPN

[14] SERVIDOR VPN: Acepta la conexión VPN de un cliente.

[14] CLIENTE VPN: el computador da inicio a la conexión VPN puede ser un computador individual o una red distinta a la que se requiera conectar.

[15] TÚNEL: se transmitirán datos encriptados.

PROTOCOLOS DE TUNNELING: Se crean estándares en cual se rige a los túneles y a la conexión de los datos que fueron encriptados.

[16] DATOS DE TÚNEL: son los datos que se ejecutan en el túnel.

RED DE TRÁNSITO: Es la red pública que encapsula a todos los datos.

CONEXIÓN VPN: Se realiza la conexión punto a punto.

3.6.1.1 CONEXIONES DE VPN

Existen 3 tipos de conexiones

- **ACCESO REMOTO**

  [16] Esta conexión la realiza un cliente remoto. En este caso el servidor VPN provee acceso a recursos del servidor o también de la red que se encuentre conectada, luego los paquetes de la VPN se producen en el acceso remoto del cliente.

- **DE ROUTER A ROUTER**

  Se establecen dos routers para luego unir dos capas de red conectándose el cliente con el servidor, para autenticar y abastecer los recursos del servidor.

- **VPN INTERNA**

  [17] Es la más fácil de utilizar dentro de una empresa estableciendo acceso remoto, conectándose a la propia red LAN, siendo que solo el personal autorizado tiene acceso a cualquier información.

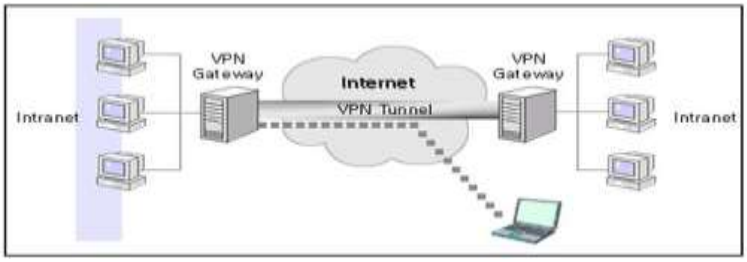
TECNOLOGÍA DE TÚNEL

[18] "Túnel" se conoce como la encapsulación y la transmisión de datos VPN, o paquetes. IPSec permite cargas útiles a cifrar y encapsulando en un encabezado IP para que pueda ser enviada a la red interna corporativa y/o Internet.

3.7 TECNOLOGÍA DE TÚNEL

[18]"Túnel" se conoce como la encapsulación y la transmisión de datos VPN, o paquetes. IPSec permite cargas útiles a cifrar y encapsulando en un encabezado IP para que pueda ser enviada a la red interna corporativa y/o Internet.

Imagen 1. Esquema de Red Tunel



Fuente: Vivanco / 2003

3.8 IPSEC

[19] IPSec protege, garantiza y autentifica datos entre dispositivos IPSec pares mediante el suministro de paquetes de datos por autenticación. Los flujos de datos entre pares IPSec son confidenciales y protegidos. Las direcciones de origen y destino están codificadas. El datagrama IP original se deja intacto. El encabezado IP original se copia y se traslada a la izquierda y se convierte en un nuevo encabezado IP. La cabecera IPSec se inserta entre estas dos cabeceras. El datagrama IP puede ser autenticado y encriptado.

3.8.1 Estructura IPSEC

[20]El protocolo contiene un primer encabezado llamado Cabecera de Autenticación

- Autenticación (AH), el cual provee integridad y autenticación del origen y protección contra duplicados.

La Autenticación de Encabezado IPSec protege la integridad de la mayoría de los campos de encabezado de IPv6, excepto a aquellos que cambian sobre los enrutamientos, de la misma forma como lo hace el campo “Límite de Salto” del paquete, adicionalmente el AH autentica el origen por medio de un algoritmo de cifrado.[20]

El segundo encabezado llamado “Encapsulado de Seguridad de Carga Útil” - IPsec (ESP Encapsulating Security Payload), el cual provee confidencialidad, autenticación del nodo origen, integridad interna del paquete y protección contra duplicación.[21]

3.8.2 TÚNEL VPN

El túnel es la ruta de acceso o conexión lógica que encapsula los paquetes de viaje a través de la red de tránsito. El protocolo de túnel cifra el marco original para que su contenido no pueda interpretarse.

Túneles VPN pueden crearse en las siguientes capas de la Interconexión de Sistemas Abiertos (OSI), modelo de referencia:

- Capa de enlace de datos - la capa 2: protocolos de VPN que operan este punto son capa-to-Point Tunneling Protocol (PPTP) y Protocolo de túnel de capa 2 (L2TP).
- Network Layer - capa 3: IPSec puede operar como una VPN en la red de protocolo de la capa de modelo de referencia OSI. [22]

Los principales protocolos de túnel que poseen las redes privadas virtuales son los siguientes:

- Protocolo PPTP.
- Protocolo L2TP/IPSec.
- Protocolo OpenVPN SSL/TLS.[22]

3.9 PROTOCOLO PPTP

[23]Point-To-Point Tunneling Protocolo (PPTP) permitía el intercambio seguro de datos de un cliente a un servidor formando una Red Privada Virtual, empleando una red de trabajo TCP/IP.

Entre los puntos fuertes de PPTP se encuentran su facilidad de configuración en entornos Windows, su capacidad para trabajar sobre demanda, y su soporte multiprotocolo que le permite funcionar sobre infraestructuras de área de trabajo existentes como Internet o conexiones de acceso telefónico PPP.

3.10 PROTOCOLO L2TP

[24]L2TP (Layer 2 Tunneling Protocol) es un protocolo utilizado por redes privadas virtuales que fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos.

L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete de datos, incluyendo X.25, Frame Relay y ATM.[23]

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel.

Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.[24]

3.11 PROTOCOLO DE IP SECURITY

Imagen 2. Tecnologías usadas en Ipsec

Fuente: http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPSec/ipsec.pdf

IP Security (IPSec) proporciona una base estable y duradera para proporcionar seguridad de capa de red.

IPSec soporta todos los algoritmos criptográficos que se utilizan hoy en día y también puede ajustarse a algoritmos nuevos, más potentes que vayan surgiendo.

[24] El protocolo IPSec cubre las siguientes cuestiones de seguridad principales:

- **Autenticación de origen de datos**
- Verifica que cada datagrama ha sido originado por el remitente indicado.
- **Integridad de datos**
- Verifica que el contenido de un datagrama no se ha cambiado por el camino, ni deliberadamente ni debido a errores aleatorios.
- **Confidencialidad de datos**
- Oculta el contenido de un mensaje, normalmente mediante cifrado.
- **Protección de reproducción**
- Impide que un agresor pueda interceptar un datagrama y reproducirlo posteriormente.

1.- Tabla de Comparación de entre los principales protocolos VPN

Tabla 3. Comparativa de protocolos VPN

CARACTERÍSTICAS	PROTOCOLO PPTP	PROTOCOLO L2TP/IPSEC	PROTOCOLO OPENVPN SSL/TLS
Fuerza de Cifrado	128 bits con protocolo MPPE.	256 bits con cifrado AES.	256 bits con cifrado AES.
Nivel de Seguridad	Normal	Bueno	Muy Bueno
Plataformas Soportadas	Windows, Linux, Mac, Android, iPhone	Windows, Linux, Mac, Android, iPhone	Windows, Linux, Mac, Android, iPhone
Rendimiento	Muy Bueno	Muy Bueno	Muy Bueno
Acceso a puertos VPN aleatorios	No	No	Si mediante el puerto: 443/TCP
Riesgos de vulneración	Cuenta con Encriptación básica.	Se encarga de comprobar la integridad de los datos y los encapsula dos veces mediante encriptación.	Utiliza métodos de máxima encriptación. Identificando el acceso a los datos con certificados y claves digitales.
Seguridad Ofrecida	Media	Media	Alta

Fuente: los investigadores

3.12 EL MODELO OSI

3.12.1 RESENA

[7]El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como "modelo OSI", (en inglés, Open System Interconnection) es un modelo de referencia para los protocolos de la red (no es una arquitectura de red), creado en el año 1980 por la Organización Internacional de Normalización (ISO).1 Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones (UIT) y, desde 1984, la Organización

Internacional de Normalización (ISO) también lo publicó con estándar. Su desarrollo comenzó en 1977.

3.12.1.1 El modelo de referencia OSI

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

Se puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej. Hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aun cuando el transmisor y el receptor tengan distintos tipos de medios de red.

Imagen 3. Capas de modelo Osi

Fuente: https://users.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf IMAGEN 3

3.12.2 CAPAS DEL MODELO OSI

El modelo OSI se divide en 7 capas empezando por:

3.12.2.1 Capa Física

Es la capa más baja del modelo OSI. Es la que se encarga de la topología de red y de las conexiones globales de la computadora hacia la red, se refiere tanto al medio físico como a la forma en la que se transmite la información. [7]

Sus principales funciones se pueden resumir como:

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

3.12.2.2 Capa de Enlace de Datos

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

Es uno de los aspectos más importantes que revisar en el momento de conectar dos ordenadores, ya que está entre la capa 1 y 3 como parte esencial para la creación de sus protocolos básicos (MAC, IP), para regular la forma de la conexión entre computadoras, determinando el paso de tramas (unidad de medida de la información en esta capa, que no es más que la segmentación de los datos trasladándolos por medio de paquetes), verificando su integridad, y corrigiendo errores. [7]

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

3.12.2.3 Capa de Red

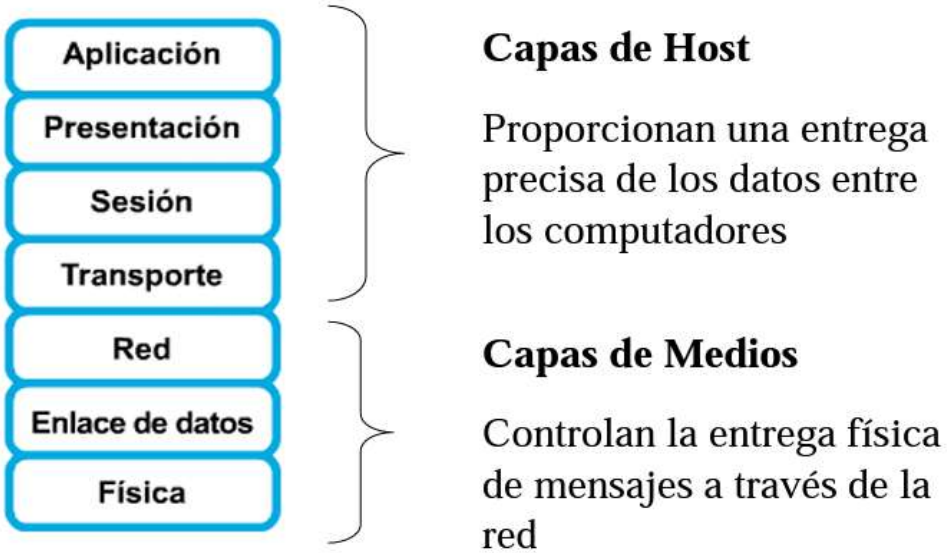
Se encarga de identificar el enrutamiento existente entre una o más redes. Las unidades de datos se denominan paquetes, y se pueden clasificar en protocolos enrutables y protocolos de enrutamiento.7

- **Enrutables:** viajan con los paquetes (IP, IPX, APPLETALK)
- **Enrutamiento:** permiten seleccionar las rutas (RIP, IGRP, EIGRP, OSPF, BGP)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente, sino que utilicen dispositivos intermedios.

Los dispositivos que facilitan tal tarea se denominan encaminadores o enrutadores, aunque es más frecuente encontrarlo con el nombre en inglés routers. Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de determinadas máquinas o limitar el acceso a ciertas de ellas. [7]

Imagen 4. Capa de Host vs Capa de Medios



Fuente: https://users.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

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

3.12.2.4 Capa de Transporte

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

La PDU (unidad de información) de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP, el primero orientado a conexión (transmisión verificada, eventualmente retransmitida) y el otro sin conexión (pueden perderse algunos datos por el camino). Trabajan, por lo tanto, con puertos lógicos y junto con la capa red dan forma a los conocidos como Sockets IP: Puerto (ejemplo: 191.16.200.54:80). [12]

3.12.2.5 Capa de Sesión

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles. [13]

3.12.2.6 Capa de Presentación

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

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. Por ejemplo, un mismo sitio web puede adecuar la presentación de sus datos según se acceda desde un computador convencional, una tableta, o un teléfono inteligente. [21]

Esta capa también permite cifrar los datos y comprimirlos. Por lo tanto, podría decirse que esta capa actúa como un traductor. [22]

3.12.2.7 Capa de Aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (Post Office Protocol y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar. [16]

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación, pero ocultando la complejidad subyacente. [17]

3.13 EL MODELO TCP/IP

3.13.1 **El modelo de referencia TCP/IP**

[17]Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el Protocolo de control de transmisión/Protocolo Internet (TCP/IP). El modelo de referencia TCP/IP y la pila de protocolo TCP/IP hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, a casi la velocidad de la luz. El modelo TCP/IP tiene importancia histórica, al igual que las normas que permitieron el desarrollo de la industria telefónica, de energía eléctrica, el ferrocarril, la televisión y las industrias de vídeos.

Imagen 5. Modelo de Referencias TCP/IP

Fuente: https://users.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

3.14 Encapsulamiento de Datos

- **1.Crear los datos.**

Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la internetwork. [18]

- **2.Empaquetar los datos para ser transportados de extremo a extremo.**

Los datos se empaquetan para ser transportados por la internetwork. Al utilizar segmentos, la función de transporte asegura que los hosts del mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable. [10]

- **3. Anexar (agregar) la dirección de red al encabezado.**

Los datos se colocan en un paquete o datagrama que contiene el encabezado de red con las direcciones lógicas de origen y de destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada. [15]

- **4. Anexar (agregar) la dirección local al encabezado de enlace de datos.**

[16] Cada dispositivo de la red debe poner el paquete dentro de una trama. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

- **5. Realizar la conversión a bits para su transmisión.**

[17] La trama debe convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio (por lo general un cable). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio en la internetwork física puede variar a lo largo de la ruta utilizada. Por ejemplo, el mensaje de correo electrónico puede originarse en una LAN, cruzar el backbone de un campus y salir por un enlace WAN hasta llegar a su destino en otra LAN remota. Los encabezados y la información final se agregan a medida que los datos se desplazan a través de las capas del modelo OSI.

3.15 TIPOS DE REDES

3.15.1 Redes LAN (Local Área Network) o Red de Área Local.

Una LAN es un conjunto de computadoras personales y de otros tipos que están interconectadas ya sea por medio de líneas telefónicas o fibra óptica, dentro de una zona limitada, para que los usuarios puedan además de intercambiar información compartir hasta un costoso periférico (como una impresora láser) y extraer programas y datos almacenados de un servidor de

archivos. Los usuarios se pueden comunicar unos con otros a través del 3 correo por medio de los servidores con el fin de compartir programas multiusuarios y accesar a bases de datos compartidas. [9]

3.15.2 Redes WAN (Wide Área Network) o Redes de Área Amplia.

Es una red generalmente formada por varias LANs interconectadas por medio de cables de alto desempeño y abarcan una extensa área geográfica. Entre las WAN más grandes se encuentran: la Arpanet (Advanced Research Projects Agency), que fue creada por la Secretaría de Defensa de los Estados Unidos y se convirtió en lo que es actualmente la WAN mundial: Internet, a la cual se conectan actualmente miles de redes universitarias, de gobierno, corporativas y de investigación. [9]

3.15.3 Redes MAN (Metropolitan Área Network) o Red de Área Metropolitana.

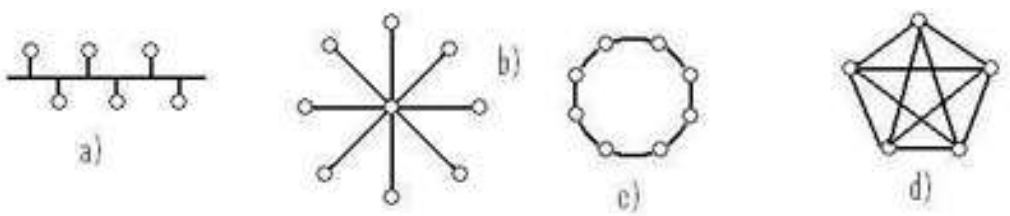
Una MAN es una red que está compuesta por varias LAN conectadas por un enlace de mayor velocidad en varias zonas. Una red de este tipo se puede utilizar, por ejemplo, en un campus Universitario donde se encuentran conectados diversos edificios como la biblioteca, centros de investigación, administración académica y la casa del estudiante entre 4 otros. Este tipo de red ocupa un área geográfica más amplia que una LAN, pero más pequeña que una WAN.[10]

3.16 TOPOLOGÍA DE LAS REDES

[9]Existen básicamente cuatro tipos de redes de las cuales de desprenden los siguientes tipos

- Red Tipo Bus
- Red Tipo Estrella
- Red Tipo Anillo
- Red Tipo Malla
- Red Tipo Hibrida

Imagen 6. Topología de redes: a) Bus b) Estrella c) Anillo d) Malla

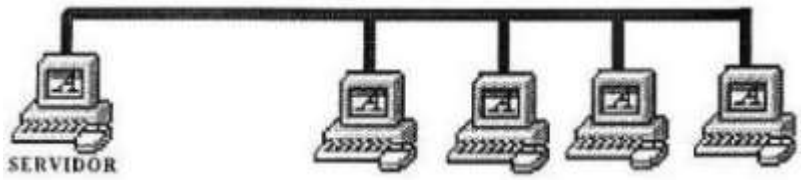


Fuente: https://uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Redes%20privadas%20virtuales.pdf

3.16.1 Red Tipo Bus

En esta tipología se utiliza un cable o una serie de cables como eje central al cual se conectan todas las computadoras. En este conductor se efectúan todas las comunicaciones entre computadoras. Esta red beneficia en su aplicación cuando no se requiere la conexión de múltiples computadores.[20]

Imagen 7. Estructura de la Red Tipo Bus

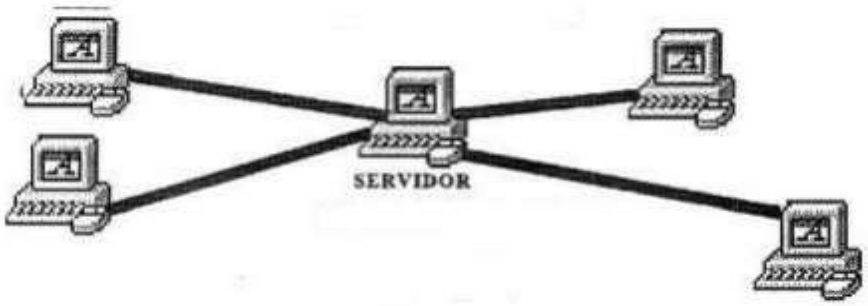


Fuente: http://platea.pntic.mec.es/~lmarti2/cableado.htm

3.16 .2 Red Tipo Estrella

Se caracteriza por tener un núcleo del cual se desprenden líneas hacia varias terminales. Fueron las primeras en utilizarse en el mundo de la computación. Esta tipología es útil cuando de tiene una computadora central muy potente rodeada de otras de menor potencia. Esta tipología es la más común porque es la que más utilizan las redes de Ethernet.[10]

Imagen 8. Estructura Red Tipo Estrella

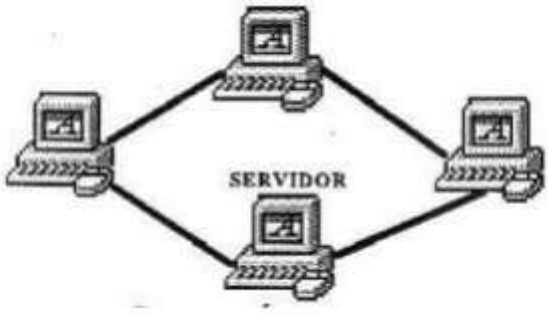


Fuente: http://platea.pntic.mec.es/~lmarti2/cableado.htm

3.16.3 Red Tipo Anillo

[10]Esta tipología utiliza un bus como eje central para conectar todos los equipos, sin embargo, dicho bus forma un anillo. Esta topología es utilizada en redes Token Ring y FDDI además de que es favorecida por los principales proveedores de acceso a internet.

Imagen 9. Estructura de Red Tipo Anillo

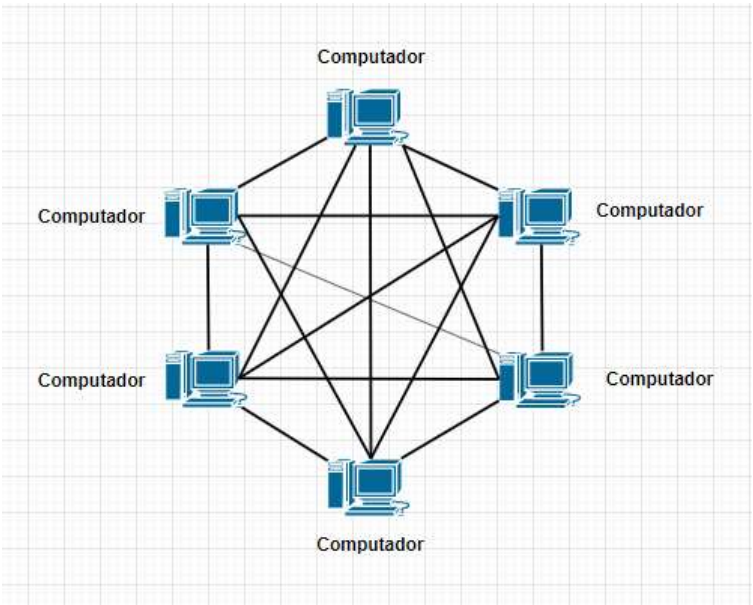


Fuente: http://platea.pntic.mec.es/~lmarti2/cableado.htm

3.16.4 Red Tipo Malla

[10] En esta tipología, todos los dispositivos o algunos de ellos son conectados con todos los demás con el fin de conseguir redundancia y tolerancia a fallos. Si un enlace falla, la información puede fluir por otro enlace. Las redes de más suelen implementarse solamente en redes WAN.

Imagen 10. Estructura Red Tipo Malla

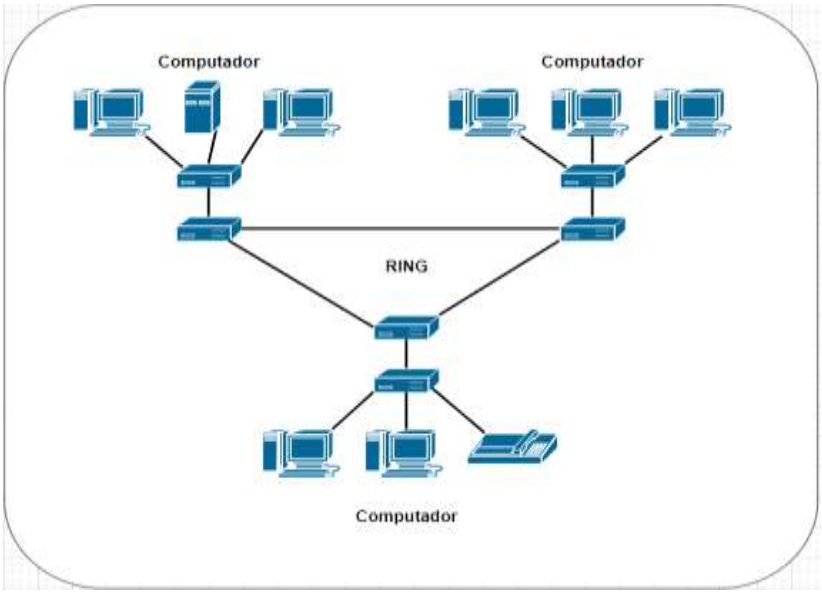


Fuente: los investigadores

3.16.5 Red Tipo Hibrida

La topología hibrida es una red que utiliza combinaciones de las topologías anteriores.

Imagen 11. Estructura de la Red Tipo Hibrida



Fuente: los investigadores

3.17 PROTOCOLOS DE REDES

[16] EL protocolo de una red se utiliza en la informática para nombrar a las normativas y los criterios que fijamos por cómo nos debemos comunicarnos con diversos sistemas de interconexión a través de este protocolo se conectan a una red pueden intercambiar datos, pues existen diversos protocolos y estándares así como también modelos que determinan el funcionamiento general de las redes destacando el modelo OSI y el TCP/IP , cada modelo tiene su estructura y su funcionamiento de una red de manera distinta .

El modelo OSI cuenta con capas muy definidas y con funciones diferencias y TCP/IP con cuatro capas diferentes que combinan las funciones existentes en las siete capas del modelo OSI, estos son los siguientes protocolos de red.[17]

3.17.1 HTTP

[19]es un protocolo sin estado de la capa de aplicación para sistemas de información de hipertexto distribuidos y colaborativos, HTTP se basa en el envío de mensajes sobre el protocolo TCP

- el cliente envía un mensaje de petición a un servidor solicitando realizar una acción
- el servidor envía un mensaje de respuesta a la petición del cliente

las versiones más sofisticadas son

http /1.1: versiones utilizadas mayormente desde finales de los 90

3.17.2 HPP/2

[12]Versión desplegada en los últimos años mejorando la codificación de mensajes, respuestas sobre una conexión TCP iniciadas por un servidor.

[23]Pues ambas versiones del protocolo son compatibles en términos de semántica y estructura de los mensajes, cambiando principalmente la codificación de los mensajes y el transporte de los mismos mediante conexiones TCP. Los recursos se identifican en HTTP mediante identificadores uniformes de recurso.

[13]Uri es una secuencia de caracteres que compacta e identifica un recurso abstracto.URI proporciona información necesaria desde localizar y acceder a un recurso.

- Esquema: hace referencia al nombre de un esquema, que define cómo se asignan los identificadores en su ámbito. Los esquemas habituales en la Web serán http y https.

- Autoridad: elemento de una autoridad jerárquica de asignación de nombres, típicamente basado en un nombre de dominio de DNS o una dirección de red (IP, IPv6) y, opcionalmente, un número de puerto.

- Ruta: elemento que identifica un recurso en el ámbito del esquema y autoridad proporcionados, típicamente organizado jerárquicamente en fragmentos separados por “/”.

- Consulta: datos no jerárquicos que permiten, en combinación en la ruta, identificar el recurso. Es habitual representarlo como uno o más pares nombre/valor.

- Identificador de fragmento: identifica un recurso secundario en el contexto del recurso primario como, por ejemplo, un fragmento concreto de una página Web

3.17.3 FTP

[22]El protocolo FTP permite copiar ficheros de miles de ordenadores diferentes de todas las partes de Internet, estos ficheros tienen todo tipo de información que se puede ir almacenando en un ordenador .Como todos los servicios de Internet ,FTP utiliza a cliente/servidor siendo necesario ejecutar un programa cliente en el ordenador que será el encargado de conectarse al programa servidor, que se encuentra en otro ordenador remoto, siendo así que el programa cliente transmite órdenes al servidor . El ordenador del usuario se denomina máquina local mientras que el otro ordenador, el servidor de ficheros se le denomina máquina remota FTP utiliza dos modos de transferencia de archivos.

3.17.4 SMTP

[23] El protocolo para transferencia de simple de correo es un protocolo de red en donde se intercambian mensajes de correo electrónico entre computadoras u otros dispositivos como puede ser teléfonos móviles, impresoras etc. Es decir que es un protocolo de conexión de internet que se encuentra en la capa de aplicación del modelo OSI pues la última capa de este modelo llama a la interfaz de las aplicaciones de comunicación y la red que transmite los mensajes.

4. MATERIALES Y MÉTODOS

4.1 PROPUESTA DE LA INVESTIGACIÓN A REALIZAR

La presente investigación tipo como objetivo Implementar Una red VPN VIRTUAL PRIVATE NETWORK mediante el uso de protocolos IPSEC y TCP/IP, permitiendo la implementación de una red VPN en la empresa que permitirá la integración de los datos mejorando su control y protección mediante la aplicación de protocolos de seguridad, y autenticaciones de usuario, para

mayor privacidad de la empresa y de los equipos informáticos con los que cuenta la oficina principal. Pues La VPN será capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos que no estén autorizados, la VPN implementada deberá dar dirección al cliente en la red privada esperando que las direcciones privadas se conserven entre sí, generando y renovando claves de codificación tanto para el cliente como para el Servidor .Al realizar la implementación de la VPN nos basaremos de su disponibilidad, control, Compatibilidad, Seguridad, Confiabilidad, Autenticación de Datos y Usuarios que se conecten a la VPN. Esperando de esta Manera que se integren Elementos como el Servidor VPN, cliente VPN ,Túnel para datos Encriptados.

4.2 Problema

En la actualidad la empresa "Distribuidora Gómez" cuentan con una infraestructura de red en la cual todos los empleados pueden ingresar a los datos existentes en las máquinas de la oficina principal, por lo que se conoce que existe una configuración de red local en la empresa a la que no deben tener acceso las personas que no se encuentren verificadas.

Actualmente la empresa realiza sus procesos de monitoreo y transmisión de información, por medio de correo electrónico, medios de almacenamiento externo, o aplicaciones de acceso remoto con el fin de precautelar la información que maneja la oficina principal. Al utilizar este tipo de medios para el manejo de la información, se cuenta con un alto riesgo de que la misma pueda sufrir alteraciones o pueda perderse, por lo que la implementación de una red VPN en la empresa permitirá la integración de los datos mejorando su control y protección mediante la aplicación de protocolos de seguridad, y autenticaciones de usuario, para mayor privacidad de la empresa y de los equipos informáticos con los que cuenta la oficina principal.

4.3 Solución

Como Solución del Proyecto de Investigación se propone Establecer una comunicación con los equipos Físicos de la Empresa mediante una VPN con este fin de brindar seguridad y confianza al momento de monitorear o transferir Datos. La empresa "Distribuidora Gómez" se verá beneficiada con la implementación del proyecto, ya que permitirá que la misma potencie sus procesos de ventas, de artículos de construcción y material ferretero, motivo por el que la empresa decide mejorar los procesos de control y gestión de la información de su oficina

principal optimizando los recursos existentes y agilizando los procesos de transacciones diarias de la empresa, de esta manera se proyecta un proceso de interconexión de redes la cual permita al gerente acceder a los datos de forma remota desde su hogar hacia la oficina principal de la empresa y sus demás departamentos.

Actualmente dentro de la empresa “Distribuidora Gomez” se conoce que los distintos procesos administrativos que se realizan en la oficina principal presentan un estado de potencial riesgo de pérdida y daño de la información, por lo que la gerencia de la empresa requiere un sistema de comunicación remoto el cual permita la gestión de la información desde un punto A un punto B, de manera rápida, segura y en tiempo real, siendo el campo de acción para el presente proyecto el área de informática y finanzas, impactando con la solución a estos departamentos permitiendo la interconexión entre la empresa y el hogar del gerente.

Pues tiempo atrás la red se encontraba en el siguiente estado:

4.4 Estructura de la red

Infraestructura de red compuesta por 5 pc

PC 1: Administración

PC 2: Auxiliar

PC 3: SRVDISTGOMEZ

PC 4:USER-PC

PC 5: JIMENA

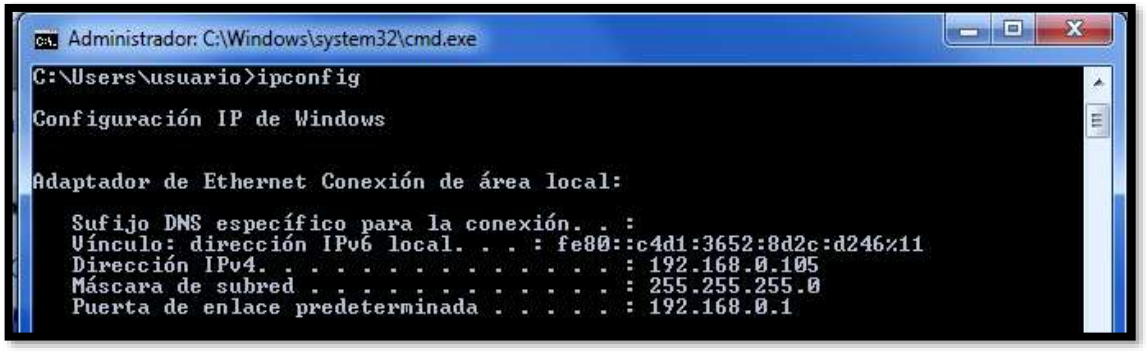
Imagen 12. Infraestructura de Red

Fuente: los investigadores

Computadores, router y dispositivos conectados en red local

4.4.1 Ip Address De La Máquina 1 o Servidor

Imagen 13. Ip address de la maquina



Fuente: los investigadores

4.4.2 Creación De Servidor Vpn En Maquina 1 Con Windows 7

Ingresando a Panel de control como siguiente las Redes e Internet para proceder a las Conexiones de Red

Imagen 14. Conexiones de red

Fuente: los investigadores

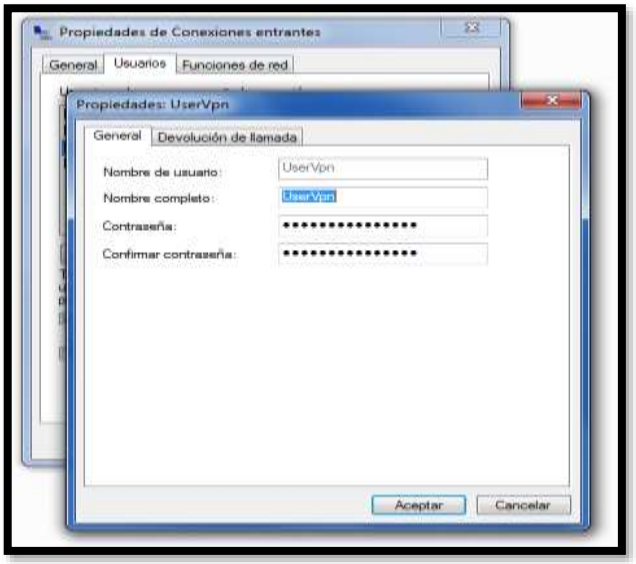
4.4.3Asignación de un usuario y contraseña para la creación del túnel VPN

De la siguiente Manera ingresamos a Propiedades de Conexiones Entrantes, Usuarios, General.

Nombre de Usuario: UserVpn

Nombre Completo: UserVpn

Imagen 15. Propiedades VPN



Fuente: los investigadores

4.4.4 Configuración del protocolo TCP 1723 y puertos de conexión para habilitar la VPN

Ingresando a Protocolos y Puertos

Escogemos TCP

Escogemos Puertos Locales y Específicos

Imagen 16. Protocolos y puertos

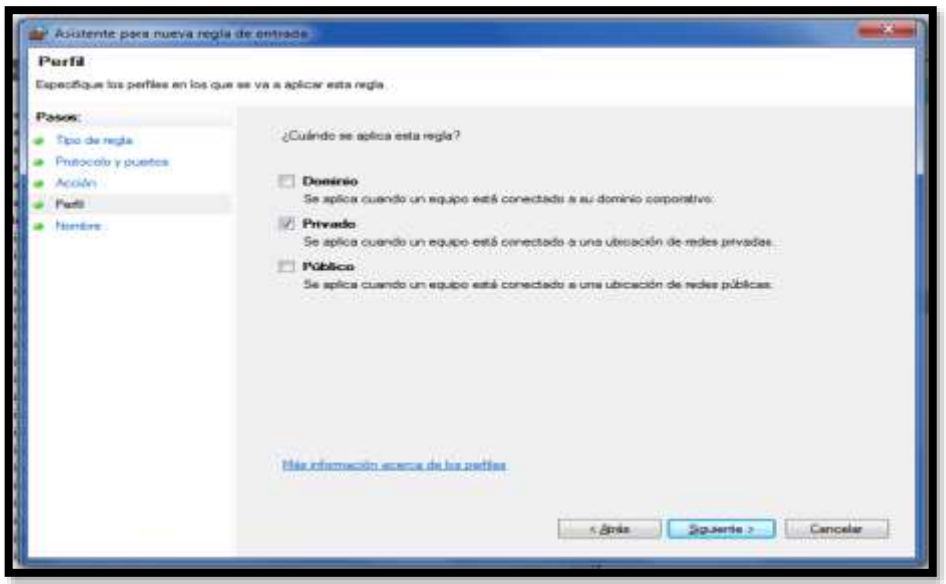
Fuente: los investigadores

4.4.5 Asignación de privacidad para la aplicación de la VPN-Asistente para nueva regla de Entrada

Perfil: Especifique los perfiles en los que se va a aplicar la regla

Privado: Se aplica cuando un equipo está conectado a una ubicación de redes privadas

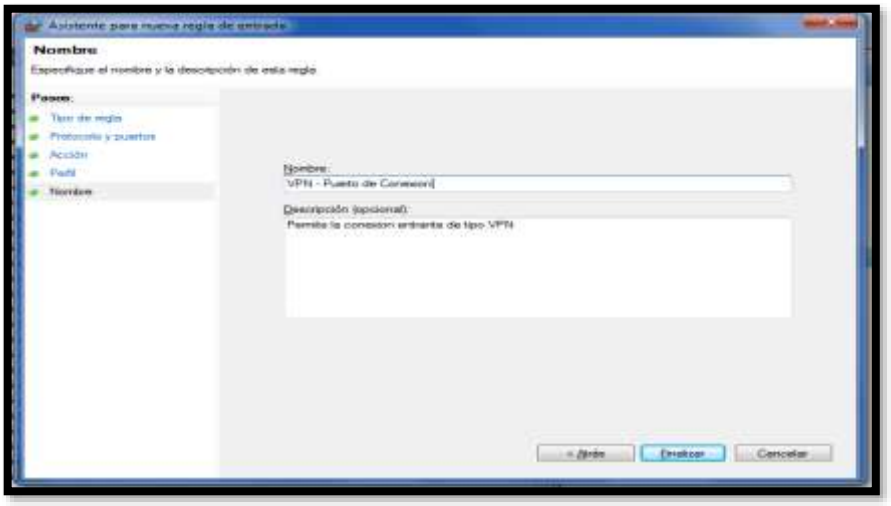
Imagen 17. Perfil



Fuente: los investigadores

4.4.6 Nombre y descripción del protocolo Tcp creado para la red

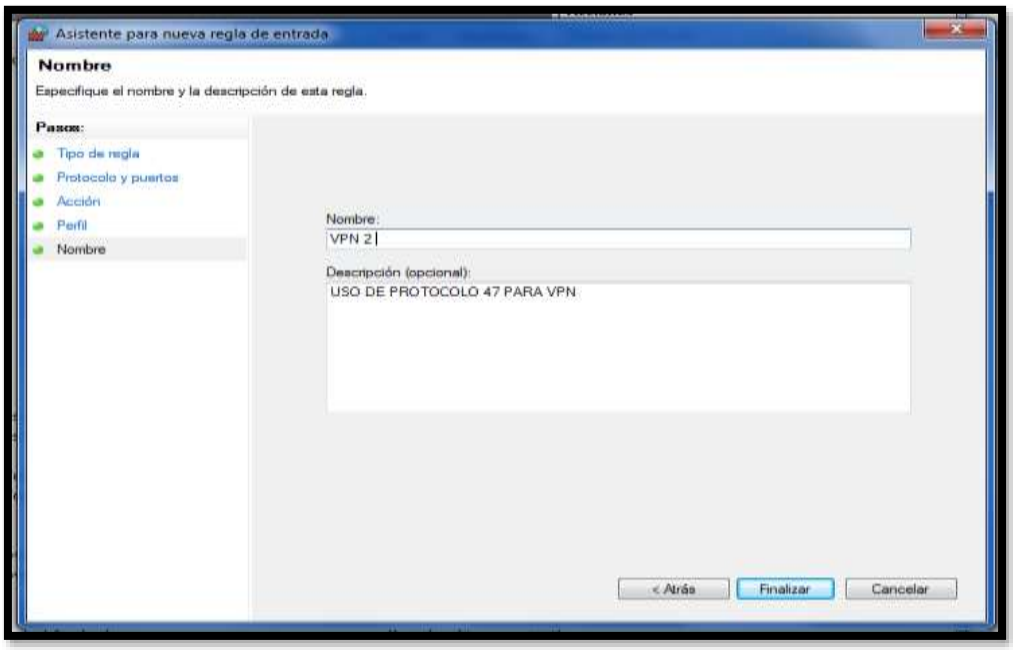
Imagen 18. Nombre y descripción VPN



Fuente: los investigadores

4.4.7 Configuración del protocolo UDP 47 para la validación de conexión

Imagen 19. Descripción de protocolo



Fuente: los investigadores

4.4.8 Configuración de reglas de acceso mediante el uso del protocolo 47 UDP en Router "EMPRESA"

Imagen 20. Activación de puertos

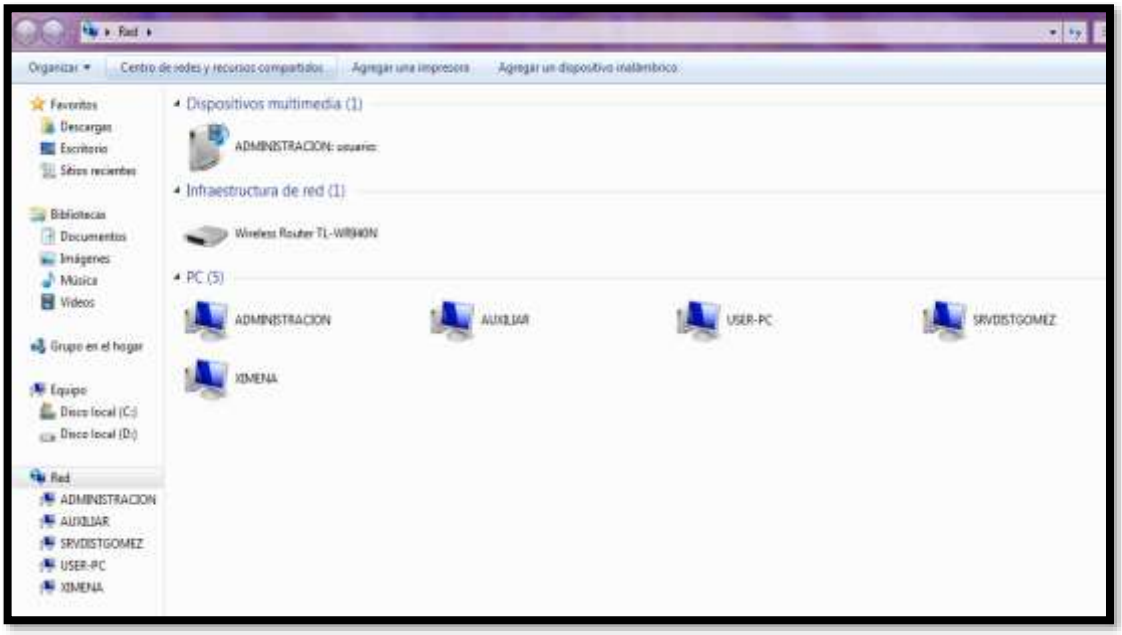
Fuente: los investigadores

4.4.9 Configuración de red en maquina 2 usuario "hogar"

Estructura de red maquina 2

PC2:Auxiliar

Imagen 21. Configuración de red



Fuente: los investigadores

4.4.10 Informacion de conexiones y redes activas

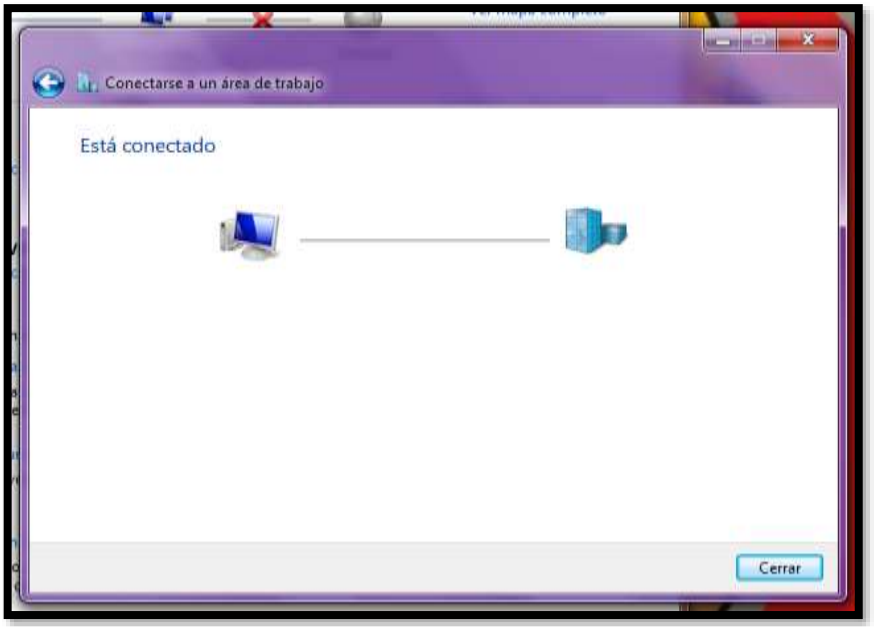
Imagen 22. Redes activas

Fuente: los investigadores

4.4.11 Conexión al servidor VPN

Estado :Conectado

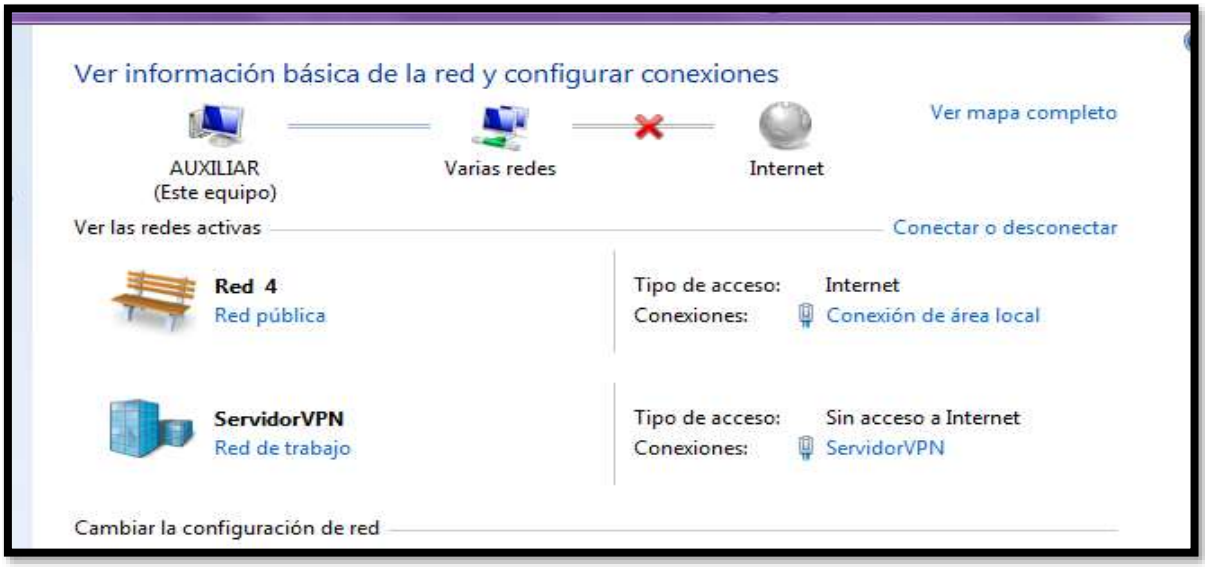
Imagen 23. Área de trabajo



Fuente: los investigadores

4.4.12 Mapa de red local conexión Servidor VPN y Usuario VPN “maquina 1” y “maquina 2”

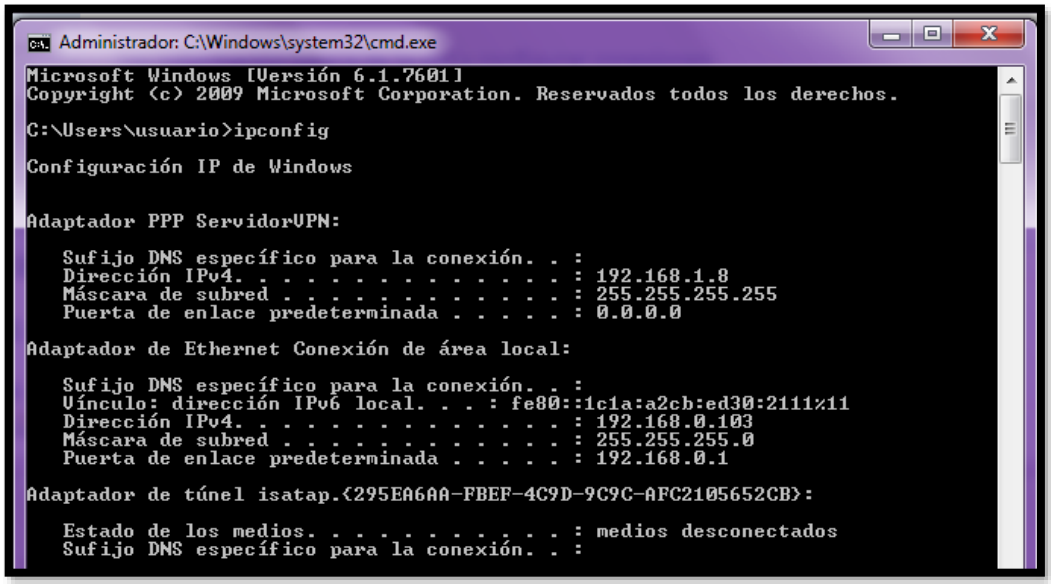
Imagen 24. Mapa de red local



Fuente: los investigadores

4.4.13 Verificación de acceso y conexión al Servidor VPN

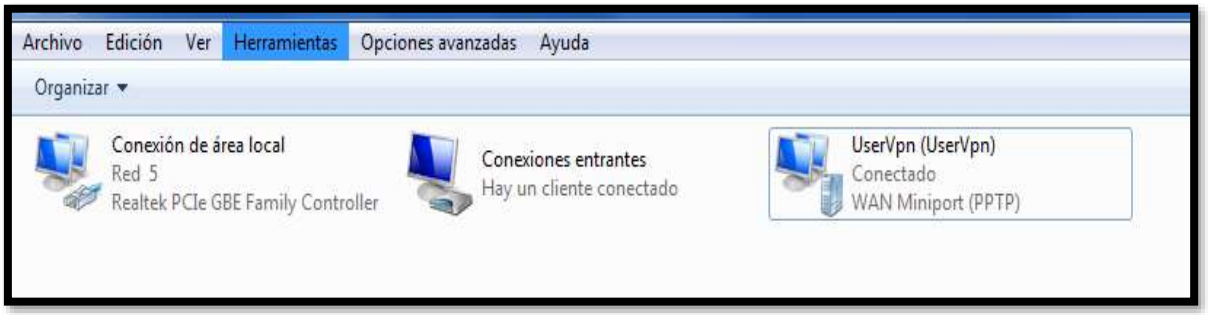
Imagen 25. Acceso y conexión al servidor



Fuente: los investigadores

4.4.14 Verificación de conexión de usuario VPN desde maquina 2 “red hogar”

Imagen 26. Red hogar



Fuente: los investigadores

4.4.15 Estado de conexión con maquina dos Cliente VPN

Imagen 27. Estado de conexión

Fuente: los investigadores

Acceso a la conexión remota mediante usuario y contraseña entre maquina 2 y servidor maquina 1

Imagen 28. Servidor VPN

Fuente: los investigadores

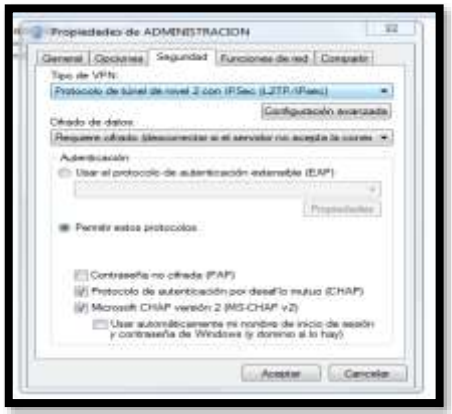
4.4.16 Validación de nivel y protocolo de seguridad IPSEC

Propiedades de Administración -Seguridad

Tipo VPN

Protocolo de túnel de nivel 2 con IPSec(L2TP/Ipsec)

Imagen 29. Propiedades de administración



Fuente: los investigadores

Error de conexión maquina 2

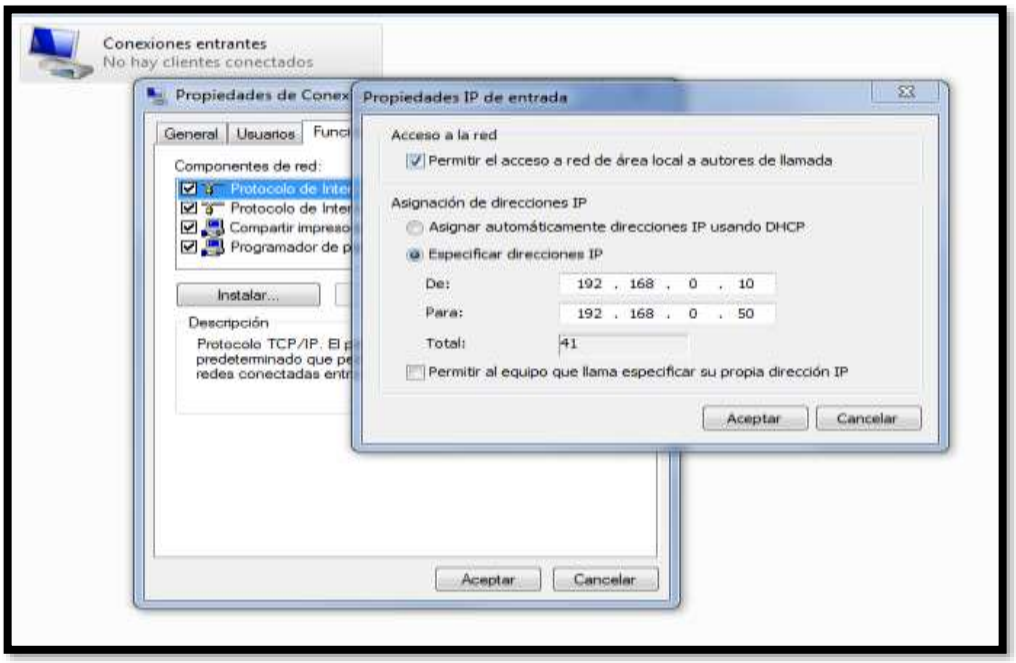
4.4.17 Dirección Ip asignada para la conexión por medio de VPN

Propiedades IP de Entrada

Permitir el acceso a Red de área local a autores de llamada

Asignación de Direcciones IP

Imagen 30. Acceso a la red



Fuente: los investigadores

4.4.18 Configuración de puertos de entrada para conexión VPN

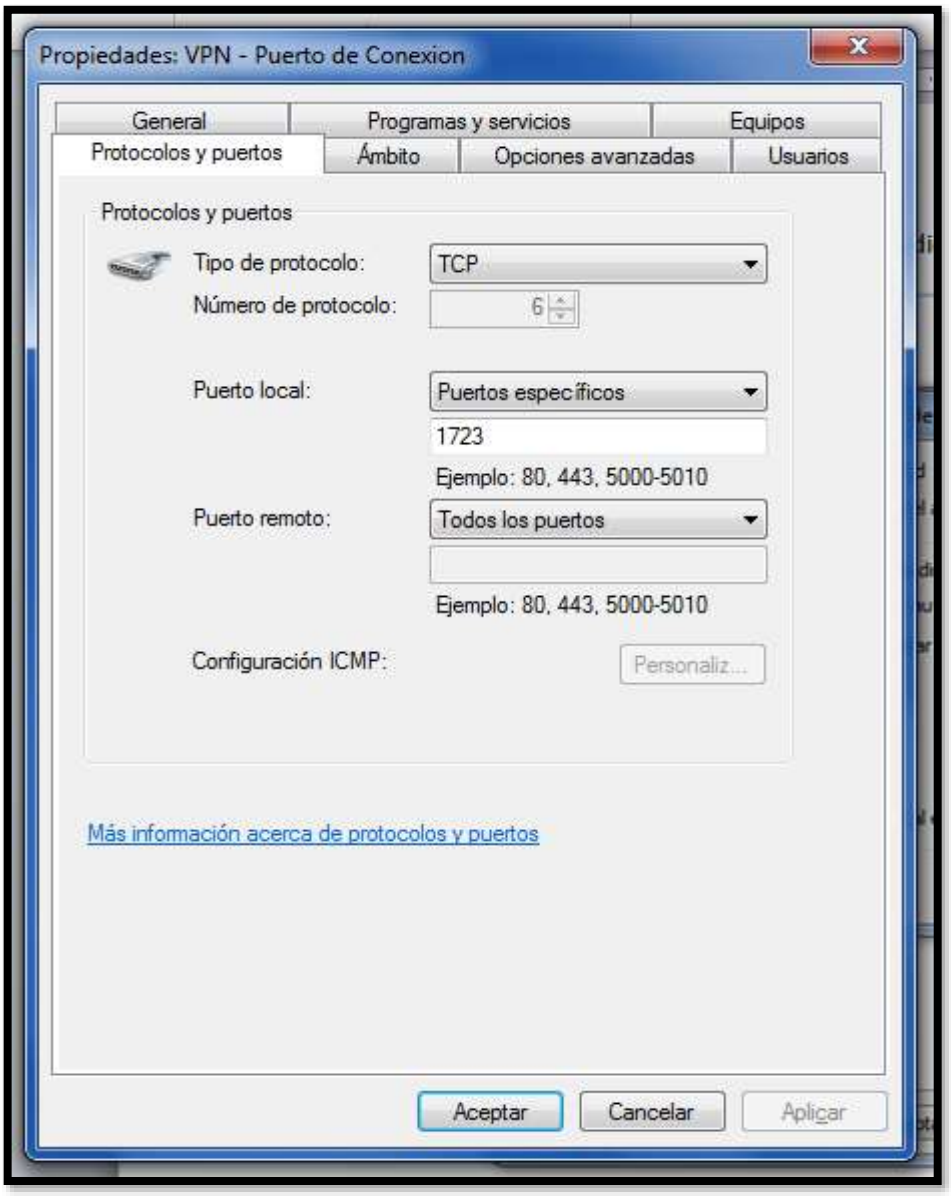
Propiedades VPN -Puertos de Conexión

General

Protocolos y Puertos

4.4.19 Tipo de Protocolo TCP

Imagen 31. Puerto de Conexión



Fuente: los investigadores

4.5 Objetivos y Entregables

- Se Implementará una red VPN que proporcione confianza y seguridad en el manejo de la información, mediante la utilización de los protocolos IPsec y TCP/IP como una alternativa para el acceso remoto a los datos de la empresa de Distribución de material de Construcción y Ferretero “Distribuidora Gómez”.

- En donde se Definen las bases teóricas para la elaboración de una propuesta mediante diagramas lógicos de red para estructurar un proceso de diseño de la VPN, determinando las características necesarias para la implementación de una red VPN.

- Determinando la metodología más adecuada para la implementación de los protocolos Ipsec para la VPN con la finalidad de mejorar la seguridad en la misma, Obteniendo una estructura básica para la implementación de una VPN

- Implementación en la red VPN en la Empresa de Distribución de material de Construcción y Ferretero “Distribuidora Gómez” para la conexión de usuarios de forma remota, detallando sobre los recursos necesarios para la VPN

4.6 TIPOS DE INVESTIGACIÓN

Para este proyecto se aplicó una metodología de investigación deductiva e inductiva para determinar y validar una estrategia de mejoramiento de la seguridad informática en la empresa “Distribuidora Gómez” por medio del uso de una Red Privada Virtual.

4.6.1 METODOS DE INVESTIGACION

4.6.1.1 Método Deductivo

El razonamiento deductivo utiliza el método deductivo que relaciona tres momentos de la deducción:

- Axiomatización (1er principio) se parte de axiomas; verdades que no requieren demostración
- Postulación se refiere a los postulados, doctrinas asimiladas o creadas
- Demostración, referido al acto científico propio de los matemáticos, lógicos, filósofos.

A pesar de sus limitaciones, es de utilidad para la investigación, ofrece recursos para unir la teoría y la observación, además de que permite a los investigadores deducir a partir de la teoría los fenómenos que habrán de observarse. Las deducciones hechas a partir de la teoría pueden proporcionar hipótesis que son parte esencial de la investigación científica.

4.6.1.2 Método Inductivo

El método inductivo se conoce como experimental y sus pasos son:

- Observación
- Formulación de hipótesis
- Verificación
- Tesis
- Ley
- Teoría.

La teoría de la falsación funciona con el método inductivo, por lo que las conclusiones inductivas sólo pueden ser absolutas cuando el grupo a que se refieran será pequeño: por ejemplo, si uno advierte que todos los alumnos de pelo rizado de un grupo escolar lograron en ortografía calificaciones superiores a las del promedio, una conclusión legítima será que todos los morenos de ese grupo muestran calificaciones superiores a las del promedio. Pero no es legítimo extraer conclusiones acerca de las calificaciones en ortografía de los pelirrojos en otros grupos ni en grupos futuros.

4.6.2 Método Empírico

4.6.2.1 Observación

A través de la Observación se planea, controla y valida la investigación, estableciendo una relación directa con los investigadores y el objeto de estudio. Para luego analizar resultados de investigación y llegar al objetivo final, en donde se mostrará efectos confiables y validados de lo observado.

4.6.2.2 Entrevista

Una Entrevista es el intercambio de ideas y opiniones, en donde se establezca una conversación entre dos o más Personas, pues las personas presentes dialogan sobre un asunto importante. Además, este método permitirá obtener como resultados opiniones, sugerencias y criterios de la Persona encargada de responder a la Entrevista. Se toma en consideración que se aplica la

entrevista a la Gerente General de la Empresa de distribución de material de construcción y Ferreteo “Distribuidora Gomez”

5. ANALISIS Y DISCUSION DE LOS RESULTADOS

5.1 ANALISIS DE LA ENTREVISTA

¿Cuál Es Su Nombre?

Mi Nombre es Zoila Jacqueline Gomez Masabanda

¿Qué Cargo Desempeña en Esta Empresa?

Actualmente soy Gerente Propietario de Distribuidora Gomez

¿Cuáles Son Los Problemas principales referentes a seguridad que la Empresa Tiene?

Principalmente tenemos el problema de los virus informáticos cuando se hace uso del navegador de internet, al igual que existe el problema del robo y filtraje de información y datos de los equipos que tenemos conectados en la red de la empresa.

¿Al navegar en internet Usted tiene acceso libre y sin restricción a chats y páginas web y otra información?

Si y esto nos presenta una dificultad, dado que los empleados hacen uso del internet y redes sociales en horas laborales, lo que crea un bajo rendimiento al momento de desempeñarse en sus labores asignadas, por lo que esto representa un problema para nosotros con nuestros trabajadores.

¿Usted Conoce lo que es una Vpn?

Si, eh escuchado que es un tipo de conexión de red que nos ayuda a proteger la información que utilizamos en los equipos y que también nos permite tener más seguridad al momento de navegar por el internet y descargar archivos desde un navegador.

¿Desearía que se realice la implementación de una Vpn en la Empresa?

Si, porque nos ayudaría a mejorar la seguridad y los respaldos de la información y del sistema contable y de inventario que manejamos dentro de nuestros equipos informáticos.

¿Conoce usted los tipos de seguridad en una Red Vpn?

No, solo conozco los aspectos básicos del funcionamiento de una red VPN.

¿Estaría de acuerdo en recibir una capacitación básica sobre el uso y aplicación de una red Vpn?

Si, porque me permitiría conocer más sobre las ventajas del uso de esta herramienta y también para poder comprender como esta queda implementada dentro de mi empresa.

5.2 ANALISIS GENERAL

5.2.1 INFRAESTRUCTURA RED ANTIGUA

Todos los empleados pueden ingresar a los datos existentes en las máquinas de la oficina principal, por lo que se conoce que existe una configuración de red local en la empresa a la que no deben tener acceso las personas que no se encuentren verificadas.

5.2.2 INFRAESTRUCTURA Y SUMINISTROS

Tabla 4. Infraestructura Física

"DISTRIBUIDORA GOMEZ"

INFRAESTRUCTURA FISICA - SUMINISTROS

Implementos	Descripción
Cable UTP	CATEGORIA 6 – IPV6
Tarjeta Ethernet	• 10/100/1000 VELOCIDAD • BANDA ANCHA
Router EMPREZA	Router d-link EGREEN: Permiten la conexióna redes de cualquier tipo (ADSL2+, VDSL2, Gigabit, E1/T1, Wifi, 3G, etc.), conexión a redes públicas analógicas odigitales (BRI/PRI)). InterfacesEthernet 10/100/1000. Seguridad (WEP/WPA/WPA2). INALAMBRICO 450MBPS
Router HOGAR	Router Jensen OF omni lite: Permiten la conexióna redes de cualquier tipo (ADSL2+, VDSL2, Gigabit, E1/T1, Wifi, 3G, etc.), conexión a redes públicas analógicas odigitales (BRI/PRI)). InterfacesEthernet 10/100/1000. Seguridad (WEP/WPA/WPA2).
Proveedor	• PUNTONET MAQUINA 1 • IP: 179.49.14.73 • WINDOWS 7
Maquina 1	• Window 7 • 32 bits core I5 • Ip: 192.168.0.108 • Disco Duro 1tb • Asus cpu

Maquina 2	• Window 7 • 32 bits core I5 • Ip: 1192.168.1.111 • Disco Duro 1tb • Asus cpu
Maquina 3	• WINDOWS 7 • 64 BITS core I5 • DNS: 192.168.0.1 • Disco Duro 1tb • ASUS CPU
Maquina 4	• WINDOWS 7 • 64 BITS core I5 • IP: 192.168.0.140 • Disco Duro 1tb • ASUS CPU

Pues tiempo atrás la red se encontraba en el siguiente estado:

5.2.3 Estructura de la red

Infraestructura de red compuesta por 5 pc

PC 1: Administración

PC 2: Auxiliar

PC 3: SRVDISTGOMEZ

PC 4:USER-PC

PC 5: JIMENA

Imagen 32. Infraestructura de Red

Fuente: los investigadores

Computadores, router y dispositivos conectados en red local

IP ADDRESS DE LA MAQUINA 1 O SERVIDOR

Imagen 33. Dispositivos conectados en red local

Fuente: los investigadores

5.2.4 INFRAESTRUTURA DE RED ACTUAL

Se Establece una comunicación con los equipos Físicos de la Empresa mediante una VPN con este fin de brindar seguridad y confianza al momento de monitorear o transferir Datos. La empresa “Distribuidora Gómez” se verá beneficiada con la implementación del proyecto, ya que permitirá que la misma potencie sus procesos de ventas, de artículos de construcción y material ferretero, motivo por el que la empresa decide mejorar los procesos de control y gestión de la información.

Tabla 5. Presupuesto para Diseño e Implementación

"DISTRIBUIDORA GOMEZ"

DISEÑO E IMPLEMENTACION

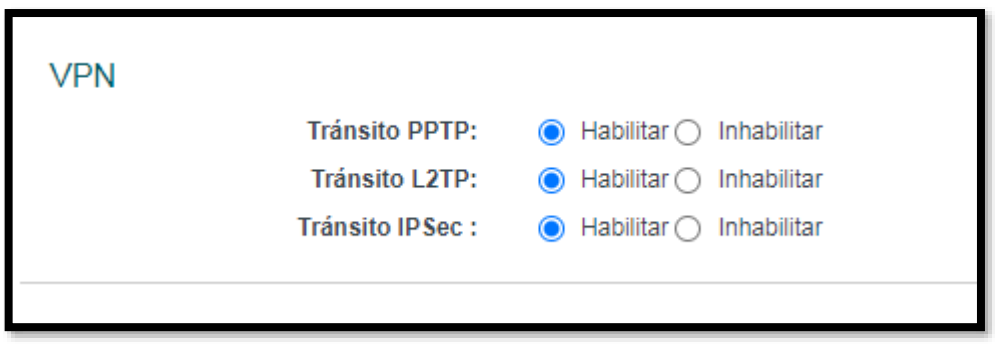
Fase	Descripción
Software	Licencia Windows 7
Sistemas Operativos	Licencia Windows 7
Protocolo de Enrutamiento	Protocolo Ipsec
VPN	Configuración del servidor yclientes VPN TUNEL ISATAP
PROTOCOLO TCP/IP	PPPoE

Fuente: los investigadores

5.2.5 CONFIGURACIÓN DE ROUTER

Procedemos a la Configuración de router empresa habilitación de protocolos de seguridad

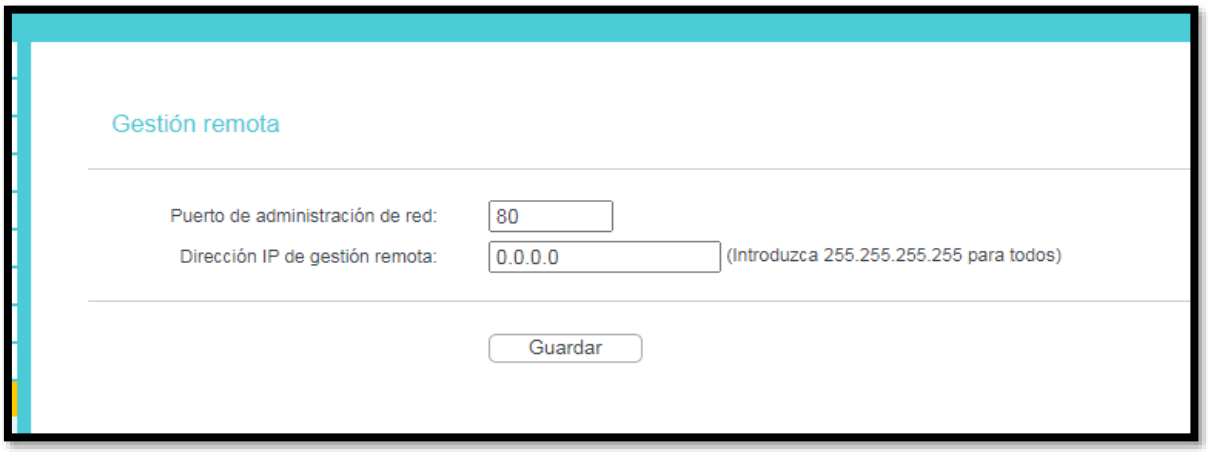
Imagen 34. Configuración de router



Fuente: los investigadores

Puertos para la gestión de conexión remota desde el servidor Vpn, para las maquinas cliente.

Imagen 35. Servidor Vpn, para las maquinas cliente



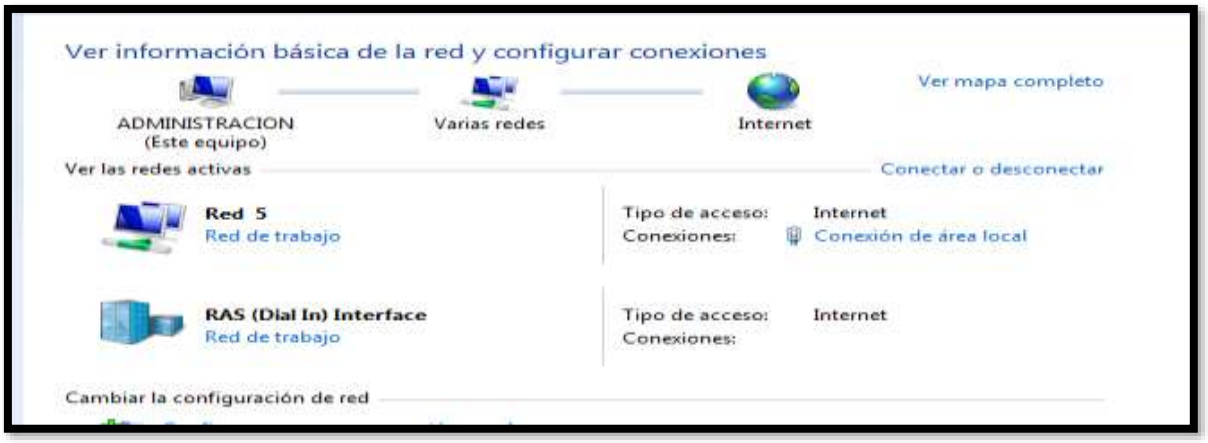
Fuente: los investigadores

Mapa de conexión maquina servidor y maquina cliente

Imagen 36. Servidor y maquina cliente

Fuente: los investigadores

Imagen 37. ***Configuración de conexión***



Fuente: los investigadores

5.2.6 MAQUINA CLIENTE -XIMENA

Conexión de red maquina cliente a máquina servidor mediante el túnel Vpn creado y uso del protocolo de seguridad Ipsec

Imagen 38. Conexión de red maquina cliente

Fuente: los investigadores

- Panel de control
- redes e Internet
- Conexiones de red

Imagen 39. Administración área local 2

Fuente: los investigadores

5.2.7 IMPLEMENTACION

Tabla 6. Presupuesto Diseño e Implementación

"DISTRIBUIDORA GOMEZ"

FASES PARA EL DISEÑO E IMPLEMENTACION

FASES PARA EL DISEÑO E IMPLEMENTACION	
FASE DE DISEÑO	Planeamiento de la red. Diseño de la red local
	Estudio de restricciones físicas yrequerimientos de los usuarios
	Definir entorno de hardware y software
	Direccionamiento IP de las Sedes

FASE DE IMPLEMENTACION	Preparación del local de instalación einstalación de la red. Instalación de la red LAN en cada sede.
	Configuración de los Dispositivos deconexión (Router, servidor, computadores)
	Configuración de los Equipos de cada sede
FASE FINAL	Capacitación de los empleados
	Administración de Red(Mantenimiento Continuo - Solución Integrada de Problemas) Semestral

Fuente: los investigadores

5.2.8 VALIDACION DE EXPERTOS

Se presenta un informe de opinión de expertos pues es una validación útil para verificar la fiabilidad de nuestro proyecto de investigación reconociendo que otros expertos cualifiquen y den su punto de vista u opinión acerca de la "IMPLEMENTACIÓN DE UNA RED VPN "VIRTUAL PRIVATE NETWORK" PARA LA MEJORA DE LA SEGURIDAD DENTRO DE LAED LOCAL INALÁMBRICA DE LA EMPRESA DE DISTRIBUCIÓN DE MATERIAL DE CONSTRUCCIÓN Y FERRETERO "DISTRIBUIDORA GÓMEZ", MEDIANTE EL USO DE PROTOCOLOS IPSEC Y TCP/IP"(se adjunta en anexos- validación de expertos).

Experto1

- Ing. Byron Paúl Yambay Quishpe

Experto 2

- Ing. Jefferson Eduardo Benavides Agua

6. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La red VPN dentro de la empresa presenta una solución en cuanto a la seguridad y protección de la información, beneficiando en el gasto en cuanto a transferencia de información entre los equipos informáticos de la oficina principal.

- Mediante la implementación de la VPN se logra la conexión de los equipos dentro de una red LAN interna en la empresa, a través de medios de autenticación los cuales proporcionen una seguridad extra en el cifrado de esta información.

- Se Cuenta con la seguridad necesarias para la protección de este tipo de información con el fin de precautelar los datos que se manejan dentro del servidor principal de la empresa, razón por la cual la VPN integra los equipos informáticos y sus redes internas mediante el uso de red "LAN" usando los recursos públicos disponibles.

RECOMENDACIONES

- Una VPN representa una gran herramienta para la solución de problemas de seguridad para las empresas por lo que se recomienda su implementación con el fin de mejorar la confidencialidad e integridad de los datos internos de la empresa.

- Si se realiza implementación de Vpn deberá analizar el esquema de la red sus interconexiones, así como también la topología de las redes, su servidor sus terminales para que en la fase final se llegue a una buena implementación, así como su funcionalidad, seguridad y política.

- Se recomienda el uso de direcciones Ip dinámicas durante la configuración de la red VPN para potenciar la escalabilidad y rendimiento de la misma de requerirse a futuro la conexión de nuevos equipos.

7. BIBLIOGRAFIA

1) (SN), México, (2018), Red Privada Virtual, Extraído de:https://www.cisco.com/c/es_mx/products/security/vpn-endpoint-security-clients/what-is-vpn.html
2) Escuela Superior de Valparaíso, (2020), Chile, El Modelo Osi, Extraído de: https://www.eiv.cl/wp-content/uploads/2020/03/4H-MODELO-OSI.pdf
3) Galarza.M, Santos. A, (SF), Ecuador, Fundamentos de Computación, Extraído de:https://www.ecotec.edu.ec/documentacion/investigaciones/estudiantes/trabajos_de_clases/1580_TRECALDE_0033.pdf
4) Universidad de Buenos Aires, (2018), Argentina, El modelo Osi, Extraído de: https://users.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf
5) Goujon.A, (2019), Que es una vpn y cómo funciona para la privacidad de la información -Extraído de:https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/
6) Alexandro G, (2018), México, Redes Privadas Virtuales, Extraído de: https://uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Redes%20privadas%20virtuales.pdf
7) Enrique V, (2018), Administración y Gestión de redes, Extraído de: http://informatica.uv.es/it3guia/AGR/apuntes/teoria/documentos/VPN.pdf
8) Solano Y, (2021), Ecuador, Análisis de las arquitecturas de conexión de Redes Privadas Virtuales VPNS para la transmisión de videoconferencia, Extraído de: http://dspace.espoch.edu.ec/handle/123456789/5596
9) Matalgah, Mustafa & Qaddour, Jihad. (2019). Remote access virtual private network architecture for high-speed wireless internet users. Wireless Communications and Mobile Computing. 4. 567 - 578. 10.1002/wcm.197.
10) Vivanco M, Percy (2019) Desarrollo de una virtual private network (VPN) para la interconexión de una empresa con sus sucursales en provincias. (Tesis para el Título de Ingeniero de Sistemas). Lima: Universidad Nacional Mayor de San Marcos.
11) Newman, D. (2018). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. Caracas, Venezuela. Extraído de: https://www.redalyc.org/pdf/761/76109911.pdf
12) Quesada, D. (2019). Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja. (Ecuador). Extraído de:

https://dspace.unl.edu.ec/jspui/bitstream/123456789/17159/1/Quezada%20Lozano%2C%20Henry%20Daniel.pdf

13) Flores, C. Sangurima, M. (2020). (Ecuador). Elaboración de un tutorial para la construcción de una red virtual privada (VPN). Extraído de: https://dspace.uazuay.edu.ec/bitstream/datos/2337/1/06838.pdf
14) S.N. (2021). Túneles VPN L2TP. Extraído de: https://www.voipdo.com/wpcontent/uploads/2018/08/VPN-L2TP.pdf
15) Vivar J. (2021). Seguridad en Ipv6 con Ipsec. Chile. Extraído de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=http%3A%2F%2Fwww.umag.cl%2Fbiblioteca%2Ftesis%2Fvivar_soto_2008.pdf&clen=516391&chunk=true
16) Moreira A.(2018).diseño de una vpn (virtual private network) para acceder vía wi-fi a la red inalámbrica de la facultad de ciencias matemáticas y físicas para la carrera de networking y telecomunicaciones de la universidad de guayaquil.extraído de:http://repositorio.ug.edu.ec/bitstream/redug/11933/1/B-CINT-PTG-N.67%20ROBINSON%20MOREIRA%20ALEJANDRO.pdf
17) Jaramillo A.(2018). Análisis comparativo entre VPN IPSEC y DMVPN (Dynamic Multipoint Virtual Private Network) para mejorar el desempeño de redes privadas sobre internet. extraido de: http://dspace.espoch.edu.ec/handle/123456789/9301
18) Ona D.(2019).análisis e implementación de una red privada virtual vpn con túneles de seguridad en el transporte de datos con un servidor centos linux: caso práctico: propuesta de implementación en la unidad de admision y nivelacion de la universidad técnica de cotopaxi - extraido de :http://repositorio.utc.edu.ec/handle/27000/3671
19) Heysen L.(2019).Implementación de una virtual private network para la interconexión de la empresa albis s.a. con sus sucursales en provincias-chiclayo extraido de : http://190.223.55.253/bitstream/UDCH/799/1/Empastado%20Tesis.pdf
20) Dordoigne .Redes informaticas Nociones fundamentales(Protocolos,arquitecturas,redes inalambricas,Virtualizacion,Seguridad disponible en :https://books.google.es/books?hl=es&lr=&id=Huwy1L0PEq8C&oi=fnd&pg=PA348&dq=protocolo+de+redes&ots=N-0o8qaTbv&sig=2qrDzd05YFmIQRfaeJT7Drc7vqM#v=onepage&q=protocolo%20de%20redes&f=false
21) Arias.J 2020.Protocolo Http disponible en :http://www.it.uc3m.es/jaf/aw/transparencias/http.pdf

22) Cobo.A 2019.Protocolo de transferencia de archivos FTP disponible en :ANGEL_LUIS_COBO_2 (csif.es)

23) Becerril .S.2019.Seguridad en el correo electrónico disponible en:FRAUDE ELECTRÓNICO (unam.mx)

24) Ona D.(2018).análisis e implementación de una red privada virtual vpn con túneles de seguridad en el transporte de datos con un servidor centos linux: caso práctico: propuesta de implementación en la unidad de admisión y nivelación de la universidad técnica de Cotopaxi - extraído de :http://repositorio.utc.edu.ec/handle/27000/3671. PAG 37

25) Nacato M.(2021).Diseño e implementación de una red privada virtual Vpn para la empresa Hato Telecomunicaciones. Disponible en Repositorio Digital - EPN: Diseño e implementación de una red privada virtual (VPN) para la empresa Hato telecomunicaciones

26) Toro H.(2018).Análisis de decisiones de inversión utilizando el criterio valor presente neto en riesgo (VPN en riesgo), disponible en: https://www.redalyc.org/pdf/430/43019324020.pdf

8. ANEXOS

ANEXO N0:1 Informe de Plagio

Ouriginal

Document Information

Analyzed document	Andaluz_Guanoluisa_Tesis.docx (D143365206)
Submitted	2022-08-29 19:02:00
Submitted by	
Submitter email	jorge.rubio@utc.edu.ec
Similarity	5%
Analysis address	jorge.rubio.utc@analysis.urkund.com

JORGE BLADIMIR RUBIO PENAHERRERA

Sources included in the report

W	URL: http://190.223.55.253/bitstream/UDCH/799/1/Empastado%20Tesis.pdf Fetched: 2022-08-29 19:04:00	2
W	URL: https://www.cisco.com/c/es_mx/products/security/vpn-endpoint-security-clients/what-is-vpn.html Fetched: 2022-08-29 19:02:00	1
W	URL: https://1library.co/document/z3do527y-estudio-tecnologias-vpn-interconexion-sitios-remotos.html Fetched: 2022-06-25 03:58:12	3
SA	**10833-Hilario Yacsavilca, Miguel Angel_.pdf** Document 10833-Hilario Yacsavilca, Miguel Angel_.pdf (D54441778)	1
SA	**Tarea+5_Ensayo+sobre+Ciberseguridad+en+los+Sistemas+de+Informaci%C3%B3n_Grupo+No.+4.pdf** Document Tarea+5_Ensayo+sobre+Ciberseguridad+en+los+Sistemas+de+Informaci%C3%B3n_Grupo+No.+4.pdf (D61633361)	1
W	URL: http://docplayer.es/161828390-Estudio-e-implementacion-de-la-red-vpn-arka-s-a-fredy-mesa-romo.html Fetched: 2022-05-29 12:57:17	1
SA	**Tesis_final_Alex_Jaramillo.docx** Document Tesis_final_Alex_Jaramillo.docx (D39303842)	1
SA	**tesis cristhian 1.docx** Document tesis cristhian 1.docx (D30484677)	2
SA	**Tesis 2.docx** Document Tesis 2.docx (D126661273)	1
W	URL: http://dspace.espoch.edu.ec/handle/123456789/5596 Fetched: 2022-08-29 19:03:00	1

Entire Document

1. INTRODUCCIÓN 2.1. EL PROBLEMA. En la actualidad la empresa "Distribuidora Gómez" cuentan con una infraestructura de red en la cual todos los empleados pueden ingresar a los datos existentes en las máquinas de la oficina principal, por lo que se conoce que existe una configuración de red local en la empresa a la que no deben tener acceso las personas que no se encuentren verificadas. Actualmente la empresa realiza sus procesos de monitoreo y transmisión de información, por medio de correo electrónico, medios de almacenamiento externo, o aplicaciones de acceso remoto con el fin de precautelar la información que maneja la oficina principal. Al utilizar este tipo de medios para el manejo de la información, se cuenta con un alto riesgo de que la misma pueda sufrir alteraciones o pueda perderse, por lo que la implementación de una red VPN en la empresa permitirá la integración de los datos mejorando su control y protección mediante la aplicación de protocolos de seguridad, y autenticaciones de usuario, para mayor privacidad de la empresa y de los equipos informáticos con los que cuenta la oficina principal.
2.1.1 Situación Problemática

ANEXO NO:2 Hojas De Vida

Anexo A: Hoja de Vida del Tutor

HOJA DE VIDA

1. DATOS PERSONALES

Apellidos: RUBIO PEÑAHERRERA	C.I.: 0502222292
Nombres: JORGE BLADIMIR **Fecha de nacimiento:** 16 DE MAYO DE 1976 **Lugar de trabajo I: Universidad Técnica de Cotopaxi**	CÓDIGO ORCID: https://orcid.org/0000-0001-9620-1437 **Lugar:** LATACUNGA **Cargo I:** Docente Investigador – Titular Agregado 1
Dirección domiciliaria: Pujilí, calle Gabriel Álvarez 1-13 y Juan José Merizalde	**Ciudad**: Pujilí
Teléfonos oficina: **domicilio:**	**Fax:**
E-mail: Jorge.rubio@utc.edu.ec	**Celular**:0995220308

2. FORMACIÓN ACADÉMICA

N°	Títulos de Pregrado	Universidad	País	Año
1	Ingeniero en Informática y Sistemas Computacionales	Universidad Técnica de Cotopaxi	**Ecuador**	2003

Nº	Títulos de Posgrado	Universidad	País	Año
1	Magister en Gerencia Informática mención Desarrollo de Software y Redes	**Pontificia Universidad Católica del Ecuador**	**Ecuador**	2010
2	Diploma Superior en Gerencia Informática	**Pontificia Universidad Católica del Ecuador**	**Ecuador**	2007

3. EXPERIENCIA PROFESIONAL

N°	EMPRESA-INSTITUCIÓN	CARGOS	DE MES-AÑO	A MES-AÑO
1	Universidad Técnica de Cotopaxi	**Docente Titular**	**12/2010**	-------
2	Pontificia Universidad Católica del Ecuador Sede Ambato	**Docente de Posgrado**	**06/2011**	**12/2018**

Anexo B: Hoja de Vida De los Investigadores

Alex Agustín Andaluz Guerrero

Edad: 26 años

0992791749 alexagu23@hotmail.com Latacunga / Cotopaxi

HABILIDADES

- Manejo del estrés y Trabajo en equipo
- Diseño de proyectos electornicos
- Conducción de vehículos

Software: Excel, Word, PowerPoint, Outlook, Photoshop, Illustrator, Wordpress, **Aplicativos de Trabajo de Adobe, Paquetes de Windows,**

Aplicativos Android, Uso de Herramientas Cisco, Linux, Arduino.

IDIOMAS

Español

Inglés

EDUCACIÓN

2011
Quito /Ecuador

Título de Maestro de Taller en Electrónica Aplicada
Colegio Técnico Electrónico Pichincha

2013
Quito / Ecuador

Título de Bachillerato en Ciencias Químico – Biológicas
Unidad Educativa Liceo Matovelle

2017
Latacunga / Ecuador

Ingeniería en Informática y Sistemas Computacionales
Universidad Técnica de Cotopaxi

EXPERIENCIA PROFESIONAL

Oct 2017 / Nov 2021
Valle de los chillos / Ecuador

Distribuidora Gómez, Empresa de Distribución de Material de Construcción y Ferretero

- Asesoria y Capacitacion del uso de Medios Tecnologicos,
- Mantenimiento Preventivo y Correctivo de Equipos de Trabajo.
- Ayudante de TI, y cobranzas.

Ene 2018 / Feb 2018
Toacaso / Cotopaxi / Ecuador

Consejo Nacional Electoral delegación Provincial de Cotopaxi

- Operador de Mesa Atención Preferente - Comicios Electorales
- Encargado de Brindar Información y Asistencia a Personas Adultas, y Tercera Edad.

Nov. 2018 – Juil. 2022
Latacunga / Ecuador

Ylax Systems, Variedades, Tecnologia y Papeleria.

Anexo C: Hoja de Vida De los Investigadores

HOJA DE VIDA

DATOS PERSONALES

NOMBRES Y APELLIDOS:	Jessica Alexandra Guanoluisa Guanoluisa
FECHA DE NACIMIENTO:	16/agosto/1994
CÉDULA DE CIUDADANÍA:	0504415431
SEXO:	Femenino
DIRECCIÓN:	Latacunga, San Felipe
TELÉFONO:	0979166662
E-MAIL:	jessica.guanoluisag1@utc.edu.ec

FORMACIÓN ACADÉMICA

PRIMARIA |	Colegio Sagrado Corazón de Jesús
SECUNDARIA|	Colegio Tecnico Luis Fernando Ruiz
	Título de bachiller gestión y organización de la secretaria.
SUPERIOR|	Universidad Técnica de Cotopaxi
	Egresada- Informática y Sistemas Computacionales

Anexo N0:3) PRESUPUESTO

9. PRESUPUESTO

Tabla 7. Gastos Directos Del Proyecto De Investigación

RECURSOS	CANTIDAD	UNIDAD	V.UNITARIO	V. TOTAL
Internet	200	horas	0.60	12.00
Impresiones	120	hojas	0.10	120.00
Cuadernos	2	unidad	1.25	2.50
Esferos	4	unidad	0.30	1.20
Carpeta	1	unidad	0.45	0.45
Routers	2	unidad	115.50	231
Flash memory	2	unidad	15	30
TOTAL				**397.15**

Fuente: los investigadores

Los Gastos Directos son los recursos necesarios que se utilizaran para el proyecto de investigación donde se muestran la cantidad de los recursos, las unidades su valor monetario, así como también el valor total de los insumos correspondientes.

Tabla 8. Gastos Indirectos Del Proyecto de Investigación

RECURSOS	CANTIDAD	UNIDAD	V.UNITARIO	V. TOTAL
Transporte	6	Pasajes	1.50	9.00
Comunicación	5	recargas	10.00	50.00
TOTAL				**59.00**

Fuente: los investigadores

Los Gastos Indirectos esta desarrollada por el transporte y la comunicación para el desarrollo del proyecto de investigación consta de cantidad, unidad, valor unitario y el total.

Gastos Generales

Tabla 9. Gastos Totales Del proyecto de Investigación

Recursos	**Presupuesto Del Proyecto De Investigación**
	Valor Totales
Gastos Directos	**397.15**
Gastos Indirectos	**59.00**
Gastos Imprevistos	**100.00**
Total	**556.15**

Fuente: los investigadores

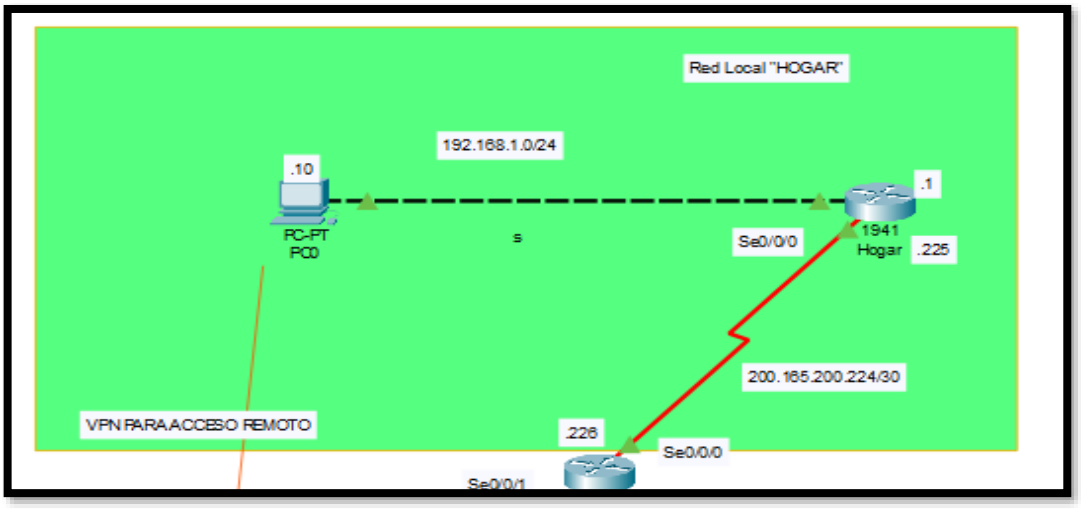
Los Gastos Generales para el proyecto de Investigación es la sumatoria de todos los insumos de gastos directos e indirectos y también se agregan los gastos imprevistos que se tendrá durante el proceso del proyecto.

ANEXO N0:4 PROTOTIPO

10. DISEÑO DEL PROTOTIPO O ESTUDIO PREVIO

1.- Estructura de la Red Local “HOGAR” diseño realizado mediante el uso del Software Cisco Packer Tracer

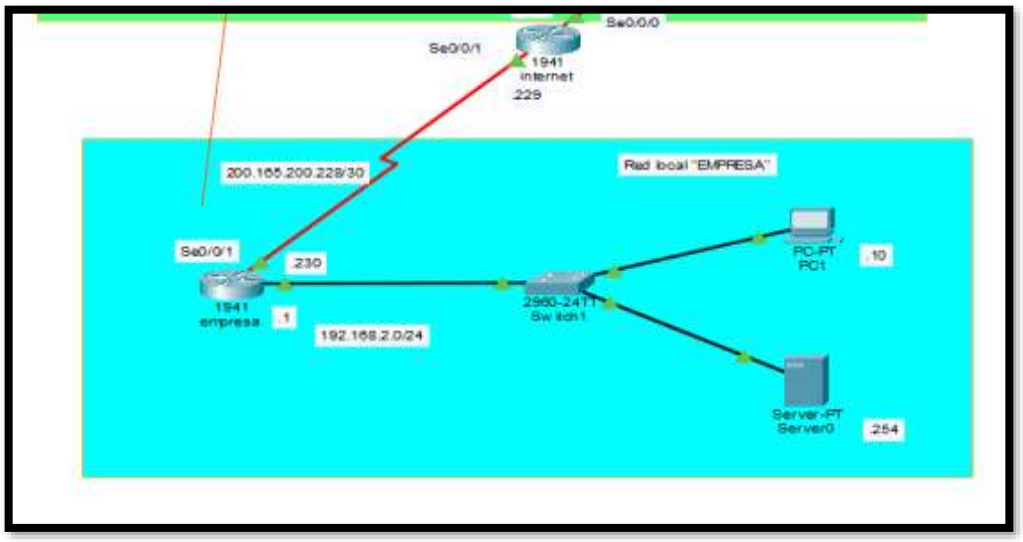
Imagen 40. Estructura de Red Local "HOGAR"



Fuente: los investigadores

2.- Estructura de la Red Local “EMPRESA” diseño realizado mediante el uso del Software Cisco Packer Tracer.

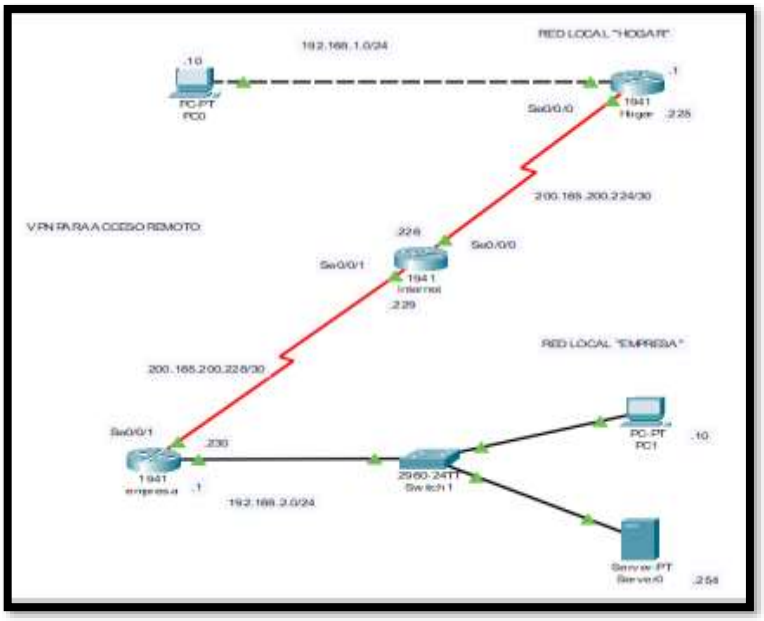
Imagen 41. Estructura de Red Local "Empresa"



Fuente: los investigadores

3.- Estructura Completa de la Red Local diseñada para la implementación de la VPN

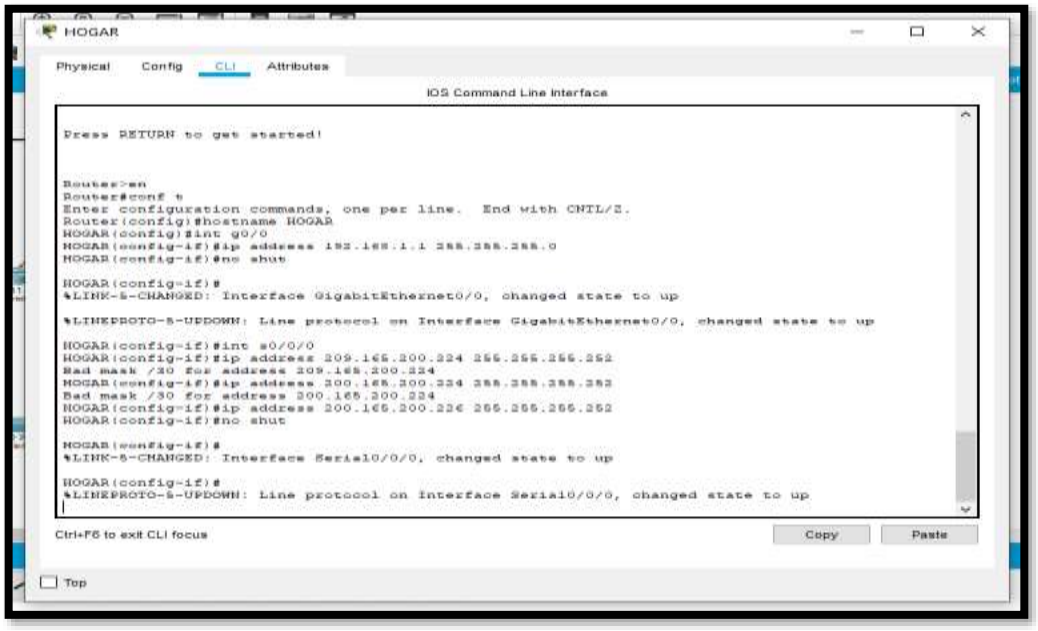
Imagen 42. Estructura de Red Completa para implementación de VPN



Fuente: Autores

4.- Configuración del Router "HOGAR" asignación de direcciones IP.

Imagen 43. Configuración Router "HOGAR"



Fuente: los investigadores

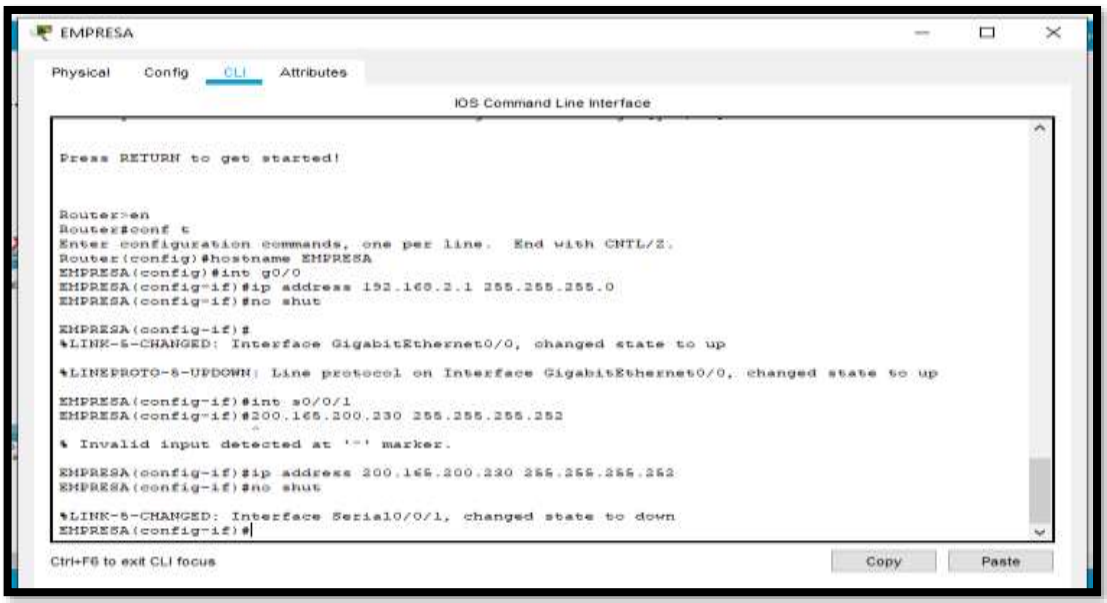
5.- Configuración del Router “Internet” el cual permitirá posterior a su configuración la implementación de la VPN

Imagen 44. Configuración Router "INTERNET"

Fuente: los investigadores

6.- Configuración del Router “EMPRESA”

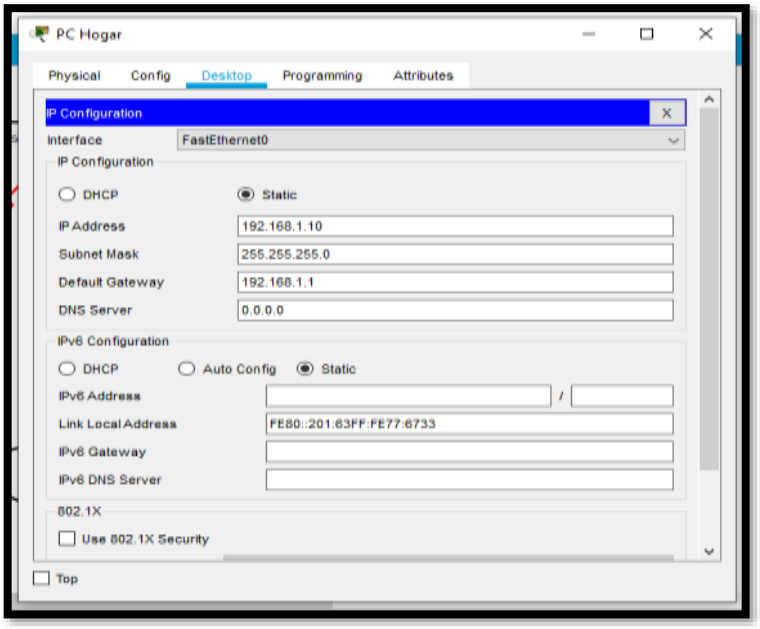
Imagen 45. Configuración del Router "EMPRESA"



Fuente: los investigadores

7.- Configuración de las maquina PC Hogar, para el Administrador de la empresa.

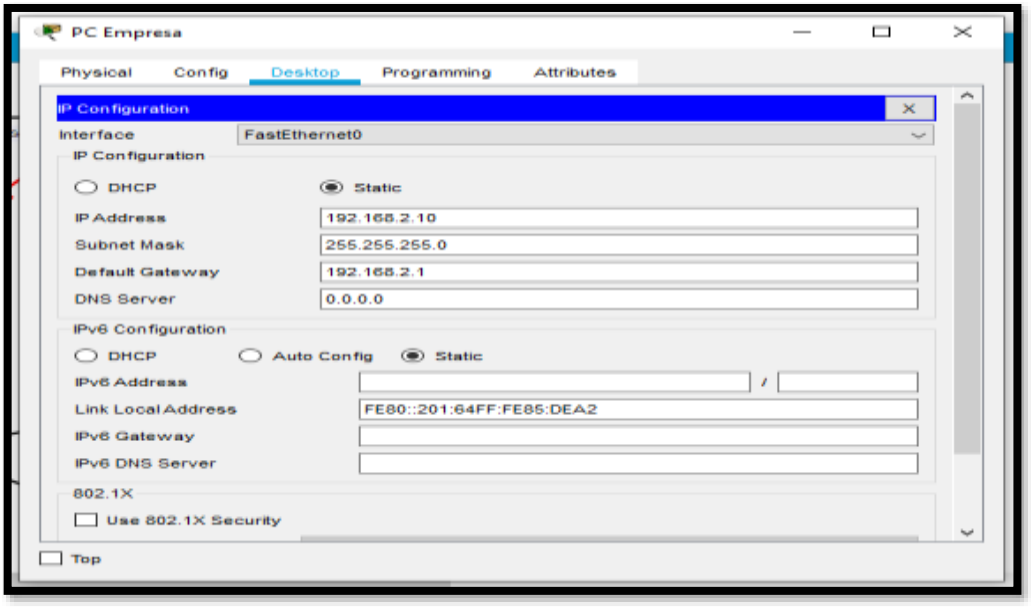
Imagen 46. Configuración Maquina PC Hogar



Fuente: los investigadores

8.- Configuración de la PC Empresa, la cual permitirá el acceso a la secretaria encargada de la oficina principal.

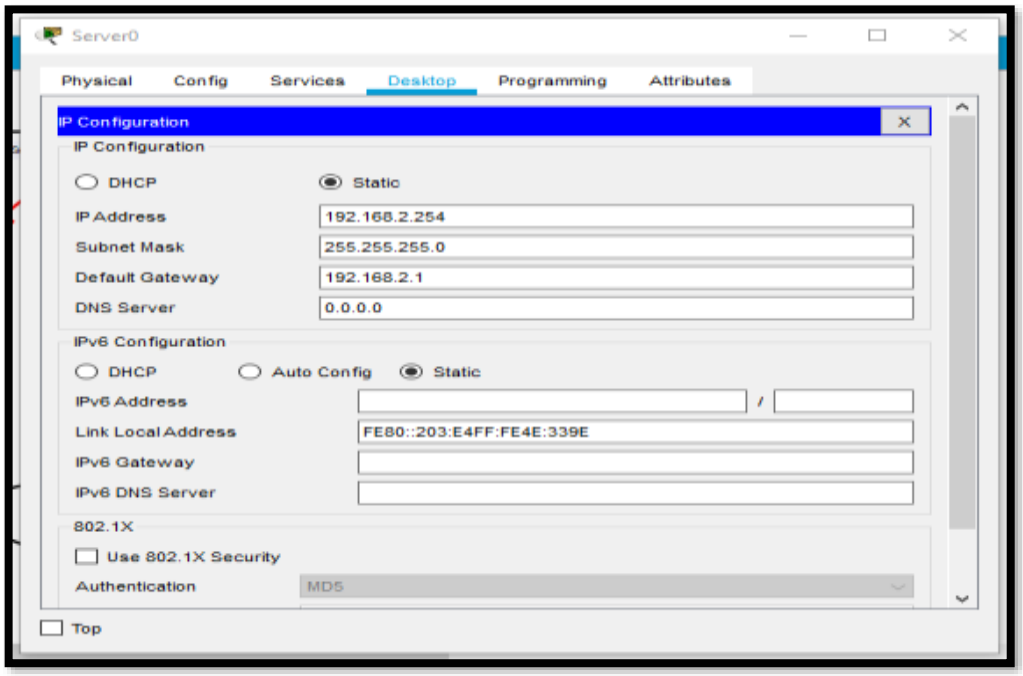
Imagen 47. Configuración PC Empresa



Fuente: los investigadores

9.- Configuración del Servidor principal de la empresa, el cual también maneja un sistema de cámaras de vigilancia.

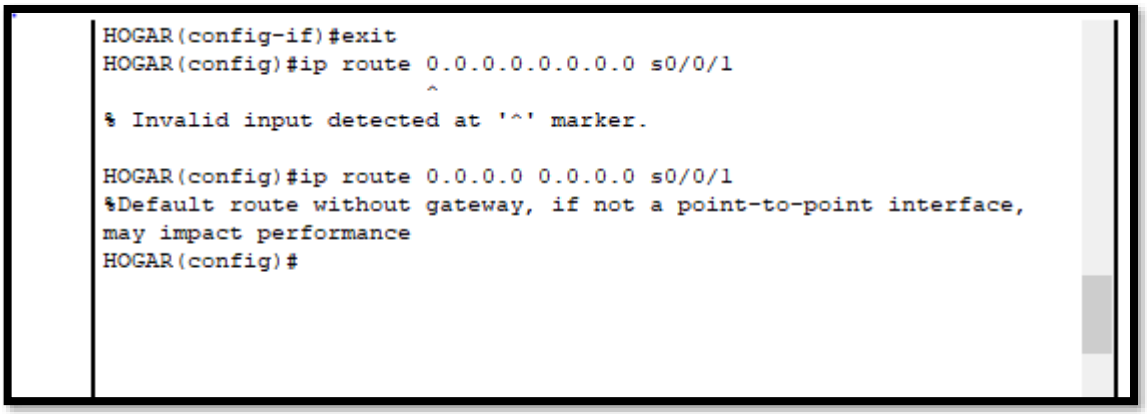
Imagen 48. : Configuración del Servidor Empresarial



Fuente: los investigadores

10.- configuración de una ruta por defecto para el Router HOGAR

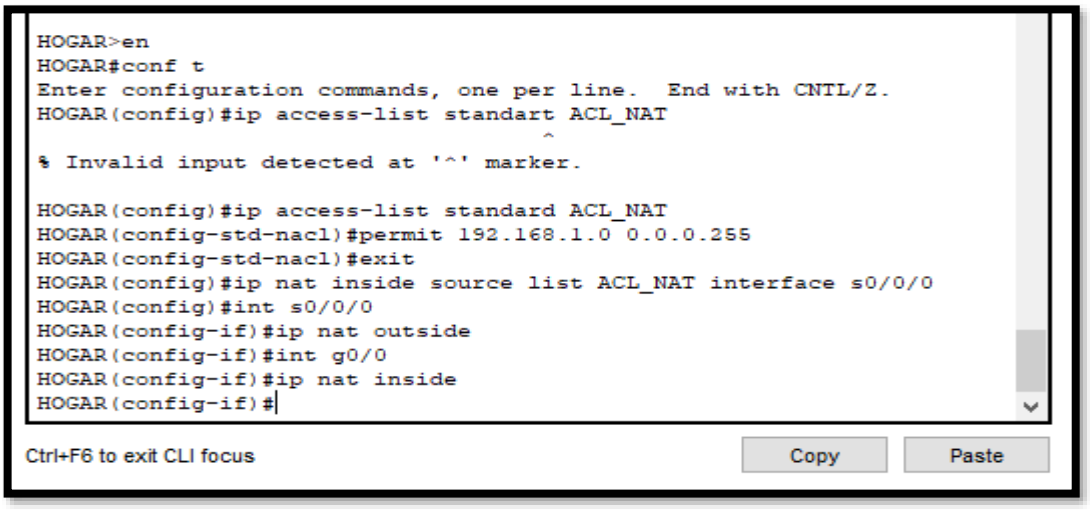
Imagen 49. Configuración de Ruta por defecto



Fuente: los investigadores

11.- Creación y validación de una lista de acceso a la red local otorgando permisos de conexión a la IP (192.168.1.0)

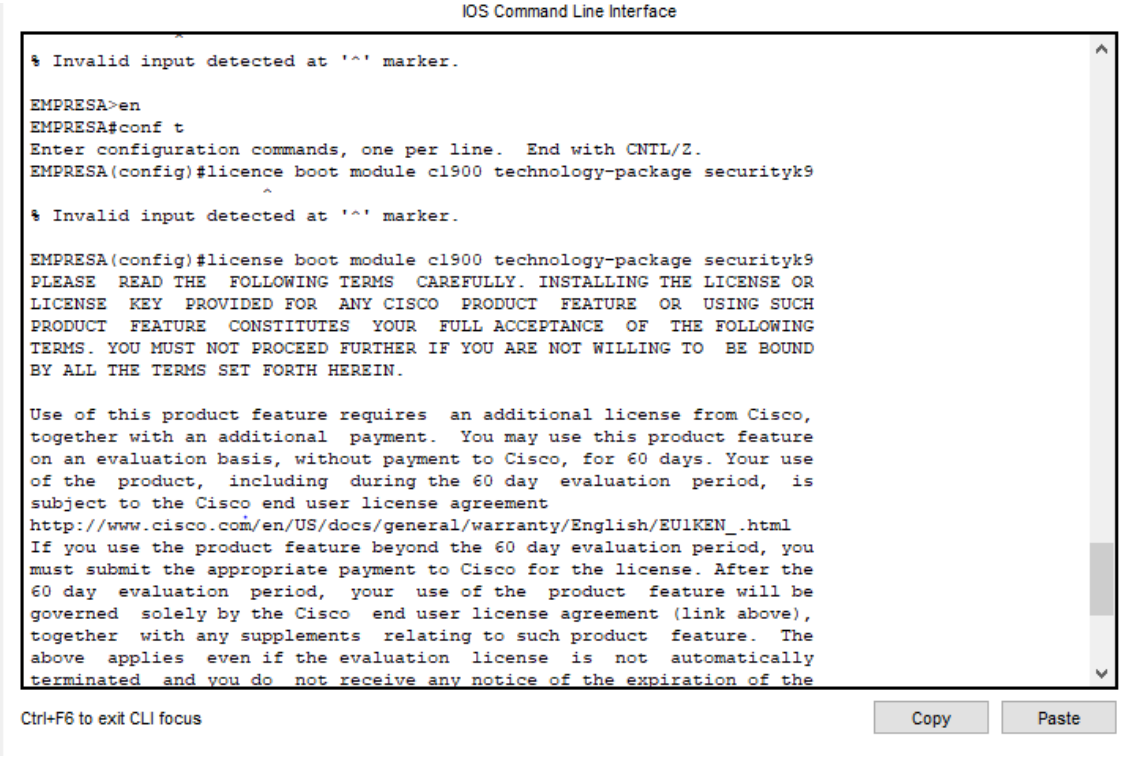
Imagen 50. Creación y Validación de Lista de acceso



Fuente: los investigadores

12.- validación de licencia de seguridad para el correcto funcionamiento de la VPN

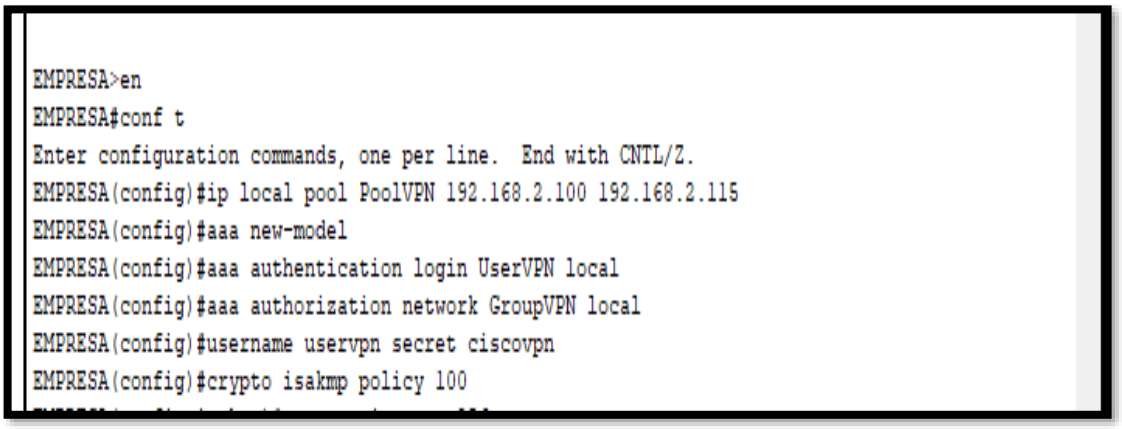
Imagen 51. Activación licencias de seguridad



Fuente: los investigadores

12.- configuración de la IP local y creación de la autenticación “Usuario”,” Contraseña” para el uso mediante la VPN

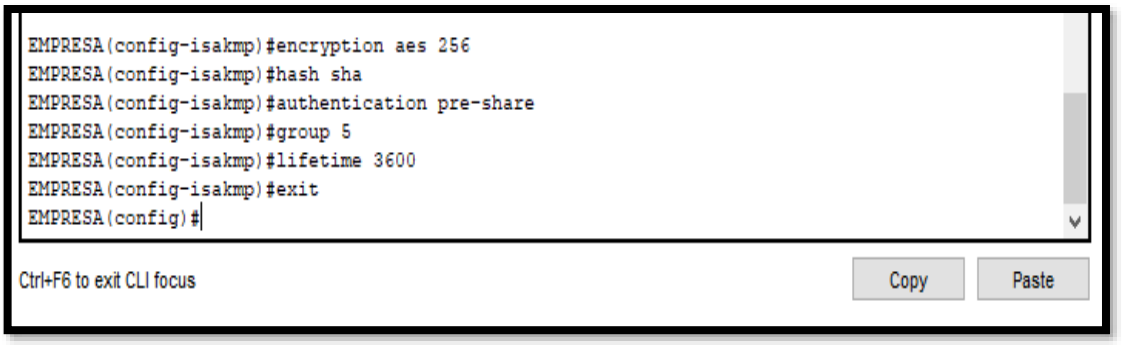
Imagen 52. Creación de autenticación "Usuario" y "Contraseña"



Fuente: los investigadores

13.- creación del método de encriptación para la seguridad de la VPN

Imagen 53. Método de Encriptación



Fuente: los investigadores

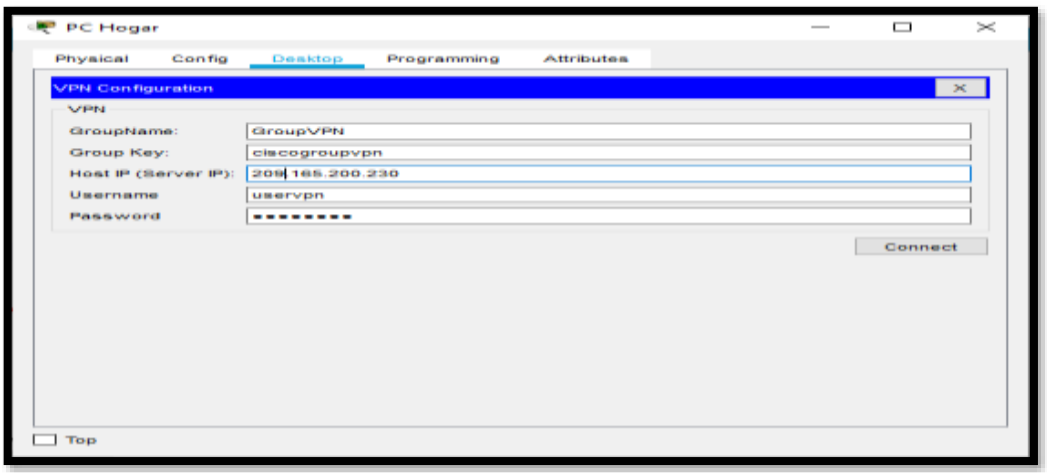
14.- configuración del del cliente mediante el método ISAKMP

Imagen 54. Configuración del Cliente VPN uso de método ISAKMP

Fuente: los investigadores

15.- Acceso a la VPN mediante las autenticaciones creadas “usuario”,” contraseña” en la maquina PC HOGAR.

Imagen 55. Acceso a la VPN



Fuente: los investigadores

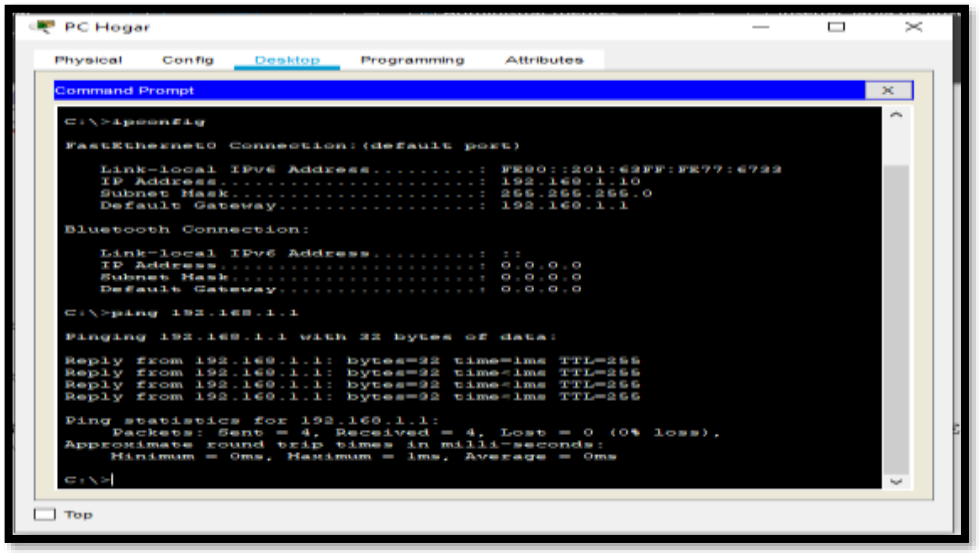
ANEXO N0:05 PRUEBAS

PRUEBAS DE FUNCIONAMIENTO

1.- Paso 1

1.1.- Prueba de conexión se realiza un ping a la IP (192.168.1.1) de la máquina PC Hogar.

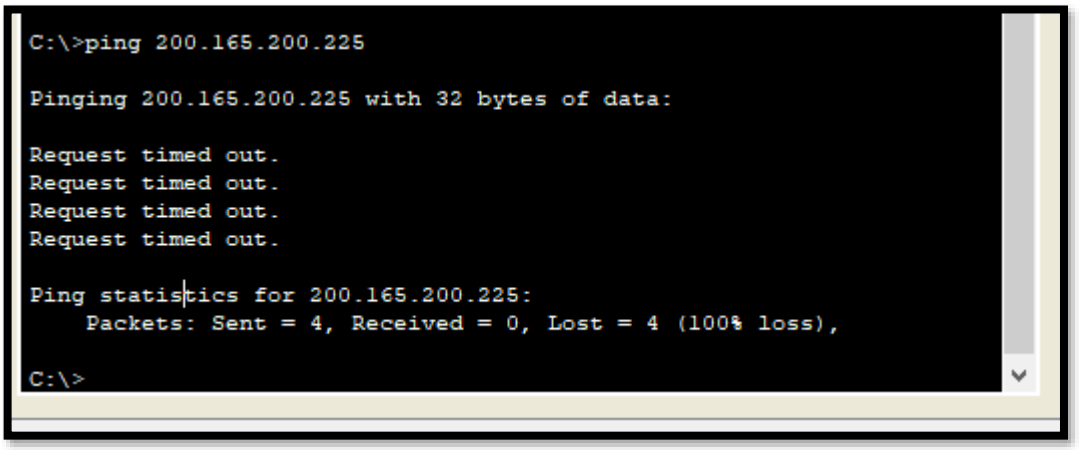
Imagen 56. Prueba mediante ping en la PC HOGAR



Fuente: los investigadores

1.2.- Prueba de conexión se realiza un ping a la IP (200.165.200.225) del router Internet con el fin de verificar si existe conexión. Con error.

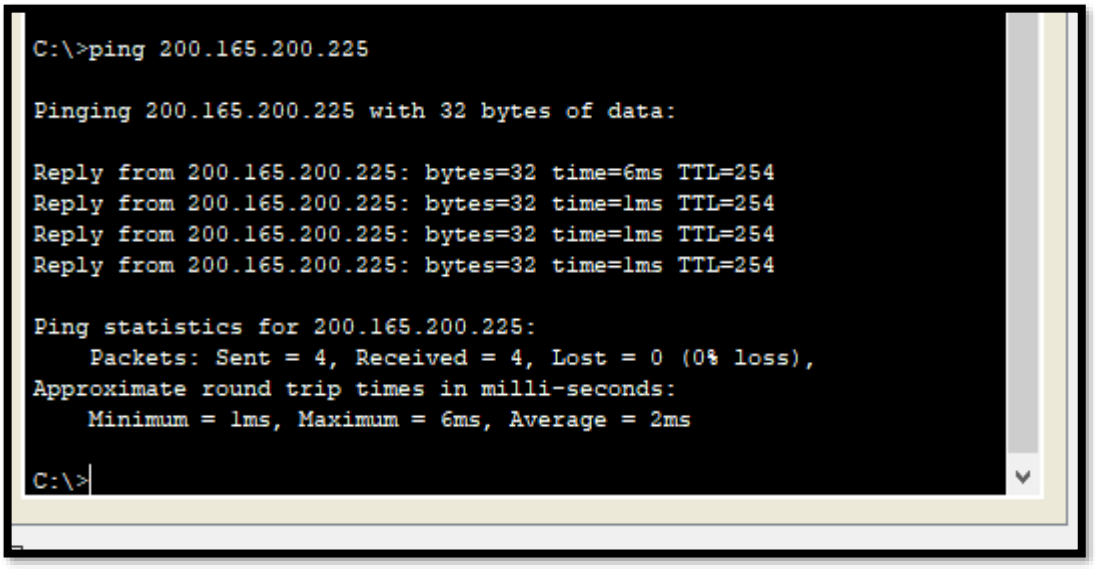
Imagen 57. Prueba de conexión estado Fallido



Fuente: los investigadores

1.3.- Prueba de conexión se realiza un ping a la IP (200.165.200.225) del router Internet con el fin de verificar si existe conexión después de haber creado y permitido el uso de una lista de acceso. Sin error de conexión.

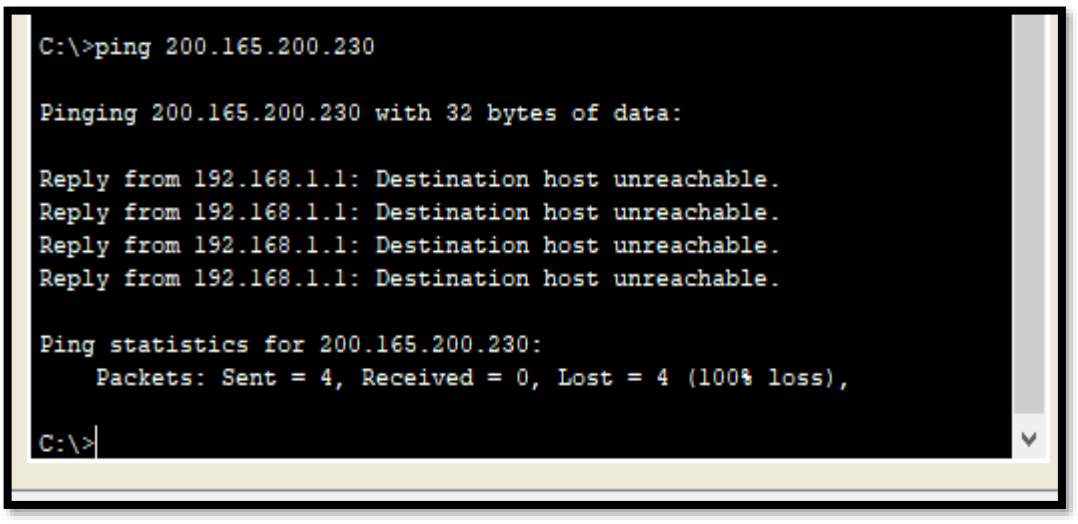
Imagen 58. Prueba de conexión estado Exitoso



Fuente: los investigadores

1.4.- Prueba de conexión se realiza un ping a la IP (200.165.200.230) del router Internet con el fin de verificar si existe conexión después de haber creado y permitido el uso de una lista de acceso.

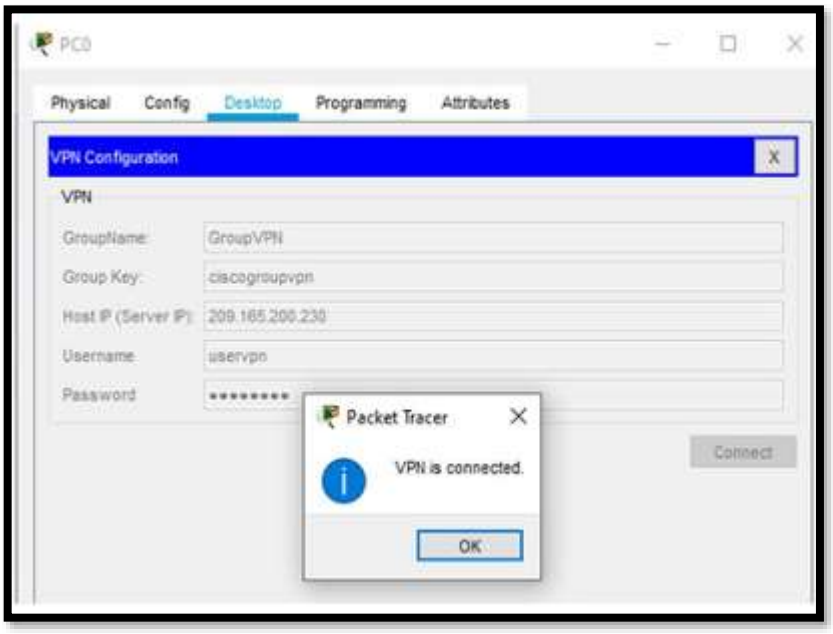
Imagen 59. Prueba de Ping



Fuente: los investigadores

1.5.- Prueba de conexión después de la implementación del método ISAKMP para la aplicación de la VPN.

Imagen 60. Estado de conexión VPN



Fuente: los investigadores

ANEXO N0:06 VALIDACIONES

11. VALIDACION DE EXPERTOS

Anexo 1. Validación de expertos

INFORME DE OPINIÓN DE EXPERTOS

1. DATOS GENERALES:

- **Nombres del Experto:**

  Byron Paúl Yambay Quishpe

- **Grado Académico.**

  Superior

- **Profesión:**

  Ingeniero Informática en Sistemas Computacionales

- **Institución donde labora:**

  Yambay y Asociados

- **Cargo que desempeña:**

  Trabajador Independiente

2. TEMA DE INVESTIGACIÓN A VALIDAR

Implementación de una Red VPN "Virtual Private Network" para la mejora de la seguridad dentro de la red local inalámbrica de la Empresa de distribución de material de Construcción y Ferretero "Distribuidora Gómez", mediante el uso de protocolos Ipsec y Tcp/Ip.

3. TABLA DE VALIDACIÓN

INDICADORES DE EVALUACIÓN	CRITERIOS	Muy Malo	Malo	Regular	Bueno	Muy Bueno
		1	2	3	4	5
1. Claridad de la investigación	Está formulada con un lenguaje apropiado que facilita su comprensión.					5
2. Objetividad de la Investigación	Está expresada en conductas observables y medibles.					5

3. Consistencia de la Investigación	Existe una organización lógica en los contenidos y relación con la teoría					5
4. Coherencia de la Investigación	Existe relación de los contenidos con las metodologías de investigación					5
5. Pertinencia de la Investigación	Existe pertinencia de la investigación con la realidad de las VPNs.					5
	La Investigación proporciona acceso a la tecnología actual					5
	La Investigación proporciona nuevos conocimientos en lo referente a Redes e Infraestructura					5
	La Investigación permite la implementación de modelos y técnicas seguridad Informática					5
	SUMATORIA PARCIAL	0	0	0	0	40

SUMATORIA TOTAL	**40**

RESULTADOS DE LA VALIDACIÓN

Valoración total cuantitativa: 40

Opinión: FAVORABLE ____**X**_____ DEBE MEJORAR _____

NO FAVORABLE _____

OBSERVACIONES

Se evidencia que el proyecto está bien estructurado, al igual que la implementación dentro de la empresa, se considera que es un gran aporte en la mejora de la seguridad de la red y equipos informáticos.

Firma:

Byron Paúl Yambay Quishpe

C.c:060301384-8

Anexo 1. Validación de expertos

INFORME DE OPINIÓN DE EXPERTOS

1. DATOS GENERALES:

- **Nombres del Experto:**

  Jefferson Eduardo Benavidez Agua

- **Grado Académico.**

  Superior

- **Profesión:**

  Ingeniero en Informática y Software.

- **Institución donde labora:**

  MR.TONER .

- **Cargo que desempeña:**

  Trabajador Independiente Gerente Propietario.

2. TEMA DE INVESTIGACIÓN A VALIDAR

Implementación de una Red VPN Virtual Private Network, para la mejora de la seguridad dentro de la red local inalámbrica de la Empresa de distribución de material de Construcción y Ferretero "Distribuidora Gómez", mediante el uso de protocolos Ipsec y Tcp/Ip.

3. TABLA DE VALIDACIÓN

INDICADORES DE EVALUACIÓN	CRITERIOS	Muy Malo	Malo	Regular	Bueno	Muy Bueno
		1	2	3	4	5
1. Claridad de la investigación	Está formulada con un lenguaje apropiado que facilita su comprensión.					5
2. Objetividad de la Investigación	Está expresada en conductas observables y medibles.					5

3. Consistencia de la Investigación	Existe una organización lógica en los contenidos y relación con la teoría					5
4. Coherencia de la Investigación	Existe relación de los contenidos con las metodologías de investigación					5
5. Pertinencia de la Investigación	Existe pertinencia de la investigación con la realidad de las VPNs.					5
	La Investigación proporciona acceso a la tecnología actual					5
	La Investigación proporciona nuevos conocimientos en lo referente a Redes e Infraestructura					5
	La Investigación permite la implementación de modelos y técnicas seguridad Informática					5
SUMATORIA PARCIAL		0	0	0	0	**40**
SUMATORIA TOTAL		**40**				

RESULTADOS DE LA VALIDACIÓN
Valoración total cuantitativa: 40

Opinión: FAVORABLE ____**X**_____ DEBE MEJORAR _____

NO FAVORABLE _____

Observaciones:

Es un proyecto interesante y a futuro se aconseja desarrollarlo más ampliamente y proyectarse a instituciones públicas y privadas.

Firma:

Jefferson Eduardo Benavides Agua

CC.: 0201889599